REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Mouloud Mammeri de Tizi-Ouzou
Faculté de génie électrique et d'informatique
Département d'informatique

Mémoire de fin d'études

En vu de l'obtention du diplôme de master (LMD) en informatique

Thème

Conception et réalisation d'un cryptosystème biométrique pour l'authentification

Dirigé par :

Mme Ferhaoui CHERIFFI

Réalisé par :

MAWUENA RUKUNDO Aristide Alexis

Promotion 2016-2017

REMERCIEMENT

Je tiens avant tout à remercier le Très Haut qui m' a donné la volonté et le courage pour la réalisation de ce travail et sans qui je n'en serais certainement pas là. "Que le nom de l'Eternel soit béni, Dès maintenant et à jamais!".

Je remercie vivement Mme Ferhaoui CHERIFFI, ma promotrice pour l'assistance et la disponibilité qu'elle m'a accordé tout au long de la rédaction de ce mémoire et de mon travail de recherche.

Que les membres de jury trouvent ici l'expression de mes sincères remerciements pour l'honneur qu'ils me font en acceptant de juger mon modeste travail.

Je remercie très particulièrement la Communauté des PERES BLANCS de Tizi-Ouzou pour leurs patiences à mon égard, pour leurs encouragements, surtout pour tous ce qu'ils ont fait et pour tous les moyens mis à ma disposition pour que je puisse effectuer mes recherches et travailler sereinement.

J'aimerai profiter de l'occasion pour exprimer ma gratitude particulière envers tous les membres de ma famille et spécialement ma maman et tous mes amis qui m'ont soutenu et encourager.

DU PLUS PROFOND DE MON CŒUR, MERCI!!!

Dédicaces

Je dédie ce travail à :

Toute ma famille et spécialement à ma maman extraordinaire, mais également à toute ma famille à Tizi-Ouzou. Pour leurs réconforts moral et psychologiques.

A tous mes amis qui sont toujours auprès de moi et qui m'ont encouragés dans ce travail des fois même sans en comprendre les difficultés ou même en étant loin de moi.

A mes pères préférés Guy SAWADOGO, René MOUNKORO et Vincent KIYEREREZI.

A mon pays le Burundi et à l'Algérie. A tous ceux qui ont contribués de près ou de loin à mon éducation et qui ont contribuer à faire de moi celui que je suis devenu.

A toutes ces personnes, burundaises, algériennes et de partout ailleurs, qui ont fait de mon séjour en Algérie un moment appréciable, qui m'ont enrichi par leurs cultures et leurs façons de penser.

A tous mes promotionnels, mais également à tous ceux qui ont contribués de prés ou de loin à la réalisation de ce modeste travail.

MAWUENA RUKUNDO Aristide Alexis

Table des matières

Table des figures

Liste des tableaux

INTRODUCTION GENERALE

Il est facile d'observer la façon dont le besoin de sécurité de l'homme évolue très vite vers la hausse. Il suffit d'observer toutes les solution de sécurisation offerte et cela quelque soit le champ d'application de cette sécurité. Il y'a trente à vingt ans, par exemple, il fallait être lourdement armée pour dérober de l'argent dans une banque, de nos jours une personne compétente peut commettre un délit du même ordre avec un ordinateur est une connexion internet.

En informatique ce besoin de sécurité n'est pas en reste. Pour répondre à ce besoin de sécurité, il faut être en mesure d'assurer certain service tel que la capacité à reconnaitre des individus de façon sûre, sécurisé des transactions, protéger des systèmes informatique d'une mauvaise utilisation, d'une panne etc.

Pour reconnaitre quelqu'un de façon sécurisé, de nombreux moyen ont été mis au point tel que la possession d'un document (passeport, carte bancaire, etc), ou la connaissance d'une information (mot de passe, schéma etc.). Ces deux méthodes, les plus répandues, ne sont cependant pas efficaces contre la fraude car elles présentent l'inconvénient d'utiliser des identifiants externes qui peuvent être dérobés ou être perdus. Une solution à ce problème est la biométrie.

La biométrie est un moyen de se faire reconnaitre qui ne peut se perdre et qui est difficilement falsifiable car elle est basée sur des identifiants internes qui représentent ce que nous sommes (ADN etc.) ou qui représentent notre façon de faire les choses (démarche, signature, etc.).

Un système biométrique peut être considéré comme un système de traitement de signal [1] avec une architecture de reconnaissance de formes. Il capte le signal biométrique, le traite puis extrait un ensemble de caractéristiques représentatives appelées modèle biométrique [1](biometric template) qui seront ensuite comparées à un modèle préalablement stocké sur une base de données.

Malgré les avantages des systèmes biométriques, des questions sur la sécurité des systèmes biométriques se posent. Le stockage des modèles biométriques de référence pose de sérieux problèmes de sécurité: manipulation d’informations sensibles, reconstruction de la biométrie d’origine à partir du modèle stocké, construction d’un échantillon biométrique falsifié ou l’impossibilité de révoquer l’identifiant biométrique lorsqu’un vol d’identité à eu lieu.

Techniquement nous pouvons résumé les vulnérabilités de ces systèmes à ceci: les modèles biométriques sont enclin à quelques variations dues aux temps (changement de la formes du visages avec l'âge, pousse de barbe), dues également aux captures de

caractéristiques qui se font dans des conditions souvent très différentes (luminosité, angle de capture, etc.). A cause de ces légères variations il est impossible de lui appliqué les protections traditionnelles tel que le hachage sur les mots de passe (car la moindre variation par rapport au modèle de référence engendrerai un défaut de reconnaissance dans le cas d'un hashage).

La question qui se pose est donc, comment protéger des données biométriques de façon à ce qu'elles soit utilisable pour la reconnaissance sans pour autant qu'elles puissent compromettre l'utilisateur?

Cette question implique qu'il faudrait rechercher des solutions techniques , qui compléteraient la technologie biométrique, afin de protéger les données de référence. Toutefois, il faut évaluer à quel point la préservation de la vie privée par ces techniques additionnelle affecte les performances de reconnaissance. Car les objectifs de sécurité et de vie privée sont souvent contradictoires et l'un des défis majeurs est de garantir une somme positive entre les deux.

Les techniques les plus prometteuses de protection du modèle biométrique reposent sur des approches de transformations cryptographiques où une version transformée du modèle d'origine est enregistré. La comparaison se fera donc entre des modèles transformés, et ces modèles transformer serviront à faire de la crypter des clé. Le but de ce travail est de combiner la cryptographie à la biométrie pour tirer les avantages des deux méthodes afin de combler les lacunes l'une de l'autre. La partie biométrique servira à protéger la clé et à faciliter le déchiffrement tandis que la partie cryptographique servira à protéger les données biométriques cela nous garantissant une sécurité mutuelle (simultanée) de la clé par le modèle biométrique et inversement.

Dans ce travail nous allons étudier la biométrie ainsi que les principes de la cryptographie ainsi que les différentes solutions en développement visant notre problématiques, nous allons en fonction de cet étude choisir la solution et le type de données biométriques qui nous paraitront les plus adaptés à répondre à notre problématique.

Le but finale sera de mettre au point une application de reconnaissance biométrique qui allierait la biométrique à cryptographie, garantissant une sécurité mutuelle (simultanée) de la clé par le modèle biométrique et inversement. Pour ce faire nous avons adopté la démarche qui suit:

- Dans le chapitre premier nous présentons un état de l'art sur la biométrie.
- Dans le second chapitre nous parlons des différentes façon de garantir la sécurité et nous introduisons l'étude de la cryptographie du chapitre troisième.
- Dans le troisième chapitre nous parlons des systèmes cryptographique ainsi que des travaux sur les systèmes cryptographique biométrique, à partir de ce chapitre nous aurons suffisamment de pré requis pour entamer la conception est la réalisation de notre application.
- Nous allons ensuite dans le chapitre quatrième parler de la conception de notre application ainsi que de sa réalisation

- Ensuite un dernier chapitre traitera des performances de l'application
- une conclusion générale fera ensuite le point sur notre travail ainsi que des différentes perspective à envisager.

CHAPITRE PREMIER

BIOMÉTRIE: CONCEPT APPLICATIONS ET ENJEUX

I.1. Introduction

La sécurité est un besoin important pour l'homme. Au fil du temps, avec les progrès techniques, les besoins de l'homme ont évolué et son besoin de sécurité a augmenté. L'insécurité devenant grandissante dans certains domaines, des moyens informatiques ont été mis en œuvre pour essayer de contrer cette tendance. Vérifier l'identité des individus est devenu un des moyens d'assurer cette sécurité.

Des moyens d'identification ont été mis en place se basant sur la possession de certains documents comme la carte d'étudiant, le passeport, etc. Ou se basant sur la connaissance de l' individus comme les mots de passe ou des numéros d'identification. Ces systèmes de vérification ont cependant des limites comme l'oubli d'un mot de passe ou la perte d'un document. D'autres moyens ont été développé pour contourner ces limitations, moyens qui ne sont plus basés ni sur la possession de documents ou la connaissance d'un individus mais basés cette fois sur des informations propres à chaque individus. Ces méthodes sont regroupées sous le nom de biométrie.

Etymologiquement le mot "biométrie" vient du grec ancien βίος (bios) « vie » et -mètre, du grec ancien μέτρον (metron) « mesure» [2], littérairement biométrie veut dire mesure du vivant.

Le mot biométrie désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans notre contexte plus précis de reconnaissance et d'identification d'individus, il existe deux définitions principales qui se complètent :

1. *La biométrie est la science qui étudie à l'aide de mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé*[1],
2. *Toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier l'identité qu'un individu affirme*[2].

En bref, la biométrie est l'analyse mathématique des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable[3]. La biométrie repose sur le principe de la reconnaissance de caractéristiques physiques.

[1] Selon le CLUSIF (CLUB de la Sécurité des systèmes d'Information Français.)
[2] Selon la RAND Public Safety and Justice (Woodward J.D. & al., *Biometrics, A Look at Facial Recognition*, Documented Briefing prepared for the Virginia State Crime Commission.)

La gamme d'indices généralement visés par la biométrie offrent une preuve irréfutable de l'identité d'une personne puisqu'elles constituent des caractéristiques biologiques uniques qui distinguent une personne d'une autre et ne peuvent être associées qu'à une seule personne

La biométrie permet de reconnaitre et d'identifier les identités des individus en utilisant leur caractéristiques physiques [4] (biologiques et/ou morphologiques) ou comportementales.

Ces caractéristiques physiques peuvent se regrouper sous le terme de *modalités biométriques.*

Dans ce chapitre nous allons nous contenter de présenter la biométrie et les systèmes biométrique de la façon la plus clair mais aussi concise. Nous allons commencer par présenter une brève histoire de la biométrie.

I.2. Origine de la biométrie

Bien que beaucoup ne s'en rende pas compte, la biométrie possède une longue histoire. Depuis la nuit des temps l'homme reconnaît ses semblables grâce aux traits de leurs visages, de leur voix ou de leur morphologie. Mais ce qui nous concerne n'est pas ce processus naturel mais plutôt de la technologie biométrique en elle-même.

Cette technologie biométrique n'est elle-même pas nouvelle. Selon [6] l'utilisation des empreintes digitales est attesté depuis très longtemps déjà en Nouvelle-Ecosse, à Babylone ou encore en Chine. Les empreintes digitales semblent tombé dans l'oubli.

Dans les années 1890 des policiers parisiens commence à utiliser les mesures des différentes parties du corps pour identifier des criminels[5]. Partant du principe qu'à vingt ans l'ossature humaine se stabilise, neuf mesures vont être réalisées. Il y a d'abord la mensuration de l'envergure c'est à dire la longueur d'un bout de bras à l'autre, puis la taille, la hauteur du buste, la longueur et la largeur de la tête, la longueur de l'oreille droite, la longueur du pied gauche, la longueur de la coudée gauche enfin la longueur du médius gauche (le majeur) comme on peut le voir d'après [7].

Cette méthode a permis une évolution considérable dans l'identification des suspects. En effet 49 personnes ont été identifiées en 1883, 241 en 1884 et 1187 en 1887. Elle est rapidement adoptée par les polices étrangères. Par la suite, Bertillon est nommé chef du service de « l'identité judiciaire » à Paris le 16 août 1883 [6]. Quelques années plus tard, en 1888, des clichés photographiques de profil et de face des suspects seront ajoutés en respectant toutefois certaines conditions pour plus de précision. Le bertillonnage reste utilisé dans certain endroit jusque dans les années 1970.

Assez vite, il fini par devenir évident que le bertillonnage n'est pas fiable. A ce moment là, Scotland Yard développe une technique de reconnaissance basé sur la reconnaissance des empreintes digitales. Après cela, d'autres techniques font leurs apparitions.

C'est Sir Francis Galton qui met en évidence l'unicité des dessins digitaux (propres à chaque doigt et à chaque individu) et leur pérennité (les empreintes ne changent pas au cours de la vie). [8] nous apprends que Galton est le premier à définir les points caractéristiques des empreintes en utilisant le terme de « minuties ».

En 1892, les policiers Argentins réaliseront la première identification de l'histoire judiciaire à partir de cette nouvelle technique en identifiant l'auteur d'un infanticide nommé Francisca Rojas. A Londres, en 1901, on peut lire dans [8] que le procédé d'identification des récidivistes par les empreintes digitales remplace officiellement le Bertillonnage.

Les empreintes digitales ont eu de plus en plus la cote, mais c'est en 1975 que leur analyse a connu une petite révolution: comme on peut lire dans [8] le FBI finance le développement de capteurs permettant d'extraire les minuties (caractéristiques d'une empreinte digitale) d'une fiche d'empreintes digitales. Cependant, àprés [6]seules les minuties elles-mêmes étaient gardées, du fait que le coût d'entreposage numérique était prohibitif.[6]

Mais c'est en 1994 que le FBI entreprend une contribution majeure à la reconnaissance des empreintes digitales. C'est le commencement de l'IAFIS *(lntegrated Automated Fingerprint Identification System)* qui est basé sur trois aspects, d'abord l'acquisition d'une empreinte digitale, l'extraction de ses caractéristiques puis leur comparaison. Cependant, il faudra attendre cinq ans, soit en 1999, pour que les composantes majeures du IAFIS deviennent opérationnelles . Dès lors, tous les systèmes d'empreintes digitales sont inter-opérationnels. De nos jours cette technologie est même disponible sur les téléphones portables.

En 1985 un système biométrique basé sur la géométrie de la main est breveté.[6] de Lors des Jeux Olympiques de 1996, c'est la solution qui avait été retenue pour accéder au village olympique. C'est aussi la solution qu'a retenu le service des migrations américain pour identifier les travailleurs frontaliers, qui effectuent des allers-retours fréquents entre les Etats-Unis et les autres pays. Au Musée de Louvre, l'accès à certaines salles est réservé pour le nettoyage. L'ouverture se fait par indentification palmaire. Et avec la baisse des coûts, la biométrie palmaire d'implante de plus en plus dans les quartiers résidentiels réservés.

Concernant la reconnaissance faciale, L'une des premières tentatives de reconnaissance de visage est faite par Takeo Kanade en 1973 lors de sa thèse de doctorat à l'Université de Kyoto[10]. Entre décembre 1993 et août 1996, le programme de la technologie d'identification de visage (FERET) contrôlé par le DARPA[3] et le NIST[4] est implanté et son utilisation massive est faite lors d'un événement sportif en 2001 (Superbowl). Lors duquel chaque personnes est à son insu et sans son consentement son visage comparé à ceux compris dans une banque de données de criminels et terroristes:.

La biométrie rétinienne a commencé en 1935 où, dans un article du New York State Journal of Medecine, la question de l'identification par l'utilisation des vaisseaux sanguins sur

[3] Defense Advanced Research Projects Agency
[4] National Institute of Standards and Technology

la rétine était soulevée. Plus les recherches ont été poussées, plus la conclusion s'est avérée que chaque rétine serait unique et ne changerait pas au cours de la vie sauf par certains traumatismes ou maladies (surtout oculaires).

Malgré tout, il faut attendre 1984 pour que la compagnie, formée en 1976, EyeDentify développe le premier lecteur de rétine commercial (le Eyedentification 7,5). Cette compagnie reste la plus importante, sinon la seule, à produire ce type d'équipement biométrique.

Pour l'iris, l'histoire commence en 1936 où l'ophtalmologiste Frank Burch décrit pour la première fois le concept d'iris comme moyen d'identification. Cependant, ce concept est resté sans suites jusqu'en 1985, où les ophtalmologistes Léonard Flom et Aran Safir ont affirmé que chaque iris était unique et pouvait ainsi servir à l'identification des individus. Deux années plus tard, en 1987, ils reçoivent un brevet pour ce concept. C'est en 1995 que les trois scientifiques de la Defense Nuclear Agency complètent et testent avec succès l'algorithme de reconnaissance automatique de l'iris et c'est la même année que le produit de ces recherches est commercialisé avec l'apparition sur le marché du premier lecteur d'iris.

Ceci n'étant qu'un très bref historique des systèmes biométriques, nous pouvons quand même voir que l'histoire de la biométrie bien que récente (exception faites des empreintes digitales). Ce bref aperçu peu suggérer à quel point ce domaine est vaste. Dans ce qui suit nous allons parler des systèmes biométriques.

I.3. Les systèmes biométriques

Un système biométrique est essentiellement un système de reconnaissance de formes qui se défini comme suit:

I.3.1. Définition

Un système biométrique est un système qui permet la reconnaissance d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissables et vérifiables[11].

dans [5] il est défini deux modes de fonctionnement d'un système biométrique:

- Identification: Procédé permettant de déterminer l'identité d'une personne, il ne comprend qu'une étape: L'utilisateur fournit un échantillon biométrique qui va être comparé à tous les échantillons biométriques contenus dans la base de données biométriques du système. Si l'échantillon correspond à celui d'une personne de la base, on renvoie son numéro d'utilisateur.
- Authentification :Procédé permettant de vérifier l'identité d'une personne. Il comprend deux étapes :
  - L'utilisateur fournit un identifiant « Id » au système de reconnaissance. L'utilisateur fournit par après un échantillon biométrique qui va être comparé à l'échantillon biométrique correspondant à l'utilisateur « Id » contenu dans la base de données biométriques du système. Si la comparaison correspond, l'utilisateur est authentifié.

Nous allons présenter différentes modalités biométriques et ainsi dégager les avantages et les inconvénients des uns par rapport aux autres.

I.3.2. Architecture d'un système biométrique

Il existe toujours au moins deux modules dans un système biométrique comme indiqué dans [12] : le module d'apprentissage et celui de reconnaissance. Le troisième module est le module d'adaptation. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

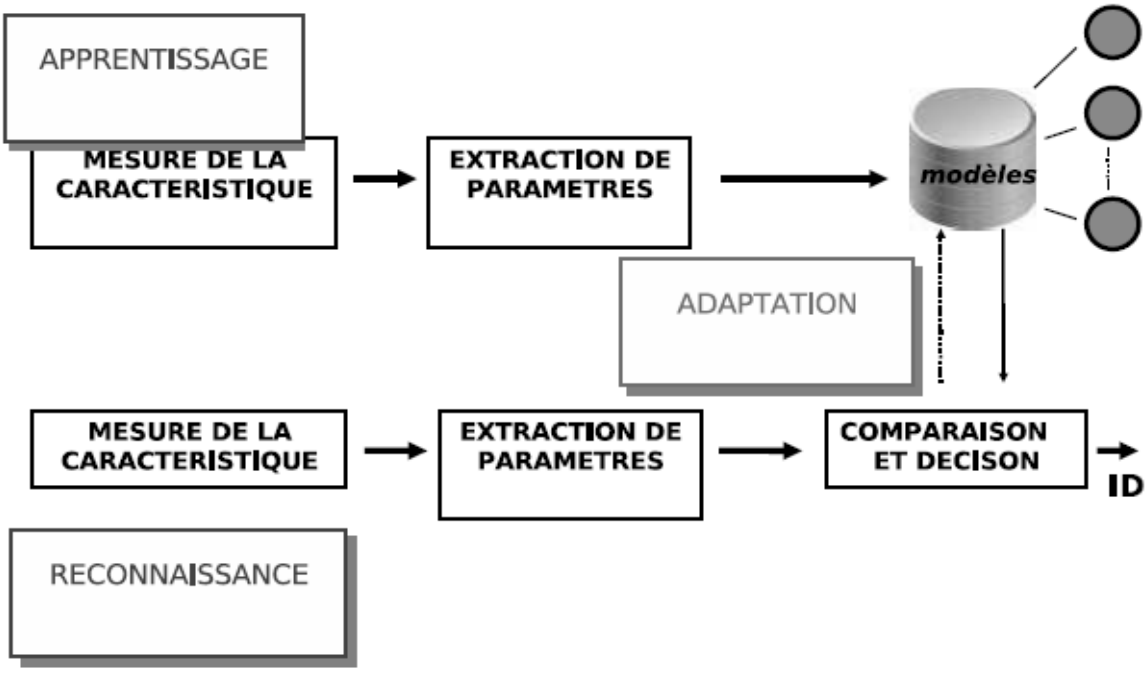


Figure I.1:Architecture d'un système d'un système biométrique

En fait les sous modules de capture et d'extraction de caractéristiques sont utilisés par les modules d'apprentissage et de reconnaissance, tandis que les sous-modules de comparaison et de décision sont utilisés par les modules de reconnaissance et d'adaptation.

Les rôles de ces modules comme indiqué par [13] sont les suivants:

a. Module d'apprentissage

Pendant de l'apprentissage, la caractéristique est tout d'abord mesurée grâce à un capteur; on parle d'acquisition ou de capture. En général, cette capture n'est pas directement enregistrer et des transformations lui sont d'abord apportées. En effet, le signal contient de l'information non nécessaire à la reconnaissance et seuls les paramètres pertinents sont extraits. Le résultat obtenu est une représentation du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Il comporte donc les sous modules suivant:

- Le **sous-module de capture:** responsable de l'acquisition des données biométriques (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.),
- Le **sous-module d'extraction de caractéristiques:** prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations de la même personne

Il est également à noter que la qualité du capteur peut beaucoup influencer les performances du système. Le mieux est la qualité du système d'acquisition, le moins il y aura de prétraitement à effectuer pour extraire les paramètres du signal.

b. Module de reconnaissance

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possible du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances.

Ce module possède donc les deux sous modules vue précédemment mais à cela on peut rajouter:

- Le **sous-module de comparaison:** compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux,
- Le **sous-module de décision:** vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type: "qui suis-je? Dans ce mode, le système compare le signal mesuré avec les différents modèle contenus dans la base de données (problème de type 1 : n). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données.

En mode vérification, le système doit répondre à une question de type: "suis-je bien la personne que je prétends être?". L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individus est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (problème de type 1:1). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. Identification et vérification sont donc deux problèmes différents. L'identification peut être une tâche redoutable lorsque la base de données contient des milliers voir des millions

d'identités, tout particulièrement lorsqu'il existe des contraintes de type "temps réel" sur le système.

c. Module d'adaptation

Pendant l'apprentissage, le système biométrique ne capture en général que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus les caractéristiques de cette biométrie ainsi que ses conditions d'acquisitions peuvent varier. L'adaptation est donc nécessaire pour maintenir voir améliorer la performance d'un système utilisation après utilisation. L'adaptation peut se faire en mode supervisé ou non supervisé mais le second mode est loin le plus utile en pratique .

Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à réestimer (revoir les calculs, en vue d'obtenir de nouvelles valeurs moyennes caractérisant l'individu). En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. L'adaptation non supervisée peut poser un problème en cas d'erreur du module de reconnaissance. L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix.

I.3.3. Performance des systèmes biométriques

Un système biométrique peut être évaluer sur trois critères principaux:

- La précision
- L'efficacité ou vitesse d'exécution
- Le volume de données pouvant être gérer.

Nous allons nous focaliser beaucoup plus sur le premier point car c'est celui la qui nous intéresse pour la suite de ce mémoire.

Nous avons précédemment vu qu'un système biométrique peut fonctionné en mode identification ou en mode authentification. Dans ces deux cas, il existe des mesures de précision différentes.

a. Performance des systèmes biométriques pour l'authentification

Trois critères principaux sont utilisés pour décrire la performance d'un système biométrique pour l'authentification, à savoir:

- Le **taux de faux rejet** (“False Reject Rate” ou **FRR**):Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système
- le **taux de fausse acceptation** (“False Accept Rate” ou **FAR**). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système
- de **taux d’égale erreur** (“Equal Error Rate” ou **EER**). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce

point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

La figure suivante illustre la distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système biométrique.

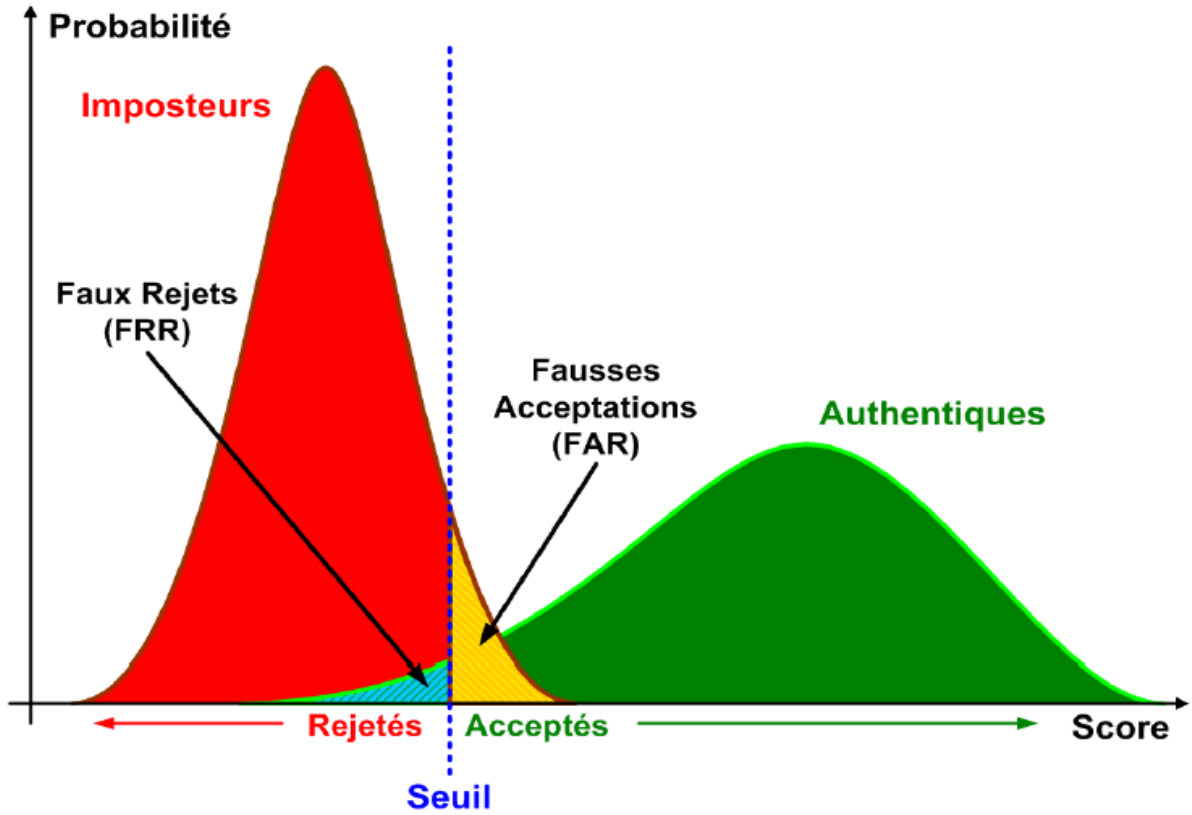


Figure I. 2:Distributions des taux de vraisemblance des utilisateurs légitimes

Sur la figure 2 il est représenté la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs légitimes et les imposteurs d'un système de vérification donné. Les FAR et FRR sont représentés en hachuré (respectivement Jaune et Bleu). Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision θ est bas, plus le système acceptera d'utilisateurs légitimes mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision θ est élevé, plus le système rejettera d'imposteurs mais plus il rejettera aussi d'utilisateurs légitimes. Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps.

La courbe dite **ROC** (**Receiver Operating Characteristic**), représentée à la figure 3, permet de représenter graphiquement la performance d'un système d'authentification pour les différentes valeurs de θ [14]. Le taux d'erreur égal (Equal Error Rate ou **EER**) correspond au point **FAR** = **FRR**, c'est-à-dire graphiquement à l'intersection de la courbe **ROC** avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que le **EER** ne résume en aucun cas toutes

les caractéristiques d'un système biométrique. Le seuil θ doit donc être ajusté en fonction de l'application ciblée: haute sécurité, basse sécurité ou compromis entre les deux.

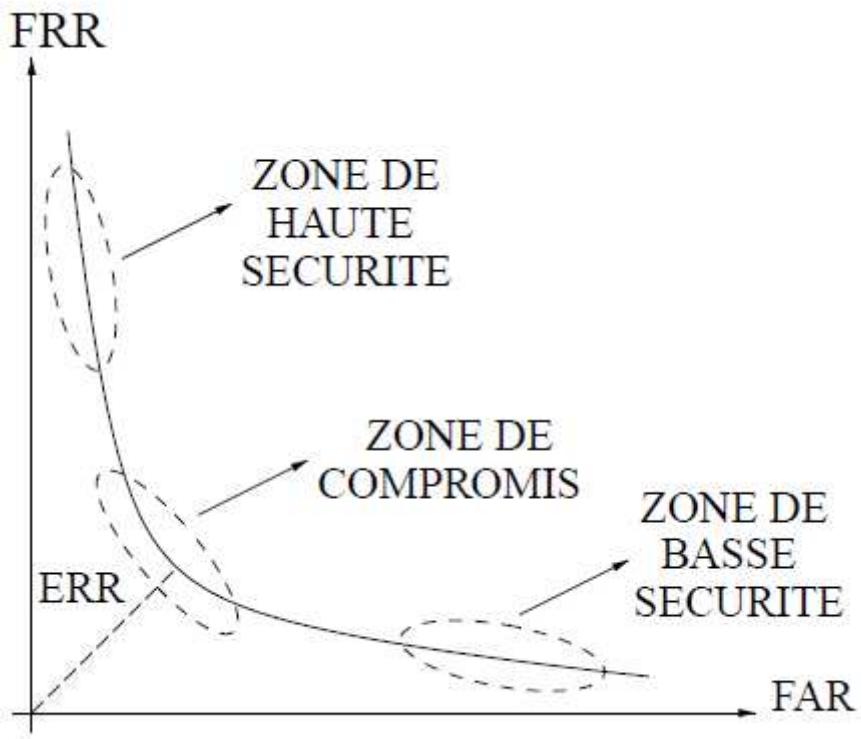


Figure I. 3: courbe ROC

b. Performance des systèmes biométriques pour l'indentification

Pour l'identification on utilise ce que l'on appelle une courbe **CMC**[14] (pour "**Cumulative Match Characteristic**" en anglais). La courbe CMC donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang et représente la probabilité que le bon choix se trouve parmi les N premiers. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit deux images, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible.

Enfin, il faut savoir que la courbe **CMC** n'est qu'une autre manière d'afficher la performance d'un système biométrique et peut également être calculée à partir du **FAR** et du **FRR**. Une étude comparative précisant le lien entre les courbes **CMC** et **ROC** peut être trouvée.

Dans ce qui suit nous allons comparés quelques modalités biométriques les plus utilisées pour avoir une idée de leurs avantages et inconvénients afin de pouvoir choisir ultérieurement la modalité la mieux adapté à notre tâche.

I.3.4. Modalités biométriques

Il existe de nombreuse modalités biométriques. Entre autres L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier pour ne citer que cela.

a. Caractéristiques d'une modalité biométrique

Les modalités biométriques représentent ce que l'on est et permettent de prouver notre identité. Pour que des caractéristiques collectées puissent être qualifiées de modalités biométriques, elles doivent être :
– *universelles* (exister chez tous les individus),
– *uniques* (permettre de différencier un individu par rapport à un autre),
– *permanentes* (peu variable dans le temps),
– *enregistrables* (collecter les caractéristiques d'un individu avec son accord),
– *mesurables* (autoriser une comparaison future).

b. Quelques modalités biométriques

Des exemples de ces différentes modalités sont présentés dans le tableau suivant:

Caractéristique biologiques	**Caractéristiques morphologiques**	**Caractéristiques comportementales**
ADN	Empreinte digitales	Démarche
Sang	Forme de la main	Parole
Odeur	Forme du visage	Dynamique de frappe sur un clavier
Urine	Forme de l'iris	Dynamique de signature
Salive	Forme de la rétine	Gestuelle

Tableau I. 1:Classification des différentes modalités

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leurs fiabilités et leurs performances et d'autres qui sont toujours en cours d'évolution. Nous allons nous contenter de faire un rapide aperçu de certaines technologies biométriques basé sur les modalités morphologique présenté dans le tableau 1.

1) l'empreinte digitale

Il s'agit d'une des premières biométries utilisées dans des machines d'authentification, il s'agit également de la plus répandue. La formation des empreintes dépend des conditions initiales du développement embryogénique, ce qui les rend uniques à chaque personne et même à chaque doigt.

Les empreintes digitales sont formées par les crêtes (ridge) et les vallées (furrow) présentes sur la surface du bout des doigts. Les empreintes digitales ne sont pas totalement déterminées par la génétique et des propriétés physiques tel que la pression au cours de la formation de l'individus puisque même des jumeaux monozygotes ont des empreintes différentes.

Cependant les empreintes digitales sont une mesure biométrique assez mal acceptée par les utilisateurs à cause de l'association qui est souvent faite avec la criminologie.

[12]

Figure I. 4: Exemple d'empreinte digitales

Il existe différents types de capteurs, plus ou moins chers, plus ou moins robustes aux impostures (faux doigts). Ce sont les performances du couple (capteur-algorithme) qui devraient être vérifiées et ceci en fonction du contexte d'utilisation. C'est une biométrie très fiable comme l'affirme [16] avec un FAR entre 0,005 et 0,1% et le FRR entre 0,01 et 0,2%.

Avantages	Inconvénients
– Technologie la plus éprouvé techniquement et la plus connue – Caractéristiques difficile à dupliquer – Petite taille du lecteur facilitant son intégration dans la majorité des applications – Faible coût des lecteurs – Bon compromis entre le taux de faux rejet et de fausse acceptation.	– Acceptabilité moyenne de la part du grand publique – besoin de coopération de l'utilisateur – Certain systèmes peuvent accepter un moulage de doigt ou un doigt coupé

Tableau I. 2:Avantage et inconvénients de la modalité empreinte digitale

2) l'iris

La reconnaissance de l'iris est une technologie plus récente puisqu'elle ne s'est véritablement développée que dans les années 80, principalement grâce aux travaux de J. Daugman [17].

L’iris est la région annulaire située entre la pupille et le blanc de l’oeil. Les motifs de l’iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d’un même individu sont différents. L’iris n’est pour l’instant pas modifiable par intervention chirurgicale. La reconnaissance de l’iris est donc aussi considérée comme une des méthodes biométriques les plus fiables qu’il soit.

La capture de l’iris se fait par une caméra standard. Du fait des contraintes sur l’éclairage de l’œil, le capteur doit être assez proche de celui-ci (un mètre maximum) ce qui restreint les applications d’une telle technologie. L’éclairage de l’oeil doit être uniforme et il faut éviter les reflets. Bien que la reconnaissance de l’iris soit moins contraignante que la reconnaissance de la rétine, les gens ont également du mal à accepter cette biométrie.[13]

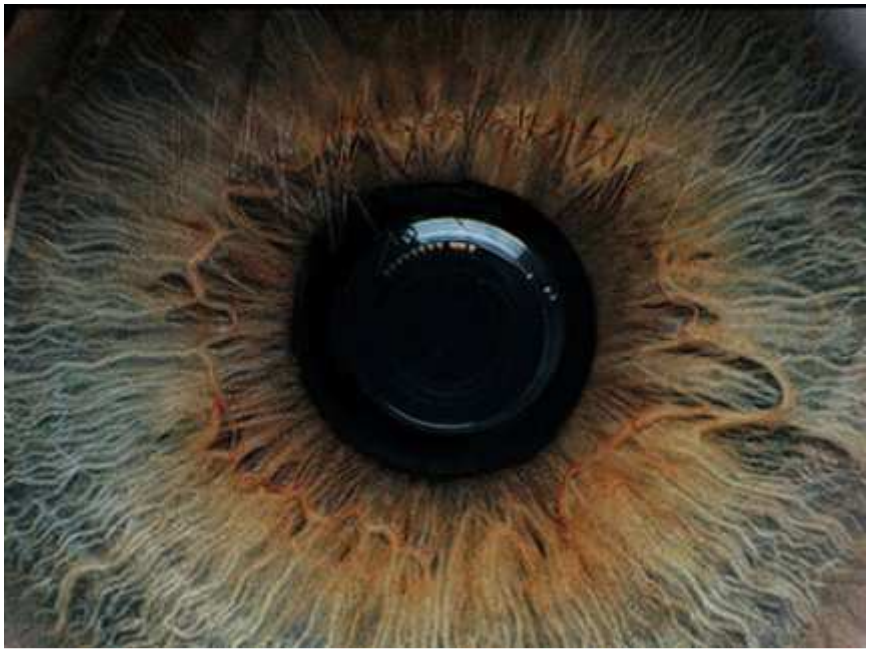


Figure I. 5: Image d'un iris

Cette biométrie utilise une identification coopérative dans le sens où la participation de l'individus à identifier est requise. Elle est considéré comme intrusive mais est très stable et très fiable avec un FAR de 0,0001% et un FRR entre 0,25 et 0,5%.

Avantages	Inconvénients
– Grande quantité d'information contenue dans l'iris – Caractéristique inchangeable – stable durant la vie d'un individus	– nécessité d'avoir un éclairage restreint – aisément capturable

Tableau I. 3: Avantage et inconvénients de la modalité iris

3) la rétine

Les technologies rétiniennes n'ont jamais vraiment été publiquement utilisées, mais il y a quelques cas. D'abord à Fallujah, en Irak, où, après avoir assiégé la ville, les autorités états-uniennes ont imposé une carte obligatoire à tous les résidents, qui doit être portée en tout

temps et qui inclut les empreintes digitales et l'empreinte de la rétine [18]. Cette technologie est aussi utilisée pour certaines installations militaires et gouvernementales [19].

Figure I. 6: Image d'une rétine

Cependant la reconnaissance de la rétine est une méthode assez ancienne puisque les premières études remontent aux années 30. Les motifs formés par les veines sous la surface de la rétine sont uniques et stables dans le temps. Ils ne peuvent être affectés que par certaines maladies. Pour ces raisons, la reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres. Les systèmes d'acquisition de la rétine sont coûteux. L'image est obtenue en projetant sur l'œil un rayon lumineux de faible intensité dans les fréquences visibles ou infrarouges. L'oeil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes ce qui demande une grande coopération de sa part. Les personnes hésitent en général à approcher un organe aussi sensible que l'oeil près de l'appareil de mesure ce qui explique pourquoi malgré son efficacité cette méthode est mal acceptée par le grand public.

Avantages	Inconvénients
– Empreinte peu exposée aux blessure – difficile à dupliquer – Taux de faux rejet et de fausse acceptation sont faibles – stable durant la vie d'un individus	– Intrusif et mal accepté par le public – Technologie biométrique la plus chère – Modalité non adapté pour un flux de passage important

Tableau I. 4: Avantage et inconvénients de la modalité rétine

4) la géométrie de la main

Cette méthode consiste à déterminer les caractéristiques de la main d'un individu : sa forme, la longueur, la largeur, la courbure des doigts, *etc*. Les systèmes de reconnaissance de la géométrie de la main sont simples d'usage. L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à positionner ses doigts. Ces appareils peuvent être difficiles à utiliser pour certaines catégories de population pour lesquelles étendre la main est un problème, telles que les personnes âgées ou celles qui ont de l'arthrite. Une photo de la face de la main est ensuite prise par un appareil photo numérique. Une photo de profil peut aussi être prise pour obtenir de l'information sur l'épaisseur de la main. En raison de la taille du système de capture, ce type de technologie est limité à certaines applications. La géométrie de la main a un faible pouvoir discriminant et les systèmes peuvent être facilement trompés par de vrais jumeaux ou même par des personnes de la même famille. Il existe une alternative à la géométrie de la main : la géométrie des doigts qui s'appuie sur la forme du majeur et de l'index.[13]

Souvent préféré aux empreintes mais moins fiable et plus variable dans le temps. L'authentification par cette méthode est coopérative mais peu intrusive, elle laisse peu de traces. Cette caractéristique est relativement variable et relativement fiable le FAR est situé autour de 0,1% et le FRR autour de 0,1%.

Avantages	Inconvénients
– bien accepté de la par des usagers – simplicité d'utilisation – résultat indépendant de l'umidité et de l'état de propreté des doigts	– Intrusif et mal accepté par le public – Risque de fausses acceptations pour des jumeaux ou des membres d'une même famille.

Tableau I. 5: Avantage et inconvénients de la modalité géométrie

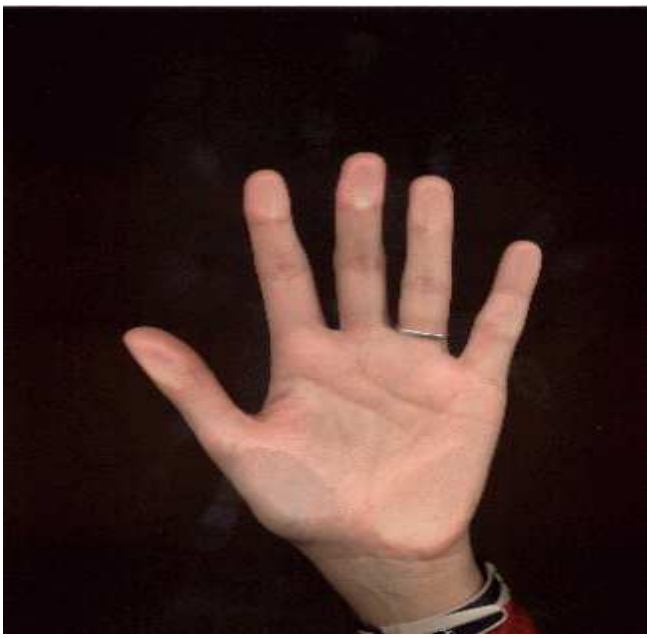


Figure I. 7: Paume de la main

La géométrie de la main est une technologie très utilisée. Par exemple, Hydra-Québec l'utilise pour quiconque veut accéder à sa centrale nucléaire Gentilly-2. C'est aussi la norme pour les centrales nucléaires aux ÉtatsUnis[20].

5) le visage

Les technologies biométriques qui se concentrent sur le visage sont plus récentes, mais ce sont celles qui connaissent l'essor le plus grand.[6]

Le visage étant la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, cela peut expliquer l'engouement pour ces technologie pourquoi elle est en général très bien acceptée par les utilisateurs. De plus le système d'acquisition est soit un appareil photo, soit une caméra numérique, la capture ne demande donc pas beaucoup de moyen.

Idéalement, un système de reconnaissance faciale doit pouvoir identifier des visages présents dans une image ou une vidéo de manière automatique. Le principe de fonctionnement de base d'un système de reconnaissance faciale peut être résumé en quatre étapes (comme l'indique la figure suivante): les deux premières s'effectuent *en amont* du système et les deux dernières représentent la *reconnaissance* à proprement dit (extraction et comparaison des caractéristiques).[15]

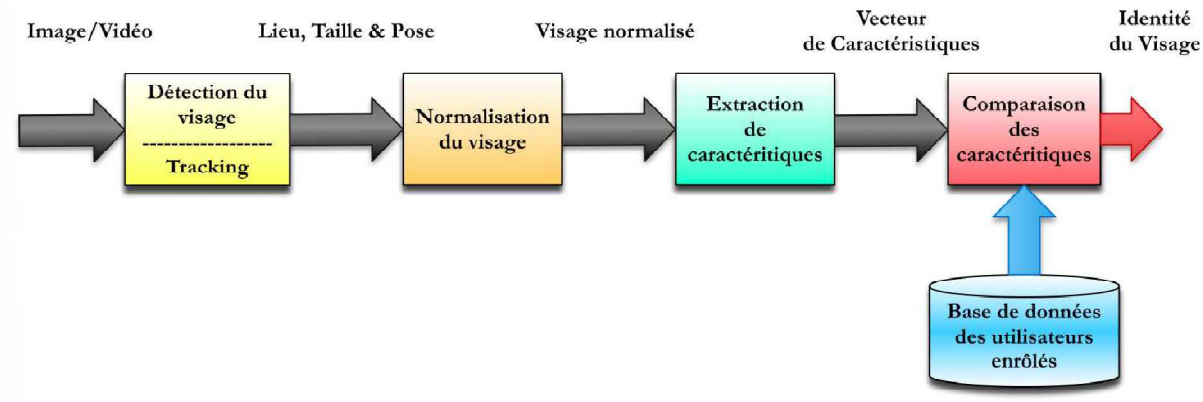


Figure I. 8: déroulement d'une reconnaissance faciale

La difficulté de la reconnaissance de visage varie énormément suivant que l'acquisition se fait dans un environnement contrôlé ou non. Dans un environnement contrôlé, des paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra au sujet sont des paramètres maîtrisés par le système. Dans un environnement non-contrôlé, une série de pré-traitements sont souvent nécessaires avant de faire la reconnaissance à proprement parler. Il faut tout d'abord détecter la présence ou l'absence de visage dans l'image (détection du visage). Le visage doit ensuite être normalisé (égalisation d'histogramme, etc.). Enfin, si nous travaillons sur un flux vidéo, le système doit suivre le visage d'une image à l'autre (face tracking).

Nous pouvons distinguer deux types de techniques parmi les méthodes globales cités en [15] :

- les techniques linéaires: La technique linéaire la plus connue et sans aucun doute l'analyse en composantes principales (PCA), également appelée transformée de Karhunen-Loeve. Le PCA fut d'abord utilisé afin de représenter efficacement des images de visages humains. En 1991, cette technique a été reprise dans le cadre plus spécifique de la reconnaissance faciale sous le nom de méthode des Eigenfaces. Il existe d'autres technique cependant tel que l'analyse discriminante linéaire (LDA) ou l'analyse en composantes indépendantes (ICA)
- les techniques non linéaires: des techniques non linéaires basées sur la notion mathématique de noyau ("kernel") comme le Kernel PCA et le Kernel LDA ont été développé plus tard. Ici, une projection non linéaire (réduction de dimension) de l'espace de l'image sur l'espace de caractéristiques ("feature space") est effectuée ; les variétés présentes dans l'espace de caractéristiques résultant deviennent simple, de même que les subtilités des variétés qui sont préservées. Bien que les méthodes basées sur le noyau peuvent atteindre une bonne performance sur les données d'entraînement, il ne peut pas en être de même pour de nouvelles données en raison de leur plus grande flexibilité ; contrairement aux méthodes linéaires.

Cette biométrie peut être Coopérative ou pas. Elle est assez bien acceptée et naturelle cela dit le visage est très variable et les technologie utilisé sont peu fiable car le FAR est compris entre 0,3 et 5% et le FRR entre 5 et 45%.

Avantages	Inconvénients
– très bine accepté par le public – Technique peu coûteuse – Ne demande aucune action de l'usager, pas de contact physique.	– sensible à l'environnement – sensible aux changements – vrais jumeaux non différenciés

Tableau I. 6: Avantage et inconvénients de la modalité visage

La tableau suivant présente un bref comparatif des principales modalités vues ci-dessus:

modalité	Universalité	Unicité	permanence
Visage	Haute	faible	Moyenne
Empreinte	Moyenne	Haute	Haute
Géométrie de la main	Moyenne	Moyenne	Moyenne
Iris	Haute	Haute	Haute
rétine	Haute	Haute	Moyenne

Tableau I. 7: Comparatif de quelques biométries morphologiques

Nous venons de voir que toutes les modalités présentes des lacunes et des avantages. De plus pour chaque technologie il existe toujours des personnes réfractaire (travailleur manuel pour les empreintes digitales ou géométrie de la main, des jumeaux ou personnes ressemblant pour la reconnaissance faciale, etc.).

Dans ce qui suit une solution aux problèmes rencontrer par ses systèmes est proposée.

I.3.1. L'approche multimodale

Il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles.

Afin d'améliorer l'efficacité on peut combiner ces systèmes avec la possession d'un document ou la connaissance d'un mot de passe. Une autre possibilité est d'utiliser plusieurs modalité en même temps. Cette façon de faire se nomme multimodalité. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système.

Il existe plusieurs forme de système multimodaux comme présenté dans [13] et [15]:

1. ***systèmes multiples biométriques*** : par exemple combiner reconnaissance du visage, reconnaissance des empreintes digitales et reconnaissance du locuteur. C'est le sens le plus classique du terme multimodal. L'un des premiers systèmes biométriques multimodaux utilise les caractéristiques du visage de et la voix. On s'attend à ce que des traits biométriques décorrélés (comme les empreintes digitales et l'iris) fournissent une nette amélioration de la performance d'un système que des traits biométriques corrélés (comme la voix et les mouvements des lèvres). Le coût de déploiement de ce genre de systèmes est plus dû à l'introduction de nouveaux capteurs et, par conséquent, au développement d'interfaces utilisateur appropriées. La précision en reconnaissance peut significativement être améliorée en utilisant un nombre croissant de traits biométriques, bien que le phénomène problématique de la dimensionalité grandissante ("curse-of-dimensionality") devrait imposer une limite à ce nombre. Ce problème de dimensionalité limite le nombre d'attributs (ou de caractéristiques) utilisés dans un système de classification de formes lorsque l'on possède seulement un faible nombre d'échantillons d'entraînement. Le nombre de traits biométriques utilisés dans une application spécifique est également limité par des considérations pratiques comme le coût de déploiement, le temps d'enrôlement, le temps de retour ("throughput time") ou encore le taux d'erreur attendu.

2. ***systèmes multiples d'acquisition*** : dans ces systèmes, un même trait biométrique est analysé à l'aide de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images. Par exemple, un système peut enregistrer le contenu de la texture 2D du visage d'une personne avec une caméra CCD et la forme de la surface 3D du visage avec une autre gamme de capteurs dans le but de procéder à la reconnaissance. Dans ce cas, c'est l'introduction des capteurs 3D servant à mesurer la variation de la surface du visage qui est responsable de l'augmentation du coût du système biométrique multimodal ou encore par exemple utiliser deux scanners différents (l'un optique, l'autre thermique) pour la reconnaissance d'empreintes digitales

3. ***mesures multiples d'une même unité biométrique*** : ces systèmes utilisent tout simplement plusieurs instances d'un même trait biométrique. Par exemple, les iris gauches et droits d'un individu peuvent être utilisés afin de vérifier son identité. Ces systèmes ne nécessitent généralement pas l'introduction de nouveaux capteurs, pas plus qu'ils n'entraînent le développement de nouveaux algorithmes d'extraction de caractéristiques ou de reconnaissance et sont, par conséquent, rentables. A titre d'information, les systèmes automatisés d'identification d'empreintes digitales ("Automated Fingerprint Identification Systems", AFIS) tirent profit de capteurs capables d'acquérir rapidement les empreintes des dix doigts d'un utilisateur

4. ***instances multiples d'une même mesure*** : Un unique capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de ce trait, ou pour obtenir une représentation plus complète du caractère sous-jacent. Par exemple, un système de reconnaissance faciale peut capturer (et enregistrer) le profil frontal du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale

5. ***algorithmes multiples*** : utiliser différents algorithmes de reconnaissance sur le même signal d'entrée. dans ces systèmes, les mêmes données biométriques sont traitées à travers plusieurs algorithmes. Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte digitale afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système. Ainsi, ce genre de système ne nécessite pas de capteurs supplémentaires et n'oblige pas l'utilisateur à interagir avec de multiples capteurs, d'où l'amélioration de la commodité d'utilisation.

Il convient de comparer les mérites respectifs de chacune de ces formes de multimodalité. Les critères retenus sont les différences de coût, de gêne pour l'utilisateur et de quantité d'information par rapport à un système biométrique unimodale.

I.4. Application de la biométrie

D'après Acuity Market Intelligence dans [25], les applications de la biométrie en 2017 se repartissent ainsi:

Service d'identité:

C'est son utilisation la plus fréquente notamment pour l'identification avec les passeport, les permis de conduire, les carte d'identité , etc. Il représente 46.55% de la demande de la biométrie.

Accès logique:

Soit 31.87% de la demande en biométrie. Elle représente la demande des constructeurs d'appareil électroniques tel que les téléphones les ordinateurs entre autres.

Contrôle d'accès physique

Contrôle d'accès physique 13.60%:pour l'accès dans les endroits sécurisés tels que les aéroports les gares, etc.

Surveillance et monitoring

Qui représente 7.99% de la demande. Mais qui est une des application les plus immédiates de Jusque-là, la biométrie est utilisée pour éviter les fraudes et usurpations d'identité, d'après [23] la biométrie va s'étendre à d'autres secteurs d'application, comme la sécurité sur Internet ou la santé.

I.5. Part du marché de la biométrie

Selon l'agence "Markets & Markets" dans [23], le marché mondial de la biométrie représente 8,5 milliards d'euros en 2015, et devrait atteindre une valeur de 32.73 milliards de dollars en2022, avec un taux de croissance annuel de 20,8% de 2013 à 2019.

Comme indiqué sur la figure 9 ci-dessous nous 31% du marché de la biométrie est consacré aux méthodes de reconnaissance de l'empreinte digitale contre 16% pour l'iris et 15% pour le visage. L'institut d'études Yole Développement estime que les technologies d'empreintes digitales dominantes évolueront progressivement vers des solutions multimodales. il souligne également que le secteur des applications smartphone constitue le moteur majeur du développement de la biométrie à près de 66% du marché total de la biométrie.

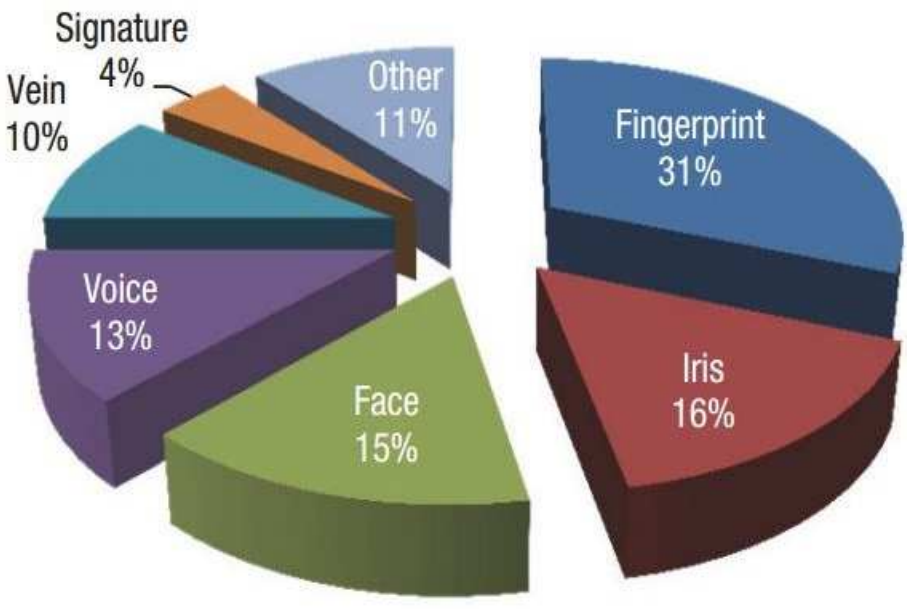


Tableau I. 8: Part du marché de la biométrie d'après Markets and Markets

I.6. Conclusion

La biométrie est un vaste domaine qui est toujours en constante évolution. Il existe une pléthore d'algorithmes et de modalité, nous n'avons ici fait que présenté les plus pratiques

dans le cadre de notre travail de mémoire et avons écartés les modalités tels que la voix, l'odeur, la démarche etc.

Nous avons tenter de décrire la biométrie ainsi que les systèmes biométrique d'une façon concise mais clair. Nous avons après la rédaction de ce chapitre suffisamment de bagage pour mieux comprendre la suite de notre projet.

Dans le chapitre suivant nous allons aborder le thème de la sécurité des systèmes informatiques.

CHAPITRE DEUXIEME

SECURITE DE L'INFORMATION

II.0. Introduction

Les systèmes d'information sont actuellement utilisés de façon généralisé dans le fonctionnement des administrations publiques (banques, douanes, polices), des entreprises mais aussi dans la vie de tous les jours des particuliers. Les services auxquels ils donnent accès nous sont tout aussi indispensables dans des cas comme l'approvisionnement en eau ou en électricité.

Comme nous pouvons le constater par l'abondance des réseaux sociaux, la communication, occupe une grande place dans nos sociétés. L'expansion rapide d'Internet a donné aux systèmes d'information une dimension incontournable au développement même de l'économie et de la société.

En Algérie les systèmes d'information sont en pleine évolution. Selon l'Autorité de régulation de la Poste et des télécommunications (ARPT), le nombre d'abonnés à internet à augmenté de 24,64% [26]; dans le monde, on compte 3,77 milliards d'internaute soit 50% de la population mondiale[27]; chaque minute Amazone fait plus de 200 milles dollars de ventes, plus de 100heures de vidéo sont chargés sur Youtube et plus de 18 térabytes de données en connexion sans fils sont utilisées au Etats-Unis[28]. C'est dire quelle importance dont jouissent les Systèmes.

Au vue de l'importance économique et social que revêtent les systèmes informatiques il en découle une nécessité de sécurité de ces dernières. dans ce chapitre, nous allons parler de la sécurité informatique, nous allons commencé par donner les définitions de base relatif à la sécurité des systèmes informatique nous parlerons également des objectifs qu'elle se fixe. Nous allons aborder les différents risques et les menaces des systèmes d'informations, nous parlerons des attaques possibles sur les systèmes informatiques et des différentes solutions à ces menaces. Nous développons plus particulièrement une de ces solution, à savoir la cryptographie.

II.1. Définitions et concepts de la sécurité informatique.

La sécurité informatique à pour but de sécuriser des systèmes informatiques. Pour pouvoir mieux comprendre la notion de sécurité, il est important de bien comprendre son but ainsi que la manière dont elle doit garantir le bon fonctionnement.

II.1.1. La sureté de fonctionnement

La sureté de fonctionnement d'un système informatique [30] est l'aptitude à délivrer un service de confiance justifiée.

Selon les application auxquelles on destine le système l'accent peut être mis sur différent critères de la sureté de fonctionnement. On peut citer les critères suivants:

- La disponibilité (availability): Le fait d'être prêt à l'utilisation.
- La fiabilité (reliability): Qui consiste en la continuité du service.

- La sécurité innocuité (safety): Qui consiste en l'absence de conséquence catastrophique sur l'environnement.
- La confidentialité (confidentiality): Qui consiste en l'absence de divulgation non autorisé de l'information.
- L'intégrité (integrity): Qui consiste en l'absence d'altérations inappropriées de l'information.
- La maintenabilité (maintainability): Qui consiste en l'aptitude à être réparé ou à évoluer.

Par rapport à la préservation de la confidentialité, de l'intégrité et de la disponibilité, la sureté de fonctionnement est désigné comme la sécurité-immunité (security) que l'on désigne simplement par sécurité.

Dans ce qui suit nous allons parler des différentes entraves à la sécurité informatique.

II.1.2. Les entraves à la sureté de fonctionnement

Les entraves à la sureté de fonctionnement sont regroupés au sein de trois notions constituer de la défaillance, la faute et l'erreur. Un système est dit défaillant lorsque le service délivré dévie du service correct.

La partie de l'état du système pouvant entraîner une défaillance est une erreur et la cause de cette erreur est la faute.

Un système peut défaillir de plusieurs manières différentes ce qui conduit à la notion de mode de défaillance que l'on peut caractériser selon quatre points de vue [30]:

- Le **domaine** : une défaillance peut être:
  - une défaillance en valeur (la valeur du service délivré ne permet plus l'accomplissement de la fonction du système)
  - une défaillance temporelle (les conditions temporelles de délivrance du service ne permettent plus l'accomplissement de la fonction du système) ;
- La **détectabilité** : une défaillance peut être:
  - signalée (le service délivré est détecté comme incorrect, et signalé comme tel)
  - non signalée (la délivrance d'un service incorrect n'est pas détectée) ;
- La **cohérence** : une défaillance peut être:
  - cohérente (le service incorrect est perçu identiquement par tous les utilisateurs)
  - byzantine (certains ou tous les utilisateurs perçoivent différemment le service incorrect) ;
- Les **conséquences** : peuvent être:
  - bénigne (les conséquences sont du même ordre de grandeur que le bénéfice procuré par le service délivré en l'absence de défaillance)
  - catastrophique (les conséquences sont incommensurablement différentes du bénéfice procuré par le service délivré en l'absence de défaillance).

Les fautes quant à elles peuvent être regroupé en trois groupes: les fautes de développement, les fautes physiques et les fautes d'interaction. Les fautes se caractérisent par les attributs suivant [30]:

- **La phase de création ou d'occurrence**: distingue les fautes de développement, qui sont créées durant le développement du système ou la maintenance en vie opérationnelle, des fautes opérationnelles, qui surviennent durant les périodes de délivrance du service au cours de la vie opérationnelle;
- **Les frontières du système**: distinguent les fautes internes qui sont localisées à l'intérieur des frontières du système, des fautes externes, localisées à l'extérieur des frontières du système et pouvant propager des erreurs à l'intérieur du système
- **La cause phénoménologique**: distingue les fautes naturelles dues à des phénomènes naturels et sans intervention humaine directe des fautes dues à l'homme
- **La dimension:** distingue les fautes matérielles des fautes logicielles
- **L'objectif:** distingue les fautes malveillantes, c'est-à-dire introduites par un humain avec l'objectif malveillant de causer des dommages au système, des fautes non malveillantes, c'est-à-dire introduites sans objectif malveillant
- **L'intention:** distingue les fautes délibérées, résultant d'une décision, des fautes non délibérées ne résultant pas d'une décision consciente;
- **La capacité:** distingue les fautes d'incompétence, qui résultent d'un manque de compétence professionnelle ou de l'inadéquation de l'organisation du développement du système, des fautes accidentelles, créées par inadvertance;
- **La persistance**: distingue les fautes permanentes, dont la présence est continue, des fautes transitoires dont la présence est temporairement bornée.

Une faute est active lorsqu'elle produit une erreur. Une faute active est soit une faute interne qui était préalablement dormante et qui a été activée par le processus de traitement, soit une faute externe. Une faute interne peut alterner entre les états dormant et actif.

Une erreur peut être latente tant qu'elle n'a pas été reconnue en tant qu'erreur, ou détectée par un algorithme ou mécanisme de détection car elle produit une défaillance. Une erreur latente peut être corrigée avant d'être détectée. Une défaillance survient lorsqu'une erreur affecte le service délivré par le système, donc lorsqu'elle traverse l'interface système-utilisateur. La conséquence de la défaillance d'un composant est une faute interne pour le système et une faute externe pour les composants avec lesquels il interagit.

II.1.3. Les moyens pour la sureté de fonctionnement

Les moyens de la sûreté de fonctionnement sont les méthodes et techniques permettant de fournir au système l'aptitude à délivrer un service conforme à l'accomplissement de sa fonction, et de donner confiance dans cette aptitude [30]. Cet ensemble de méthodes et de techniques peut être classé en quatre catégories [29] :

- La **prévention des fautes**: ou comment empêcher l'occurrence ou l'introduction de fautes; elle est principalement obtenue par des méthodes de spécification et de développement relevant de l’ingénierie des systèmes ;

- La **tolérance aux fautes**: ou comment fournir un service à même de remplir la fonction du système en dépit des fautes; elle est mise en œuvre par la détection d'erreurs et le rétablissement du système ;
- L'**élimination des fautes:** ou comment réduire la présence (le nombre, la sévérité) des fautes; elle peut être réalisée pendant la phase de développement d'un système par vérification, diagnostic et correction, ou pendant sa phase opérationnelle par maintenance ;
- La **prévision des fautes**: ou comment estimer la présence, la création et les conséquences des fautes; elle est effectuée par évaluation du comportement du système par rapport à l'occurrence des fautes, à leur activation et à leurs conséquences.

C'est en utilisant ces moyens de manière combinée que l'on peut obtenir un système qui soit sûr de fonctionnement. Ainsi, l'association entre élimination de fautes et prévision des fautes peut être considérée comme la validation de la sûreté de fonctionnement, c'est-à-dire comment avoir confiance dans l'aptitude du système à délivrer un service conforme à l'accomplissement de sa fonction. De même, l'élimination des fautes est souvent étroitement associée à la prévention des fautes, l'ensemble constituant l'évitement des fautes, c'est-à-dire tendre vers un système sans faute[30].

II.1.4. La sécurité immunité ou sécurité informatique

On peut la désigné simplement par le terme sécurité lorsque il n'y a pas d'ambigüité avec la sécurité innocuité. Il est définir la sécurité des systèmes informatiques vis-à-vis de leur seule capacité à résister à des agressions externes physiques (incendie, inondation, bombes, etc.) ou logiques (erreurs de saisie, intrusions, piratages, logiques malicieuses, etc.). Cependant dans [29] La sécurité est plutôt considérer[5] comme la combinaison des trois critères à savoir: la Confidentialité, l'intégrité, et la disponibilité.

Comme nous l'avons vue dans II.1.1, ces trois précédents critères sont des critères de la sureté de fonctionnement [29][30].

La confidentialité définit l'absence de divulgation non autorisée de l'information. Une attaque contre la confidentialité par une personne malveillante consiste à tenter de récupérer des informations pour lesquelles elle ne possède pas d'autorisation, soit en tentant d'y accéder sur le système, soit en écoutant les communications réseaux, soit de toute autre façon possible. Cela signifie que le système informatique doit empêcher les utilisateurs de lire une information confidentielle s'ils n'y sont pas autorisés, et empêcher les utilisateurs autorisés à lire une information de la divulguer à d'autres utilisateurs non autorisés. Cette seconde condition est souvent négligée car plus difficile à assurer.

L'intégrité peut se définir comme l'absence d'altération inappropriée de l'information. Une attaque contre l'intégrité vise à introduire de fausses informations, ou à modifier ou détruire l'information existante. Cela implique que le système informatique doit empêcher une modification indue de l'information, c'est-à-dire une modification par des utilisateurs non autorisés ou une modification incorrecte par des utilisateurs autorisés, s'assurer qu'aucun

[5] Ce sens est le plus souvent choisi par les spécialistes de l'audit de sécurité lorsqu'ils doivent évaluer les risques liés à l'informatique pour une entreprise.

utilisateur ne puisse empêcher la modification légitime de l'information, faire en sorte que l'information soit créée et, enfin, vérifier qu'elle est correcte. Il convient de préciser que le terme modification doit être entendu ici au sens large, comprenant à la fois la création d'une nouvelle information, la mise à jour d'une information existante, et la destruction d'une information.

La disponibilité est le fait que le système soit prêt à délivrer son service. Une attaque contre la disponibilité peut avoir deux origines. La première consiste à déjouer les politiques de sécurité et à exploiter une faute pour qu'elle produise une erreur affectant la délivrance du service. La seconde méthode consiste à engorger le système de demandes de service valides afin d'occuper le système et rendre sa disponibilité faible ou inexistante pour l'utilisateur légitime. Cela signifie que le système informatique doit fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier, et faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information. La disponibilité implique également des contraintes plus ou moins précises sur le temps de réponse du service fourni par le système informatique. Une atteinte contre la disponibilité est souvent appelée déni de service.

La sécurité revêt parfois d'autres formes et par conséquent peut représenter d'autres caractéristique, telles que l'intimité (privacy), l'authenticité, l'auditabilité, la pérennité, l'exclusivité, la non répudiation etc. Ces caractéristiques de la sécurité peuvent être assuré par la disponibilité, l'intégrité et la confidentialité appliquées à des données et à des métadonnées[6] [29].

En définitive la sécurité informatique consiste donc à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu [32].

Il existe aussi un grand nombre de terme spécifique à la sécurité. Quelques uns de ces termes sont[33]:

- une Vulnérabilité (faiblesse / faille): une vulnérabilité est une faute accidentelle, ou intentionnelle, malveillante ou non, dans les spécifications, la conception ou la configuration du système, ou dans la manière dont il est utilisé, qui peut être exploitée pour créer une intrusion.
- Une attaque: faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire, y compris les attaques lancées par des outils automatiques : vers, virus, zombies, etc. elle ne doit pas être confondue avec une intrusion.
- Une intrusion: faute malveillante interne d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Dans ce qui suit nous allons voir les différents outils utilisés pour effectuer une attaque sur des système ainsi que les outils de protection utilisés pour s'en protéger.

[6] les métadonnées correspondent à des informations indirectes reliées aux données ou aux services

II.2. Outils utilisés pour les attaques

Il existe de nombreux outils pour attaquer des systèmes. Certains sont plus sophistiqués que d'autres et sont souvent utilisés comme des armes contre des états ou des entreprises.

II.2.1. Les bombes logiques

Sont appelés bombes logiques les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système (fournie par le BIOS) [34], le lancement d'une commande, ou n'importe quel appel au système.

Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de bombe à retardement ou de bombe temporelle), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur : la bombe logique Tchernobyl s'est activée le 26 avril 1999 [35], jour du 13ème anniversaire de la catastrophe nucléaire.

Ces programmes constituent assez souvent la charge finale d'un virus. C'est la raison pour laquelle les bombes logiques sont souvent assimilées par erreur [36], aux virus et aux vers.

Un exemple célèbre de bombe logique est celui d'un administrateur système ayant implanté un programme vérifiant la présence de son nom dans les registres de feuilles de paie de son entreprise. En cas d'absence de ce nom (ce qui signifie que l'administrateur a été renvoyé), le programme chiffrait tous les disques durs. L'entreprise ne possédant pas la clef de chiffrement qui a été utilisée[37], ne pouvait plus accéder à ses données.

L'objectif de ce genre d'outils est plutôt le déni de service.

II.2.2. Cheval de Troie

La notion de cheval de Troie informatique [37][38], correspond intimement à la version historique de l'Iliade d'Homère.

Un cheval de Troie est un programme simple, composé de deux parties, le module serveur et le module client. Le module serveur, installé dans l'ordinateur de la victime, donne discrètement à l'attaquant accès à tout ou une partie de ses ressources, qui en dispose via le réseau (en général), grâce à un module client (il est le « client » des « services » délivrés inconsciemment par la victime).

Le module serveur est un programme généralement dissimulé dans un autre programme, anodin et « attractif ». L'exécution de ce dernier, au minimum une fois, installe à l'insu la partie serveur du cheval de Troie.

Le module client, une fois installé, cette fois volontairement, dans la machine de la victime, recherche sur le réseau, grâce à la commande « ping », les machines infectées par le module serveur puis en prend le contrôle, lorsqu'il a obtenu en retour, l'adresse IP et le port (TCP ou UDP) des machines accessibles. Cette prise de contrôle lui permet de mener un nombre plus ou moins grand, selon la nature du cheval de Troie, d'actions offensives:

redémarrage de la machine, transfert de fichiers, exécution de code, destruction de données, écoute du clavier etc.

Figure II. 1: Mécanisme de fonctionnement d'un cheval de Troie[38]

Ces logiciels, comme pour les bombes logiques, sont détectés de manière inégale. Un cheval de Troie, non diffusé sur Internet, bien programmé, à toutes les chances de contourner un antivirus.

II.2.3. Porte dérobées

Une porte dérobée peut être définis[39][40], en sécurité informatique, comme étant un programme ou une fonction invisible donnant directement accès à l'intrusion de logiciels malveillants (comme les chevaux de Troie) pour permettre à un ou plusieurs individus malfaisants de prendre totalement ou partiellement le contrôle d'un ordinateur à l'insu de son utilisateur légitime.

Une porte dérobée se traduit habituellement par l'existence d'un moyen d'accès non autorisé, dissimulé dans un programme, pour faciliter l'intrusion des pirates informatiques et l'installation d'autres malwares.

La porte dérobée est diffusée par les mêmes voies que les virus afin d'infester un maximum de machines. Elle va ensuite s'arranger pour être lancé automatiquement à chaque démarrage de la machine infestée puis va maintenir un port ouvert dès qu'il y a connexion. Certains s'attaquent à des canaux de communications particuliers. Son action se limite à cela. Son objectif est de préparer une attaque ultérieur.

L'attaque, elle, se fera en 2 temps : l'attaquant utilisera d'abord un Scanner d'adresses IPs et de ports pour chercher, sur Internet, une machine (une adresse IP parmi un intervalle d'adresses IPs) dont un port est maintenu ouvert par son backdoor, puis il effectuera une tentative d'exploit[7] ou autre forme d'attaque préparée par le backdoor[8]. Le backdoor n'est donc pas réellement une malveillance. Il la précède. Il se pose donc 2 problèmes, tous les deux de nature "faille de sécurité" :

[7] exploitation d'une faille de sécurité
[8] porte dérobée en anglais

- Le maintien ouvert d'un port qui est, en lui-même, une faille de sécurité.
- La faille de sécurité préalable qui à permis l'implantation de ce backdoor.

Bien qu'il soit difficile de la trouver, une fois fait il ne suffit pas de supprimer la porte dérobée, il faut aussi trouver par où on a pu l'installer.

II.2.4. Virus informatiques

Le véritable nom donné aux virus est CPA soit Code Auto-Propageable [41][40], mais par analogie avec le domaine médical, le nom de "virus" leur a été donné. Un virus informatique est un programme, généralement de petite ou très petite taille, doté des propriétés suivantes : infection ; multiplication ; possession d'une fonction nocive.

Les virus se reproduisent en infectant des « applications hôtes », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois le même fichier. Ils intègrent pour cela dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la signature virale.

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de recherche de signature (scanning).

Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "virus polymorphes".

Il existe plusieurs type de virus à savoir:

- **Virus mutants:** En réalité, la plupart des virus sont des clones, ou plus exactement des «virus mutants», c'est-à-dire des virus ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou leur signature. Le fait qu'il existe plusieurs versions (on parle de variantes) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données.
- **Virus polymorphes:** Dans la mesure où les antivirus détectent notamment les virus grâce à leur signature (la succession de bits qui les identifie), certains créateurs de virus ont pensé à leur donner la possibilité de modifier automatiquement leur apparence, tel un caméléon, en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature, de façon à ce que seuls ces virus soient capables de reconnaître leur propre signature. Ce type de virus est appelé «virus polymorphe» (mot provenant du grec signifiant «qui peut prendre plusieurs formes»).
- **Rétrovirus:** On appelle « rétrovirus » ou « virus flibustier » (en anglais bounty hunter) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

- **Virus de secteur d'amorçage**: On appelle « virus de secteur d'amorçage » (ou virus de boot), un virus capable d'infecter le secteur de démarrage d'un disque dur (MBR, soit master boot record), c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.
- **Virus trans-applicatifs** (virus macros): Avec la multiplication des programmes utilisant des macros, Microsoft a mis au point un langage de script commun pouvant être inséré dans la plupart des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic. Ces virus arrivent actuellement à infecter les macros des documents Microsoft Office, c'est-à-dire qu'un tel virus peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (généralement Windows). Or, de plus en plus d'applications supportent Visual Basic, ces virus peuvent donc être imaginables sur de nombreuses autres applications supportant le VBScript.

On emploie souvent de façon impropre le mot virus pour désigner d'autres programmes nocifs (malwares), en particulier les vers, dont nous allons traiter dans ce qui suit.

II.2.5. Vers informatiques

Un ver informatique (en anglais worm) est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau[35][42][43], sans avoir besoin d'un support physique ou logique pour se propager; un ver est donc un virus réseau. En informatique un ver est un programme nocif qui diffère des virus par plusieurs points.

Tout d'abord le ver est un programme autonome qu'on peut retrouver sur le disque dur, contrairement aux virus qui se dissimulent comme des parasites dans des fichiers ou dans le code exécutable.

Un ver peut arriver directement par le réseau en profitant d'un port ouvert, mais la méthode la plus classique consiste à s'introduire sous la forme d'une pièce jointe attachée à un mail. Certains s'exécutent alors directement à la simple lecture du mail. Mais la plupart du temps il faut cliquer sur la pièce jointe pour que le ver s'exécute.

Un ver ne se multiplie pas localement, contrairement aux virus mais sa méthode la plus habituelle de propagation consiste à s'envoyer dans des mails générés automatiquement. Ces mails sont expédiés à l'insu de l'utilisateur vers diverses adresses.

Les vers actuels se propagent principalement grâce à la messagerie grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes à tous ces destinataires. Depuis la prolifération des virus (due notamment à la prolifération des générateurs de virus), le nombre de nouveaux vers est en net recul. Cependant, il en existe toujours.

Ces vers sont la plupart du temps des scripts ou des fichiers exécutables envoyés en pièces jointes et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier joint.

Voici une liste non exhaustive d'extensions de fichiers pouvant être infectés par des vers ou des virus:

386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP.

II.2.6. Spyware

Le mot spyware est la contraction de spy et software. Un spyware, en français "espiogiciel" ou "logiciel espion", est un programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via internet ou tout autre réseau informatique[44][35], sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Une autre définition du spyware pourrait être un logiciel commercial (c'est-à-dire légalement disponible dans le commerce, payant ou gratuit) que son mode de financement ou son mode de fonctionnement amène à recueillir puis transmettre à un tiers des données personnelles concernant ses utilisateurs, sans avoir obtenu au préalable une autorisation explicite et éclairée de ces derniers. Les spywares sont donc différents des chevaux de Troie et autres enregistreurs de frappes au clavier (keyloggers), contrairement à une déformation récente de leur définition, même si ces derniers peuvent également être utilisés pour collecter et envoyer des données sensibles, dans un but cette fois clairement malveillant. Ces derniers sont détectés et supprimés de façon systématique par les antivirus, ce qui n'est pas le cas des spywares, qui peuvent malgré tout avoir été installés volontairement par certains utilisateurs.

Les spywares ne sont pas forcément illégaux car la licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé ! En revanche étant donné que la longue licence d'utilisation est rarement lue en entier par les utilisateurs, ceux-ci savent très rarement qu'un tel logiciel effectue ce profilage dans leur dos.

Nous continuons le travail par une étude des outils de protection contre les attaques.

II.3. Outils de protection contre les intrusions

Nous allons maintenant abordé le sujet des outils et mécanisme de protection contre les intrusions.

Il existe plusieurs solution pour se protéger des attaques. Les plus utilisées sont:

II.3.1. Les antivirus

Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les virus présents dans votre micro, et de prendre des mesures pour les empêcher de nuire [45].

Son fonctionnement ne consiste pas qu'à rechercher des virus dans le système[46][47]. Le rôle de l'antivirus consiste aussi à éviter l'attaque virale, en analysant le comportement.

Pour détecter un virus, il peut se servir de plusieurs techniques:

- Détection de signature ou scanning: C'est la méthode la plus ancienne. Elle se base sur le fait que chaque Virus a une signature unique. Lorsqu'il rencontre un problème, l'Antivirus interroge sa base de données de référence pour savoir à qui il a affaire et prendre les mesures qui s'imposent. Le point faible de cette méthode est que certains virus changent justement de signature lorsque ils se copient
- Contrôle d'intégrité: Elle consiste à vérifier si les fichiers n'ont pas été modifiés depuis leur installation, s'ils sont bien dans leur version originale (vérification des date / heure et taille entre autres). L'inconvénient est que les virus les plus récents ne modifient pas les dates d'accès des fichiers, ou les rétablissent après avoir les avoir infectés.
- Analyse heuristique: Cette méthode permet de détecter des virus inconnus. l'Antivirus simule l'exécution d'un programme inconnu dans une zone sûre de votre disque dur pour voir ce qu'il pourrait se passer.
  Le point faible est qu'elle provoque parfois de fausses alertes.
- Surveillance du comportement des logiciels: Cela consiste à intervenir quand un programme a un comportement inhabituel ou non approprié. En cas de détection d'un comportement suspect qu'il ne connait pas, il envoie alors immédiatement, via le réseau internet, les informations collectées chez l'Éditeur de l'Antivirus pour analyse. L'intérêt est que cet acte en apparence isolé a une résonance communautaire exponentielle : si dans les heures qui suivent un grand nombre d'ordinateurs de par le monde remontent le même problème, les équipes de surveillance vont mettre au point une solution le plus rapidement possible qui sera donc téléchargé durant l'une des mises à jour de la base virale.

Un bon antivirus doit intervenir au moment même de l'entrée ou de la tentative d'entrée d'une peste quelconque. Lorsque le virus a été découvert, l'antivirus peut :

- nettoyer les fichiers infectés en éradiquant les virus
- supprimer les fichiers infectés (attention aux problèmes que cela peut poser)
- écarter le virus dans une zone du disque dur où il ne peut nuire : on parle alors d'une mise en quarantaine
- signaler son impuissance

Il existe des tests pour vérifier l'efficacité de son antivirus. Il suffit par exemple d' écrire la chaine de caractère suivante "**X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*** "[9] dans un fichier texte et de l'enregistrer.

[9] Il est intéressant de noter qu'il m'a été impossible d'envoyer un mail contenant ce chapitre en pièce jointe à cause de cette chaine de caractère, le motif du non envoi du mail étant que celui-ci avait été identifié comme potentiellement dangereux.

Normalement, si la protection en temps réel est active une alerte doit se déclencher automatiquement sinon il faut scanner le fichier manuellement.

II.3.2. Les pare-feux

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais[35][48]), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Il peut prendre la forme d'un composant logiciel (programme de sécurité) ou d'un composant matériel (routeur), mais l'opération effectuée reste la même dans les deux cas : analyser le trafic réseau entrant afin de vérifier qu'il ne contient pas de données répertoriées sur liste noire. Les pare-feu analysent chaque « paquet » de données (fragment d'un ensemble plus volumineux de données ainsi réduit pour en faciliter la transmission) pour vérifier qu'il ne contient aucun élément malveillant.

Ces analyses peuvent prendre plusieurs formes. Un pare-feu peut passer au crible toutes les requêtes d'accès et analyser le service en étant à l'origine pour vérifier que le nom de domaine et l'adresse Internet sont connus. Il peut également examiner en intégralité chaque paquet de données entrantes à la recherche de chaînes de code répertoriées sur liste noire. Enfin, un pare-feu peut analyser les paquets d'après leur similitude avec d'autres paquets récemment envoyés et reçus. Si les paquets comportent des niveaux de similitude acceptables, ils sont autorisés à entrer.

Parmi les éventuels inconvénients figure notamment un ralentissement du trafic réseau, en particulier si les paquets sont entièrement analysés

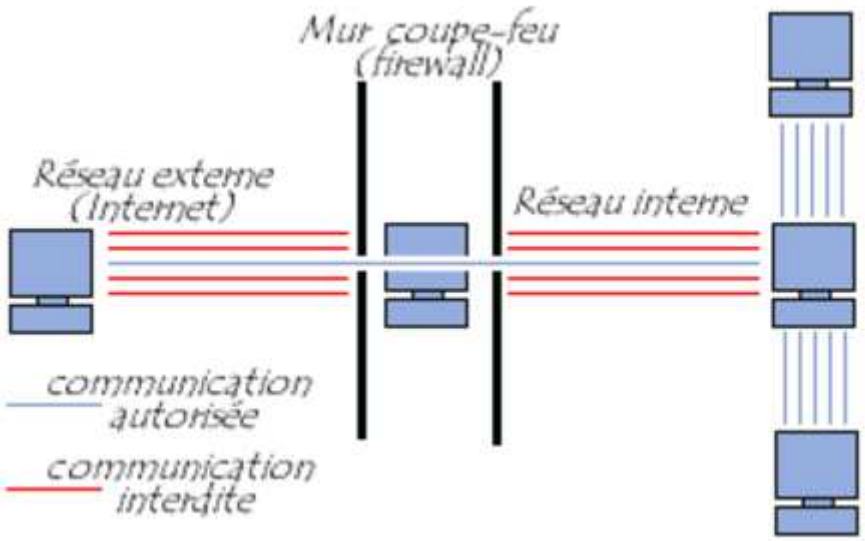


Figure II. 2: Illustration d'un pare-feu[35]

II.3.3. Logiciel anti-espion

Un logiciel anti-espion permet de protéger [49] un système contre les fenêtres publicitaires, le ralentissement de la performance et les menaces contre la sécurité provoquées

par des logiciels espions et d'autres logiciels indésirables. Pour faire face aux dernières formes de logiciel espion, il est nécessaire de mettre à jour le logiciel anti-espion.

II.3.4. La cryptographie

La cryptographie [50] permet d'assurer les fonctions principales de la sécurité des systèmes d'informations : la détection de la perte de l'intégrité, l'identification des interlocuteurs, l'authentification et la non-répudiation des messages, et la confidentialité des informations.

D'après le dictionnaire Larousse [51] la cryptographie est Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données.

La fonction première de la cryptographie est donc tout d'abord de protéger des données pour que même si un tiers arrive à y avoir accès, il ne puisse pas avoir accès à l'information que ces données renferme sans y être autoriser par la connaissance d'un secret.

Cette technique est utilisé depuis l'antiquité. Le mot cryptographie vient des mots en grec ancien kruptos (κρυπτός) « caché » et graphein (γράφειν) « écrire ».

Cette méthode de sécurité à l'avantage d'assurer une grande partie de la sécurité à elle seule et est l'objet de notre travail.

Nous commençons par définir certain termes relatif à la cryptographie [52].

- chiffrement : transformation à l'aide d'une clé d'un message en clair (dit texte clair) en un message incompréhensible (dit texte chiffré) pour celui qui ne dispose pas de la clé de déchiffrement (en anglais encryption key ou private key pour la cryptographie asymétrique) ;
- chiffre : utilisation de la substitution au niveau des lettres pour coder ;
- code : utilisation de la substitution au niveau des mots ou des phrases pour coder ;
- coder : action réalisée sur un texte lorsqu'on remplace un mot ou une phrase par un autre mot, un nombre ou un symbole ;
- cryptogramme : message chiffré ;
- cryptosystème : algorithme de chiffrement;
- décrypter : retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement;
- cryptographie : étymologiquement « écriture secrète », devenue par extension l'étude de cet art (donc aujourd'hui la science visant à créer des cryptogrammes, c'est-à-dire à chiffrer) ;
- cryptanalyse : science analysant les cryptogrammes en vue de les décrypter ;
- cryptologie : science regroupant la cryptographie et la cryptanalyse.
- cryptolecte : jargon réservé à un groupe restreint de personnes désirant dissimuler leur communication.
- Clé : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un

algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

Le champ d'application de la cryptographie est vaste et il existe de nombreux algorithmes et protocoles qui peuvent regrouper en trois catégories à savoir:

- Les algorithmes de chiffrement faible
- Les algorithmes de cryptographie symétriques
- Les algorithmes de cryptographie asymétriques

a) Les algorithmes de chiffrement faible

Les premiers algorithmes [53] utilisés pour crypter un message étaient plutôt rudimentaires. En effet , ils consistaient pour la plupart à un simple remplacement de caractères par d'autres. La confidentialité de l'algorithme était la clé de ce système pour éviter un décryptage rapide. Cela suivait le principe évoqué par Kerckhoffs, qui affirmait que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef.

Les deux exemples les plus connus sont le chiffre de César et le chiffre de Vigenère.

b) Les algorithmes de cryptographie symétriques

Un algorithme symétrique est un algorithme qui permet de transformer un texte en clair en texte chiffré en utilisant une clé [54][55] et de retransformer le texte chiffré en texte en clair en utilisant la même clé.

Le secret de la communication est uniquement assuré par la clé qui est utilisée lors de la phase de chiffrement et de déchiffrement. L'algorithme utilisé ne fait pas partie du secret.

On parle d'algorithmes symétriques car c'est la même clé qui sert à la fois au chiffrement et au déchiffrement du message.

Figure II. 3: Illustration de la cryptographie symétriques

La faiblesse de cet algorithme est qu'il repose uniquement sur la non divulgation de cette clef secrète. Si la clef secrète est dévoilée, alors n'importe qui pourra consulter les messages chiffrés avec celle-ci. De plus, le transport de la clef secrète entre Alice et Bob reste problématique.

Il existe deux types d'algorithmes à clef secrète. Certains traitent le message en clair un bit à la fois, ceux ci sont appelés stream cipher pour algorithmes de chiffrement continu.

D’autres opèrent sur le message en clair par groupe de bits. Ces groupes sont appelé blocs, ces algorithmes sont appelés block ciphers ou algorithme de chiffrement par bloc.

c) Les algorithmes de cryptographie asymétriques

On parle d'algorithmes asymétriques [54][55] car ce n'est pas la même clé qui sert au chiffrement et au déchiffrement. Dans le cas de ces algorithmes, on parlera alors de clé privée et de clé publique. Ces deux clés, clé privée et clé publique, sont intimement liées par une fonction mathématique complexe.

Les algorithmes asymétriques possèdent 2 modes de fonctionnement:

- Le mode chiffrement dans lequel l'émetteur chiffre un fichier avec la clé publique du destinataire pour chiffrer. Le destinataire utilise sa clé privée pour déchiffrer le fichier. Dans ce mode, l'émetteur est sûr que seul le destinataire peut déchiffrer le fichier.

- Le mode signature dans lequel l'émetteur signe un fichier avec sa propre clé privée. Le destinataire utilise la clé publique de l'émetteur pour vérifier la signature du fichier. Dans ce mode, le destinataire est sûr que c'est bien l'émetteur qui a envoyé le fichier.

Ainsi pour résumer :

- ✓ L'émetteur chiffre avec la clé publique du destinataire, le destinataire déchiffre avec sa clé privée.
- ✓ L'émetteur signe avec sa clé privée, le destinataire vérifie la signature avec la clé publique de l'émetteur.

Cet algorithme semble beaucoup plus adapter que les algorithmes à clef secrète pour sécuriser les communications. Cependant, cette algorithme ne peut pas substituer les algorithmes à clef secrète essentiellement pour une raison: Les algorithmes à clef publique sont généralement beaucoup plus lents à traiter que les algorithmes à clef secrète.

Dans le chapitre III nous allons voir en plus en détail les systèmes cryptographiques.

II.4. Conclusion

Dans ce chapitre nous avons présenté un état de l'art sur la sécurité informatique. Cet état de l'art avait pour but d'introduire le suivant chapitre sur la cryptographie et les cryptosystèmes. Nous tenons à préciser que pendant les lectures que nous avons effectuer sur la sécurité nous avons pris conscience que c'est un vaste domaine et que le chapitre que nous avons écrit à ce sujet et très bref en comparaison.

Nous retenons de ce chapitre que pour protéger un système informatique il faut instaurer une véritable politique de sécurité. Il faut savoir ce qui doit être protéger, de quoi il doit être protéger, évaluer les risques et déterminer une liste de contre mesure.

Bien évidement une sécurité à 100% reste un idéal à atteindre, surtout devant le grand nombre des menaces qui mettent en danger les systèmes d’informations. D’où l'importance d'une politique de sécurité efficace en prenant compte des risques encouru par un système

informatique et en comparant les coûts que peuvent générer les problèmes résultants de ces risques avec le coût nécessaire à la mise en place des solutions pour éviter ces problèmes.

Nous avons parlé de la cryptographie dans le paragraphe II.3.4, dans le chapitre suivant nous allons traiter de la cryptographie plus amplement et aussi parler de la cryptographie biométriques ainsi que des différents travaux déjà effectué à ce sujet.

CHAPITRE TROISIÈME

LES CRYPTOSYSTEMES BIOMETRIQUES

III.0. Introduction

La cryptographie de nos jours recouvre de nombreux domaines et est utilisé pour fournir de nombreux services. Les technologies de l'information s'étant universalisées au fil des années, il est devenu moins probable de protéger une information confidentielle ou critique. Le but premier de la cryptographie est donc de sécurisé une information en la rendant inintelligible à une personne ne disposant pas du droit de jouir de cette information. Mais de nos jours, on ne peut plus limiter la cryptographie à cette simple utilisation car elle est désormais utilisé pour beaucoup d'autre problème de sécurité comme nous allons le voir tout au long de ce chapitre.

Ce chapitre est organisé comme suit, nous allons commencé par présenter la cryptographie, nous parlerons des différentes techniques utilisées ainsi que de leurs utilisations. Apres cela nous verrons ensuite les systèmes cryptographique où nous parlerons de la sécurité des systèmes cryptographiques ainsi que de l'approche utilisés c'est-à-dire des cryptosystèmes biométrique. Nous décrirons deux possibilités: le fuzzy vault et le fuzzy commitment. Nous ferons ensuite une synthèse sur ces deux méthodes.

Nous passons donc à la première partie de ce chapitre qui fixe un état de l'art sur la cryptographie.

III.1. La cryptographie

Ainsi que nous l'avons vu dans l'introduction, la cryptographie sert à résoudre un certain nombre de problèmes liés à la sécurité. Elle peut être défini comme suit:

III.1.1. Définitions

Issu du grec Cryptos (caché ou secret) et graphie (écriture), la cryptographie désigne la science de l'écriture secrète [56]. Le service de base fourni par la cryptographie est la capacité de transmettre une information entre deux correspondants sans que celle ci ne soit accessible à des personnes tierces. Elle est également défini comme l'étude des systèmes mathématiques, informatiques et électroniques propres à résoudre les problèmes de confidentialité et d'authentification [57].

Actuellement, en plus de la confidentialité, la cryptographie sert également à résoudre d'autres problèmes relatif à la sécurité tel que: l' authentification, l'intégrité et la non répudiation.

En cryptographie on rencontre souvent le terme chiffrement qui se définit comme l'action de rendre impossible à la compréhension un document dit « texte clair » en remplaçant ses données par un code dit « texte chiffré » [58]. Le déchiffrement consiste en

l'action inverse tandis que le décryptage consiste à retrouver le texte clair à partir du texte chiffré lorsqu'on ne connait pas la clé[57].

Il existe de nombreuses techniques cryptographiques que l'on peut diviser en deux groupes

III.1.2. Techniques et algorithmes cryptographiques générales

Dans ce qui suit, nous présentons quelques principales techniques cryptographiques pour nous permettre d'entamer les crypto-systèmes biométriques qui seront vu plus loin dans ce chapitre.

Les principales technique cryptographique sont:

a) Chiffrement à clé secrète

Le terme de chiffrement symétrique s'applique lorsque les clés de chiffrement et déchiffrement peuvent se déduire (en temps polynômial)[59] l'une de l'autre. En pratique il faut la même clé pour chiffrer et déchiffrer.

Mathématiquement parlant on dispose de deux fonctions: une fonction E qui à un texte clair ***m*** et une clé secrète **K** fais correspondre un texte chiffré **c= E(*m*, K)**, et la fonction de déchiffrement **D** qui à un texte chiffré **c** et une clé **K** fait correspondre le texte clair ***m=D(c,K)*** si ***c*** est le chiffré de m avec la clé ***K***. Cette dernière est en générale obtenu de façon aléatoire.

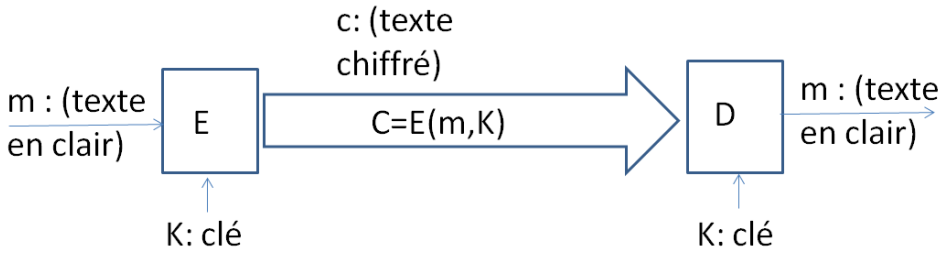


Figure III. 1:Schéma d'un système de chiffrement à clé secrète

Ces systèmes de chiffrement peuvent être divisés à leur tour en deux groupes de méthodes:

- les chiffrement à flot: une méthode de chiffrement à flot opère individuellement sur chaque bit du texte à chiffré en utilisant une transformation qui varie en fonction de la position du bit d'entrée.
- les chiffrement par bloc: un système de chiffrement par bloc opère avec une transformation fixe qui s'applique sur des blocs de texte de taille fixe. Ces méthodes sont plus utilisé avec comme exemple le DES, le 3-DES le AES etc.

b) Chiffrement à clé publique

Ces méthodes de chiffrement sont introduites par Diffie et Hellman qui propose l'utilisation d'un couple de clés: l'une servant au chiffrement et l'autre au déchiffrement. Dans un système utilisant un tel principe, chaque utilisateur A dispose d'une paire de clés: une clé privée et une clé public. La clé publique est publiée et connue de tout le monde tandis que la clé privé n'est connue que de l'utilisateur A. Il est, en pratique, impossible de déterminer la clé privée de A à partir de la clé publique.

Il existe deux fonctions publiques D et E qui servent respectivement au chiffrement et au déchiffrement. Lorsqu'on veut envoyer un texte chiffré y à A il suffit d'utilisé la fonction de chiffrement D sur le texte clair x avec la clé d_A pour obtenir le chiffré $y= D(d_a, x)$. Pour avoir accès à x, A doit utiliser la fonction E sur le crypté y avec la clé privée e_A, ce qui permet de réobtenir $x=E(e_A,y)$.

Il faut noté que les deux fonction E et D sont publique, il n'y a que la clé privée qui soit un secret. Cette technique n'est en général utilisé que pour les chiffrement des messages court correspondant essentiellement à échanger des clés, à cause de la lenteur des primitives cryptographiques correspondantes. Ces systèmes cryptographique repose justement sur la difficulté d'effectuer en pratique certains calculs.

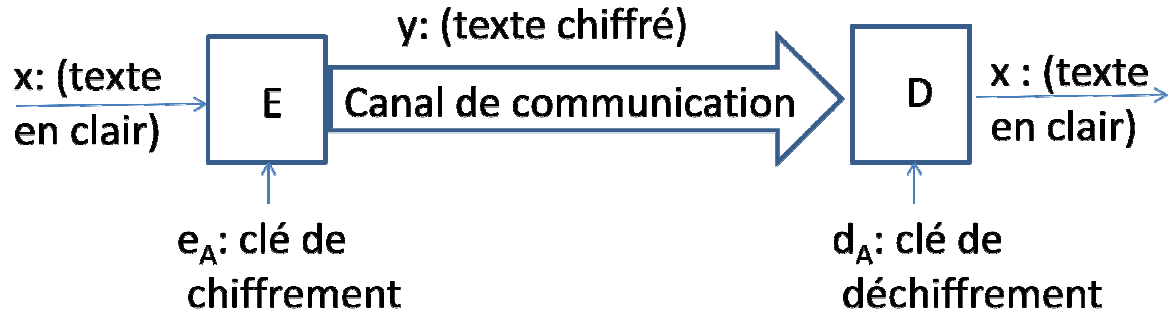


Figure III. 2: Schéma de fonctionnement du chiffrement à clé publique

Malgré une telle efficacité un des problèmes qu'elle pose est un problème de gestion de clé qui est: Comment évité que la clé ne soit exposée, soit pendant qu'elle est stockée, soit pendant son utilisation?

Une solution possible pour résoudre ce problème est l'objectif de ce travail, que nous aborderons plus loin au point III.3.

Des exemples de systèmes de chiffrement clés publiques sont:

- RSA (Rivest Shamir Adleman): C'est un système basé sur la difficulté de factoriser un produit de deux nombres premiers . Associé à l'encodage KEM (Key Encapsulation Mechanism)
- Diffie-Hellman: premier système de chiffrement à clé publique permettant l'échange de clé. Il utilise la difficulté du problème du logarithme discret sur certains groupes et utilise des paire de clés publiques et privées éphémeres.
- McEliece: système basé sur la difficulté du décodage d'un code correcteur linéaire binaire quelconque et sur l'indistinguabilité des codes de Goppa.
- Rabin: système basé sur la difficulté d'extraire une racine carrée modulo un produit n de deux grands nombres premiers.

c) *Fonctions de hachage cryptographiques*

Une fonction de hachage transforme un long message en un bloc court, de taille fixe. L'image d'un message par une fonction de hachage s'appelle le haché du message ou empreinte du message.

Supposons *k* un nombre fixé qui représente un nombre d'octet, une fonction de hachage est une application:

$$h: B^* \rightarrow B^k$$

qui vérifie les propriétés suivantes:

- Résistance à la détermination de l'antécédent de h, ce qui veut dire qu'en pratique il est impossible de déterminer, à partir d'un haché *m*, un message *M* ayant ce haché.
- Résistance à la détermination d'une deuxième préimage, ce qui veut dire que si on donne un message M_1 ainsi que son haché $h(M_1)$ il est en pratique impossible d'obtenir un message M_2 différent de M_1 ayant le même hachage tel que $h(M_1)= h(M_2)$
- Résistance aux collisions, ce qui signifie qu'il est impossible en pratique de construire deux messages M_1 et M_2 ayant le même haché: $h(M_1)=h(M_2)$.

En pratique, il n'est pas possible, avec un hachage cryptographique, de haché un texte aussi long qu'on veut. Il existe un limite d'utilisation selon la longueur de l'empreinte. Il est conseillé de prendre une taille de haché d'au moins 256 bits.

Quelques exemples de fonctions de hachage cryptographiques sont:

- SHA-2 (Secure Hash Algorithm 2) a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits.
- Utilisation des système de chiffrement par bloc (exemple AES)

d) *Signature*

La signature est une primitive cryptographique qui sert à garantir l'intégrité d'un message, fournit l'authentification du signataire et assure la non répudiation.

Une tel primitive fonctionne comme suit:

- Un haché "m" du message "M" est calculé avec une fonction de hachage publique "h" tel que $m=h(M)$.
- Chaque utilisateur A dispose d'une clé privé d_A et d'une clé publique e_A; Le système définit une fonction signature S qui à une clé privé d_a et un haché m fait correspondre $s= S(d_A, m)$, appelé appendice de la signature de M par A.
- A peut alors transmettre le message signé (M,s).

- Le système dispose également d'une fonction V, qui à une clé publique e_A et un message signé (M,s) fait correspondre la V(e_a, M, s) qui vaut vrai si (M, s) correspond bien à un message signé par A ou faux s sinon.

Un tel processus implique bien l'intégrité du message, l'authentification du signataire et la non répudiation, puisque la clé publique est à la disposition de tout le monde, tout le monde peut vérifier qu'il s'agit bien d'un message signé par A.

Il existe aussi des algorithmes dits à recouvrement de message utilisés pour signé des messages courts, dans lesquels on ne hache pas le message mais où le message est récupéré a partir de la signature.

La signature est parfois utilisé à des fins d'authentification mais elle offre cependant des fonctionnalités qui vont au-delà de celles requise par l'authentification. Par exemple l'authentification ne requiert pas la non répudiation. Cette dernière peut être éventuellement indésirable pour l'authentification.

Des exemples de systèmes de signature sont:

- le système RSA utilisé "à l'envers": Celui qui signe chiffre avec sa clé privé. Tout le monde peut alors vérifier avec la clé publique de celui qui à signé.
- Le DSS[10] Qui utilise le DSA[11] basé sur la difficulté du problème du logarithme discret sur le groupe multiplicatif **Z/pZ, p** étant un grand nombre premier.

III.1.3. Techniques et primitives cryptographiques spécialisés

Il existe d'autres techniques qui en collaboration avec les techniques vus à la partie III.1.2 sont utilisé dans des protocoles plus spécialisés, comme par exemple le vote électronique ou encore la monnaie numérique. Nous n'allons pas décrire ces protocoles, nous allons plutôt traiter de protocoles pouvant être considéré comme rudimentaire et servant de base à des protocoles plus complexes. Ils se situe à la limite de primitives cryptographiques et protocoles cryptographiques.

Ces techniques sont entre autres la signature en aveugle, les preuves à divulgation nulle, les mises en gages, le chiffrement homomorphique, le partage de secret et le mix net.

a) La signature en aveugle

La signature en aveugle consiste à faire signer une autorité sans que celle-ci ne sache ce qu'elle signe [60] et sans que l'utilisateur qui obtient cette signature ne puisse être tracé. Elle implique deux propriétés:

- L'autorité ne peut pas prendre connaissance du document au moment de la signature.
- Si le document signé revient à la vue de l'autorité, celle-ci ne peut déterminer dans quel circonstance elle à signé ni qui lui à demandé de signer.

[10] Digital Signature standard
[11] Digital Signature Algorithm

Elle est surtout utilisé pour le cas de la monnaie électronique, elle permet par exemple d'effectuer un achat sans que la banque ne sache où on a effectuer un achat, protégeant ainsi l'intimité de l'utilisateur.

b) Les preuves à divulgation nulles

Une preuve à divulgation nulle de connaissance est un concept utilisé en cryptologie dans le cadre de l'authentification et de l'identification. Cette expression désigne un protocole sécurisé dans lequel une entité nommée "fournisseur de preuve" ou "prouveur", prouve mathématiquement à une autre entité, le « vérificateur », qu'il connait un secret sans toutefois révéler une autre information qui pourrait permettre de calculer une information que le vérificateur n'aurait pu calculer sans les communication du prouveur.

Du point de vue de la terminologie, on parlera de prouveur (respectivement de vérificateur honnête lorsque celui-ci respecte le protocole. On parle de tricheur lorsqu'il s'agit d'un prouveur ou un vérificateur qui ne respecte pas le protocole imposé.

Un exemple de preuve à divulgation nulle est l'identification de Fiat-Shamir. Une telle preuve peut parfois être modifié en signature.

c) Les mises en gage

En cryptologie, la mise en gage est une méthode par laquelle un premier parti, souvent appelé Alice, "met en gage" un bit d'information envers un deuxième parti, souvent appelé Bob. Ceci se fait sans que la valeur du bit soit révélée et de telle sorte que la mise en gage peut être révélée, ou "ouverte", plus tard par Alice et vérifiée par Bob [61]. Là on exige bien sur que la valeur du bit n'ait pas pu être modifiée après l'engagement.

d) Le chiffrement homomorphique

C'est un chiffrement qui permet un certain anonymat. Soit $\boldsymbol{\varepsilon}$ un chiffrement probabiliste. Soit M l'espace des textes clairs et C l'espace des chiffrés. On suppose que M et C sont des groupes pour les opérations respectives $\oplus$ et $\otimes$. Le chiffrement ε est homomorphique si étant donnés deux chiffrés $c_1 = \boldsymbol{\varepsilon}(m_1, r_1)$ et $c_2 = \boldsymbol{\varepsilon}(m_2, r_2)$ obtenu avec des aléas r_1 et r_2, il existe un aléa r tel que:

$$C_1 \otimes C_2 = \boldsymbol{\varepsilon}(m_1 \oplus m_2, r).$$

Dans un tel cas il est possible de déchiffrer un $\otimes$ de plusieurs chiffré sans les déchiffré individuellement. Cela permet d'éviter de savoir qui à chiffrer quoi.

e) Le partage de secret

Le partage de secret est une technique en cryptographie qui permet de partager un secret entre participants et de ne permettre la reconstitution de ce secret que si t participants au moins ce mettent d'accord pour reconstituer le secret. C'est le cas par exemple d'une clé privée partagée entre n autorités et où déchiffrer un message chiffrée avec une clé publique correspondante demande la participation d'au moins t détenteurs du secret. On peut citer dans cette catégorie le partage à seuil de Shamir.

f) Le mix net

Le mix net, est une méthode concurrente du chiffrement homomorphe, et qui permet de ne pas pouvoir tracer qui à chiffré quoi. Il repose sur chiffrement aléatoire qui permet de calculer sans repasser par le texte clair, une nouvelle forme aléatoire du chiffré du même texte clair.

III.2. Les systèmes cryptographiques

Les systèmes cryptographiques se sont développés en trois phases successives. À l'origine, l'algorithme de chiffrement et la clé de chiffrement des systèmes cryptographiques étaient tous deux gardés secrets. Ensuite, l'algorithme de chiffrement est rendu public, mais les clés de chiffrement restent secrètes. C'est là la caractéristique des systèmes cryptographiques à clé secrète comme le système DES. Pour finir, sont mis au point les systèmes cryptographiques à clé publique, tel le système RSA; dans ces systèmes, l'algorithme de chiffrement et la clé de chiffrement sont tous deux publics, et le secret n'est plus constitué que par la clé de déchiffrement, différente de la clé de chiffrement à laquelle elle est malgré ça mathématiquement liée.

On doit une tel évolution en partie à Auguste Kerckhoffs dans [63] où il donne des conditions qu'un système cryptographique doit remplir pour qu'il soit le plus sûr possible [57]:

i. le système doit être matériellement, sinon mathématiquement, indéchiffrable
ii. Il ne doit pas exiger le secret, ce dernier peut tomber dans les mains de l'ennemi sans inconvénient
iii. La clé doit pouvoir être communiqué et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondant
iv. pouvant être applicable à la communication télégraphique
v. pouvant être poratif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
vi. Le système doit être d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

De façon générale, un système cryptographique est satisfaisant, pour une application donnée, s'il répond à trois conditions fondamentales [62]: la simplicité du chiffrement et du déchiffrement, même si ceux-ci ont recours à des algorithmes complexes; la difficulté d'utilisation des clés de chiffrement pour les non-initiés; l'absence de liens entre la confidentialité de l'algorithme de chiffrement et le chiffrement lui-même. Malgré tout, la sécurité d'un système cryptographique n'est jamais supérieure à la sécurité du mode de transmission de ses clés secrètes. Un système cryptographique peut se définir comme suit:

III.2.1. Définitions

Ensemble d'instruments, de documents et de techniques associées permettant le chiffrement et le déchiffrement des données selon une méthode particulière [62].

Les cryptosystèmes qui nous intéressent dans le cadre de ce mémoire sont les cryptosystèmes biométriques. Il s'agit en fait d'une combinaison entre la cryptographie et la

biométrie. L'enjeu majeur de ces systèmes est la protection des données biométrique ainsi que la gestion des clé cryptographique.

III.2.2. Sécurité des systèmes cryptographiques

Sécurité parfaite

Shannon à introduite la notion de système cryptographiquement sûrs. Nous avons vu qu'un système cryptographique est constituer de:

- un ensemble fini *M* de textes clairs
- un ensemble fini *C* de textes chiffrés
- un ensemble fini *K* de clés

Par définition un système cryptographique pour lequel on choisit une nouvelle clé pour chaque nouveau texte, est parfaitement sûr si:

$$\forall x \in M, \forall y \in C, P(x|y) = P(x)$$

Autrement dit, la probabilité d'un texte clair x sachant que le texte chiffré est y est la même que la probabilité de x. Le texte chiffré dans ce cas n'apporte aucun renseignement sur le texte clair.

On peut également dire qu'un système cryptographique est sur si:

$$|K| \geq |C| \geq |M|$$

Ou encore si les deux condition suivante sont remplies:

- Toutes les clés sont équiprobables
- pour chaque x ∈ *M* et chaque y ∈ *C* il existe une unique clé *k* vérifier $e_k(x)=y$.

Si on considère la notion de sécurité parfaite [72], il existe un paradoxe mathématique qui stipule que la cryptographie à clé publique, étant donné que l'attaquant dispose de la clé publique et du cryptogramme[12], n'est pas, confidentiellement parlant, parfait et qu'en pus il existe suffisamment d'information dans le cryptogramme et la clé publique pour déterminer le message clair. Cependant ce résultat n'indique pas comment récupérer ces informations.

Sécurité calculatoire

La notion sécurité parfaite est extrêmement exigeante. Quelque soit la puissance de l'adversaire, la connaissance du texte chiffré ne lui apporte aucune information sur le texte clair, si ce n'est sa longueur. En contrepartie un tel système est tellement exigeant qu'il n'est pas envisageable pour une large utilisation commode. Sachant que la puissance de l'adversaire n'est pas illimité on est amené à limité les exigences.

La sécurité calculatoire est basée sur la mesure de la quantité de calcul nécessaire pour casser un système. On dit qu'un procédé est sûr au sens de la théorie de la complexité si le meilleur algorithme pour le casser nécessite *n* opérations où n est un nombre beaucoup trop

[12] texte ou message chiffré.

grand pour que cet algorithme soit applicable en pratique. Dans la pratique, on dit souvent qu'un système est sûr si la meilleure attaque connue ne peut se faire dans un laps de temps de calcul raisonnable. Le problème de cette approche c'est que la sureté d'un cryptosystème est basée sur la non découverte d'un algorithme plus efficace.

Sécurité des cryptosystèmes biométriques

Des cas particulier de cryptosystèmes sont les cryptosystèmes biométriques car pour obtenir la clé il faut présenté une donnée biométrique. La sécurité de tels systèmes dépend donc avant tout de la partie biométrique, en particulier, elle dépend de la capacité que peuvent avoir les utilisateur pour berner le système en se faisant passer pour ceux qu'il ne sont pas. Autrement dit un tel système dépend du False Acceptance Rate (FAR). Le Système biométrique le plus sûr de ce point de vue serait celui dont le FAR est 0.

Dans ce qui suit nous allons traiter des Cryptosystèmes biométriques.

III.3. Les cryptosystèmes biométriques

III.3.1. Introduction

Nous avons vu dans le premier chapitre que la biométrie présente de nombreux avantages dont celui de rehausser niveau de sécurité comparativement au mots de passe en évitant le problème de l'oubli de mots de passe. De façon générale l'utilisation de la biométrie se fait par comparaison d'une donnée X' à une donnée X préenregistré quelques part. On détermine ensuite un niveau de proximité entre les deux données, puis, en fonction d'un degré de proximité seuil, on décide si la donnée permet de reconnaitre/d'identifier une personne ou pas. Le problème de sécurité que pose la biométrie est la protection de la donnée biométrique lors d'une transmission sur un réseaux ouvert par exemple.

Dans le cas de cryptosystèmes biométriques, la biométrie peut être utilisé pour protéger une clé cryptographique, tandis que la clé est utilisé pour protéger la donnée biométrique.

Il y'a trois façon majeur de lié la biométrie à la cryptographie [64]: biometrics key release (libération de la clé par biométrie), biometrics key generation (génération de clé par biométrie) et enfin biometrics key binding (liaison de la clé à la biométrie).

III.3.2. Liaison entre cryptographie et biométrie

Il existe trois façons différentes de lié la biométrie à la cryptographie et cela se fait selon trois modes:

Dans le mode **biometrics key release**: Il s'agit de protéger une clé qui sera libéré uniquement dans le cas d'une authentification par biométrie. Il s'agit d'un système biométrique protégeant un système cryptographique.

Dans le mode **biometrics key generation:** Dans un tel système la clé cryptographique est dérivée de la donnée biométrique. Cette donnée biométrique permet donc de calculer une clé cryptographique, qui serait unique, obtenu à partir du calcul sur la donnée biométrique.

Enfin de le mode **biometrics key binding:** Dans ce mode, le système lie une clé cryptographique avec les données biométriques de l'utilisateur au moment de l'enrôlement. La clé ne sera retrouvé que dans le cas d'une authentification réussi.

Les systèmes à génération et à liaison de clé semble plus sécurisé car dans les systèmes "release", l'authentification et la libération de la clé sont deux parties séparés. Cependant, quel que soit le mode de fonctionnement du cryptosystème biométrique, il existe une très grande différence dans la gestion d'une clé cryptographique et le fonctionnement d'un système biométrique. Cette différence réside dans le fait qu'un système cryptographique ne requiert pas un modèle de stratégie complexe pour la reconnaissance comme pour les systèmes biométriques. Les cryptosystèmes dépendent le plus souvent de l'exactitude de correspondance entre les clé. C'est-à-dire qu'il ne tolère pas un seul bit de différence. Les système biométrique quant à eux sont connu pour admettre une correspondance approximative dépendant d'un certain seuil de correspondance.

Le problème qui se pose alors est comment bâtir un pont entre l'impossibilité d'exactitude de la biométrie et la nécessité d'exactitude de la cryptographie.

III.3.3. Etat de l'art sur les cryptosystèmes biométriques

De nombreux travaux, sur différentes modalités biométrique, ont été effectuer sur les cryptosystèmes biométriques aussi appelé bio-cryptosystèmes. Ces cryptosystèmes biométriques peuvent être classés en trois catégories. Systèmes dédiés à l'authentification (key release et key binding), systèmes dédiés à la protection des données biométriques et systèmes qui assurent les deux aspects.

Nous nous intéressons ici plus aux deux modes considérés comme les plus sur, c'est-à-dire le mode key generation et key binding.

Le concept initial cryptographie utilisant l'empreinte digital est du à Tomko et al [65]. L'empreinte digitale était utilisée pour générer des nombres aléatoires qui à leurs tours étaient utilisés pour générer des clés.

Plus tôt Bodo [66] avait suggéré d'extraire une clé cryptographique à partir de données biométriques, l'inconvénient de la méthode proposé est qu'il est impossible de changé cette clé une fois qu'elle est compromise.

Pour les systèmes basé sur la protection de données biométriques nous pouvons cité Tuyls et al [76] qui propose d'utiliser une version une version modifier de la donnée biométrique . Dodis et al s'inspirent de ces travaux pour développer la notion de fuzzy extractors qui permettent d'extraire des clé fortes à partir de données bruitée variable et non uniforme.

Davida et al [77] sont les premier à faire des travaux sur des systèmes dédiés à l'authentification (key binding et key génération). Ils proposent de travailler sur l'Iris en utilisant sa texture. Toujours dans la même optique que Davida et al, Monrose et al propose de rendre un mot de passe plus sécurisé en le combinant à la dynamique de frappe. Ils proposent de mesurer des caractéristiques telles que la durée de frappe le temps de latence etc.

Une autre approche est proposé par Janbandhu et Siyal [67] cette approche suggère de générer une signature à partir d'une modalité biométrique en utilisant des algorithmes standard de cryptographie. L'avantage de leur méthode et que la clé peut être changé mais nécessite une exactitude du modèle biométrique, ce qui est irréaliste pour toutes les modalité à l'exception de l'ADN.

Bien d'autre systèmes ont été proposé par exemple Hao et Chen [68] ont travaillé sur les signatures écrites et ont défini 43 paramètres tel que la vélocité, la pression, l'altitude etc. Ils ont quantifier chaque caractéristiques en bit qui ont ensuite été concaténé en chaine binaire.

Juels et Wattenberg propose le protocole "fuzzy commitment scheme" [69] ou engagement flou. Cette méthode fait partie des systèmes dédié à l'authentification en mode key binding avec protection de données biométriques. Une donnée biométrique est supposé être en forme de chaine de caractères. On applique l'opérateur ensuite le XOR sur la chaine de caractère avec un mot. C'est le haché de cette valeur qui sera stocké ainsi que le mot qui à était utilisé pour faire le xor. Il suffit pour reconnaitre un individus d'effectuer le xor avec le même mot effectuer une correction d'erreur puis voir si les hachés correspondent.

En plus de ces nombreux protocoles Juels et Sudan [70] propose un nouveau protocole nommé fuzzy vault (ou encore coffre fort secret). ce protocole permet de disposé d'un code sur base d'une donnée biométrique, mais dans le cas du fuzzy vault il s'agit plutôt d'utilisé un polynôme p(x) à la place d'un mot de passe. Il est question ici de calculer les valeur de p(xi) les xi étant des valeurs extraites de données biométriques. On forme ainsi un ensemble de points (xi,p(xi)) dit R.. On rajoute a cet ensemble des points obtenus de façon aléatoire mais qui ne coïncide pas avec les points obtenus à partir des données biométriques. Pour authentifier un utilisateur il faut alors extraire ses données biométriques x'i. A partir de ces valeurs x'i on va rechercher dans l'ensemble des points R tous les points (xi,p(xi)) ayant des abscisses proches de x'i puis essayer de retrouver le polynôme. Si les données biométriques, de celui qui s'authentifie permettent de retrouver suffisamment de point pour retrouver le polynôme de départ alors il s'agit de la personne à identifier.

Pour notre travail nous allons voir avec plus de détails le fuzzy commitment et le fuzzy vault qui nous intéresse le plus.

III.3.4. Principe et fonctionnement du fuzzy commitment

L'idée globale de ce protocole est de s'abstraire de la comparaison à une donnée biométrique stocké. Juels et Wattenberg sont les premiers à proposer cette solution dites Fuzzy commitment, qui comme nous l'avons indiqué précédemment veut dire engagement flou.

La méthode dite du fuzzy commitment se décompose en deux étapes : enrôlement puis authentification. Habituellement en biométrie, l'étape d'enrôlement consiste à relever plusieurs fois la donnée biométrique de l'utilisateur (son empreinte par exemple) afin de

constituer une valeur de référence. L'étape d'authentification consiste ensuite à comparer la valeur à vérifier à la valeur de référence pour déterminer si l'utilisateur courant est bien celui attendu.

La méthode du fuzzy commitment suit ces deux étapes sauf que la valeur de référence stockée n'est pas une donnée biométrique et ne permet pas de retrouver la donnée biométrique utilisée pour la générer. Pour ce faire, le fuzzy commitment utilise un ensemble de mots de code dans $\{0,1\}^n$ et une fonction de hachage H .

Déroulement de l'enrôlement

1) Un utilisateur U présente son empreinte biométrique représentée sous la forme d'une suite x de n bits.
2) Le système choisit aléatoirement un mot de code c ∈ {0,1}n et calcule (c−x,H (c)).
3) Le fuzzy commmitment de l'utilisateur U est le couple (c−x,H (c)). Cette donnée est stockée, le reste est effacé.
4) A la fin de cette étape, le système authentifiera comme étant U tout utilisateur capable de produire une empreinte biométrique permettant de retrouver le mot de code c.

Déroulement de l'Authentification

Supposons qu'un utilisateur se présente sous l'identité de U et que son signal biométrique courant soit x'.Le système utilise x' pour vérifier l'engagement $(c-x,H(c))$. Pour cela, il faut:

1) Calculer (c−x)+x′. Si l'utilisateur était bien celui qu'il prétend être, alors son empreinte biométrique courante x′ devrait être proche de son empreinte biométrique de référence x et par voie de conséquence $(c-x)+x'$ devrait être proche de c, au sens de la métrique de Hamming. Si la distance entre $(c-x)+x'$ et c est inférieure à la distance du code, alors le mot de code c', le plus proche de $(c-x)+x'$ est égal à c. On utilise la notion de codes correcteurs.
2) Vérifier que $H(c') = H(c)$ où c' est le mot de code le plus proche de $(c-x)+x'$.

L'idée de Juels et Wattenberg apporte, en théorie, une solution au problème posé.

Malheureusement, leur approche repose sur l'hypothèse qu'une donnée biométrique dispose d'une représentation binaire standard, stable en taille et ordonnée. Ce qui n'est pas le cas en pratique pour des modalités comme l'empreinte digitale lorsque l'on utilise la caractérisation habituelle basée sur la localisation des minuties. La représentation n'est pas stable en taille puisqu'une minutie peut apparaître ou disparaître suivant la qualité de la capture. La représentation n'est pas non plus ordonnable, pour la même raison.

Notions de codes correcteurs

Nous ne présentons ici que les notions de codages utiles à la compréhension du schéma. Les codes correcteurs d'erreurs sont utilisés de façon à permettre la correction des erreurs de transmission d'un message sur un canal de communication. Les codes reposent sur l'ajout d'information redondante au message avant sa transmission. La redondance d'information permet de détecter la présence d'erreurs si le message reçu est changé (codes

détecteurs), voire de reconstituer le message original (codes correcteurs). Dans ce schéma, ce sont les codes correcteurs qui sont utilisés pour atténuer les variations du signal biométrique. Formellement, un code correcteur d'erreur sur un espace de message M = $\{0,1\}^k$ consiste en un ensemble de mots de code C ⊂ $\{0,1\}^n$ où n > k. L'ensemble C est associé à une fonction d'encodage que nous noterons encode et à une fonction de décodage que nous noterons decode.

La fonction encode est une injection M →C qui associe à chaque mot m de k bits de M un unique mot de code c de C. La fonction decode est une application de {0,1}n →C∪∅ qui fait correspondre à chaque mot m de n bits le mot de code le plus proche de m quand cela est possible et ∅ sinon. La métrique utilisée est la distance de Hamming selon laquelle la distance entre deux chaînes de bits de même longueur est le nombre de bits dont elles diffèrent. La distance d'un code est la plus petite distance entre 2 mots de codes. Pour qu'un mot de n-bits puisse être décodé, il faut qu'il soit à une distance inférieure à $\frac{d-1}{2}$ d'un mot du code et donc avoir au plus $\frac{d-1}{2}$ erreurs. Le pouvoir de correction d'un code est la distance minimale à un mot de code pour qu'un message puisse être décodé.

Utilisation des codes correcteur en Fuzzy commitment

Comme cela a été expliqué, les codes correcteurs implique un changement d'une information ou d'un message en un mot de code proche. Cependant dans le cas de la biométrie, on à pas la possibilité de rajouter des informations redondante à la donnée biométrique. La donnée biométrique est juste considéré comme un mot de code déjà corrompu. Par conséquent, il n'y a pas de liaison entre un espace de message M à l'ensemble de mot de codes, en fait, il n'y a pas d'espace de message M. On ne recourt qu'à la moitié du processus de correction d'erreur en utilisant que la fonction decode.

III.3.5. Fuzzy vault

Juels et Sudan ont proposé une autre approche appelée fuzzy vault dans [70]. L'authentification d'un utilisateur repose, là encore, sur sa capacité à présenter une donnée biométrique permettant de retrouver un secret. Le secret en question est un polynôme P de degrè n. Lors de l'étape d'enrôlement, le système calcule un fuzzy vault V , littéralement coffre fort flou, à partir de P et de l'ensemble des minuties de l'empreinte de l'utilisateur. L'utilisateur est authentifié lorsqu'il est possible de retrouver P à partir de V et des données biométrique qu'il fournies. Plus précisément, l'algorithme de Juels et Sudan peut se présenter comme suit :

Enrôlement

Considérons un utilisateur U, l'ensemble des caractéristiques $\{a_i\}_{1\leq i\leq t}$ apparaissant dans capture de donnée biométrique et un polynôme P de degré k où $t > k$. Nous calculons tout d'abord l'ensemble des points $R_1 = \{(a_i, P(a_i)\}_{1\leq i\leq t}$. Nous générons ensuite un second ensemble de points $R_2 = \{(x_j, y_j\}_{1\leq j\leq n}$ tels que $x_j \neq a_i$ et $y_j \neq P(a_i)$ pour tout $1 \leq i \leq t$ et tout $1 \leq j \leq n$. L'ensemble R_2 est destiné à brouiller l'information venant de R_1. Le coffre-fort flou de l'utilisateur U est l'ensemble $V_U = R_1 \cup R_2$. Cet ensemble est rendu publique, le reste est effacé.

Authentification

Lorsqu'un utilisateur souhaite s'authentifier en temps que U, il présente sa modalité biométrique et l'ensemble des caractéristiques de cette modalité $\{b_i\}_{1\leq i\leq t'}$ sont extraites. Nous sélectionnons ensuite dans V_U l'ensemble des points de la forme (x,y) où x est proche d'une valeur b_i. Si la donnée biométrique proposée est suffisament proche de la donnée de l'utilisateur U alors ce procédé permet de retrouver suffisamment de points de R_1 pour pouvoir reconstruire P par interpolation de Lagrange. Si c'est le cas, l'utilisateur est authentifié en tant que U.

L'approche du fuzzy vault présente l'avantage d'être utilisable en pratique. Clancy et Dennis ont présenté dans [18] de bons résultats pratiques en prenant P un polynôme de degré 14 dans $F_q[X]$ où $q = 251^2$. Ils proposent de publier un ensemble V_U de 313 points contenant entre 25 et 60 vrais points. L'étude de Clancy et Dennis s'appuie sur une représentation pré-alignée des minuties, dans Uludag et Jain présentent dans [74] une étude similaire dans laquelle les minuties ne sont pas pré-alignées. Le problème de cette seconde méthode est qu'elle nécessite de publier un ensemble de points dans lequel certaines abscisses correspondent à des minuties. C'est la faiblesse de cette approche. Si cette approche était utilisée, il faudrait, en pratique, renouveler régulièrement l'ensemble des points publiés. L'ensemble des vrais points se définirait alors simplement par l'intersection de tous les ensembles publiés. Par ailleurs, Chang et Li ont étudié dans [75] le problème général du calcul d'un ensemble de valeur R_2 destiné à masquer un autre ensemble R_1. Leur travail a montré que le calcul de R_2 est difficile dès que la distribution des points de R_1 n'est pas uniforme.

III.3.6. Synthèse

Nous avons choisit de nous concentrer sur le fuzzy Vault, et le fuzzy commitment qui sont des schéma dits *Key binding.* Ils ont l'avantage sur les systèmes *Key release* et *Key generation* d'être plus sûr notamment par le fait que les modules de biométrie et de cryptographie sont liée (par rapport à *Key release*) et aussi il est possible de changer la clé cryptographique qui n'est pas générer à partir de la donnée biométrique.

Les deux méthodes sur lesquelles nous nous sommes focalisé utilise toutes des codes correcteurs d'erreur. Dans tous les ouvrages que nous avons pu voir, il est proposé d'utiliser des codes correcteurs d'erreur linéaire, et en particulier le code Reed Solomon.

la méthode du fuzzy commitment de Juels et Wattenberg présente l'avantage par rapport à celle du fuzzy vault de ne pas publier des données permettant pas de recalculer les données biométriques de l'utilisateur. Cependant il pose un certain nombre de problème tel que la nécessité d'avoir des données biométriques uniformisé et nécessitant une représentation canonique et stable des caractéristiques biométriques, alors que ce n'est pas le cas pour les empreintes digitales par exemple car ces caractéristiques biométriques sont présentées par des minuties qui peuvent apparaitre ou disparaitre suivant la capture.

De même que le schéma de Juels and Wattenberg, le fuzzy vault est conceptuellement simple et peu être implémenté en utilisant n'importe que code correcteur. Il possède l'avantage

de ne pas imposé que les données à analysé soit ordonné ou canonique et de permettre une analyse simple de données non uniforme, cependant, il nécessite plus de mémoire et sa complexité algorithmique est plus grande que celle du fuzzy commitment.

Cette partie sur la biométrie nous à permis de faire un pont entre la biométrie et la cryptographie. Nous avons pu fixer les bases nécessaires à notre travail.

Pour la suite de notre travail nous avons choisi d'utiliser le fuzzy commitment par rapport au fuzzy vault car celui-ci présente deux avantages considérable par rapport au fuzzy vault à savoir:

1) Protection de la donnée biométrique: La données biométrique n'est pas stocké, et il est impossible à partir des données enregistré de retrouver la donnée biométrique si on ne la possède pas déjà.
2) La simplicité algorithmique: Alors que le fuzzy vault est basé sur des opérations polynomiale, le fuzzy commitment lui se base sur des opérations de soustraction et d'addition, ce qui représente un gros avantage quant à l'implémentation sur des appareil de faible puissance de calcul tel que les systèmes embarqués.

Pour développer cette méthode nous allons utiliser une modalité biométrique permettant d'obtenir des données biométriques canonique car le fuzzy commitment comme vu précédemment nécessite des données de format bien déterminer et précise en terme de taille et d'ordre.

Nous allons nous servir de l'iris comme modalité biométrique pour les nombreux avantages de cette modalité décrits dans le chapitre premier.

III.4. conclusion

Dans ce chapitre, nous avons présenté la cryptographie, ainsi que les cryptosystèmes biométriques. Nous avons commencé par parler des principales primitives cryptographiques à usage générales. Nous avons également vu les principaux algorithmes et primitives cryptographiques spécialisé. Nous avons après cela fait eu un aperçu sur les cryptosystèmes en générales et de la sécurité des systèmes biométriques avant de parler des cryptosystèmes biométriques en particulier. Nous avons également rappelé les notions de correction d'erreur.

S'agissant des cryptosystèmes biométriques nous avons fait un rapide état de l'art avant de parler plus spécialement des méthodes fuzzy commitment et fuzzy vault. L'avantage de ces méthodes est de ne pas stocker de données biométriques protégeant ainsi la vie privée de l'utilisateur mais aussi en protégeant une clé cryptographique. Ces deux méthodes permettent de pouvoir révoquer la donnée secrète si celle ci était compromise, sans que la donnée biométrique soit compromise pour autant.

Le plus gros du travail pour ce chapitre à été de consulter la littérature en rapport avec les cryptosystème biométriques, cela nous permet dans ce qui suit à commencer en pratique la réalisation de notre cryptosystème.

CHAPITRE QUATRIÈME

CONCEPTION ET RÉALISATION

IV.0. Introduction

Après avoir étudié l'état de l'art en cryptosystème biométrique, nous allons dans le présent chapitre décrire la démarche de conception et de réalisation de notre application. Pour ce mémoire, l'objectif de notre application est d'être en mesure d'authentifier un utilisateur à l'aide d'une donnée biométrique et d'une clé sans passer par le stockage de la donnée biométrique et sans avoir à utiliser la clé. La donnée biométrique sert à protéger la clé et inversement la clé permet de ne pas avoir à stocké la donnée biométrique protégeant ainsi la donnée biométrique.

L'application que nous avons réalisé va nous servir d'avantage à des fin de test. Le plus gros du travail est plutôt algorithmique est le nombre d'interfaces d'utilisation de l'application en est réduit.

IV.1. Conception

Dans le chapitre dédié à la biométrie nous avons donné l'architecture de tout système biométriques. C'est sur cette même architecture que nous avons basé la réalisation de notre application.

IV.1.1. Acteur du système

Notre application peut avoir deux acteurs à savoir:

- Un administrateur: qui va s'occuper de l'enrôlement de la personne à authentifier, ainsi que de son authentification ultérieur. Cet administrateur peut également effectuer des test de performance de l'application.
- Un individu test: cherchant à s'authentifier ou demandant un enrôlement.

IV.1.2. Diagramme des cas d'utilisation

Nous savons qu'un système biométrique est composé au moins un module pour l'enrôlement et d'un module de reconnaissance. Notre application aura donc ces ceux modules ci-haut mentionnés auxquels nous allons rajouter un module d'évaluation. Dans notre cas la reconnaissance sera une authentification.

A partir de cela nous obtenons le diagramme des cas d'utilisation décrit par la *figure IV.1*. A partir de ce diagramme des cas d'utilisation nous pouvons faire une description textuelle des cas d'utilisation.

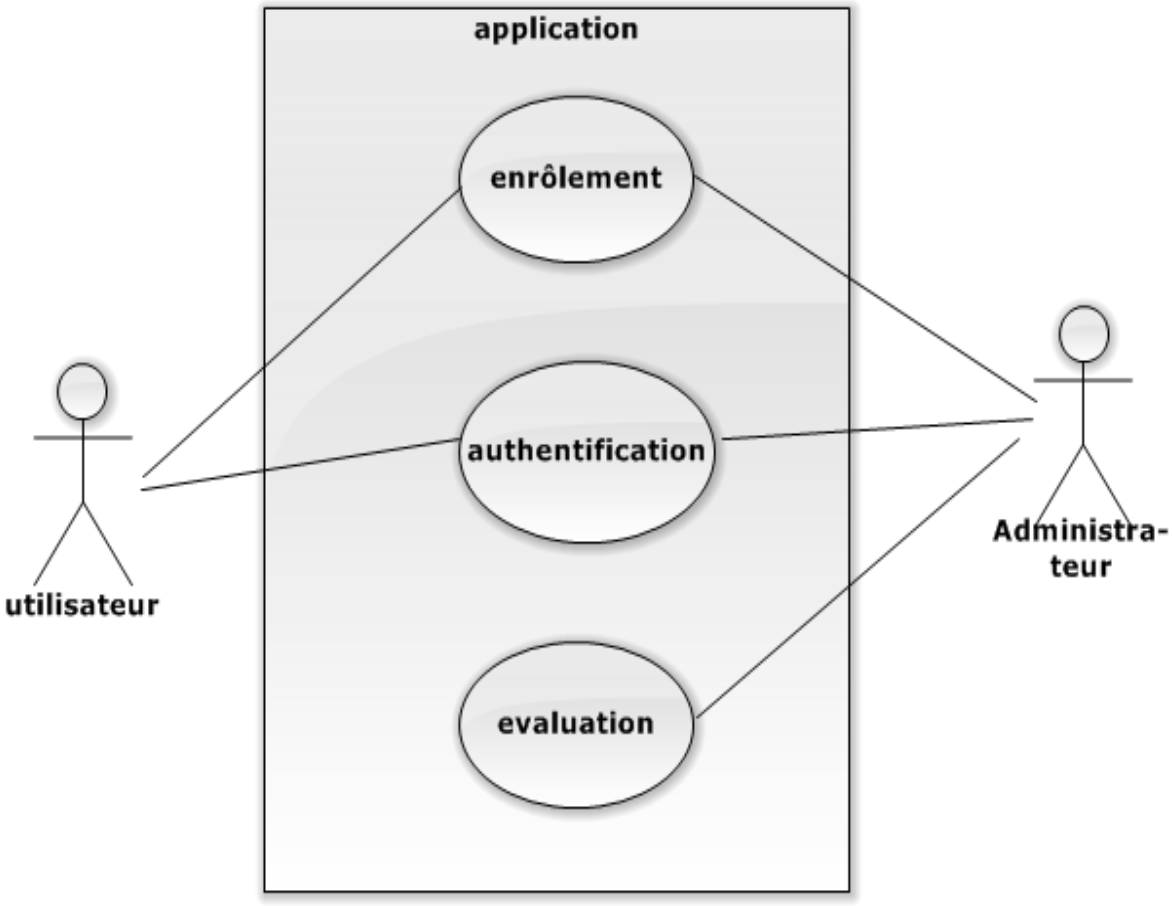


Figure IV.1: Diagramme des cas d'utilisation

Il est possible que l'administrateur et l'utilisateur soit une même personne.

IV.1.3. Description textuelle des cas d'utilisation

Nous procédons à la description textuelle des cas d'utilisations de notre application. La description d'un cas d'utilisation se fait en scenario.

Un *scénario* représente une succession particulière d'enchaînements, s'exécutant du début à la fin du cas d'utilisation, un *enchaînement* étant l'unité de description de séquences d'actions[78].

Un cas d'utilisation contient en général un scénario nominal et plusieurs scénarios alternatifs (qui se terminent de façon normale) ou d'erreur (qui se terminent en échec). On peut d'ailleurs proposer une définition différente pour un cas d'utilisation : « ensemble de scénarios d'utilisation d'un système reliés par un but commun du point de vue d'un acteur »[78].

Dans ce qui suit, nous décrivons le fonctionnement de l'application, afin d'en faciliter la réalisation.

- **Cas d'utilisation: Enrôler l'utilisateur**

Titre: Enrôler l'utilisateur

Résumé: Ce cas d'utilisation permet à l'utilisateur de se faire enrôler comme paramètre à un prétraitement en vue d'une reconnaissance ultérieure de l'individu appris.

Acteurs: Utilisateur, Administrateur. **Date de mise à jour:** 18/07/2017

Date de création: 02/07/2017 **Responsable:** MAWUENA RUKUNDO Aristide Alexis

Description du scenario:

Pré-condition:

Ouvrir le répertoire contenant l'application dans matlab.

Scénario nominale:

1) L'utilisateur lance l'application en lançant la commande Biocryptosys.
2) Le système affiche l'interface d'accueil.
3) L'utilisateur clique sur le bouton "Enrôler l'utilisateur".
4) Le système lance une nouvelle interface servant à l'enrôlement de l'utilisateur
5) L'utilisateur saisi une clé
6) L'utilisateur charge un iris en appuyant sur sélectionner l'iris.
7) L'administrateur lance le cryptage des information en appuyant sur le bouton calculer
8) Le système extrait les caractéristiques de l'iris.
9) Le système effectue génère un mot de code.
10) Le système effectue le cryptage simultané de la clé et des caractéristique de l'iris.
11) Le système enregistre un haché de la clé et le résultat du cryptage de la clé avec les caractéristiques de l'iris
12) le système indique que les calculs sont terminés.

Scénario alternatif:

A1: L'utilisateur ne choisit pas d'iris.
L'enchaînement démarre au point 7) du scénario nominal.

8) Le système signale à l'utilisateur qu'un iris n'a pas été selectionné.
9) L'utilisateur sélectionne un iris.

Le scénario nominal reprend au point 7).

Scénario alternatif:

A2: l'utilisateur ne saisit pas de clé ou ne saisit pas de correspondant aux exigences de taille.
L'enchaînement démarre au point 7) du scénario alternatif.

8) L'utilisateur entre à nouveaux une clé.

Le scénario nominal reprend au point 7).

- **Cas d'utilisation: Authentifier l'utilisateur**

Titre: Authentifier l'utilisateur

Résumé: Ce cas d'utilisation permet à l'utilisateur de se faire authentifier à partir uniquement de son iris.

Acteurs: Utilisateur, Administrateur.

Date de mise à jour: 18/07/2017

Date de création: 02/07/2017

Responsable: MAWUENA RUKUNDO Aristide Alexis

Description du scenario:

Pré-condition:

Ouvrir le répertoire contenant l'application dans matlab.

Scénario nominale:

1) L'utilisateur lance l'application en lançant la commande Biocryptosys.
2) Le système affiche l'interface d'accueil.
3) L'utilisateur clique sur le bouton "Authentifier l'utilisateur".
4) Le système lance une nouvelle interface servant à l'authentification de l'utilisateur
5) L'utilisateur charge un iris en appuyant sur sélectionner l'iris.
6) L'administrateur lance le déchiffrement des information en appuyant sur le bouton Authentifier
7) Le système extrait les caractéristiques de l'iris.
8) Le système charge l'empreinte de la clé ainsi que les informations mutuellement crypté de la clé et de l'iris.
9) Le système effectue le déchiffrement de la clé à partir des caractéristique de l'iris puis hache le résultat.
10) Le système compare l'empreinte de la clé à l'empreinte obtenu par déchiffrement avec l'iris
11) le système indique si l'authentification à réussi ou échoué.

Scénario alternatif:

A2: L'utilisateur ne choisit pas d'iris.

L'enchaînement démarre au point 6) du scénario nominal.

7) Le système signale à l'utilisateur qu'un iris n'a pas été selectionné.
8) L'utilisateur sélectionne un iris.

Le scénario nominal reprend au point 6).

- **Cas d'utilisation: Evaluer le système**

Titre: Evaluer le système

Résumé: Ce cas d'utilisation permet de savoir dans quel mesure le système est performant et va servir à tester l'application

Acteurs: Administrateur.

Responsable: MAWUENA RUKUNDO Aristide Alexis

Date de création: 02/07/2017

Description du scenario:

Date de mise à jour: 18/07/2017

Pré-condition:

Ouvrir le répertoire contenant l'application dans matlab.

Scénario nominale:

1) L'administrateur lance l'application en lançant la commande Biocryptosys.
2) Le système affiche l'interface d'accueil.
3) L'administrateur clique sur le bouton "Evaluer le FRR et FAR".
4) Le système lance une nouvelle interface servant à évaluer le FRR et FAR
5) L'administrateur choisit l'indice à calculer
6) Le système calcul les valeurs demander puis les affiches à la fin

Après avoir expliciter dans ce paragraphe la conception, de manière théorique de notre systèmes, nous allons présenter son implémentation.

IV.2. Réalisation

Après ce paragraphe qui traite de la phase de conception de notre application, nous pouvons dès à présent voir ce qui concerne son implémentation et parler de façon globale de l'environnement de travail, des outils, tant matériels que logiciels, utilisés pour le développement de notre application.

IV.2.1. Matériel de développement

Nous avons développé notre application sur un ordinateur portable de marque Toshiba et ayant les propriétés suivante:

Modèle	Satellite P870
Processeur	Intel Core i7 -3600QM
Ram	8079 Mo
Processeur	2.30 GHz
Système d'exploitation	Windows 7 édition Familiale Premium 64-bit

Tableau IV. 1: Matériel de développement et de test

IV.2.2. Outil logicielle

Pour le développement de notre application nous avons utiliser l'outils logicielles MATLAB. Le choix de l'outil de programmation s'est fait le critère de la puissance du à la lourdeur des calcul à effectuer par notre application.

MATLAB est une abréviation de Matrix LABoratory. Écrit à l'origine, en Fortran, par Cleve Moler a la fin des années 1970, optimisé pour le traitement des matrices, d'où son nom. MATLAB est un environnement puissant et complet en plus il est disponible sur plusieurs plateformes. C'est un environnement ouvert et programmable qui permet de gagner en de productivité et en créativité. MATLAB permet également d'effectuer une programmation d'interface graphique.

Nous avons implémenté l'application de cryptographie biométrique dans l'environnement de programmation **MATLAB 2010a**. Il est possible que des version plus récente de l'environnement offre de meilleurs résultats.

Cet outil de programmation possède un langage qui à des avantages très intéressants pour les applications sur l'image et qui permet également une facilité de programmation : La portabilité de logiciel (simplifie le processus de programmation sous Windows) et un facilité de manipulation des matrices ce qui est important dans le cas de notre application.

IV.3. Présentation de l'application.

Notre application ne se compose que de trois interfaces à savoir:

IV.3.1. interface d'accueil

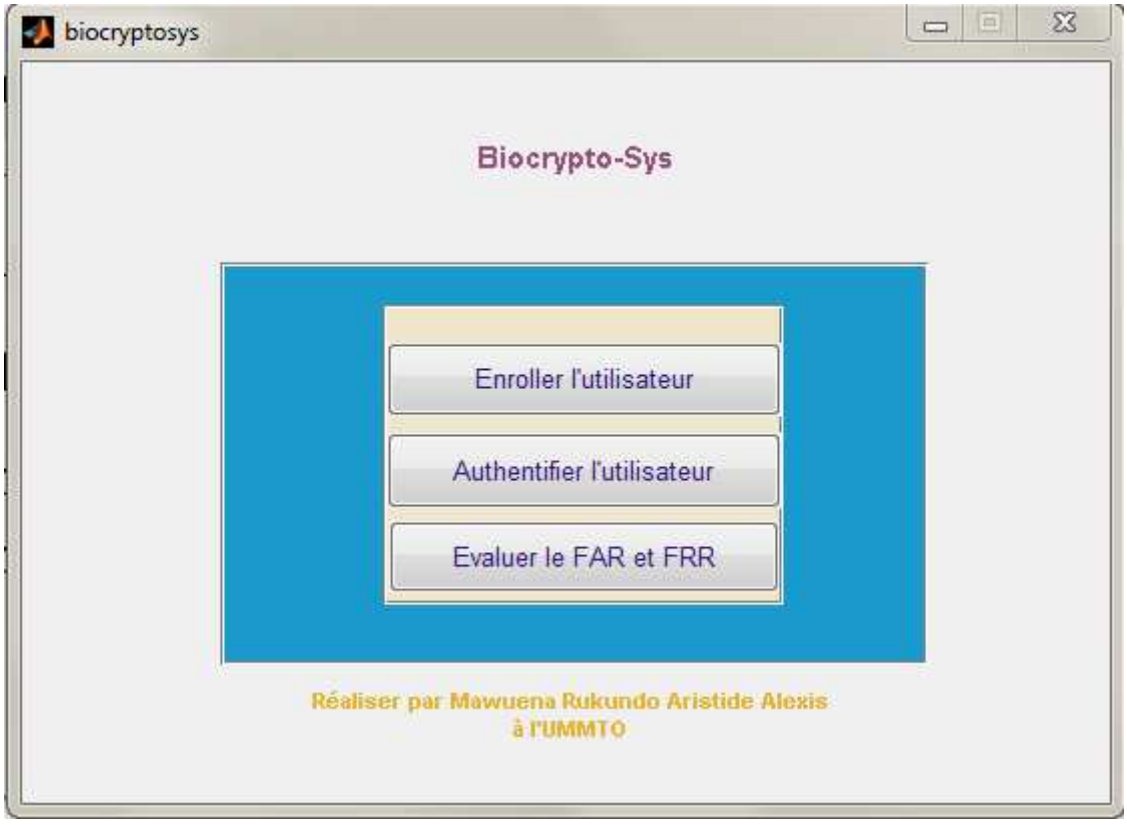


Figure IV.2:Interface d'accueil

Sur cette vue nous remarquons qu'il y a trois boutons qui renvoie aux trois autres activités principales de notre application.

IV.3.2. L'interface d'enrôlement

Les vues suivantes permettent d'illustrer les interfaces rencontré au cours de l'enrôlement.

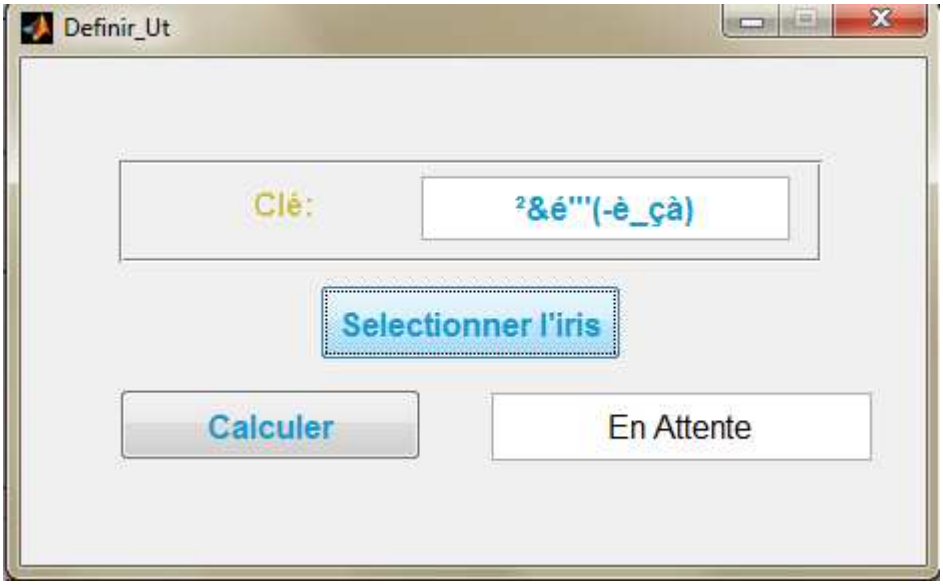


Figure IV. 3: Interface d'enrôlement

Lorsqu'on clique sur sélectionner l'iris une nouvelle fenêtre qui permet d'explorer le contenu de l'ordinateur apparait pour permettre de sélectionner un iris:

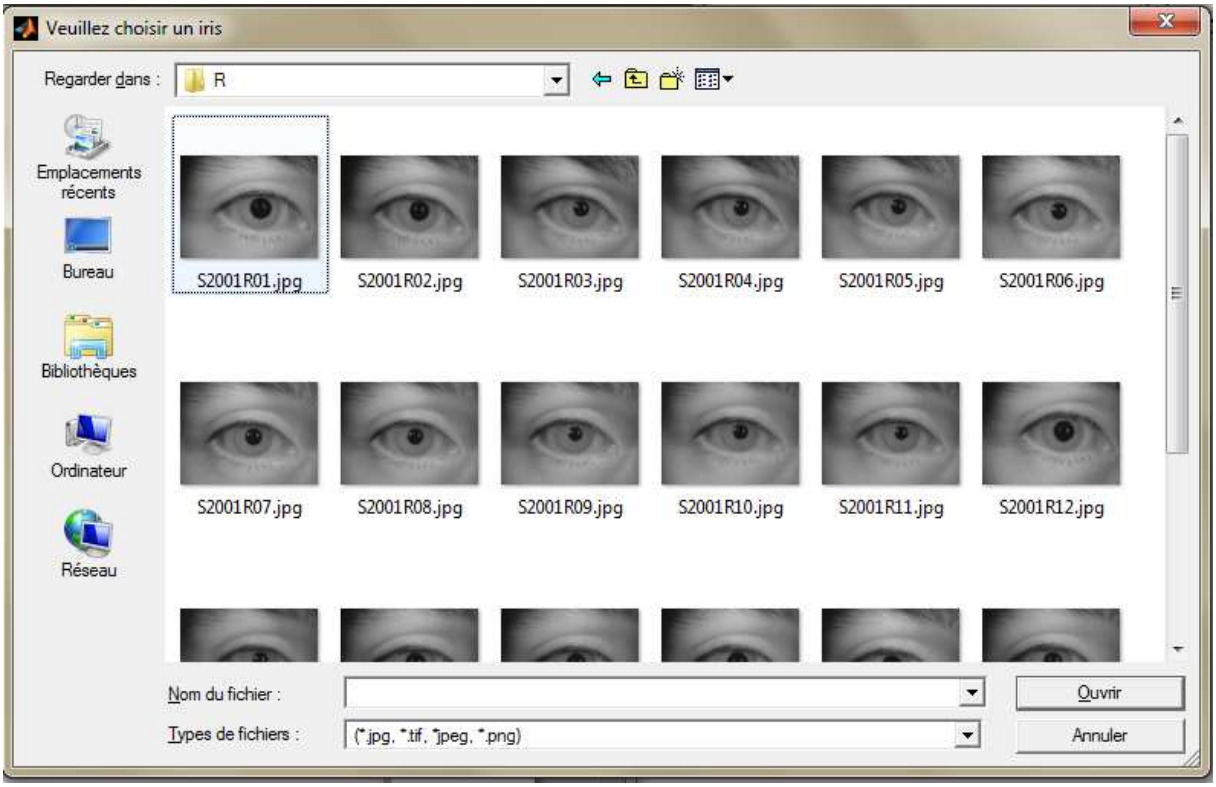


Figure IV.4: Explorateur de l'application

IV.3.3. Authentification de l'utilisateur

Cette interface permet de sélectionner un iris afin d'authentifier l'utilisateur.

Figure IV.5: Interface d'authentification

Cette interface donne également accès à un explorateur permettant de sélectionner une image d'iris.

IV.3.4. Interface d'évaluation

C'est par cette interface que nous pouvons évaluer la performance de notre application.

Figure IV.6: Interface d'évaluation

C'est grâce à cette partir de l'application que nous avons pu déterminer la taille optimal de la clé à utiliser dans notre application. Nous allons aborder plus en détail l'évaluation de notre application dans le chapitre suivant.

IV.4. Conclusion

Dans ce chapitre nous avons abordé la conception et la réalisation de notre cryptosystème biométrique. Nous avons présenté les outils tant matériels que logiciels utilisés pour son développement. Nous avons également présenté le langage utilisé pour sont développement. Enfin nous avons présenté les interfaces utilisateurs de notre application. Pour ce travail sur la biométrie de l'Iris nous nous sommes basé sur les travaux de Libor Masek. [80]

Dans ce qui suit nous allons présenter les résultats aux tests de notre cryptosystème biométrique.

CHAPITRE CINQUIÈME

TESTS EXPÉRIMENTAUX ET RÉSULTATS

V.0. Introduction

Dans ce dernier chapitre nous allons traiter des performances de notre application. Pour évaluer notre application nous avons utiliser deux critères servant à déterminer la précision de l'application. Ces deux critères dont nous avions déjà parlés ultérieurement sont le FAR et le FRR. Pour rappel le FRR désigne le taux de faux rejet, où des individus légitimes ne sont pas reconnu, et le FAR désigne plutôt le taux de fausse acceptation, où des individus non légitimes sont reconnus.

Pour calculer le FRR nous effectuons une tentative d'authentification de chaque iris par rapport aux autres iris de sa classe (du même individu). Il suffit alors de divisé ce nombre par le nombre de test effectué.

Quant au FAR, nous l'avons calculer en essayant d'authentifié des personnes non légitime. un iris d'une classe est comparer à un iris de toutes les autres classes puis on divise par le nombre de tests effectués.

Nous avons aussi testé notre application par rapport à la taille des clés. Théoriquement avant de lancer les tests nous avons pensé que plus la clé serait petite, plus la capacité de corriger les erreurs des mots de code Reed Solomon serait grande et plus le FRR serait petit, mais cela implique que le FAR serait également élevé. Nous avons tenter de voir si cette théorie est vérifié, de plus nous avons chercher à voir quels seraient les effets de la variation de temps d'exécution par rapport à la longueur des clés.

Avant de présenter les résultats obtenus nous allons dans ce qui suit parler de la base de données utilisée pour notre évaluation.

V.1. La base de donnée CASIA

Pour répondre à des nécessités de recherche et de développement de solutions biométriques basée sur l'iris, un groupe de recherche de la Chinese Academy of Sciences' Institute of Automation (CASIA) à développer une base donnée, l'a mise à la disposition de la communauté biométrique internationale [79] et continue à la développer depuis 2002. Plus de 3000 utilisateurs depuis 70 [79] pays l'ont téléchargée et l'ont utilisé pour leurs travaux.

Cette base de donné CASIA contient des milliers d'iris contenu dans différents sous ensembles pouvant être utilisés selon les nécessité de recherche.

Les sous ensembles de la base de données CASIA sont:

- **CASIA-Iris-Interval**: contenant les iris ayant une très bonne qualité d'image pour un meilleur travail sur la texture de l'iris.

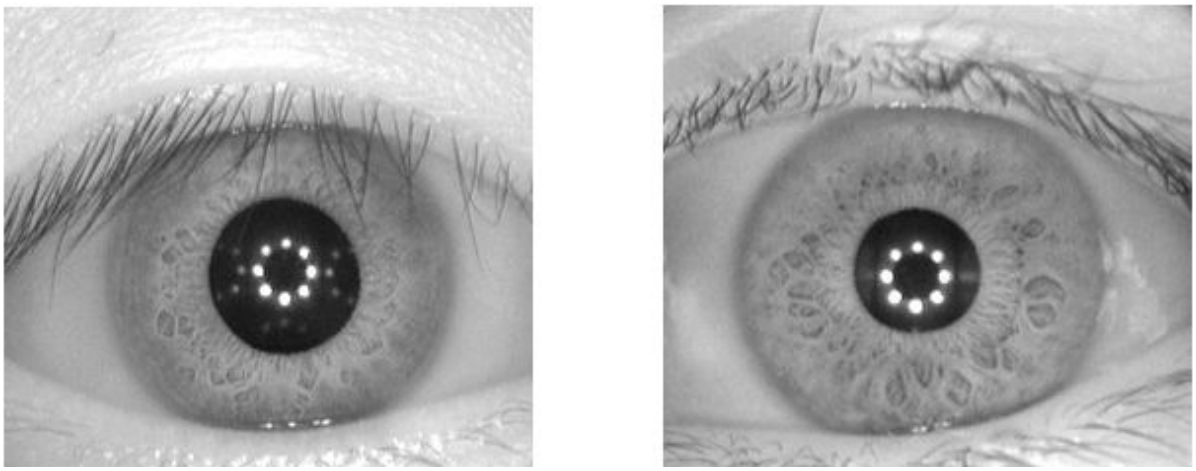


Figure V. 1: Exemple d'iris de la base CASIA-Iris-Interval

- **CASIA-Iris-Lamp**: Contenant des iris prise avec des variations de condition d'éclairage pour produire plus de variation intra-classe. cet ensemble contient des iris avec des déformations élastique du à l'expansion et à la contraction de la pupille qui se rapproche beaucoup des conditions réelles.

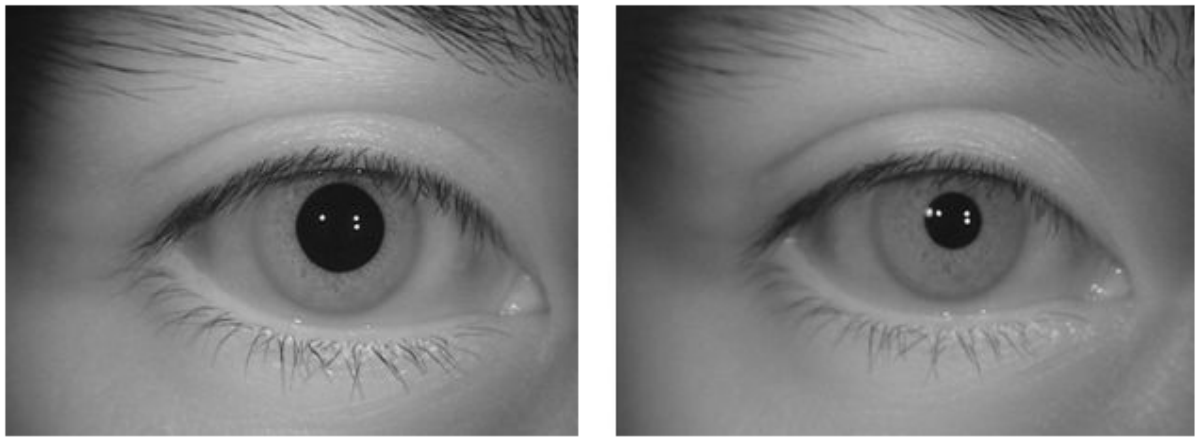


Figure V. 2: Exemple d'iris de la base CASIA-Iris-Lamp

- **CASIA-Iris-Twins:** Contient les images d'iris de 100 pairs de jumeaux pour permettre le travail sur les similarités et différences des iris des jumeaux.

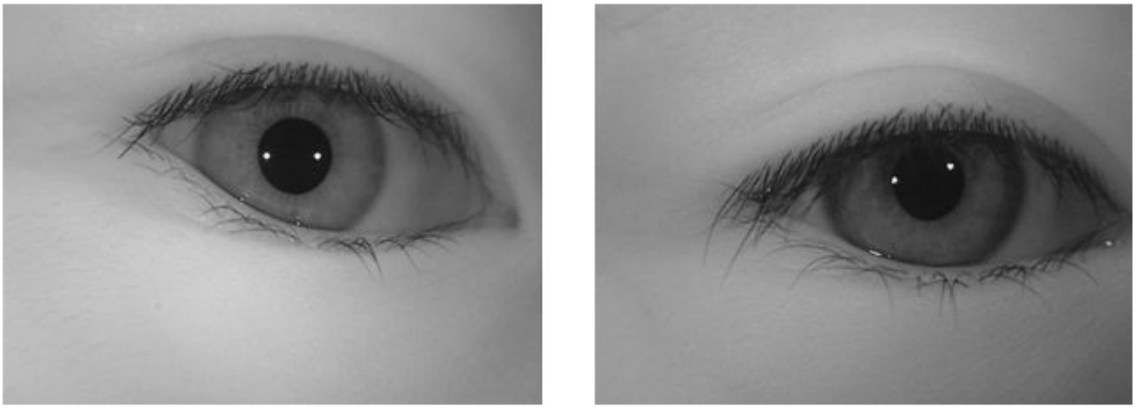


Figure V. 3: Exemple d'iris de la base CASIA-Iris-Twins

- **CASIA-Iris-Distance**: Contient des images d'iris prises à distance comprise entre 2.4 et 3 m.

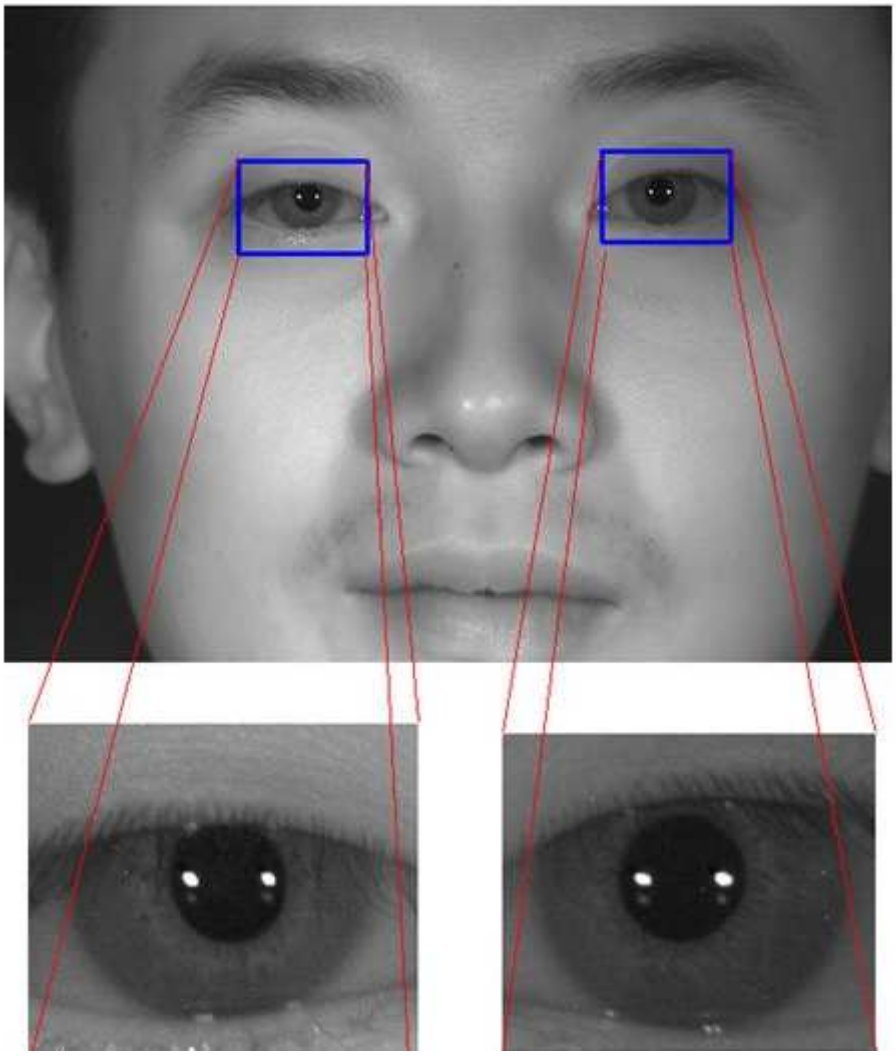


Figure V. 4: Exemple d'iris de la base CASIA-Iris-Distance

- **CASIA-Iris-Thousand**: contient 20,000 images d'iris de 1000 sujets. La source principale de variation à l'intérieur d'une classe est due au port de lunette ou de réflexion de lumière

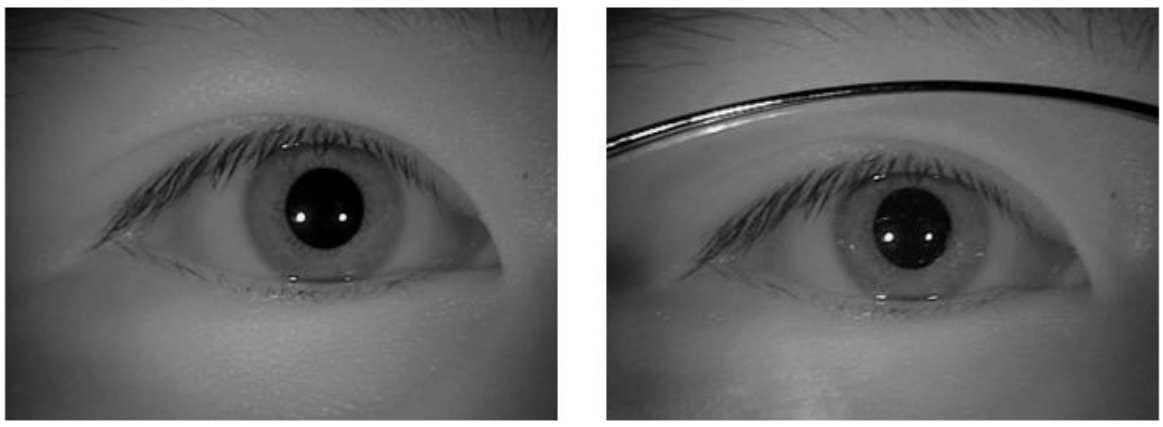


Figure V. 5:Exemple d'iris de la base CASIA-Iris-Thousand

- **CASIA-Iris- Syn**: contient 10,000 images de 1000 classes. La particularité de cette classe est qu'elle est composé d'image d'iris synthétisées. Ces images sont visuellement réaliste et il est très difficile de les distingué visuellement des vrai iris.

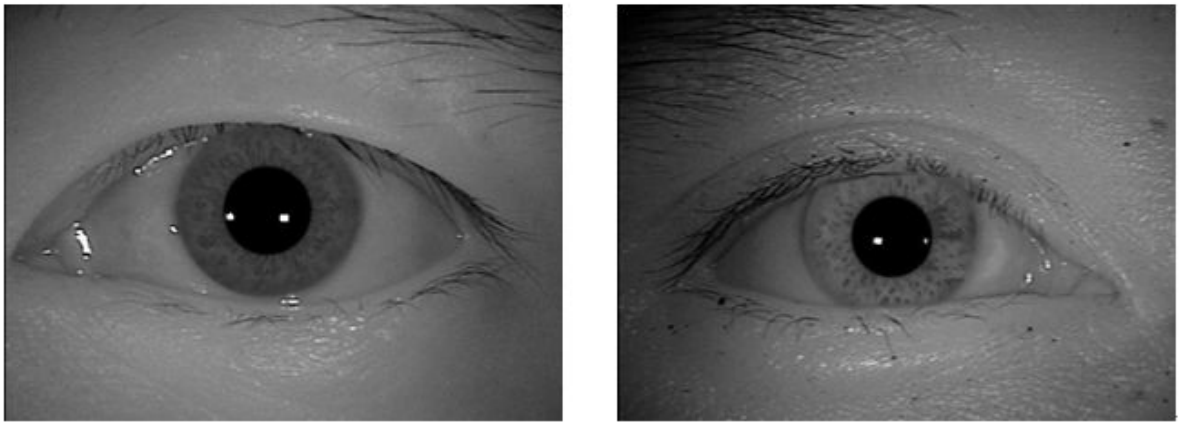


Figure V. 6: Exemple d'iris de la base CASIA-Iris-Syn

Pour notre mémoire nous avons utilisé le sous ensemble CASIA-Iris-Lamp Contenant des iris prise avec des variations de condition d'éclairage impliquant les déformation élastique de l'iris. œil

Les règles de nommage de chaque image dans ce sous ensembles sont les suivantes:

- $chemin d'accès$/CASIA-Iris-Lamp/YYY/E/S2YYYENN.jpg
- YYY: Identifiant unique du sujet dans le sous ensemble
- E: ‘L’ dénote l'œil gauche and ‘R’ dénote l'œil droit
- NN: l'index de l'image dans la classe.

V.2. Implémentation des test et déroulement

Comme nous l'avons indiqué dans le chapitre précédent nous avons rajouter à notre application une partie pour l'évaluation. Cette partie permet de tenter plusieurs authentification à la fois sans avoir à le faire manuellement.

Pour pouvoir faire plusieurs tests automatiques nous avons du modifié la base de donnée utilisé et placé des iris dans un même dossier en les organisant de façon à avoir 5 iris par classe les uns à la suite des autres. nous avons utilisé 10 classes pour les tests.

Nous avons fixé différentes taille de clés. Les tailles de clé choisi pour les tests sont: 130 bits, 250 bits, 510bits, 810bits, 1010 bits, 2010bits et 5010bits.

Les résultats obtenu lors de l'évaluation sont indiquer dans le tableau suivant:

	FRR		FAR	
taille de la clé	Valeur	Temps (sec)	Valeur	Temps (sec)
130 bits	0,4	518,29	0,6444	818,36
250 bits	0,43333	643,79	0,62222	1006,25
510 bits	0,43333	670,27	0,51111	883,592
810 bits	0,46667	609,95	0,42222	953,27
1010 bits	0,46667	595,98	0,35556	926,133
2010 bits	0,6	492,88	0,17778	674,2
5010 bits	0,8	198,5	0,022222	288,595

Tableau V.1: résultats des tests d'évaluation

Commentaire: Nous constatons comme nous l'avions prédit théoriquement que plus la clé est petite le FRR est petit et le FAR est grand ceci est expliqué par la capacité de correction qui est grande, ce qui permet d'accepter la majorités des personnes légitimes mais aussi de laisser la chance même aux intrus qui auraient présentés des modèles proches de personnes légitimes (d'où FAR est grand). En augmentant la taille de la clé, la capacité de correction diminue freinant ainsi une personne légitime à s'authentifier(d'où le FRR grand) et du coup même les intrus sont freinés (FAR petit).

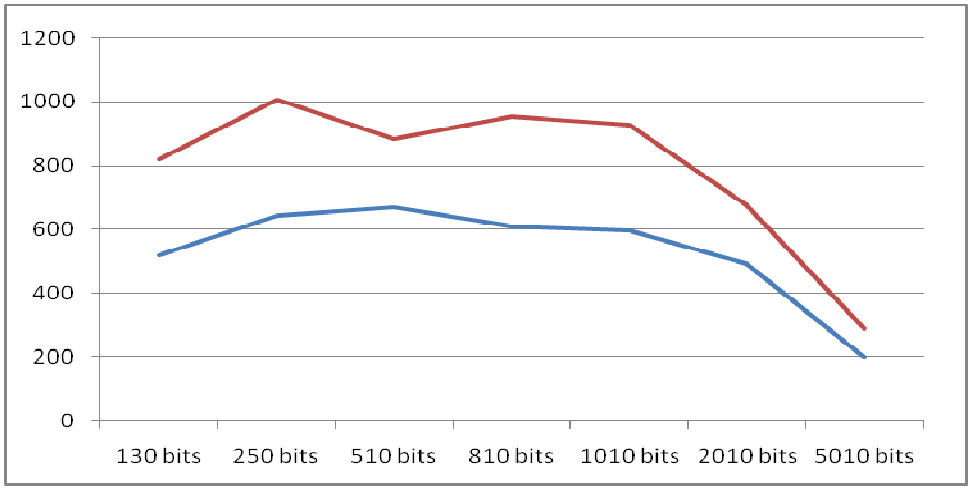
Pour mieux illustrer ces résultats nous avons tirés les graphe suivant:

→: Taux du FAR,

→:Taux du FRR

Figure V. 7: Variation des taux d'erreur en fonction de la taille de la clé

Une deuxième courbe (Figure V.8) représente les temps d'exécution pour les calculs des deux taux. Nous constatons qu'il y'a une forte variation du temps d'exécution en fonction de la taille de la clé. Nous constatons que la courbe le temps en seconde à tendance à être moyen pour des petites valeurs de clé. Ce temps augmente, Pour des tailles de clé moyenne puis se remet à chuté vers une valeur assez basse.



→: Temps de calcul du FAR,

→:Temps de calcul du FRR

Figure V. 8: Comparaison des courbes des temps d'exécution de l'évaluation.

Commentaire: l'explication de ce phénomène est simple, il n'est pas du au fait de la reconnaissance d'iris mais plutôt au fait de la génération de code correcteur d'erreur. Lorsque la clé dont on va générer le mot de code est petite, la génération du mot de code est simple à effectuer est prend donc un temps relativement faible. Puis au fur et à mesure que la taille de a clé augmente, le temps augmente également. Mais arrivé à un certain seuil il y'a de moins en moins d'information de redondance à générer ce qui explique que le temps de génération de mot de code remet à devenir petit.

Il est intéressant de constater que c'est au moment ou les courbes s'inverse, c'est-à-dire au moment où on a atteint un maximum d'information à coder pour un maximum de bit que de redondance que nous avons les meilleurs résultats.

Cela nous permet de déduire qu'une bonne clé pour notre système serait compris entre la 900bits ou 1500: une tel clé offre le meilleur compromis mais dans ce cas la vérification prend le plus de temps.

Après cela, Nous avons fixé la taille de notre clé dans le système à 1210 bits. pour obtenir de meilleur compromis.

V.3. Conclusion

Dans ce chapitre nous avons effectué des tests sur notre application affin de savoir quelles étaient les performance de notre système. Nous avons au cours de nos test varié les tailles des clé pour voir quel serait la taille de la clé permettant d'obtenir le meilleur résultat d'authentification. Grâce à ces tests nous avons pu fixer la taille de la clé à utiliser pour notre application. Nous nous sommes basé sur une taille de clé offrant les meilleur résultats mais qui hélas provoque également un plus grand temps d'exécution. Cependant pour une authentification unique la différence ne se fait pas tellement ressentir.

CONCLUSION GENERALE

Dans ce mémoire, nous avons travaillé sur la biométrie, en particulier l'authentification par l'iris. Au tout début de ce travail nous avions parlé des vulnérabilités qui affectent les systèmes biométriques. Nous avons également étudié des méthodes possibles pour la sécurisation des modèles biométriques. Nous avons brièvement parlé des solutions proposé par la littérature mais deux méthodes en cours de développement ont retenues notre attention le Fuzzy vault et le Fuzzy commitment. Nous avons détaillé les algorithmes de ces deux dernières méthode dans ce mémoire, et finalement nous avons opté pour l'utilisation du Fuzzy commitment pour le gain en terme de coût d'exécution.

L'objectif de notre mémoire était de rechercher et implémenter une solution technique, qui compléterait la technologie biométrique, afin d'effectuer une double protection: protection des données biométriques de référence et protection de clé cryptographique. Il était également question, après avoir réalisé notre application d'évaluer les performances du système.

Nous avons conçu une application d'authentification dont les données biométriques sont protégées de façon qu'il est impossible de retrouver des données biométriques originales à partir des informations stocké, et aussi dont les données biométrique permette de sécurisé l'utilisation d'une clé. Ainsi le problème d'oublie ou de perte de clé est résolu et il le problème de sécurisation de la biométrie (protection de la vie privée) est assuré.

Cependant notre approche possède encore des lacunes. Notamment en ce qui concerne le temps d'exécution. Nous avons également constater que plus la clé était petite, plus le FRR diminue, cependant le FAR augmente et inversement plus la clé est grande plus le FAR est petit mais le taux FRR augmente en conséquence.Nous avons opté pour l'utilisation de clé intermédiaire pour avoir un compromis acceptable

Au cours du développement de l'application nous avons utilisé des données des paramètres qui offraient de meilleurs résultat mais le temps de calcul devenait tellement long que cela était irraisonnable. Il serait intéressant de développer le système avec un autre mécanisme de correction des erreurs, peu être cela pourrait-il pallier à notre problème de temps. Il serait également intéressant d'améliorer l'interface utilisateur pour rajouter une vue des différents phase de traitement de l'iris pour une meilleur présentation. Il serait aussi intéressant d'essayer de développer une application qui permette de choisir différente modalité ou même plusieurs modalité en même temps. Cela serait nos perspectives d'avenir.

Références

[1]: Rima Ouidad Belguechi. Sécurité des systèmes biométriques : révocabilité et protection de la vie privée. Traitement des images. Ecole nationale Supérieure en Informatique Alger, 2015.

[2]: https://fr.wiktionary.org/wiki

[3]: http://www.futura-sciences.com/tech/definitions/tech-biometrie-2049/

[4]: Cours 6: Biométrie, Odile PAPINI, disponible sur: http://odile.papini.perso.esil.univmed.fr/sources/SSI.html

[5]: http://www.memoireonline.com/04/12/5741/m_Conception-et-realisation-dun-systeme-de-vote-electronique-pour-le-parlement-cas-du-senat-c6.html

[6]: la biométrie, sa fiabilité et ses impacts sur la pratique de la démocratie libérale, Frédéric MASSICOTTE, Novembre 2007

[7]: https://investigationderrierelescrimes.wordpress.com/2013/12/18/le-bertillonnage-technique-scientifique/

[8]: https://www.police-scientifique.com/specialites/empreintes-digitales-et-traces-papillaires/

[9]: http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/main.shtml

[10]: (en) Rabia Jafri et Hamid R. Arabnia, « A Survey of Face Recognition Techniques », Journal of Information Processing Systems, vol. 5, no 2, juin 2009

[11]: http://www.memoireonline.com/02/13/6979/m_Reconnaissance-de-visages-par-Analyse-Discriminante-LineaireLDA-2.html

[12]: UMMTO, mémoire de magister en électronique, option: télédétection;" détection et identification de personne par méthode biométrique" par Boudjellal Sofiane.

[13]: An Introduction to Biometrics Audio and Video-Based Person Authentification, Florent PERRONNIN et Jean-Luc DUGELAY, 2007

[14]: J. Egan, « Signal Detection Theory and ROC Analysis », Academic Press, New-York, 1975.

[15]: thèse de doctorat, Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris, Nicolas MORIZET, 2009.

[16]: Cours, Techniques et Usages Biométriques, Bernadette Dorizzi, 2004

[17]: J. Daugman, « High Confidence Visual Recognition of Persons by a Test of Statistical Independence », IEEE Transactions on Pattern Analysis and Machine Intelligence.

[18]: Jones, Alex, Fallujah Residents Face Choice: Retina Sean and Take ID Card.... Or Die

[19]: http://www.technovelgy.com/ctiTechnology-Article.asp?ArtNum=16

[20]: http://www.stevenspublishing.com/Stevens/SecProdPub.nsf/frame?open&redirect=http://www .stevenspublishing.com/stevens/secprodpub.nsf/d3d5b4f938b22b6e8625670c006dbc58/2a9 e1688dd432ca88625711 f0062b8c7?OpenDocument

[21]: Institut des Télécommunication d'Oran, mémoire de fin d'études pour l'obtention du diplôme d'ingénieur en télécommunications: "système de reconnaissance et d'apprentissage" par Mr. Kelbouza Abdessamed et Mr. Lakhache Ahmed, 2005
[22]: www.memoireonline.com
[23]: Markets and markets, "Biometric System Market by Authentication Type (Single-Factor: (Fingerprint, IRIS, Palm Print, Face, Vein, Signature, Voice), Multi-Factor), Component (Hardware and Software), Function (Contact and Non-contact), Application, and Region - Global Forecast to 2022", novembre 2016
[24]: http://www.biometrie-online.net/actualites/articles/313-les-applications-du-futur-de-la-biometrie
[25]: http://www.biometrie-online.net/biometrie/le-marche
[26]: http://www.algeriesite.com/fr/news-d-algerie/96563-internet.php
[27]: http://www.blogdumoderateur.com/chiffres-internet/
[28]: http://welab4u.fr/index.php/2017/01/28/en-2016-chaque-minute-sur-internet/
[29]: Université de Toulouse, Thèse de doctorat," *Protection des systèmes informatiques contre les attaques par entrées-sorties*" par Fernand Lone Sang, le 27 novembre 2012
[30]: Université de Toulouse, Thèse de doctorat," *Evaluation quantitative de la sécurité informatique : approche par les vulnérabilités*" par Géraldine Vache-Marconato, 8 décembre 2009
[31]: Jean-Claude Laprie,"*Sureté de fonctionnement des systèmes: concepts de base et terminologie*". Revue de l'Electricité et de l'Electronique (REE), Novembre 2004
[32]: Jean François Pillou, "*Tout sur les systèmes d'informations*", Paris Dunod 2006
[33]: "*Malicious and Aaccidental Fault Tolerance in Internet Applications : conceptual model and architecture*", MAFTIA Project Delivrable D21, 2003
[34]: http://www.topvirus.com/appli.php
[35]: http://www.commentcamarche.net
[36]: http://securiteinformatique.unblog.fr/2008/06/06/ii1les-bombes-logiques/
[37]: http://securiteinformatique.unblog.fr/2008/06/05/ii2les-chevaux-de-troie/
[38]: https://www.leblogduhacker.fr/fonctionnement-dun-cheval-de-troie/
[39]: http://assiste.com/Backdoor.html
[40]: http://www.anti-cybercriminalite.fr/article/quest-ce-quune-porte-dérobée
[41]: http://www.futura-sciences.com/tech/definitions/informatique-virus-informatique-2434/
[42]: https://www.securiteinfo.com/attaques/divers/vers.shtml
[43]: http://www.futura-sciences.com/tech/definitions/informatique-ver-informatique-2435/
[44]: http://www.secuser.com/dossiers/spywares_generalites.htm
[45]: http://www.vulgarisation-informatique.com/fonctionnement-antivirus.php
[46]: https://sospc.name/antivirus-fonctionnement/
[47]: https://info.sio2.be/infobase/18/2.php
[48]: https://www.kaspersky.fr/resource-center/definitions/firewall
[49]: https://www.microsoft.com/fr-fr/security/resources/antispyware-whatis.aspx

[50]: http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101000925
[51]: http://www.larousse.fr/dictionnaires/francais/cryptographie/20864
[52]: https://fr.wikipedia.org/wiki/Cryptographie
[53]: http://tpe-cryptologie-2013.e-monsite.com/pages/page-1.html
[54]: http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html
[55]: http://ram-0000.developpez.com/tutoriels/cryptographie/
[56]: http://rainet.telecom-lille.fr/unit/securite/francais/s1/p03_securite_s01.htm
[57]: P Barthélemy, R Rolland, P Véron, *Cryptographie : principes et mises en œuvre - 2e édition revue et augmentée*, édition Lavoisier, mai 2012
[58]: http://www.linternaute.com/dictionnaire/fr/definition/
[59]: Nadia El Mrabet, *Les concepts fondamentaux de la cryptographie*, Université de Caen, mars 2010
[60]: http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/sigindeniable
[61]: http://dictionnaire.sensagent.leparisien.fr/Mise%20en%20gage/fr-fr/
[62]: https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/systeme_cryptographique.html
[63]: Auguste Kerckhoffs, *La cryptographie militaire, journal des sciences militaires, vol. IX*,1983
[64]: Jing Dong et Tieniu Tan, "*Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations*" National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing,Chine
[65]: G.J. Tomko, C. Soutar, and G.J. Schmidt. *Fingerprint controlled public key cryptographicsystem*. U.S. Patent 5541994, July 30, 1996.
[66]: A. Bodo. *Method for producing a digital signature with aid of a biometric feature.* German patent DE 42 43 908 A1, June 30, 1994.
[67]: P.K. Janbandhu and M.Y. Siyal. Novel biometric digital signature for internet based applications. Information Management and Computer Security, 9(5):205C212, 2001.
[68]: F. Hao and C.W. Chan. Private key generation from on-line handwritten signatures. *Information Management and Computer Security*, 10(2):159–164, 2002.
[69]: A. Juels and M.Wattenbeg. A fuzzy commitment scheme. In 6th ACM Conference on Computer and Communications Security, pages 28–36, 1999.
[70]: A. Juels and M. Sudan. *A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory*, 2002.
[71]: F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
[72]: C.E. Shannon, *A mathematical Theory of Communication*, 1948
[73]: T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure smartcardbased fingerprint authentication. In Workshop on Biometrics Methods and Applications, New York, NY, USA, 2003. ACM Press.
[74]: U. Uludag and A.K. Jain. Fuzzy fingerprint vault. In Proc. Workshop : Biometrics : Challenges Arising from Theory to Practice, pages 13–16, 2004

[75]: Ee-Chien Chang and Qiming Li. Hiding secret points amidst chaff. In EUROCRYPT, 2006.

[76]: J.-P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In Proc. 4th International Conference on Audio- and Video-based Biometric Person Authentication, 2003.

[77]: G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through on-line biometric identification. In Proc. 1998 IEEE Symposium on Privacy and Security, pages 148-157, 1998.

[78]: "UML 2 par la pratique", Pascal Roque, Edition Eyrolles, 2006.

[79]: http://biometrics.idealtest.org

[80]: Libor Masek, Peter Kovesi. MATLAB Source Code for a Biometric Identification System Based on Iris Patterns. The School of Computer Science and Software Engineering, The University of Western Australia. 2003.