الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة الشهيد الشيخ العربي التبسي - تبسة
Université Echahid Cheikh Larbi Tébessi – Tébessa
Faculté des Sciences et de la Technologie
Département d'Électronique et de Communications

MEMOIRE

جامعة الشهيد الشيخ العربي التبسي تبسة
قسم الالكترونيك والاتصالات
كلية العلوم والتكنولوجيا

Présenté pour l'obtention du **diplôme** de **Master Académique**

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : Ania Si Said et Safoua Maallem

THEME

Optimisation d'un système biométrique sécurisé à l'aide de filtres orientés

Présenté et évalué, le 09/06/2026 , par le jury composé de :

Nom et prénom		Grade	Qualité
M.	Karim Ferroudji	MCB	Président
M.	Abdallah Meraoumia	Prof.	Rapporteur
M.	Lotfi Houam	MCB	Examinateur

Promotion : 2025/2026

الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة الشهيد الشيخ العربي التبسي – تبسة
Université Echahid Cheikh Larbi Tébessi – Tébessa
Faculté des Sciences et de la Technologie
Département d'Électronique et de Communications

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : Ania Si Said et Safoua Maallem

THEME

Optimisation d'un système biométrique sécurisé à l'aide de filtres orientés

Présenté et évalué, le 09/06/2026 , par le jury composé de :

Nom et prénom		Grade	Qualité
M.	Karim Ferroudji	MCB	Président
M.	Abdallah Meraoumia	Prof.	Rapporteur
M.	Lotfi Houam	MCB	Examinateur

Promotion : 2025/2026

من قال: «أنا لها» نالها، وأنا لها وإن أبت رغماً عنها أتيتُ بها.
لم تكن الرحلة قصيرة، ولا ينبغي لها أن تكون، ولم يكن الحلم قريبًا ولا الطريق محفوفًا بالتسهيلات، لكنني فعلتها ونلتها.

إلى الذي زيّن اسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل، من علّمني أن الدنيا كفاح وسلاحه العلم والمعرفة، داعمي الأول في مسيرتي وسندي وقوتي وملاذي بعد الله، إلى فخري واعتزازي ...
(أبي)

وإلى من جعل الله الجنة تحت أقدامها، واحتضنني قلبها قبل يديها، وسهّلت لي الشدائد بدعائها، إلى القلب الحنون والشمعة التي أضاءت لي الليالي المظلمات، سر قوتي ونجاحي...
(أمي)

وإلى ضلعي الثابت وأمان أيامي، إلى من شددت عضدي بهم فكانوا لي ينابيع أرتوي منها، إلى خيرة أيامي وصفوتها، إلى قرة عيني...
(إخوتي وأختي)

وإلى التي شاركتني تعب هذا العمل قبل فرحته، وكانت خير سند ورفيقة طوال هذا الطريق، فخففت عني الكثير من التعب والضغط، وسيبقى هذا العمل شاهدًا على أجمل لحظات التعاون والصبر والاجتهاد التي جمعتنا ...
(صديقتي ورفيقة مشواري صفوى)

ولكل من كان عونًا وسندًا في هذا الطريق، للأصدقاء الأوفياء ورفقاء السنين، ولأصحاب الشدائد والأزمات، شكرًا لكنّ على المحبة والوفاء والدعم الصادق ...
(سماح وعليا)

إلى القلب الحنون الذي ملأ حياتي حبًا ودفئًا وطمأنينة، كم تمنيتُ وجودكِ بجانبي لتشاركي فرحتي بهذا الإنجاز، لكنكِ رحلتِ عن عيني ولم ترحلي عن قلبي، فما زالت ذكرياتكِ الجميلة تسكن روحي ويكبر الحنين إليكِ يومًا بعد يوم، رحمكِ الله بقدر طيبة قلبكِ ونقاء روحكِ، وجعل قبركِ روضةً من رياض الجنة ...
(جدتي رحمها الله)

أهديكم جميعًا هذا الإنجاز وثمرة نجاحي التي طالما تمنيتها، وها أنا اليوم أقطف أول ثمارها بفضل الله سبحانه وتعالى، فالحمد لله على ما وهبني .

Anía SI SAID

بِسْمِ اللهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ﴾

إلى كلٍّ من أنار لي عتمة الطريق وترك في روحي أثرًا لا يُنسى، إلى أساتذتي الذين كانوا الضوء حين خفت النور، والأمل حين ضاق الطريق، غرستم في داخلي حبَّ العلم حتى صار الحلم واقعًا، لكم مني دعاءٌ لا ينقطع وامتنانٌ لا يزول.

إلى من قال الله تعالى فيهما :

﴿وَقُلْ رَبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا﴾

إلى من كلَّله الله بالهيبة والوقار، إلى الذي زيَّن اسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل، إلى من علَّمني أن الدنيا كفاح وسلاحها العلم والمعرفة، إلى من غرس في روحي مكارم الأخلاق، داعمي الأول في مسيرتي، وسندي وقوتي بعد الله .

(والدي الحبيب)

إلى من جعل الله الجنة تحت أقدامها، إلى اليد الخفية، والقلب الحنون، ونور دربي بدعائها... يا من كنتِ سندي في كل خطوة، ومعلمتي الأولى، وأفخر أنكِ معلمة تحمل رسالة العلم بكل إخلاص، فكنتِ قدوةً لي في العطاء والصبر...

(والدتي الحبيبة)

إلى ضلعي الثابت، وأمان أيامي، وملهمَي نجاحي، إلى من شددتُ عضدي بهما فكانا لي ينابيع أرتوي منها، إلى خيرة أيامي وصفوتها، إلى قرة عيني.

(أخي وأختي)

إلى من رحل عن هذه الدنيا وبقي أثره حيًّا في قلبي لا يغيب، إلى من تجلَّى كرمه في اسمه ومعناه حضورًا واهتمامًا وحنانًا، أسأل الله أن يتغمَّدك بواسع رحمته، وأن يجعل قبرك روضةً من رياض الجنة، ويجزيك عنّي خير الجزاء...

(عمي عبد الكريم)

إلى من كنَّ لي سندًا جميلًا ودعمًا صادقًا في مسيرتي، وكانت كلماتهن دائمًا بلسمًا يشجّعني ويقوّيني على الاستمرار... شكرًا لقلوبكن الحنونة التي لا تبخل بالدعاء والمحبة...

(خالاتي الغاليات وبناتهن)

إلى من كانت معي في هذا الطريق، نحمل التعب بصمتٍ جميل، ونتقاسم اللحظات الصعبة كأننا روحٌ واحدة في جسدين، لم يكن الطريق سهلًا ولا الأيام خفيفة، لكن وجودكِ جعل لكل تعبٍ معنى، ولكل جهدٍ قيمة. فكلما أثقلنا الإرهاق خفَّفته ابتسامتكِ، وكلما ضاق بنا الوقت وسَّعته روح التعاون بيننا، حتى صار العمل رحلةً مليئة بالتحدي والأمل. ومع الوصول إلى هذه اللحظة، أدركتُ أن النجاح لم يكن مجرد نتيجة، بل كان ثمرة صبرٍ مشترك وجهدٍ متقاسم، فصار أخفَّ وأجمل لأننا عشنا تفاصيله معًا من البداية إلى النهاية. شكرًا لكِ لأنكِ كنتِ السند والرفيقة التي لا تُعوَّض .

(آنيا)

إلى من كنتنَّ لي كتفًا لا يميل، وقلبًا لا يتغير، وضوءًا لا ينطفئ في عتمة الأيام، إلى من وقفن بجانبي في لحظات الضعف قبل الفرح، وشاركنني التعب قبل النجاح، وكنَّ لي سندًا حقيقيًا في كل خطوة، فبكنَّ يهون الصعب ويجمل الطريق، وبوجودكنَّ يزهر الأمل رغم كل الظروف. شكرًا لكنَّ من القلب على الوفاء والمحبة والدعم الذي لا يُقدَّر بثمن .

(سماح وعليا)

أهديكم هذا الإنجاز وثمرة نجاحي التي طالما تمنيتها، وها أنا اليوم أقطف أول ثمارها، راجيةً من الله سبحانه وتعالى أن ينفعني بما علَّمني، وأن يعلِّمني ما أجهل، وأن يجعله حجةً لي لا عليَّ .

Safoua MAALLEM

Remerciement

Nous exprimons nos plus sincères remerciements et notre profonde gratitude aux éminents Professeurs Abdallah Meraoumia et Dr Yacine Belhocine, pour leur encadrement scientifique de grande qualité, leurs conseils précieux et leur accompagnement constant tout au long de ce travail. Leur rigueur académique, leur patience et leur soutien continu ont constitué un véritable pilier qui nous a permis de surmonter les difficultés et de mener ce projet à terme avec persévérance et détermination.

Nous adressons également notre profonde reconnaissance à notre chère famille, qui a été notre premier soutien et notre refuge inestimable. Leur amour, leurs sacrifices et leurs encouragements constants ont été une source essentielle de force et de motivation tout au long de notre parcours.

Nous tenons enfin à remercier l'ensemble de nos enseignants, qui ont contribué de près ou de loin à notre formation académique et personnelle. Par leurs enseignements, leurs conseils et leur bienveillance, ils ont éclairé notre chemin et enrichi notre parcours universitaire.

Ce travail est le fruit de votre soutien, de votre confiance et de votre présence précieuse à nos côtés .

A. Si Said et S. Maallem

Résumé : *Les systèmes biométriques occupent aujourd'hui une place importante dans les domaines de la sécurité et de l'authentification grâce à leur capacité à identifier les individus à partir de caractéristiques physiologiques ou comportementales. Cependant, ces systèmes restent exposés à plusieurs menaces telles que le spoofing, le vol des templates biométriques et les attaques sur les canaux de transmission.*

Ce mémoire présente une étude des systèmes biométriques, de leurs vulnérabilités ainsi que des principales techniques de protection utilisées pour renforcer leur sécurité. Une attention particulière est accordée à la protection des templates biométriques à travers des mécanismes de chiffrement et des méthodes anti-spoofing.

Dans ce contexte, une approche sécurisée est proposée en utilisant les projections spatiales guidées par le chaos, l'optimisation par essaim de particules (PSO) ainsi qu'un schéma de chiffrement adapté à la protection des caractéristiques biométriques. Cette approche vise à améliorer la sécurité, l'intégrité et la robustesse du système face aux différentes attaques.

Mots clés : *Biométrie, Sécurité des systèmes biométriques, Chiffrement, PSO, Chaos, Anti-spoofing, Protection des templates.*

Abstract: *Biometric systems play an important role in security and authentication fields due to their ability to identify individuals using physiological or behavioral characteristics. However, these systems remain vulnerable to several threats such as spoofing, biometric template theft, and transmission channel attacks.*

This dissertation presents a study of biometric systems, their vulnerabilities, and the main protection techniques used to enhance their security. Particular attention is given to biometric template protection through encryption mechanisms and anti-spoofing methods.

In this context, a secure approach is proposed using chaos-guided spatial projections, Particle Swarm Optimization (PSO), and an encryption scheme adapted for biometric feature protection. The proposed approach aims to improve the security, integrity, and robustness of the biometric system against different attacks.

Index term*: Biometrics, Biometric System Security, Encryption, PSO, Chaos, Anti-spoofing, Template Protection.*

ملخص: *تحتل الأنظمة البيومترية مكانة مهمة في مجالات الأمن والمصادقة بفضل قدرتها على التعرف على الأفراد اعتمادًا على الخصائص الفيزيولوجية أو السلوكية. ومع ذلك، تبقى هذه الأنظمة عرضة لعدة تهديدات مثل التزوير، وسرقة القوالب البيومترية، والهجمات التي تستهدف قنوات نقل البيانات.*

يقدم هذا العمل دراسة حول الأنظمة البيومترية، والثغرات الأمنية التي قد تؤثر عليها، بالإضافة إلى أهم تقنيات الحماية المستخدمة لتعزيز أمنها. كما تم التركيز على حماية القوالب البيومترية باستعمال آليات التشفير وتقنيات مكافحة التزوير.

وفي هذا الإطار، تم اقتراح مقاربة آمنة تعتمد على الإسقاطات المكانية الموجهة بالفوضى، وخوارزمية تحسين سرب الجسيمات (PSO)، بالإضافة إلى مخطط تشفير مخصص لحماية الخصائص البيومترية. وتهدف هذه المقاربة إلى تحسين أمن وسلامة وموثوقية النظام البيومتري ضد مختلف الهجمات.

الكلمات المفتاحية : *القياسات الحيوية، أمن الأنظمة البيومترية، التشفير، PSO، الفوضى، مكافحة التزوير، حماية القوالب البيومترية.*

Table des Matières

Introduction Générale 01

Chapitre I : Biométrie et Sécurité de l'Information

Introduction 05

I.1 Sécurité de l'information 05

I.1.1 Définition et objectifs de la sécurité de l'information 05

I.1.2 Confidentialité, intégrité et disponibilité 06

I.1.3 Menaces, vulnérabilités et modèles d'attaque 06

I.2 Techniques de protection de l'information 09

I.2.1 Cryptographie 10

I.2.2 Stéganographie 11

I.2.3 Tatouage numérique 11

I.2.4 Comparaison entre cryptographie, stéganographie et Tatouage 11

I.3 La biométrie 12

I.3.1 Définition et historique de la biométrie 12

I.3.2 Propriétés des caractéristiques biométriques 12

I.4 Modalités biométriques 13

I.4.1 Biométrie physiologique 13

I.4.2 Biométrie comportementale 14

I.5 Architecture et classification d'un système biométrique 15

I.5.1 Etapes d'un système biométrique 16

I.5.2 Phases d'un système biométrique 16

I.6 Système biométrique uni modaux et multimodaux Multimodale 19

I.7 Critères de performance et indicateurs 20

I.8 Vulnérabilités et attaques courantes 21

I.8.1 Attaques sur les capteurs (spoofing) 21

I.8.2 Attaques sur les Template biométriques 22

I.8.3 Attaques sur la communication et les canaux de données 22

I.8.4 Attaques sur les systèmes multimodaux ou distribués 22

Conclusion 22

Chapitre II : Sécurité des systèmes biométriques

Introduction 24
II.1 Biométrie et sécurité 24
II.1.1 Rôle de la biométrie dans l'authentification sécurisée 24
II.1.2 Applications de la biométrie dans la sécurité informatique et physique 24
II.2 Protection des Templates biométriques 25
II.2.1 Vulnérabilités des Template 25
II.2.2 Méthodes de protection 26
II.2.3 Comparaison des méthodes 28
II.3 Sécurité des systèmes biométriques 28
II.3.1 Modèles de menace pour les systèmes biométriques 28
II.3.2 Attaques sur les composants internes 29
II.3.3 Attaques logicielles et attaques par élévation de privilèges 29
II.4 Sécurité des canaux de transmission 30
II.4.1 Transfert de données biométriques 30
II.4.2 Protocoles sécurisés pour la transmission 30
II.4.3 Attaques réseau 31
II.5 Système proposé 32
II.5.1 Sécurité et intégrité des caractéristiques 32
II.5.2 Exigences préliminaires 35
Conclusion 42

Chapitre III : Résultats expérimentaux

Introduction 44
III.1 Base de données 44
III.2 Résultats expérimentaux 44
III.2.1 Configuration du système 45
III.2.2 Protocole d'évaluation 45
III.3 Evaluation du système biométrique 45
III.3.1 Représentation des filtres (PCA et SC) 46
III.3.2 Système non sécurisé 47
III.3.3 Système sécurisé 50
III.3.4 Système Optimisé 51
III.3.5 Système fusionné 53

III.4 Evaluation du système proposé 54
III.4.1 Analyse statistique par histogramme..... 54
III.4.2 Analyse de l'espace des clés..... 55
III.4.3 Analyse de la sensibilité des clés..... 55
III.4.4 Suite de tests d'aléatoire NIST..... 56
Conclusion..... 57
Conclusion générale et perspectives..... 59
Bibliographies..... 62

Liste des Figures

Figures		Page
I.1	La triade CIA de la sécurité de l'information.	6
I.2	Classification des types d'attaques en sécurité de l'information	9
I.3	Exemple de modalités biométriques	12
I.4	trait biométrique : empreintes	13
I.5	Un exemple de l' empreinte palmaire humaine	13
I.6	trait biométrique : visage	14
I.7	trait biométrique : iris	14
I.8	trait biométrique : signature	15
I.9	Enrôlement d'une personne dans le système biométrique	17
I.10	vérification de la personne dans le système biométrique.	18
I.11	Identification de la personne dans le système biométrique	18
I.12	illustration du FRR et du FAR	20
I.13	Graph démonstratif de l'EER	21
I.13	Deux exemples d'attaque sur le capteur biométrique	22
II.1	Schéma conceptuel de l'idéologie de l'attaque de l'homme du milieu	32
II.2	schéma globale de système biométrique	33
II.3	Schéma de génération des projections spatiales chaotiques	38
II.4	Schéma du chiffrement sinusoïdal des caractéristiques	41
III.1	Filtres PDVs-SC et PDVs-PCA de taille 11 × 11 générés à partir d'un ensemble images de veines palmaires.	46
III.2	Évaluation des systèmes non sécurisés à base de filtres PCA	48
III.3	Évaluation des systèmes non sécurisés à base de filtres SC	49
III.4	Évaluation des systèmes non sécurisés les plus performants : analyse des courbes DET et CMC	50
III.5	Comparaison des systèmes sécurisés et non sécurisés les plus performants : analyse de la courbe DET	51

III.6	Courbe de convergence de l'optimisation des paramètres des filtres PDV-PCA et PDV-SC	52
III.7	Comparaison des systèmes sécurisés et optimisés les plus performants : analyse de la courbe DET	53
III.8	Évaluation des system : analyse des courbes DET et CMC	53
III.9	Histogramme des modèles biométriques	54

Liste des tableaux

Table		Page
II.1	Comparaison des principales méthodes de protection des templates biométriques	28
III.1	Analyse de la sensibilité à la clé à l'aide du coefficient de corrélation (%).	56
III.2	Résultats de la suite de tests de hasard du NIST	57

Liste d'abréviation

AFH : Alignment-Free Hashing

AI : Artificial Intelligence

APC / PCA : Analyse en Composantes Principales / Principal Component Analysis

CLAHE : Contrast Limited Adaptive Histogram Equalization

CMC : Cumulative Match Characteristic

CNN : Convolutional Neural Network

DET : Detection Error Tradeoff

EER : Equal Error Rate

FAR : False Acceptance Rate

FRR : False Rejection Rate

HE : Homomorphic Encryption

HOG : Histogram of Oriented Gradients

IoM : Index-of-Max

IoT : Internet of Things

K-SVD : K-Singular Value Decomposition

LAN : Local Area Network

MAE : Mean Absolute Error

MITM : Man-In-The-Middle attack

NIR : Near Infrared

NIST : National Institute of Standards and Technology

OMP : Orthogonal Matching Pursuit

PDV : Patch Decomposition-based Veins

PDV-PCA : Patch Decomposition-based Veins with Principal Component Analysis

PDV-SC : Patch Decomposition-based Veins with Sparse Coding

PolyU : Hong Kong Polytechnic University

PSO : Particle Swarm Optimization

ROI : Region of Interest

RSA : Rivest–Shamir–Adleman

SC : Sparse Coding

SVD : Singular Value Decomposition

SVM : Support Vector Machine

Wi-Fi : Wireless Fidelity

XOR : Exclusive OR

Introduction Générale

Introduction

La sécurité de l'information est devenue un enjeu majeur dans les environnements numériques modernes, caractérisés par une croissance rapide des systèmes informatiques et des échanges de données. Avec l'augmentation des cybermenaces et la sophistication des attaques, les méthodes traditionnelles d'authentification, telles que les mots de passe et les cartes à puce, montrent leurs limites en raison de leur vulnérabilité aux attaques comme le vol, la duplication ou les attaques par force brute. Dans ce contexte, les systèmes biométriques se sont imposés comme une alternative fiable, permettant d'authentifier un individu à partir de caractéristiques uniques, qu'elles soient physiologiques (empreintes digitales, visage, iris) ou comportementales (voix, signature).

Malgré leurs nombreux avantages en termes de précision et de facilité d'utilisation, les systèmes biométriques présentent également des défis importants en matière de sécurité. L'un des problèmes majeurs réside dans la protection des Template biométriques, qui constituent des représentations numériques sensibles et non renouvelables des caractéristiques d'un individu. Contrairement aux mots de passe, les données biométriques ne peuvent pas être modifiées en cas de compromission, ce qui les rend particulièrement critiques.

Ainsi, ces systèmes peuvent être exposés à diverses attaques, telles que l'inversion de Template, les attaques par rejeu ou encore les intrusions dans les bases de données.

Afin de répondre à ces problématiques, plusieurs approches ont été développées, notamment le chiffrement des données biométriques, les techniques de biométrie révocable (Cancelable Biometrics) ainsi que des méthodes hybrides combinant transformation et protection cryptographique. Ces solutions visent à garantir la confidentialité, l'intégrité et la non-

inversibilité des Template biométriques, tout en préservant les performances du système en termes de reconnaissance.

Dans ce cadre, le présent travail s'inscrit dans une démarche visant à concevoir et évaluer un système biométrique sécurisé intégrant des techniques avancées d'extraction, de transformation et de protection des caractéristiques. L'approche proposée repose sur la combinaison de méthodes de réduction de dimensionnalité, telles que l'Analyse en Composantes Principales (PCA), et de techniques de représentation parcimonieuse comme le Sparse Coding (SC). À cela s'ajoutent des méthodes d'optimisation, notamment l'algorithme d'optimisation par essaim de particules (PSO), ainsi que des transformations basées sur le chaos, permettant de générer des Template biométriques sécurisés et difficilement inversibles. Par ailleurs, ce travail vise à évaluer les performances du système proposé selon plusieurs critères, tels que la précision de reconnaissance, la robustesse et le coût computationnel. Une attention particulière est accordée à l'analyse de la sécurité, à travers l'étude de la sensibilité des clés et l'application de tests statistiques de type NIST, afin de vérifier le caractère aléatoire et la solidité du mécanisme de protection mis en œuvre. L'objectif principal est d'assurer un compromis optimal entre performance et sécurité, condition essentielle pour toute application biométrique réelle.

Le manuscrit est organisé en trois chapitres :

Le premier chapitre Présente les fondements de la sécurité de l'information et des systèmes biométriques, en abordant leurs concepts de base, leurs architectures ainsi que les principales menaces.

Le deuxième chapitre est consacré à la protection des Template biométriques et à la description détaillée du système proposé, incluant les différentes techniques utilisées.

Le troisième chapitre expose les résultats expérimentaux obtenus, suivis d'une analyse approfondie des performances et de la sécurité du système.

Chapitre 1

Biométrie et Sécurité de l'Information

Résumé

Dans ce chapitre, on trouvera un aperçu du fondement de la sécurité d'informations périmétrie et d'informations systèmes biométriques par présentation de la triade CIA composée de la confidentialité, l'intégrité et la disponibilité, mais également les principales techniques de sécurité tels que la cryptographie, la stéganographie ou le filigrane numérique. On trouvera également les types et l'architecture d'un système biométrique, ainsi que les composants et les indicateurs de performance associés, les principales vulnérabilités de sécurité telles que le spoofing, le vol de modèle, l'interception de communication, ainsi que les mesures de sécurité renforcées pour les informations périmétrie.

I.1 Sécurité de l'information

I.2 Techniques de protection de l'information

I.3 La biométrie

I.4 Types de biométrie

I.5 Architecture et classification des systèmes biométriques

I.6 Phases d'un système biométrique

I.7 Vulnérabilités et attaques courantes

Introduction

Au fil des dernières années, le volume des données sur lesquelles l'utilisateur manipule n'a pas cessé d'évoluer, ce facteur sécuritaire en imposant d'autant plus l'idée d'une sécurisation de l'information. "Sécuriser l'information signifie la protéger des usages non autorisés, des accès non autorisés, des changements non autorisés." Il s'agit là d'une question essentielle des systèmes de traitement et de transmission des données informatiques. Dans ce chapitre, abordera d'une manière générale la sécurité d'information, la biométrie et ses dispositifs, avant d'aborder ce qu'est la caractéristique première des systèmes utilisés pour authentifier ou identifier la personne.

I.1 Sécurité de l'information

La sécurité de l'information se base sur plusieurs idées et règles qui protègent les données contre les menaces internes et externes.

I.1.1 Définition et objectifs de la sécurité de l'information

La sécurité de l'information englobe l'utilisation de contrôles d'accès physiques et logiques aux données afin de garantir la bonne utilisation des données et d'interdire toute modification, destruction, divulgation, perte ou accès non autorisé ou accidentel aux enregistrements et fichiers automatisés ou manuels, ainsi que la perte, les dommages ou l'utilisation abusive des actifs informationnels [1].

L'objectif principal de la sécurité de l'information est de protéger l'actif informationnel. Plus précisément, la sécurité de l'information vise à :

- Protéger les trois dimensions classiques de l'information : la confidentialité, l'intégrité et la disponibilité.
- Garantir les caractéristiques de confidentialité, d'intégrité et de disponibilité par la mise en œuvre de contrôles.
- Protéger les systèmes informatiques contre les menaces auxquelles ils sont exposés [2]. Gérer le risque sur les systèmes informatiques.

I.1.2 Confidentialité, intégrité et disponibilité (CIA)

La triade CIA (Confidentialité, Intégrité, Disponibilité) constitue les trois concepts de base de la sécurité [3]. Chaque entreprise a des objectifs et des besoins de sécurité spécifiques, et chaque panneau, mécanisme et mesure de protection en matière de sécurité est mis en place pour poursuivre ces concepts.

- **Confidentialité :** elle désigne la protection des informations sensibles contre tout accès ou divulgation non autorisés, garantissant que seules les personnes ou entités autorisées peuvent accéder à certaines données [4].
- **Intégrité :** il s'agit de protéger les informations contre toute modification ou altération non autorisée, en garantissant l'exactitude, la cohérence et la fiabilité des données tout au long de leur cycle de vie. [4] Des méthodes telles que les fonctions de hachage et les signatures numériques sont utilisées pour vérifier l'intégrité des données.
- **Disponibilité :** il s'agit de garantir que les ressources et les données du réseau sont accessibles et utilisables par les personnes autorisées chaque fois que cela est nécessaire, en minimisant les perturbations opérationnelles et en assurant un accès continu [4].



Figure I.1: La triade CIA de la sécurité de l'information [4]

I.1.3 Menaces, vulnérabilités et modèles d'attaque

La sécurité de l'information repose essentiellement sur la compréhension et l'analyse des menaces, des vulnérabilités présentes dans les systèmes, ainsi que des méthodes d'attaque.

Ces trois éléments sont étroitement liés et permettent de mieux comprendre comment un système d'information peut être compromis.

- **Les menaces :** Une menace pour le cyber sécurité est un acteur malveillant qui accède sans autorisation à des réseaux informatiques ou au réseau d'une autre personne ou organisation dans le but d'endommager, de perturber ou de voler des données [5]. Parmi ces menaces, on trouve :

- **Rootkits :** Les rootkits sont des programmes malveillants qui s'installent sur un système pour obtenir des droits élevés tout en restant cachés [7]. Ils permettent à un attaquant de contrôler et de surveiller l'ordinateur à distance sans être détecté, souvent sur une longue période**.**
- **Virus informatique :** sont des programmes malveillants généralement conçus dans le but de causer des dommages aux systèmes informatiques. Ils se caractérisent par leur capacité à se reproduire et à se propager vers d'autres systèmes sans le consentement ni la connaissance de l'utilisateur [8]. De plus, ces virus peuvent modifier leur propre code ou permettre aux copies générées de se modifier elles-mêmes. Ils affectent ainsi les performances des ordinateurs et des dispositifs de communication, entraînant des ralentissements ou des dysfonctionnements de certaines fonctionnalités**.**
- **Vers informatiques :** Le ver informatique est un logiciel malveillant capable de se diffuser automatiquement d'un ordinateur à un autre, sans nécessiter l'intervention de l'utilisateur [9]. Il peut également être considéré comme un ensemble de codes programmés qui se reproduisent de manière autonome et perturbent le fonctionnement normal des systèmes informatiques.

  Ces programmes présentent plusieurs caractéristiques. Ils sont contagieux, car ils se propagent entre machines via les réseaux ou les supports de stockage amovibles. Ils peuvent aussi rester cachés et difficiles à détecter en s'intégrant dans les programmes du système afin d'échapper aux antivirus [10]. En outre, ils ont la capacité de muter lors de leur propagation, ce qui augmente leur diversité, et ils sont généralement destructeurs, car ils peuvent dégrader les performances des ordinateurs et perturber leur fonctionnement.

- **Chevaux de Troie** : c'est un type de logiciel malveillant (malware) qui se fait passer pour un programme légitime, offrant souvent un service utile ou attrayant afin d'inciter l'utilisateur à l'exécuter. Cependant, une fois activé, il réalise des actions non autorisées et nuisibles à

l'insu de l'utilisateur [11]. Ce type de logiciel exploite les privilèges du système de l'utilisateur pour effectuer des opérations cachées, telles que l'accès aux données, leur vol ou leur destruction, ainsi que la compromission de la sécurité du système.

- **Les vulnérabilités :** Une vulnérabilité est une faille dans un produit ou un système qui peut potentiellement permettre à un attaquant de compromettre la confidentialité [6], l'intégrité ou la disponibilité de ce produit ou système.

Les différents types de vulnérabilités sont :

- **Vulnérabilités logicielles :** Les vulnérabilités logicielles sont des erreurs ou des failles présentes dans la conception, l'implémentation ou le fonctionnement d'un logiciel. Elles peuvent être exploitées par des attaquants pour contourner les mécanismes de sécurité et accéder au système de manière non autorisée, ce qui peut entraîner des pertes ou des dommages [12]. Ces failles proviennent souvent d'erreurs dans le code source et peuvent provoquer de graves problèmes de sécurité si elles sont exploitées. Par exemple, elles peuvent permettre le vol de données, l'accès non autorisé ou l'exécution d'activités malveillantes qui compromettent la sécurité du système et des utilisateurs.
- **Vulnérabilités réseaux :** désignent des failles présentes dans un réseau qui peuvent être exploitées par des personnes malveillantes afin d'obtenir un accès non autorisé, d'intercepter des données ou de perturber le fonctionnement des services. Elles peuvent se retrouver dans différents équipements comme les imprimantes, les systèmes DVR/NVR, les systèmes de pointage, les points d'accès, ainsi que les caméras de vidéosurveillance (CCTV), mais aussi dans certains protocoles tels que RDP [13]. Dans ce contexte, ces failles peuvent conduire à la fuite de données sensibles lorsque des utilisateurs non autorisés partagent le même réseau local (LAN), surtout si certains ports restent accessibles en interne, même lorsqu'ils sont normalement protégés par un pare-feu vis-à-vis d'Internet.
- **Serveur Web :** Ces vulnérabilités résultent d'erreurs de conception et d'ingénierie ou d'une mauvaise utilisation [6]. Les attaques par renfilage et par usurpation d'identité sont des exemples d'attaques causées par des vulnérabilités des serveurs Web.
- **Vulnérabilité matérielle :** Une vulnérabilité matérielle correspond à une faiblesse présente dans les composants physiques d'un système, pouvant être exploitée par un attaquant dans un but malveillant, comme le vol de données, la compromission de l'intégrité du système ou encore son dysfonctionnement. [14]. Ces vulnérabilités peuvent être introduites de manière intentionnelle, par exemple sous forme de portes dérobées ou de chevaux de Troie matériels, ou de manière non intentionnelle, à la suite d'erreurs de conception ou de fabrication.

- **Modèles d'attaque :** Les systèmes d'information sont exposés à plusieurs catégories d'attaques qui visent soit à collecter des informations, soit à perturber ou altérer les données et services , Ces attaques sont les suivantes :

- **Attaques actives:** Attaques dans lesquelles l'attaquant s'implique dans l'analyse ou la surveillance des données. En d'autres termes, l'objectif principal de l'attaquant est d'obtenir les informations en transit [15]. Ces types d'attaques sont difficiles à détecter car aucune modification des données n'est effectuée par l'attaquant.

▪ Modification : Lorsqu'un nœud malveillant modifie l'itinéraire de routage, l'expéditeur envoie le message via un itinéraire plus long. Cette attaque provoque un retard de communication entre l'expéditeur et le destinataire.

▪ Fabrication : Un nœud malveillant génère un faux message de routage [16]. Cela signifie qu'il génère des informations incorrectes sur l'itinéraire entre les appareils**.**

- **Attaques passives:** Contrairement aux attaques actives , les attaques passives sont basées sur une modification du message original ou la création d'un faux message. Ces types d'attaques sont faciles à détecter mais très difficiles à prévenir [15]. Ces attaques peuvent prendre la forme d'une interruption, d'une modification ou d'une fabrication**.**

▪ Analyse du trafic : Dans le cadre d'une attaque par analyse du trafic, un pirate tente de détecter le chemin de communication entre l'expéditeur et le destinataire. Il peut ainsi déterminer la quantité de données qui transitent entre l'expéditeur et le destinataire. L'analyse du trafic n'entraîne aucune modification des données.

▪ Il s'agit d'une attaque passive qui se produit dans un réseau mobile ad hoc. Le principal objectif de cette attaque est de découvrir des informations secrètes ou confidentielles à partir des communications [16]. Ces informations secrètes peuvent être la clé privée ou publique de l'expéditeur ou du destinataire, ou toute donnée secrète.

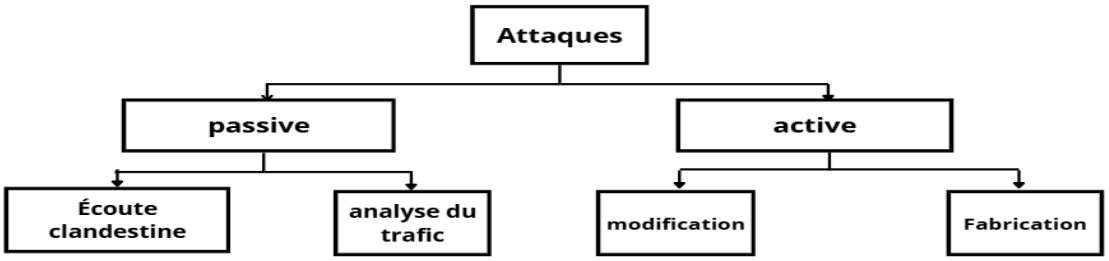


Figure I.2: Classification des types d'attaques en sécurité de l'information**.** [16]

I.2 Techniques de protection de l'information

Plusieurs techniques sont mises en œuvre afin d'assurer la protection des informations et de garantir leur confidentialité, leur intégrité et leur disponibilité.

I.2.1 Cryptographie

La cryptologie regroupe deux domaines complémentaires : la cryptographie, dédiée à la conception des mécanismes de protection de l'information, et la cryptanalyse, qui vise à évaluer leur robustesse face aux attaques. La cryptographie se décline principalement en deux approches, à savoir la cryptographie symétrique, la cryptographie asymétrique et fonctions de hachage :

- **La cryptographie symétrique**, La cryptographie symétrique repose sur l'utilisation d'une clé secrète partagée entre les utilisateurs afin de chiffrer et déchiffrer les informations échangées. La sécurité de ce type de système dépend essentiellement de la confidentialité de cette clé, puisqu'un attaquant ne doit ni accéder au contenu des messages ni réussir à retrouver la clé à partir des communications interceptées. Dans les études de sécurité, l'attaquant est souvent représenté comme une entité capable de choisir des textes clairs et d'obtenir leurs versions chiffrées à travers un oracle de chiffrement, dans le cadre d'un modèle appelé attaque à texte clair choisi. Une attaque est considérée performante lorsqu'elle permet de récupérer la clé plus efficacement qu'une recherche exhaustive parmi toutes les clés possibles. L'analyse des vulnérabilités et des techniques d'attaque appliquées aux systèmes de chiffrement constitue le domaine de la cryptanalyse, qui regroupe plusieurs méthodes destinées à évaluer la robustesse des algorithmes. [17] Parmi les approches les plus connues figure la cryptanalyse différentielle, basée sur l'étude des variations entre les textes clairs et les textes chiffrés afin de détecter d'éventuelles faiblesses dans le système cryptographique.
- **La cryptographie asymétrique** repose sur l'utilisation de deux clés différentes pour chaque utilisateur : une clé publique, partagée librement, et une clé privée, conservée de manière confidentielle. Dans ce contexte, si Alice désire envoyer un message sécurisé à Bob, elle chiffre les données à l'aide de la clé publique de Bob. À la réception, Bob utilise sa propre clé privée pour retrouver le message original. [40] Ce mécanisme garantit que seul le destinataire concerné peut lire les informations échangées, même si la clé publique est accessible à tous.
- **Une fonction de hachage** Les fonctions de hachage occupent une place essentielle dans la vérification de l'intégrité des données en cryptographie. Elles reposent sur des algorithmes mathématiques capables de transformer un message de longueur quelconque en une valeur condensée de taille fixe, appelée empreinte numérique, propre à chaque message. Cette empreinte permet de détecter toute modification apportée aux données originales. Afin d'assurer un niveau élevé de sécurité, une fonction de hachage doit être robuste face aux différentes

attaques cryptanalytiques. [18] Sa fiabilité est principalement évaluée à travers plusieurs propriétés fondamentales, notamment la résistance à la pré-image, la résistance à la seconde pré-image ainsi que la résistance aux collisions.

I.2.2 Stéganographie

La stéganographie consiste à cacher des informations à l'intérieur d'un support numérique de manière à ce qu'un observateur ne puisse pas soupçonner leur existence. Dans cette approche, l'objectif principal n'est pas la robustesse mais plutôt l'indétectabilité des données dissimulées. Contrairement à la cryptographie, qui protège l'information par le chiffrement, la stéganographie repose sur la dissimulation de l'information au sein d'un contenu numérique [19]. Par ailleurs, la stéganalyse représente la discipline chargée d'analyser et de détecter la présence éventuelle de données cachées. Elle vise à évaluer la sécurité des techniques de stéganographie et à identifier leur utilisation dans des contextes réels.

I.2.3 Tatouage numérique

Le tatouage numérique est une technique qui consiste à insérer une information cachée dans une image numérique de manière discrète afin d'assurer la protection et la sécurisation des données. Cette méthode doit respecter plusieurs contraintes essentielles, notamment l'imperceptibilité afin de préserver la qualité visuelle de l'image, la robustesse pour résister aux différentes altérations, ainsi que la sécurité garantissant la confidentialité des informations intégrées. [21] Dans le cas du tatouage aveugle, l'extraction de la marque s'effectue sans utiliser l'image originale, ce qui rend cette approche particulièrement adaptée aux applications de protection des contenus numériques.

I.2.4 Comparaison entre cryptographie, stéganographie et Tatouage

La cryptographie, le tatouage numérique et la stéganographie représentent trois approches complémentaires dédiées à la protection des informations numériques, chacune répondant à un objectif spécifique. La cryptographie vise principalement à rendre les données illisibles aux utilisateurs non autorisés grâce aux mécanismes de chiffrement et de déchiffrement afin d'assurer la confidentialité, l'intégrité et l'authenticité des informations. De son côté, le tatouage numérique consiste à intégrer des informations directement dans un support multimédia, comme une image, une vidéo ou un fichier audio, dans le but de garantir l'identification, la traçabilité ainsi que la protection des droits d'auteur. Quant à la stéganographie, elle cherche à dissimuler l'existence même d'un message secret à l'intérieur d'un média de couverture de manière imperceptible. [26] Ainsi, tandis que la cryptographie protège le contenu

des données, le tatouage numérique sécurise le support multimédia et la stéganographie cache la présence de l'information elle-même.

I.3 La biométrie

La biométrie constitue une technologie d'identification basée sur l'exploitation des caractéristiques physiologiques et comportementales propres à chaque individu.

I.3.1 Définition et historique de la biométrie

La biométrie désigne l'ensemble des technologies permettant l'identification ou la vérification automatique de l'identité d'un individu à partir de ses caractéristiques physiologiques ou comportementales, telles que les empreintes digitales, le visage, l'iris ou la voix, qui sont considérées comme uniques et fiables pour l'authentification. L'utilisation des caractéristiques humaines pour l'identification remonte à plusieurs siècles, où la reconnaissance des individus se faisait de manière visuelle et empirique, avant de connaître un développement scientifique au XIXe siècle avec les travaux d'Alphonse Bertillon sur l'identification anthropométrique, suivis par l'adoption des empreintes digitales comme méthode plus précise et largement utilisée dans les domaines policier et judiciaire. [27]. Par la suite, la biométrie a évolué grâce aux avancées technologiques et informatiques, devenant aujourd'hui un élément central des systèmes modernes de sécurité, d'authentification et de contrôle d'accès.

I.3.2 Propriétés des caractéristiques biométriques

La biométrie repose sur des caractéristiques propres à chaque individu, contenant des informations suffisantes pour assurer son identification et sa distinction des autres personnes [41]. Une caractéristique physiologique ou comportementale peut être considérée comme une modalité biométrique lorsqu'elle répond aux critères suivants :

- **Universelle** : présente chez l'ensemble des individus.
- **Distinctive** : capable de différencier une personne d'une autre.
- **Durable** : relativement stable au cours du temps.
- **Acquérable** : pouvant être capturée et enregistrée avec l'accord de l'utilisateur.



Figure I.3: Exemple de modalités biométriques. [41]

I.4 Modalités biométriques

Les modalités biométriques basées sur des caractéristiques humaines, se divisent en deux types : morphologiques, comportement

I.4.1 Biométrie physiologique

Ces modalités biométriques se caractérisent par leur unicité et leur stabilité durent le temps. Elles reposent sur l'analyse de caractéristiques physiques propres à chaque individu, telles que le visage, l'iris, la rétine, l'ADN, la géométrie de la main, l'empreinte palmaire ou encore l'empreinte digitale. Grâce à leur permanence au cours de la vie, ces traits constituent des éléments fiables pour les systèmes d'identification biométrique [42]. Parmi les principales méthodes d'identification physiologique, on peut citer :

- **Empreintes digitales :** Les empreintes digitales représentent la méthode d'identification personnelle la plus populaire et fiable. Chaque empreinte présente un motif unique de lignes et de points caractéristiques (minuties) propres à chaque doigt [28]. C'est la comparaison de ces minuties qui permet d'identifier avec précision une personne.



Figure I.4: trait biométrique : empreintes [28]

- **Empreinte palmaire :** La biométrie palmaire est une technologie biométrique qui utilise les caractéristiques uniques et fiables de la paume de la main, telles que les lignes principales, les minuties, les rides et les crêtes, pour l'identification des individus [31]. Le palmprint humain est constitué de trois types de motifs principaux : les lignes principales, les rides et les crêtes épidermiques. Il contient également d'autres informations telles que la texture, les indentations et diverses marques [43].



Figure I.5 : Un exemple de l'empreinte palmaire humaine.

- **Visage :** Cette approche biométrique exploite l'image du visage pour identifier une personne [29]. Les caractéristiques extraites doivent être uniques à chaque individu et constantes au fil du temps, de sorte que l'âge ou d'autres changements physiologiques n'affectent pas la reconnaissance.



Figure I.6: trait biométrique : visage [29]

- **Iris :** La biométrie par iris repose sur la capture de l'image de la partie visible de l'œil à l'aide d'un capteur. L'iris présente des motifs extrêmement complexes et pratiquement uniques à chaque individu, ce qui le rend presque impossible à falsifier. Ses caractéristiques restent globalement stables au cours de la vie, la variation de couleur n'ayant pas d'impact puisque l'analyse se fait en niveaux de gris [29]. Toutefois, des facteurs comme la distance au capteur, les reflets ou l'utilisation de faux yeux peuvent affecter la précision, d'où l'intérêt d'intégrer certaines propriétés dynamiques de l'œil pour renforcer la fiabilité de l'identification.

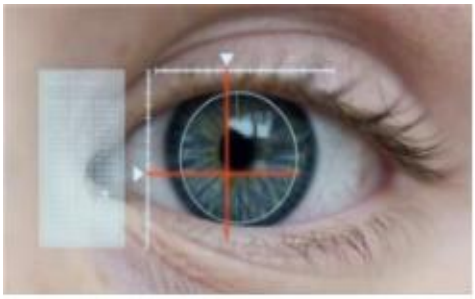


Figure I.7: trait biométrique : iris [29]

- **ADN :** L'Acide Désoxyribonucléique (ADN) est présent dans toutes les cellules du corps et est unique à chaque individu, ce qui permet une identification fiable à partir de petits échantillons tels que la peau, le sang ou la salive. Aujourd'hui, son usage reste principalement limité à la justice en raison du temps et du coût d'analyse [29]. Malgré cela, l'ADN est au centre des recherches biométriques, car il constitue la méthode d'identification la plus précise, surpassant largement les autres techniques avec une marge d'erreur quasi négligeable.

I.4.2 Biométrie comportementale

La biométrie comportementale est une branche de la biométrie basée sur l'analyse des comportements humains, tels que la marche, la voix ou la signature, afin d'identifier ou de vérifier l'identité d'une personne [44].

- **Signature :** est une méthode biométrique couramment utilisée pour vérifier l'identité d'une personne, notamment dans les transactions du quotidien. Son analyse peut se faire soit à partir de son aspect visuel (mode statique), soit en prenant en compte des éléments dynamiques comme la vitesse et la pression du stylo, ce qui améliore la précision [22]. Cependant, cette approche présente certaines limites, car la signature peut varier avec le temps ou selon l'état de l'individu, ce qui peut réduire la fiabilité du système.



Figure I.8: trait biométrique : signature [34]

- **Frappe au clavier :** frappe au clavier représente une caractéristique comportementale propre à chaque individu, reflétant sa manière personnelle d'écrire sur un support numérique. Elle peut être comparée à une forme de graphologie adaptée à l'environnement informatique. Les systèmes de reconnaissance exploitent plusieurs paramètres, tels que la vitesse de saisie, l'ordre des lettres, les intervalles de temps entre les frappes, ainsi que les pauses entre les mots, et parfois même l'identification de séquences ou de mots spécifiques.
- **Voix :** La reconnaissance vocale est une méthode biométrique permettant d'identifier une personne grâce à sa voix. Le signal vocal est d'abord enregistré par un microphone, puis converti en données numériques exploitables. Ensuite, plusieurs caractéristiques sont extraites, comme la fréquence, la tonalité, le rythme et la vitesse de parole, afin d'être comparées à celles stockées dans une base de données pour vérifier l'identité du locuteur [27]. Cette technologie est utilisée dans différents domaines, notamment les systèmes de dictée vocale, les applications de commande vocale et les services téléphoniques automatisés, ainsi que dans la sécurité et les enquêtes. Toutefois, elle reste sensible aux bruits, aux variations de la voix et à la différence entre le langage humain naturel et le traitement des machines, ce qui peut limiter sa précision

I.5 Architecture et classification d'un système biométrique

L'architecture d'un système biométrique définit l'organisation de ses composants et permet de distinguer plusieurs types de systèmes selon leur mode de fonctionnement.

I.5.1 Etapes d'un système biométrique

Un système biométrique permet d'identifier ou d'authentifier une personne à partir de ses caractéristiques biologiques ou comportementales. Il se compose principalement de trois éléments :

- **Etape d'acquisition :** Cette étape consiste à capturer les données biométriques d'un individu . Par exemple, un capteur d'empreintes digitales qui image la structure des crêtes et des vallées du doigt d'un utilisateur [32].
- **Etape d'extraction de caractéristiques :** dans lequel les données biométriques acquises sont traitées afin d'extraire un ensemble de caractéristiques saillantes ou discriminantes. [34] Par exemple, la position et l'orientation des points de minuties (singularités locales des crêtes et des vallées) dans une image d'empreinte digitale sont extraites dans le module d'extraction de caractéristiques d'un système biométrique basé sur les empreintes digitales.
- **Etape de comparaison :** dans lequel les caractéristiques lors de la reconnaissance sont comparées aux modèles stockés afin de générer des scores de correspondance. Par exemple, dans le module de correspondance d'un système biométrique basé sur les empreintes digitales, le nombre de détails correspondants entre les images d'empreintes digitales saisies et celles du modèle est déterminé et un score de correspondance est communiqué [33]. Le module de correspondance comprend également un module de prise de décision, dans lequel l'identité déclarée par l'utilisateur est confirmée (vérification) ou l'identité de l'utilisateur est établie (identification) sur la base du score de correspondance.
- **Etape de décision :** l'étape de décision consiste à exploiter les caractéristiques biométriques préalablement extraites et traitées afin de déterminer l'identité de l'individu ou d'associer l'échantillon biométrique à la classe correspondante [33] .

I.5.2 Phases d'un système biométrique

Un système biométrique fonctionne suivant un ensemble de phases successives allant de l'acquisition des données jusqu'à la décision finale d'authentification ou d'identification.

- **Phase d'enrôlement :** La première utilisation d'un système biométrique nécessite une étape d'inscription, au cours de laquelle les caractéristiques biométriques de l'utilisateur sont acquises et enregistrées dans la base de données. [35] Selon le système, ces données peuvent être accompagnées d'informations biographiques afin de compléter le profil de l'utilisateur.

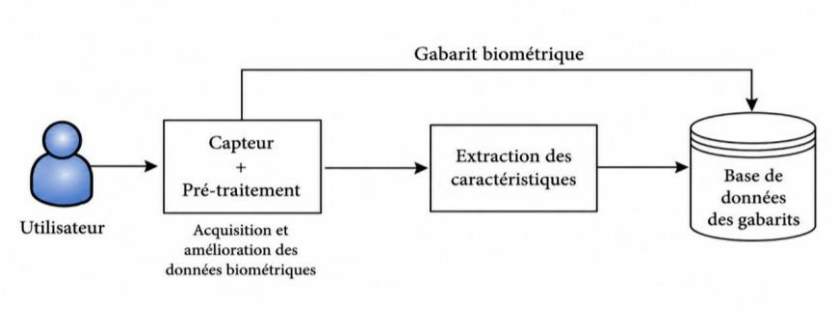


Figure I.9: Enrôlement d'une personne dans le système biométrique.

- **Phase de reconnaissance :**Cette phase est composée de deux modes est authentification et l'identification.

- **Mode authentification :** Le mode vérification d'un système biométrique consiste à contrôler si l'utilisateur est bien celui qu'il prétend être. Pour ce faire, le système capture les données biométriques de l'utilisateur et les compare uniquement au modèle enregistré correspondant à l'identité déclarée, souvent après saisie d'un code personnel (PIN) et fourniture d'un trait biométrique [35]. Cette comparaison, appelée 1:1, valide l'identité si le degré de similarité est suffisant. Dans le cas contraire, l'utilisateur est rejeté et considéré comme un imposteur. Ainsi, le mode vérification répond à la question : « Suis-je vraiment M. X ? » [23].

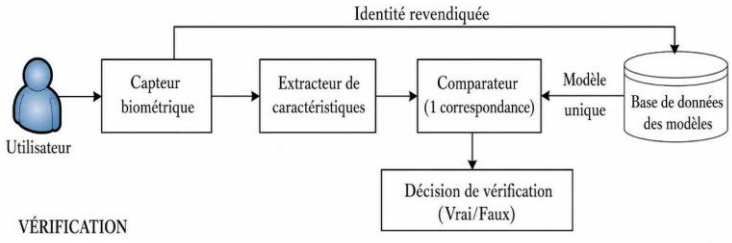


Figure I.10: vérification de la personne dans le système biométrique [45].

- **Mode d'identification :** La vérification biométrique dans le système proposé repose sur l'analyse des caractéristiques des veines palmaires extraites à partir des images acquises. Après la capture de l'image, un prétraitement basé sur des filtres PDV est appliqué afin d'améliorer la qualité des structures vasculaires et de renforcer les motifs veineux d'intérêt. Ensuite, une réduction de dimension et une extraction des caractéristiques discriminantes sont réalisées à l'aide de l'algorithme PCA, permettant de représenter efficacement les informations biométriques essentielles [24]. Par la suite, la technique de Sparse Coding (SC) est utilisée afin de générer une représentation compacte et robuste des caractéristiques extraites, favorisant une meilleure discrimination entre les individus. Lors de la phase de vérification, les signatures biométriques obtenues sont comparées aux templates

enregistrés dans la base de données afin de confirmer l'identité de l'utilisateur. Les résultats expérimentaux montrent une performance élevée du système, avec un taux de vérification correcte atteignant 99,99 %, ce qui démontre l'efficacité et la fiabilité du processus de vérification biométrique proposé.

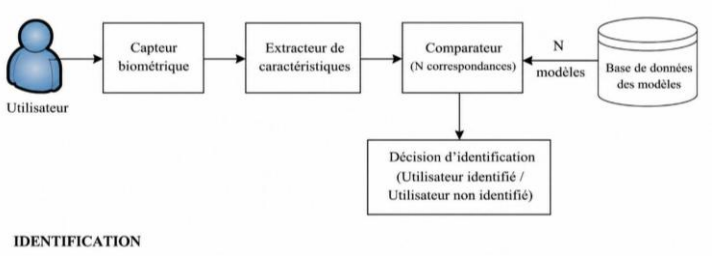


Figure I.11: Identification de la personne dans le système biométrique [45].

I.6 Systèmes uni modaux et multimodaux Multimodale

- **Systèmes uni modaux :** Un système biométrique uni modal utilise une seule caractéristique biométrique, telle que l'empreinte digitale, le visage ou l'iris, afin de vérifier ou d'identifier une personne. Malgré sa simplicité d'utilisation, ce type de système présente certaines limitations, notamment une diminution des performances en cas de faible qualité des données acquises, de ressemblances importantes entre individus ou encore face aux attaques d'usurpation [30]. Ces contraintes peuvent affecter la robustesse et la fiabilité du système dans des applications réelles.
- **Systèmes multimodaux :** Les systèmes biométriques multimodaux utilisent plusieurs caractéristiques biométriques complémentaires, extraites à l'aide de différentes méthodes spécifiques. Contrairement aux systèmes uni-modaux, ils offrent un niveau de sécurité plus élevé face aux attaques par usurpation d'identité, ainsi qu'une meilleure fiabilité et robustesse dans des environnements variables et dynamiques [20]. Par exemple, l'empreinte digitale, qui est une modalité biométrique très utilisée pour la reconnaissance et la vérification, peut rencontrer plusieurs limitations telles que la présence de cicatrices, des images déformées, des coupures, ou encore des empreintes sales, grasses ou partiellement altérées par des cellules mortes. De plus, ce type de modalité peut être vulnérable aux attaques de type spoofing, pouvant provoquer des altérations ou des imitations du motif original.

- Systèmes multi-capteurs : Ils reposent sur l'acquisition d'une même modalité biométrique à l'aide de plusieurs capteurs, afin d'améliorer la fiabilité et la qualité des données collectées.
- Systèmes multi-instances **:** Ces systèmes exploitent plusieurs instances d'une même caractéristique biométrique appartenant à un individu. Par exemple, différentes vues du visage,

telles que les profils gauche et droit, peuvent être capturées afin de confirmer l'identité d'une personne.

- Systèmes multi-algorithmes : Ils reposent sur le traitement d'une même donnée biométrique à l'aide de plusieurs algorithmes. Cette diversité peut intervenir au niveau de l'extraction, en exploitant différents ensembles de caractéristiques, et/ou au niveau de la comparaison, en appliquant plusieurs méthodes de mise en correspondance.
- Systèmes multi-échantillons **:** Ils consistent à utiliser un même capteur pour collecter plusieurs échantillons d'un même trait biométrique, afin de prendre en compte les variations possibles de ce trait et d'en obtenir une représentation plus fidèle et plus complète.
- Systèmes multimodaux : Ces systèmes établissent l'identité d'un individu à partir de plusieurs caractéristiques biométriques distinctes [31]. Par exemple, la combinaison de traits biométriques indépendants sur le plan physique, comme les empreintes digitales et l'iris, permet d'obtenir de meilleures performances que l'association de caractéristiques corrélées, telles que la voix et les mouvements des lèvres.

I.7 Critères de performance et indicateurs

Dans ce type de système, la décision se limite généralement à accepter ou refuser un utilisateur. [25] Deux erreurs principales peuvent alors apparaître : d'une part, la fausse acceptation, lorsque le système considère à tort un imposteur comme un utilisateur légitime ; d'autre part, le faux rejet, lorsque l'accès est refusé à un utilisateur authentique. Pour évaluer ces erreurs, on utilise deux mesures dépendant d'un seuil de décision.

- **Taux de faux rejet (False Rejection Rate ou FRR) :** le taux de faux rejets représente le rapport entre le nombre d'utilisateurs légitimes refusés à tort et le nombre total de tentatives authentiques. Ici, une tentative imposteur correspond à une comparaison entre données de personnes différentes, tandis qu'une tentative authentique concerne des données issues d'un même individu.

$$\mathbf{FRR} = \frac{\textbf{Nombre de faux rejet}}{\textbf{nombre total de tentatives d'accès authentiques.}} \qquad \text{(I.1)}$$

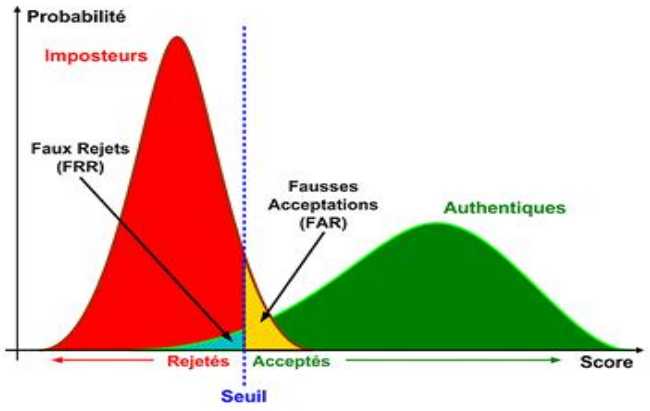


Figure I.13: illustration du FRR et du FAR. [39]

- **Taux de fausse acceptation (False Acceptante Rate – FAR) :** Le taux de fausses acceptations (FAR) correspond au rapport entre le nombre d'imposteurs acceptés par erreur et le nombre total de tentatives d'imposteurs [25].

$$\boldsymbol{FAR} = \frac{\boldsymbol{Nombre\ de\ faux}\ \textbf{acceptation}}{\boldsymbol{nombre\ total\ de\ tentatives\ d'accès\ imposteurs.}} \qquad \text{(I.2)}$$

- **Taux d'égale erreur (Equal Error Rate) :** correspond au point où les deux types d'erreurs du système, à savoir les fausses acceptations (FAR) et les faux rejets (FRR), prennent la même valeur . Ce point est souvent utilisé comme référence pour évaluer les performances, car il représente un compromis équilibré entre sécurité et accessibilité, indépendamment du contexte d'utilisation [30].

$$\boldsymbol{EER} = \boldsymbol{FAR} = \textbf{FRR} \qquad \text{(I. 3)}$$

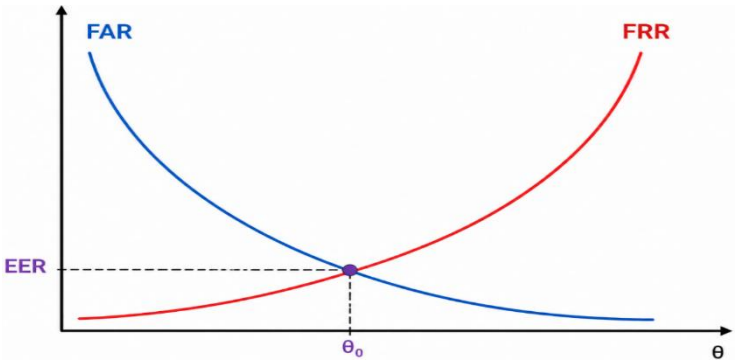


Figure I.14: Graph démonstratif de l'EER. [30]

I.8 Vulnérabilités et attaques courantes

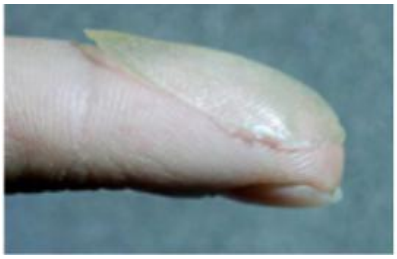
Les systèmes biométriques, bien qu'efficaces pour l'authentification, présentent plusieurs vulnérabilités exploitées par différents types d'attaques :

I.8.1 Attaques sur les capteurs (spoofing)

Les attaques contre les capteurs, souvent appelées attaques directes ou attaques par usurpation, consistent à soumettre au capteur un trait biométrique contrefait ou reproduit. L'efficacité de ces attaques repose sur le fait que le capteur biométrique est incapable de détecter si le trait biométrique soumis est « faux » (usurpé) ou « réel ». Par conséquent, le capteur génère une image qui est ensuite traitée et potentiellement reconnue comme un trait biométrique « réel » et authentique.

Les attaques par usurpation sont considérées comme un danger sérieux car elles :

- Elles consistent à voler, copier et reproduire synthétiquement un trait biométrique afin d'obtenir un accès non autorisé.
- Elles sont beaucoup plus faciles à réaliser que d'autres types d'attaques, car elles ne nécessitent aucune connaissance du système (telle que l'extraction de caractéristiques ou l'algorithme de correspondance utilisé).
- Elles sont effectuées dans le domaine analogique, en dehors des limites numériques du système, ce qui signifie que les techniques de protection numériques telles que le hachage et le cryptage ne sont pas efficaces contre elles [36].



(a) Empreinte digitale



(b) iris

Figure I.15 : Deux exemples d'attaque sur le capteur biométrique**.** [37]

I.8.2 Attaques sur les Template biométriques

Ce type d'attaque se produit sur la base de données des modèles. La base de données des modèles peut être ajoutée, modifiée ou supprimée**.** [38] Les modèles peuvent également être volés, ce qui peut être très dangereux.

I.8.3 Attaques sur la communication et les canaux de données

Sans la mise en place de mécanismes de sécurité adéquats, un pirate informatique peut intercepter les échanges de données biométriques (écoute clandestine), les modifier ou insérer de fausses informations en s'interposant dans la communication (attaque de type Man-in-the-Middle) [37]. Il peut également réutiliser des données biométriques déjà transmises (attaque par Replay) ou altérer les résultats produits par le module de comparaison afin de compromettre la décision d'authentification.

I.8.4 Attaques sur les systèmes multimodaux ou distribués

Les attaques contre les systèmes biométriques multimodaux consistent à créer des données d'entrée modifiées (exemples adverses) destinées à manipuler le modèle d'apprentissage profond pour provoquer une mauvaise classification ou une mauvaise prédiction, [35] ciblant spécifiquement le processus d'authentification.

Conclusion

Ce chapitre à montré que, devant les techniques et la montée des activités en ligne, la sécurité de l'info dépend beaucoup de méthodes d'authentification sûres. La biométrie devient une bonne solution, donnant aux systèmes un accès sûr aux données privées. Les idées présentées ici servent de base pour regarder les faiblesses et les mécanismes plus avancés de protection, touchés dans les chapitres d'après.

Chapitre 2

Sécurité des systèmes biométriques

Résumé

Dans ce chapitre, nous avons présenté les fondements de la sécurité des systèmes biométriques ainsi que leur rôle dans l'authentification sécurisée et leurs différentes applications. Nous avons également étudié les vulnérabilités des templates biométriques et les principales méthodes de protection, telles que le chiffrement et la biométrie révocable. Par ailleurs, nous avons analysé les menaces et attaques ciblant les systèmes biométriques, ainsi que la sécurité des canaux de transmission et les protocoles associés. Enfin, nous avons introduit le système proposé, basé sur une approche sécurisée intégrant des techniques avancées telles que les projections guidées par le chaos, l'optimisation par PSO et un schéma de chiffrement, afin d'améliorer la robustesse, la fiabilité et la sécurité globale.

II.1 Biométrie et sécurité

II.2 Protection des Templates biométriques

II.3 Sécurité des systèmes biométriques

II.4 Sécurité des canaux de transmission

II.5 Système proposé

Introduction

Dans ce chapitre, nous nous intéressons à la sécurité des systèmes biométriques, en particulier à la protection des templates qui représentent des données sensibles. Nous commençons par présenter les principales menaces auxquelles ces systèmes peuvent être exposés, comme le vol, la falsification ou encore les attaques sur les capteurs et les canaux de transmission. Ensuite, nous passons en revue les solutions existantes pour renforcer leur sécurité, telles que le chiffrement et la biométrie révocable. Enfin, nous proposons une approche basée sur des techniques avancées, dans le but d'améliorer la fiabilité et la robustesse du système.

II.1 Biométrie et sécurité

La biométrie occupe une place importante dans la sécurité moderne grâce à sa capacité à identifier les individus de manière fiable. Cette section présente son rôle dans l'authentification et ses domaines d'application.

II.1.1 Rôle de la biométrie dans l'authentification sécurisée

À l'heure actuelle, les technologies biométriques jouent un rôle fondamental dans les mécanismes de sécurité. Elles permettent une authentification fiable en se basant sur l'analyse de caractéristiques physiques ou comportementales propres à chaque individu. En offrant des méthodes d'accès plus résistantes aux tentatives de fraude, la biométrie contribue à renforcer la sécurité des systèmes d'information. Son champ d'application est très large, allant des dispositifs mobiles aux infrastructures sensibles telles que les aéroports. Par ailleurs, l'intégration de mécanismes de protection des données biométriques participe à la préservation de la vie privée [46]. Grâce à son évolution continue, la biométrie s'impose aujourd'hui comme un élément clé de l'authentification sécurisée, bien que son déploiement efficace demeure un enjeu important.

II.1.2 Applications de la biométrie dans la sécurité informatique et physique

Les technologies biométriques sont largement utilisées dans la sécurité physique et informatique pour renforcer la protection des systèmes et assurer une authentification fiable des utilisateurs. Elles reposent sur l'exploitation de caractéristiques physiques telles que les empreintes digitales, la reconnaissance faciale ou l'iris, afin de vérifier l'identité des individus dans les systèmes de contrôle d'accès, les dispositifs d'entrée sécurisés et les systèmes d'identité nationale [47]. En sécurité informatique, elles permettent à la fois une authentification statique basée sur des traits physiques et une authentification continue fondée sur des comportements comme la dynamique de frappe ou les mouvements de la souris. De plus, elles sont intégrées dans les dispositifs mobiles et les systèmes IoT pour sécuriser l'accès, et peuvent être combinées avec d'autres facteurs comme les mots de passe ou les toques dans des systèmes multi-facteurs afin de renforcer la sécurité, notamment dans les environnements sensibles. Elles sont également utilisées dans des applications critiques telles que le contrôle d'accès aux infrastructures sécurisées, le vote électronique et la vérification d'identité dans les transports, offrant ainsi une solution rapide, fiable et efficace contre les limites des méthodes traditionnelles d'authentification [48]. En conclusion, la biométrie constitue une solution essentielle pour améliorer la sécurité et garantir une identification précise et fiable des utilisateurs dans différents domaines.

II.2 Protection des Template biométriques

La protection des templates biométriques est essentielle pour garantir la confidentialité et l'intégrité des données. Cette partie présente les principales vulnérabilités ainsi que les méthodes de protection existantes.

II.2.1 Vulnérabilités des Template

La vulnérabilité des Template biométriques réside dans le fait que ces données sensibles sont permanentes et non modifiables en cas de compromission, contrairement aux mots de passe, ce qui représente un risque important pour la vie privée des utilisateurs. Dans de nombreux systèmes traditionnels, ces templates sont soit insuffisamment protégés, soit sécurisés à l'aide de techniques de chiffrement classiques nécessitant un déchiffrement lors de l'authentification, ce qui peut exposer les données à des attaques.

Pour limiter ces risques, le cadre proposé repose sur des techniques avancées de protection des templates biométriques telles que le hachage Index-of-Max (Io) et le hachage sans alignement (AFH). Ces approches permettent de générer des templates sécurisés, Cancelable et non corrélables [49]. Elles garantissent l'irréversibilité (impossibilité de retrouver les données ori-

ginales), l'unlinkabilité (difficulté de relier plusieurs templates d'un même individu) et la révocabilité (possibilité de remplacer un Template compromis), tout en maintenant de bonnes performances de reconnaissance et en assurant la confidentialité des données biométriques .

II.2.2 Méthodes de protection

Afin de limiter les risques liés aux vulnérabilités des templates biométriques, plusieurs mécanismes de protection ont été développés pour sécuriser le stockage et l'utilisation des données.

- **Chiffrement des templates :** Le chiffrement des templates biométriques constitue une méthode de protection visant à sécuriser les données biométriques en les transformant sous une forme chiffrée ou hachée afin d'empêcher tout accès non autorisé aux informations originales. Parmi les techniques utilisées figurent le chiffrement homomorphique (Homomorphique Encryptions - HE), qui permet d'effectuer des opérations de comparaison directement sur les données chiffrées sans nécessiter leur déchiffrement, garantissant ainsi une meilleure confidentialité des templates biométriques. D'autres approches reposent sur le hachage cryptographique et non cryptographique, où les templates sont convertis en codes binaires difficiles à inverser. Les méthodes cryptographiques offrent un niveau élevé de sécurité, tandis que les méthodes non cryptographiques présentent une meilleure tolérance aux variations biométriques. Ces techniques sont généralement appliquées au niveau des caractéristiques extraites (factures) avant leur stockage ou leur utilisation dans le processus d'authentification. Malgré leur efficacité, certaines études montrent que certains schémas de protection peuvent rester vulnérables à des attaques avancées capables de tenter la reconstruction des données biométriques originales à partir des templates protégés [50]. Ainsi, le chiffrement des templates contribue à renforcer la confidentialité et la sécurité des systèmes biométriques tout en limitant les risques de compromission des données sensibles.
- **Biométrie révocable et transformée :** La protection révocable des templates biométriques vise à garantir la sécurité et la confidentialité des données biométriques tout en permettant leur remplacement en cas de compromission. Cette approche repose sur l'utilisation d'un réseau neuronal convolutif pré-entraîné, tel que VGG-16, afin d'extraire des caractéristiques biométriques robustes et discriminantes à partir des images d'empreintes digitales. Les caractéristiques extraites sont ensuite transformées en vecteurs binaires puis protégées grâce à un chiffrement chaotique basé sur une clé générée par un système chaotique, comme la carte logistique. Une opération XOR est appliquée afin de rendre le Template irréversible et difficile à reconstruire sans la clé appropriée. Par la suite, les données chiffrées sont encodées dans un filtre de

Bloom amélioré intégrant un mécanisme de relocalisation permettant de réduire les collisions et d'améliorer davantage la sécurité. Cette transformation garantit une protection non inversible empêchant toute récupération des caractéristiques biométriques originales. De plus, le système assure la révocabilité des templates, puisqu'un nouveau Template peut être généré simplement en modifiant la clé chaotique, tandis que la comparaison biométrique s'effectue directement dans le domaine chiffré sans exposer les données sensibles [51]. Ainsi, cette approche permet d'assurer une protection efficace des templates biométriques tout en préservant la confidentialité et la sécurité des utilisateurs.

- **Schémas hybrides et protection multi-niveaux :** Les systèmes hybrides de protection des templates biométriques visent à renforcer la sécurité des données biométriques lors de leur stockage et de leur utilisation dans les systèmes d'authentification, tout en maintenant de bonnes performances de reconnaissance. Cette approche repose principalement sur la combinaison des biométries annulables et des techniques cryptographiques. Les biométries annulables appliquent des transformations non inversibles aux caractéristiques biométriques afin de générer des templates modifiés et difficiles à reconstruire, assurant ainsi la protection de la vie privée et l'irréversibilité des données. En complément, les crypto systèmes, tels que le RSA modifié, permettent de chiffrer ces templates transformés afin de renforcer leur sécurité même en cas de compromission de la base de données [52]. La combinaison de ces deux techniques permet de réduire les risques d'attaques telles que la reconstruction, la falsification ou l'interception des données biométriques, tout en garantissant la confidentialité et l'intégrité des informations biométriques .

Les schémas de sécurité biométrique multi-niveaux reposent sur l'utilisation de plusieurs couches de protection afin de renforcer la sécurité des systèmes d'authentification et de limiter les risques d'accès non autorisé. Ils combinent généralement la biométrie avec d'autres mécanismes tels que la détection d'anomalies, les politiques de contrôle d'accès et les systèmes d'alerte, ce qui permet de construire une architecture de sécurité plus robuste et plus fiable. Les approches récentes intègrent également des techniques multimodales et comportementales, en associant par exemple la reconnaissance faciale à d'autres facteurs d'authentification pour améliorer la précision et la résistance du système. De plus, l'utilisation de l'intelligence artificielle permet d'assurer une surveillance continue et une prise de décision en temps réel, renforçant ainsi la capacité du système à détecter les menaces [53]. Ces architectures multi-niveaux sont particulièrement efficaces car chaque couche ajoute une protection supplémentaire, garantissant

qu'une éventuelle faille dans un niveau ne compromette pas l'ensemble du système, ce qui améliore significativement la robustesse et la sécurité globale des systèmes biométriques .

II.2.3 Comparaison des méthodes :

La comparaison suivante présente les caractéristiques et les avantages principaux de chaque méthode de protection des modèles biométriques, à savoir : les techniques cryptographiques, les méthodes modifiables et révoquées, ainsi que les approches hybrides multi-niveaux, afin d'évaluer leur efficacité en termes de sécurité, de fiabilité et d'efficacité opérationnelle.

Tableau II.1 : Comparaison des principales méthodes de protection des templates biométriques [54]

Critère	Chiffrement des Templates	Biométrie Révocable/Transformée	Schémas Hybrides et Multi-Niveaux
Sécurité	Très élevée, dépend des clés cryptographiques	Bonne si transformation non-inversible	Très élevée, multilatère
Révocabilité	Possible via re-chiffrement ou mécanismes clés	Facile avec des transformations réinitialisa blés	Faible à modérée, dépend de la conception
Performance	Peut être lourde computationnellement	Légère, adaptée aux dispositifs limités	Variable, souvent plus coûteux
Complexité	Élevée, nécessite infrastructure cryptographique	Faible à moyenne	Haute, nécessite intégration complexe

II.3 Sécurité des systèmes biométriques

La sécurité des systèmes biométriques vise à protéger les données biométriques et le fonctionnement du système contre toute tentative d'attaque, de falsification ou d'accès non autorisé. Étant donné que les données biométriques sont uniques et impossibles à changer (contrairement aux mots de passe), leur protection est essentielle.

II.3.1 Modèles de menace pour les systèmes biométriques

Les systèmes biométriques présentent plusieurs limitations intrinsèques et vulnérabilités qui affectent leur fiabilité et leur sécurité. Tout d'abord, en raison de la variabilité naturelle des échantillons biométriques d'un même individu, le système peut générer deux types d'erreurs : le faux rejet (False Non-Match), qui empêche l'accès à un utilisateur légitime, et la fausse acceptation (False Match), qui permet l'intrusion d'un imposteur, souvent sans effort (zéro-effort Attac). Ensuite, ces systèmes sont exposés à diverses attaques adversaires provenant d'acteurs internes ou externes. Les attaques internes incluent la collusion, la coercition, la négligence ou

la fraude lors de l'enrôlement, tandis que les attaques externes ciblent l'infrastructure à travers des techniques telles que les chevaux de Troie, les attaques de type Man-In-The-Middle et les attaques par rejeu (replay attacus). Par ailleurs, les systèmes biométriques sont vulnérables à des attaques spécifiques comme les attaques par usurpation (spoofing), où des caractéristiques biométriques falsifiées (par exemple, une empreinte artificielle) sont présentées au capteur, compromettant ainsi la détection de vivacité (liens détection) [55]. Enfin, la fuite des gabarits biométriques (Template laquage) constitue un risque majeur, car la compromission des templates stockés peut permettre la reconstruction des données biométriques originales, ce qui est particulièrement critique puisque les traits biométriques sont irrévocables .

II.3.2 Attaques sur les composants internes

Les attaques sur les composants internes des systèmes biométriques se manifestent principalement par des manipulations durant la phase d'entraînement ou lors de la phase de test. Lors de l'entraînement, un attaquant peut injecter ou modifier malicieusement des données dans la base de données d'apprentissage du détecteur de vivacité ou du modèle de reconnaissance, afin d'influencer la manière dont le système apprend et classe les traits biométriques. Cette modification peut également impliquer la corruption logique des algorithmes ou seuils internes, comme le seuil de vivacité ou de correspondance, pour faire en sorte que le système identifie systématiquement des imposteurs comme des usagers légitimes ou vice versa. Plus précisément, il peut intervenir en ajustant ces seuils pour favoriser une identité spécifique ou pour rejeter tout nouvel utilisateur, compromettant ainsi l'intégrité ou la disponibilité du système. Par ailleurs, des attaques ciblant directement le module de reconnaissance ou le modèle de reconnaissance biométrique permettent de manipuler les résultats de reconnaissance, en biaisant le processus d'identification via des techniques d'attaque d'évasion ou de polisotin. Enfin, la modification ou l'injection de données dans la base biométrique peuvent fausser la correspondance, facilitant des erreurs d'authentification ou permettant à un attaquant de se faire passer pour un utilisateur légitime [56]. Toutes ces stratégies exploitent les vulnérabilités internes pour compromettre la fiabilité, la confidentialité et la disponibilité du système biométrique, rendant la sécurité de ses composants cruciale pour prévenir de telles attaques.

II.3.3 Attaques logicielles et attaques par élévation de privilèges

Les attaques logicielles ainsi que les attaques par élévation de privilèges représentent des menaces importantes en cybersécurité

- **Attaques logicielles :** Les attaques logicielles consistent à exploiter des failles présentes dans les systèmes, les applications ou les réseaux afin d'obtenir un accès non autorisé ou de

provoquer des dommages. Dans les environnements cloud, elles peuvent viser les volumes importants de données échangées entre les entreprises et les fournisseurs de services, ce qui peut entraîner des fuites d'informations ou des compromissions du système [57]. Ces attaques peuvent également être réalisées par des utilisateurs internes malveillants qui disposent déjà d'un accès légitime, ce qui les rend encore plus difficiles à détecter .

- **Élévation de privilèges :** L'élévation de privilèges correspond à des techniques utilisées par un attaquant ou un utilisateur malveillant pour obtenir des droits d'accès plus élevés que ceux qui lui ont été initialement attribués. Les utilisateurs internes représentent un risque particulier, car ils disposent déjà de certains privilèges qu'ils peuvent exploiter à des fins malveillantes. Ce type d'attaque permet d'effectuer des actions non autorisées, d'accéder à des données sensibles ou encore de perturber le fonctionnement des services [58]. Leur détection reste difficile, car elles se déroulent souvent de manière discrète à l'intérieur du système.

II.4 Sécurité des canaux de transmission

La sécurité des canaux de transmission consiste à protéger les données lorsqu'elles sont échangées entre différents systèmes.

II.4.1 Transfert de données biométriques

Le transfert des données biométriques est une étape très sensible en raison de la nature personnelle, unique et permanente de ces données. Il présente plusieurs risques majeurs tels que l'interception, le vol d'identité, les cyberattaques, ainsi que les attaques de type spoofing ou Man-In-The-Middle. Les systèmes centralisés augmentent encore ces vulnérabilités, rendant les fuites de données particulièrement graves et irréversibles. En plus des risques techniques, le transfert international des données pose aussi des défis juridiques liés aux différentes lois de protection des données [54]. Pour limiter ces problèmes, il est nécessaire d'utiliser des méthodes de sécurité robustes comme le chiffrement, le contrôle d'accès et la surveillance continue, ainsi que des mécanismes de sécurité modernes visant à améliorer la protection et la gestion des échanges de données.

II.4.2 Protocoles sécurisés pour la transmission

Les protocoles sécurisés pour la transmission permettent de protéger les données échangées contre l'interception ou l'accès non autorisé. Ils utilisent des mécanismes comme le chiffrement et l'authentification pour garantir la confidentialité des informations, surtout lorsqu'il s'agit de données sensibles comme les données biométriques. Parmi ces protocoles, on trouve notamment le Fuzzy Vault et le Fuzzy Commitment, adaptés à la protection des données biométriques.

- **Fuzzy Vault :** fuzzy vault est une technique cryptographique qui permet de sécuriser un secret à partir de données imprécises ou instables, comme les caractéristiques biométriques. Le système commence par encoder un secret aléatoire dans un polynôme de degré donné, puis évalue ce polynôme sur un ensemble de points extraits des données biométriques de l'utilisateur authentique. Ces paires de points véritables sont ensuite mélangées avec un grand nombre de points leurres (chaff points) générés aléatoirement et ne satisfaisant pas le polynôme, pour former un ensemble désordonné appelé fuzzy vault. Lors de l'authentification, un nouvel ensemble de données biométriques est extrait et utilisé pour tenter de retrouver suffisamment de points correspondant à ceux du fuzzy vault. Si l'intersection contient au moins un certain nombre de points, il est possible de reconstruire le polynôme original par interpolation et de récupérer le secret. Ce mécanisme offre une tolérance aux variations naturelles des données biométriques tout en rendant difficile la récupération du secret pour un attaquant, grâce à l'ajout des points leurres [55]. Ainsi, le fuzzy vault garantit à la fois sécurité et robustesse face aux imprécisions inhérentes aux mesures biométriques, sans nécessiter un ordre précis des données, ce qui le rend particulièrement adapté aux systèmes d'authentification biométrique .
- **Fuzzy Commitment :** est un schéma cryptographique utilisé pour sécuriser des données biométriques en associant une clé secrète à la biométrie de manière à pouvoir la récupérer même en cas de légères variations. Son principe consiste à encoder une clé secrète à l'aide d'un code d'erreur correction, puis à "fuser" cette clé avec la représentation biométrique lors de l'enrôlement, créant ainsi un helper data qui ne révèle pas la biométrie originale [56]. Lors de la vérification, une nouvelle capture biométrique est combinée avec ce helper data pour permettre la récupération de la clé secrète grâce à l'erreur correction, tolérant ainsi les petites différences dans la biométrie entre l'enregistrement initial et la tentative d'authentification .

II.4.3 Attaques réseau :

Une attaque réseau est considérée une action malveillante qui consiste à perturber, voler, modifier, ou intercepter les données qui passent à travers le réseau informatique (comme Internet, le Wi-Fi, et le LAN).

- **Attaque de l'homme du milieu :** est une attaque de sécurité dans laquelle un attaquant s'interpose entre deux entités communicantes afin d'intercepter [57], écouter ou modifier les échanges de données sans autorisation**.**

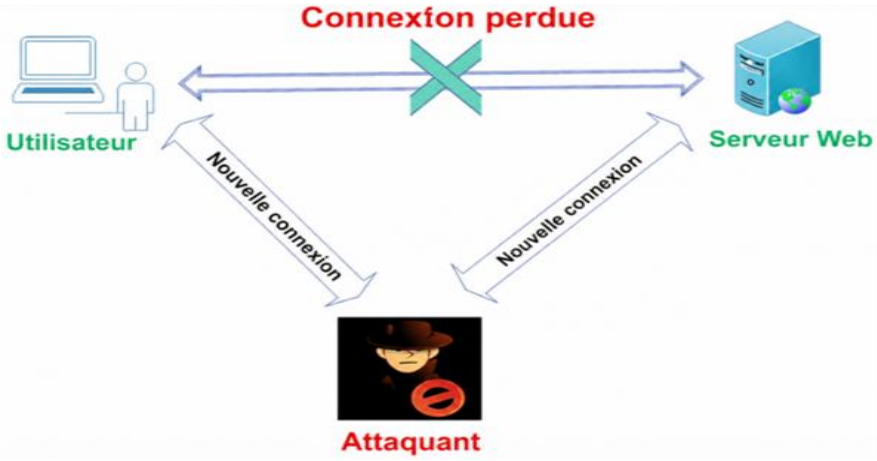


Figure II.1. Schéma conceptuel de l'idéologie de l'attaque de l'homme du milieu [57].

II.5 Système proposé

Dans ce travail, nous présentons un système biométrique sécurisé qui résiste efficacement aux attaques de spoofing. Notre approche repose sur un processus complet qui combine l'extraction de caractéristiques, l'optimisation, ainsi que des mécanismes de protection et de chiffrement des données biométriques.

Les approches classiques se limitent généralement à l'extraction et à la classification des caractéristiques. En revanche, notre système inclut des étapes supplémentaires visant à renforcer la sécurité, améliorer la capacité de discrimination des caractéristiques et assurer la révocabilité de ces dernières.

II.5.1 Sécurité et intégrité des caractéristiques

La sécurité et l'intégrité des données biométriques sont essentielles dans tout système de reconnaissance. En effet, les données biométriques sont très sensibles. Il est donc nécessaire de les protéger contre toute tentative de modification, vol ou réutilisation frauduleuse. Ainsi, notre méthode assure la protection des caractéristiques biométriques en les intégrant avec les mécanismes d'optimisation et de chiffrement. L'objectif est de garantir que les caractéristiques biométriques extraites soient à la fois discriminantes et sécurisées, tout en les rendant impossibles à l'attaque.

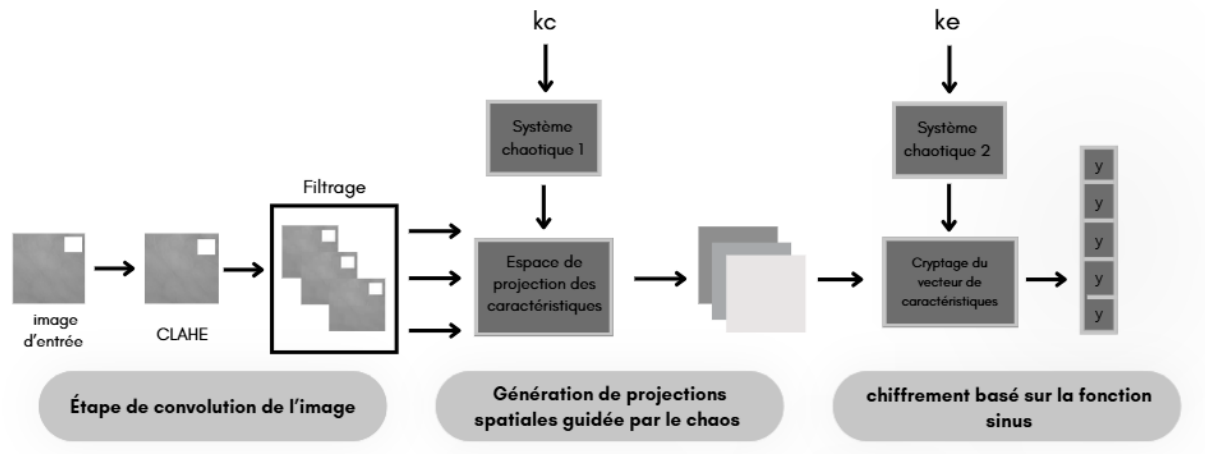


Figure II.2: schéma globale de système biométrique

Afin d'améliorer encore la robustesse et le pouvoir discriminant de l'extraction de caractéristiques, un cadre de traitement en plusieurs étapes est proposé. La méthode proposée suit un cadre comprenant une étape de filtrage, une projection basée sur le chaos utilisant la carte logistique et la génération de matrices chaotiques, ainsi qu'un filtrage gaussien 3D pour l'élimination du bruit et le raffinement des caractéristiques. Par la suite, HOG est utilisé pour obtenir un vecteur de caractéristiques compact et très discriminant à des fins de reconnaissance.

- **Etape 01 : Prétraitement (CLAHE)**

Tout d'abord, l'image d'entrée $I(x, y)$ est améliorée à l'aide de la méthode CLAHE afin d'augmenter le contraste local :

$$I_e(x, y) = CLAHE(I(x, y)) \quad \text{(II.1)}$$

Ou: I(x,y) représente l'image d'entrée, où $x$et $y$sont les coordonnées des pixels, c'est-à-dire qu'ils définissent la position de chaque pixel ainsi que son intensité. La fonction $CLAHE(\cdot)$est une opération qui améliore le contraste local de l'image en la divisant en petites régions et en traitant chaque région séparément tout en réduisant l'amplification du bruit. Enfin, $I_e(x, y)$représente l'image résultante après amélioration, où les détails sont plus visibles et le contraste est mieux équilibré par rapport à l'image original

- **Etape 02 : Filtrage et extraction de patches**

L'image améliorée est ensuite filtrée à l'aide d'un ensemble de filtres $\{F_k\}_{k=1}^{K}$. Chaque filtre est appliqué par convolution sur l'image afin d'obtenir différentes cartes de caractéristiques. Ainsi, on a :

$$I_k(x, y) = I_e(x, y) * F_k(x, y), \qquad k = 1,2, \dots, K \quad \text{(II.2)}$$

Où $(*)$désigne l'opération de convolution. On obtient alors plusieurs cartes de caractéristiques, chacune mettant en évidence des structures locales différentes de l'image, telles que les contours, les textures ou les variations d'intensité.

- **Etape 03 : Projection chaotique**

Pour chaque carte filtrée, une projection chaotique est appliquée en utilisant la carte logistique :

$$x_{n+1} = ax_n(1 - x_n) \quad \text{(II.3)}$$

Ou: x_n représente la valeur actuelle, x_{n+1}la valeur suivante, et $a$est un paramètre de contrôle qui influence le comportement de la suite (stable ou chaotique).

À partir de cette suite, on génère une matrice chaotique $C_k(x, y)$contenant des valeurs pseudo-aléatoires. Ensuite, cette matrice est combinée avec chaque carte filtrée par une multiplication élément par élément :

$$\mathrm{I}'_{\mathrm{k}}(x, y) = I_k(x, y) \cdot C_k(x, y) \quad \text{(II.4)}$$

Ainsi, chaque pixel de l'image est modifié par une valeur chaotique correspondante. Cette opération introduit une forte variabilité non linéaire dans les données, ce qui rend les informations plus complexes et améliore la sécurité ainsi que la robustesse du système.

- **Etape 04 : Extraction des caractéristiques (HOG)**

Les caractéristiques sont extraites à partir du volume filtré $V_g$en utilisant le descripteur Histogram of Oriented Gradients (HOG), qui permet de représenter l'information structurelle de l'image à travers les variations locales d'intensité.

1. Calcul des gradients : Dans un premier temps, les gradients de l'image sont calculés selon les directions horizontale et verticale

$$G_x = \frac{\partial V_g}{\partial x}, G_y = \frac{\partial V_g}{\partial y} \quad \text{(II.5)}$$

Ou : V_g le volume ou image filtrée, G_x: gradient selon l'axe horizontal, G_y: gradient selon l'axe vertical et $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$: dérivées partielles représentant les variations d'intensité

2. Calcul de l'amplitude et de l'orientation

$$M = \sqrt{G_x^2 + G_y^2} \quad \text{(II.6)}$$

$$\theta = \arctan\left(\frac{G_y}{G_x}\right) \quad \text{(II.7)}$$

où : M c'est la magnitude du gradient (intensité du changement) , θ: orientation du gradient (direction du changement) et $\mathrm{G_x}, \mathrm{G_y}$: composantes des gradients

3. Construction des histogrammes d'orientation

$$H = HOG(V_g) \quad \text{(II.8)}$$

Où : Hc'est le vecteur final de caractéristiques HOG, $HOG(\cdot)$: fonction de calcul des histogrammes d'orientation et V_g: image filtrée

Chaque histogramme représente la distribution des directions des contours dans une région locale de l'image.

II.5.2 Exigences préliminaires

Afin de satisfaire les exigences préliminaires, nous avons intégré un ensemble de techniques clés visant l'extraction des caractéristiques, l'amélioration des performances et la sécurisation du système.

- Construction de banques de filtres (PCA et SC) : Afin d'améliorer la qualité de la représentation des données biométriques, la banque de filtres repose sur deux approches complémentaires : l'Analyse en Composantes Principales (ACP) et le Sparse Coding (SC).

Dans un premier etape , l'image biométrique est décomposée en petits blocs appelés patches, afin de capturer les informations locales.

Soit une image :

$$I \in R^{H \times W} \quad \text{(II.9)}$$

Où : Hdésigne la hauteur de l'image et Wsa largeur.

Des patches de taille $p \times p$sont ensuite extraits à partir de l'image :

$$P_{i,j} = I(i: i + p - 1, j: j + p - 1) \quad \text{(II.10)}$$

Où : $P_{i,j}$représente un patch local extrait à la position (i, j), et $p$correspond à la taille du patch.

Chaque patch est ensuite transformé en vecteur colonne par une opération de vectorisation :

$$X_{i,j} = vec(P_{i,j}) \in \mathbb{R}^{p^2} \quad \text{(II.11)}$$

où $\mathrm{vec}(\cdot)$désigne l'opération de mise en forme du patch en vecteur.

Afin de réduire l'influence des variations d'illumination, une normalisation est appliquée en soustrayant l'intensité du pixel central :

$$X_{i,j} = X_{i,j} - I_c \quad \text{(II.12)}$$

Où : $I_c$représente l'intensité du pixel central du patch.

Enfin, l'ensemble des patches extraits est regroupé sous forme d'une matrice de données :

$$X = [x_1, x_2, \dots, x_N] \quad \text{(II.13)}$$

Où $x_1, x_2, \dots, x_N$ représentent les vecteurs des patches et N désigne le nombre total de patches extraits.

- Construction des filtres par PCA : L'Analyse en Composantes Principales (PCA) est utilisée pour extraire les directions principales de variation dans les données. Elle permet de construire des filtres représentant les structures globales des images biométriques.

1. Calcul de la moyenne : Dans cette étape, on calcule le vecteur moyen de tous les patches extraits

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \text{(II.14)}$$

Où : x_i représente un patch vectorisé , N le nombre total de patches et μ c'est la moyenne globale des données

2. Centrage des données :

$$\tilde{X} = X - \mu \quad \text{(II.15)}$$

Ou : X c'est la matrice des patches et $\tilde{X}$ les données centrées

On soustrait la moyenne de chaque patch pour éliminer l'effet global (comme l'illumination). Cela permet de garder uniquement les variations importantes entre les données.

3. Matrice de covariance :

$$C = \frac{1}{N}\tilde{X}\tilde{X}^T \quad \text{(II.16)}$$

Où : C c'est la matrice de covariance et N: nombre de patches

On calcule la matrice de covariance pour mesurer la relation entre les différentes dimensions des patches. Elle permet d'identifier les directions principales de variation.

4. Décomposition en valeurs propres :

$$Cv_k = \lambda_k v_k \quad \text{(II.17)}$$

Où : v_k le vecteur propre (direction principale) et λ_k la valeur propre (importance de la direction)

On décompose la matrice de covariance pour obtenir les directions principales (vecteurs propres) et leur importance (valeurs propres). Les plus grandes valeurs propres contiennent l'information la plus importante.

5. Sélection des composantes principales :

$$W = [v_1, v_2, \dots, v_k] \quad \text{(II.18)}$$

Où : W c'est matrice des vecteurs sélectionnés et v_k les vecteurs propres triés selon les valeurs propres

6. Transformation en filtres :

$$F_k = R(v_k, p, p) \quad \text{(II.19)}$$

Ces filtres capturent les structures globales telles que les contours et les gradients.

- Construction des filtres par Sparse Coding (SC) : L'Analyse en Composantes Principales (ACP) se base sur une vue globale des données. Le Sparse Coding (SC) cherche à décrire chaque patch avec un petit nombre de filtres. Cette approche saisit les structures locales fines et renforce le pouvoir discriminant des caractéristiques extraites.

▪ Modélisation mathématique du Sparse Coding : Soit $X = [\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N] \in \mathbb{R}^{p^2 \times N}$ la matrice contenant les vecteurs patches extraits de l'image.

Le principe du Sparse Coding consiste à approximer chaque vecteur $\mathbf{x}_i$ comme une combinaison linéaire d'un nombre réduit d'atomes issus d'un dictionnaire D:

$$X \approx D \cdot A \quad \text{(II.20)}$$

Où : X la matrice des patches ,D c'est le dictionnaire (filtres appris) et A les coefficients d'activation.

▪ Problème d'optimisation : L'objectif est de minimiser l'erreur de reconstruction tout en imposant une contrainte de parcimonie :

$$\min_{D,A} \|X - DA\|_F^2 \text{ sous la contrainte } \| a_i \|_2 \leq T \quad \text{(II.21)}$$

Où : $\|\cdot\|_F$ désigne la norme de Frobenius et $X - DA$: erreur de reconstruction

▪ Étapes de résolution :

1. Codage parcimonieux (OMP) : Pour un dictionnaire fixé D, chaque vecteur $\mathbf{x}_i$est représenté par :

$$a_i = arg\min_a \| x_i - Da \|_2^2 \;\; s.c. \;\; \| a \|_0 \leq T \quad \text{(II.22)}$$

Ou: x_i: patch, a_i les coefficients du patch, T c'est le nombre maximal de filtres utilisés et $\| a \|_0$ c'est le nombre de coefficients non nuls

Cette étape est généralement résolue par l'algorithme Orthogonal Matching Pursuit (OMP).

2. Mise à jour du dictionnaire (K-SVD) : Une fois les coefficients calculés, le dictionnaire est mis à jour en minimisant :

$$\min_{D,A} \|X - DA\|_F^2 \quad \text{(II.23)}$$

Chaque atome $d_k$est ajusté en utilisant une décomposition en valeurs singulières (SVD):

$$E_k = X - \sum_{j \neq k} d_j a_j \quad \text{(II.24)}$$

$$\min_{d_k, a_k} \|E_k - d_k a_k\|_F^2 \quad \text{(II.25)}$$

Où : E_k: erreur associée au filtre k, d_j: filtres du dictionnaire et a_j: coefficients associés

- Construction des filtres : À l'issue de l'apprentissage, les colonnes du dictionnaire Dreprésentent les filtres :

$$F_k = R(d_k, p, p) \quad \text{(II.26)}$$

- **Génération de projections spatiales guidée par le chaos :** Cette étape consiste à générer des projections spatiales en utilisant un système chaotique. Contrairement aux méthodes classiques, cette approche permet d'obtenir des filtres pseudo-aléatoires offrant une meilleure diversité et robustesse.

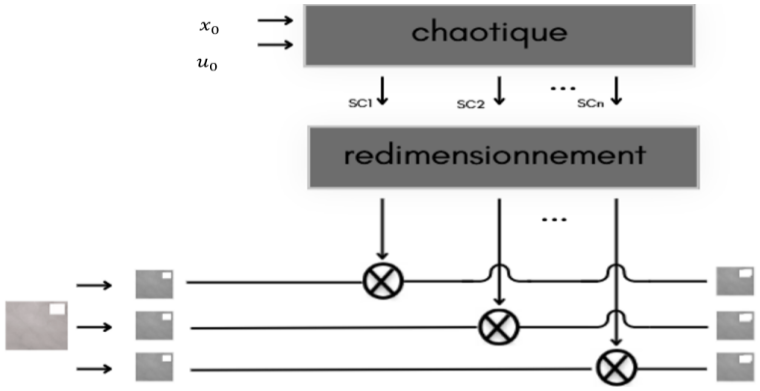


Figure II.3: Schéma de génération des projections spatiales chaotiques

➢ **Étape 01 :** Génération de la suite chaotique

La suite chaotique est générée à l'aide de la carte logistiqu

$$x_{i+1} = a \,.\, x_i.\,(1 - x_i) \quad \text{(II.27)}$$

Où : x_i la valeur courante de la suite, x_{i+1}la valeur suivante et a le paramètre de contrôle

Cette équation produit une séquence non linéaire, sensible aux conditions initiales, idéale pour générer des valeurs pseudo-aléatoires.

➢ **Etape 02 :** Génération d'une matrice chaotique

À partir des suites (S_i), générées par des systèmes chaotiques:

$$S_i = \{x_1, x_2, \dots, x_{h\times w}\} \quad \text{(II.28)}$$

Les différentes séquences sont ensuite réorganiser sous formes des espaces de projection (Matrices de la même taille que l'image originale) :

$$M_i = F_R(S_i) \in \mathbb{R}^{h\times w} \quad \text{(II.29)}$$

Où F_R est une fonction de réorganisation, $h \times w$ les dimensions de la matrice et M_i matrice de projection obtenue. Cette étape permet de transformer une suite 1D en une structure 2D exploitable comme masque spatial.

➢ **Etape03** : Projection spatiale chaotique

La matrice chaotique est appliquée sur chaque carte filtrée :

$$I'_k(x, y) = I_k(x, y) \cdot M_k(x, y) \quad \text{(II.30)}$$

Où : $I_k(x,y)$ k-ième image filtrée, $M_k(x,y)$ la matrice chaotique associée, $I'_k(x,y)$: image projetée et $(\cdot)$ produit élément par élément

Cette opération modifie les valeurs spatiales de l'image de manière pseudo-aléatoire, ce qui augmente la diversité des caractéristiques extraites.

- **Optimisation par essaim de particules** : Pour optimiser les paramètres du système proposé, nous utilisons l'algorithme d'optimisation par essaim de particules (PSO). L'algorithme d'optimisation par essaim de particules (PSO) imite le comportement collectif des oiseaux et des bancs de poissons. L'algorithme d'optimisation par essaim de particules (PSO) trouve la solution optimale dans l'espace de grande dimension.

➢ Formulation du problème: Le but de l'optimisation est de déterminer les paramètres optimaux du modèle chaotique utilisés dans la projection spatiale. Le vecteur des variables à optimiser est défini par :

$$x = [\mathrm{x}_0, \mathrm{u}_1, \mathrm{u}_2, \dots, \mathrm{u}_k] \tag{II.31}$$

Où : x le vecteur des paramètres à optimiser, x_0 condition initiale de la suite chaotique u_i le paramètres de contrôle du système

➢ Fonction objective: Le problème d'optimisation consiste à minimiser une fonction objectif définie par les performances du système :

$$\min_x f(x) \tag{II.32}$$

Où: $f(\mathbf{x})$ fonction de performance du système

➢ Modélisation des particules : Dans PSO, chaque particule correspond à une solution candidate :

$$x_i = (x_{i1}, x_{i2}, \dots, x_{id}) \tag{II.33}$$

Dans notre cas :

$$x_i = [x_0, u_1, u_2, \dots, u_k] \tag{II.34}$$

Où : x_i la position de la particule i et d: dimension du problème

➢ Équations d'évolution du PSO :

- Mise à jour de la vitesse :

$$v_i^{t+1} = w v_i^t + c_1 r_1 (p_i - x_i^t) + c_2 r_2 (g - x_i^t) \tag{II.35}$$

Où: v_i^t la vitesse de la particule à l'itération t, w la factrice d'inertie, c_1, c_2 les coefficients d'apprentissage, r_1, r_2 les nombres aléatoires dans $[0, 1]$, p_i la meilleure position individuelle et g la meilleure position globale.

- Mise à jour de la position :

$$v_i^{t+1} = x_i^t + v_i^{t+1} \quad \text{(II.36)}$$

Où : x_i^{t+1} la nouvelle position et x_i^t la position actuelle

➢ Lien avec la Logistique Map: Dans l'implémentation proposée, on réalise l'optimisation de façon indirecte en utilisant une dynamique chaotique définie par la Logistique Map :

$$x_{t+1} = ax_t(1 - x_t) \quad \text{(II.37)}$$

Les paramètres utilisés dans la projection sont ensuite définis par :

$$U_i = 3.57 + 0.42 \cdot u_i \quad \text{(II.38)}$$

Ou : x_t la valeur de la suite chaotique, a le paramètre de contrôle et U_i paramètres utilisés dans la projection

ce qui garantit :

$$u_i \in [3.57,3.99]$$

intervalle correspondant au régime chaotique.

➢ Rôle dans la projection spatiale : Dans la fonction Projections PC, ces paramètres sont utilisés pour générer des matrices aléatoires :

$$\text{ImgCONVPr}_\text{i} = \text{ImgCONV}_i \odot M_i \quad \text{(II.39)}$$

Où : $ImgCONV_i$ l'image filtrée, M_i la matrice chaotique et $\odot$ produit élément par élément

➢ Interprétation mathématique : Même si le PSO n'est pas mis en place directement, le système applique le même principe:

- exploration de l'espace des solutions via chaos
- recherche de paramètres optimaux
- amélioration des performances globales

La solution optimale est alors donnée par :

$$x^* = arg\ min\ f(x) \quad \text{(II.40)}$$

- **Schéma de chiffrement basé sur la fonction sinus:** Pour assurer la sécurité des caractéristiques biométriques, on propose un schéma de chiffrement basé sur la fonction sinus. Cette méthode utilise la nature non linéaire et pseudo-aléatoire de la fonction sinus pour réaliser une transformation difficilement réversible sans la connaissance des paramètres secrets.

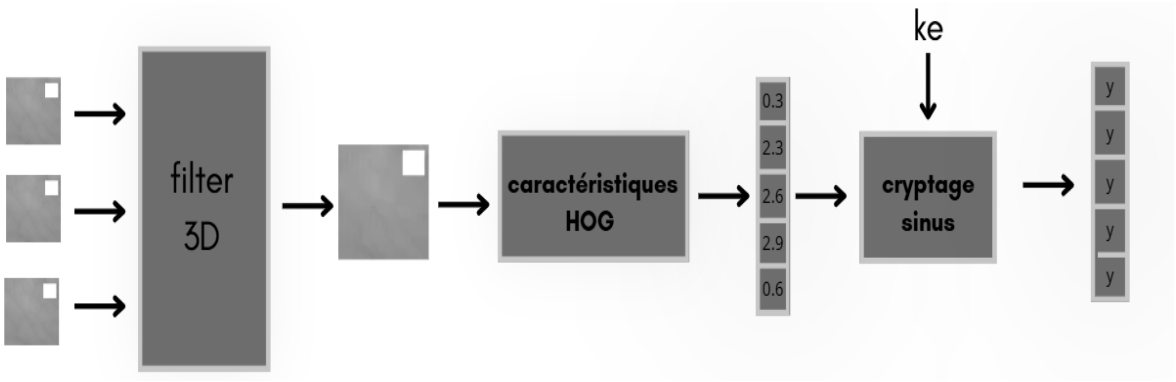


Figure II.4: Schéma du chiffrement sinusoïdal des caractéristiques

➢ Modélisation mathématique : Soit le vecteur de caractéristiques extrait :

$$F = [f_1, f_2, \dots, f_N] \in \mathbb{R}^N \quad \text{(II.41)}$$

Où f_i représente la i-ème composante et N la dimension du vecteur.

Le principe du chiffrement consiste à appliquer une transformation non linéaire sur chaque composante du vecteur F.

➢ Fonction de chiffrement : La transformation sinusoïdale est définie par :

$$c_i = \sin(\alpha \cdot f_i + \beta) \quad \text{(II.42)}$$

Où α est un facteur d'échelle (clé secrète) et β est un décalage de phase (clé secrète).

Le vecteur chiffré est alors :

$$C = [c_1, c_2, \dots, c_N] \quad \text{(II.43)}$$

Cette transformation permet de rendre la relation entre les données originales et les données chiffrées fortement non linéaire.

➢ Intégration du chaos : Afin de renforcer la sécurité, les paramètres αet βpeuvent être générés à partir d'un système chaotique tel que la Logistic Map :

$$x_{t+1} = a x_t (1 - x_t) \quad \text{(II.44)}$$

On obtient ainsi :

$$c_i = \sin(\alpha \cdot f_i + \beta) \quad \text{(II.45)}$$

Où $\alpha_i$et $\beta_i$dépendent de la suite chaotique générée. Cette approche introduit une variabilité dynamique qui augmente la complexité du chiffrement.

➢ Propriétés du schéma :

▪ Non-linéarité : La fonction sinus est fortement non linéaire :

$$c_i = \sin(\cdot) \quad \text{(II.46)}$$

- Rend la reconstruction des données originale complexe.

▪ Sensibilité aux paramètres : Une faible variation des clés entraîne une grande variation du signal chiffré :

$$\Delta c_i \gg \Delta f_i \tag{II.47}$$

propriété essentielle pour le sécurit

- Distribution bornée : Les valeurs chiffrées vérifient :

$$c_i \in [-1,1] \tag{II.48}$$

ce qui garantit une dispersion pseudo-aléatoire des données.

➢ Interprétation dans le système proposé : Dans le système proposé, le processus de sécurisation des données biométriques repose sur une chaîne de traitement composée de plusieurs étapes successives : extraction des caractéristiques, projection chaotique, puis chiffrement sinus. Après l'extraction des caractéristiques biométriques, une projection chaotique est appliquée afin d'introduire une transformation non linéaire des données, augmentant ainsi leur complexité et leur robustesse face aux attaques potentielles. Ensuite, un mécanisme de chiffrement basé sur une fonction sinus est utilisé pour renforcer la confidentialité des informations biométriques et assurer une meilleure protection contre les accès non autorisés. Cette combinaison permet d'améliorer simultanément la sécurité et la fiabilité du système proposé.

➢ Inversion (cas théorique) : Si les paramètres sont connus, une inversion théorique est possible :

$$f_i = \frac{\arcsin(c_i)}{\alpha} \tag{II.49}$$

Cependant, en pratique, cette inversion est difficile à cause de :

- la périodicité de la fonction sinus.
- la présence de bruit.
- la variabilité des paramètres.

Conclusion

L'analyse menée dans ce chapitre met en évidence l'importance cruciale de la sécurité dans les systèmes biométriques, notamment en ce qui concerne la protection des templates, qui constituent des éléments hautement sensibles. Les différentes vulnérabilités identifiées ainsi que les multiples vecteurs d'attaque démontrent que ces systèmes restent exposés à des risques significatifs. Les mécanismes de protection étudiés, tels que le chiffrement, la biométrie révocable et les approches hybrides, offrent des solutions pertinentes, bien qu'ils présentent certaines limites en termes de complexité et de performance. Dans ce contexte, l'intégration de techniques avancées apparaît comme une nécessité afin d'assurer un niveau de sécurité plus élevé. Ainsi, les concepts développés dans ce chapitre constituent une base fondamentale pour la mise en œuvre et l'évaluation de l'approche proposée dans la suite de ce travail.

Chapitre 3

Résultats expérimentaux

Résumé

Dans ce chapitre, nous avons présenté une étude expérimentale complète visant à évaluer les performances et la sécurité du système biométrique proposé. Nous avons d'abord décrit la base de données utilisée ainsi que la configuration du système et le protocole d'évaluation adopté. Ensuite, nous avons analysé les performances du système à travers différentes configurations, notamment le système non sécurisé, sécurisé, optimisé et fusionné, tout en mettant en évidence l'impact des filtres (PCA et SC) sur la qualité de reconnaissance. Les résultats ont montré une amélioration progressive des performances, particulièrement grâce à l'optimisation et à la fusion. Par ailleurs, nous avons évalué la sécurité du système à travers plusieurs analyses, telles que l'étude statistique par histogramme, l'analyse de l'espace des clés, la sensibilité aux clés ainsi que les tests d'aléa NIST. L'ensemble des résultats confirme l'efficacité, la robustesse et le haut niveau de sécurité du système proposé.

III.1 Base de données

III.2 Résultats expérimentaux

III.3 Evaluation du système biométrique

III.3 Evaluation du système proposé

Introduction

Ce chapitre est consacré à la validation expérimentale du système biométrique proposé L'objectif principal est d'évaluer ses performances ainsi que son niveau de sécurité dans différents scénarios. Pour cela, nous nous appuyons sur une base de données adaptée, que nous présentons dans un premier temps. Ensuite, nous décrivons la configuration du système et les différentes stratégies mises en œuvre. Enfin, nous exposons le protocole expérimental suivi, avant d'analyser les résultats obtenus

III.1 Base de données

Pour évaluer les performances de notre système, nous avons utilisé la base de données publique d'empreintes palmaires développée par l'Université Polytechnique de Hong Kong (PolyU) [59]. Cette base de données se compose d'images multispectrales d'empreintes palmaires collectées auprès de 400 individus à l'aide d'un dispositif d'imagerie multispectrale spécialisé.

Les participants comprennent à la fois des étudiants et des membres du personnel de PolyU, dont 195 hommes et le reste des femmes, âgés de 20 à 60 ans. Chaque sujet a participé à deux sessions d'acquisition, fournissant environ 12 images (six par session), avec un intervalle moyen de neuf jours entre les sessions.

Toutes les images ont été capturées dans des conditions d'éclairage variées afin d'introduire une variation intra-classe. La base de données comprend un total de 14 400 images, réparties sur quatre bandes spectrales : Rouge (R), Vert (G), Bleu (B) et proche infrarouge (NIR), avec 3 600 images par bande.

Dans nos expériences, nous utilisons la bande NIR, qui permet de capturer efficacement le motif des veines de la paume (modalité des veines palmaires).

III.2 Résultats expérimentaux

Cette section présente les résultats expérimentaux du système proposé. Nous décrivons d'abord la configuration adoptée, puis le protocole d'évaluation utilisé pour analyser les performances.

III.2.1 Configuration du système

Les expériences ont été réalisées à l'aide du logiciel MATLAB 2014a, sous le système d'exploitation Windows 11 Professionnel. La plateforme matérielle utilisée est un ordinateur portable HP ProBook 640 G2, équipé d'un processeur Intel(R) Core(TM) i5-6300U cadencé à 2.40 GHz et d'une mémoire vive de 8 Go. L'implémentation du système biométrique proposé repose à la fois sur les fonctions intégrées de MATLAB et sur des routines spécifiques développées pour répondre aux besoins de l'étude.

III.2.2 Protocole d'évaluation

Afin d'évaluer les performances du système biométrique proposé, une base de données composée de 6 000 images appartenant à 500 individus a été utilisée. Chaque individu dispose de 12 images. Cette base a été divisée en deux sous-ensembles : 60 % pour l'apprentissage (soit 7 images par individu, totalisant 3 500 images) et 40 % pour les tests (soit 5 images par individu, totalisant 2 500 images). Lors de la phase de test, un grand nombre de comparaisons a été effectué en utilisant un classificateur SVM linéaire, générant des scores pour les utilisateurs légitimes ainsi que pour les utilisateurs imposteurs.

L'étude expérimentale a été structurée en deux parties principales. La première vise à évaluer les performances du système en termes de précision et d'efficacité, tandis que la seconde est consacrée à l'analyse du niveau de sécurité offert par l'approche proposée, notamment à travers l'utilisation de techniques basées sur des systèmes chaotiques pour la protection des caractéristiques biométriques.

III.3 Evaluation du système biométrique

Dans cette partie, nous évaluons les performances du système biométrique proposé à travers une méthodologie expérimentale rigoureuse, basée sur la construction et l'apprentissage d'une banque de filtres combinant l'Analyse en Composantes Principales (PCA) et la représentation parcimonieuse (Sparse Coding – SC). L'objectif principal est d'évaluer la capacité du système à extraire des caractéristiques discriminantes à partir des images biométriques, tout en assurant une représentation robuste et efficace des données.

Le processus d'évaluation comporte plusieurs étapes essentielles. Dans un premier temps, on extrait un ensemble de patches à partir des images d'apprentissage à l'aide d'une technique de décomposition locale (PDV), afin de capturer les variations spatiales et les micro-textures

caractéristiques. Ces patches sont ensuite exploités pour construire une base d'apprentissage riche et représentative.

On commence par extraire les composantes les plus importantes à l'aide de l'Analyse en Composantes Principales (PCA). Cette méthode réduit la dimension des données tout en conservant l'essentiel de l'information, ce qui améliore la représentation et réduit le bruit.

Dans une deuxième étape, on applique la représentation parcimonieuse (SC) en construisant un dictionnaire initial avec l'algorithme K-means, puis en l'optimisant avec l'algorithme K-SVD. Ce dernier alterne entre deux opérations principales : le codage parcimonieux (via OMP – Orthogonal Matching Pursuit) et la mise à jour du dictionnaire. Cette procédure itérative permet d'obtenir des filtres adaptés aux structures intrinsèques des données biométriques.
Cette méthode d'évaluation expérimentale repose sur la modification des paramètres importants du système, notamment la taille des filtres (patchSize) et le nombre de filtres (dictSize). En effet, ces deux paramètres ont un impact direct sur la qualité de la représentation et donc sur la performance du système en termes de reconnaissance.

Finalement, les filtres extraits par la PCA ainsi que ceux obtenus par la SC sont analysés visuellement afin d'évaluer leur aptitude à extraire des traits discriminants. Cette analyse visuelle, couplée aux mesures quantitatives, permet de mieux comprendre le comportement de chaque type de filtre en fonction de la performance du système.

De ce fait, cette méthodologie souligne l'efficacité de la combinaison PCA–SC dans la représentation des caractéristiques biométriques, qui a un impact positif sur la performance du système.

III.3.1 Représentation des filtres (PCA et SC) :

Afin d'analyser les caractéristiques extraites par les approches PDVs-PCA et PDVs-SC, les filtres convolutionnels générés sont représentés en trois dimensions dans la figure 3.1.

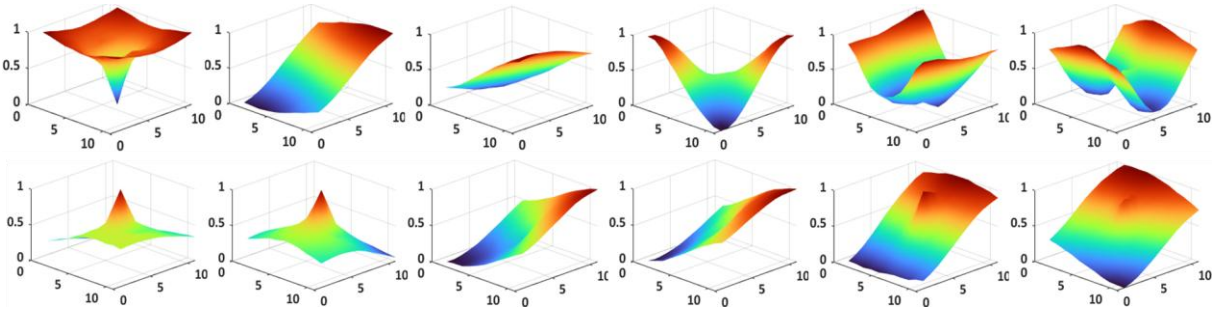


Figure III.1 : Filtres PDVs-SC et PDVs-PCA de taille 11 × 11;(En haut) Filtres basés sur PDVs-PCA et (en bas) Filtres basés sur PDVs-SC.

La figure 3.1 présente les filtres convolutionnels de taille (11 * 11) générés à partir des images de veines palmaires en utilisant les approches PDVs-PCA et PDVs-SC. Les filtres obtenus par la méthode PDVs-PCA sont affichés dans la première ligne, tandis que ceux issus de la méthode PDVs-SC sont représentés dans la deuxième ligne.

On observe que les filtres basés sur PCA présentent des variations plus régulières et progressives, traduisant une représentation globale des caractéristiques principales des images biométriques. En revanche, les filtres basés sur SC mettent davantage en évidence certaines structures localisées et des réponses plus discriminantes.

Cette différence reflète le comportement des deux approches d'extraction de caractéristiques et influence directement les performances du système biométrique proposé.

III.3.2 Système non sécurisé :

Cette section porte sur la construction et l'évaluation des banques de filtres pour les deux méthodes de représentation des données, à savoir l'Analyse en Composantes Principales (PCA) et le Sparse Coding (SC), utilisées dans le système biométrique proposé. L'objectif est d'étudier l'impact des caractéristiques de la méthode de codage des filtres sur les performances globales du système.

Dans les deux cas, la génération des filtres repose sur un processus d'apprentissage à partir de patches extraits de la Région d'Intérêt (ROI). Ces patches contiennent les informations texturales locales qui caractérisent les motifs biométriques.

Le nombre de filtres est fixé dans l'intervalle [2, 3, 4, 5, 6] afin d'analyser l'influence de la taille du dictionnaire sur la qualité de la représentation des données. De plus, différentes tailles de filtres sont considérées : 7×7, 9×9, 11×11, 13×13 et 15×15. Ce choix permet d'étudier l'effet de l'étendue spatiale sur les capacités d'extraction des caractéristiques.

L'approche basée sur la PCA consiste à apprendre un dictionnaire de filtres via la projection des patches sur les principales directions de variance de la distribution des données. Ces directions correspondent aux vecteurs propres de la matrice de covariance et constituent une représentation compressée de l'espace d'entrée.

À l'inverse, la méthode Sparse Coding (SC) consiste à apprendre un dictionnaire de manière optimisée, où chaque patch est représenté comme une combinaison parcimonieuse des atomes du dictionnaire. Ainsi, les filtres obtenus présentent un pouvoir discriminant potentiellement plus élevé que ceux issus de la PCA.

Les expériences sont menées avec différents paramètres de filtres afin d'identifier la configuration optimale en termes de performances du système biométrique.

Les résultats expérimentaux fournissent des informations importantes sur l'influence de la taille du filtre et du nombre de filtres sur le taux d'erreur de reconnaissance du système biométrique proposé basé sur l'empreinte de la paume. Dans ce contexte, la performance des filtres basés sur PCA est d'abord analysée. Les résultats correspondants sont illustrés à l'aide de graphiques en barres groupées.

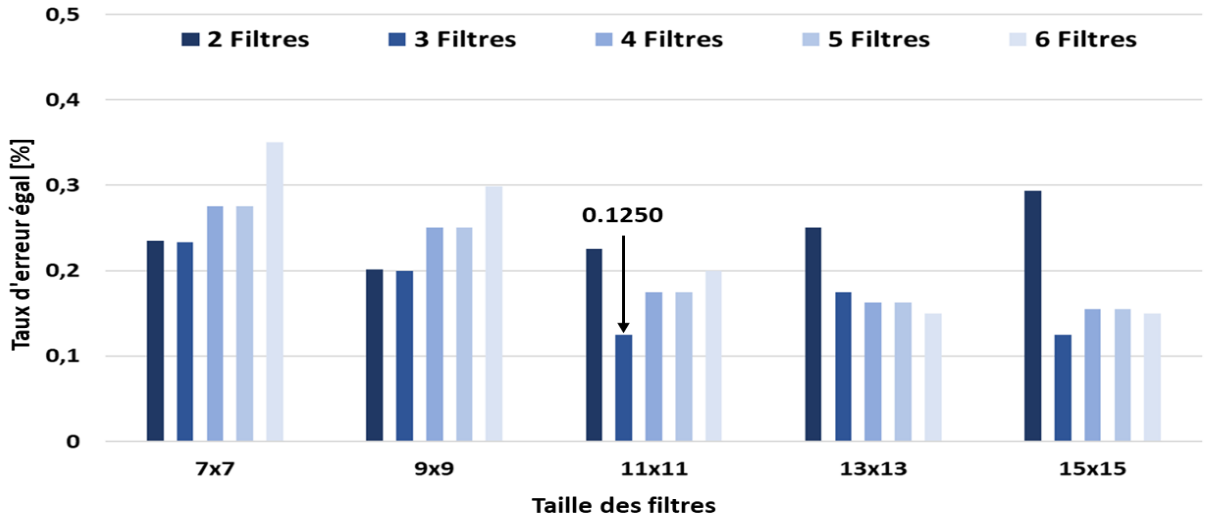


Figure III.2: Évaluation des systèmes non sécurisés à base de filtres PCA

À partir des résultats présentés ci-dessus, on peut constater que les performances du système dépendent fortement à la fois de la taille des filtres et du nombre de filtres utilisés. L'utilisation de petits filtres (7×7) entraîne des valeurs élevées de l'EER, surtout lorsque le nombre de filtres augmente, ce qui indique de faibles performances dues à l'incapacité de ces filtres à discriminer efficacement l'information. La valeur maximale de l'EER, proche de 0,35% pour $T_0 = 0{,}7146$, a été observée avec la configuration (7×7×6 filtres) .En revanche, les performances du système s'améliorent avec l'utilisation de grands filtres, mais les meilleurs résultats sont obtenus avec des tailles de filtres intermédiaires (11×11). Cela s'explique par le fait que les filtres de taille intermédiaire permettent d'extraire l'information tout en réduisant simultanément le bruit.

Les résultats de l'expérience ont également montré que le nombre de filtres utilisés joue un rôle crucial. L'utilisation d'un nombre approprié de filtres (environ 3) donne de meilleures performances que l'utilisation d'un nombre plus élevé (jusqu'à 6), où les performances du système se dégradent. Cela peut être attribué au surapprentissage (overfitting) ou à l'introduction d'informations redondantes dans le système. La valeur minimale de l'EER, égale à 0,125% a $T_0 = 0{,}729$, a été obtenue dans deux configurations : (11×11, 3 filtres) et (15×15, 3 filtres). Néanmoins, la configuration (11×11, 3 filtres) apparaît comme la plus préférable, car elle offre des performances similaires avec une complexité moindre et une meilleure efficacité.

L'étape suivante consiste à analyser la performance des filtres basés sur le Sparse Coding (SC), suivie de la présentation des résultats correspondants à l'aide de diagrammes en barres groupées.

Les filtres de petites dimensions (par exemple (7×7)) présentent des performances relativement faibles, car ils ne parviennent pas à extraire suffisamment d'informations discriminantes à partir des données. Avec l'augmentation de la taille des filtres, on observe une amélioration progressive des performances, en particulier pour les filtres de dimensions intermédiaires (par exemple (11×11) et (13×13)), grâce à un compromis adéquat entre l'extraction des caractéristiques et la réduction du bruit.

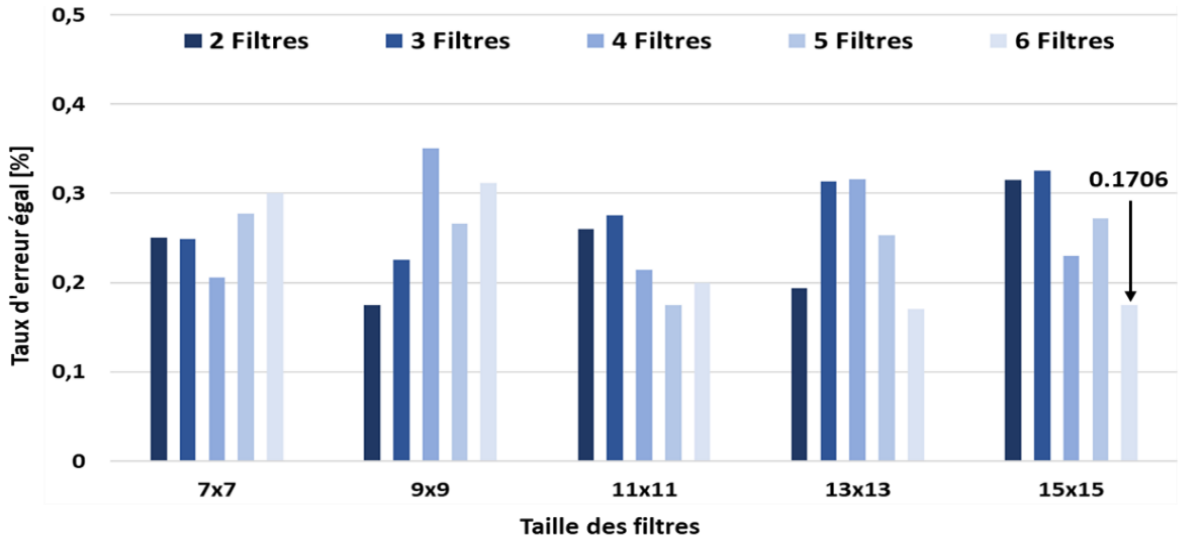
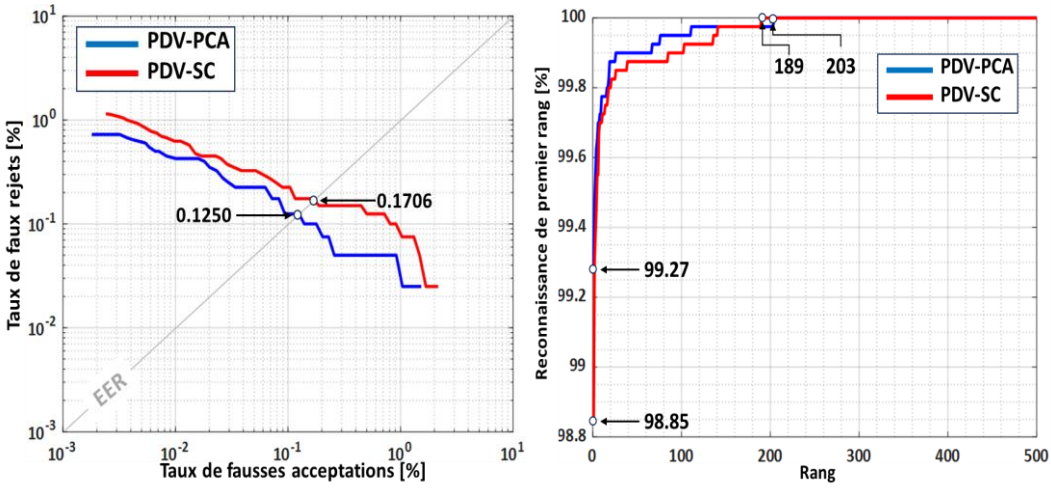


Figure III.3: Évaluation des systèmes non sécurisés à base de filtres SC

Cependant, cette amélioration ne peut pas être considérée comme totalement régulière, car par exemple la configuration (9×9 avec 4 filtres) donne les plus mauvaises performances, avec une EER atteignant 0,35% pour $T_0 = 0{,}7058$. Ce résultat peut être expliqué par une représentation inadéquate des caractéristiques ou par l'introduction d'informations redondantes affectant la capacité discriminante du système.

Par ailleurs, en ce qui concerne le nombre de filtres, l'approche optimale semble consister à choisir un nombre suffisamment élevé mais pas excessif, afin d'éviter les redondances et les informations non pertinentes.

Ainsi, la configuration optimale est (13×13 avec 6 filtres), qui donne la plus faible valeur d'EER, soit 0,1706% pour $T_0 = 0{,}7184$.



(a) (b)

Figure III.4: Évaluation des systèmes non sécurisés les plus performants : analyse des courbes DET et CMC : (a) courbes DET et (b) courbes CMC

La comparaison des performances entre les deux approches PDV-PCA et PDV-SC, évaluées à l'aide des courbes DET et CMC, met en évidence une supériorité globale de la méthode PDV-PCA. En effet, l'analyse des courbes DET montre que cette approche présente un Equal Error Rate (EER) plus faible, estimé à 0,125% a $T_0 = 0{,}729$, contre 0,1706 % pour $T_0 = 0{,}7184$.dans le cas de PDV-SC. Cette différence traduit une meilleure capacité de discrimination entre les classes ainsi qu'une réduction des erreurs de classification et des fausses acceptations/rejets.

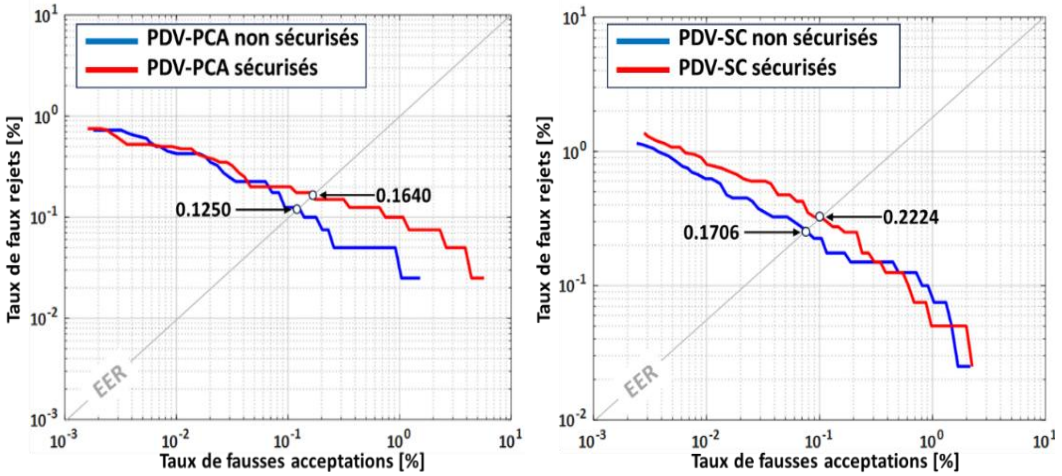
Par ailleurs, l'analyse des courbes CMC montre que l'approche PDV-PCA atteint des taux de reconnaissance légèrement supérieurs à ceux obtenus par PDV-SC. Le taux de reconnaissance maximal obtenu avec PDV-PCA atteint environ 99,27 %, tandis que celui de PDV-SC est d'environ 98,85 %. De plus, PDV-PCA présente une meilleure stabilité aux premiers rangs, ce qui reflète une capacité plus efficace à identifier correctement les individus dès les premières correspondances.

En outre, les courbes CMC indiquent que les deux méthodes convergent progressivement vers des taux de reconnaissance proches de 100 % lorsque le rang augmente. Toutefois, l'approche PDV-PCA conserve un avantage global en maintenant des performances plus élevées sur l'ensemble des rangs évalués.

Ainsi, ces résultats expérimentaux confirment que l'approche PDV-PCA est plus performante et plus robuste que PDV-SC, aussi bien en termes de précision de reconnaissance que de fiabilité globale du système biométrique.

III.3.3 Système sécurisé :

Le système proposé repose sur l'utilisation d'un chiffrement basé sur un système chaotique, caractérisé par une forte sensibilité aux conditions initiales et un comportement pseudo-aléatoire. Dans cette étude, les paramètres chaotiques ont été volontairement modifiés, ce qui influence directement la transformation des données biométriques et peut altérer les caractéristiques discriminantes extraites. Cette variation des paramètres explique en grande partie les fluctuations des performances observées après sécurisation. En effet, la comparaison entre les systèmes sécurisés et non sécurisés montre une augmentation du taux d'erreur (EER) dans les deux cas, passant de 0.1250 à 0.1640 pour l'approche PDV-PCA et de 0.1706 à 0.2224 pour PDV-SC. Toutefois, cette dégradation reste plus modérée pour PDV-PCA, ce qui indique une meilleure robustesse face aux perturbations introduites par le chiffrement chaotique, contrairement à PDV-SC qui apparaît plus sensible aux variations des paramètres.



(a) (b)

Figure III.5: Comparaison des systèmes sécurisés et non sécurisés les plus performants : analyse de la courbe DET : (a) systèmes à filtre PDV-PCA et (b) systèmes à filtre PDV-SC

III.3.4 Système Optimisé :

La courbe de convergence met en évidence l'efficacité de l'algorithme d'optimisation par essaim de particules (PSO) dans l'amélioration des performances du système à travers la minimisation itérative du taux de faux rejets (FRR). Dans cette étude, le PSO est paramétré avec 15 itérations et un essaim composé de 2 particules, ce qui permet d'assurer un compromis entre efficacité d'optimisation et coût computationnel. Comme illustré par la figure, le FRR diminue rapidement au cours des premières itérations, traduisant une exploration et une exploitation efficaces de l'espace de recherche.

Cette amélioration devient ensuite progressive, jusqu'à atteindre une phase de stabilisation vers les dernières itérations, ce qui confirme la convergence de l'algorithme. Par ailleurs, le

système basé sur PDV-PCA présente une convergence plus rapide et atteint des valeurs de FRR plus faibles que le système PDV-SC, qui nécessite un nombre d'itérations plus élevé pour se stabiliser et affiche des performances relativement inférieures. Ces résultats démontrent la capacité du PSO à optimiser efficacement les paramètres du système, tout en validant la pertinence du paramétrage adopté.

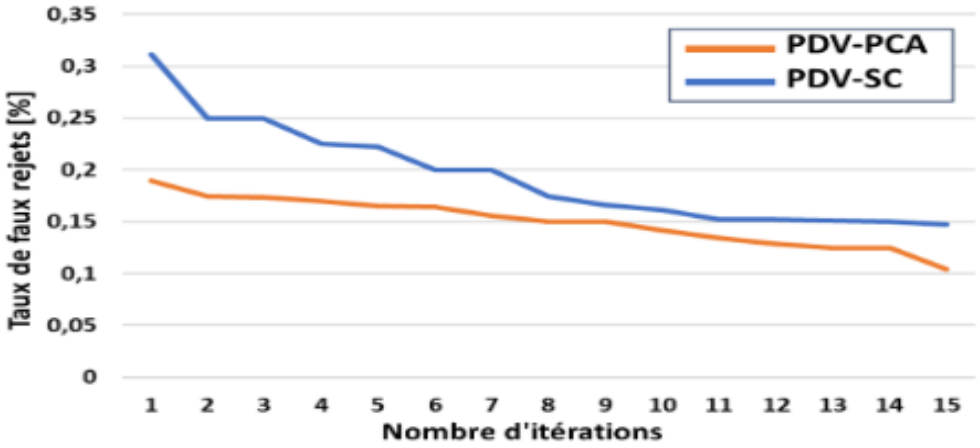
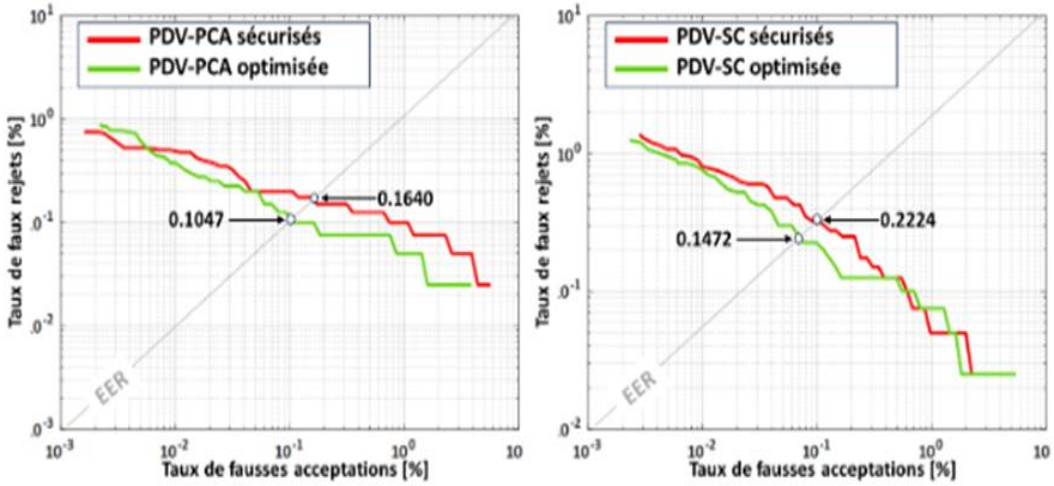


Figure III.6: Courbe de convergence de l'optimisation des paramètres des filtres PDV-PCA et PDV-SC

La figure illustre une comparaison des performances des systèmes biométriques fondés sur les approches PDV-PCA et PDV-SC, en distinguant les versions sécurisées et optimisées à travers les courbes DET, qui expriment le compromis entre le taux de fausses acceptations (FAR) et le taux de faux rejets (FRR). Globalement, on constate que les systèmes optimisés présentent des courbes plus proches de l'origine, traduisant une réduction simultanée des erreurs et donc une amélioration notable des performances.

Plus précisément, dans le cas de PDV-PCA, le taux d'erreur égal (EER) passe de 0,1640 % pour $T_0 = 0.7071$ à 0,1047 % pour $T_0 = 0.7397$ après optimisation, tandis que pour PDV-SC, il diminue 0,2224% pour $T_0 = 0.7077$ à 0,1472% pour $T_0 = 0.737$, ce qui confirme l'efficacité du processus d'optimisation dans les deux approches. Toutefois, la comparaison met en évidence que PDV-PCA optimisée offre les meilleures performances globales, avec le plus faible EER, contrairement à PDV-SC qui reste légèrement moins performante.



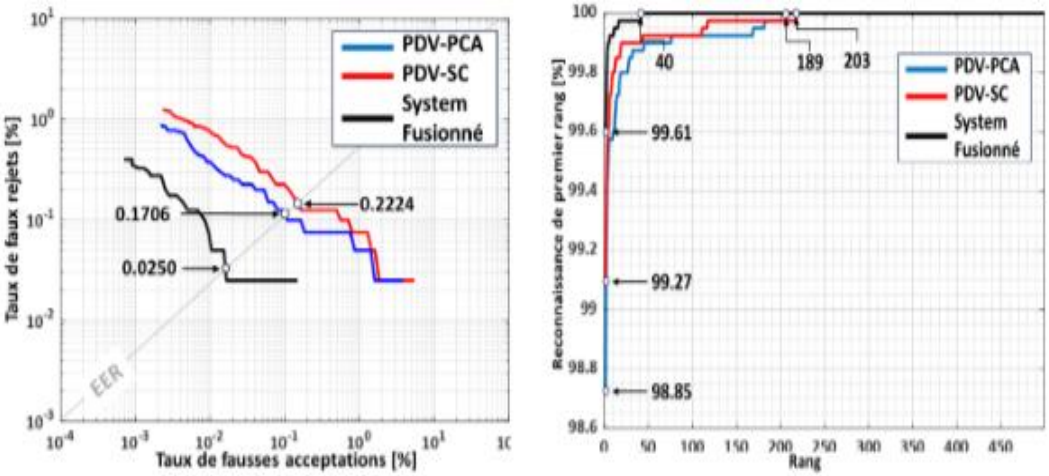
(a) (b)

Figure III.7 : Comparaison des systèmes sécurisés et optimisés les plus performants : analyse de la courbe DET : (a) systèmes à base de filtres PDV-PCA et (b) systèmes à base de filtres PDV-SC

Cette différence s'explique par le fait que les systèmes sécurisés privilégient principalement la protection des données et la robustesse, ce qui peut impacter les performances, alors que les systèmes optimisés reposent sur des techniques d'ajustement des paramètres visant à minimiser les erreurs et à améliorer le compromis entre précision et fiabilité.

III.3.5 Système fusionné :

Dans ce travail, un système biométrique basé sur la fusion des approches PDV-PCA et PDV-SC a été proposé afin d'améliorer la robustesse et la précision de la reconnaissance. La fusion est réalisée au niveau des scores, permettant de combiner les décisions issues de chaque méthode après normalisation et d'exploiter leur complémentarité.



(a) (b)

Figure III.8 : Évaluation des system : analyse des courbes DET et CMC : (a) courbes DET et (b) courbes CMC

Les résultats expérimentaux montrent une amélioration significative des performances. Le système fusionné atteint un taux d'erreur égal (EER) de 0.0250%, nettement inférieur à ceux obtenus par PDV-SC (0.1706%) et PDV-PCA (0.2224%), ce qui traduit une réduction importante des erreurs de classification. Par ailleurs, le taux de reconnaissance au premier rang atteint 99.61% , confirmant une meilleure capacité d'identification.

Cette amélioration s'explique par le fait que la fusion permet de compenser les limites de chaque méthode individuelle, en renforçant la séparation entre les classes authentiques et imposteurs. Ainsi, le système proposé offre un compromis optimal entre précision et robustesse, le rendant plus performant et mieux adapté aux applications biométriques réelles.

III.4 Evaluation du système proposé :

Cette section vise à évaluer la robustesse du système proposé du point de vue sécuritaire. L'analyse porte principalement sur l'espace des clés, la sensibilité aux clés ainsi que le caractère aléatoire des données générées.

III.4.1 Analyse statistique par histogramme

L'analyse par histogramme est une technique qui permet de représenter et d'analyser la distribution statistique des niveaux d'intensité des pixels dans une image [60].

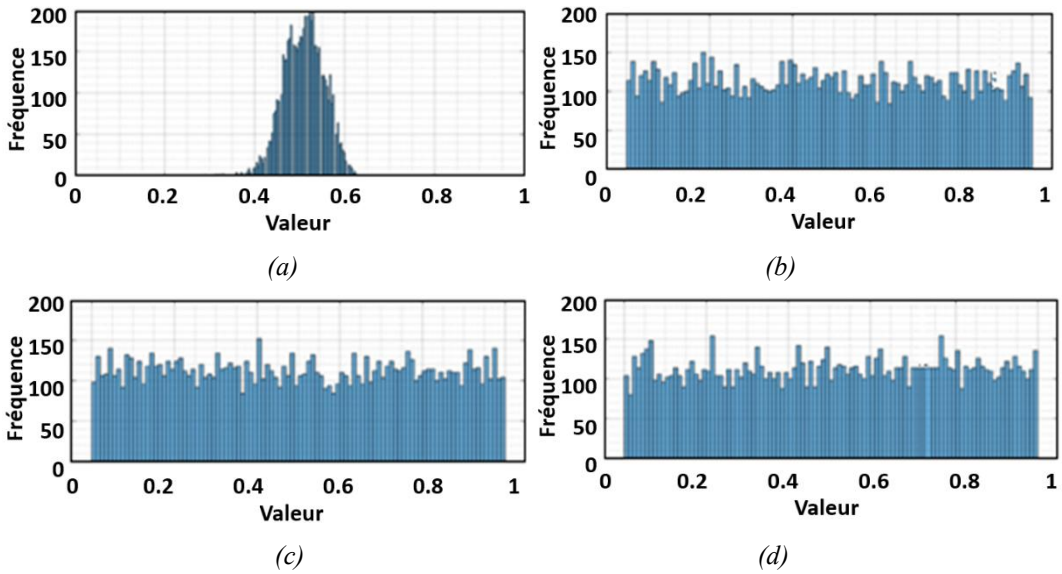


Figure III.9 : Histogramme des modèles biométriques, (a) Original, (b) Modèle biométrique crypté à l'aide de $\mathcal{K}_{\mathcal{E}}^{1}$, (c) Modèle biométrique crypté à l'aide de $\mathcal{K}_{\mathcal{E}}^{2}$, (d) Modèle biométrique crypté à l'aide de $\mathcal{K}_{\mathcal{E}}^{3}$.

La figure III.9 montre que l'histogramme du modèle biométrique original possède une structure organisée reflétant les caractéristiques intrinsèques des données biométriques. Après chiffrement, les histogrammes obtenus avec les clés $\mathcal{K}_{\mathcal{E}}^{1}$, $\mathcal{K}_{\mathcal{E}}^{2}$ et $\mathcal{K}_{\mathcal{E}}^{3}$ deviennent quasi uniformes et

aléatoires. Malgré de très faibles variations entre les clés, les modèles biométriques chiffrés présentent des distributions totalement différentes de celle du modèle original. Ces résultats démontrent la forte sensibilité du système aux variations de clé et confirment la robustesse du schéma de chiffrement face aux attaques par approximation de clé, puisque des clés similaires ne produisent pas des modèles biométriques similaires.

III.4.2 Analyse de l'espace des clés

La sécurité du système biométrique proposé est évaluée à travers l'analyse de l'espace des clés et la sensibilité aux clés. Le système repose sur des cartes logistiques chaotiques, où la clé secrète est constituée de la condition initiale μ et du paramètre de contrôle x_0.

La sensibilité aux clés est mesurée à l'aide de l'erreur absolue moyenne (MAE) entre deux séquences générées à partir de clés légèrement différentes :

$$\varepsilon(s_1, s_2) = \frac{1}{m}\sum_{i=1}^{m} \mid s_1(i) - s_2(i) \mid \quad (3.1)$$

Cela garantit que même une variation minimale de la clé produit des sorties significativement différentes, reflétant une forte imprévisibilité.

L'espace total des clés de la deuxième configuration dépend du fait que les paramètres de contrôle soient aléatoires ou optimisés, et s'exprime comme suit :

$$E_T^{1R} \cong 1.027.(1.112)^{2^{\eta}}.10^{32(\eta+1)}, E_T^{2R} \cong 1.027.(1.112)^{\eta}.10^{16(\eta+2)} \quad (3.2)$$

Avec le système mis à jour utilisant 5 filtres ($\eta = 5$), les espaces de clés deviennent approximativement 2^{447} (cas aléatoire) et 2^{259} (cas optimisé), tous deux suffisamment grands pour résister aux attaques par force brute.

Dans la troisième configuration, l'espace des clés est encore étendu en intégrant un chiffrement basé sur des cartes logistiques supplémentaires :

$$E_T^E \cong 2^{107} \ , \quad E_T \cong E_T^{2R}.E_T^E \approx 2^{366} \quad (3.3)$$

Cela améliore considérablement la sécurité globale du système.

III.4.3 Analyse de la sensibilité des clés

La sensibilité à la clé est une propriété fondamentale des systèmes biométriques basés sur le chaos, garantissant qu'une variation minimale de la clé secrète entraîne des sorties significativement différentes. Cette propriété renforce à la fois la sécurité et la révocabilité, car les gabarits compromis ne peuvent pas être reproduits lorsque la clé est légèrement modifiée.

Pour quantifier ce comportement, l'erreur absolue moyenne (MAE) entre deux séquences générées à partir de clés légèrement différentes est définie comme suit :

$$\varepsilon(s_1, s_2) = \frac{1}{m}\sum_{i=1}^{m} \mid s_1(i) - s_2(i) \mid \quad (3.4)$$

Où : m est la longueur de la séquence, et s_1 et s_2 sont générées à partir de clés voisines.

De plus, la similarité entre les gabarits biométriques est évaluée à l'aide du coefficient de corrélation :

$$\rho_{ij} = 100.\frac{c_{ij}}{\sigma_i \sigma_j} \tag{3.5}$$

Pour démontrer la sensibilité à la clé, trois clés sont considérées : la clé originale et deux versions légèrement perturbées avec des variations de l'ordre de 10^{-16} soit dans x_0, soit dans μ. Les coefficients de corrélation obtenus entre les gabarits biométriques sont présentés dans le tableau.

Tableau III.1: analyse de la sensibilité à la clé à l'aide du coefficient de corrélation (%)

	$H_i(K_R^1)$	$H_i(K_R^2)$	$H_i(K_R^3)$
$H_i(K_R^1)$	100.00	6.46	6.19

Les résultats montrent que l'utilisation de la même clé produit une corrélation parfaite (100 %), confirmant la stabilité du système. En revanche, l'introduction d'une légère variation de la clé réduit drastiquement la corrélation à des valeurs d'environ 6 %, ce qui démontre une forte sensibilité à la clé. Cela confirme que même des modifications négligeables de la clé génèrent des gabarits biométriques complètement différents et non corrélés, renforçant ainsi la résistance du système aux attaques et assurant une révocabilité efficace des gabarits.

III.4.4 Suite de tests d'aléatoire NIST

Analyse statistique : Afin d'évaluer davantage la robustesse du mécanisme de sécurité proposé, nous avons appliqué la suite de tests statistiques du NIST à deux configurations de notre système biométrique : le système sécurisé et le système optimisé. Cette suite permet de vérifier si une séquence donnée présente les caractéristiques statistiques d'un véritable hasard. Un test est considéré comme réussi si la valeur de p obtenue dépasse le seuil de 0,01. Comme indiqué dans le Tableau, les deux vecteurs chiffrés ont réussi la majorité des tests, ce qui indique que chaque couche de chiffrement améliore significativement le caractère aléatoire statistique et, par conséquent, renforce la sécurité globale du système. [61]

Tableau III.2 : Résultats de la suite de tests de hasard du NIST

	Test de fréquence	**Test de fréquence par blocs**	**Test de séquences**	**Test de la plus longue séquence de 1**	**Test de rang**
Système sécurisé	0.3489	0.2456	0.1394	0.3416	0.1230
Système optimisé	0.5533	0.1364	0.5564	0.1798	0.3970
	Test de fourrier	**Test de gabarits chevauchants**	**Test d'entropie approximative**	**Test sériel**	**Test des sommes cumulées**
système sécurisé	0.2013	0.3830	0.1924	0.3489	0.1364
Système optimisé	0.2131	0.6914	0.1767	0.2456	0.1394

Les résultats présentés dans le Tableau indiquent que les deux configurations, à savoir le système sécurisé et le système optimisé, ont réussi les tests de la suite statistique du NIST. Globalement, le gabarit biométrique généré par le système biométrique présente un niveau de hasard légèrement supérieur dans la majorité des tests, suggérant une distribution plus uniforme des caractéristiques aléatoires. Néanmoins, le gabarit produit par le système optimisé démontre également des niveaux satisfaisants d'aléa, indiquant une robustesse face aux attaques statistiques. Ces résultats valident la fiabilité et la sécurité des deux mécanismes de chiffrement et confirment leur efficacité à générer des vecteurs de caractéristiques avec un haut degré d'aléa et une forte résistance aux attaques par inférence et par prédiction.

Conclusion

Ce chapitre a permis d'évaluer les performances ainsi que la sécurité du système biométrique proposé. Les résultats expérimentaux montrent que l'intégration des méthodes de représentation et du mécanisme de chiffrement améliore l'efficacité globale du système sans compromettre ses performances. De plus, l'analyse de sécurité, notamment à travers les tests du NIST, confirme la robustesse et la fiabilité de la solution développée. Ainsi, le système proposé assure un bon compromis entre performance et sécurité.

Conclusion Générale

Conclusion

L'évolution rapide des technologies numériques, de l'intelligence artificielle et des systèmes connectés a profondément transformé les méthodes d'authentification et de gestion des identités. Dans ce contexte, les systèmes biométriques occupent aujourd'hui une place essentielle grâce à leur capacité à identifier ou authentifier un individu à partir de caractéristiques physiques ou comportementales uniques. Cependant, malgré leurs nombreux avantages, ces systèmes soulèvent des problématiques importantes liées à la sécurité, à la confidentialité, à la protection des données personnelles et à la fiabilité des mécanismes de reconnaissance. En effet, les templates biométriques constituent des données sensibles qui, une fois compromises, ne peuvent pas être remplacées comme un mot de passe classique. Cette réalité rend indispensable le développement de solutions biométriques capables de garantir à la fois des performances de reconnaissance élevées et un niveau de sécurité renforcé contre les différentes attaques possibles.

Dans ce mémoire, nous avons étudié les fondements de la sécurité de l'information ainsi que les principes de fonctionnement des systèmes biométriques modernes. Une analyse détaillée des principales vulnérabilités a été réalisée, notamment celles liées au vol des templates biométriques, aux attaques de rejeu, aux interceptions des canaux de transmission et aux tentatives d'usurpation d'identité. Cette étude a permis de mettre en évidence la nécessité d'intégrer des mécanismes de protection avancés afin de préserver la confidentialité et l'intégrité des données biométriques tout au long du processus d'authentification.

Afin de répondre à ces problématiques, nous avons proposé un système biométrique sécu-

risé basé sur une architecture multi-niveaux intégrant plusieurs étapes complémentaires : l'extraction des caractéristiques, leur transformation sécurisée et leur chiffrement. L'approche proposée exploite des représentations fondées sur des filtres PCA et des projections spatiales guidées par le chaos afin de générer des vecteurs de caractéristiques robustes, discriminants et difficiles à reproduire. L'utilisation de l'algorithme d'optimisation par essaim de particules (PSO) a également permis d'améliorer la sélection des paramètres optimaux du système, contribuant ainsi à une meilleure qualité des caractéristiques extraites et à une amélioration globale des performances de reconnaissance.

Par ailleurs, l'intégration du concept de biométrie révocable représente un élément central de cette contribution. Contrairement aux approches biométriques classiques, cette technique permet de transformer les données biométriques originales en versions protégées et renouvelables. Ainsi, en cas de compromission ou de fuite d'informations, il devient possible de générer un nouveau template biométrique sans avoir à modifier la caractéristique biométrique réelle de l'utilisateur. Cette propriété améliore considérablement la sécurité et la protection de la vie privée, tout en renforçant la confiance dans l'utilisation des systèmes biométriques dans des applications sensibles telles que les services bancaires, les systèmes gouvernementaux ou les infrastructures critiques.

Sur le plan expérimental, l'évaluation du système proposé a démontré son efficacité aussi bien en termes de performance qu'en matière de sécurité. Les résultats obtenus montrent que le système sécurisé conserve une précision de reconnaissance satisfaisante malgré l'ajout des mécanismes de protection et de chiffrement. La comparaison entre le système biométrique non sécurisé et le système sécurisé a mis en évidence une amélioration significative de la robustesse globale face aux attaques potentielles, tout en maintenant de bonnes performances d'authentification. Les indicateurs classiques tels que le FAR (False Acceptance Rate), le FRR (False Rejection Rate) et l'EER (Equal Error Rate) ont confirmé la fiabilité du système proposé et sa capacité à réduire les erreurs de reconnaissance.

En complément des performances biométriques, une analyse approfondie de la sécurité a également été réalisée. Celle-ci comprend l'étude de l'espace des clés, l'analyse de la sensibilité aux variations des clés, ainsi que des tests statistiques de hasard basés sur la suite NIST. Les résultats obtenus montrent que le schéma de chiffrement proposé possède une forte sensibilité aux clés et génère des distributions proches du comportement aléatoire idéal, ce qui confirme sa robustesse face aux attaques cryptographiques et aux tentatives d'approximation des clés. De plus, les histogrammes des données chiffrées et les différentes analyses statistiques démontrent

que le système réduit considérablement les corrélations présentes dans les données biométriques originales, rendant ainsi toute tentative de reconstruction extrêmement difficile.

Enfin, l'intégration de concepts modernes tels que le stockage décentralisé, les architectures distribuées et la technologie blockchain ouvre des perspectives particulièrement prometteuses pour la gestion sécurisée et transparente des identités numériques. Ces technologies permettent non seulement d'améliorer la traçabilité et la protection des données biométriques, mais également de réduire les risques liés aux points uniques de défaillance dans les systèmes centralisés traditionnels.

Malgré les résultats encourageants obtenus dans ce travail, certaines limites subsistent, notamment en ce qui concerne la complexité computationnelle, le temps de traitement et la scalabilité du système lorsqu'il est appliqué à de très grandes bases de données biométriques ou à des environnements temps réel. Des perspectives futures pourraient donc porter sur l'optimisation des performances, la réduction des coûts de calcul, ainsi que l'intégration de techniques d'intelligence artificielle et d'apprentissage profond afin d'améliorer davantage l'efficacité, l'adaptabilité et la robustesse du système proposé.

Ainsi, ce travail constitue une contribution pertinente au développement de systèmes biométriques sécurisés, fiables et adaptés aux applications réelles. Il met en évidence l'importance d'associer des mécanismes avancés de protection des données, des techniques d'optimisation intelligentes et des approches cryptographiques modernes afin de construire des solutions biométriques capables de répondre aux exigences croissantes de sécurité et de confidentialité dans les environnements numériques actuels et futurs.

Bibliographies

[1] Collard, G., Ducroquet, S., Disson, E., & Talens, G. (2017, May). A Definition Of Infor-Mation Security Classification In Cybersecurity Context. In 2017 11th International Confer-Ence On Research Challenges In Information Science (Rcis) (Pp. 77-82). Ieee. Doi: 10.1109/Rcis.2017.7956520

[2] Aguilar Quintero, N. A., Velásquez Pérez, T., & Castro Silva, H. F. (2019). Information Se-Curity Model. Case Study Higher Education Institution. Journal Of Physics: Conference Series, 1257(1), 012014. Https://Doi.Org/10.1088/1742-6596/1257/1/012014

[3] Surwade, Y., & Patil, H. J. (2024). Web Technologies From Web 2.0 To Web 4.0. Ssrn Elec-Tronic Journal. Https://Doi.Org/10.2139/Ssrn.488008

[4] Osazuwa, C. M. (2024). Confidentiality, Integrity, And Availability In Network Systems: A Review Of Related Literature. International Journal Of Innovative Science And Research Tech-Nology. Doi:10.5281/Zenodo.10464076

[5] International Organization For Standardization. (2018). Iso/Iec 27005:2018 — Information Technology — Security Techniques — Information Security Risk Management.

[6] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehen-Sive Review Of Cyber Security Vulnerabilities, Threats, Attacks, And Solutions. Electronics, 12(6), 1333. Https://Doi.Org/10.3390/Electronics12061333

[7] Pham, D. P. (2022). Leveraging Side-Channel Signals For Iot Malware Classification And Rootkit Detection (Doctoral Dissertation, Université Rennes 1).

[8] Zayyad, M. A. (2023). Systematic Study Of Computer Virus Using Virus Definition And Scan-Ning Techniques. Asian Journal Of Research In Computer Science, 16(4), 230-238.

[9] Cohen, S., Bitton, R., & Nassi, B. (2024). Here Comes The Ai Worm: Unleashing Zero-Click Worms That Target Genai-Powered Applications. Arxiv Preprint Arxiv:2403.02817.

[10] Wang, R., Xue, Y., & Xue, K. (2023). Dynamic Analysis And Optimal Control Of Worm Propa-Gation Model With Saturated Incidence Rate. Frontiers In Physics, 10, 1098040.

[11] Admoni, A. (2025). " A Horse With No Name"*: The Role Of Trojan Horse In Cyber Warfare During Its' First Decade (1972-1983). Historical: Journal Of History And Social Scienc-Es, 4(3), 293-306.

[12] Iannone, E., Guadagni, R., Ferrucci, F., De Lucia, A., & Palomba, F. (2022). The Secret Life Of Software Vulnerabilities: A Large-Scale Empirical Study. Ieee Transactions On Software Engineering, 49(1), 44-63

[13] Fine, Z., & Hirschprung, R. S. (2026). Mapping Privacy Vulnerabilities In Local Area Network (Lan) Environments. Sensors, 26(3), 763. Https://Doi.Org/10.3390/S26030763

[14] Prinetto, P., & Roascio, G. (2020, August). Hardware Security, Vulnerabilities, And Attacks: A Comprehensive Taxonomy. In Itasec (Pp. 177-189).

[15] Verma, R., & Dhiman, J. (2022). Implementation Of Improved Cryptography Algorithm. International Journal Of Information Technology And Computer Science, 14(2), 45-53. Doi: 10.5815/Ijitcs.2022.02.04

[16] Pawar, M. V., & Anuradha, J. (2015). Network Security And Types Of Attacks In Network. Pro-Cedia Computer Science, 48, 503-506 , Https://Doi.Org/10.1016/J.Procs.20-15.04.126

[17] Baudrin, J. (2024). Algebraic Properties Of Symmetric Ciphers And Of Their Non-Linear Com-Ponents (Doctoral Dissertation, Sorbonne Université)

[18] Zellagui, A., Hadj-Said, N., & Ali Pacha, A. (2021). Sécurité Des Fonctions De Hachage Cryp-Tographique. Communication Science Et Technologie, 19(1), 13-21

[19] Bas, P., Doerr, G., Furon, T., & Puech, W. (2023, August). Histoire Récente De La Sécurité Des Contenus Multimédia Un Focus Sur La Dissimulation D'information. In Gretsi 2023-29e Colloque Francophone De Traitement Du Signal Et Des Images (Pp. 1-4)

[20] Dargan, S., & Kumar, M. (2020). A Comprehensive Survey On The Biometric Recognition Sys-Tems Based On Physiological And Behavioral Modalities. Expert Systems With Applications, 143, 113114

[21] Fernandez, P., Sablayrolles, A., Furon, T., Jégou, H., & Douze, M. (2022, September). Ta-Touage Numérique D'images Dans L'espace Latent De Réseaux Auto-Supervisés. In Gretsi 2022-Colloque Francophone De Traitement Du Signal Et Des Images (Pp. 1-4)

[22] Orrù, G., Rattani, A., Rida, I., & Marcel, S. (2024). Recent Advances In Behavioral And Hid-Den Biometrics For Personal Identification. Pattern Recognition Letters, 185, 108-109

[23] Toufik, H. (2016). Reconnaissance Biométrique Multimodale Basée Sur La Fusion En Score De Deux Modalités Biométriques: L'empreinte Digitale Et La Signature Manuscrite Cursive En Ligne. Université Badji Mokhtar–Annaba.

[24] Szymoniak, S., & Kubanek, M. (2025). Biometry-Based Verification System With Symmetric Key Generation Method For Internet Of Things Environments. Scientific Reports, 15(1), 5464

[25] Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A., & Lan, G. L. (2022). Mobile Behavioral Biometrics For Passive Authentication. Pattern Recognition Let-Ters, 157, 35–41. Https://Doi.Org/10.1016/J.Patrec.2022.03.014

[26] Melouah Messaouda , Driche Imane, "Tatouage Numérique Des Données Biomédicales Dans Le Domaine Des Transformée" , 2022/2023.

[27] Lucia, C., Zhiwei, G., & Michele, N. (2023). Biometrics For Industry 4.0: A Survey Of Recent Applications. Journal Of Ambient Intelligence And Humanized Computing, 14(8), 11239-11261

[28] Salturk, T., & Kahraman, N. (2025). The Role Of Multiple Data Characteristics In Eeg-Based Biometric Recognition: The Impact Of States, Channels, And Frequencies. Ieee Access. [29] Huang, J., Xue, Y., & Liu, L. (2023). Dynamic Signature Verification Technique For The Online And Offline Representation Of Electronic Signatures In Biometric Systems. Processes, 11(1), 190.

[29] C. Medjahed, A. Rahmoun, C. Charrier, And F. Mezzoudj, "A Deep Learning-Based Multimodal Biometric System Using Score Fusion," Iaes Int. J. Artif. Intell, Vol. 11,No. 1, P. 65, 2022

[30] Khider, A. (2023, March 2). Un Système Biométrique Multimodal Basé Sur La Fusion Visage-Iris. Https://Dspace.Univ-Guelma.Dz/Xmlui/Handle/123456789/14246

[31] Oloyede, M. O., & Hancke, G. P. (2016). Unimodal And Multimodal Biometric Sensing Sys-Tems: A Review. Ieee Access, 4, 7532-7555. Doi: 10.1109/Access.2016.2614720

[32] Shen, C., Yu, S., Wang, J., Huang, G. Q., & Wang, L. (2024). A Comprehensive Survey On Deep Gait Recognition: Algorithms, Datasets, And Challenges. Ieee Transactions On Biomet-Rics, Behavior, And Identity Science, 7(2), 270-292

[33] Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics Recognition Using Deep Learning: A Survey. Artificial Intelligence Review, 56(8), 8647-8695

[34] Hezil, N. (2017). Intitulée: Méthode Hybride En Biométrie: Application A La Paume De La Main &Amp; L'oreille Présentée Par: Nabil Hezil Option: Images Et Signaux Biométriques Thèse Dirigée (Doctoral Dissertation, Guelma)

[35] Li, L., Correia, P. L., & Hadid, A. (2018). Face Recognition Under Spoofing Attacks: Counter-Measures And Research Directions. Iet Biometrics, 7(1), 3-14

[36] Rathgeb, C., & Uhl, A. (2022). Cancelable Biometrics And Template Protection Techniques: A Review. Information Fusion, 78, 39–61

[37] Dahea, W., & Fadewar, H. S. (2018). Multimodal Biometric System: A Review. International Journal Of Research In Advanced Engineering And Technology, 4(1), 25-31…37

[38] Alghamdi, S. M., Jarraya, S. K., & Kateb, F. (2024). Enhancing Security In Multimodal Bio-Metric Fusion: Analyzing Adversarial Attacks. Ieee Access. Doi: 10.1109/Access.2024.3435527

[39] Rotella, Y. (2025). Eléments De Cryptanalyse (Doctoral Dissertation, Université Paris-Saclay)

[40] Elazab, H. (2023). Analyse Des Technologies Authentifications Biométriques Pour Renforcer La Sécurité Des Systèmes Informatiques. Travail De Bachelor Réalisé En Vue De L'obtention Du Bachelor Hes

[41] Habibu, T., Luhanga, E. T., & Sam, A. E. (2022). The Usage Of Biometric Technology Applications. Recent Advances In Biometrics, 45

[42] Alrawili, R., Alqahtani, A. A. S., & Khan, M. K. (2024). Comprehensive Survey: Biometric User Authentication Application, Evaluation, And Discussion. Computers And Electrical Engineering, 119, 109485

[43] Hezil, N., & Boukrouche, A. (2017). Multimodal biometric recognition using human ear and palmprint. *IET Biometrics*, *6*(5), 351-359

[44] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE Access*, *12*, 64300-64334.

[45] Sharma, S., & Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. *IET blockchain*, *4*(2), 124-151.

[46] Goh, Z. H., Wang, Y., Leng, L., Liang, S. N., Jin, Z., Lai, Y. L., & Wang, X. (2022). A Framework For Multimodal Biometric Authentication Systems With Template Protection. Ieee Access, 10, 96388-96402.

[47] Hahn, V. K., & Marcel, S. (2022). Biometric Template Protection For Neural-Network-Based Face Recognition Systems: A Survey Of Methods And Evaluation Techniques. Ieee Transactions On Information Forensics And Security, 18, 639-666.

[48] Zhong, L., Li, Y., & Zhou, F. (2026, January). A Revocable Fingerprint Template Protection Method Based On Deep Features And Improved Bloom Filter. In Proceedings Of The 2026 5th International Conference On Big Data, Information And Computer Network (Pp. 828-833).

[49] Sardar, A., Umer, S., Rout, R. K., & Pero, C. (2023). Face Recognition System With Hybrid Template Protection Scheme For Cyber–Physical-Social Services. Pattern Recognition Letters, 174, 17-24.

[50] Salihu, Y. A., Yakubu, Y., & Muhammad, S. (2026). Multi-Level Intrution Detection Using Deep Learning For Face Recognition Sytem. International Journal Of African Innovation And Multidisciplinary Research.

[51] Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric Template Attacks And Recent Protection Mechanisms: A Survey. Information Fusion, 103, 102144.

[52] Park, S. H., Lee, S. H., Lim, M. Y., Hong, P. M., & Lee, Y. K. (2024). A Comprehensive Risk Analysis Method For Adversarial Attacks On Biometric Authentication Systems. Ieee Access, 12, 116693-116710.

[53] Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: a systematic review. IEEe Access, 9, 34541-34557.

[54] Malik, G. (2024). Biometric Authentication-Risks And Advancements In Biometric Security Systems. Journal Of Computer Science And Technology Studies, 6(3), 159-180.

[55] Arman, S., Yang, T., Shahed, S., Mazroa, A., Attiah, A., & Mohaisen, L. (2024). A Comprehensive Survey For Privacy-Preserving Biometrics: Recent Approaches, Challenges, And Future Directions. Computers, Materials, & Continua, 78(2), 2087.

[56] Elrefaei, L. A., & Al-Mohammadi, A. M. (2022). Machine Vision Gait-Based Biometric Cryptosystem Using A Fuzzy Commitment Scheme. Journal Of King Saud University-Computer And Information Sciences, 34(2), 204-217.

[57] Muzammil, M. B., Bilal, M., Ajmal, S., Shongwe, S. C., & Ghadi, Y. Y. (2024). Unveiling Vulnerabilities Of Web Attacks Considering Man In The Middle Attack And Session Hijacking. Ieee Access, 12, 6365-6375.

[58] Mehmood, M., Amin, R., Muslam, M. M. A., Xie, J., & Aldabbas, H. (2023). Privilege Escalation Attack Detection And Mitigation In Cloud Using Machine Learning. Ieee Access, 11, 46561-46576

[59] Kumar, A. (2025). Biometrics Research and Innovation Centre. Biometrics Research and Innovation Centre. https://web.comp.polyu.edu.hk/biometrics/

[60] Alexan, W., Shabasy, N. H. E., Ehab, N., & Maher, E. A. (2025). A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. Scientific Reports, 15(1), 31246.

[61] Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically Secured Pseudo-Random Number Generators: Analysis and Evaluation Using the NIST Statistical Test Suite. Mathematics, 11(23), 4812.