Université Dr. Yahia Farès de Médéa



Institut Des Sciences Et De La Technologie
Département Du Génie Électrique Et De l'Informatique
2ème Année Mastère Systèmes Intelligents Et Communicants

Mémoire pour obtenir le grade de Mastère

« Cryptographie Des Visages »
Le Modèle
De Protection Et D'Implémentation
D'un Système De Reconnaissance
De Visages En 2D

Encadreur : Ms. SOLTANE Mohamed.

Étudiante : TCHOKETCH KEBIR Samira.

Soutenue le 29 juin 2013

Remerciement

Je remercie mon dieu, qui m'a aidé pour réaliser ce petit travail.

Je passe mes grands remerciements à ma petite famille surtout mes parents, à tous mes professeurs, mes camarades, et à mon promoteur.

Avec toutes mes respects et mes salutations merci à tout le monde.

Samira TCHOKETCH KEBIR

Juin 2013

Note :

[ ] : référence de textes.
[- -] : référence d'images.

Le contenu de la mémoire

La mémoire se constitue de:

- Introduction Générale.

- Chapitre I : La Biométrie.
  Une présentation générale du domaine de la biométrie.

- Chapitre II : Les Systèmes Biométriques.
  L'utilisation de la biométrie dans les systèmes de reconnaissance.

- Chapitre III : La reconnaissance faciale.
  La reconnaissance faciale par un cerveau et par un système biométrique.

- Chapitre IV : Les modèles de protection des données biométriques.
  Les plans développés pour protéger l'information biométrique.

- Chapitre V : Le plan des données assistantes.
  Cas particulier de protection de l'information biométrique en détails.

- Chapitre VI : Implémentation et résultat.
  Construction d'un système de reconnaissance de visages.
  - Images visages : base ORL.
  - Transformation (Extraction des caractéristiques) : méthode ACP.
  - Modèle de protection : le plan des données assistantes.
  - Codage des clés : Chiffrement Standard Avancé, CSA.

- Conclusion Générale.

- Annexe A : Analyse en Composantes Principales, ACP.
  Méthode pour l'extraction du contenu de l'image et la reconstruction de cette dernière.

- Annexe B : Chiffrement Standard Avancé, CSA.
  Algorithme de codage symétrique.
  (En, Advanced Encryption Standard AES).

- Références et bibliographie.

Table des matières

Abréviations 10

Introduction Générale 11

Chapitre I : La Biométrie 14

I. 1. Introduction 15
I. 2. Définition de la biométrie 15
I. 3. Histoire de la biométrie 15
I. 4. Classes de la biométrie 16
I. 4.1. Biométrie douce 16
I. 4.2. Biométrie traditionnelle 17
I. 5. Types de modalités biométriques 18
I. 5.1. Modalités biométriques physiologiques 18
I. 5.1.1. Visage 18
I. 5.1.2. Iris 18
I. 5.1.3. Empreinte du doigt 19
I. 5.1.4. Rétine 20
I. 5.1.5. Géométrie de la main 20
I. 5.1.6. Système de configuration des veines 21
I. 5.2. Modalités biométriques biologiques 21
I. 5.2.1. ADN 21
I. 5.3. Modalités biométriques comportementales 21
I. 5.3.1. Frappe au clavier 21
I. 5.3.2. Reconnaissance vocale 22
I. 5.3.3. Dynamique de signature 22
I. 5.3.4. Dynamique d'écriture 22
I. 5.3.5. Tic 22
I. 5.4. Modalités biométriques vestimentaires 23
I. 6. Fonctions de la biométrie 23
I. 7. Comparaison entre les modalités biométriques 23
I. 8. Application de la biométrie 24
I. 9. Conclusion 24

Chapitre II : Systèmes Biométriques 25

II. 1. Introduction 26
II. 2. Définition d'un système biométrique 26
II. 3. Architecture d'un système biométrique 26
II. 4. Fonctionnement d'un système biométrique 27
II. 4.1. Étape d'enrôlement 27
II. 4.2. Étape d'authentification 28
II. 4.2.1. Mode vérification 28
II. 4.2.2. Mode identification 28
II. 4.2.3. Mode test 28

II. 5. Performance des systèmes biométriques 29
II. 6. Types de systèmes biométriques 30
II. 6.1. Systèmes biométriques selon le nombre des modalités biométriques 30
II. 6.1.1. Systèmes biométriques uni modaux 30
II. 6.1.2. Systèmes biométriques multimodaux 31
II. 6.2. Systèmes biométriques selon le traitement des modalités biométriques 33
II. 6.2.1. Systèmes multi-échantillons 33
II. 6.2.2. Systèmes multi-capteurs 33
II. 6.2.3. Systèmes multi-algorithmes 33
II. 6.2.4. Systèmes multi-instances 33
II. 6.3. Systèmes biométriques hybrides 34
II. 7. Systèmes biométriques adaptatifs 34
II. 8. Domaine d'application des systèmes biométriques 34
II. 9. Quelques exemples d'application des systèmes biométriques 34
II. 10. Intérêt des systèmes biométriques 35
II. 11. Quelques problèmes de la biométrie 35
II. 12. Conclusion 36

Chapitre III : Reconnaissance Faciale 37

III. 1. Introduction 38
III. 2. Concept 38
III. 3. Composantes d'un visage 38
III. 3.1. Composantes externes 38
III. 3.2. Composantes internes 38
III. 4. Codage des actions du visage 39
III. 5. Reconnaissance d'un visage 40
III. 5.1. Reconnaissance par le cerveau humain 40
III. 5.2. Reconnaissance par le système biométrique 42
III. 5.2.1. Acquisition de l'image biométrique 43
III. 5.2.2. Prétraitement de l'image acquise 43
III. 5.2.3. Détection de visages dans l'image 44
III. 5.2.4. Extraction des caractéristiques du visage 45
III. 5.2.4.1. Modèle de forme active 45
III. 5.2.4.1.1. Modèle de forme active 2D 45
III. 5.2.4.1.2. Modèle de forme active 3D 46
III. 5.2.4.2. Modèle complet 46
III. 5.2.4.2.1. Modèle complet 2D 46
III. 5.2.4.2.2. Modèle complet 3D 47
III. 5.2.5. Authentification (Classification) du visage 47
III. 6. Difficultés de la reconnaissance faciale 48
III. 7. Domaine d'application de la reconnaissance faciale 49
III. 8. Problèmes des systèmes de reconnaissance faciale 49
III. 9. Conclusion 49

Chapitre IV : Modèles de protection de l'information biométriques 50

IV. 1. Introduction 51
IV. 2. Protection de l'information biométrique 52
IV. 2.1. Approche de transformation des traits 52
IV. 2.1.1. Transformation inversible 53
IV. 2.1.2. Transformation non-inversible 53
IV. 2.2. Approche crypto-système biométrique 53
IV. 2.2.1. Crypto-système par liaison de la clé 54
IV. 2.2.2. Crypto-système par génération de la clé 54
IV. 2.3. Approche hybride transformation\crypto-système 54
IV. 3. Modèle de protection de l'information biométrique 54
IV. 3.1. Plan du Coffre Flou 54
IV. 3.1.1. Calcule de la clé du Coffre Flou 55
IV. 3.1.2. Codage du Coffre Flou 56
IV. 3.1.3. Décodage du Coffre Flou 57
IV. 3.1.4. Exemple général 58
IV. 3.2. Plan des Données Assistantes (HDS) 59
IV. 3.2.1. HDS au cours du processus d'enrôlement 60
IV. 3.2.2. HDS au cours du processus d'authentification 60
IV. 4. Conclusion 61

Chapitre V : Plan des Données Assistantes 62

V. 1. Introduction 64
V. 2. Extraction de caractéristiques 64
V. 3. Réduction de dimension 64
V. 4. Binarisation 64
V. 5. Sélection des bits fiables 65
V. 6. Génération du code aléatoire 67
V. 7. Codage correcteur d'erreurs 67
V. 7.1. Concepts 67
V. 7.2. Implémentation 67
V. 7.3. Redondance et fiabilité 68
V. 7.4. Code correcteur d'erreurs 68
V. 7.5. Quelques codes correcteurs 69
V. 7.5.1. Code de Répétition 69
V. 7.5.2. Code de Sommes De Contrôle 70
V. 7.5.3. Code de Reed Solomon 71
V. 8. Codage ou hachage de la clé aléatoire 74
V. 9. XOR 74
V. 10. Stockage 74
V. 11. Conclusion 74

Chapitre VI : Implémentation Et Résultats 75

VI. 1. Introduction 76
VI. 2. Concepts et définitions (ORL, ACP, CSA) 76
VI. 2.1. Base des visages ORL 76
VI. 2.2. Analyse En Composantes Principales ACP 76
VI. 2.3. Chiffrement Standard Avancé CSA 76
VI. 3. Description de l'étude réalisée (réalisation théorique) 77
VI. 4. Implémentation (Réalisation logicielle -Matlab-) 79
VI. 4.1. Phase d'enrôlement 79
VI. 4.1.1. Cas 1 : seul individu, plusieurs images échantillons 81
VI. 4.1.2. Cas 2 : plusieurs individus, une seule image échantillon 82
VI. 4.1.3. Cas 3 : plusieurs individus, plusieurs images échantillons 83
VI. 4.2. La phase d'authentification 84
VI. 4.3. Le bilan des expériences 89
VI. 4.3.1. Cas 1 : seul individu, plusieurs images échantillons 90
VI. 4.3.2. Cas 2 : plusieurs individus, une seule image échantillon 97
VI. 4.3.3. Cas 3 : plusieurs individus, plusieurs images échantillons 101
VI. 5. Avantages et inconvénients du système reconstruit 105
VI. 6. Conclusion 103

Conclusion Générale 107

Annexe A : Analyse en composantes principales (ACP) 111
(En, Principal Components Analysis PCA)

Annexe B : Chiffrement Standard Avancé (CSA) 117
(En, Advanced Encryption Standard AES)

Références et Bibliographie 123

Liste des Figures

Figure 01 : Iris 18
Figure 02 : Différentes Images d'Iris 19
Figure 03 : Empreinte de la main 19
Figure 04 : Minuties de l'empreinte, Empreinte 19
Figure 05 : Doigt, Empreinte du doigt 20
Figure 06 : Rétine 20
Figure 07 : Géométrie de la main 20
Figure 08 : ADN, Molécule d'ADN 21
Figure 09 : Frappe au clavier 21
Figure 10 : Signal de la parole 22
Figure 11 : Dynamique d'écriture 22
Figure 12 : Composantes d'un système biométrique 27
Figure 13 : Plan du processus général d'authentification biométrique 29
Figure 14 : Quelques systèmes biométriques 35
Figure 15 : Régions de reconnaissance des visages chez les humains 41
Figure 16 : Détection de visage 44
Figure 17 : Modèle de forme active en 2D 45
Figure 18 : Modèle de forme active en 3D 46
Figure 19 : Modèle complet en 2D 46
Figure 20 : Modèle complet en 3D 47
Figure 21 : Autre modèles complets en 3D 47
Figure 22 : Approches de protection de la base des données biométrique 51
Figure 23 : Catégories des modèles de protection 52
Figure 24 : Coffre floue 55
Figure 25 : Plan des Données Assistantes 59
Figure 26 : Modèle de protection « le plan des données assistantes » 63
Figure 27 : Redondance et fiabilité 68
Figure 28 : Code correcteur d'erreurs 28
Figure 29 : Système de reconnaissance de visages (HDS, AES, ORL) 77
Figure 30 : Exemple de paramètres du test (Cas1) 81
Figure 31 : Exemple de visages d'apprentissage (Cas1) 81
Figure 32 : Exemple de paramètres du test (Cas2) 82
Figure 33 : Exemple de visages d'apprentissage (Cas2) 82
Figure 34 : Exemple de paramètres du test (Cas3) 83
Figure 35 : Exemple de visages d'apprentissage (Cas3) 83
Figure 36 : Exemple de test de reconnaissance 1 (Cas3) 87
Figure 37 : Exemple de test de reconnaissance 2 (Cas3) 87
Figure 38 : Exemple de test de reconnaissance 3 (Cas3) 88
Figure 39 : Exemple de test de reconnaissance 4 (Cas3) 88
Figure 40 : Courbes FRR, FAR, et ROC (Cas 1) 96
Figure 41 : Distribution des résultats FRR et FAR (Cas 1) 96
Figure 42 : Courbes FRR, FAR, et ROC (Cas 2) 99
Figure 43 : Distribution des résultats FRR et FAR (Cas 2) 100
Figure 44 : Courbes FRR, FAR, et ROC (Cas 3) 104
Figure 45 : Distribution des résultats FRR et FAR (Cas 3) 104
Figure 46 : Exemple, (1) Visages d'apprentissage, (2) Visages propres 116

Abréviations

CLUSIF : Club de la Sécurité de l'Information Français.
CNIL : Commission Nationale de l'Informatique et des Libertés.
NIST: The National Institute of Standards and Technologies.

PIN : Personal Identification Number.

FAR : False Acceptation Rate.
FRR : False Rejection Rate.
EER : Equal Error Rate.
FER : Failure To Enroll Rate.
FCR : Failure To Capture Rate.

CIN : Carte d'Identité Nationale.
INES : Identité Nationale Électronique Sécurisée.

CRC : Cyclic Redundancy Check.

ECC : Error Correction Code.
CCE : Code Correcteur d'Erreurs.

ARQ : Automatic Repeat Request.
RAR : Requête Automatique de répétition.

PCA : Principal Components Analysis.
ACP : Analyse en Composantes principales.

ICA : Indépendant Components Analysis.
ACI : Analyse en Composantes Indépendantes

LDA : Linear Discriminant Analysis.
ALD : Analyse Linéaire Discriminante.

AES : Advanced Encryption Standard.
CSA : Chiffrement Standard Avancé.
(Le Standard du Chiffrement Avancé).

HDS : Helper Data Scheme.
PDA : Plan des données assistantes.

ORL : Olivetti Research Laboratory.

Introduction Générale

Introduction Générale

L'évolution de la technologie a causé plusieurs problèmes de l'insécurité surtout dans les grandes organisations comme : les entreprises, les usines (médicales,…), les régions industrielles (nucléaires, pétrolières,…) et militaires, où le contrôle d'accès et la gestion de flux de personnes est obligatoire, parce que l'accès non autorisé d'un intrus peut causer dans un jour des dégâts irréformables. Donc, la prudence en avance et la prise de précautions préventives sont indispensables.

Parmi les moyens d'authentification souvent utilisés : le contrôle des individus par les documents personnels comme : la carte d'identité, le passeport, le permet de conduire, …, ou par les codes personnels comme : code PIN, mot de passe, matricule,…, ou bien par les deux : un document et un code personnel. Mais toutes ces méthodes sécuritaires peuvent être perdues ou falsifiées. Par conséquence, leur fiabilité est moyenne, et dans quelques cas nulle.

Après plusieurs années de recherche et d'expérience, les développeurs ont trouvé un autre modèle de sécurisation, plutôt un modèle d'authentification qui se base sur la reconnaissance des modalités biométriques propres à l'individu qui sont invariables dans le temps comme : le visage, l'empreinte (doigt, paume de la main,…), l'iris, la rétine,… d'une manière plus efficace. Le principe d'utilisation de ces modalités biométriques est la numérisation de leurs images (conversion en digital) par des lois spécifiques, et le stockage de ces données numériques avec l'identité de la personne dans des supports de stockage afin de les comparer au future avec autres données de test si elles sont identiques ou non. Après d'autres études, ils ont trouvé aussi d'autres caractéristiques aidant à la reconnaissance de personnes qui ne sont pas uniques et peuvent être variables comme : la couleur des yeux et des cheveux, la taille, le poids, etc.

La découverte de la biométrie a changé le monde de la sûreté à partir d'un état traditionnel moins fiable vers un état plus moderne et efficace surtout après l'apparition des systèmes biométriques qui fonctionnent en deux étapes : enrôlement (sauvegarde) et authentification (test de reconnaissance). Cependant, la transaction avec des données biométriques secrètes rencontre des risques majeurs comme : perte, modification, violation, et falsification. Par conséquence, le système ne sera plus fiable pour authentifier des personnes correctement. Donc, une décision a été prise qui est la protection de l'information biométrique.

Parmi les modèles de protection des informations biométriques ce de *Juels* et *Wattenberg* « l'Engagement Flou » (En, Fuzzy commitement) en 1999, et aussi « le Coffre Flou » (En, Fuzzy vault) par *Juels* et *Sudan* en 2002, et le dernier modèle « le Plan Des Données Assistantes ». En réalité, ces modèles de protection permettent de transformer l'information biométrique par des fonctions inversibles (Possibilité de recalculer l'information biométrique originale après la transformation) ou non inversibles et permettent aussi de la coder à l'aide d'une clé aléatoire générée aléatoirement ou extraite à partir des informations biométriques. Dans tous les cas, l'information se sera stockée sous une forme cryptée et impossible d'extraire la clé originale dans l'absence des données

biométriques requêtes originales, et la sécurité du système dépend aussi de la robustesse de la fonction de codage de la clé (code) aléatoire.

La reconnaissance faciale est le domaine biométrique le plus utilisé surtout pour le contrôle d'accès et la gestion des données multimédias et numériques. Les premières recherches en reconnaissance automatique de visage sont commencées dans les années 1960. Et malgré que des modifications et des développements importants soient réalisés, il reste toujours des questions supplémentaires dans ce domaine qui demandent des réponses et des justifications précises et exactes.

L'étude réalisée dans cette mémoire se constitue d'un système de reconnaissance de visage. Lors de la phase d'enrôlement, les données biométriques (Les traits des visages) sont extraites par l'Algorithme de l'Analyse En Composantes Principales (ACP) en utilisant les variables : vecteurs et valeurs propres. Les données obtenues sont protégées par le plan des données assistantes PDA (En, Helper Data Sheme) par la liaison (XOR) avec une clé générée aléatoirement, et elles sont encore enregistrées dans la base de données du système biométrique comme des données d'aide. La clé aléatoire générée pour chaque image visage est codée par le Chiffrement Standard Avancé CSA (En, Advanced Encryption Standard AES), et chaque clé codée doit être stockée dans la base de données du système biométrique. Les mêmes étapes seront réalisées lors de la phase d'authentification sauf qu'il y a une récupération des informations à partir de la base du système au lieu d'enregistrement. La dernière étape est réalisée à l'aide d'un classifieur (Un comparateur) qui compare la clé aléatoire recalculée et codée par le chiffrement standard avancé lors de la phase d'authentification avec la clé aléatoire codée correspondante dans la base de données du système biométrique, le classifieur calcule le degré de similitude (les scores) entre ces deux clés et fourni le résultat d'authentification. Les résultats obtenus après plusieurs expériences sont déjà mentionnés dans le chapitre « Implémentation et résultats ».

Chapitre I :

Biométrie

I. 1. Introduction

L'accès aux organisations sécurisées est contrôlé par deux moyens distincts : la méthode « token-based » par exemple : passeport,… et la méthode « knowledge-based » tels que : code PIN, mot de passe,… . Toutes ces moyennes d'identification peuvent être perdues, oubliées, volées, divulguées ou falsifiées, donc l'accès non autorisé reste comme un problème pour les personnes et les systèmes contrôleurs.

Cependant, une nouvelle technologie appelée « la biométrie » a été apparu, elle repose sur l'identification des composantes biologiques (ADN,…), physiologiques (empreinte digitale,…) ou comportementales (La démarche,…) car elles sont propres à l'individu, ce qui offre beaucoup plus de sécurité, intimité et confiance.

I. 2. Définition de la biométrie

Le sens premier du mot « biométrie » étant repris par le terme « Biostatistique » (l'application de la science statistique à la biologie) qui signifie « mesure + vivant » ou « mesure du vivant », et désigne dans un sens très large l'étude quantitative des êtres vivants, [1.1].

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques, ou biologiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour un seul individu. [2].

Les caractéristiques biométriques peuvent être « passives » (restent les mêmes durant toute la vie de la personne) comme : l'empreinte digitale, rétine, … ou « actives » (en changement continue) comme : visage, signature, …, [3].

I. 3. Histoire de la biométrie

À partir des premiers siècles, les êtres humains avaient conscience des formes particulières de l'empreinte digitale, de la main, du visage, et des pieds. Ils ont utilisé (Surtout les chinois et les Japonais) ces traces physiques comme un style de communication et spécialement de signature, sans connaître leurs caractéristiques propres, [4].

Le 17^{ième} siècle, est le temps d'apparition de la première étude scientifique de l'empreinte digitale, exactement en 1684 par le scientifique Anglais *Nehemiah Grew*. Ces études ont été terminées en 1892 après la découverte que l'empreinte digitale puisse identifier les individus, à la suite de la première identification d'une criminelle par ses empreintes digitales, [4].

En 1775, le pasteur suisse *Jean-Gaspard Lavater* essaye d'identifier les personnes à partir de leurs visages. Quelques années plus tard, le médecin allemand, *François-Joseph Gall* propose d'étudier la forme du crâne aussi, [4].

Dès 1883, le criminologiste Français *Alphonse Bertillon* utilise des outils anthropométriques pour effectuer 11 mesures anatomiques par individu. Autrement, ces mesures représentent les caractéristiques principales d'un visage permettant d'identifier une personne entre le public telles que : le front, le nez, l'oreille droite, la couleur des cheveux et celle de l'iris. Dès le succès immédiat de cette méthode, l'anthropométrie judiciaire devient « le bertillonnage », [4].

Et ainsi de suite, les recherches ont continue pour intégrer la biométrie avec les documents d'identité officiels. Et voici quelques dates importantes, [4]:

- Pendant la Révolution Française, les citoyens doivent présenter aux autorités de la police un document appelé « carte de sûreté », [4].

- Sous la III° République, le problème de distinction entre les français et les étrangers (Problème de nationalité) est posé? La solution est le port d'un « carnet anthropométrique », contenant deux photos et les empreintes digitales des 2 mains, [4].

- Dans les années 1980, le projet d'informatiser la carte d'identité est commencé. La première carte informatisée est délivrée en 1990, [4].

- En 1995, le ministre de l'Intérieur *Charles Pasqua*, introduit la carte sécurisée et informatisée, [4].

- En 2007, une nouvelle carte d'identité est délivrée en France : la « carte INES » (Identité nationale électronique sécurisée). Carte à puce contenant les données biométriques du visage et de l'empreinte digitale, [4].

- En 2010 une « carte nationale » d'identification est proposée : carte à puce contenant les données biométriques (empreinte digitale, visage et/ou iris), [4].

- Projet future, l'intégration des informations génétiques dans la carte d'identité, [4].

I. 4. Classes de la biométrie

Dans le domaine de la biométrie, on peut distinguer deux classes biométriques essentielles, qu'elles sont :

- La biométrie douce.
- La biométrie traditionnelle.

I. 4.1. Biométrie douce

Le terme « biométrie douce » désigne les signes que les humains utilisent pour se reconnaître entre eux et différencier les uns des autres, mais qui ne sont pas uniques et ne peuvent pas permettre une identification exacte, [1.1].

Exemples des biométries douces :

- **Physiques :**
  - Couleur de la peau, des yeux, des cheveux.
  - Présence d'une barbe, des moustaches, ou des cheveux.
  - Taille et poids.
  - Forme du visage et du corps.
  - Les marques physiques : tâches, cicatrices,…
  - …

- **Comportementales :**
  - Démarche.
  - Frappe au clavier.
  - Tic.
  -…

- **Éléments attachés aux personnes :**
  - Couleur des vêtements.
  - Tatouage.
  - Maquillage.
  - Accessoires (bijoux, …)
  - …

- **Vestimentaires :**
  - Port de lunettes, d'un chapeau,…
  - …

, [1.2].

Malgré que les biométries douces soient insuffisantes pour identifier les personnes, mais elles partagent de nombreux avantages avec les biométries classiques, et elles ont de plus des avantages spécifiques : ces biométries ne sont pas intrusives, sont faciles à calculer, compréhensibles et acceptables par les humains, [1.2].

Dans la pratique, […] le problème se complexifie dans la mesure où il faut disposer d'algorithmes très élaborés qui peuvent décrypter rapidement le film du mouvement et le comparer à celui stocké dans la base. La solution ? " […] Un deuxième concept sur lequel nous travaillons : la biométrie douce […], on note des caractéristiques physiques comme la couleur des yeux, les lunettes, la barbe... Ce qui permet de classer les individus dans des catégories […], [5]. Ainsi, si la personne recherchée et appartient à une catégorie soft bien déterminée, inutile de perdre du temps en analysant l'ensemble de tous les fichiers stockés, [5].

I. 4.2. Biométrie traditionnelle

Le terme de la biométrie traditionnelle désigne les traits comme : le visage, l'empreinte digitale, le réseau veineux, l'iris, la rétine, …

I. 5. Types de modalités biométriques

Les modalités biométriques peuvent être classées en quatre catégories principales :

- Modalités biométriques physiologiques.
- Modalités biométriques biologiques.
- Modalités biométriques comportementales.
- Modalités biométriques vestimentaires.

I. 5.1. Modalités biométriques physiologiques

La biométrie physiologique regroupe les éléments suivants : le visage, L'iris, l'empreinte, la rétine, le réseau veineux,…

I. 5.1.1. Visage

Le visage de l'être humain est la partie frontale de la tête. Il représente l'interface principale d'identification des personnes. Il se compose de plusieurs organes pour chaque individu qu'ils sont : les yeux, le nez, la bouche, les oreilles, les sourcils, les cheveux, les joues…

Généralement les points essentiels dans un visage permettant de le représenter d'une manière entière sont les sommets des coins du : nez, bouche, yeux, oreilles, les sourcils,… et les points primordiales formant le tour du visage comme : le dessus du front, les côtes des joues, …

I. 5.1.2. Iris

[…] L'iris est une membrane circulaire et contractile de la face antérieure du globe oculaire. Il constitue la partie colorée visible de l'œil […], [6]. Il a la caractéristique de l'unicité : toujours différent même entre jumeaux, entre l'œil gauche et droit, ..., indépendant du code génétique de l'individu, et très difficile à falsifier, [2].

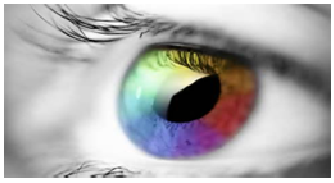


Figure 1 : Iris, [-1-].

En effet, l'iris présente une quasi-infinité de points caractéristiques (que certains comparent en nombre à ceux de l'ADN), qui ne varient pratiquement pas pendant la vie de la personne contrairement à la couleur de l'iris qui peut être changée. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc, [2].

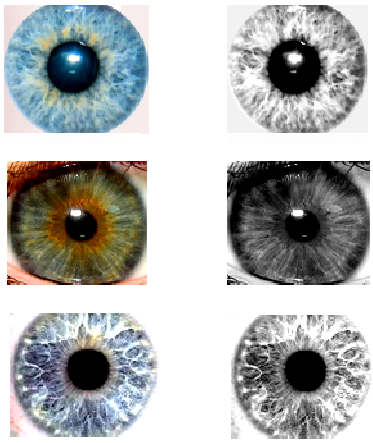

[-2.1-]
[-2.2-]
[-2.3-]

Figure 2 : Différentes images d'iris, [-2-].

I. 5.1.3. Empreinte du doigt

L'empreinte est le dessin représenté par les crêtes et les sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu, [2]. Il existe deux types d'empreintes : l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (sueur ou autre résidu déposé sur un objet), [1.1].



Figure 3 : Empreinte de la main, [-3-].

L'empreinte digitale est l'information numérique fournie par le dessin de l'empreinte. Il est presque impossible d'utiliser toutes les informations de ce dessin (car elles sont trop nombreuses pour chaque individu), on préférera donc d'extraire les points caractéristiques (les "minuties") principales telles que les bifurcations de crêtes, les îles, etc. [2].

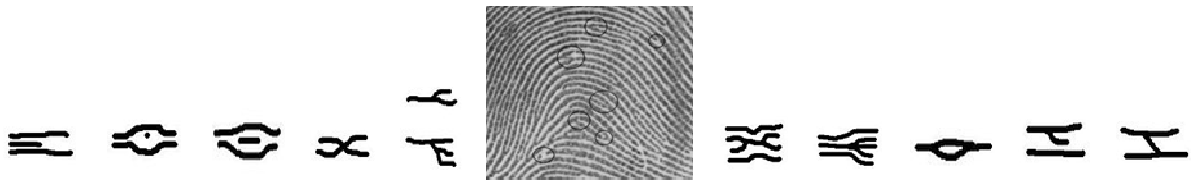


Figure 4 : Minuties de l'empreinte [-4.1-], Empreinte [-4.2-], [-4-].

Pour un doigt, une empreinte complète contient en moyenne une centaine de ces points caractéristiques. On peut extraire environ 40 de ces points (12 jusqu'à 8 au minimum), il est statistiquement impossible de trouver deux individus ont les mêmes 12 points caractéristiques, [2].




Figure 5 : Doigt [-5.1-], Empreinte du doigt [-5.2-], [-5-].

I. 5.1.4. Rétine

Le dessin (schéma) formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'œil) est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut ainsi fournir jusqu'à 400 points caractéristiques par sujet, [2].

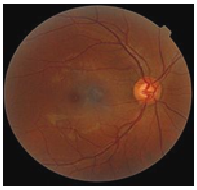
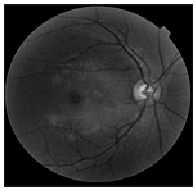



Figure 6 : Rétine, [-6-].

La mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), qui effectue ensuite un balayage de la rétine, [2].

I. 5.1.5. Géométrie de la main

La géométrie de la main consiste à mesurer plusieurs caractéristiques de la main telle que la forme de la main, la longueur et la largeur des doigts, la forme des articulations, les longueurs inter-articulations, etc. La technologie associée à cela est principalement l'imagerie infrarouge, [2].

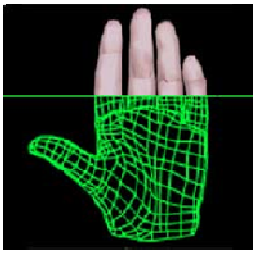


Figure 7 : Géométrie de la main, [-7-].

I. 5.1.6. Système de configuration des veines

Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main, …) pour garder quelques points caractéristiques. Cette technique est habituellement combinée à une autre (la géométrie de la main, …), [2].

I. 5.2. Modalités biométriques biologiques

La biométrie biologique essentielle est l'ADN.

I. 5.2.1. ADN : acide désoxyribonucléique

[…] Principal constituant des chromosomes, qui sert de support à l'information génétique et à sa transmission héréditaire […], [6].





Figure 8 : ADN, [-8.1-], Molécule d'ADN [-8.2-], [-8-].

I. 5.3. Modalités biométriques comportementales

La biométrie comportementale regroupe les éléments suivants : le frappe au clavier, le rythme de marche, la reconnaissance vocale, la dynamique de signature, la dynamique d'écriture, le tic, le mouvement des yeux, la façon de sourire et rire,…

I. 5.3.1. Frappe au clavier

Les facteurs comportementaux sont : les durées entre frappes, la fréquence des erreurs, durée de la frappe elle-même... . Les frappes au clavier sont influencées par plusieurs facteurs : le texte que l'on tape, sa nature et la façon de taper au clavier, [2].

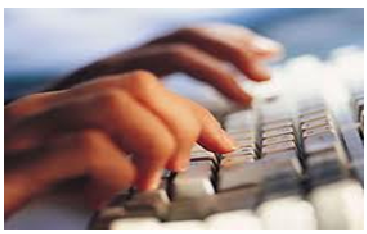


Figure 9 : Frappe au clavier, [-9-].

I. 5.3.2. Reconnaissance vocale

[…] Technologie informatique permettant à un système de reconnaître les paroles prononcées par l'utilisateur […], [6] et identifier ce dernier à partir de son voix en basant sur les caractéristiques du signal (fréquence, …) trouvées par le traitement numérique du signal.

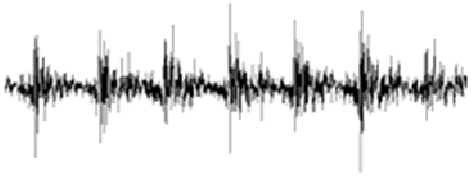


Figure 10 : Signal de la parole.

I. 5.3.3. Dynamique de signature

Ce type de biométrie est utilisé pour des applications spécifiques (documents électroniques, rapports, contrats...). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo. Ce dispositif mesure plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression, les accélérations, et le temps total, etc. [2].

I. 5.3.4. Dynamique d'écriture



Figure 11 : Dynamique d'écriture.

I. 5.3.5. Tic

[…] Le tic est la répétition habituelle et inconsciente d'un geste, d'une attitude, d'une parole ou d'une tournure […], [6].

I. 5.4. Modalités biométriques vestimentaires

Parmi les biométries vestimentaires essentielles, on mentionne : port de lunettes, port d'un chapeau, …

I. 6. Fonctions de la biométrie

Pour qu'un trait soit utilisé comme modalité biométrique, il faut qu'il vérifie les conditions suivantes :

- **Universalité :** chaque personne utilisant le système biométrique doit posséder le trait, [1.3], [2].
- **Unicité :** le trait doit être différent d'une personne à l'autre. , [1.4].
- **Mesurabilité :** le trait doit être mesurable, et facile ou possible à acquérir, [1.3].
- **Permanence :** bon permanence du trait signifie qu'il est invariant durant le temps, [1.3], [2].
- **Acceptabilité :** combien les individus accepte la biométrie d'un trait, [1.3].
- **Performance** (Efficacité) : Justesse, rapidité, et robustesse de la technologie utilisant le trait, [1.3], [2].
- **Fiabilité** (Confiance) : difficulté d'imiter le trait par la modification ou le remplacement, [1.3], [2].
- **Coût** (de la technologie) : lecteurs, capteurs, temps de calcul, etc. [2].

Il y a une autre propriété, mais elle n'est obligatoire pour qu'une modalité soit sélectionnée comme biométrique :

- **Intrusivité** : est l'existence d'un contact direct entre le capteur utilisé (Détecteur) et l'individu à reconnaître.
  - La reconnaissance faciale est une modalité « non intrusive ».
  - L'empreinte digitale est une modalité « intrusive », [7].

I. 7. Comparaison entre les modalités biométriques

Dans le tableau suivant, on compare les différentes modalités biométriques à l'aide des fonctions de la biométrie :

	Universalité	Permanence	Performance	Coût	Unicité
Visage	↑	↔	↓	↔	↓
Iris	↑	↑	↑	↑	↑
Rétine	↑	↔	↑	↑	↑
Oreille	/	/	/	/	/
Géométrie de la main	↔	↔	↔	↔	↔
Empreinte digitale	↔	↑	↑	↔	↑
Voix	↔	↓	↓	↓	↓
Signature	↓	↓	↓	↓	↓
Réseau veineux	/	/	/	/	/
Face thermo gramme	↑	↓	↔	/	↑

	Collectabilité	Acceptabilité	Intrusivité
Visage	↑	↑	×
Iris	↔	↓	√
Rétine	↓	↓	√
Oreille	/	/	/
Géométrie de la main	↑	↔	√
Empreinte digitale	↔	↔	√
Voix	↔	↑	×
Signature	↑	↑	√
Réseau veineux	↓	↓	√
Face thermo gramme	↑	↑	×

, [2][8][9].

Signification des signes utilisés dans le tableau au dessus :

↑ : Élevé × : Non
↔ : Moyenne √ : Oui
↓ : Réduit

I. 8. Application de la biométrie

Le rôle principal de la biométrie est l'authentification des personnes d'une manière sûre et évidente, sans aucune confusion entre les personnes.

I. 9. Conclusion

La diversité de l'information biométrique : visage, empreinte, iris, rétine, … et ses propriétés spécifiques comme : l'unicité, l'universalité, la permanence, … offrent un niveau de sécurité plus élevé. Donc, la biométrie est un moyen robuste d'authentification et représente un grand défi contre la fraude.

Chapitre II :

Systèmes Biométriques

II. 1. Introduction

Pour acquérir l'image biométrique exacte de n'importe quelle caractéristique ou trait d'une personne, on a besoin d'un appareil spécialisé pour garder le dessin (le schéma) de ce trait, même si l'obtention de l'image est possible manuellement (Ex : empreinte digitale), les points caractéristiques de l'image biométriques sont multiples, les calculs sont complexes, et le risque d'erreurs augmente durant l'identification de la personne. Cette ancienne méthode est couteuse en termes de temps, efforts et complexité pour une seule personne, donc elle est évidemment incompatible dans le cas d'authentification d'une population de centaines ou milliers de personnes.

La rapidité pour obtenir l'information originale des traits, de calcul, de décision, etc. et l'exactitude des résultats ont imposé les chercheurs à développer des systèmes contenants des composantes intégrales et complètes, ces systèmes sont appelées « Les systèmes biométriques ».

II. 2. Définition d'un système biométrique

« Un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance des caractéristiques propres à l'individu » (d'après le CLUSIF), [1.3].

II. 3. Architecture d'un système biométrique

Un système biométrique typique peut être représenté par six modules principaux :

- **Le module de capture (détecteur de forme) :** est le responsable d'acquisition des données biométriques d'un individu. Par exemple, cela peut être un appareil photo, un lecteur d'empreintes digitales, ou une caméra de surveillance, etc. Le module de capture peut fonctionner en mode « référence » ou en mode « authentification », [10][8].

- **Le module de prétraitement :** pour enlever le bruit et les erreurs de capture, on améliore quelques défauts par la normalisation de l'image d'entrée en utilisant, [1.3][8] :
  - Normalisation de la taille de l'image.
  - Égalisation de l'histogramme.
  - Normalisation d'illumination.
  - Filtration du médian.
  - Filtration passe-haut.
  - Translation et rotation.
  - Normalisation des arrières plans.

  , [11].

- **Le 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 représentation numérique compacte des données du trait. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe, [13][8]**.**

- **Le module de stockage :** pour conserver les informations des modalités biométriques des utilisateurs autorisés sous forme d'une base de données comme des informations de référence, [8].

- **Le module de correspondance (classification) :** utilise un classifieur qui compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude « les scores » (ou de divergence) entre les deux, [10][8].

- **Le module de décision :** vérifie l'identité affirmée par un utilisateur (vérification) ou détermine l'identité d'une personne (identification), en basant sur le degré de similitude « Les scores » entre les caractéristiques extraites et le(s) modèle(s) stocké(s), [10][8].

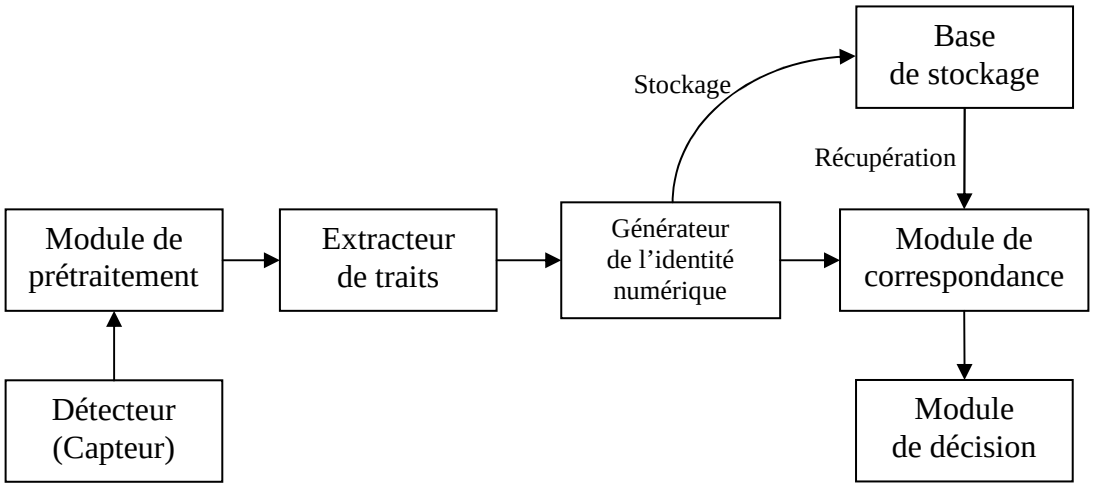


Figure 12: Composantes d'un système biométrique, [-12-].

II. 4. Fonctionnement d'un système biométrique

Le système biométrique fonctionne en deux étapes essentielles :

- Étape d'enrôlement
- Étape d'authentification
  - Vérification
  - Identification
  - Test

II. 4.1. Étape d'enrôlement

L'enrôlement est l'enregistrement de l'identité d'utilisateur avec ces informations biométriques après l'extraction dans la base de donnés du système biométrique comme référence, Ces informations sont appelées « informations de référence » [8].

II. 4.2. Étape d'authentification

L'authentification est l'extraction des informations biométriques d'un utilisateur, qui sont appelées « informations d'authentification ». Le module d'attachement compare « les informations de référence » stockées dans la base de données du système biométrique avec celles d'authentification et calcule le degré de similarité « les scores ». La décision se base sur la valeur du score qui est calculée à partir l'un des trois modes suivants, [8] :

II. 4.2.1. Mode vérification

Est-ce que l'utilisateur actuel est le même enregistré ?

C'est une comparaison 'un' à 'un', le système vérifie « les informations d'authentification » avec « les informations de référence » de l'utilisateur actuel à l'aide d'un nom d'utilisateur, une carte à puce, [7], un matricule ou un mot de passe. Si les informations comparées sont identiques (ou presque identiques) la demande sera acceptée sinon la demande sera rejetée.

II. 4.2.2. Mode identification

Qui est l'utilisateur actuel ?

C'est une comparaison 'un' à 'N', le système considère que l'utilisateur actuel est enregistré dans sa base de données biométriques et vérifie ses « informations d'authentification » avec « les informations de référence » de tous les utilisateurs, [7]. S'il ya des informations correspondantes au utilisateur actuel, le système lui donnera l'identification correspondante sinon la demande sera rejetée.

II. 4.2.3. Mode test

Est-ce que l'utilisateur actuel est une personne autorisée (enregistrée ou non) ?

L'utilisateur actuel, ses informations de référence peuvent être enregistrées dans la base de données et peuvent être non. Cette méthode est semblable à la méthode d'identification sauf que la sortie soit acceptation ou refus, [12].

Ainsi, on peut distinguer deux types de mode test :

- Test positif : permet de prouver l'existence des « informations de référence » de l'utilisateur actuel dans la base de données du système biométrique.

- Test négatif : permet de prouver l'inexistence des « informations de référence » de l'utilisateur actuel dans la base de données du système biométrique.

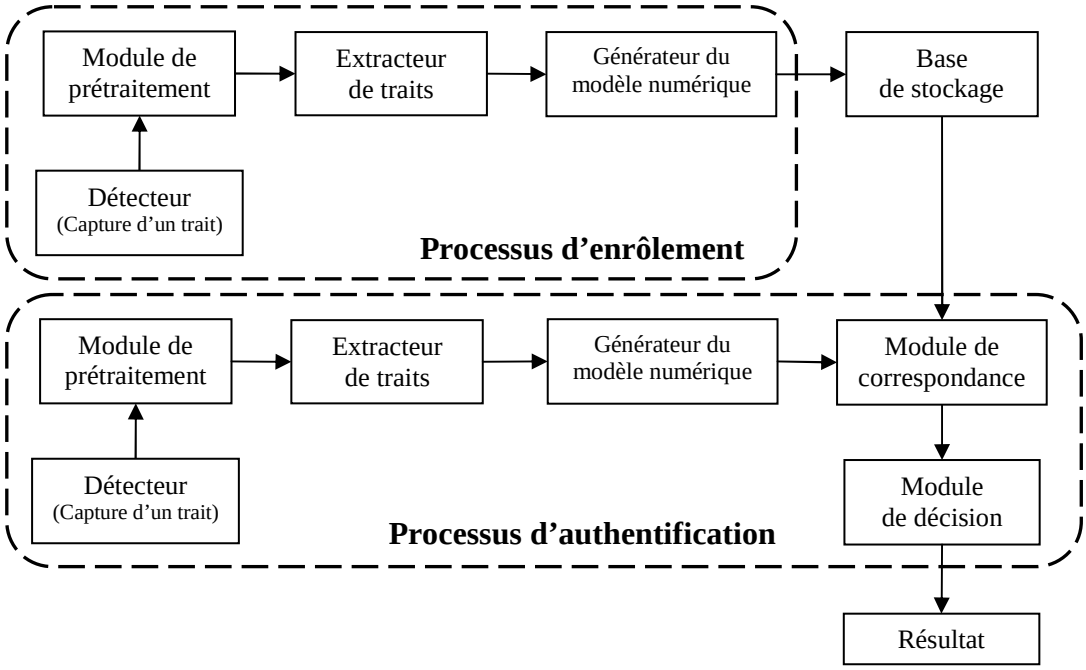


Figure 13 : Plan du processus général d'authentification biométrique, [-13-].

II. 5. Performance des systèmes biométriques

La performance d'un système biométrique est mesurée à l'aide des taux suivants :

- **Le taux de faux rejets (False Rejection Rate, FRR) :**
  Faux rejet : est le fait de rejeter une personne autorisée en temps réel,
  Car la mesure biométrique présente trop d'écart par rapport à la mesure de référence pour cette même personne.
  Un système fonctionnel aura un FRR le plus bas possible, [2][1.3].

$$\boldsymbol{FRR = \frac{Nombre\ de\ faux\ rejets}{Nombre\ total\ d'acces\ client}}$$

Équation FRR, [13].

- **Le taux de fausses acceptations (False Acceptation Rate, FAR) :**
  Fausse acceptation : est le fait d'accepter une personne non-autorisée.
  C'est le cas de falsification des données par un intrus, ou une confusion avec autres données par le système.
  Un système sûr aura un FAR le plus bas possible, [2][1.3].

$$\boldsymbol{FAR = \frac{Nombre\ de\ fausses\ acceptations}{Nombre\ total\ d'acces\ imposteurs}}$$

Équation FAR, [13].

- **Le taux d'égalité d'erreur (Equal Error Rate, EER) :**
  Ce taux est calculé à partir des deux premiers critères. Ce point correspond à FRR = FAR, [10][1.3]. C'est le point de la jonction des courbes, [2].

- **Le taux d'échec d'enrôlement (Failure To Enroll Rate, FER) :**
  Le taux des cas où il est impossible d'extraire les informations biométriques (image flou), [1.3].

- **Le taux d'échec de capture (Failure To Capture Rate, FCR) :**
  Le taux des cas ou il n'est pas possible de détecter une image biométrique d'entrée (absence de l'image), [1.3].

- **Capacité du système (System capacity) :**
  Le nombre maximal des utilisateurs stockés dans la base du système biométrique, [1.3].

II. 6. Types de systèmes biométriques

Les systèmes biométriques peuvent être classés selon deux facteurs : le nombre de modalités biométriques acquises, et les traitements appliqués pour étudier ces modalités.

II. 6.1. Systèmes biométriques selon le nombre des modalités biométriques

Les systèmes biométriques dans ce cas peuvent être uni-modaux ou multimodaux.

II. 6.1.1. Systèmes biométriques uni modaux

Le Système biométrique uni modal utilise un seul trait physiologique ou comportemental pour authentifier les personnes.

Une seule modalité ne permet pas d'effectuer la reconnaissance d'une manière fiable à cause de plusieurs facteurs qu'ils sont :

- **Bruit introduit par le capteur**, [10][8]**:** le bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. Par exemple, la poussière ou les taches des mains sur un lecteur d'empreintes, une mauvaise illumination, etc, [10].

Le module de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique, et des données bruitées peuvent influencer négativement sur la précision du système, [10].

- **Non-universalité**, [10][8]**:** Le principe d'universalité est nécessaires pour les modalités biométriques face à un système de reconnaissance biométrique. Cependant, toutes les modalités biométriques ne sont pas vraiment universelles. Par exemple : les gens qui ont des handicaps liés à la main, cicatrices, etc. ne peuvent pas fournir une empreinte digitale complète ou nette, [10].

La non-universalité entraîne des erreurs d'enrôlement ("Failure To Enroll", FTE) et/ou des erreurs de capture ("Failure To Capture", FTC) dans un système biométrique, [10].

- **Manque d'individualité :** les caractéristiques extraites à partir des données biométriques de différents individus peuvent être relativement similaires. Par exemple, certaines personnes peuvent avoir des images faciales identiques à cause des facteurs génétiques (père et fils, vrais jumeaux, deux personnes semblables, etc.), [10].

Ce manque d'unicité augmente le taux de fausse acceptation ("False Accept Rate", FAR) d'un système biométrique, [10].

- **Représentation variante :** C'est le cas ou « les informations d'authentification » ne sont pas identiques à celles « de référence », Ceci est connu sous le nom de "variations intra-classe" qui peuvent être dues par :

- Une mauvaise interaction de l'utilisateur avec le capteur (ex : changement de pose).
- Remplacement des capteurs par d'autres (ex : Qualité de capture)
- Changements de conditions de l'environnement (ex : changements en éclairement).
- Changements de trait (ex : Apparition de cicatrices).

, [10][8].

Grandes variations intra-classe augmentent généralement le taux de faux rejet ("False Reject Rate", FRR) d'un système biométrique. [10].

- **Sensibilité aux attaques**, [10][8]**:** bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est possible de tromper un système biométrique en utilisant des modalités biométriques falsifiées (Exemple : empreinte digitale) , [10] ou semblables (Exemple : visage).

Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaques que les modalités biométriques physiologiques, [10].

Les taux d'erreurs associés à des systèmes biométriques uni modaux sont élevés. Pour éviter ou pallier ces inconvénients, on utilise plusieurs modalités biométriques au niveau d'un même système biométrique, on parle alors d'un « système biométrique multimodal », [10].

II. 6.1.2. Systèmes biométriques multimodaux (multi-biométriques)

Les systèmes multimodaux intègrent des systèmes uni modaux séquentiellement (en série) ou parallèlement (simultanément) [1.3] ce qui permet de combiner les preuves présentées par différentes modalités biométriques pour authentifier un individu (Exemple : un système biométrique multimodal utilise les caractéristiques du visage et de la voix), [10]. La construction d'un système multi-biométrique est afin de réduire le taux de faux rejet FRR et le taux de fausses acceptations FAR causées par la non-universalité ou la falsification d'un trait, [8], Ou bien par le bruit produit par le capteur ou l'individu lui-même.

La précision de reconnaissance dans les systèmes biométriques multimodaux peut être améliorée par le nombre de traits biométriques, qui doit être limité par des considérations pratiques comme le coût de déploiement, le temps d'enrôlement, le temps de calcul (prise de décision) ou encore le taux d'erreur, [10].

La conception d'un système biométrique multimodal nécessite la conception d'une Interface Homme-Machine (IHM) adéquate afin de permettre une acquisition efficace des informations biométriques d'un individu, en respectant la réalisation des conditions suivantes :

- **Le coût :** le coût dépend du nombre de capteurs utilisés, du temps d'acquisition et de calcul des données biométriques, les exigences de stockage et le degré de commodité perçue par l'utilisateur, [10].

- **Les sources de l'information biométrique :** la détermination des sources de l'information biométrique à utiliser (Exemple pour le contrôle d'accès : visage et empreinte du doigt), et le choix des plus pertinentes (adéquates) pour une application précise, [10].

- **La séquence de tâches :** c'est la manière de transaction avec les informations biométriques, c'est-à-dire : définir les cas d'acquisition/traitement en parallèle (simultanément), et les cas d'acquisition/traitement en série (successivement), [10].

- **Le type d'information :** la sélection des informations qui doivent être fusionnées (caractéristiques, scores, décisions), et l'étude de l'influence de la corrélation entre les sources fusionnées. [10].

- **La méthode de fusion :** c'est la réalisation d'un plan de fusion de plusieurs sources d'information accomplissant une performance optimale du système biométrique, [10].

Quelques paramètres :

- Fusion au niveau du capteur peut être organisée en trois catégories : [1.3]
  (1) Un seul capteur, plusieurs instances,
  (2) des capteurs multiples intra-classe,
  (3) des capteurs multiples inter classe.

- Fusion au niveau des fonctions peut être organisée en deux catégories : [1.3]
  (1) intra-classe
  (2) interclasse

- Intra-classe est classé en quatre catégories : [1.3]
  (1) même capteur, mêmes fonctionnalités.
  (2) même capteur, des caractéristiques différentes.
  (3) différents capteurs, mêmes fonctionnalités.
  (4) différents capteurs, des caractéristiques différentes.

Remarque : « fonctionnalité » signifie la tâche réalisée par le capteur.

La performance d'un système biométrique multimodal est souvent évalué par : la précision de reconnaissance, la capacité de stockage (nombre de personnes) du système, le coût résultant par l'ajout de nouveaux capteurs et du temps de calcul supplémentaire de plusieurs modalités durant la phase d'enrôlement et d'authentification, [10].

II. 6.2. Systèmes biométriques selon le traitement des modalités biométriques

Il existe quatre types de systèmes différents dans la manière de traitement de l'information biométrique :

- Systèmes multi-échantillons.
- Systèmes multi-capteurs.
- Systèmes multi-algorithmes.
- Systèmes multi-instances.

II. 6.2.1. Systèmes multi-échantillons

Un seul 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, [10].

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, [10].

II. 6.2.2. Systèmes multi-capteurs

Dans ces systèmes, le même trait biométrique est analysé à l'aide de plusieurs capteurs afin d'extraire des informations diverses, [10].

Par exemple, dans un système, un capteur enregistre la forme 2D d'un visage et un autre enregistre la forme 3D, [10].

II. 6.2.3. Systèmes multi-algorithmes

Dans ces systèmes, les mêmes données biométriques sont traitées par plusieurs algorithmes, [10].

Par exemple, pour enlever les actions faciales ou normaliser la pose du visage, des algorithmes de récupération de forme sont appliqués sur les données du visage au lieu de prendre plusieurs ou nouvelles images.

II. 6.2.4. Systèmes multi-instances

Ces systèmes utilisent tout simplement plusieurs instances d'un même trait biométrique. Par exemple, les empreintes des dix doigts, les iris gauches et droits, le réseau veineux des deux mains, … d'un seul utilisateur, [10].

II. 6.3. Systèmes biométriques hybrides

Le terme de « système hybride » est utilisé pour se référer aux systèmes qui intègrent un sous-ensemble des fonctionnalités de la multi-biométrique ou le multitraitement, [10].

II. 7. Systèmes biométriques adaptatifs

Les systèmes biométriques adaptatifs intéressent à l'auto-mise à jour des bases de données ou des modèles enregistrés selon la variation intra-classe des données opérationnelles. Les avantages doubles de ces systèmes résolvent le problème des données limitées de formation des images et le suivi des variations temporelles de l'entrée donnée par l'intermédiaire d'adaptation, [1.3].

Tout d'abord, avec un système biométrique adaptatif, il ne faut plus de recueillir un grand nombre d'échantillons biométriques au cours de la procédure d'inscription. Deuxièmement, il n'est plus nécessaire de se réinscrire ou recycler le système à partir du zéro afin de faire face à un environnement changeant. Pour toute erreur de classification (cas de refus) par le système biométrique, une adaptation du système est appliquée en utilisant l'échantillon d'imposteur. Cette pratique permet de réduire considérablement le coût du maintien d'un système biométrique, [1.3].

II. 8. Domaine d'application des systèmes biométriques

Généralement, un système biométrique est utilisé pour l'identification ou pour la vérification dans les cas suivants :

- Sécurité
  - Authentification de personnes, [14].
  - Contrôle d'accès, [1.1].
  - Gestion de flux de personnes, [14].
  - Contrôle des conditions de respect de la sécurité [1.4]
- Contrôle et gestion de l'exécution d'une procédure particulière, [1.4].

II. 9. Quelques exemples d'application des systèmes biométriques

- Système de gestion des postes frontières basé sur la biométrie, [14].

- Système pour le contrôle d'identité par l'empreinte digitale du doigt, [14].

- Système de lecture et de vérification des documents électroniques, [14].
  Exemples : passeports biométriques, permis de conduire, carte d'identité nationale CIN,…

- Système de recensement biométrique de populations, [14].

- La sécurité des transactions monétaires par la sécurisation des applications monétiques. [14].

- Vidéo surveillance : traitement, stockage, et suppression automatiques des images reçues, [1.4].

- Robotique : La robotique industrielle, la robotique domestique, la robotique médicale et encore la robotique militaire, [1.5].



Lecteur d'empreinte du doigt, [-14.1-].



Lecteur d'empreinte du doigt, [-14.2-].



Vidéo surveillance, [-14.3-].



Lecteur réseau veineux de la main, [-14.4].



Lecteur d'empreinte de la paume de main, [-14.5-].

Figure 14 : Quelques systèmes biométriques, [-14-].

II. 10. L'intérêt des systèmes biométriques

- Rapidité et fiabilité d'authentification.
- Facilité et simplicité d'utilisation.
- Sécurité d'information, d'argent, des personnes.
- Résolution des problèmes de falsification, vol, agression et autres types de crime dans un temps convenable.

II. 11. Quelques problèmes de la biométrie

- Sécurisation de la base biométrique.
- Mise à jour de la base de données biométriques.
- Diminution des taux FRR et FAR.
- Le cas des personnes invalides.

II. 12. Conclusion

La fusion (intégration) de la biométrie et la technologie pour construire des systèmes biométriques a changé le domaine d'authentification vers un état plus moderne, rapide et fiable surtout après l'application de l'approche de la multi-biométrique, multitraitement et l'approche d'auto-adaptation dans ces systèmes biométriques.

Chapitre III :

Reconnaissance Faciale

III. 1. Introduction

L'image visage est le moyen le plus directe et le plus simple pour reconnaître la personne, même à partir d'une loin distance. C'est pourquoi qu'elle est utilisée comme modalité principale dans les systèmes d'authentification surtout dans la vidéo surveillance.

La reconnaissance faciale peut être réalisée par l'intégration d'un capteur à une base de données contenant un nombre très grand d'informations biométriques des visages de personnes. Et lors de la capture d'un individu, un système automatique peut détecter le visage et le traiter soit pour vérifier s'il est enregistré ou pour l'identifier.

Pour les systèmes de reconnaissance faciale de contrôle, il est possible d'enregistrer de nouvelles personnes non sauvegardées, c'est-à-dire une auto-adaptation de la base afin de détecter des suspects ou déclencher une alerte.

III. 2. Concept

Le visage de l'humain représente l'interface principale de reconnaissance des personnes entre eux.

III. 3. Composantes d'un visage

Généralement, on classe les composantes du visage en deux catégories :

- Composantes externes : yeux, bouche, nez, oreilles,…
- Composantes internes : les muscles,…

III. 3.1. Composantes externes

Les organes : yeux, bouche, nez, oreilles, joues… représentent l'aspect général externe d'un visage utilisé pour se distinguer entre les personnes. On mentionne aussi: la barbe, les cheveux, les moustaches, et les sourcils.

III. 3.2. Composantes internes

La structure interne du visage est formée par les muscles de la face ou plutôt les muscles de la mimique (38 muscles).

Exemple de muscles superficiels (25 muscles) :

- Muscle occipital-frontal (impair).
- Muscles auriculaires (muscles antérieur, supérieur et postérieur).
- Muscle orbiculaire de l'œil (parties orbitaire, palpébrale).
- Muscle élévateur commun de la lèvre supérieure et de l'aile du nez.
- Muscle petit zygomatique.
- Muscle grand zygomatique.
- Muscle orbiculaire de la bouche, (impair).
- Muscle abaisseur de l'angle de la bouche.

Exemples de muscles profonds (13 muscles) :

- Muscle corrugateur du sourcil.
- Muscle nasal (parties transverse et alaire).
- Muscle élévateur de la lèvre supérieure.
- Muscle abaisseur de la lèvre inférieure.

, [1.6].

III. 4. Codage des actions du visage

Le « système de codage des actions faciales (FACS) », en anglais « facial action coding system » est une méthode de description des mouvements du visage (les expressions faciales) développée par les psychologues *Paul Ekman* [1.7] (Américaine, [1.8]) et *Wallace Friesen* en 1978, [1.7].

Dans le système FACS, les contractions et les décontractions du visage (Les mouvements du visage) sont décomposées en « unité d'action (UA) » (action unit, AU), d'où chaque UA correspond à la contraction ou à la détente d'un ou plusieurs muscles, qui se traduit par un mouvement d'une partie du visage. Le système FACS se base sur la description de 46 UAs identifiées par un numéro dans la nomenclature FACS, on cite parmi eux les exemples suivants, [1.7] :

N° : UA	**Nom de l'action**	**Muscle actionneur**
0	Visage neutre	Relaxation de tous les muscles du visage
1	Remontée interne des sourcils	Muscle frontales médiales
2	Remontée externe des sourcils	Muscle frontales latérales
5	Ouverture entre la paupière supérieure et les sourcils	Muscle orbiculaire de l'œil
6	Remontée des joues	Muscle orbiculaire de l'œil (orbital)
7	Tension de la paupière	Muscle orbiculaire de l'œil (palpébral)
8	Lèvres fermées	Muscle orbiculaire de la bouche
10	Remontée de la partie supérieure de la lèvre	Muscle releveur de la lèvre supérieure
12	Étirement du coin des lèvres	Muscle grand zygomatique
16	Ouverture de la lèvre inférieure	Muscle abaisseur de la lèvre inférieure
17	Élévation du menton	Muscle Mentonnier
20	Étirement externe des lèvres	Muscle risorius et le muscle du cou
21	Tension du cou	muscle du cou
22	Lèvres en "O"	Muscle orbiculaire de la bouche
23	Tension refermante des lèvres	Muscle orbiculaire de la bouche
24	Lèvres pressées	Muscle orbiculaire de la bouche
26	Ouverture de la mâchoire	muscle temporal et un autre
43	Yeux fermés	Relaxation du l'élévateur palpébral supérieur
45	Clignotement	Relaxation d'élévateur palpébral supérieur contraction du muscle orbiculaire de l'œil
46	Clignement de l'œil	Muscle orbiculaire de l'œil

, [1.7].

P. Ekman a fondé une école de formation à la lecture des expressions émotionnelles sur un visage. Il est par exemple possible de distinguer deux types de sourires, [1.7] :

- Le sourire vrai : involontaire, qui met en contraction les muscles *zygomatique majeur* et le muscle *orbiculaire de l'œil*.
- Le sourire faux : ou sourire social, volontaire dans lequel seul le muscle *zygomatique* est contracté.

L'intensité des unités d'action est notée par les lettres A à E (d'une intensité minimale à une maximale), [1.7].

- A : Trace
- B : Léger
- C : Marqué ou prononcé
- D : Sévère ou extrême
- E : Maximum

Et voici quelques exemples des unités d'action avec leurs expressions, [1.7] :

Joie	6+12
Surprise	1+2+5B+26
Peur	1+2+4+5+20+26
Colère	4+5+7+23

Remarque :

L'avantage d'étudier les expressions faciales est de récupérer la forme originale d'un visage après une déformation par les actions de visage (les contractions et les décontractions) par des algorithmes spécifiques.

III. 5. Reconnaissance d'un visage

La reconnaissance faciale à été premièrement étudiée dans un cerveau humain pour distinguer les différentes régions et chemins reliées à la reconnaissance des visages et leur fonctionnement. Et après la compréhension du voyage de l'image dans le champ visuel de l'être humain, des études ont été réalisées pour reconstruire un système industriel de reconnaissance automatique de visages sur des principes biologiques.

III. 5.1. Reconnaissance par le cerveau humain

(La neurobiologie de la reconnaissance des visages)

[…] Des études ont permis d'identifier chez l'homme sain plusieurs régions du cerveau qui s'activent davantage lorsqu'on présente des photographies ou des dessins de visages que d'autres catégories d'objets […], [15].

[…] La région la plus sensible à la présentation des visages est localisée à la jonction du lobe occipital et du lobe temporal inférieur, au niveau du gyrus fusiforme. Pour cette raison, certains chercheurs lui ont donné le nom d' « aire fusiforme faciale »

(fusiform face area en anglais ou FFA), même si cette région est aussi activée (mais moins) par les autres objets. Une autre région, postérieure, au niveau occipital inférieur droit, présente le même type de réponse : c'est l'aire occipitale des visages (en anglais occipital face area, OFA) […], [15].

[…] Les aires OFA et FFA de l'hémisphère droit sont plus activées par les visages que celles de l'hémisphère gauche. Ces observations confirment la dominance […] des deux régions cérébrales de l'hémisphère droit, au niveau occipital et temporal (les aires FFA et OFA) pour la reconnaissance des visages […], ils sont nécessaires pour percevoir les aspects singuliers d'un visage, permettant de l'identifier en tant qu'individu […], [15].

[…] Ces aires cérébrales sont davantage activées par les visages que par d'autres catégories d'objets. Comment savoir si elles sont particulièrement impliquées dans la perception et la reconnaissance des visages ? Précisément en étudiant les personnes atteintes de « prosopagnosie » […], [15].

[…] Le terme de prosopagnosie est utilisé pour la première fois en 1947 par un neurologue allemand, *Joachim Bodamer*, qui le forme à partir des mots grecs *prosopon* (visage) *agnosis* (sans connaissance), c'est-à-dire absence de connaissance des visages. Cette définition s'accompagnait d'une description de plusieurs cas et laissait croire qu'il existerait dans le cortex cérébral une région responsable de la faculté de reconnaître les visages. Lorsque cette région est détruite à la suite d'un accident vasculaire ou d'un traumatisme crânien, la personne présenterait un trouble prosopagnosique pur, c'est-à-dire une perte de la capacité à reconnaître les visages, en l'absence de difficultés pour reconnaître les objets […], [15].

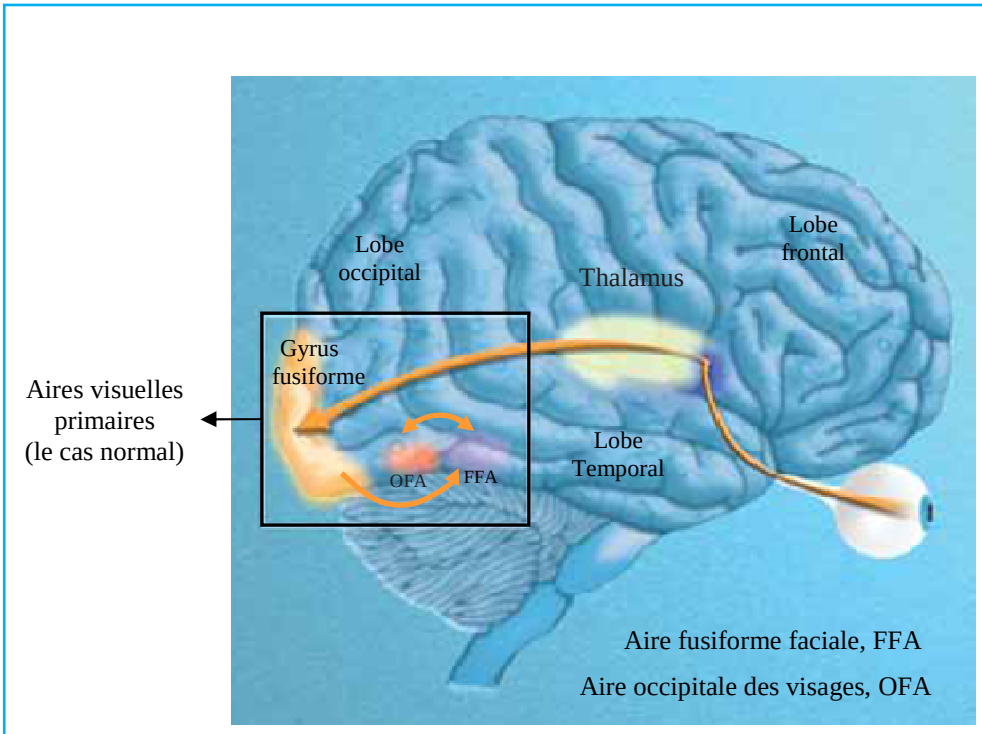


Figure 15 : Les régions de reconnaissance des visages chez les humains dans le cas normal, [-15-].

[…] Quand on présente des photographies de visages aux sujets, quelle est la séquence des réponses dans ces régions du cerveau ? L'information visuelle en provenance de la rétine se projette, via le corps genouillé latéral du thalamus, à l'arrière du cerveau au niveau du cortex visuel primaire. L'information est ensuite transmise vers des régions de plus en plus antérieures, selon deux voies de traitement principal : vers le lobe pariétal pour ce qui concerne la localisation de l'information dans l'espace, et vers le lobe temporal pour ce qui concerne la reconnaissance des objets et des visages. Tandis que les neurones des régions postérieures traitent une petite partie du champ visuel et répondent à des propriétés simples […], les neurones des régions antérieures présentent un champ récepteur beaucoup plus large et répondent à des stimulus plus complexes, par exemple des combinaisons de traits, des scènes complexes ou des visages […], [15].

[…] En accord avec cette conception hiérarchique du système visuel, il a été suggéré que les réponses aux visages au niveau de la FFA dépendent de la transmission d'informations traitées dans la région postérieure, l'OFA. Cette dernière région constituerait en quelque sorte l'entrée du système de reconnaissance des visages dans le cerveau […], [15].

Donc, […] dans le cas normal, des signaux passent directement des aires visuelles à l'aire FFA, court-circuitant l'aire OFA alors que les neurobiologistes pensaient que les aires étaient activées dans l'ordre, des plus postérieures au plus antérieures. L'aire OFA interviendrait ensuite dans l'analyse détaillée du visage, contribuant à l'identification de la personne […], [15].

Après des recherches neurobiologiques supplémentaire, les chercheurs ont déduit qu'en réponse aux visages : dans le cerveau normal, la région du gyrus fusiforme droit « l'aire FFA » – antérieure – peut être activée indépendamment de l'aire OFA (en l'absence de transmission d'informations en provenance de l'aire OFA) – postérieure – du même hémisphère, et assurer la détection du visage. Toutefois, cette représentation initiale du visage serait grossière, et nécessiterait divers mécanismes permettant d'affiner l'image du visage dans le cerveau. Certains de ces processus seraient localisés au niveau de l'aire OFA, qui contient des neurones dont le champ récepteur plus réduit permettrait d'encoder les détails du visage. Une sorte de boucle réentrante pourrait se mettre en place entre ces régions critiques pour discriminer et reconnaître les visages, [15].

III. 5.2. Reconnaissance par le système biométrique

Un système biométrique de reconnaissance de visage représente un cerveau industriel de la partie visuelle, qui nécessite en premier temps la sauvegarde ou bien l'apprentissage des visages, et en deuxième il permet de tester des images visages quelconques et décide si elles sont connues ou non. Les systèmes de reconnaissance consistent généralement des étapes suivantes :

- L'acquisition de l'image biométrique.
- Le prétraitement de l'image.
- La détection de visages.
- L'extraction des caractéristiques du visage.
- L'authentification (Classification) du visage.

III. 5.2.1. Acquisition de l'image biométrique

L'acquisition est le point d'entrée du processus de reconnaissance de visage. C'est le module où l'image visage sous considérations et conditions est présentée dans le système. Le module d'acquisition peut demander l'image visage à partir différents environnements : un fichier stocké dans une mémoire, un papier utilisé par l'intermédiaire d'un scanner, ou une image capturée au temps réel à l'aide d'une caméra, [11].

III. 5.2.2. Prétraitement de l'image acquise

Les images visages sont souvent normalisées afin d'améliorer la performance du système de reconnaissance. Tous ou quelques pas de prétraitements suivants peuvent être implémentés dans un système de reconnaissance de visage :

- **Normalisation de la taille :** Il est d'habitude de changer la taille de l'image acquise à une taille par défaut tel que 128×128 pixels selon les paramètres du système (Sur laquelle le système de reconnaissance de visage opère), [11].

- **Égalisation de l'histogramme :** elle est souvent utilisée dans les images trop sombres (obscures) ou très claires dans l'ordre d'améliorer la qualité de l'image. Elle modifie le contraste de l'image (l'écart entre les valeurs les plus clairs et les valeurs les plus foncées), et comme résultat des traits important du visage deviennent plus nets, [11].

- **Filtre de la médiane :** Pour les images bruitées, spécialement lesquelles obtenues par une caméra. Le filtre de la médiane peut nettoyer l'image sans perte d'information, [11].

- **Filtre passe-haut :** L'extracteur de trait basant sur le plan de visage peut offrir des résultats tels que ceux obtenue par un plan de détection. Le filtre passe-haut augmente l'accentuation de détails tel que les contours, ce qui améliore la performance de détection des formes, [11].

- **Normalisation des arrières plans :** dans l'ordre de traiter les informations faciales, les arrières plans du visage doivent être normalisés, surtout dans le cas des systèmes ou l'image entière est utilisée. Donc le module de prétraitement doit être capable de détecter le contour de visage afin d'homogénéiser le reste de l'image et obtenir un arrière plan homogène, [11].

- **Normalisation de translation et rotation :** dans quelques cas, il est possible de traiter des images visages dont la tête est décalée ou tournée selon une orientation parmi les directions suivantes (haut, bas, gauche, droite, haut-droite, haut-gauche, …). Mais dans le cas des systèmes basant sur la vue frontale seulement ou profil, la normalisation de rotation de la tête est nécessaire, [11].

- **Normalisation d'illumination :** Les images visages prises dans différentes intensités d'illumination peuvent réduire la performance du système de reconnaissance, spécialement pour les systèmes de reconnaissance des visages basant sur l'Analyse En Composantes Principales où une information entière est utilisée pour la reconnaissance.

Une photo peut être vue comme un vecteur de reflets (niveaux de gris) $\boldsymbol{r(x)}$ **.** Ainsi sous une illumination uniforme $\boldsymbol{I}$ la photo correspondante est donnée par :

$$\boldsymbol{r`(x) = I.r(x)}$$

La normalisation est réaliser par imposer un niveau d'illumination $\boldsymbol{I_0}$ en un point de référence $\boldsymbol{x_0}$ d'une photo, et la photo normalisée est donc donnée par :

$$\boldsymbol{r``(x) = \frac{I_0.r`(x)}{Ix_0}}$$

Remarque : s'il y a plusieurs points de références $\boldsymbol{x_i}$, on utilise la moyenne de ces points de références $\boldsymbol{moy}\{\boldsymbol{x_i}\}$, [11].

III. 5.2.3. Détection de visages dans l'image

La détection de visage est un domaine de la vision par ordinateur consistant à détecter un visage humain dans une image numérique. C'est un cas spécifique de « détection d'objet », où l'on cherche à détecter la présence et la localisation précise d'un ou plusieurs visages dans une image, [1.9].

[…] La détection de visage a de très nombreuses applications directes en vidéosurveillance, biométrie, robotique, commande d'interface homme-machine, photographie, indexation d'images et de vidéos, recherche d'images par le contenu, etc. Elle permet également de faciliter l'automatisation complète d'autres processus comme la reconnaissance de visage ou la reconnaissance des expressions faciales […], [1.9].

[…] Plusieurs travaux de recherches ont été effectués dans ce domaine. Ils ont donné lieu au développement d'une multitude de techniques allant de la simple détection du visage, à la localisation précise des régions caractéristiques du visage, tels que : les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc. […], [7].

Parmi les méthodes de détection des visages : segmentation, détection de contours, …. …



Figure 16 : Détection de visage, [-16-].

III. 5.2.4. Extraction des caractéristiques du visage (Codage des traits du visage)

Après l'accomplissement de quelques prétraitements (Si nécessaire), l'image normalisée du visage est présentée devant le module d'extraction de traits dans l'ordre de former une signature numérique qui sera utilisée durant la classification, [11].

Afin d'extraire les caractéristiques et différents traits du visage, On passe par deux étapes différentes : la première se base sur l'extraction des régions entières du visage, elle est implémentée avec une approche globale de reconnaissance du visage. La deuxième extrait les points spécifiques des différentes régions caractéristiques du visage, tels que : les coins des yeux, de la bouche et du nez. Elle est utilisée avec une méthode locale de reconnaissance, [7].

Dernièrement, autres méthodes sont développées pour extraire le contenu complet d'une image comme l'Analyse En Composantes Principales (ACP), qui a l'avantage de garder toute l'information contenant dans l'image sans perte, ce qui améliore la performance de reconnaissance du système.

Plusieurs recherches et études montrent que les caractéristiques pertinentes dans la reconnaissance faciale soient : les cheveux, le contour du visage, le nez, les yeux et la bouche, et que la partie supérieure du visage soit plus utile pour la reconnaissance faciale que la partie inférieure, [7].

Après l'extraction des caractéristiques du visage sous forme digital, le générateur du modèle de référence construit une signature biométrique numérique qu'elle est stockée ultérieurement dans la base de données.

Et voici quelques méthodes à suivre afin d'extraire les caractéristiques des visages : le modèle de forme active, le modèle complet, l'Analyse En Composantes Principales, …

III. 5.2.4.1. Modèle de forme active

La forme active est une méthode de représentation du visage par la détermination des points principaux du visage. Et après la liaison de chaque deux points adjacents par une droite, on obtient le plan du visage.

III. 5.2.4.1.1. Modèle de forme active 2D

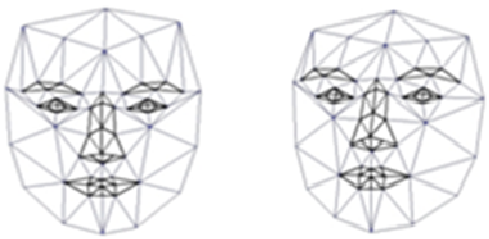


Figure 17 : Modèle de forme active en 2D, [-17-].

- On ne conserve que la forme et pas la texture.
- Vecteur des caractéristiques = Vecteur des coordonnées des sommets (les points) qui forment le visage [16], ou les mesures entre les sommets reliés. Ces coordonnées et ces mesures sont calculées par exemple, par la projection en un plan 2 dimensions (x, y).

III. 5.2.4.1.2. Modèle de forme active 3D

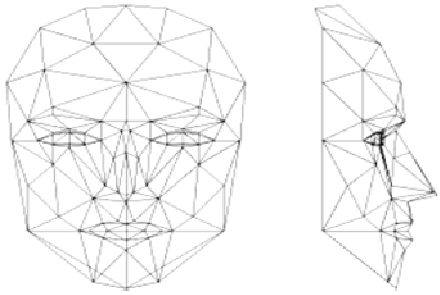


Figure 18 : Modèle de forme active en 3D, [-18-].

- On ne conserve que la forme et pas la texture.
- Vecteur des caractéristiques = Vecteur des coordonnées des sommets (les points) qui forment le visage [16], ou les mesures entre les sommets reliés. Ces coordonnées et ces mesures sont calculées par exemple, par la projection en un plan 2 dimensions (x, y) ou 3 dimensions (x, y, z).

III. 5.2.4.2. Modèle Complet

Le modèle complet signifie qu'on garde toute l'image soit en 2D ou en 3D :

III. 5.2.4.2.1. Modèle complet 2D



Figure 19 : Un modèle complet en 2D, [-19-].

- On conserve toute l'image.
- On représente l'image par un tableau (1D ou 2D), dont chaque case contient la valeur d'un pixel.
- Parmi les méthodes utilisées pour traiter ces types d'images :
    - Analyse en Composantes Principales (APC), [17].
    - Analyse en Composantes Indépendantes (ACI).
    - Analyse Linéaire Discriminante (LDA).

III. 5.2.4.2.2. Modèle complet 3D



Figure 20 : Modèle complet en 3D, [-20-].

- On conserve toute l'image.
- On représente l'image par un tableau (1D ou 2D), dont chaque case contient la valeur d'un pixel.
- Parmi les méthodes utilisées pour traiter ces types d'images :
    - Analyse en composantes principales (PCA), [17].
    - Analyse en composantes indépendantes (ICA).
    - Analyse linéaire discriminante (LDA).



Figure 21 : Autres modèles complets en 3D, [-21-].

III. 5.2.5. Authentification (Classification) du visage (Identification et/ou vérification)

La reconnaissance d'un visage est une méthode utilisée pour identifier les personnes à partir de leurs visages, et aussi pour les classifier comme connues ou inconnues, en basant sur une base de visages enregistrés comme connus. Dans cette étape et à l'aide d'un classifieur, les traits extraits sont comparés à ceux stockés dans la base de données des visages du système. Après cette comparaison, l'image visage est classifiée comme connue ou inconnue, avec la possibilité d'enregistrer les nouveaux individus inconnus, [11].

La reconnaissance d'un visage requête est obtenue par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données. La reconnaissance dépend du mode de comparaison utilisé : vérification ou identification, [7].

Les méthodes de reconnaissance (de classification) des visages :

- Classifieur non linéaire
- Classifieur linéaire
    1. PCA : Principal Components Analysis (Eigenface).
    2. LDA : Linear Discriminant Analysis (Fisherface).
    3. ICA : Independant Components Analysis.
    4. SVM : Support Vector Machine.
    5. …
- Autres classifieur
    1. Hiden Marcov Model.
    2. Active Appearance Model (AAM).
    3. …

III. 6. Difficultés de la reconnaissance faciale

Le processus de reconnaissance du visage rencontre souvent des difficultés liées aux personnes et/ou leur environnement tels que :

- **Orientation (pose) :** les mesures des images d'un visage se changent en fonction de l'orientation de ce dernier (face [0°], profil [90° ou -90°], et autres positions dans l'intervalle [-180°,180°]), [7][1.5]. Quand le visage a une orientation profil < 30° ou < -30 dans le plan image, il peut être normalisé. Cependant, lorsque la rotation est hors l'intervalle [-30,30] la normalisation géométrique n'est plus possible, [7].

- **Caractéristiques particulières :** la présence ou l'absence des composantes faciales temporaires tels que la barbe, les moustaches, le maquillage et les lunettes ont une grande influence sur les composantes structurales du visage, surtout au niveau de la forme, de la couleur, et de la mesure des parties du visage, [7][1.9], ce qui cause une défaillance du système de reconnaissance, [7].

- **Les occultations :** les visages peuvent être partiellement occultés (cachés) par d'autres objets (porte, …), accessoires (écharpe, chapeau, …) ou personnes (tête, main, …). [7][1.9].

- **Les conditions d'illumination et la qualité de l'image :** l'éclairage de la source lumineuse et sa intensité, et encore les caractéristiques du capteur influencent sur la qualité d'apparition des visages dans l'image acquise, [7][1.9]. […] En effet, le changement d'apparence d'un visage du à l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entraîner une mauvaise classification des images d'entrées […], [7].

- **Les expressions faciales :** modifient la géométrie du visage, ce qui nécessite des traitements additifs de l'image acquise pour récupérer les traits originaux du visage, [1.9]. […] La déformation du visage qui est due par les expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale située dans la partie supérieure du visage reste quasi invariable donc elle est généralement suffisante pour effectuer une identification […], [7].

- **Variabilité intrinsèque des visages humains :** (couleur, taille, forme), [1.9]. La mise à jour de la base de données des visages enregistrés dans le système biométrique est nécessaire d'une manière périodique (annuelle, bisannuelle, …) car la face d'une personne se varie d'une façon continue en taille (amaigrissement, grossissement), en couleur (blanchissement, noircissement), en trait (cicatrice, tache,…) et en âge (enfant, jeune, homme,…)

III. 7. Domaine d'application de la reconnaissance faciale

- Sécurité.
  - Détecter des suspects, [18].
  - Suivre le trajet emprunté par un criminel ou un suspect, [18].
  - Vidéosurveillance.
- Gestion.
- Contrôle.

III. 8. Problèmes des systèmes de reconnaissance faciale

- Mise à jour de la base de données des visages enregistrés.
- Flicage d'un grand nombre de personnes, [18].

III. 9. Conclusion

Le processus de la reconnaissance faciale est réalisé par un ensemble de tâches successives dans un système biométrique : acquisition et prétraitement de l'image, la détection de visage et dernièrement l'authentification d'un visage.

Malgré que la reconnaissance automatique faciale n'ait pas des résultats déterminismes et évidentes à cause de variation de l'orientation, les conditions d'illuminations, les expressions faciales, … . Mais, elle offre généralement un taux d'erreurs acceptable.

Chapitre IV :

Modèles De Protection De L'Information Biométrique

IV. 1. Introduction

L'unicité de l'information biométrique (traits propres à l'individu) a posé plusieurs problèmes de sécurité et de confidentialité, c'est à dire : si l'information biométrique est perdue ou volée il ne sera pas possible de la remplacer par une autre.

Afin d'éviter ces risques, plusieurs modèles de protection des données biométriques ont été conçus. Ces modèles peuvent être regroupés en trois approches : approche transformation (conversion, changement, calcul,…), approche crypto-système (cryptage) et l'approche hybride (transformation, crypto-système). Donc, au lieu de stocker l'information biométrique sous sa forme originale, il est préféré de stocker le modèle transformé, crypté, ou transformé-crypté.

L'approche transformation peut être annulable (révocable), par contre l'approche crypto-système ne peut être jamais annulable (irrévocable).

Parmi les modèles de protection conçus :
- L'engagement flou (En anglais, Fuzzy Commitement), par Juels et Wattenberg.
- Le coffre flou (En anglais, Fuzzy Vault), par Juels et Sudan.
- Le plan des données assistantes (En anglais, Helper Data Sheme).

Le schéma suivant montre les différentes approches de protection de l'information biométrique et leur application dans un système biométrique :

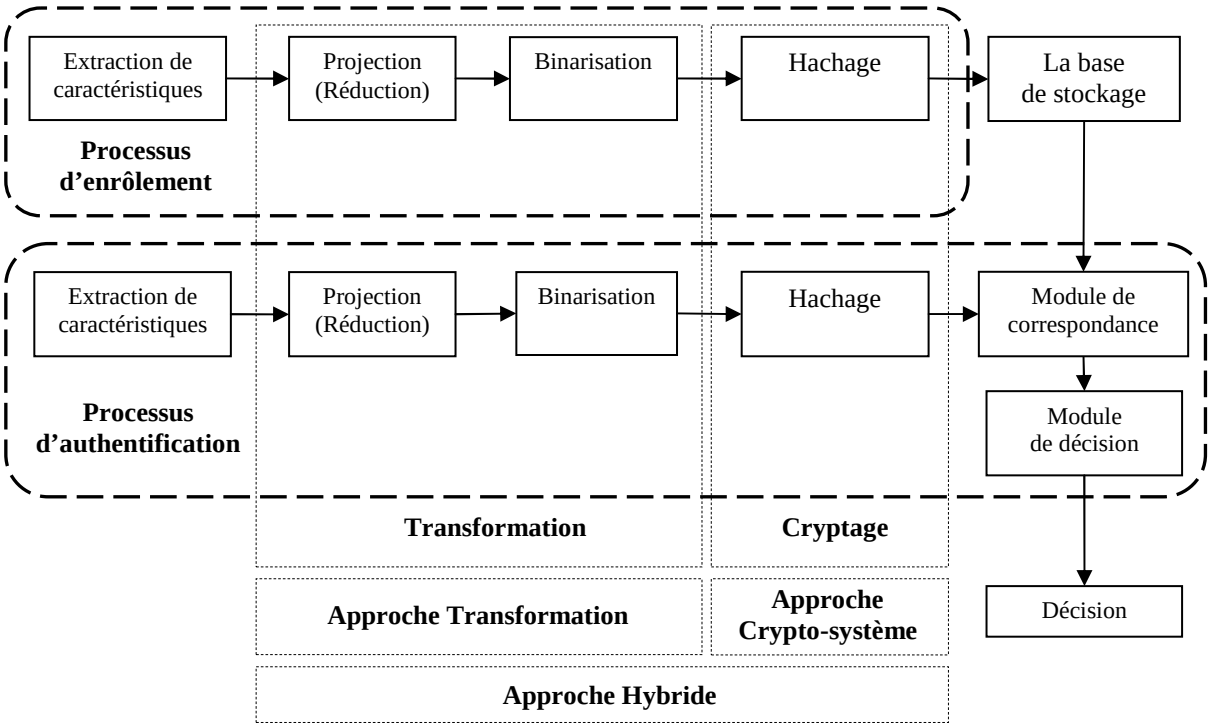


Figure 22 : Approches de protection de la base des données biométriques, [-22-].

IV. 2. Protection de l'information biométrique

Le plan de la protection peut être devisé en deux catégories : Approche *transformation des traits* et l'approche *crypto-système biométrique*.

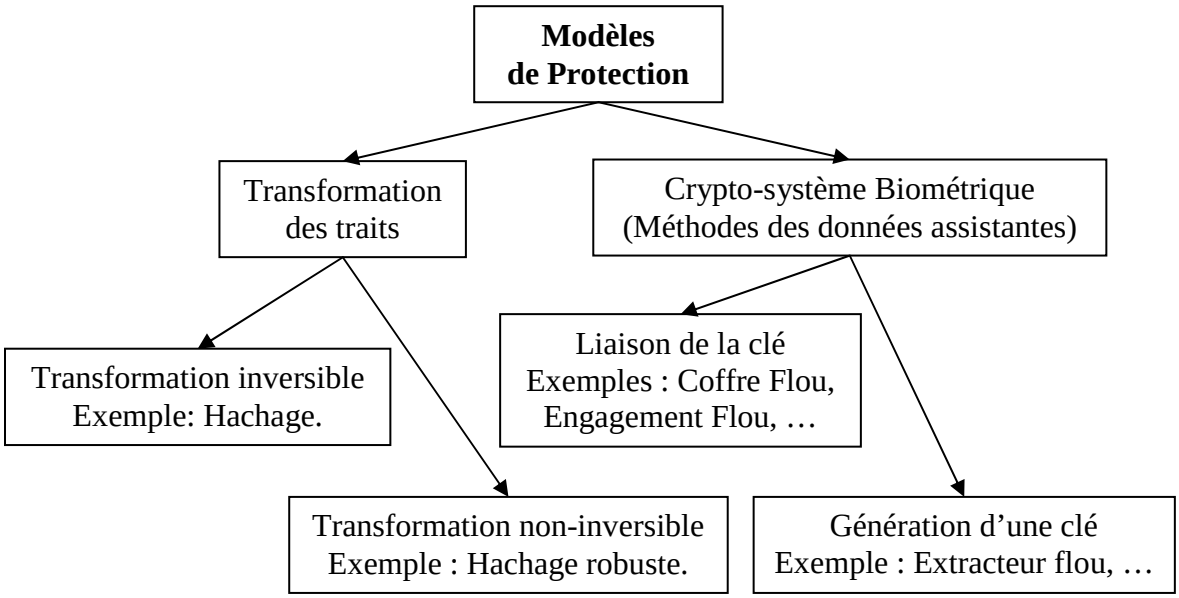


Figure 23 : Catégories des modèles de protection, [-23-].

- La projection, pour réduire la dimension des données biométriques, [19].
- La fonction de hachage est appliquée pour protéger les informations, [19] et réduire sa dimension.

Un plan idéal de protection de la base biométrique doit posséder les propriétés suivantes :

- **Confidentialité :** l'impossibilité de compatibilité entre les bases de données, [20].
- **Révocabilité :** possibilité d'annuler des données biométriques compromisses et les remplacer par d'autres correspondantes, [20].
- **Sécurité :** difficulté d'obtenir la base biométrique originale à partir de la base biométrique sécurisée, [20].
- **Performance :** le plan de la protection de la base biométrique ne doit pas réduire la performance de la reconnaissance (FAR et FRR), [20].

IV. 2.1. Approche de transformation des traits

Une fonction de transformation est appliquée sur le modèle biométrique, puis le modèle transformé est stocké dans la base de données. Les paramètres de la fonction de transformation sont généralement obtenus à partir d'une clé aléatoire ***K*** ou un mot de passe. La même fonction de transformation est appliquée à un modèle biométrique

requête, et le modèle requête transformé est comparé avec le modèle original transformé. La fonction de transformation peut être catégorisée en tant que *transformation inversible* et *transformation non inversible*, [20].

IV. 2.1.1. Transformation inversible

La transformation inversible est réalisée par une fonction associée à un mot de passe qui doit être fourni par l'utilisateur. La fonction ne s'active sauf dans la présence des données biométriques avec un mot passe, ce dernier doit être stocké dans la base et rappelé par l'utilisateur lors de la phase d'authentification. L'utilisation d'un mot de passe augmente le nombre de personnes enregistrées, [20].

La fonction de transformation est inversible, […] donc si un adversaire a gagné l'accès à la clé et le modèle transformé, il pourra récupérer le modèle biométrique original (ou une approximation de celui-ci). Par conséquent, la sécurité de la base biométrique dépend de la sécurité du mot de passe […], [20].

IV. 2.1.2. Transformation non-inversible

La transformation non inversible se réfère à une fonction à un seul sens de calcul, qui est facile à calculer au sens directe (en temps polynomial) et difficile dans le sens inverse. Comme la méthode précédente, La fonction ne s'active sauf dans la présence des données biométriques avec un mot de passe, ce dernier doit être stocké dans la base et rappelé par l'utilisateur lors de la phase d'authentification, [20].

[…] La caractéristique principale de cette approche est que, même si le mot de passe et/ou le modèle transformé sont connus, il est mathématiquement difficile (en terme de complexité) pour un adversaire de récupérer le modèle biométrique original […], [20].

IV. 2.2. Approche crypto-système biométrique

Le crypto-système biométrique est développé pour *sécuriser une clé cryptographique* en utilisant les traits biométriques ou *générer directement une clé cryptographique* à partir les traits biométriques, [20].

Les crypto-systèmes biométriques sont appelés aussi « les données assistantes », à cause du stockage des informations biométriques sous forme codée comme données assistantes. […] Les données d'assistance ne révèlent aucune information significative sur le modèle biométrique original. La clé extraite lors de la phase d'authentification à partir les caractéristiques biométriques requêtes doit être vérifiée par le décodage de correction d'erreurs, qui est utilisé pour gérer les variations intra-classe de l'utilisateur [...], [20].

Les crypto-systèmes biométriques peuvent être classifiés en systèmes par *liaison de la clé* et systèmes par *génération de la clé*, [20].

IV. 2.2.1. Crypto-système par liaison de la clé

Dans un système à liaison de la clé, l'information biométrique est intégrée avec une clé aléatoire, le modèle crypté est stocké dans la base de données comme des données assistantes. Les données assistantes ne donnent aucune information sur la clé ou l'information biométrique originaux (difficulté de décodage du modèle) dans l'absence de l'information biométrique requête originale de l'utilisateur, [20].

Généralement la clé de codage est codée par un codeur de correction d'erreurs (ajout de redondance dans la clé) avant la liaison avec l'information biométrique durant la phase d'enrôlement, afin de corriger les erreurs de la clé extraite requête pendant la phase d'authentification, [20].

Le *plan d'engagement flou* (En anglais, Fuzzy commitment scheme) proposé par *Juels* et *Wattenberg* est l'exemple le plus connu de l'approche liaison de la clé. Autres méthodes de protection de la base biométrique comme : le *Coffre Flou* proposé par Juels et Sudan, *le codage de source distribué* peuvent être considérés comme des crypto-systèmes par liaison de la clé, [20].

IV. 2.2.2. Crypto-système par génération de la clé

La cryptographie par génération directe de la clé, son principe est que les données assistantes soient dérivé à partir les données biométriques seulement, Et la clé du codage soit généré directement à partir les données assistantes et les données biométriques requêtes par des lois spécifiques, [20].

L'*Extracteur Flou* proposé par *Dodis* et *al* est parmi les méthodes de crypto-système par génération de la clé.

IV. 2.3. Approche hybride transformation\crypto-système

Quelques modèles de protection utilisent deux approches à la fois, par exemple : transformation inversible et crypto-système par liaison de la clé, cette fusion d'approches est appelée l'approche hybride. [20].

IV. 3. Modèles de protection de l'information biométrique

On mentionne deux modèles : le coffre flou, et le plan des données assistantes.

IV. 3.1. Plan du Coffre Flou (Fuzzy Vault Sheme)

[…] Le Coffre Flou proposé par *Juels* et *Sudan* en 2002, un autre modèle pour sécuriser la base de données biométriques […], [21].

Le point de départ de la construction du *Coffre Flou* est *l'Engagement Flou* de *Juels* et *Wattenberg*, qui est aussi basé sur l'utilisation des codes de correction d'erreurs, [22].

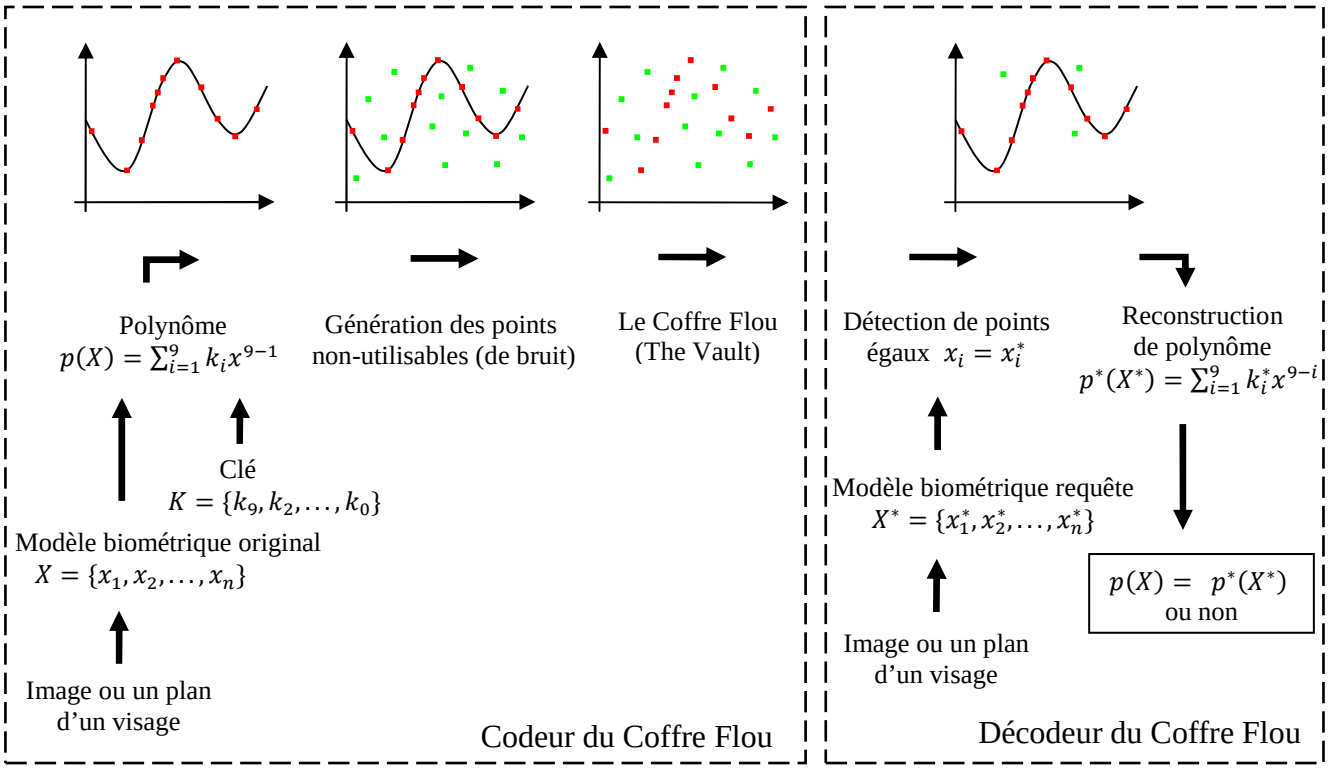


Figure 24 : Coffre floue, [-24-].

IV. 3.1.1. Calcule de la clé du Coffre Flou

Une clé secrète $\boldsymbol{K}$ est chaque information qui est besoin d'être protégée. La clé $\boldsymbol{K}$ est générée comme 128-bits aléatoire en utilisant un générateur de code aléatoire (la clé peut être codée par la cryptographie symétrique AES, Advanced Encryption Standard), [23].

L'algorithme de décodage du coffre flou décode plusieurs clés secrètes (polynômes reconstruis). Pour identifier quelle clé est la secrète originale, on a besoin d'ajouter quelques informations additives dans la clé secret $\boldsymbol{K}$ avant le codage. Par la vérification de la validité (la justesse) de ces informations additives durant le décodage on peut décider si la clé secrète est originale ou non, [23].

Cyclic Redundancy Check ($\boldsymbol{CRC}$) est une généralisation du théorème de bit de parité qui est utilisé pour la détection de l'erreur. Dans le cas du Coffre Flou, l'utilisation de valeurs incorrectes lors de la phase de décodage cause une reconstruction incorrecte du polynôme, [23].

Dans l'implémentation du Coffre Flou, $\boldsymbol{16\ bits\ CRC}$ de données sont calculés à partir de la clé secrète $\boldsymbol{K}$. Donc, la probabilité d'une erreur aléatoire indétectable (échec de décodage) est $\boldsymbol{2^{-16}}$. Les $\boldsymbol{16\ bits\ CRC}$ de données peuvent être représentées sous forme d'un polynôme $\boldsymbol{g_{CRC}(a) = a^{16} + a^{15} + a^2 + 1}$. $\boldsymbol{16\ bits\ CRC}$ sont ajoutés à la droite de la clé secrète originale $\boldsymbol{K}$ ($\boldsymbol{128\ bits}$), On obtient $\boldsymbol{144\ bits}$ de données $\boldsymbol{SC}$. À partir de cette étape, tous les calcules seront fait en *Galois Fields* avec une cardinalité 65536 (Des nombres ≤ 65536 représentés par 16 bits en binaire) notée par $\boldsymbol{GF(2^{16})}$, [23].

La donnée $\boldsymbol{SC}$ est utilisée pour trouver les coefficients du polynôme $\boldsymbol{p}$: $\boldsymbol{144\ bits\ SC}$ peuvent être représentés sous forme d'un polynôme avec $\mathbf{9}$ (144/16) coefficients en $\boldsymbol{GF(2^{16})}$ de degré $\boldsymbol{D = 8}$, [23].

$$\boldsymbol{p(x) = k_8x^8 + k_7x^7 + \ldots + k_1x^1 + k_0}$$

(Simplement, $\boldsymbol{SC}$ est divisée en $\mathbf{9}$ segments de $\boldsymbol{16\ bits}$, et chaque segment est déclaré comme un coefficient spécifique $\boldsymbol{k_i}$ and $\boldsymbol{i = \{8,7,6,5,4,3,2,1,0\}}$, [23].

Donc, la clé calculée est : $\boldsymbol{K = (k_8, k_7, \ldots, k_0)}$.

Remarque :

Galois Field (*Finite Field* en anglais, et *Corps Fini* en Français) est une structure algébrique dont l'addition et la multiplication sont faits par les opérations XOR et AND, [1.10]. Pour tout nombre premier $\boldsymbol{\alpha}$ et tout entier non nul $\boldsymbol{\beta}$, il existe un corps de cardinalité $\boldsymbol{\alpha^{\beta}}$ qui se présente comme l'extension de degré $\boldsymbol{\beta}$ du corps [1.11]. Le corps fini de cardinalité $\boldsymbol{\alpha^{\beta}}$ est noté $\boldsymbol{F_{\alpha^{\beta}}}$ (*Field*, en anglais) ou $\boldsymbol{GF(\alpha^{\beta})}$ (Galois Field, en anglais), [1.11].

IV. 3.1.2. Codage du Coffre Flou

Un modèle biométrique ou un ensemble non-ordonné $\boldsymbol{X = \{x_1, x_2, \ldots, x_n\}}$ est sécurisé par une clé $\boldsymbol{K = (k_8, k_7, \ldots, k_0)}$. Un polynôme $\boldsymbol{p(X) = \sum_{i=1}^{9} k_i x^{9-i}}$ est construit à l'aide des composantes de la clé secrète, [21].

$\boldsymbol{R}$ est calculé par le polynôme $\boldsymbol{p(X)}$ pour chaque valeur du modèle biométrique $\boldsymbol{X}$, $\boldsymbol{R = \{(x_i, p(x_i))\}}$. Quelques points aléatoire sont générés $\boldsymbol{C = \{(absC_i, ordC_i)\}}$ et ajoutés à l'ensemble $\boldsymbol{R}$, ces points additifs sont non-authentiques (En, chaff points), d'où $\boldsymbol{absC_i}$ n'appartient pas à $\boldsymbol{X}$ et $\boldsymbol{ordC_i}$ n'appartient pas à $\boldsymbol{p(X)}$. Donc, $\boldsymbol{R = R \cup C}$, [21].

Les points authentiques et non-authentiques sont stockés dans le Coffre Flou, [24]. La sécurité du Coffre Flou dépend du nombre des points non-authentiques ajoutés à l'ensemble $\boldsymbol{R}$, [22].

- **L'algorithme de codage du Coffre Flou**

Un ensemble $\boldsymbol{E}$. (Par exemple, $\boldsymbol{E = R}$ les nombres réels)
Entrée : Paramètres $\boldsymbol{k, n}$ et $\boldsymbol{r}$ tel que $\boldsymbol{k \leq n \leq r}$.
Une clé secrète $\boldsymbol{K \epsilon E^k}$. (L'exemple standard $\boldsymbol{k = 8}$)
Un ensemble $\boldsymbol{X = \{x_1, x_2, \ldots, x_n\}}$, $\boldsymbol{x_i \epsilon E}$.
Sortie : Un ensemble $\boldsymbol{R}$ de points $\boldsymbol{\{(x_i, y_i)\}_{i=1}^{r}}$ tel que $\boldsymbol{\{x_i, y_i\} \epsilon E}$.
$\boldsymbol{R, C \leftarrow \emptyset}$;
// Génération de points authentiques
$\boldsymbol{Pour\ (i = 1)}$ à $\boldsymbol{(n)\ faire}$
$\boldsymbol{(x_i, y_i) \leftarrow (x_i, p(x_i))}$;
$\boldsymbol{R \leftarrow R\ U\ (x_i, y_i)}$;
$\boldsymbol{Fin\ Pour}$;

// Génération de points non-authentiques
$\boldsymbol{Pour}\ (\boldsymbol{i = n + 1})$ à $(\boldsymbol{r})\ \boldsymbol{faire}$
$\boldsymbol{x_i} \in \boldsymbol{F - X}$; ($\boldsymbol{x_i}$ différent à $\boldsymbol{X}$)
$\boldsymbol{y_i} \in \boldsymbol{F} - \{\boldsymbol{p}(\boldsymbol{x_i})\}$; ($\boldsymbol{y_i}$ différent à $\boldsymbol{p}(\boldsymbol{x_i})$)
$\boldsymbol{C} \leftarrow \boldsymbol{C\ U}\ (\boldsymbol{x_i}, \boldsymbol{y_i})$;
$\boldsymbol{Fin\ Pour}$;
$\boldsymbol{Sortie}\ \boldsymbol{R} \leftarrow \boldsymbol{R} \cup \boldsymbol{C}$;

, [22]

IV. 3.1.3. Décodage du Coffre Flou, [22]

Le décodage du Coffre Flou dépend de la reconstruction du polynôme de la clé secrète. Un utilisateur présente ses traits biométriques $\boldsymbol{X}^*$, et cherche à s'authentifier dans le Coffre Flou, [25].

Un utilisateur essaye de décoder le Coffre Flou en utilisant la requête biométrique $\boldsymbol{X}^* = \{\boldsymbol{x_1^*}, \boldsymbol{x_2^*}, \ldots, \boldsymbol{x_n^*}\}$. Les points utilisés dans la reconstruction des polynômes sont trouvés par la comparaison des valeurs de $\boldsymbol{X}^*$ avec les valeurs de $\boldsymbol{X}$, d'où $\boldsymbol{R} = \{\ (\boldsymbol{x_i}, \boldsymbol{p}(\boldsymbol{x_i})\ \}$. Si $(\boldsymbol{x_j^*} = \boldsymbol{x_i})$, donc le point correspondant dans le coffre $\{(\ \boldsymbol{x_l'}, \boldsymbol{y_l'}) = (\boldsymbol{x_j^*} = \boldsymbol{x_i}, \boldsymbol{p}(\boldsymbol{x_i}))\}$ est ajouté à la liste des points de décodage $\boldsymbol{R'}$. Finalement, On obtient une liste de $\boldsymbol{m}$ points Avec $\boldsymbol{m} \leq \boldsymbol{n}$, [23].

$$\boldsymbol{R'} = \{(\ \boldsymbol{x_1'}, \boldsymbol{y_1'}), (\ \boldsymbol{x_2'}, \boldsymbol{y_2'}), \ldots, (\ \boldsymbol{x_m'}, \boldsymbol{y_m'})\}$$

Pour la reconstruction d'un polynôme de degré $(\boldsymbol{9 - 1})$, toutes les combinaisons possible de $(\boldsymbol{9})$ points à partir $\boldsymbol{R'}$ sont identifiées, [25] avec un nombre total de combinaisons $\boldsymbol{C_m^9}$. Chaque combinaison est utilisée pour retrouver le polynôme correspond à la clé secrète originale en utilisant l'interpolation de Lagrange, [23].

Par exemple, donnant la combinaison $\boldsymbol{r'}(\boldsymbol{9\ points}) \in \boldsymbol{R'}(\boldsymbol{m\ points})$, avec $\boldsymbol{m} \geq \boldsymbol{9}$.

$$\boldsymbol{r'} = \{(\ \boldsymbol{x_1'}, \boldsymbol{y_1'}), (\ \boldsymbol{x_2'}, \boldsymbol{y_2'}), \ldots, (\ \boldsymbol{x_9'}, \boldsymbol{y_9'})\}$$

, [23][25].

Le polynôme peut être reconstruit comme suivant :

$$\boldsymbol{p^*(x)} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{9}} \boldsymbol{p_i^*(x)}$$

$$\boldsymbol{p_i^*(x)} = \boldsymbol{y_i'} \prod_{\boldsymbol{j=1, i \neq j}}^{\boldsymbol{9}} \frac{\boldsymbol{x - y_j'}}{\boldsymbol{y_i' - y_j'}}$$

, [25].

$$\boldsymbol{p^*(x) = y'_1 \frac{(x-y'_2)(x-y'_3)\dots(x-y'_9)}{(y'_1-y'_2)(y'_1-y'_3)\dots(y'_1-y'_9)} + \dots +}$$

$$\boldsymbol{+ y'_n \frac{(x-y'_1)(x-y'_2)\dots(x-y'_{9-1})}{(y'_9-y'_1)(y'_9-y'_2)\dots(y'_9-y'_{9-1})}}$$

, [23].

Les calcules sont faits en $\boldsymbol{GF(2^{16})}$ afin d'obtenir le polynôme suivant:

$$\boldsymbol{p^*(x) = k_8^* x^8 + k_7^* x^7 + \dots + k_1^* x^1 + k_0^*}$$

, [23].

Les étapes de la régénération de la clé secrète du Coffre Flou sont réalisées d'une manière inversée pour obtenir $\boldsymbol{144\ bits\ SC^*}$. Pour vérifier l'originalité de la clé reconstruite, on divise le polynôme correspondant à $\boldsymbol{SC^*}$ avec $\boldsymbol{CRC}$ polynôme primitif : $\boldsymbol{g_{CRC}(a) = a^{16} + a^{15} + a^2 + 1}$. Si le reste est zéro (ou si $\boldsymbol{16\ bits\ CRC^*}$ calculées = $\boldsymbol{16\ bits\ CRC}$ reçus), donc la clé calculée est originale sinon la clé n'est pas originale, [25].

$\boldsymbol{SC^*}$ est segmentée en 2 parties : les premiers $\boldsymbol{128\ bits}$ sont $\boldsymbol{K^*}$ et les restes à droite sont les $\boldsymbol{16\ bits\ CRC}$. La clé cryptographique $\boldsymbol{K}$ est la première partie de $\boldsymbol{128\ bits}$ de $\boldsymbol{K^*}$, [23].

IV. 3.1.4. Exemple général, [21][23]**:**

• n=3
• Les traits biométriques sont définies par $X = \{2, -1, 5, -2\}$.
• La clé $K = (1, 2, -3)$
• Construction du polynôme :

$$p(X) = \sum_{i=1}^{n} k_i x^{n-i} = x^2 + 2x^1 - 3$$

• La projection est $p(X) = \{(2, 5); (-1, -4); (5, 32); (-2, -3)\}$;
• Les points non-authentiques C = {(0, 2); (3, −1)} sont ajoutés à l'ensemble $R = p(X) \cup C$
• R = {(2, 5) ; (0, 2) ; (−1, −4) ; (5, 32) ; (3, −1) ; (−2, −3)}

Le Coffre Floue permet la sécurisation des ensembles non ordonnés comme les données de minuties des empreintes digitales ou des points de visage 2D, son application à des données de visages 3D n'est pas facile, et un problème se posera si un modèle contient la même valeur plusieurs fois.
, [21][23].

IV. 3.2. Plan des Données Assistantes (HDS)

[…] En 1999, *l'engagement flou* à été proposé par *Juels* et *Wattenberg* pour protéger les données biométriques en utilisant un schéma cryptographique existant. Les mots de passe ne sont jamais stockés en une forme de texte en clair mais sous une forme cryptée. Le système peut authentifier un utilisateur sans connaître le mot de passe original. En conséquence, un modèle flou peut être généré à partir des données biométriques et peut être sauvegardé avec des fonctions cryptographiques. Pourtant, le système de protection doit avoir une tolérance aux variations des données biométriques dues au bruit de mesure ou la modification des modalités […]. Pour éviter ce problème, le code de correction d'erreurs est utilisé, [26].

[…] Plus tard, le schéma de données assistantes […] a été développé pour rendre l'idée de l'Engagement Flou possible pour les systèmes biométriques. Le plan des données assistantes peut extraire des modèles sécurisés de données biométriques. Ce gabarit sécuritaire est stable aux variations biométriques et il est impossible de récupérer les informations biométriques d'origine de celui-ci […], [26].

Remarque :

L'expression « le mot de passe » dans le paragraphe au dessus signifie « la clé aléatoire » (Le code aléatoire).

Le schéma suivant représente le plan des données assistantes :

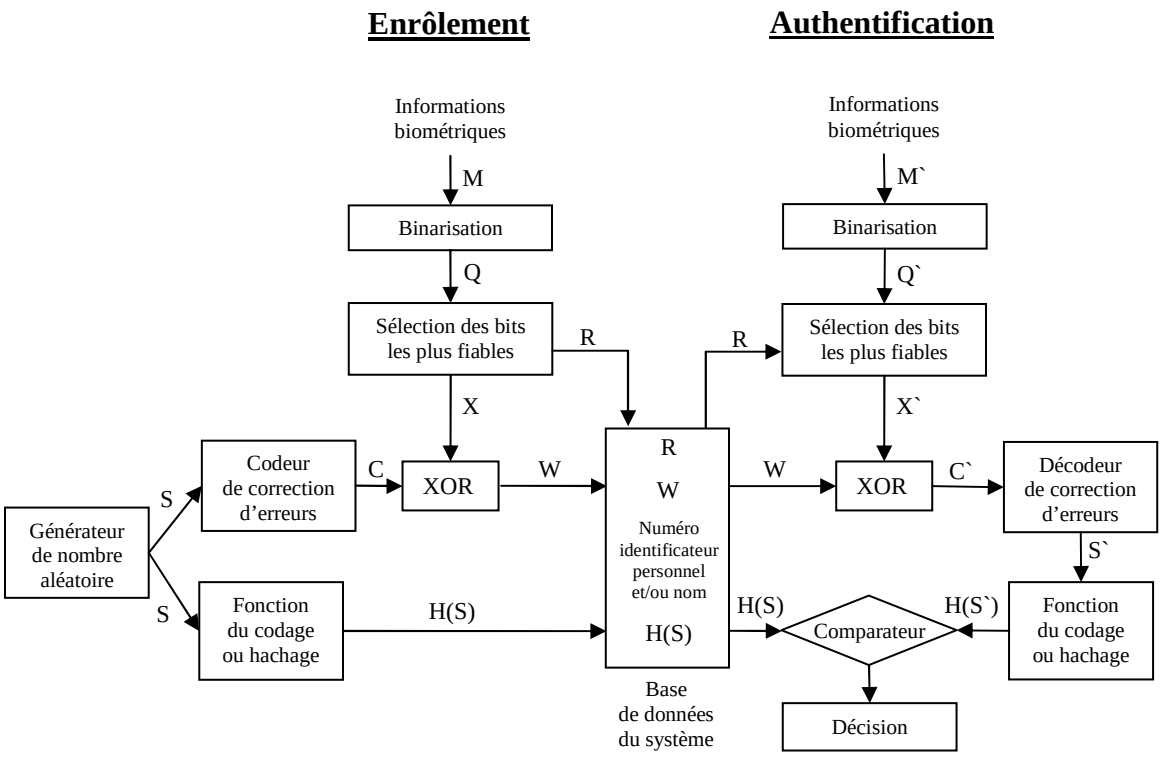


Figure 25 : Plan des Données Assistantes, [-25-].

IV. 3.2.1. HDS au cours du processus d'enrôlement, [26]

- **M**, le modèle biométrique original (Les caractéristiques après l'extraction).

- La Binarisation permet de convertir le modèle biométrique **M** en un vecteur binaire **Q**.

- Un générateur de nombre aléatoire génère un code secret **S**.

    - **S** est haché et stocké.

    - **C**, un codeur de correction d'erreurs ajoute la redondance dans une copie du code secret original **S**. Par conséquence, le code résultant **C** est plus long que **S**.

- Si le vecteur **Q** est plus long que le code **C**, la plupart des bits fiables dans **Q** seront sélectionnés pour former **X**, qu'il a la même longueur que **C**. **R** indique la position des bits les plus fiables sélectionnés.

- **W**, le résultat de la fonction XOR bit à bit de **X** et **C**, est appelé « donnée assistante » (helper data, en anglais).

- Au lieu de stocker le code **S**, le vecteur de positions **R**, les données assistantes **W**, le code secret **h(S)** et l'information d'identité de l'utilisateur seront stockés dans la base de données.

, [26].

IV. 3.2.2. HDS au cours du processus d'authentification, [26]

- **M`**, le modèle biométrique d'authentification ou bien de test (Les caractéristiques après l'extraction). **M`** est potentiellement déformé par un bruit.

- La Binarisation c'est la conversion du modèle biométrique **M`** en un vecteur binaire **Q`**.

- Avec l'identité réclamée, **R**, **W** et **h(S)** sont récupérés à partir de la base de données.
- Si le vecteur **Q`** est plus long que le mot code **W**, les bits fiables dans **Q`** seront sélectionnés pour former **X`**, qui a la même longueur que **W** en utilisant le vecteur **R** qui indique la position des bits les plus fiables à sélectionner.

- **C`**, le résultat de la fonction XOR bit à bit de **W** et **X`**. **C`** peut être aussi pratiquement déformé par un bruit.

- Le décodeur de correction d'erreur en suivant corrige les erreurs dans **C`**, le résultat est le code secret **S`**.

- Par la comparaison de **h(S)** et **h(S`)**, une réponse positive ou négative est fournie pour la question d'authentification.

, [26].

IV. 4. Conclusion

Les modèles de protection de l'information biométrique représentent une structure robuste pouvant affronter et éviter les attaques de falsification et de vol.

Par conséquence, ces méthodes de protection provoquent plusieurs inconvénients sur la fiabilité du système biométrique tels que : la complexité du calcul, stockage d'un grand nombre d'informations dans la base des données (Charge importante de la mémoire), et évidemment l'augmentation du temps de réponse du système.

Chapitre V :

Plan Des Données Assistantes

Le plan des données assistantes

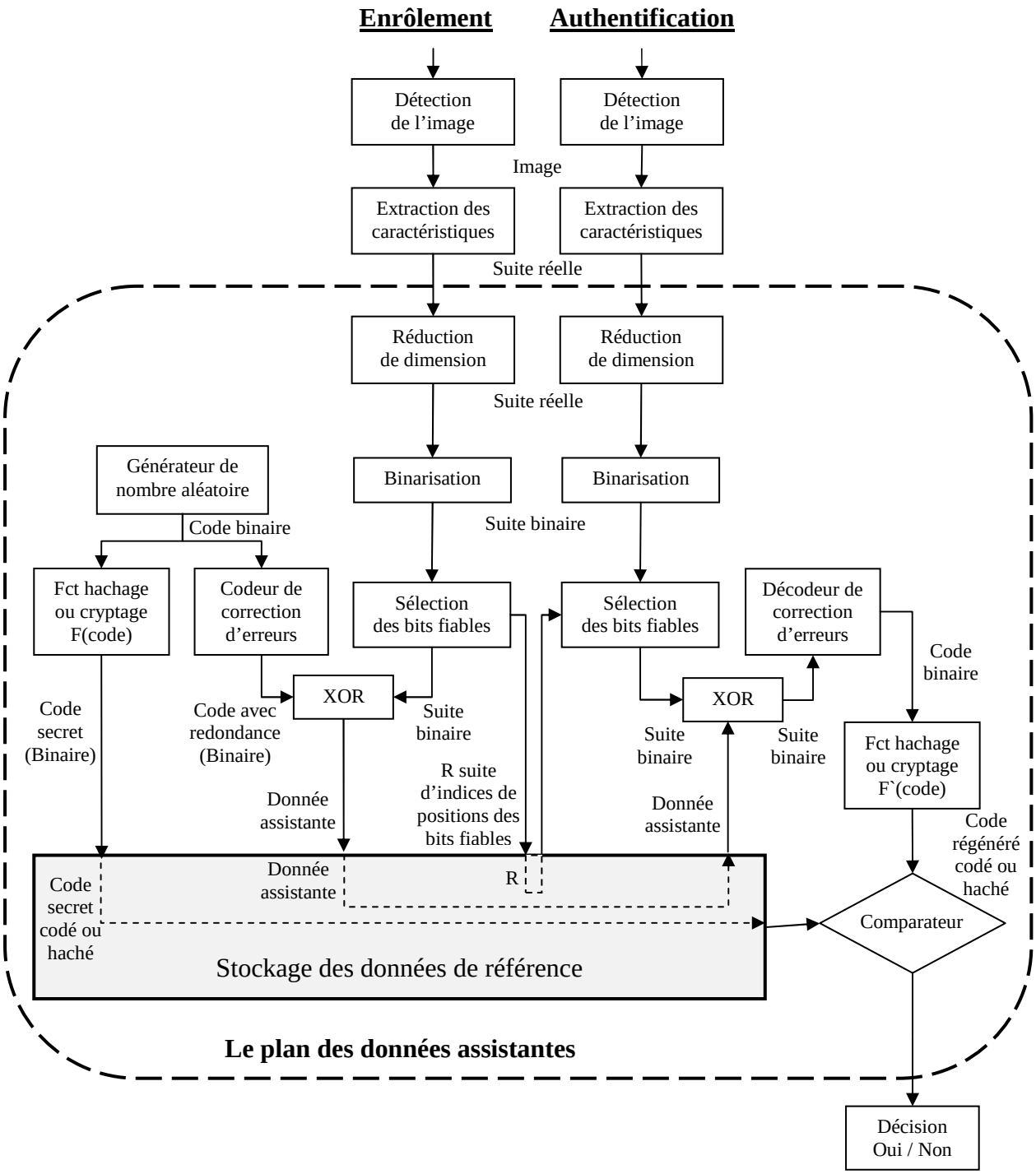


Figure 26 : Modèle de protection « le plan des donnes assistantes ».

Suite réelle : mesure, résultat de calculs.
Suite entière : pixel.

V. 1. Introduction

Le plan des données assistantes est un modèle hybride de protection (transformation, crypto-système) des informations biométriques. Ce plan permet d'extraire l'information de la modalité biométrique à partir d'une image acquise et la relier avec un code (clé) généré aléatoirement et codé par un codeur de correction d'erreurs, la donnée résultante est stockée dans la base de données du système biométrique comme des données assistantes. Ces données assistantes seront récupérées lors de la phase d'authentification et reliées avec les infos biométriques requêtes afin de régénérer le code aléatoire.

À la fin, une comparaison est effectuée entre le code aléatoire crypté ou haché et stocké dans la base avec le code régénéré afin de calculer le degré de similitude (les scores).

V. 2. Extraction de caractéristiques

(Construction des modèles biométriques réels)

L'analyse en composantes principales (PCA) est adoptée comme un extracteur de traits. Elle est une méthode de lecture non supervisée, [27]. Voir (**Annexe A**)

V. 3. Réduction de dimension

La projection dans l'espace visage par PCA permet de réduire le nombre de variables (La dimension). Voir (**Annexe A**).

V. 4. Binarisation, [28][29][26]

(Construction des modèles biométriques binaires).

$\boldsymbol{N}$: nombre d'utilisateurs.
$\boldsymbol{M}$: nombre d'images échantillons de la même modalité biométrique par utilisateur.
$\boldsymbol{X_n}$: l'ensemble des images échantillons de la même modalité biométrique de l'utilisateur $\boldsymbol{n}$.
$\boldsymbol{X_{ni}}$: l'image échantillon n° $\boldsymbol{i}$ de l'utilisateur $\boldsymbol{n}$.
$\boldsymbol{k}$: la taille des vecteurs des images échantillons.

$\forall$ L'utilisateur $\boldsymbol{n} \in \{\boldsymbol{1}, \dots, \boldsymbol{N}\}$: $\boldsymbol{X_n} = \{\boldsymbol{X_{n1}}, \boldsymbol{X_{n2}}, \dots, \boldsymbol{X_{nM}}\} \ \boldsymbol{\epsilon} \ \boldsymbol{R^k}$

$$\boldsymbol{X_n} = \begin{bmatrix} \boldsymbol{X_{n1}} & \boldsymbol{X_{n2}} & \dots & \boldsymbol{X_{nM}} \\ = & = & & = \\ \boldsymbol{x_{1,1}} & \boldsymbol{x_{1,2}} & & \boldsymbol{x_{1,M}} \\ \boldsymbol{x_{2,1}} & \boldsymbol{x_{2,2}} & & \boldsymbol{x_{2,M}} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{x_{k,1}} & \boldsymbol{x_{k,2}} & & \boldsymbol{x_{k,M}} \end{bmatrix}$$

- Moyenne de l'utilisateur $\boldsymbol{n}$: (La moyenne intra-classe)

$$\boldsymbol{moy_n = mean\ \{X_n\} = mean\{X_{n1}, X_{n2}, \dots, X_{nM}\}}$$

$$\boldsymbol{moy_n = \frac{1}{M} \sum_{i=1}^{M} X_{ni}}$$

$\boldsymbol{n \in \{1, \dots, N\}} \rightarrow$ Pour le calcul de moyennes des autres utilisateurs.

- Moyenne générale de tous les utilisateurs : (La moyenne interclasse)

$$\boldsymbol{moy = mean\{moy_n\} = mean\{moy_1, moy_2, \dots, moy_N\} \quad n \in \{1, \dots, N\}}$$

$$\boldsymbol{moy = \frac{1}{N} \sum_{n=1}^{N} moy_n}$$

- Binarisation

Pour chaque utilisateur $\boldsymbol{n}$ un vecteur binaire $\boldsymbol{B_{i,n}}$ est construit comme suivant :

$\forall$ L'utilisateur $\boldsymbol{n \in \{1, \dots, N\}}$: $$\boldsymbol{B_{i,n} = \begin{cases} 1, & moy_{i,n} > moy_{i,1} \\ 0, & moy_{i,n} \leq moy_{i,1} \end{cases} \qquad i \in \{1, 2, \dots, k\}}$$

, [28][29][26].

Remarque : On peut utiliser le médian au lieu de la moyenne, [26].
Exemple : médian {1, 2, 4, 5}= **3** → {1, 2, **3**, 4, 5}

V. 5. Sélection des bits fiables

Pour sélectionner les bits les plus fiables dans un modèle biométrique binaire. On peut suivre l'une des méthodes suivantes :

- **Méthode 1 :** [26][30]

[…] Elle est basée sur l'estimation de la probabilité d'erreur de chaque bit. Seulement les bits avec les probabilités les plus réduites sont sélectionnés. La probabilité d'erreur dépend de la distance entre $\boldsymbol{moy_n}$ et $\boldsymbol{moy}$ […].

$$\boldsymbol{P_e = \frac{|moy_n - moy|}{\sigma_n}}$$

$\boldsymbol{\sigma_n}$: la déviation standard de $\boldsymbol{X_n}$ **.**

Remarque : Dans le cas d'utilisation de la médian au lieu de la moyenne, $\boldsymbol{P_e}$ devient :

$$\boldsymbol{P_e = |moy_n - moy|}$$

, [26][30].

- **Méthode 2 :** [21][31]

Le but est de trouver quelles composantes du vecteur de trait avec les fiabilités maximales. La fiabilité $\boldsymbol{R}$ peut être aussi écris comme $(\mathbf{1} - \boldsymbol{BER})$, [21].
BER : bit error rate (Taux d'erreurs d'un bit).

$$\boldsymbol{R_n} = \frac{\mathbf{1}}{\mathbf{2}}\left(\mathbf{1} + \mathbf{fct_erreur}\left(\frac{|\boldsymbol{moy_n} - \boldsymbol{moy}|}{\sqrt{\mathbf{2}\,\boldsymbol{\sigma_n^2}}}\right)\right)$$

$\boldsymbol{\sigma_n^2}$: la variance de la moyenne de l'utilisateur $\boldsymbol{n}$.
$\mathbf{fct_erreur}$: fonction d'erreur pour chaque élément d'un vecteur réel.

, [21][31].

- **Méthode 3:** [29]

Le but est de trouver celles composantes d'un vecteur de trait avec les fiabilités maximales :

$$\boldsymbol{\sigma_n^2} = \frac{\mathbf{1}}{\boldsymbol{M-1}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} (\boldsymbol{X_{ni}} - \boldsymbol{moy_n})^{\mathbf{2}}$$

$$\boldsymbol{R_n} = \frac{\mathbf{1}}{\mathbf{2}}\left(\mathbf{1} + \mathbf{fct_erreur}\left(\frac{\boldsymbol{moy_n} - \boldsymbol{moy}}{\sqrt{\mathbf{2}\,\boldsymbol{\sigma_n^2}}}\right)\right)$$

$\boldsymbol{\sigma_n^2}$: déviation standard des images échantillons $\{\mathbf{1}, \dots, \boldsymbol{M}\}$ de l'utilisateur $\boldsymbol{n}$ (de $\boldsymbol{X_n}$).
$\mathbf{fct_erreur}$: fonction d'erreur pour chaque élément d'un vecteur réel.

, [33].

Autres formules de la déviation standard :

$$\boldsymbol{\sigma_n^2} = \left(\frac{\mathbf{1}}{\boldsymbol{M}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} (\boldsymbol{X_{ni}} - \boldsymbol{moy_n})^{\mathbf{2}}\right)^{\mathbf{1/2}}$$

$$\boldsymbol{\sigma_n^2} = \left(\frac{\mathbf{1}}{\boldsymbol{M-1}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} (\boldsymbol{X_{ni}} - \boldsymbol{moy_n})^{\mathbf{2}}\right)^{\mathbf{1/2}}$$

, [32].

V. 6. Génération du code aléatoire

À chaque image entrée un nouveau code est généré aléatoirement. D'une part, une copie de ce code est hachée et stockée dans la base de données du système. D'autre part, le code passe vers le codeur de correction d'erreurs.

Remarque :
La longueur du code généré doit être inférieure à la longueur des bits fiables choisis.

V. 7. Codage correcteur d'erreurs

Pour chaque utilisateur (image), La clé générée par le générateur de code aléatoire doit être codée par un codeur de correction d'erreurs lors de la phase d'enrôlement. Généralement un code de correction est utilisé pour vérifier la justesse de la clé (le code aléatoire) par un décodeur de correction d'erreurs lors de la phase d'authentification.

V. 7.1. Concepts

L'idée générale pour la réalisation de détection et de correction d'erreur est d'ajouter certaines redondances (des données supplémentaires) à un message, qui peuvent être utilisées pour vérifier la cohérence du message, et corriger les erreurs s'il est erroné, [1.12].

Le plan de détection et de correction des erreurs peut être systématique ou non-systématique :

- Le schéma systématique : l'émetteur envoie les données d'origine attachées avec un nombre fixe de bits de contrôle (les données de parité), qui sont dérivés plus tard à partir les bits de données par un algorithme. Le récepteur applique le même algorithme pour les bits de données reçues et compare leurs valeurs avec les bits de contrôle reçues, s'ils sont égaux le message reçu est correct, [1.12].

- Le schéma non-systématique : le message d'origine est transformé en un message codé qui a au moins autant de bits que le message d'origine, [1.12].

V. 7.2. Implémentation

La correction des erreurs peut être généralement réalisée en :

- Requête Automatique de répétition (RAR) : Chaque bloc de données reçues est vérifié à l'aide du code de détection d'erreurs utilisé, et si la vérification échoue, la retransmission des données sera demandée jusqu'à ce que les données puissent être vérifiées, [1.12].

- Code de Correction d'Erreurs (CCE) : l'émetteur code les données en utilisant un code correcteur par l'ajout de la redondance aux niveaux du message. Les données reçues après la transmission sont vérifiées par un décodeur de correction d'erreurs (recalcule des bits de contrôle). Si les bits de contrôle calculés et reçus sont égaux, donc le message reçus est correct, [1.12].

- Hybride (RAR et CCE): RAR et CCE peuvent être combinés, tels que des erreurs mineures sont corrigées par le correcteur d'erreurs, et les erreurs majeures sont corrigées par une demande de retransmission, [1.12].

Remarque : dans le cas en cours d'étude « le Plan des Données Assistantes », il n'est pas possible de garder ni l'information biométrique originale ni le code aléatoire original, mais on enregistre le code redondant lié avec les données biométriques originales pour qu'il soit possible de vérifier la justesse de la clé après la régénération durant la phase d'authentification. C'est pourquoi qu'on s'intéresse par le codage de correction d'erreurs.

V. 7.3. Redondance et fiabilité

Durant l'étape de récupération des informations à partir d'un support de stockage ou par calcul, s'il y a un changement de bits (modification) donc l'information qui sera obtenue est évidement erronée. Pour cette raison, il faut ajouter quelques informations additives « Les redondances » ou bien « Le code correcteur d'erreur », ce dernier permet à analyser et à corriger l'erreur au niveau de l'information récupérée.

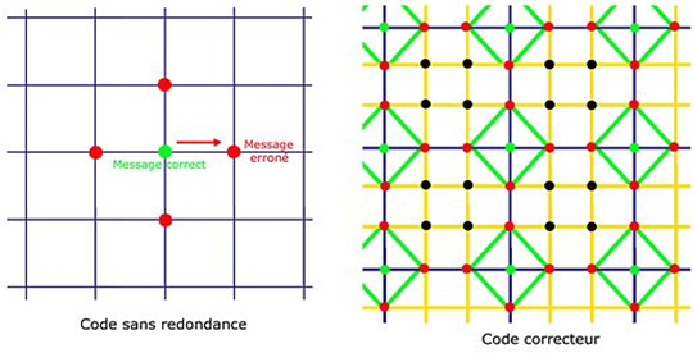


Figure 27 : Redondance et fiabilité, [-27-].

V. 7.4. Code correcteur d'erreurs

Un code correcteur d'erreurs (CCE) est un système d'ajout de données redondantes, (des données de parité) à un message, de telle sorte qu'il peut être récupéré par un récepteur, même si un certain nombre d'erreurs (jusqu'à la capacité du code utilisé) ont été introduits, pendant la transmission ou le stockage. Les codes correcteurs d'erreurs sont fréquemment utilisés dans les liaisons de communication, ainsi que pour le stockage fiable dans les médias tels que CD, DVD, disques durs ROM et mémoire RAM, [1.12].

Voici quelques différents types de codes correcteurs, [1.12] :

- Code de Répétition
- Code de Somme
- Code de Hamming
- Code de Golay
- Code de Reed-Müller
- Code de Reed-Solomon

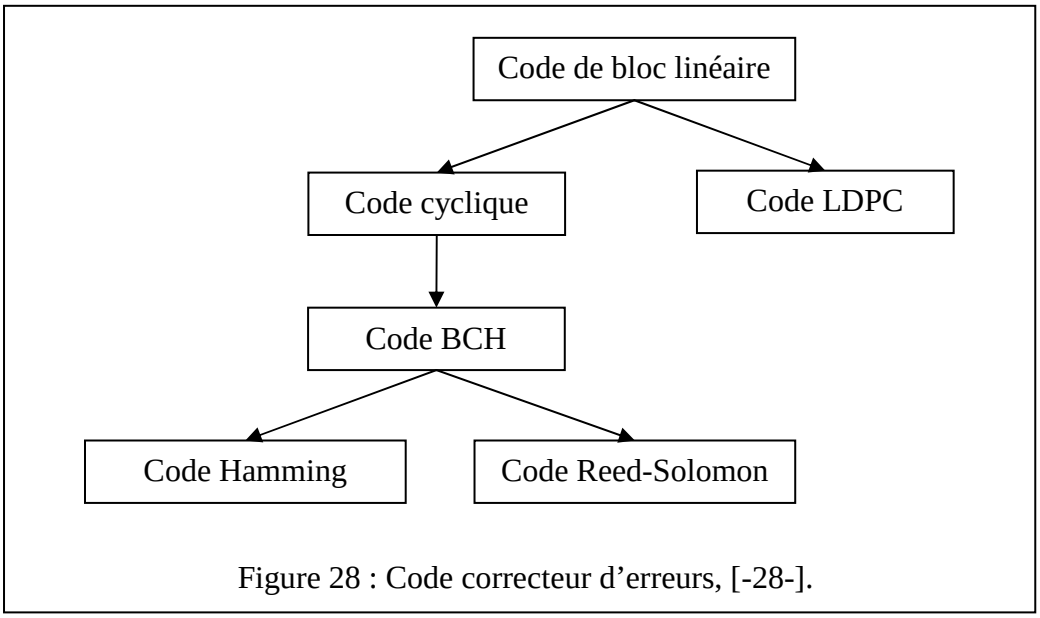


Figure 28 : Code correcteur d'erreurs, [-28-].

V. 7.5. Quelques codes correcteurs

Parmi les codes correcteurs les plus simples et les plus utilisés, on mentionne : Code de répétition, Code de sommes de contrôle, Code de Reed Solomon, etc.

V. 7.5.1. Code de répétition [1.13]

Le code de répétition permet de répéter chaque bloc de taille $\boldsymbol{m}$ bits situé au niveau d'un message de taille $\boldsymbol{n}$ bits, et $\boldsymbol{n \geq m}$, trois fois successivement pour former un message de taille $\boldsymbol{n \times m}$:

Bloc **1**	Bloc **2**	…	…	Bloc ($\boldsymbol{^n/_m}$)
Bit (**1**) … bit (**m**)	Bit ($\boldsymbol{m+1}$) … bit ($\boldsymbol{2 \times m}$)	…	…	Bit ($\boldsymbol{2 \times m}$) + **1**… bit (**n**)

Bloc **1**	Bloc **1**	Bloc **1**	Bloc **2**	Bloc **2**	Bloc **2**	…	Bloc ($\boldsymbol{^n/_m}$)	Bloc ($\boldsymbol{^n/_m}$)	Bloc ($\boldsymbol{^n/_m}$)

- **Algorithme du code de répétition**
  (On considère que les tableaux contiennent des valeurs binaires)

$\boldsymbol{Data}$: $tableau$ [1 … n] ;
$\boldsymbol{Bloc}$: $tableau$ [1 … m] ;
$\boldsymbol{newData}$: $tableau$ [1 … $n \times m$] ;
$Lire\ ou\ importer\ \boldsymbol{Data}$;
$Pour\ \boldsymbol{i = 1}$ à $\boldsymbol{n}, pas\ d'incrément\ \boldsymbol{m}$;
    $\boldsymbol{Bloc} \leftarrow prendre\ \boldsymbol{m}\ elts$ à $partir\ \boldsymbol{Data}$; $//pos\ 1er\ elts = i$
    $\boldsymbol{newData} \leftarrow concatener\ (\boldsymbol{newData}, concatener\ (\boldsymbol{bloc}, \boldsymbol{bloc}, \boldsymbol{bloc}))$;
$Fin\ Pour$;

- **Exemple d'un code de répétition :** [1.13]

Taille du bloc	Data	Ajout de redondance
1 bit	0	000
1 bit	1	111
2 bits	01	01 01 01
3 bits	101	101 101 101

Ce code correcteur possède : l'avantage de non seulement détecter une erreur, mais aussi de permettre une correction automatique, et l'inconvénient est que sa dimension est élevée par rapport à la longueur du message originale, [1.13].

V. 7.5.2. Code de Sommes De Contrôle

La somme de contrôle est une méthode basée sur la somme des bits de chaque bloc de taille $\boldsymbol{m}$ bits situés successivement au niveau d'un message de taille $\boldsymbol{n}$ bits, et $\boldsymbol{n} \geq \boldsymbol{m}$. Elle permet d'ajouter le bit $\mathbf{0}$ après $\boldsymbol{m}$ bits de chaque bloc si la somme est pair et le bit **1** sinon, [1.13].

- **Algorithme du code Somme De Contrôle**
  (On considère que les tableaux contiennent des valeurs binaires)

$\boldsymbol{Data}$: $tableau\ [1 \ldots n]$;
$\boldsymbol{Bloc}$: $tableau\ [1 \ldots m]$;
$\boldsymbol{newData}$: $tableau\ [1 \ldots n \times m]$;

$Lire\ ou\ importer\ \boldsymbol{Data}$;
$Pour\ \boldsymbol{i} = \mathbf{1}$ à $\boldsymbol{n}, pas\ d'incrément\ \boldsymbol{m}$;
    $\boldsymbol{Bloc} \leftarrow prendre\ \boldsymbol{m}\ elts$ à $partir\ \boldsymbol{Data}$; $//pos\ 1er\ elts = i$
    $Si\ somme\ des\ elts\ de\ (\boldsymbol{bloc})\ est\ pair$
        $\boldsymbol{newData} \leftarrow concatener\ (\boldsymbol{newData}, concatener\ (\boldsymbol{bloc}, \mathbf{0}))$;
    $Sinon$
        $\boldsymbol{newData} \leftarrow concatener\ (\boldsymbol{newData}, concatener\ (\boldsymbol{bloc}, \mathbf{1}))$;
    $Fin\ si$;
$Fin\ Pour$;

- **Exemple du code de Somme De Contrôle**

Taille du bloc	Data	Somme des bits de data	Ajout de redondance
2 bit	00	Pair	00**0**
2 bit	01	Impair	01**1**
2 bit	11	Pair	11**0**
3 bits	110	Paire	110**0**
4 bits	1011	Impair	1011**1**

V. 7.5.3. Code de Reed Solomon

Un code de Reed Solomon est noté par : $\boldsymbol{RS}\ (\boldsymbol{n}, \boldsymbol{k})$

- $\boldsymbol{n}$: le nombre de symboles transmis.
- $\boldsymbol{k}$: le nombre symboles de l'information.
- $\boldsymbol{m}$: le nombre de bits par symboles.

, [1.14].

- **Exemple d'un code de Reed-Solomon**

$\boldsymbol{N = 5}$; $\boldsymbol{k = 3}$; $\boldsymbol{m = 8}$;

<u>Cas 1</u> : calcul en décimal, [1.14].

1°) On considère un bloc de 3 nombres à transmettre :

$$02\ 09\ 12\ /_{(base\ 10)}$$

2°) On ajoute deux nombres de redondance.

- Le premier est la somme des 3 nombres (La somme simple transmise) :

$$(02 + 09 + 12)\ /_{base\ 10} = 23\ /_{base\ 10}$$

- Le second est la somme pondérée des 3 nombres, (La somme pondérée transmise) :

$$(02 \times 1) + (09 \times 2) + (12 \times 3)\ /_{base\ 10} = 56\ /_{base\ 10}$$

3°) À la sortie du codeur, le bloc à transmettre est :

$$02\ 09\ 12\ 23\ 56/_{(base\ 10)}$$

4°) Suite à une perturbation, le récepteur reçoit :

$$02\ \mathbf{13}\ 12\ 23\ 56/_{(base\ 10)}$$

5°) À partir des données reçues, le décodeur calcule :

- La somme simple reçue :

$$(02 + 13 + 12)\ /_{base\ 10} = 27\ /_{base\ 10}$$

- La somme pondérée reçue :

$$(02 \times 1) + (\mathbf{13} \times 2) + (12 \times 3)\ /_{base\ 10} = 64\ /_{base\ 10}$$

6°) Valeur de l'erreur :

$$\boldsymbol{Valeur_erreur = la\ somme\ simple\ reçue - Somme\ simple\ envoyee}$$

$$Valeur\ de\ l'erreur = (27 - 23)\ /_{base\ 10} = 4\ /_{base\ 10}$$

7°) La position de l'erreur :

$$\boldsymbol{Pos_erreur = (Som\ ponderee\ reçue - Som\ ponderee\ transmise)/valeur\ d'erreur}$$

$$Position\ de\ l'erreur = \frac{(64 - 56)}{4}\ /_{base\ 10} = 2\ /_{base\ 10}$$

8°) Code correcte :

$$\boldsymbol{Valeur\ correcte = valeur\ reçu\ du\ rang\ «\ position\ d'erreur\ »\ -\ «\ valeur\ d'erreur\ »}$$

$$Valeur\ correcte = (13 - 04)\ /_{base\ 10} = 9\ /_{base\ 10}$$

9°) L'information originale est :

$$02\ \mathbf{09}\ 12\ /_{(base\ 10)}$$

, [1.14].

<u>Cas 2</u> : calcul en binaire

1°) On considère un bloc de 3 nombres à transmettre :

$$0000\ 0010, 0000\ 1001, 0000\ 1100\ /_{(base\ 2)} = 02\ 09\ 12\ /_{(base\ 10)}$$

2°) On ajoute deux nombres de redondance.

- Le premier est la somme des 3 nombres (la somme simple transmise):

$$(0000\ 0010 + 0000\ 1001 + 0000\ 1100)/_{(base\ 2)} = 0001\ 0111/_{\text{base2}}$$

$$23/_{(base\ 10)} = 0001\ 0111\ /_{(base\ 2)}$$

- Le second est la somme pondérée des 3 nombres (La somme pondérée transmise)

$$(0000\ 0010 \times 1) + (0000\ 1001 \times 10) + (0000\ 1100 \times 11)/_{(base\ 2)} = 0011\ 1000/_{\text{base2}}$$

$$56/_{(base\ 10)} = 0011\ 1000\ /_{(base\ 2)}$$

3°) À la sortie du codeur, le bloc à transmettre est :

$$0000\ 0010, 0000\ 1001, 0000\ 1100, 0001\ 0111, 0011\ 1000/_{(base\ 2)} = 02\ 09\ 12\ 23\ 56/_{(base\ 10)}$$

4°) Suite à une perturbation, le récepteur reçoit :

$$0000\ 0010, 0000\ 1\mathbf{1}01, 0000\ 1100, 0001\ 0111, 0011\ 1000/_{(base\ 2)} = 02\ \mathbf{13}\ 12\ 23\ 56/_{(base\ 10)}$$

5°) À partir des données reçues, le décodeur calcule :

- La somme simple reçue :

$$(0000\ 0010 + 0000\ 1\mathbf{1}01 + 0000\ 1100\ )/_{(base\ 2)} = 0001\ 1011/_{\text{base2}}$$

$$0001\ 1011/_{\text{base2}} = 27\ /_{base\ 10}$$

- La somme pondérée reçue :

$$(0000\ 0010 \times 1) + (0000\ 1\mathbf{1}01 \times 10) + (\ 0000\ 1100 \times\ 11)/_{(base\ 2)} = 0100\ 0000/_{\text{base2}}$$

$$0100\ 0000/_{\text{base2}} = 64\ /_{base\ 10}$$

6°) Valeur de l'erreur :

$$\boldsymbol{Valeur_erreurs\ =\ la\ somme\ simple\ reçue\ -\ Somme\ simple\ transmise}$$

$$Valeur\ de\ l'erreur = 0001\ 1011 - 0001\ 0111\ /_{\text{base2}} = 0000\ 0100/_{\text{base2}} = 4\ /_{base\ 10}$$

7°) La position de l'erreur :

$$\boldsymbol{Pos_erreur\ =\ (Som\ pondérée\ reçue\ -\ Som\ pondérée\ transmise)/valeur\ d'erreur}$$

$$Position\ de\ l'erreur\ = \frac{0100\ 0000 - 0011\ 1000}{0000\ 0100}\ /_{\text{base2}} = 0000\ 0010/_{\text{base2}} = 2\ /_{base\ 10}$$

8°) Code correcte :

$$\boldsymbol{Valeur\ correcte\ =\ valeur\ reçu\ du\ rang\ «\ position\ d'erreur\ »\ -\ «\ valeur\ d'erreur\ »}$$

$$Valeur\ correcte = 0000\ 1101 - 0000\ 0100\ /_{\text{base2}} = 0000\ 1001/_{\text{base2}} = 9\ /_{base\ 10}$$

9°) L'information originale est :

$$0000\ 0010, \mathbf{0000\ 1001}, 0000\ 1100\ /_{(base\ 2)} = 02\ \mathbf{09}\ 12\ /_{(base\ 10)}$$

V. 8. Codage ou hachage de la clé aléatoire

Pour chaque code aléatoire généré, une copie de ce dernier doit être codée ou hachée afin de la stocker dans la base du système biométrique sous une forme sécurisée.

V. 9. XOR

Une opération logique est appliquée entre le vecteur binaire des bits fiables sélectionnés et le code binaire aléatoire généré, [26].

V. 10. Stockage

Après la réalisation des étapes précédentes, une base de données est formée contenant les informations nécessaires pour les calculs des informations d'authentifications, [30].

V. 11. Conclusion

Les étapes attachées d'un plan de données assistantes permet de transformer l'information biométrique originale en une autre information de valeurs binaire, et la relier avec une clé aléatoire, ce qui offre un niveau de sécurité plus élevé pour ces données secrètes.

Mais, cette méthode protective a posé d'autres problèmes comme : l'augmentation du taux de faux rejet et le taux de fausse acceptation à cause des variations intra-classe de l'utilisateur du système biométrique. Ces variations intra-classe ne sont pas accepter par le modèle de protection, même l'utilisation d'un codeur de correction d'erreurs ne supprime pas toutes les erreurs appartenant à cette information biométrique.

Chapitre VI :

Implémentation Et Résultats

Système de reconnaissance des visages par :
Base des visages ORL.
Traitement d'images par ACP.
Protection par le Plan des données assistantes.
Cryptage par AES.

VI. 1. Introduction

Tous les concepts et les principes étudiés en avance dans les chapitres : la biométrie, les systèmes biométriques, la reconnaissance faciale, les modèles de protection de l'information biométrique et le Plan Des Données Assistantes, sont employés pour réaliser un système de reconnaissance de visage en deux dimensions. L'innovation ou bien le développement ajouté à ce système est l'utilisation de la base des visages ORL comme source d'image, la méthode de traitement d'images ACP pour l'extraction du contenu des images et dernièrement la méthode de codage CSA pour chiffrer les clés aléatoires de liaison. Les résultats des tests du système seront mentionnés ultérieurement.

VI. 2. Concepts et définitions (ORL, ACP, CSA)

On définie les méthodes appliquées dans le système de reconnaissance réalisé qu'elles sont :

- La base des visages ORL.
- L'Analyse En Composantes Principales ACP.
- Le Chiffrement Standard Avancé CSA.

VI. 2.1. Base des visages ORL

Le répertoire de la base des visages $\boldsymbol{ORL}$ contient un ensemble des images visages prise entre Avril 1992 et Avril 1994 dans le laboratoire de recherche Olivetti.

La base regroupe $\mathbf{40}$ répertoires nommés $\boldsymbol{Sx}$ et $\boldsymbol{x} \boldsymbol{\epsilon} \{\mathbf{1}, \mathbf{2}, \dots, \mathbf{40}\}$, dont chacun contient $\mathbf{10}$ différentes images nommées $\boldsymbol{y}$ et $\boldsymbol{y} \boldsymbol{\epsilon} \{\mathbf{1}, \mathbf{2}, \dots, \mathbf{10}\}$ du visage de la même personne. Les images sont en format $\boldsymbol{PGM}$ et en taille ($\mathbf{92} \times \mathbf{112}$). Elles sont prises devant un arrière-plan homogène et en position frontale.

Les différences entre les images du même répertoire (même personne) sont :
- Variation de l'intensité lumineuse.
- Variation des expressions faciales (yeux fermées/ouvertes, …).
- Variation des détails du visage (avec lunette/sans lunette, …).
- Variation de la position du visage et sa taille dans l'image.

VI. 2.2. Analyse En Composantes Principales ACP

L'Analyse En Composantes Principales ACP est une méthode de calcul, qui se base sur le calcul des valeurs et vecteurs propres et la projection dans l'espace visage. Elle permet d'extraire le contenu d'une image et de reconstruire cette dernière à partir de ces données extraites. (Voir l'**Annexe A**).

VI. 2.3. Chiffrement Standard Avancé CSA

Le Chiffrement Standard Avancé CSA (En, Advanced Encryption Standard AES) est un algorithme de chiffrement symétrique (Une seule clé est utilisée pour le codage et le décodage). (Voir l'**Annexe B**)

VI. 3. Description de l'étude réalisée (réalisation théorique)

Le système de reconnaissance de visage réalisé fonctionne en deux phases essentielles : l'enrôlement et l'authentification, selon le mode vérification (comparaison un à un), c'est-à-dire : comparaison des informations de test courantes avec seulement les informations correspondantes dans la base de données du système biométrique. Il est protégé par le plan des données assistantes (Modèle hybride : transformé/crypté) et utilise la base des visages ORL comme source d'images pour construire la base de données de référence des personnes connues par le système.

Le schéma suivant représente le plan général du système réalisé :

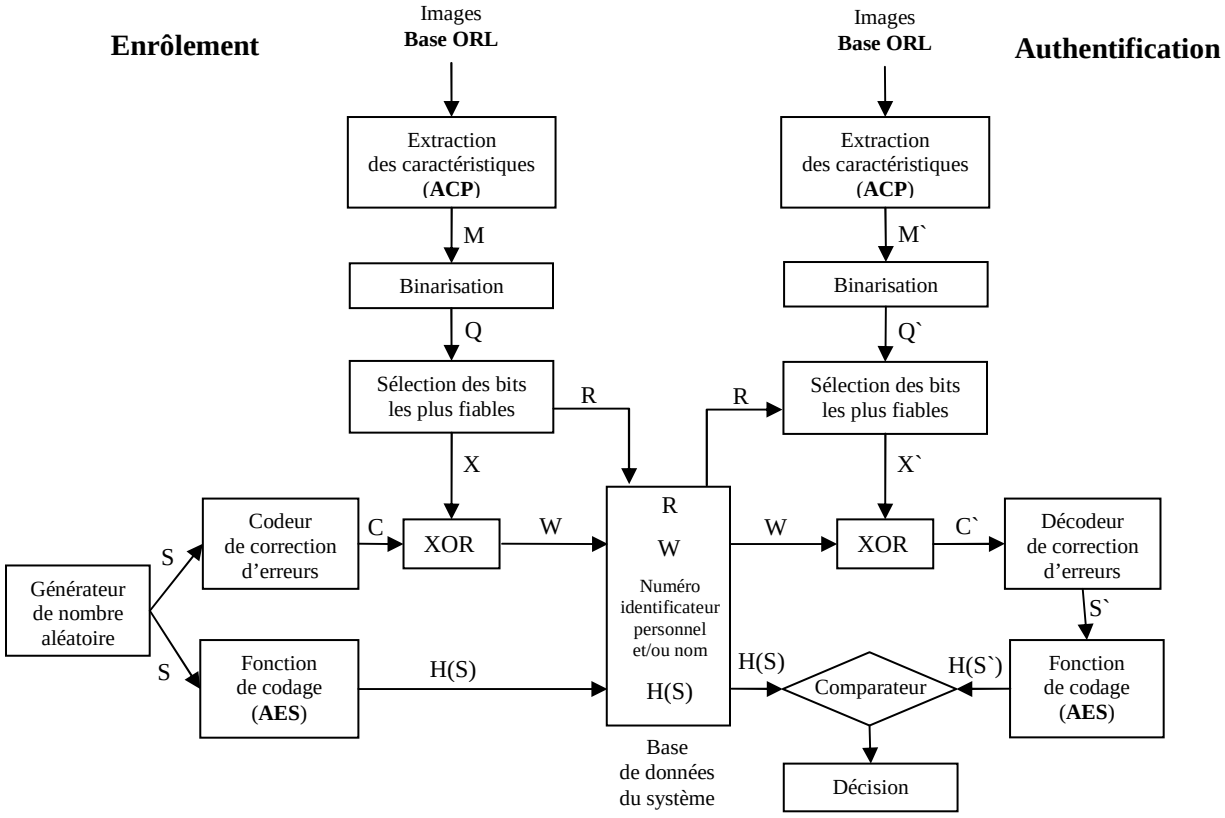


Figure 29 : Système De Reconnaissance De Visages, (HDS, AES, ORL).

Lors de la phase d'enrôlement, une image est chargée à partir de la base ORL à chaque enregistrement d'une personne, cette étape est appelée « l'acquisition de l'image ». Ensuite, l'image acquise doit passer par l'étape de prétraitement et l'étape de détection de visage. L'avantage de l'utilisation de la base ORL apparaître ici car les images sont prétraitées et la taille est ajustée d'origine. Donc, ces étapes sont annulées. Après le chargement de toutes les images des personnes qui doivent être considérées comme connues, on passe à l'étape d'extraction des caractéristiques. On utilise la méthode l'Analyse En Composantes Principales ACP pour extraire l'information contenue dans ces images par les lois des valeurs et vecteurs propres, en passant par l'espace visage et la projection dans l'espace visage on obtient les caractéristiques des personnes sous forme numérique. Cette information réduite est appelée « La Composante Principale ».

L'étape suivante est la transformation en binaire des valeurs réelles calculées des caractéristiques (Les Composantes Principales). Après la Binarisation, on sélectionne seulement les bits les plus significatifs (fiables) en utilisant une fonction de calcul de fiabilité. Les positions de ces bits fiables sont enregistrées dans la base de données du système biométrique afin de les réutiliser lors de la phase d'authentification. Au même temps, une clé aléatoire est générée par le générateur de code aléatoire, et codée par le codeur de correction d'erreurs qui permet de recopier chaque bit binaire de la clé deux (2) ou trois (3) fois (2 ou 3 bits de redondance selon le test réalisé) pour former une nouvelle clé binaire plus longue que l'originale. La suite binaire obtenue après la sélection est liée avec la clé aléatoire générée et codée par le codeur de correction d'erreurs pour obtenir une information sécurisée appelée « la donnée assistante » qui doit être stockée aussi dans la base de données du système biométrique avec une copie de la clé codée par le Chiffrement Standard Avancé CSA. Donc, le système à un nombre précise d'utilisateurs autorisés qui peuvent l'utiliser et acceptés par ce dernier.

La deuxième phase est l'authentification. À chaque test de reconnaissance durant l'étape d'acquisition de l'image, on charge une image aléatoire ou précise à partir de la base ORL. Les étapes de prétraitement et de détection de visage sont annulées. Pour extraire le contenu de l'image on utilise aussi la méthode de l'Analyse En Composantes Principales ACP. Et après la Binarisation, les bits les plus fiables doivent être sélectionnés à l'aide du vecteur des positions correspondant stocké dans la base de données du système biométrique durant la phase d'enrôlement. Le système charge la donnée assistante correspondante aussi à partir de la base de données et la relie (XOR) avec les bits les plus fiables sélectionnés, le résultat obtenue est la clé aléatoire codée par le codeur de correction d'erreurs (Mais avec certains erreurs). Pour récupérer les bits originaux de la clé, on utilise un décodeur de correction d'erreurs qui élimine les bits de redondance ajoutés et corrige les bits erronés. L'étape l'avant dernière est le codage de la clé régénérée par le Chiffrement Standard Avancé CSA. La dernière étape est la comparaison entre la clé obtenue (régénérée) et la clé stockée correspondante dans la base de données, si elles sont identiques donc l'image de test est connue sinon elle est inconnue.

Remarque 1:

2 bits de redondance : chaque bit est représenté par 3 bits (1 original et 2 copies).
3 bits de redondance : chaque bit est représenté par 4 bits (1 original et 3 copies).

Remarque 2:

La longueur (le nombre de bits) de la clé aléatoire générée, le nombre de bits de redondance à ajouter sont fixées par le programmeur selon les calculs et les remarques obtenues à chaque étape.

VI. 4. Implémentation (Réalisation logicielle -Matlab-)

L'implémentation est réalisée en deux phases : l'enrôlement et l'authentification.

VI. 4.1. Phase d'enrôlement

```
%=========================================================================
%=========================================================================
%             Réalisation d'un "Plan des Données Assistantes"
%                       (La phase d'enrôlement)
%=========================================================================
%=========================================================================
%                     1.Extraction des caractéristiques
%=========================================================================
% Les étapes d'un algorithme "Analyse en Composantes Principales, ACP"
%=========================================================================
% 1.1.    Lecture des images et construction d'une base de données
% 1.2.    Calcul de l'image moyenne
% 1.3.    Calcul de l'image différence
% 1.4.    Valeurs propres et vecteurs propres de la matrice A'A
% 1.5.    Valeurs et vecteurs propres de la matrice de covariance C=AA'
% 1.6.    //
% 1.7.    //
% 1.8.    L'espace visage
% 1.9.    La projection
%=========================================================================
%                      2. Le Plan des Données Assistantes
%=========================================================================
% Plan des données assistantes (En, Helper Data Scheme "HDS")
%=========================================================================
% 2.1.    Importation des informations
% 2.2.    //
% 2.3.    Binarisation
% 2.4.    Sélection des bits les plus fiables (En, reliable bits)
% 2.5.    Génération de code aléatoire
% 2.6.    Codage correcteur d'erreurs
% 2.7.    XOR (Code secret et les bits fiables)
% 2.8.    Cryptage ou Hachage des codes aléatoires
%=========================================================================
%                    3. Cryptage des codes par "AES"
%=========================================================================
% Les étapes d'un algorithme de codage "Advanced Encryption Standard, AES"
%=========================================================================
% 3.1.    Importation des informations nécessaires pour le codage
% 3.2.    Génération de la table "State"
% 3.3.    Initialisation de la clé
% 3.4.    XOR entre "State" initiale et la clé initiale "Cle"
% 3.5.    Expansion de la clé-AES-128 bits
% 3.6.    Substitution
% 3.7.    Rotation des lignes à gauche
% 3.8.    Mélange des colonnes indépendamment
% 3.9.    Ajout de la clé du tour
%=========================================================================
%                    4. Construction de la base des données
%=========================================================================
% Sauvegarde des informations nécessaires
%=========================================================================
% 4.1.    Base de données globale
% 4.2.    Base de données partielle
%=========================================================================
```

```
%========================================================================
%                        Références et bibliographie
%========================================================================
% Réalisation d'un "Plan des Données Assistantes" (La phase d'enrôlement)
%========================================================================
%========================================================================
% 1.   PCA
%========================================================================
% S. Mohamed (2009)
% Biometric Face recognition (PCA)
%------------------------------------------------------------------------
% Face recognition by Santiago Serrano (PCA)
% (Normalization Eigen-vector)
%------------------------------------------------------------------------
% TP Initiation au traitement d'image sous MATLAB
%------------------------------------------------------------------------
% Pradeep Buddharaju
% Face Recognition using PCA (Eigenfaces) and LDA (Fisherfaces)
%------------------------------------------------------------------------
% Face database ORL: att_faces(92×112)
% http://www.cad.zju.edu.cn/home/dengcai/Data/ORL/images.html
% http://www.uk.research.att.com/facedatabase.html
%========================================================================
%========================================================================
% 2.   Le Plan des Données Assistantes
%========================================================================
% Xuebing Zhou, Arjan Kuijper and Christoph Busch (2010)
% Template Protection For 3D Face Recognition,
% Face Recognition, Milos Oravec (Ed.), ISBN: 978-953-307-060-5, InTech,
% Available from:  http://www.intechopen.com/books/face-recognition/
%                        /template-protection-for-3d-face-recognition
%------------------------------------------------------------------------
% Xuebing Zhou
% Template Protection and its Implementation in 3D Face Recognition Systems
% Germany
%------------------------------------------------------------------------
% Daniel Hartung (2007)
% Template Protection for PCA-LDA-based 3D Face Recognition System
%========================================================================
%========================================================================
% 3.   Cryptage par "AES, Advanced Encryption Standard"
%========================================================================
% ADVANCED ENCRYPTION STANDARD (AES)
% Federal Information, Processing Standards Publication 197 (fips-197)
% November 26, 2001
% http://csrc.nist.gov/publications/
%------------------------------------------------------------------------
% Advanced Encryption Standard
% http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
%------------------------------------------------------------------------
% Kit Choy Xintong
% Understanding AES Mix-Columns Transformation Calculation
%========================================================================
```

VI. 4.1.1. Cas 1 : seul individu, plusieurs images échantillons par individu

Exemple : (Le premier individu de la base ORL)

Dans les figures suivantes, un exemple d'enrôlement d'une seule personne avec quatre (4) images échantillons de la même personne et trois (3) bits de redondance.

```
Entrez le nombre de personnes à stocker dans la base des visages ( <= 40 ) : 1

Entrez le nombre des images échantillons par personne ( <=10 ) : 4

Remarque:  "indice première image + nombre personnes <= 40"
Entrez l'indice de la première image  : 1
```

Figure 30 : Exemple de paramètres du test (Cas1).

- **L'ensemble des visages d'apprentissage (à sauvegarder)**



Figure 31 : Exemple de visages d'apprentissage (Cas1).

- **Les clés après le codage**

```
7E5225E3
5933A535
3796ADCB
9B9D2C3E
```

VI. 4.1.2. Cas 2 : plusieurs individus, une seule image échantillon par individu

Exemple : (Les 08 premiers individus de la base ORL)

Dans les figures suivantes, un exemple d'enrôlement de plusieurs personnes avec une seule (1) image échantillon pour chaque personne et deux (2) bits de redondance.

```
Entrez le nombre de personnes à stocker dans la base des visages ( <= 40 ) : 8

Entrez le nombre des images échantillons par personne ( <=10 ) : 1

Remarque:  "indice première image + nombre personnes <= 40"
Entrez l'indice de la première image  : 1
```

Figure 32 : Exemple de paramètres du test (Cas2).

- **L'ensemble des visages d'apprentissage (à sauvegarder)**



Figure 33 : Exemple de visages d'apprentissage (Cas2).

- **Les clés après le codage**

2E6882C72E6882C7**C2B5C729**C91A36A0**C91A36A0**7E5225E3**4C0943C3**C2B5C729
F983C276F983C276**4B6087E7**36C016B2**36C016B2**5933A535**5AE3573F**4B6087E7
5BEFDE3A5BEFDE3A**FECEE916**B3019E02**B3019E02**3796ADCB**8BC33D83**FECEE916
D9666624D9666624**A946ED0F**35F7B1C0**35F7B1C0**9B9D2C3E**BF8C56A9**A946ED0F

VI. 4.1.3. Cas 3 : plusieurs individus, plusieurs images échantillons par individu

Exemple : (Les 04 premiers individus de la base ORL)

Dans les figures suivantes, un exemple d'enrôlement de plusieurs personnes avec plusieurs images échantillons pour chaque personne et trois (3) bits de redondance.

```
Entrez le nombre de personnes à stocker dans la base des visages ( <= 40 ) : 4

Entrez le nombre des images échantillons par personne ( <=10 ) : 4

Remarque:  "indice première image + nombre personnes <= 40"
Entrez l'indice de la première image  : 1
```

Figure 34 : Exemple de paramètres du test (Cas3).

- **L'ensemble des visages d'apprentissage (à sauvegarder)**



Figure 35 : Exemple de visages d'apprentissage (Cas3).

- **Les clés après le codage**

FBC190B15D0F5B3E**39112914**E5B28D4A
CCDEA98A15060B17**6A7C1ECA**B1DB9043
CF5FC1DB391101AF**36EEBC88**37FA3D0B
9DE1C257A65CF0D6**7909FB74**6FFED102

VI. 4.2. La phase d'authentification

```
%=========================================================================
%=========================================================================
%            Réalisation d'un "Plan des Données Assistantes"
%                    (La phase d'authentification)
%=========================================================================
%=========================================================================

%=========================================================================
%                      1.Extraction des caractéristiques
%=========================================================================
% Les étapes d'un algorithme "Analyse en Composantes Principales, ACP"
%=========================================================================
% 1.1.    Importation de la base des données
% 1.2.    Lecture de l'image de test
% 1.3.    //
% 1.4.    Projection de l'image de test dans l'espace
%=========================================================================
%                      2. Le Plan des Données Assistantes
%=========================================================================
% Plan des données assistantes (En, Helper Data Scheme "HDS")
%=========================================================================
% 2.1.    Binarisation
% 2.2.    La sélection des bits et valeurs fiables de l'image de test
% 2.3.    Extraction du code utilisé pour coder l'image original
% 2.4.    Décodeur de correction d'erreur
%=========================================================================
%                     3. Cryptage des codes par "AES"
%=========================================================================
% Les étapes d'un algorithme de codage "Advanced Encryption Standard, AES"
%=========================================================================
% 3.1.    Importation des informations nécessaires pour le codage
% 3.2.    Génération de la table "State"
% 3.3.    Initialisation de la clé
% 3.4.    XOR entre "State" initiale et la clé initiale "Cle"
% 3.5.    Expansion de la clé-AES-128 bits
% 3.6.    Substitution
% 3.7.    Rotation des lignes à gauche
% 3.8.    Mélange des colonnes indépendamment
% 3.9.    Ajout de la clé du tour
%=========================================================================
%                     4. Authentification
%=========================================================================
% 4.1.    Comparaison entre "code enregistré" et "Code Extrait"
%=========================================================================
```

```
%=========================================================================
%                          Références et bibliographie
%=========================================================================
%            Réalisation d'un "Plan des Données Assistantes"
%                    (La phase d'authentification)
%=========================================================================
%=========================================================================
% 1.   PCA
%=========================================================================
% S. Mohamed (2009)
% Biometric Face Recognition Based ORL DATA_BASES (PCA)
%-------------------------------------------------------------------------
% Face recognition by santiago Serrano (PCA)
% (Normalization Eigen-vector)
%-------------------------------------------------------------------------
% TP Initiation au traitement d'image sous MATLAB
%-------------------------------------------------------------------------
% Pradeep Buddharaju
% Face Recognition using PCA (Eigenfaces) and LDA (Fisherfaces)
%-------------------------------------------------------------------------
% Face database ORL: att_faces(92×112)
% http://www.cad.zju.edu.cn/home/dengcai/Data/ORL/images.html
% http://www.uk.research.att.com/facedatabase.html
%=========================================================================
%=========================================================================
% 2.   Le Plan des Données Assistantes
%=========================================================================
% Xuebing Zhou, Arjan Kuijper and Christoph Busch (2010)
% Template Protection For 3D Face Recognition,
% Face Recognition, Milos Oravec (Ed.), ISBN: 978-953-307-060-5, InTech,
% Available from: http://www.intechopen.com/books/face-recognition/
%                       /template-protection-for-3d-face-recognition
%-------------------------------------------------------------------------
% Xuebing Zhou
% Template Protection and its Implementation in 3D Face Recognition Systems
% Germany
%=========================================================================
%=========================================================================
% 3.   Cryptage par "AES, Advanced Encryption Standard"
%=========================================================================
% ADVANCED ENCRYPTION STANDARD (AES)
% Federal Information,Processing Standards Publication 197 (fips-197)
% November 26, 2001
% http://csrc.nist.gov/publications/
%-------------------------------------------------------------------------
% Advanced Encryption Standard
% http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
%-------------------------------------------------------------------------
% Kit Choy Xintong
% Understanding AES Mix-Columns Transformation Calculation
%=========================================================================
```

- **Tests possibles de reconnaissance**

Pour chaque cas parmi les trois cas suivants :

- Cas 1 : seul individu, plusieurs images échantillons par individu.
- Cas 2 : plusieurs individus, seule image échantillon par individu.
- Cas 3 : plusieurs individus, plusieurs images échantillons par individu.
- Seul individu, seule image échantillon par individu (Ce cas n'est pas étudié).

On peut effectuer les tests de reconnaissance suivants :

- Test des images (noms connus, images connues).
- Test des images (noms connus, images inconnues).
  - Toutes les images échantillons inconnues.
  - Partie d'images échantillons connues et d'autres inconnues.
- Test des images (noms inconnus).

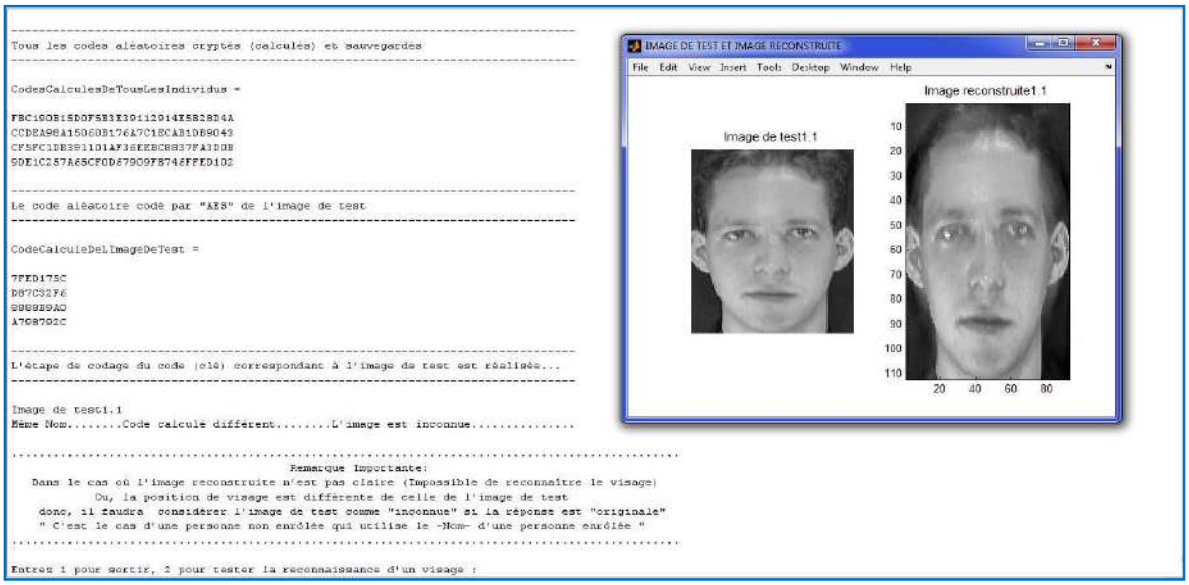
Remarque :

Connu : signifie sauvegardé dans la base de données du système.
Inconnu : signifie non-sauvegardé dans la base de données du système.

- **Exemple de test : Cas 3 (plusieurs individus, plusieurs images échantillons).**

1- Test des images (noms connus, images connues)

```
Entrez le nom de la personne (N° du répertoire): 1
Entrez le nom de l'image de test (N° de l'image) : 1
```



Remarque : classement erroné.

Figure 36 : Exemple de test de reconnaissance 1 (Cas3).

2- Test des images (noms connus, images inconnues)

- **Toutes les images échantillons inconnues**

```
Entrez le nom de la personne (N° du répertoire): 1
Entrez le nom de l'image de test (N° de l'image) : 1
```



Remarque **:** classement erroné.

Figure 37 : Exemple de test de reconnaissance 2 (Cas3).

- **Partie d'images échantillons connues et d'autres inconnues**

```
Entrez le nom de la personne (N° du répertoire): 1
Entrez le nom de l'image de test (N° de l'image) : 5
```

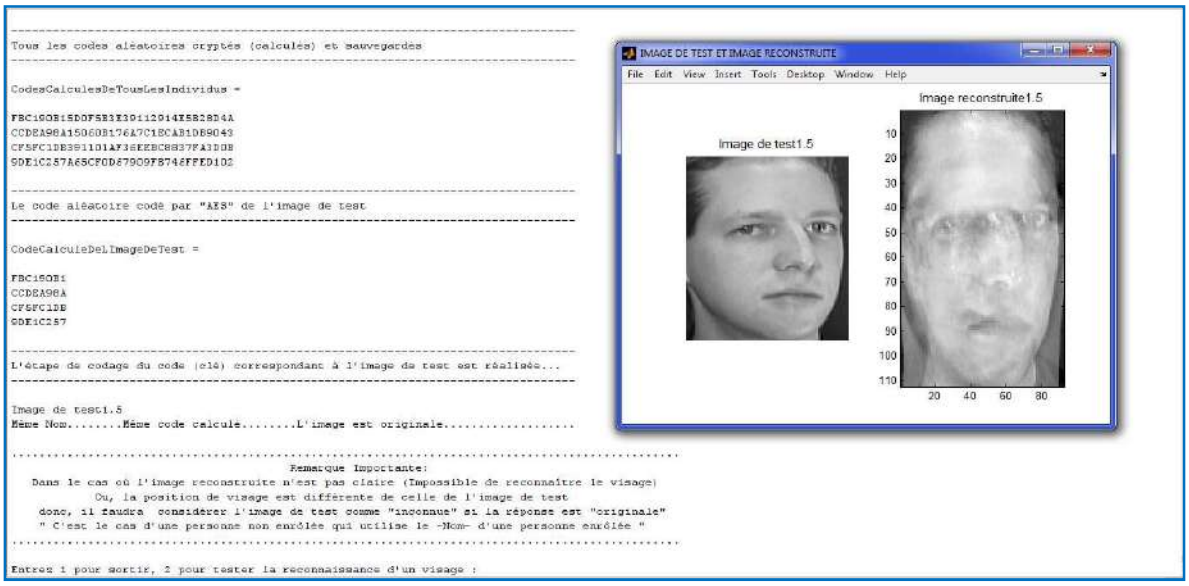


Figure 38 : Exemple de test de reconnaissance 3 (Cas3).

- **Test des images (noms inconnus)**

```
Entrez le nom de la personne (N° du répertoire): 40
Entrez le nom de l'image de test (N° de l'image) : 1
```

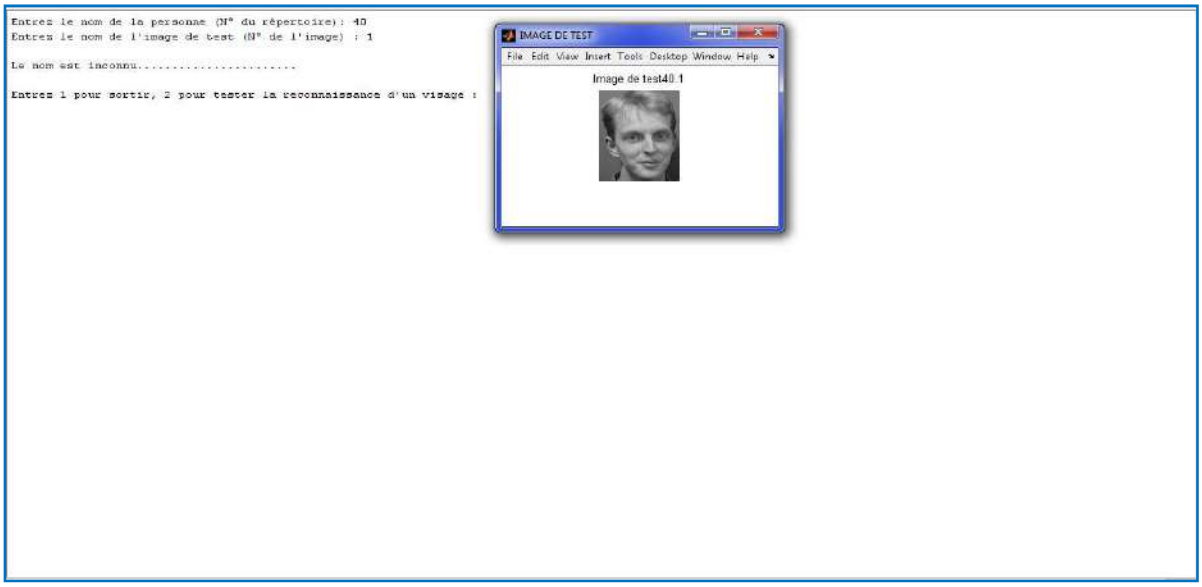


Figure 39 : Exemple de test de reconnaissance 4 (Cas3).

VI. 4.3. Le bilan des expériences

La base des visages ORL contient les images des visages de 40 personnes. Chaque personne a 10 images échantillons. L'enrôlement (sauvegarde) des images par le système de reconnaissance de visages reconstruit se fait par groupe dans chaque cas parmi les 3 cas, dont le nombre de personnes par groupe et le nombre des images échantillons enrôlés se diffèrent. On test la reconnaissance des images enrôlées et les images non enrôlées pour tous les cas. Les résultats de la reconnaissance (Les réponses du système) sont marqués dans des tableaux (1 : image connue, 0 : image inconnue).

Remarque Importante :

Pour chaque personne de la base ORL, il y a deux types de fausses acceptations :

- Fausse acceptation réelle :
  Acceptation des images (noms connus, images inconnues)
  → Toutes les images échantillons inconnues.
  → Personne inconnue dans le système qui utilise le nom d'une personne connue.
  → Le nombre maximale possible de fausses acceptations réelles (Par individu)=
  = (40 personnes -1)*10 images échantillons pour chaque personne = 390.

- Fausse acceptation irréelle :
  Acceptation des images (noms connus, images inconnues)
  → Partie d'images échantillons connues et d'autres inconnues.
  (L'image échantillon testée n'est pas enrôlée).
  → Personne connue dans le système qui utilise son nom d'origine.
  → Le nombre maximale possible de fausses acceptations irréelles (Par individu)=
  = 10 images échantillons - 4 échantillons enrôlés = 6.

Pour calculer le taux de Fausse acceptation réelle en valeur exacte, on a besoin d'effectuer 390 tests de reconnaissance pour chaque personne appartenant à cette base (ORL). Donc, pour simplifier les calculs on utilise le taux de fausse acceptation irréelle avec seulement 6 tests.

Le terme « réelle » et « irréelle » sont des mots choisis par l'auteur juste pour expliquer l'idée de la fausse acceptation.

Remarque :

Les expériences au dessous (Les trois cas) ne sont pas aléatoires. Elles représentent les meilleurs cas possibles trouvés par le programmeur après plusieurs expérimentations (tests de reconnaissance) et la comparaison de leurs résultats et les paramètres utilisées.

Rappel :

1 : signifie image connue.
0 : signifie image inconnue.

VI. 4.3.1. Cas 1 : un seul individu, plusieurs images échantillons par individu

Paramètre :

- L'enrôlement des images se fait par groupe de (01) personne.
- Quatre (04) images échantillons doivent être enrôlées pour chaque personne.
- Le nombre de groupes : 40/1=40 groupes.
- Le codeur de correction d'erreurs fonctionne en 3 bits de redondance.

Remarque :

Groupe 1	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	1	1	1	1	1	1	1	1	1

Groupe 2	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	1	1	1	1	1	1	1	1	1	1

Groupe 3	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
3	1	1	1	1	1	1	1	1	1	1

Groupe 4	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
4	1	1	1	1	1	0	1	1	1	1

Groupe 5	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
5	1	1	1	1	0	0	1	0	0	0

Groupe 6	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
6	1	1	1	1	0	0	0	0	0	1

Groupe 7	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
7	1	1	1	1	1	1	1	1	1	1

Groupe 8	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
8	1	1	1	1	1	1	1	1	1	1

Groupe 9	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
9	1	1	1	1	1	1	1	1	1	1

Groupe 10	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
10	1	1	0	0	1	1	0	1	1	1

Groupe 11	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
11	1	1	1	1	1	1	1	1	1	1

Groupe 12	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
12	1	1	1	1	1	1	1	1	1	1

Groupe 13	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
13	1	1	0	0	1	1	1	1	1	1

Groupe 14	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
14	1	1	1	1	1	1	1	1	1	1

Groupe 15	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
15	1	1	1	1	1	1	1	1	1	1

Groupe 16	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
16	1	1	1	1	1	1	1	1	1	1

Groupe 17	**Les images échantillons**									
Individus	**Échantillons Enrôlés**				**Échantillons Non Enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
17	1	1	1	1	1	0	0	0	0	0

Groupe 18	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
18	1	1	1	1	1	1	0	1	1	1

Groupe 19	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
19	1	1	1	1	1	0	1	1	1	1

Groupe 20	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
20	1	1	1	1	0	1	0	0	0	1

Groupe 21	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
21	1	1	1	1	1	1	0	0	1	0

Groupe 22	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
22	1	1	0	1	1	1	0	1	1	1

Groupe 23	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
23	0	1	1	1	1	1	1	1	0	0

Groupe 24	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
24	0	0	1	1	0	0	0	0	1	1

Groupe 25	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
25	1	1	1	1	1	1	1	1	1	1

Groupe 26	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
26	1	0	1	1	1	1	1	1	1	1

Groupe 27	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
27	1	1	1	1	1	0	0	0	0	1

Groupe 28	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
28	1	1	1	1	1	1	1	0	1	0

Groupe 29	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
29	1	1	1	1	0	0	0	0	1	0

Groupe 30	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
30	1	1	1	1	1	0	1	1	0	1

Groupe 31	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
31	1	0	0	0	0	1	1	1	1	0

Groupe 32	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
32	1	1	1	0	1	1	1	1	1	1

Groupe 33	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
33	1	1	1	1	1	1	1	0	1	1

Groupe 34	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
34	1	1	1	1	1	1	1	0	0	0

Groupe 35	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
35	1	1	0	1	0	1	1	1	0	0

Groupe 36	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
36	1	0	1	1	1	1	1	1	1	1

Groupe 37	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
37	0	1	0	1	1	1	0	1	0	0

Groupe 38	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
38	1	1	1	1	1	0	1	1	0	1

Groupe 39	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
39	0	0	1	1	1	1	1	1	1	1

Groupe 40	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
40	1	1	1	0	0	1	0	1	0	1

- Le taux de faux rejets (En anglais, False Reject Rate FRR**)**
  Remarque : calculs par 40 individus.

$$FRR = \frac{Nombre\ de\ faux\ rejets}{Nombre\ total\ d'acces\ client}$$

Nomination	**Taux FRR**	**Nomination**	**Taux FRR**	**Nomination**	**Taux FRR**	**Nomination**	**Taux FRR**
Individu 1	0.0000	Individu 11	0.0000	Individu 21	0.0000	Individu 31	0.0075
Individu 2	0.0000	Individu 12	0.0000	Individu 22	0.0025	Individu 32	0.0025
Individu 3	0.0000	Individu 13	0.0050	Individu 23	0.0025	Individu 33	0.0000
Individu 4	0.0000	Individu 14	0.0000	Individu 24	0.0050	Individu 34	0.0000
Individu 5	0.0000	Individu 15	0.0000	Individu 25	0.0000	Individu 35	0.0025
Individu 6	0.0000	Individu 16	0.0000	Individu 26	0.0025	Individu 36	0.0025
Individu 7	0.0000	Individu 17	0.0000	Individu 27	0.0000	Individu 37	0.0005
Individu 8	0.0000	Individu 18	0.0000	Individu 28	0.0000	Individu 38	0.0000
Individu 9	0.0000	Individu 19	0.0000	Individu 29	0.0000	Individu 39	0.0005
Individu 10	0.0050	Individu 20	0.0000	Individu 30	0.0000	Individu 40	0.0025

- Le taux de fausse acceptation (En anglais, False Acceptation Rate FAR)
  Remarque : calculs par 40 individus.

$$FAR = \frac{Nombre\ de\ fausses\ acceptations}{Nombre\ total\ d'acces\ imposteurs}$$

Nomination	**Taux FAR**	**Nomination**	**Taux FAR**	**Nomination**	**Taux FAR**	**Nomination**	**Taux FAR**
Individu 1	0.0722	Individu 11	0.0722	Individu 21	0.0361	Individu 31	0.0481
Individu 2	0.0722	Individu 12	0.0722	Individu 22	0.0602	Individu 32	0.0722
Individu 3	0.0722	Individu 13	0.0722	Individu 23	0.0481	Individu 33	0.0602
Individu 4	0.0602	Individu 14	0.0722	Individu 24	0.0240	Individu 34	0.0361
Individu 5	0.0120	Individu 15	0.0722	Individu 25	0.0722	Individu 35	0.0361
Individu 6	0.0120	Individu 16	0.0722	Individu 26	0.0722	Individu 36	0.0722
Individu 7	0.0722	Individu 17	0.0120	Individu 27	0.0240	Individu 37	0.0361
Individu 8	0.0722	Individu 18	0.0602	Individu 28	0.0481	Individu 38	0.0481
Individu 9	0.0722	Individu 19	0.0602	Individu 29	0.0120	Individu 39	0.0722
Individu 10	0.0602	Individu 20	0.0240	Individu 30	0.0481	Individu 40	0.0361

- Représentation en graphe des taux FRR et FAR :

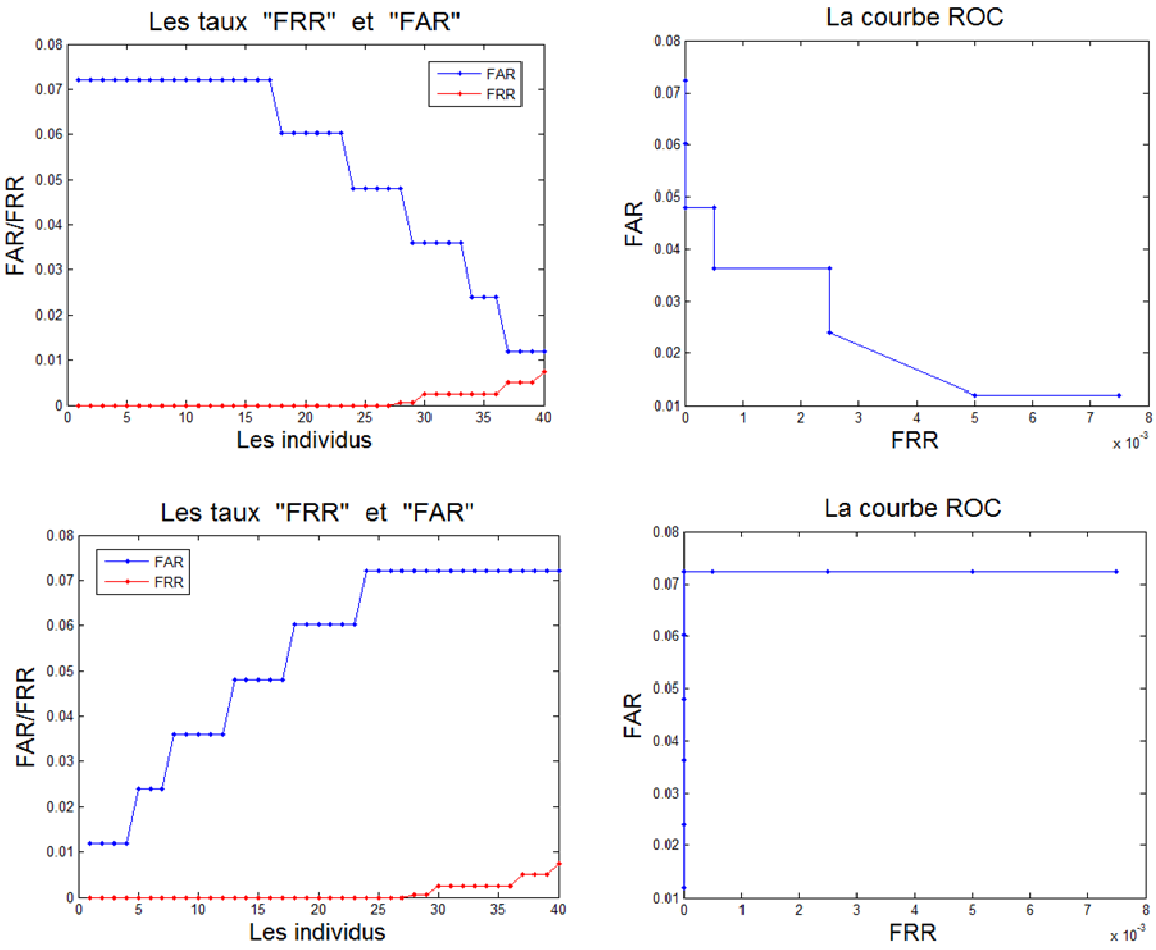


Figure 40 : Courbes FRR, FAR, et ROC (Cas 1).

- Distribution des résultats FRR et FAR :

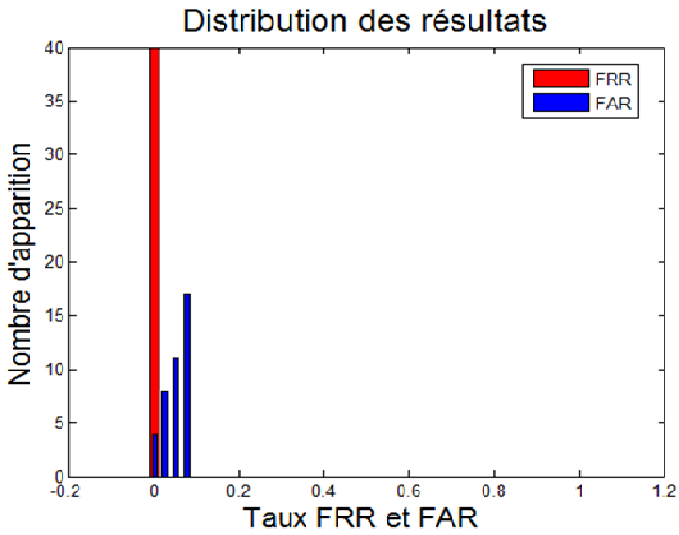


Figure 41 : Distribution des résultats FRR et FAR (Cas 1).

VI. 4.3.2. Cas 2 : plusieurs individus, une seule image échantillon par individu

Paramètre :

- L'enrôlement des images se fait par groupe de (08) personnes.
- Une (01) image échantillon doit être enrôlée pour chaque personne.
- Le nombre de groupes : 40/8= 5 groupes.
- Le codeur de correction d'erreurs fonctionne en 2 bits de redondance.

Remarque :

Groupe 1	**Les images échantillons**									
Individus	**Enrôl**	**Échantillons non enrôlés**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	1	1	0	0	0	1	0	0	0
2	1	1	1	1	1	1	1	1	0	1
3	1	1	1	1	1	1	0	0	1	1
4	1	0	0	0	0	0	0	0	0	0
5	1	1	1	1	1	1	1	0	0	0
6	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	0	1	0
8	1	1	0	0	1	1	1	0	1	0

Groupe 2	**Les images échantillons**									
Individus	**Enrôl**	**Échantillons non enrôlés**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
9	1	1	1	0	1	1	1	0	1	0
10	1	1	0	0	0	0	0	1	1	0
11	1	0	1	0	0	1	1	0	0	1
12	1	0	0	0	0	0	0	0	0	0
13	1	1	0	0	1	0	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1
15	1	0	1	1	0	0	0	1	0	0
16	1	0	0	0	0	1	0	0	0	0

Groupe 3	**Les images échantillons**									
Individus	**Enrôl**	**Échantillons non enrôlés**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
17	1	1	0	0	1	0	0	0	0	0
18	1	1	0	1	0	0	1	0	0	0
19	1	1	0	0	0	1	0	0	1	1
20	1	0	1	1	0	1	0	0	0	1
21	1	1	1	0	0	0	0	0	1	0
22	1	1	1	0	1	1	1	1	1	1
23	1	0	0	0	0	0	0	0	0	0
24	1	0	0	1	0	0	1	0	1	1

Groupe 4	Les images échantillons									
Individus	Enrôl	Échantillons non enrôlés								
	1	2	3	4	5	6	7	8	9	10
25	1	0	0	0	0	0	0	0	0	0
26	1	1	1	1	1	1	0	0	0	0
27	1	0	1	1	1	0	0	0	0	1
28	1	0	1	0	0	1	0	1	0	1
29	1	1	1	1	1	1	1	1	1	1
30	1	1	1	1	1	1	1	1	1	1
31	1	1	1	1	1	1	1	1	1	0
32	1	0	0	0	0	0	0	0	0	0

Groupe 5	Les images échantillons									
Individus	Enrôl	Échantillons non enrôlés								
	1	2	3	4	5	6	7	8	9	10
33	1	0	1	0	1	0	1	0	0	0
34	1	1	1	1	1	0	1	0	0	0
35	1	0	0	0	0	0	0	0	0	0
36	1	0	1	0	1	0	0	1	1	0
37	1	1	1	1	0	1	1	0	1	1
38	1	1	1	1	1	1	1	1	1	1
39	1	0	0	0	0	0	0	0	0	0
40	1	0	0	0	0	1	1	1	1	0

- Le taux de faux rejets (En anglais, False Reject Rate FRR**)**
  Remarque : calculs par groupe de 8 individus.

$$FRR = \frac{Nombre\ de\ faux\ rejets}{Nombre\ total\ d'acces\ client}$$

Nomination	Taux FRR	Nomination	Taux FRR	Nomination	Taux FRR	Nomination	Taux FRR
Individu 1	0.0000	Individu 11	0.0000	Individu 21	0.0000	Individu 31	0.0000
Individu 2	0.0000	Individu 12	0.0000	Individu 22	0.0000	Individu 32	0.0000
Individu 3	0.0000	Individu 13	0.0000	Individu 23	0.0000	Individu 33	0.0000
Individu 4	0.0000	Individu 14	0.0000	Individu 24	0.0000	Individu 34	0.0000
Individu 5	0.0000	Individu 15	0.0000	Individu 25	0.0000	Individu 35	0.0000
Individu 6	0.0000	Individu 16	0.0000	Individu 26	0.0000	Individu 36	0.0000
Individu 7	0.0000	Individu 17	0.0000	Individu 27	0.0000	Individu 37	0.0000
Individu 8	0.0000	Individu 18	0.0000	Individu 28	0.0000	Individu 38	0.0000
Individu 9	0.0000	Individu 19	0.0000	Individu 29	0.0000	Individu 39	0.0000
Individu 10	0.0000	Individu 20	0.0000	Individu 30	0.0000	Individu 40	0.0000

- Le taux de fausse acceptation (En anglais, False Acceptation Rate FAR)
  Remarque : calculs par groupe de 8 individus.

$$FAR = \frac{Nombre\ de\ fausses\ acceptations}{Nombre\ total\ d'acces\ imposteurs}$$

Nomination	Taux FAR	Nomination	Taux FAR	Nomination	Taux FAR	Nomination	Taux FAR
Individu 1	0.1111	Individu 11	0.1000	Individu 21	0.0681	Individu 31	0.2424
Individu 2	0.2962	Individu 12	0.0000	Individu 22	0.1818	Individu 32	0.0000
Individu 3	0.2592	Individu 13	0.1500	Individu 23	0.0000	Individu 33	0.0750
Individu 4	0.0000	Individu 14	0.2250	Individu 24	0.0909	Individu 34	0.1250
Individu 5	0.2222	Individu 15	0.0750	Individu 25	0.0000	Individu 35	0.0000
Individu 6	0.3333	Individu 16	0.0250	Individu 26	0.1515	Individu 36	0.1000
Individu 7	0.2592	Individu 17	0.0454	Individu 27	0.1212	Individu 37	0.1750
Individu 8	0.1851	Individu 18	0.0681	Individu 28	0.1212	Individu 38	0.2250
Individu 9	0.1500	Individu 19	0.0909	Individu 29	0.2727	Individu 39	0.0000
Individu 10	0.0750	Individu 20	0.0909	Individu 30	0.2727	Individu 40	0.1000

- Représentation en graphe des taux FRR et FAR :

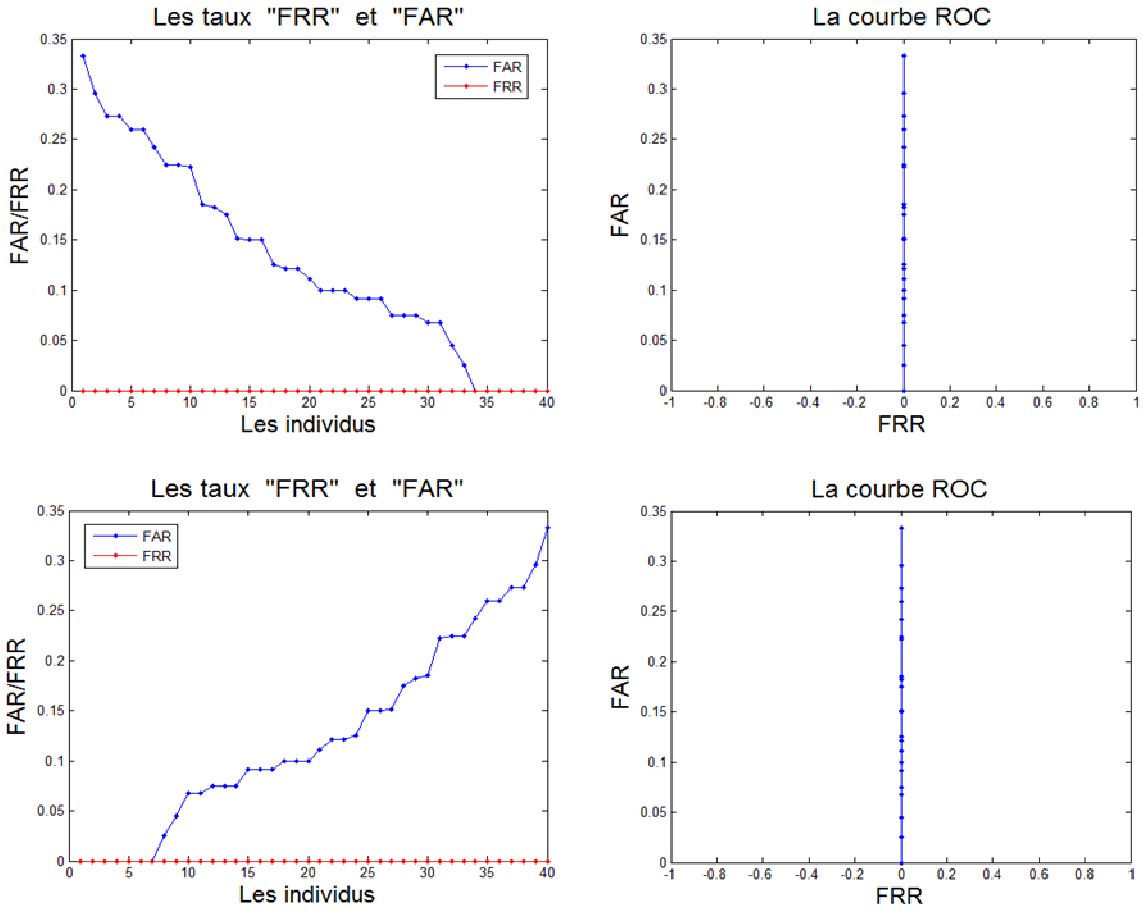


Figure 42 : Courbes FRR, FAR, et ROC (Cas 2).

- Distribution des résultats FRR et FAR :

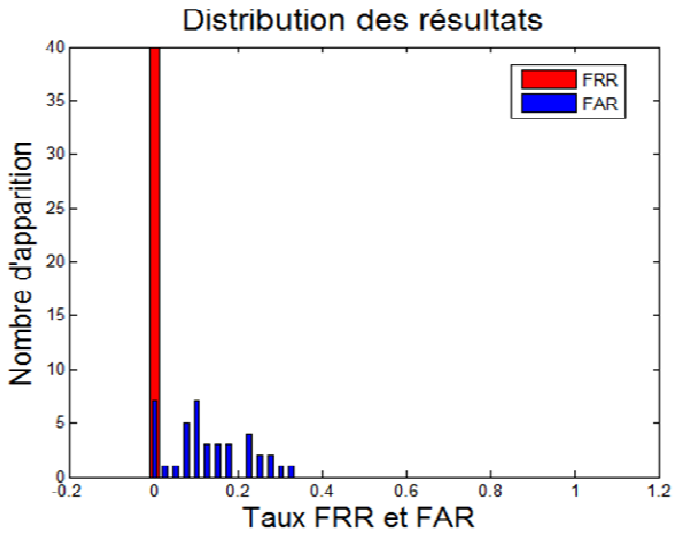


Figure 43 : Distribution des résultats FRR et FAR (Cas 2).

VI. 4.3.3. Cas 3 : plusieurs individus, plusieurs images échantillons par individu

Paramètre :

- L'enrôlement des images se fait par groupe de (04) personnes.
- Quatre (04) images échantillons doivent être enrôlées pour chaque personne.
- Le nombre de groupes : 40/4=10 groupes.
- Le codeur de correction d'erreurs fonctionne en 3 bits de redondance.

Remarque :

Groupe 1	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	0	0	1	1	0	1	1	0	1
2	1	1	1	1	1	1	0	0	1	0
3	0	1	0	1	1	1	1	0	1	1
4	1	1	1	1	1	0	1	1	1	0

Groupe 2	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
5	1	0	0	0	1	1	0	1	0	1
6	1	1	0	1	1	1	0	1	0	1
7	1	1	0	0	1	1	1	0	1	1
8	0	0	0	0	0	0	0	1	1	1

Groupe 3	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
9	1	1	1	0	0	0	1	0	0	0
10	1	1	1	1	0	1	1	0	1	1
11	0	1	1	1	1	1	0	1	1	0
12	1	1	1	1	1	1	1	1	0	1

Groupe 4	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
13	1	1	0	1	1	1	1	1	1	1
14	0	1	1	0	1	0	0	1	0	1
15	1	1	1	1	1	1	1	1	1	1
16	1	0	0	1	0	1	0	0	0	1

Groupe 5	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
17	1	1	1	1	1	1	1	1	1	1
18	1	1	1	1	0	1	0	1	1	1
19	1	1	1	0	0	0	0	0	0	1
20	1	1	1	1	1	1	1	1	1	1

Groupe 6	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
21	1	1	0	0	0	1	1	0	0	0
22	1	1	0	0	1	0	1	0	0	0
23	1	0	0	0	0	0	0	0	0	1
24	1	1	1	0	1	0	1	0	1	1

Groupe 7	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
25	1	1	1	1	1	1	0	0	1	1
26	1	0	0	1	1	0	1	1	0	0
27	1	1	1	1	1	1	1	1	1	1
28	0	1	1	0	1	0	0	1	1	1

Groupe 8	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
29	1	1	1	1	0	0	0	0	1	1
30	1	0	1	1	1	1	1	1	1	1
31	1	1	1	1	1	1	1	1	1	1
32	1	0	1	0	1	1	1	1	1	1

Groupe 9	**Les images échantillons**									
Individus	**Échantillons enrôlés**				**Échantillons non enrôlés**					
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
33	1	1	1	1	0	0	0	1	0	1
34	1	0	0	1	1	1	1	1	1	1
35	0	1	1	0	0	0	0	0	0	0
36	0	0	0	0	1	1	1	0	0	0

Groupe 10	Les images échantillons									
Individus	Échantillons enrôlés				Échantillons non enrôlés					
	1	2	3	4	5	6	7	8	9	10
37	1	0	1	0	0	0	0	0	1	0
38	1	1	1	1	1	1	1	1	1	1
39	1	1	1	1	0	0	1	1	1	1
40	1	1	0	1	1	1	1	1	1	1

- Le taux de faux rejets (En anglais, False Reject Rate FRR)
  Remarque : calculs par groupe de 4 individus.

$$FRR = \frac{Nombre\ de\ faux\ rejets}{Nombre\ total\ d'acces\ client}$$

Nomination	Taux FRR	Nomination	Taux FRR	Nomination	Taux FRR	Nomination	Taux FRR
Individu 1	0.0500	Individu 11	0.0250	Individu 21	0.0500	Individu 31	0.0000
Individu 2	0.0000	Individu 12	0.0000	Individu 22	0.0500	Individu 32	0.0500
Individu 3	0.0500	Individu 13	0.0250	Individu 23	0.0750	Individu 33	0.0000
Individu 4	0.0000	Individu 14	0.0500	Individu 24	0.0250	Individu 34	0.0500
Individu 5	0.0750	Individu 15	0.0000	Individu 25	0.0000	Individu 35	0.0500
Individu 6	0.0250	Individu 16	0.0050	Individu 26	0.0500	Individu 36	0.1000
Individu 7	0.0500	Individu 17	0.0000	Individu 27	0.0000	Individu 37	0.0500
Individu 8	0.1000	Individu 18	0.0000	Individu 28	0.0500	Individu 38	0.0000
Individu 9	0.0250	Individu 19	0.0250	Individu 29	0.0000	Individu 39	0.0000
Individu 10	0.0000	Individu 20	0.0000	Individu 30	0.0250	Individu 40	0.0250

- Le taux de fausse acceptation (En anglais, False Acceptation Rate FAR)
  Remarque : calculs par groupe de 4 individus.

$$FAR = \frac{Nombre\ de\ fausses\ acceptations}{Nombre\ total\ d'acces\ imposteurs}$$

Nomination	Taux FAR	Nomination	Taux FAR	Nomination	Taux FAR	Nomination	Taux FAR
Individu 1	0.3333	Individu 11	0.3333	Individu 21	0.0869	Individu 31	0.8571
Individu 2	0.4166	Individu 12	0.4166	Individu 22	0.0869	Individu 32	0.8571
Individu 3	0.3333	Individu 13	0.5000	Individu 23	0.0434	Individu 33	0.0952
Individu 4	0.3636	Individu 14	0.2500	Individu 24	0.1739	Individu 34	0.2857
Individu 5	0.2222	Individu 15	0.5000	Individu 25	0.3636	Individu 35	0.0000
Individu 6	0.2222	Individu 16	0.1666	Individu 26	0.2727	Individu 36	0.1428
Individu 7	0.2777	Individu 17	0.7500	Individu 27	0.5454	Individu 37	0.1000
Individu 8	0.1666	Individu 18	0.5000	Individu 28	0.3636	Individu 38	0.6000
Individu 9	0.0833	Individu 19	0.1250	Individu 29	0.2857	Individu 39	0.4000
Individu 10	0.3333	Individu 20	0.7500	Individu 30	0.8571	Individu 40	0.6000

- Représentation en graphe des taux FRR et FAR :

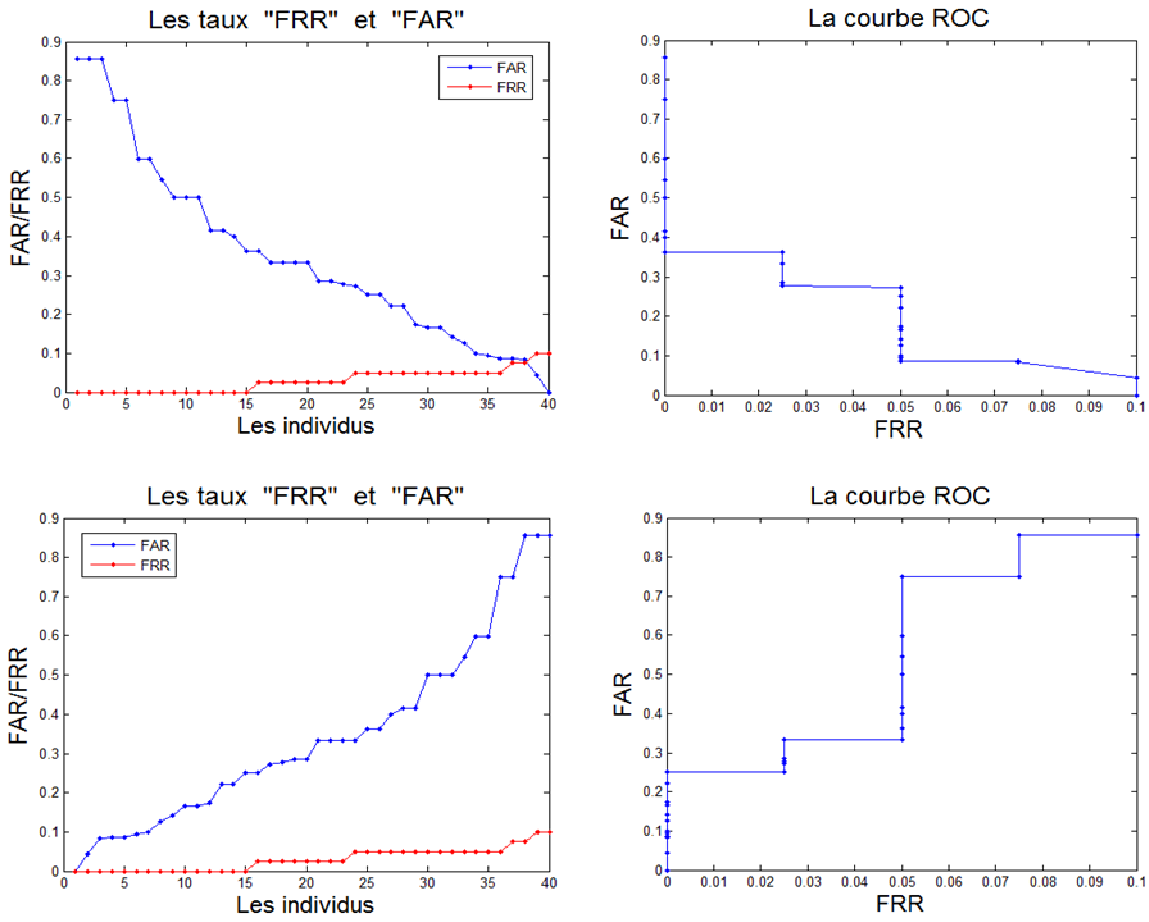


Figure 44 : Courbes FRR, FAR, et ROC (Cas 3).

- Distribution des résultats FRR et FAR :

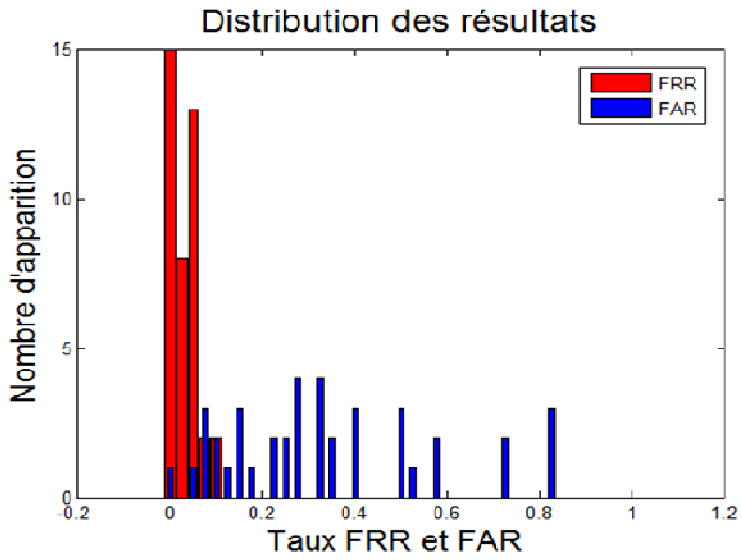


Figure 45 : Distribution des résultats FRR et FAR (Cas 3).

VI. 5. Avantages et inconvénients du système reconstruit

Remarques générales :

- Il y a des cas de fausse acceptation FAR.
- Il y a des cas de faux rejet FRR.
- Le système n'enrôle pas une ou deux images échantillons, si une seule personne est enrôlée.
- le système ne sera plus fiable lorsqu'on utilise beaucoup d'images lors de la phase d'enrôlement.
- FRR (Taux de Faux rejet) augmente lorsque :
    - Le nombre de personnes enrôlées augmente.
    - Le nombre des images échantillons augmente.

Avantage :

- Le système refuse les personnes qui ont des noms inconnus.
- Le système peut refuser des personnes non enrôlées utilisant les noms des personnes enrôlées.
- Le système peut reconnaître des images non enrôlées (inconnues) pour des personnes enrôlées (connues).

Solutions proposées :

- Construction d'une fonction de tolérance partielle avec le bruit.
- Modification du code de correction d'erreurs.
- Lecture plusieurs images échantillons lors de la phase d'authentification et l'utilisation de leur moyenne.
- Test de plusieurs images avant de prendre la décision.
- L'enrôlement de l'ensemble d'individus personne par personne, avec plusieurs images échantillons pour chaque individu.
- L'enrôlement de l'ensemble d'individus groupe par groupe, avec plusieurs images échantillons pour chaque individu.

Quelques améliorations :

- Décodage de la clé enregistrée par un décodeur AES au lieu du codage de la clé extraite (régénérée) par un codeur AES lors de la phase d'authentification.
- Comparaison de la clé enregistrée avec la clé extraite (régénérée) élément par élément, et fournir le résultat comme un pourcentage de reconnaissance du visage testé.
- Développement du programme pour qu'il soit capable d'effectuer le test d'un seul personne et une seule image échantillon.

VI. 6. Conclusion

Le système fournit les meilleurs résultats possibles dans les cas suivants :

- **Cas 1 : une seule personne et plusieurs images échantillons par personne**

- Paramètre : l codeur de correction d'erreurs fonctionne en 3 bits de redondance (chaque bit est représenté 4 fois).
- Résultat : la plupart des résultats sont justes.
- Conditions : pour que la réponse soit juste, il faut tester plusieurs images avant de donner une décision.
- Avantage : cette méthode est efficace pour : contrôle d'accès en temps réel (variation des images acquises). Et le système peut reconnaître des images non connues pour des personnes connues.

- **Cas2 : plusieurs personnes et une seule image échantillon par personne**

- Paramètre : un codeur de correction d'erreurs fonctionne en 2 bits de redondance (chaque bit est représenté 3 fois)
- Résultat : la plupart des résultats sont justes.
- Conditions : lors de la phase d'authentification, il faut présenter à chaque test de reconnaissance la même image enrôlée.
- Avantage : cette méthode est efficace pour la carte à puce, la carte d'identité, le passeport où les données biométriques sont statiques.

- **Cas 3 : plusieurs personnes et plusieurs images échantillons par personne**

- Paramètre : un codeur de correction d'erreurs fonctionne en 3 bits de redondance (chaque bit est représenté 4 fois).
- Résultat : Il y a des résultats justes et des résultats faux.
- Conditions : pour que la réponse soit juste, il faut tester plusieurs images avant de donner une décision.
- Avantage : cette méthode est efficace pour : contrôle d'accès en temps réel (variation des images acquises). le système peut reconnaître des images non connues pour des personnes connues.

Conclusion Générale

Conclusion Générale

Depuis les années passées et jusqu'à présent, la reconnaissance faciale est considérée parmi les méthodes les plus intéressantes d'authentification des personnes, à cause de sa acceptabilité par le public et la simplicité de réalisation et vérification.

La reconnaissance faciale par les systèmes biométriques est réalisée en deux parties : la première est l'enrôlement du visage (l'apprentissage et le sauvegarde) et la deuxième c'est l'authentification du visage (le test de reconnaissance). Dans chacune des deux parties, les étapes de calculs sont identiques : l'acquisition de l'image, le prétraitement, la détection, l'extraction des caractéristiques, sauf la dernière étape : dans la première partie les données calculées sont stockées dans la base de données du système biométrique comme des données de référence, et dans la deuxième étape les données calculées sont utilisées pour faire la comparaison avec les données stockées correspondantes afin de prendre la décision si la personne est connue ou non.

L'important, est que le système de reconnaissance puisse classifier un visage et décide s'il est enregistré ou non. Mais, il y a toujours des risques de falsification ou de vol des données biométriques par un intrus, donc la protection de ces donnés secrètes est nécessaire pour réduire les cas de vulnérabilité du système biométrique. C'est pourquoi, on a proposé de protéger les informations biométriques de référence par le modèle de protection à liaison de la clé « Le plan des données assistantes ».

Ce plan se constitue de deux étapes : étape transformation et étape crypto-système. Dans l'étape transformation, les informations biométriques généralement se présentent sous forme de valeurs réelles, ces valeurs réelles sont converties en binaire à l'aide d'une fonction de Binarisation à seuil (changement du type des données extraites). Au même temps dans l'étape crypto-système, un code aléatoire (Une clé binaire) est généré par le générateur de code aléatoire. L'étape crypto-système permet de coder cette base biométrique transformée à l'aide du code généré et d'enregistrer la base transformée et le code aléatoire codée (par exemple par, le chiffrement standard avancé) ou hachée dans la base de données du système biométrique.

Le système de reconnaissance de visage réalisé fonctionne en deux phases essentielles : l'enrôlement et l'authentification selon le mode vérification (comparaison un à un). Il est protégé par le plan des données assistantes (Système hybride : transformé/crypté) et utilise les images de la base des visages ORL comme source d'images pour construire la base des données de référence des personnes connues par le système.

Lors de la phase d'enrôlement, le système transforme l'information biométrique des images par la projection dans l'espace visage à l'aide de la méthode « l'Analyse En Composantes Principales », ce qui permet de réduire la dimension des données biométriques d'une manière efficace pour obtenir de ce qu'on l'appelle « Les composantes principales ». Après la projection, une Binarisation de ces composantes est appliquée, donc on obtient des informations binaires. Chaque information binaire extraite est relié avec une clé aléatoire générée par le générateur de code aléatoire et codée par un codeur de correction d'erreurs,

l'information résultante est appelée « donnée assistante ». Cette donnée assistante sous la forme protégée sera stockée dans la base de données du système biométrique, avec une copie de la clé aléatoire codée par le « Chiffrement Standard avancé, CSA » (En, advanced Encryption Standard AES), et autres informations supplémentaires nécessaires.

Lors de la phase d'authentification, les mêmes étapes que la phase d'enrôlement sont réalisées, mais avec une seule image de test à chaque fois. Dans ce cas, le système doit récupérer les informations stockées dans la base de données afin de réaliser les calculs nécessaires et précisément à partir de l'étape de sélection des bits les plus fiables. La donnée assistante correspondante à l'image de test est reliée avec la donnée binaire requête calculée pour régénérer la clé aléatoire (La clé requête). Puis, une vérification par un décodeur de correction d'erreurs est réalisée pour le but d'éliminer la redondance incluse dans la clé régénéré et corriger les erreurs causées par les variations intra-classes de l'utilisateur du système biométrique. La clé régénérée et décodée est codée aussi par le Chiffrement Standard avancé. À la fin du processus d'authentification, Le système compare d'une manière automatique la clé requête codée avec la clé codée correspondante enregistrée dans la base de données biométriques et décide si la clé régénérée est originale ou non.

Tous les concepts au dessus sont regroupés pour réaliser un système de reconnaissance de visage 2D. Afin de mesurer la performance de ce système, plusieurs expériences et calculs ont été effectués. Et à chaque test de reconnaissance, on a comparé les paramètres utilisés et les résultats obtenus, pour choisir lesquels (paramètres) fournissent une efficacité du système biométrique. Donc on a conclu quelques configurations possibles permettant de mettre le système dans un état acceptable (presque fiable). Ces configurations sont les suivantes :

1. Cas 1 :
   Seule personne, plusieurs images échantillons (3 bits de redondance).

2. Cas 2 :
   Plusieurs personnes, une seule image échantillon (2 bits de redondance).

3. Cas 3 :
   Plusieurs personnes, plusieurs images échantillon (3 bits de redondance).

4. Cas 4 :
   Seule personne, une seule image échantillon (Ce cas n'est pas encore étudié).

Quand on exécute le programme constituant le système, on marque les réponses suivantes : acceptation, rejet, fausse acceptation ou faux rejet. Mais, l'avantage est que les réponses « acceptation » soient les plus dominantes. Parmi les autres avantages marqués aussi est que le système soit capable de refuser les personnes qu'ils ont des noms inconnus, les personnes inconnues utilisant les noms des personnes connues, et puisse reconnaître des images inconnues pour des personnes connues. Cependant, il apparait des inconvénients diminuant la fiabilité du système tels que : l'enrôlement d'un grand nombre de personnes ou d'images échantillons à la fois.

Donc, pour améliorer les avantages et normaliser les inconvénients, on a proposé quelques solutions simples qu'ils sont :

- La construction d'une fonction de tolérance partielle avec le bruit.
- La modification du code de correction d'erreurs.
- La lecture de plusieurs images échantillons lors de la phase d'authentification et l'utilisation de leur moyenne.
- Le test de plusieurs images avant de prendre la décision.
- L'enrôlement personne par personne, avec plusieurs images échantillons.
- L'enrôlement par groupe, avec plusieurs images échantillons.

Et bien sur en respectant les conditions : l'enrôlement d'un nombre réduit de personnes, et un nombre réduit aussi d'images échantillons par individu pour des raisons de réduire le temps de calcul, éviter la charge des informations et améliorer la réponses du systèmes .

Donc, on conclut que la fusion d'un Plan Des Données Assistantes avec la base des visages ORL et les méthodes : l'Analyse En Composantes Principales ACP et le Chiffrement Standard avancé CSA, puisse donner des résultats acceptable. Et avec quelques améliorations supplémentaires et développements simples, le système pourra devenir fiable.

Autres détails sont disponibles dans le Chapitre « Implémentation Et Résultats ».

Annexe A :

Analyse En Composantes Principales (ACP)

A. 1. Définition

Turk et Pentland ont proposé la méthode de visage propre basée sur l'Analyse en composantes principales ACP pour la reconnaissance faciale. L'algorithme se compose de deux phases : la phase d'apprentissage et la phase de reconnaissance. Dans la phase d'apprentissage, les vecteurs propres sont calculés avec un grand nombre de visages. Ensuite, les visages sont inscrits dans un système de reconnaissance faciale par leur projection sur l'espace de visage. Dans la phase de reconnaissance, une face d'entrée inconnue peut être identifiée en mesurant les distances des coefficients entre la face d'entrée et les visages inscrits dans la base, [33].

A. 1. Concepts de l'Analyse en composantes principales

L'ensemble des images visages d'apprentissage contient $\boldsymbol{M}$ images, de dimension $\boldsymbol{N \times N.}$
L'ensemble des vecteurs visages d'apprentissage contient $\boldsymbol{\Gamma_1 , \Gamma_2 , \ldots, \Gamma_M}$ of size $\boldsymbol{N^2 \times 1.}$
[11][34]

A. 2.1. Image moyenne : [11][34]

$$\boldsymbol{\Psi = \frac{1}{M} \sum_{i=1}^{M} \Gamma_i}$$

A. 2.2. Image différence: [11][34]

$$\boldsymbol{\Phi_i = \Gamma_i - \Psi} \qquad \boldsymbol{i \in \{1, 2, \ldots, M\}}$$

A. 2.3. Matrice de covariance : [11][34]

$$\boldsymbol{C = \sum_{i=1}^{M} \Phi_i \Phi_i^T = AA^T}$$

$$\boldsymbol{A = concat(\Phi_1 , \Phi_2 , \ldots, \Phi_M) = [\, \Phi_1 , \Phi_2 , \ldots, \Phi_M]}$$

A. 2.4. Valeur propres et vecteurs propres : [34]

$$\boldsymbol{Av = \lambda v}$$

$\boldsymbol{\lambda}$ **:** Valeur propre.
$\boldsymbol{v}$ **:** Vecteur propre.

A. 2.5. Les valeurs propres et les vecteurs propres de la matrice de covariance : [34].

Il est difficile de calculer les vecteurs propres d'une matrice de taille $N^2 \times N^2$. Donc, on calcul les vecteurs propre da la matrice $L = A^T A$ de dimension $M^2 \times M^2$, qu'ils sont $v_1, v_2, \dots, v_M$ de taille $M \times 1$.

$$\mu_i = A v_i \qquad i \in \{1, 2, \dots, M\}$$

Parce que :
• Considérant les vecteurs propres v_i de $L = A^T A$ donc $A^T A\, v_i = \lambda_i v_i$

• Multipliant les deux cotés d'égalité par A , on obtient $AA^T A v_i = A\lambda_i v_i$

$$AA^T(Av_i) = \lambda_i(Av_i)$$
$$C\ (Av_i) = \lambda_i(Av_i)$$

• Donc, les vecteurs propres de la matrice de covariance: $Av_i \quad i \in \{1, 2, \dots, M\}$

- **Ordonnancement des vecteurs propres :** [11][35][12]

Les vecteurs propres sont ordonnés selon leurs valeurs propres correspondantes à partir de plus grand valeur vers la plus petite (Ordre décroissante).

A. 2.6. Espace visage : [35]

$$Ц = concat(\mu_1, \mu_2, \dots, \mu_M) = [\mu_1, \mu_2, \dots, \mu_M]$$

Les vecteurs propres $\mu_1, \mu_2, \dots, \mu_M$ forment une base : n'importe quelle vecteur Γ ou actuellement $\Phi_i = \Gamma_i - \Psi$, peut être écris comme une combinaison linéaire de vecteurs propres, [35].

$$\Phi_i = \Gamma_i - \Psi = \varphi_1\mu_1 + \varphi_2\mu_2 + \dots + \varphi_{N^2}\mu_{N^2} = \sum_{i=1}^{N^2} \varphi_i \mu_i$$

A. 2.7. Calcul de la dimension de réduction : [35]

Calculer la nouvelle dimension M'

$$Seuil < \frac{\sum_{i=1}^{M'} \lambda_i}{\sum_{i=1}^{M} \lambda_i}$$

Par exemple : Seuil $= \{0.9, 0.95, 0.98, \dots\}$

A. 2.8. Projection dans l'espace visage: [34]

Une image d'un visage peut être projetée dans l'espace visage :

$$\boldsymbol{\Omega_i} = Ц^{\boldsymbol{T}}(\boldsymbol{\Gamma_i} - \boldsymbol{\Psi}) = Ц^{\boldsymbol{T}}\boldsymbol{\Phi_i} \qquad \boldsymbol{i} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{M}\}$$

$$\boldsymbol{\Omega} = \boldsymbol{concat}(\boldsymbol{\Omega_1}, \boldsymbol{\Omega_2}, \dots, \boldsymbol{\Omega_M}) = [\boldsymbol{\Omega_1}, \boldsymbol{\Omega_2}, \dots, \boldsymbol{\Omega_M}]$$

A. 2.9. Reconstruction d'une image: [34]

$\boldsymbol{\Gamma}$ une image, $\boldsymbol{\Gamma'}$ est l'image reconstruite.

$$\boldsymbol{\Gamma'} = Ц * \boldsymbol{\Omega'} + \boldsymbol{\Psi}$$

$$\boldsymbol{\Omega'} = Ц^{\boldsymbol{T}}(\boldsymbol{\Gamma'} - \boldsymbol{\Psi}) = Ц^{\boldsymbol{T}}\boldsymbol{\Phi'}$$

A. 2.10. Rapport d'erreur de reconstruction: [11]

$$\boldsymbol{Rebuild_error_ratio} = \frac{||\boldsymbol{\Gamma'} - \boldsymbol{\Gamma}||}{||\boldsymbol{\Gamma}||}$$

A. 2.11. Distance entre test image et image reconstruite : [34]

Distance entre l'image de test $\boldsymbol{\Gamma}$ et l'image reconstruite $\boldsymbol{\Gamma'}$ de l'espace visage.

$$\boldsymbol{\varepsilon'} = ||\boldsymbol{\Gamma} - \boldsymbol{\Gamma'}|| \qquad \boldsymbol{i} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{M}\}$$

Distance euclidienne $\boldsymbol{\varepsilon_i}$ est la distance de $\boldsymbol{\Omega}$ à partir de chaque classe visage $\boldsymbol{\Omega_i}$

$$\boldsymbol{\varepsilon_i} = ||\boldsymbol{\Omega'} - \boldsymbol{\Omega_i}|| \qquad \boldsymbol{i} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{M}\}$$

A. 2.12. La distance seuil: [34]

La distance seuil $\boldsymbol{\theta}$ est la moitié de la plus grand distance entre chaque deux image visages.

$$\boldsymbol{\theta} = \frac{\mathbf{1}}{\mathbf{2}}\, \boldsymbol{max}\{||\boldsymbol{\Omega_i} - \boldsymbol{\Omega_j}||\} \qquad (\boldsymbol{i} \neq \boldsymbol{j})\ \ \boldsymbol{and}\ \ \boldsymbol{i}, \boldsymbol{j} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{M}\}$$

A. 2.13. Classification : [11]

$\boldsymbol{\Omega'}$: projection de l'image de test $\boldsymbol{\Gamma'}$ dans l'espace visage.
$\boldsymbol{\Omega_i}$: projection de l'image originale $\boldsymbol{\Gamma_i}$ (correspondante à $\boldsymbol{\Gamma'}$) dans l'espace visage.
$\boldsymbol{\theta}$: la distance seuil.

- Face connue

$$\boldsymbol{\theta} \geq \frac{||\boldsymbol{\Omega'} - \boldsymbol{\Omega_i}||}{||\boldsymbol{\Omega_i}||}$$

- Face inconnue

$$\boldsymbol{\theta} \leq \frac{||\boldsymbol{\Omega'} - \boldsymbol{\Omega_i}||}{||\boldsymbol{\Omega_i}||}$$

Il y a quatre possibilités pour une image de test :

1. Proche de l'espace visage, proche de la classe visage, (individu connu).
2. Proche de l'espace visage, n'est pas proche d'une classe visage, (individu inconnu).
3. Distant de l'espace visage, proche de la classe visage, (n'est pas une image visage), (Classification fausse).
4. Distant de l'espace visage, n'est pas proche de la classe visage, (N'est pas une image visage).

A. 3. Analyse en composantes Principales (PCA) algorithme : [34][35]

1. Suppose $\boldsymbol{M}$ vecteurs $(\boldsymbol{N \times 1})$.
2. Calcule de la moyenne $\boldsymbol{\Psi}$ $(\boldsymbol{N \times 1})$ de tous les vecteurs.
3. Calcule de la différence $\boldsymbol{\Phi_i}$ $(\boldsymbol{N \times 1})$ de chaque vecteur.
4. Calcule de la matrice $\boldsymbol{L}$ $(\boldsymbol{M \times M})$.
5. Calcule les vecteurs propres $\boldsymbol{v_i}$ $(\boldsymbol{M \times 1})$ et les $\boldsymbol{M}$ valeurs propres $\boldsymbol{\lambda_i}$ de $\boldsymbol{L}$.
6. Calcule de vecteurs propres $\boldsymbol{\mu_i}$ $(\boldsymbol{N \times 1})$ de $\boldsymbol{C}$, les $\boldsymbol{M}$ valeurs propres sont $\boldsymbol{\lambda_i}$ of $\boldsymbol{L}$.
7. Ordonner les vecteurs propres $\boldsymbol{\mu_i}$ dans l'ordre descendant de leurs valeurs propres $\boldsymbol{\lambda_i}$.
8. Calcule la nouvelle dimension $\boldsymbol{M'} < M \ll N$.
9. Choisi $\boldsymbol{M'}$ vecteurs propres avec les valeurs propres les plus grands.
10. Réduire la dimension par laisser seulement $\boldsymbol{M'}$ termes de :
    $\boldsymbol{\mu_i}$ $(\boldsymbol{N \times 1})$ et $\boldsymbol{\Phi_i}$ $(\boldsymbol{N \times 1})$.
    $\boldsymbol{\mu}$ $(\boldsymbol{N \times M'})$ et $\boldsymbol{\Phi}$ $(\boldsymbol{N \times M})$.
11. Calcule de la projection $\boldsymbol{\Omega_i}$ $(\boldsymbol{M' \times 1})$ et forme l'espace visage $\boldsymbol{\Omega}$ $(\boldsymbol{M' \times M})$.

Théorème :

[…] La meilleur petite dimension de l'espace peut être déterminé par les meilleurs vecteurs propres (les vecteurs propres correspondant aux valeurs propre les plus grandes de la matrice de covariance), aussi sont appelés « Composantes Principales », […], [35].

Remarque :

La réduction de dimension prend seulement en considération le nombre de vecteurs propres.

A. 4. Extraction des traits par PCA

Pour un système de reconnaissance de visage, on peut utiliser l'Analyse en Composante Principale pour l'extraction des traits sans perte d'information.

Dans le domaine de la reconnaissance de visage, on forme une base des images pour des individus connus, et puis on choix un ensemble d'apprentissage. Le même algorithme PCA au dessus est appliqué pour extraire les caractéristiques d'apprentissage (de référence) et les caractéristiques de test. À la fin de l'étape d'apprentissage on passe à l'étape d'authentification ou bien l'étape de test de la reconnaissance des visages pour vérifier la performance du système.

L'image suivante représente un exemple d'ensemble de visages d'apprentissage et leurs visages propres correspondant :

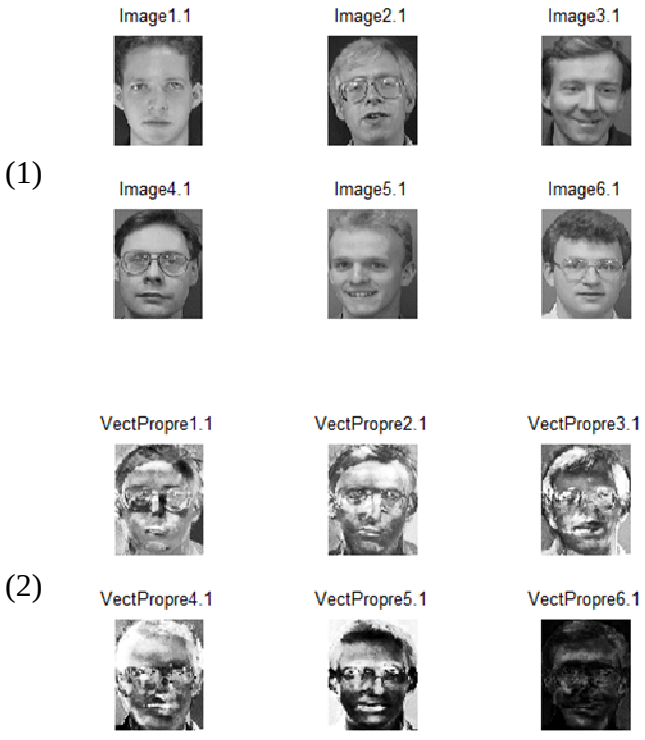


Figure 46 : Exemple, (1) Visages d'apprentissage, (2) Visages propres.

Annexe B :

Chiffrement Standard Avancé (CSA)

B. 1. Conversion en hexadécimal

Le texte binaire (en clair) à codé et la clé en binaire doivent être convertis en hexadécimal selon le tableau suivant, le codage se fait quatre bits par quatre en débutant par le bit le plus à gauche, [36]:

hexadécimal	0	1	2	3	4	5	6	7
binaire	0000	0001	0010	0011	0100	0101	0110	0111

hexadécimal	8	9	a	b	c	d	e	f
binaire	1000	1001	1010	1011	1100	1101	1110	1111

Le texte binaire (en clair) à codé doit être découpé comme suivant, [36] :

Texte $\boldsymbol{S}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	.	.	120	.	127
Bits	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	.	.	7	.	0
Octets	1								2								.	.	16		
State	S_1								S_2								.	.	S_{16}		

S_1	S_5	S_9	S_{13}
S_2	S_6	S_{10}	S_{14}
S_3	S_7	S_{11}	S_{15}
S_4	S_8	S_{12}	S_{16}

La table « State ».

La clé en binaire doit être découpée comme suivant, [36] :

Clé $\boldsymbol{C}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	.	.	120	.	127
Bits	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	.	.	7	.	0
Octets	1								2								.	.	16		
Clé	C_1								C_2								.	.	C_{16}		

C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}
C_4	C_8	C_{12}	C_{16}

La table « Clé ».

Exemple :

Texte $\boldsymbol{S}$	0	1	0	1	0	0	1	1	0	0	0	1	1	0	1	0	.	.	1	.	1
Bits	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	.	.	1	.	0
Octets	Octet 1 = 0101,0011								Octet 2 = 0001,1010								.	.	Octet 16		
State	$S_1 = 53$								$S_2 = 1a$								.	.	S_{16}		

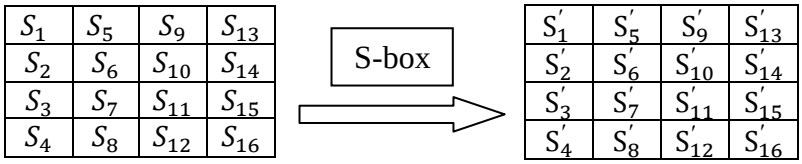
B. 2. Nombre de tours

Le nombre de tours se varie selon le tableau suivant, [36]:

	Longueur de la clé	Longueur du texte	Nombre de tours
AES-128	16 octets	16 octets	10
AES-192	24 octets	16 octets	12
AES-256	32 octets	16 octets	14

B. 3. Substitution de la table « state »

La substitution est réalisée selon l'exemple au dessus, en utilisant S-box, [36][1.15] :



Substitution des octets

Par exemple :

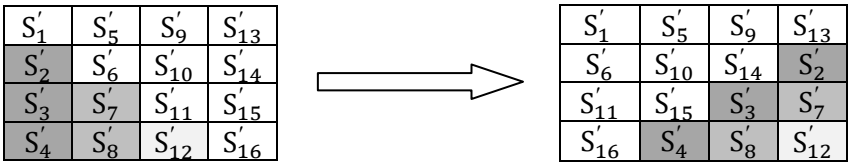
$S_1 = \{5a\}$ donc $S'_1 = \{be\}$

		y															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
x	**0**	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

La table de substitution S-Box.

B. 4. Rotation des colonnes

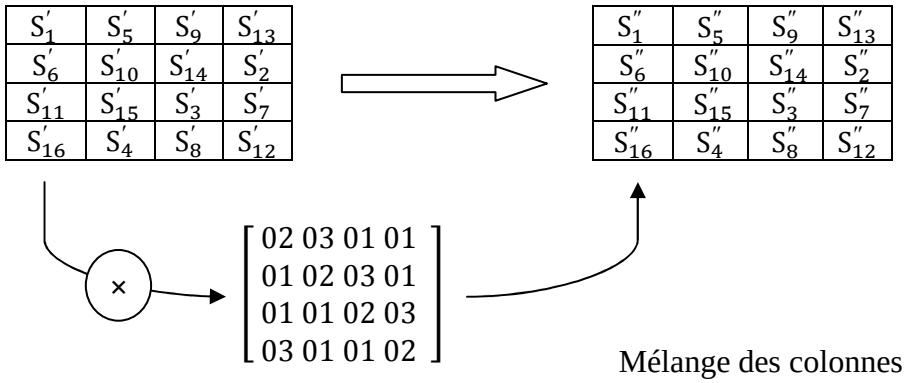
La rotation des lignes est un décalage circulaire à gauche, [36][1.15] :



Rotation des colonnes

B. 5. Mélange des colonnes

Le mélange des colonnes est la multiplication de chaque colonne de la matrice « State » par une matrice constante, [36][1.15] :



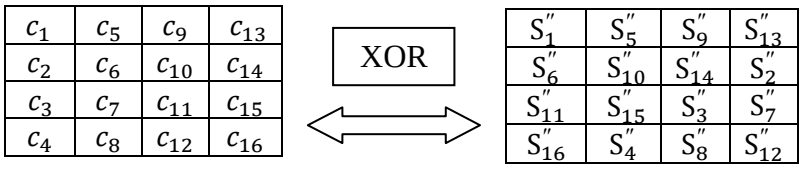
Mélange des colonnes

Les calculs sont réalisés pour chaque colonne par la formule :

$$\begin{bmatrix} S''_1 \\ S''_6 \\ S''_{11} \\ S''_{16} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} S'_1 \\ S'_6 \\ S'_{11} \\ S'_{16} \end{bmatrix}$$

B. 6. Ajout de la clé du tour

Une opération binaire bit à bit est effectuée entre la table « State » et « la clé », [36][1.15].



Ajout de la clé du tour

B. 7. Algorithme d'expansion de la clé

$Debut$
$Nt = 10$; $// \ nombre \ de \ tours.$
$Nk = 4$; $// \ nombre \ d'octets \ par \ ligne.$
$i = 4$;
$ExpCle = Cle$;
$Tant \ que \ (i \ < \ Nk \ * (Nt + 1))$
$Temp \ = \ ExpCle(i, :)$;
$ShiftRows(Temp)$; $// \ (un \ seul \ octet)$
$SubBytes(Temp)$;
$Xor_Temp = AddMConst(Temp, MConst)$; $// \ (par \ condition)$
$ExpCle(i) \ = \ ExpCle(i - Nk) \ XOR \ Xor_Temp$;
$i = i + 1$;
$Fin \ Tant \ Que$;
Fin ;

, [36].

Remarque :
$SubBytes$: substitution des octets à l'aide de la table S_box.
$ShiftRows$: décalage circulaire des octets.
$MixColumns$: Mélange des colonnes par un produit.
$AddRoundKey$: l'ajout de la clé du tour par l'opérateur XOR.

B. 8. Algorithme de codage

$Debut$
$XOR \ (State, cle)$;
$Pour \ i = \ 1$ à $10 \ faire$
$SubBytes(state)$;
$ShiftRows(state)$;
$MixColumns(state)$;
$AddRoundKey(state, cleTour)$;
$Fin \ pour$;
$SubBytes(state)$;
$ShiftRows(state)$;
$AddRoundKey(state, cleTour)$;
Fin ;

, [36].

B. 9. La matrice constante, [36]

Les valeurs de la matrice constante sont :

```
MatriceConstante= (01000000, 02000000, 04000000, 08000000, 10000000,
                   20000000, 40000000, 80000000, 1b000000, 36000000)
```

B. 10. La clé après l'expansion

```
-----------------------------------------------------------------
La matrice "CleTour" après l'expansion de la clé initiale
-----------------------------------------------------------------

CleTour =
```

2b7e1516 28aed2a6 abf71588 09cf4f3c	Clé Originale
A0FAFE17 88542CB1 23A33939 2A6C7605	Clé du tour 1
F2C295F2 7A96B943 5935807A 7359F67F	Clé du tour 2
3D80477D 4716FE3E 1E237E44 6D7A883B	Clé du tour 3
EF44A541 A8525B7F B671253B DB0BAD00	Clé du tour 4
D4D1C6F8 7C839D87 CAF2B8BC 11F915BC	Clé du tour 5
6D88A37A 110B3EFD DBF98641 CA0093FD	Clé du tour 6
4E54F70E 5F5FC9F3 84A64FB2 4EA6DC4F	Clé du tour 7
EAD27321 B58DBAD2 312BF560 7F8D292F	Clé du tour 8
AC7766F3 19FADC21 28D12941 575C006E	Clé du tour 9
D014F9A8 C9EE2589 E13F0CC8 B6630CA6	Clé du tour 10

Références
Et
Bibliographie

Références et Bibliographie

[1] . Wikipédia, l'encyclopédie libre, http://fr.wikipedia.org/

[1.1]. « http://fr.wikipedia.org/w/index.php?title=Biométrie&oldid=87891741 »

[1.2]. « http://fr.wikipedia.org/w/index.php?title=Soft_biometrics&oldid=87776090 »

[1.3]. « http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=541003846 »

[1.4]. « http://fr.wikipedia.org/w/index.php?title=osurveillance&oldid=90170153 »

[1.5]. « http://fr.wikipedia.org/w/index.php?title=Robotique&oldid=90209531 »

[1.6]. « http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Citer&page=Liste_des_muscles_du_corps_humain&id=90500209 »

[1.7]. « http://fr.wikipedia.org/w/index.php?title=Facial_action_coding_system&oldid=88604461»

[1.8]. « http://fr.wikipedia.org/wiki/Paul_Ekman »

[1.9]. « http://fr.wikipedia.org/w/index.php?title=Détection_de_visage&oldid=81719034 »

[1.10]. « http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Citer&page=Corps_commutatif&id=93774825 »

[1.11]. « http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Citer&page=Corps_fini&id=96052928 »

[1.12]. « http://en.wikipedia.org/w/index.php?title=Special:Cite&page=Error_detection_and_correction&id=541959458»

[1.13]. « http://fr.wikipedia.org/wiki/Code_correcteur»

[1.14]. « http://fr.wikipedia.org/w/index.php?title=Code_de_Reed-Solomon&oldid=93170136 »

[1.15]. Advanced Encryption Standard.
« http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard»

[2] . « http://www.securiteinfo.com/La biométrie », 21 Janvier 2002.

[3] . T. Scheidat, C. Vielhauer, *Analyzing a multimodal biometric system using real and virtual users*, Germany, SPIE-IS&T/ Vol. 6505 650512-1, 2007.

[4] . Biométrie (l'histoire), Cité des sciences et de l'industrie, 2005.
« http : www.cite-sciences.fr »

[5] . J. Dugelay dans une présentation, *Reconnaissance Faciale, De La biométrie statique à la biométrie dynamique*, IDEM MAGAZINE, 150 RUE LEGENDRE, 75017 PARIS, N° de page : 14-15, Avril 2010, Mensuel.

[6] . Microsoft Encarta 2009. 1993-2008 Microsoft Corporation.

[7] . S. GUERFI ABABSA, *Authentification d'individus par reconnaissance de Caractéristiques biométriques liées aux visages 2D/3D*, thèse 2008.

[8] . G.C. Chandran. J, Rajesh. R.S, *Performance Analysis of Multimodal Biometric System Authentication*, IJCSNS 290 International Journal of Computer Science and Network Security, VOL.9, No.3, March 2009.

[9] . *Communications of the ACM*, Pages 90-98, February 2000/Vol. 43, No. 2.

[10] . N. MORIZET, *Reconnaissance Biométrique par Fusion Multimodale du Visage Et de l'Iris*, Paris, thèse 2009.

[11] . I. ATALAY, *Face Recognition using EigenFaces*, thèse, Janvier 1996.

[12] . H. Rara, *Face Recognition (biometrics).*

[13] . W. Hizem, Capteur Intelligent pour la Reconnaissance de Visage, Paris, thèse 2009.

[14] . « http://www.gemadec.com/langue/index.php/fr/site-map/
/identification-securite-a-biometrie »

[15] . B. Rossion _C&P *Cerveau&Psycho* - N° 25.

[16] . ISIR institut des systèmes intelligent et de robotique, *Biométrie du visage.*

[17] . A. R. Calvo, Francesc Tarrés Ruiz, Jürgen Rurainsky and Peter Eisert (2008). *2D-3D Mixed Face Recognition Schemes*, Recent Advances in Face Recognition, Kresimir Delac, Mislav Grgic and Marian, Stewart Bartlett (Ed.),
ISBN: 978-953-7619-34-3, InTech, Available from:
http://www.intechopen.com/books/recent_advances_in_face_recognition/
/2d- 3d_mixed_face_recognition_schemes

[18] . http://moreas.blog.lemonde.fr/... /Notre visage: l'enjeu biométrique de demain/

[19] . Y. Feng, P.Yuen and A.Jain, A Hybrid Approach For Face Template Protection.

[20] . Anil K. Jain, K. Nandakumar, and A. Nagar. *Biometric Template Security*, USA, Décembre 2007.
Review Article in Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416, 17 pages, doi:10.1155/2008/579416.

[21] . D. Hartung, *Template Protection for PCA-LDA-based 3D Face Recognition System*, 2007.

[22] . A. Juels1 and M. Sudan2. *A Fuzzy Vault Scheme*, USA.

[23] . U. Uludag1, Sh. Pankanti2, Anil K. Jain1, *Fuzzy Vault for Fingerprints.*

[24] . J. Merkle, M. Niesing, M. Schwaiger, H. Ihmor, U. Korte, *Security Capacity of the Fuzzy Fingerprint Vault*, Germany. International Journal on Advances in Security, vol 3 no 3 & 4, pp 146-168, year 2010.
http://www.iariajournals.org/security/

[25] . Y. Wang, K.N. Plataniotis, *Fuzzy vault for face based cryptographic key generation*, Canada . Biometrics Symposium, 2007.

[26] . X. Zhou, A. Kuijper and Ch. Busch. *Template Protection for 3D Face Recognition, Face Recognition*, Milos Oravec (Ed.), 2010. ISBN: 978-953-307-060-5, InTech, Available from: http://www.intechopen.com/books/face-recognition/template-protection-for-3d-face-recognition

[27] . Y. Wang, K.N. Plataniotis. *Fuzzy vault for face based cryptographic key generation*, Canada, Proceedings of the IEEE, Biometrics Symposium, 1-4244-1549-7/07, 2007.

[28] . H. Chabanne, *C2 (Codage, Cryptographie) et Biométrie*, 2008.

[29] . M. van der Veen, Tom Kevenaar, Geert-Jan Schrijen, Ton H. Akkermans, Fei Zuo. *Face Biometrics with Renewable Templates*.

[30] . X. Zhou, *Template Protection and its Implementation in 3D Face recognition Systems*, Germany.

[31] . H. Lu, K. Martin, Francis Bui, K. N. Plataniotis, D. Hatzinakos, *Face recognition with biometric encryption for privacy-enhancing self-exclusion*, Canada.

[32] . Help Matlab.

[33] . S. Yoo, Dong-Gyu Sim, Young-Gon Kim and Rae-Hong Park (2011). *Performance Comparison of Principal Component Analysis-Based Face Recognition in Color Space*, Advanced Biometric Technologies, Dr. Girija Chetty (Ed.), ISBN: 978-953-307-487-0, InTech, Available from: http://www.intechopen.com/books/advanced-biometric-chnologies/performance-Comparison-of-principal-component- analysis-based-face-recognition-in-color-space

[34] . P. Buddharaju, *Face Recognition using PCA (Eigenfaces) and LDA (Fisherfaces).*

[35] . *Principal Components Analysis (PCA).*

[36] . *ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information, Processing Standards Publication 197 (fips-197), November 26, 2001. http://csrc.nist.gov/publications/

Références d'Images

[-1-] . Figure 1 : Iris.
« http://ts1.mm.bing.net/th?id=H.4575193510773044&pid=15.1 »

[-2-] . Figure 2 : Différentes Images d'Iris.

[-2.1-]. « http://fr.wikipedia.org/wiki/Iris_%28anatomie%29 »

[-2.2-]. « http://fr.wikipedia.org/wiki/Reconnaissance_de_l%27iris »

[-2.3-]. « http://www.securiteinfo.com/La biométrie », 21 Janvier 2002.

[-3-] . Figure 3 : Empreinte de la main.
S. Yoo, D. Sim, Y. Kim and R. Park (2011). *Performance Comparison of Principal Component Analysis-Based Face Recognition in Color Space*, Advanced Biometric Technologies, Dr. Girija Chetty (Ed.), ISBN: 978-953-307-487-0, InTech: http://www.intechopen.com/books/advanced-biometric-technologies/ performance-Comparison-of-principal-component- analysis-based-face-recognition-in-color-space

[-4-] . Figure 4 : Minuties de l'empreinte [-4.1-], empreinte [-4.2-].

[-4.1-]. « http://fr.wikipedia.org/wiki/Empreinte_digitale »

[-4.2-]. « http://www.securiteinfo.com/La biométrie », 21 Janvier 2002.

[-5-] . Figure 5 : Doigt [-5.1-], Empreinte du doigt [-5.2-].

[-5.1-]. « http://fr.wikipedia.org/wiki/Empreinte_digitale »

[-5.2-]. « http://tpepolice-scientifique.e-monsite.com/pages/i-preuves-materielles-et-etudes-realisees/empreintes-digitales.html »

[-6-] . Figure 6 : Rétine.
« http://fr.wikipedia.org/w/index.php?title=R%C3%A9tine&oldid=92799105 ».

[-7-] . Figure 7 : Géométrie de la main.
« http://archives.universcience.fr/francais/ala_cite/expositions/biometrie/nonvoyants/programme_details_6_3.htm »

[-8-] . Figure 8 : ADN [-8.1-], Molécule d'ADN [-8.2-].

[-8.1-]. « http://www.sciencepresse.qc.ca/revue-presse/2013/03/20/ladn-revele-nouvelles- surprises »

[-8.2]. Microsoft Encarta 2009. 1993-2008 Microsoft Corporation.

[-9-] . Figure 9 : Frappe au clavier.
« http://fr.evilox.com/url/vitesse-frappe-clavier »

[-12-] .Figure 12 : Composantes d'un système biométrique.
« http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=541003846 »

[-13-] . Figure 13 : Plan du processus général d'authentification biométrique.

[-13.1-]. T. Scheidat, C. Vielhauer, *Analyzing a multimodal biometric system using real and virtual users*, Germany, SPIE-IS&T/ Vol. 6505 650512-1, 2007.

[-13.2-]. *Communications of the ACM*, Pages 90-98, February 2000/Vol. 43, No. 2.

[-14-] . Figure 14 : Quelques systèmes biométriques.

[-14.1-]. « http://fr.wikipedia.org/wiki/Empreinte_digitale »

[-14.2-]. « http://www.paperblog.fr/5809099/natixis-teste-la-signature-biometrique/ »

[-14.3-]. « http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Citer&page=Vid%C3%A9osurveillance&id=90170153»

[-14.4-]. « http://www.citoyens.com/wp-content/uploads/2011/08/Piscine-Biom%C3%A9trique.jpg »

[-14.5-]. « http://ts1.mm.bing.net/th?id=H.5066408856651600&pid=15.1 »

[-15-] .Figure 15 : Régions de reconnaissance des visages chez les humains.
B. Rossion _C&P *Cerveau&Psycho* - N° 25.

[-16-] . Figure 16 : Détection de visage.
« http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Citer&page=D%C3%A9tection_d%27objet&id=90752167»

[-17-] . Figure 17 : Modèle de forme active 2D.
ISIR institut des systèmes intelligent et de robotique, *Biométrie du visage*.

[-18-] . Figure 18 : Modèle de forme active 3D.
ISIR institut des systèmes intelligent et de robotique, *Biométrie du visage*.

[-19-] . Figure 19 : Modèle complet 2D.
A. R.Calvo, F.Ruiz, J.Rurainsky and P.Eisert (2008). *2D-3D Mixed Face Recognition Schemes*, Recent Advances in Face Recognition, Kresimir Delac, Mislav Grgic and Marian, Stewart Bartlett (Ed.), ISBN: 978-953-7619-34-3, InTech, Available from:
http://www.intechopen.com/books/recent_advances_in_face_recognition/
/2d- 3d_mixed_face_recognition_schemes

[-20-] . Figure 20 : Modèle complet 3D.
A. R.Calvo, F.Ruiz, J.Rurainsky and P.Eisert (2008). *2D-3D Mixed Face Recognition Schemes*, Recent Advances in Face Recognition, Kresimir Delac, Mislav Grgic and Marian, Stewart Bartlett (Ed.), ISBN: 978-953-7619-34-3, InTech, Available from:
http://www.intechopen.com/books/recent_advances_in_face_recognition/
/2d- 3d_mixed_face_recognition_schemes

[-21-] . Figure 21 : Autres modèles complets 3D.
A. R.Calvo, F.Ruiz, J. Rurainsky and P. Eisert (2008). *2D-3D Mixed Face Recognition Schemes*, Recent Advances in Face Recognition, Kresimir Delac, Mislav Grgic and Marian, Stewart Bartlett (Ed.), ISBN: 978-953-7619-34-3, InTech, Available from:
http://www.intechopen.com/books/recent_advances_in_face_recognition/
/2d- 3d_mixed_face_recognition_schemes

[-22-] . Figure 22 : Approches de protection de la base de données biométrique.
Y.Feng, P.Yuen and A.K Jain. *A Hybrid Approach for Face Template Protection*, USA.

[-23-] . Figure 23 : Catégories des modèles de protection.
Anil K. Jain, K.Nandakumar, and A. Nagar. *Biometric Template Security*, USA, December 2007.
Review Article in Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416, 17 pages, doi:10.1155/2008/579416.

[-24-] . Figure 24 : Coffre Flou.
Anil K. Jain With A. Nagar & K. Nandakumar, *Adapting Biometric Representations for Cryptosystems*, « http://biometrics.cse.msu.edu ».

[-25-] . Figure 25 : Plan des données assistantes.
X. Zhou, A. Kuijper and C. Busch. *Template Protection for 3D Face recognition, Face Recognition*, Milos Oravec (Ed.), 2010. ISBN: 978-953-307-060-5, In Tech, Available from: http://www.intechopen.com/books/face-recognition/template-protection-for-3d-face-recognition.

[-27-] . Figure 27 : Redondance et fiabilité.
« http://fr.wikipedia.org/wiki/Code_correcteur »

[-28-] . Figure 28 : Code correcteur d'erreurs.
Help Matlab.