



République Algérienne Démocratique et Populaire -
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique
École Nationale Supérieure des Technologies Avancées



Mémoire de fin d'études
En vue de l'obtention du diplôme d'
INGÉNIEUR D'ÉTAT
Spécialité : **Systèmes de Télécommunications et Réseaux**

Thème
Développement d'une Solution IA pour la
Vérification Biométrique Sécurisée

Réalisé par :
YAKOUBI Kahina et LABIOD Wissam
Soutenu le : 23 / 06 / 2025

Membres du jury :

Nom et Prénom	Établissement	Qualité	Grade
Mme. BOUTARFA Souhila	ENSTA	Présidente	Maître de Conférences B
Mme. CHOUAF Seloua	ENSTA	Encadrante	Maître Assistant A
M. BOUZEGZEG Amine	3SPAY	Co-encadrant	Ingénieur
Mme. BOUTOUTA Dalila	ENSTA	Examineur	Maître Assistant A
M. CHERABIT Noureddine	ENSTA	Examineur	Maître Assistant A

Année universitaire : 2024/2025

Dédicace

Nous dédions ce travail à nos parents, pour leur amour inconditionnel, leur soutien moral et leurs encouragements constants tout au long de notre parcours.

À nos enseignants, pour leur patience, leur savoir et leur précieuse contribution à notre formation.

À nos camarades et amis, pour les moments partagés, l'entraide et les sourires échangés.

Ce travail est le fruit d'un effort collectif, nourri par la bienveillance et le soutien de tous ceux qui nous entourent.

Merci à tous.

Remerciements

Ce mémoire est bien plus qu'un simple travail académique. Il reflète un parcours riche en apprentissages, en rencontres et en émotions.

Nous remercions sincèrement les membres du jury pour le temps qu'ils ont accordé à l'évaluation de notre travail ainsi que pour leurs remarques constructives.

Nous tenons à remercier Madame CHOUAF Seloua, notre encadrante académique, pour sa bienveillance et ses conseils précieux.

Nous remercions Monsieur BOUZEGZEG Amine ainsi que toute l'équipe de 3S PAY pour le bon accueil, leur précieuse contribution et pour nous avoir permis de participer à une expérience professionnelle enrichissante.

Nous remercions également tous les enseignants du département Génie Électrique et Informatique Industrielle (GEII) pour la qualité de leur enseignement.

Enfin, nous remercions chaleureusement nos familles et nos amis pour leur soutien constant, leurs encouragements et leur patience. Leur présence nous a donné la force de mener ce travail jusqu'au bout.

ملخص

تتناول هذه الأطروحة مجال القياسات الحيوية، مع التركيز على جانبين أساسيين متكاملين: التعرف على الوجه وكشف حيوية الوجه. في وقت يُمثل فيه الأمن الرقمي تحديًا استراتيجيًا كبيرًا، تُختبر موثوقية أنظمة المصادقة الحيوية بشدة من خلال تقنيات احتيال متطورة بشكل متزايد، مثل الهجمات المباشرة.

يهدف هذا العمل بشكل رئيسي إلى تصميم نهج مبتكر يجمع بين معالجة الصور والذكاء الاصطناعي، قادر على المصادقة الحيوية بفعالية مع ضمان صحة مصدر الإدخال وفعاليتها. ولتحقيق هذه الغاية، درسنا المبادئ النظرية للتعرف على الوجه وكشف حيوية الوجه، بالإضافة إلى أنواع الهجمات المختلفة التي قد تواجهها هذه الأنظمة.

ثم نقدم الحل المقترح، والمتمثل في نماذج التعلم العميق، مع وصف بنيته، وخطوات تنفيذه، والنتائج التجريبية المفصلة عليها.

وأخيرًا، يُمهد التحليل النقدي لأداء النظام وقيوده آفاقًا للتحسين في الأبحاث المستقبلية أو التطبيقات الصناعية.

الكلمات المفتاحية:

القياسات الحيوية، التعرف على الوجه، كشف حيوية الوجه، معالجة الصور، الذكاء الاصطناعي.

Résumé

Ce mémoire porte sur la biométrie, en particulier la reconnaissance faciale et la détection de vivacité, deux axes clés pour renforcer la sécurité des systèmes d'authentification face aux attaques par présentation. Il propose une solution fondée sur le traitement d'images et l'intelligence artificielle, combinant plusieurs modèles d'apprentissage profond pour authentifier une identité vivante de manière fiable. Après avoir abordé les bases théoriques et les menaces existantes, le travail présente l'architecture du système, son implémentation, les résultats expérimentaux obtenus, ainsi qu'une analyse critique ouvrant sur des pistes d'amélioration futures.

Mots-clés : biométrie, reconnaissance faciale, détection de vivacité, traitement d'images, intelligence artificielle.

Abstract

This thesis addresses biometrics, focusing on facial recognition and liveness detection, two complementary pillars for secure authentication. In response to increasingly sophisticated threats such as face presentation attacks, the proposed solution leverages image processing and artificial intelligence to verify both the identity and liveliness of users. After reviewing theoretical foundations and potential attack scenarios, we describe the system's deep learning-based architecture, its implementation, and the obtained results. A critical performance analysis concludes the study, outlining paths for improvement in future applications.

Keywords : biometrics, facial recognition, liveness detection, image processing, artificial intelligence.

Table des matières

Dédicace	II
Remerciements	III
Liste des acronymes	VIII
Liste des figures	IX
Liste des tableaux	XI
Liste des symboles	XII
Introduction Générale	1
Chapitre 1: Fondements du traitement d'images et de la reconnaissance faciale pour la vérification biométrique	3
1.1 Introduction	4
1.2 Vérification biométrique : concepts et enjeux	4
1.2.1 Définition de la biométrie et des méthodes courantes	4
1.2.2 Utilisation de la biométrie dans les domaines de la sécurité et de l'identification	5
1.2.3 Importance de la fiabilité et des risques liés à l'usurpation d'identité	5
1.3 Traitement d'images pour la reconnaissance faciale	6
1.3.1 Description du processus de reconnaissance faciale	6
1.3.2 Évolution des méthodes : des traditionnelles vers les modernes	7
1.3.3 Techniques de prétraitement des images biométriques	9
1.4 Détection de vivacité et lutte contre les fraudes	10
1.4.1 Définition et rôle de la détection de vivacité dans la reconnaissance faciale	10
1.4.2 Problèmes liés aux attaques de présentation	10
1.4.3 Aperçu des méthodes utilisées pour la détection de vivacité	11
1.5 Défis du développement d'une solution de reconnaissance faciale intelligente	11
1.5.1 Contraintes techniques affectant les systèmes biométriques de reconnaissance faciale	11
1.5.2 Contraintes spécifiques liés aux biais algorithmiques et à l'équité dans la reconnaissance faciale	12
1.6 Conclusion	13
Chapitre 2: Conception et implémentation de la solution : Méthodologie adoptée et outils utilisés	14
2.1 Introduction	15
2.2 Architecture Globale de la Solution	15
2.3 Présentation l'organigramme principal de la solution proposée	15

2.4	RetinaFace : Procédure de la détection des visage	17
2.4.1	Présentation du modèle RetinaFace	17
2.4.2	Architecture globale	17
2.4.3	Principe de détection faciale par Retina Face	18
2.4.4	Présentation de l'organigramme de la détection du visage	18
2.5	Procédure de détection de vivacité	20
2.5.1	Présentation du modèle CDCN++	20
2.5.2	Architecture globale du CDCN++	20
2.5.3	Présentation du modèle MiniFASNetV1SE	20
2.5.4	Architecture globale de MiniFASNetV1SE	21
2.5.5	Présentation d l'organigramme de détection de vivacité	21
2.6	Procédure de vérification faciale	23
2.6.1	Présentation de la méthode ArcFace	23
2.6.2	Architecture globale d'ArcFace	23
2.6.3	Principe de fonctionnement	23
2.6.4	Présentation du modèle FaceNet512	24
2.6.5	Architecture globale de FaceNet512	24
2.6.6	Présentation de l'organigramme d'extraction des caractéristiques	25
2.6.7	Présentation de l'organigramme de la vérification faciale	26
2.7	Interface homme-machine en mode développeur	26
2.7.1	Point d'entrée principal : /verify	27
2.7.2	Données d'entrée	27
2.7.3	Réponse : format JSON	27
2.8	Conclusion	27
Chapitre 3: Résultats expérimentaux, analyse critique et voies d'amélioration		28
	Introduction	29
3.1	Approche d'évaluation expérimentale	29
3.1.1	Méthodologie d'évaluation	29
3.1.2	Critères d'évaluation utilisés	30
3.2	Environnement de test	31
3.2.1	Configuration matérielle	31
3.2.2	Configuration logicielle	31
3.2.3	Durée moyenne de traitement	31
3.3	Etapas du pipeline de la vérification biométrique	32
3.3.1	Présentation du processus global	32
3.3.2	Analyse détaillée du processus global	33
3.3.3	Détection de visage avec nécessité d'alignement	34
3.3.4	Cas de détection d'une attaque par présentation	36
3.4	Analyse de la distribution des différents scores calculés	37
3.4.1	Analyse des scores de similarité – Cas réels et attaques	37
3.4.2	Analyse des scores de vivacité – Cas réels et attaques	39
3.4.3	Interprétation de la courbe ROC et évaluation globale	41
3.4.4	Analyse critique	41
3.5	Analyse des erreurs et interprétation et des limites	42
3.5.1	Faux négatifs (utilisateurs légitimes rejetés)	42
3.5.2	Faux positifs (attaques acceptées)	43

3.5.3	Limites du système	43
3.6	Interface Homme Machine en mode Utilisateur	44
3.6.1	Objectifs	44
3.6.2	Présentation de l'interface	44
3.6.3	Fonctionnement de l'interface de vérification	45
3.7	Perspectives d'amélioration et travaux futurs	48
3.7.1	Amélioration de la détection de vivacité	48
3.7.2	Optimisation des performances et du code	48
3.7.3	Robustesse et diversité	49
3.7.4	Sécurité des données et expérience utilisateur	49
3.7.5	Développement d'une interface utilisateur embarquée	49
3.7.6	Reprise du mode dynamique basé sur vidéo	49
3.8	Conclusion	51
Conclusion Générale		52
	Références bibliographiques	xiii

Liste des acronymes

AAML	Additive Angular Margin Loss
ACER	Average Classification Error Rate
AUC	Area Under the Curve
BN	Batch Normalization
CDC	Central Difference Convolutional
CDCN++	Central Difference Convolutional Network++
CNN	Convolutional Neural Network
FAR	False Acceptance Rate
FC	Fully Connected layer
FLOPs	Floating Point Operations
FPN	Feature Pyramid Network
FPR	False Positive Rate
FRR	False Rejection Rate
HOG	Histogram of Oriented Gradients
HTER	Half Total Error Rate
IA	Intelligence Artificielle
IQR	Interquartile Range
IR	Infrared
LDA	Linear Discriminant Analysis
LFW	Labeled Faces in the Wild
MAFM	Multi-scale Attention Fusion Module
MIT Media Lab	Massachusetts Institute of Technology Media Lab
NAS	Neural Architecture Search
PCA	Principal Component Analysis
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic
SE	Squeeze-and-Excitation
SIFT	Scale-Invariant Feature Transform
SSH	Single Stage Head-less
TPR	True Positive Rate
ViT	Vision Transformer

Liste des figures

Figure 1.1	Quelques modalités biométriques	5
Figure 1.2	Masque 3D	6
Figure 1.3	Détection de visage	7
Figure 1.4	Représentation des points et vecteurs constituant l’empreinte faciale	7
Figure 1.5	Exemple d’application de la méthode HOG	8
Figure 1.6	Processus d’augmentation de données	9
Figure 1.7	Spoofing à base de l’utilisation de photos numériques	10
Figure 1.8	Spoofing à base de l’utilisation d’un masque photo	10
Figure 1.9	Exemples de données faciales avec répartitions biaisées.	12
Figure 2.1	Processus général de la solution de vérification biométrique proposée.	16
Figure 2.2	Principe de traitement par Retina Face.	18
Figure 2.3	Prédiction multi-tâches	18
Figure 2.4	Principe de la détection de visage considérée	19
Figure 2.5	Central Difference Convolution	20
Figure 2.6	Principe de la détection de vivacité considérée	22
Figure 2.7	Distribution des Caractéristiques 2D sous Norm-Softmax et ArcFace	23
Figure 2.8	La structure du modèle FceNet512	24
Figure 2.9	Triplet Loss : apprentissage par similarité et dissimilarité	25
Figure 2.10	Principe de l’extraction des caractéristiques considérée	25
Figure 2.11	Principe de la vérification faciale considérée	26
Figure 3.1	Aperçu de l’organisation des données	30
Figure 3.2	Extrait de la base de données représentant un même individu.	30
Figure 3.3	Images d’entrée (Dossier Temp $\leftarrow$ ID+Selfie).	32
Figure 3.4	Résultats intermédiaires du traitement (Dossier Output)	32
Figure 3.5	Résultat de détection du visage sur l’image ID	33
Figure 3.6	Résultat de détection du visage sur l’image Selfie	33
Figure 3.7	Résultat du redimensionnement spatial exigé par MiniFASNetV1SE (80x80)	33
Figure 3.8	Heatmap générée en vue de l’analyse spatio-texturale réalisée par CDCN++	34
Figure 3.9	Exemple d’exécution via l’API développée pour la vérification biométrique	34
Figure 3.10	Images avant et après la détection du visage avec alignement des yeux (crop_...).	35
Figure 3.11	Cas de détection d’une déviation (-95.15°) dans la position des yeux nécessitant un alignement automatique.	35
Figure 3.12	Résultat de l’appel de l’API /verify après prétraitement : le système a appliqué la détection et l’alignement, et retourne les scores de vivacité et de similarité.	36
Figure 3.13	Images utilisées dans la tentative d’usurpation d’identité par présentation d’un faux selfie (image scannée)	36
Figure 3.14	Echec d’authentification suite à la non détection de la vivacité du selfie	37
Figure 3.15	Boxplot des scores de similarité pour les cas réels (en vert) et les cas d’attaque (en rouge)	38

Figure 3.16	Résultats d'analyse illustrant un processus de traitement hiérarchique (détection de vivacité prioritaire à la similarité)	38
Figure 3.17	Boxplot des scores de vivacité pour les cas réels (en vert clair) et les cas d'attaque (en rouge).	39
Figure 3.18	Histogramme des scores de vivacité – Répartition des cas réels (vert clair) et des attaques (rouge).	39
Figure 3.19	Courbe ROC pour la détection de vivacité (AUC = 0,96)	41
Figure 3.20	Répartition des causes principales d'erreurs dans les cas réels	43
Figure 3.21	Interface graphique de l'application de vérification biométrique	44
Figure 3.22	Interface graphique après chargement réussi des deux images	45
Figure 3.23	Cas 1 : Authentification réussie (toutes les étapes validées)	46
Figure 3.24	Cas 2 : Plusieurs visages détectés dans le selfie – tentatives échouées	46
Figure 3.25	Cas 3 : Aucun visage détecté dans le selfie – tentatives épuisées	47
Figure 3.26	Cas 4 : Aucun visage détecté dans l'image ID	47
Figure 3.27	Cas 5 : Échec de correspondance ou visage non vivant détecté	48
Figure 3.28	Limites de détection de visage observées pour la solution exécutée en mode dynamique	50
Figure 3.29	Similarité faible malgré une vivacité confirmée, observée pour la solution exécutée en mode dynamique	50
Figure 3.30	Exemple d'illustration des frames extraits d'une vidéo et présentant des problèmes potentiels	51

Liste des tableaux

Table 1.1	Comparaison des méthodes d'authentification	6
Table 1.2	Comparaison des performances des méthodes traditionnelles et les approches modernes en reconnaissance faciale	9
Table 3.1	Résumé statistique des scores de vivacité pour les cas réels, les attaques et le total . .	40
Table 3.2	Taux d'erreur de classification pour les scores de vivacité (seuil = 0,3)	40

Liste des symboles

N1	Nombre de tentatives autorisées pour la prise de selfie en cas d'absence de visage
N2	Nombre de tentatives autorisées pour la prise de selfie en cas de détection d'une tentative d'attaque (visage non vivace)
N3	Nombre de tentatives autorisées pour la numérisation d'une pièce d'identité en cas d'absence de visage sur la partie scannée
Nmax	Nombre de tentatives maximum autorisé
N	le nombre d'échantillons dans le lot d'entraînement
θ_{y_i}	l'angle entre le vecteur d'embedding et le poids de la véritable classe
m	la marge angulaire additionnelle (généralement 0,5)
s	le facteur d'échelle (généralement 64)
θ_j	l'angle entre le vecteur d'embedding de l'échantillon i et le poids de la classe j

Introduction Générale

Dans un monde où la digitalisation des services s'accélère et les technologies numériques deviennent omniprésentes, la question de l'authentification et de la vérification d'identité est devenue centrale. Assurer que l'utilisateur est bien la personne qu'il prétend être constitue désormais un impératif incontournable dans des domaines aussi sensibles que les services bancaires, la santé, les télécommunications ou encore l'administration publique.

Parmi les différentes méthodes d'identification, la biométrie s'impose progressivement comme une solution de référence. Sa capacité à allier fiabilité, rapidité et simplicité d'usage la rend particulièrement attrayante du point de vue de sécurité et de fluidité. La reconnaissance faciale, en particulier, connaît une adoption croissante et s'intègre de plus en plus dans les processus d'authentification.

Malgré les progrès constants dans les algorithmes de reconnaissance, ces systèmes restent vulnérables à certaines formes d'attaques, notamment les attaques dites de présentation. Il s'agit de tentatives de tromperie utilisant des photographies, vidéos ou masques représentant le visage d'un tiers, capables, dans certains cas, de déjouer des modèles pourtant performants.

C'est dans ce contexte qu'émerge un besoin crucial : la capacité à vérifier que le visage présenté est bien celui d'un individu vivant. La détection de vivacité devient alors un élément fondamental, venant renforcer les systèmes de reconnaissance faciale pour prévenir les tentatives d'usurpation d'identité. Cette vérification repose sur l'analyse de signes subtils, tels que des micro-mouvements, des variations de texture ou de luminosité, difficilement reproductibles par des artefacts. L'intelligence artificielle, en particulier les techniques d'apprentissage profond, offre aujourd'hui les moyens technologiques nécessaires pour relever ce défi, en exploitant toute la richesse des signaux visuels grâce au traitement d'images.

Malgré ces avancées, de nombreux obstacles subsistent : la variabilité des conditions de capture, les biais potentiels dans les jeux de données, ou encore la nécessité de préserver une expérience utilisateur fluide tout en assurant un niveau de sécurité élevé contre les tentatives de fraude ou d'usurpation d'identité. Ces enjeux complexes appellent des solutions capables d'allier robustesse technique et adaptabilité aux contraintes du monde réel.

Le présent mémoire s'inscrit dans cette dynamique de recherche appliquée, avec pour objectif de concevoir une solution combinant détection de visage, reconnaissance faciale et détection de vivacité, visant à renforcer la fiabilité des systèmes biométriques existants.

Pour atteindre ces objectifs, nous avons suivi une démarche méthodique alliant analyse, conception et validation expérimentale. Des choix techniques ont été effectués afin de sélectionner les modèles et les algorithmes adaptés. Une base de données diversifiée, incluant des exemples réels et falsifiés, a été constituée pour entraîner et tester le modèle développé. Enfin, une évaluation des performances a été menée, en mettant l'accent sur la précision, la robustesse et la résilience face à des conditions variées.

Le mémoire est structuré comme suit :

— **Chapitre 1** : Il expose les fondements théoriques sur lesquels repose notre travail. Il présente les no-

tions essentielles liées à la biométrie, à la reconnaissance faciale et la détection de vivacité ainsi qu'aux techniques de traitement d'images nécessaires à la compréhension de notre solution.

- **Chapitre 2** : Il détaille la conception et l'implémentation de la solution proposée.
- **Chapitre 3** : Il présente les résultats expérimentaux obtenus. Une analyse critique est menée pour évaluer les performances de la solution développée, en identifiant ses limites et en proposant des pistes d'amélioration.

Enfin, une conclusion vient clôturer ce travail en récapitulant les contributions apportées pour la vérification de l'atteinte des objectifs fixés.

Chapitre 1

Fondements du traitement d'images
et de la reconnaissance faciale
pour la vérification biométrique

1.1 Introduction

À l'ère de la transformation numérique, l'authentification des utilisateurs est devenue un enjeu majeur de sécurité. Parmi les technologies émergentes, la biométrie se distingue par sa capacité à offrir une identification fiable et rapide, en s'appuyant sur les caractéristiques uniques de chaque individu. Ce premier chapitre s'attache à poser les fondements théoriques de la vérification biométrique, en mettant l'accent sur la reconnaissance faciale et son intégration au sein des systèmes de sécurité modernes. Il explore également le rôle essentiel du traitement d'images dans l'extraction et l'analyse des caractéristiques faciales, tout en présentant les enjeux liés à la détection de vivacité. À travers cette exploration, ce chapitre met en lumière les opportunités offertes par ces technologies, ainsi que les défis techniques, éthiques et sociaux qu'elles soulèvent.

1.2 Vérification biométrique : concepts et enjeux

Ce chapitre introduit les notions fondamentales de la vérification biométrique, en mettant l'accent sur la reconnaissance faciale comme méthode d'authentification fiable. Il décrit les types de données utilisées, les principes de fonctionnement des systèmes biométriques, ainsi que leurs exigences en termes de performance et de sécurité. L'accent est mis sur les défis posés par les attaques de présentation, et sur la nécessité d'intégrer des mécanismes de détection de vivacité pour renforcer la fiabilité de ces systèmes.

1.2.1 Définition de la biométrie et des méthodes courantes

La biométrie est une discipline qui s'appuie sur l'analyse des caractéristiques physiques, biologiques ou comportementales propres à chaque individu afin de permettre son identification ou son authentification. Ces caractéristiques, uniques et généralement permanentes, sont utilisées dans divers domaines pour renforcer la sécurité et simplifier les processus d'identification.[1]. Parmi les méthodes les plus utilisées, on distingue :

- **La reconnaissance par les empreintes digitales** : Chaque individu possède des motifs uniques sur la pulpe de ses doigts, formés par des crêtes et des sillons. Ces empreintes sont utilisées depuis longtemps pour l'identification en raison de leur unicité et de leur stabilité au cours du temps.
- **La reconnaissance de l'iris** : L'iris, partie colorée de l'œil, présente des motifs complexes et uniques à chaque personne. Cette méthode offre une grande précision, car l'iris est protégé et stable tout au long de la vie.
- **La reconnaissance faciale** : Cette technique analyse les traits du visage, tels que la distance entre les yeux, la forme du nez ou la structure osseuse, pour identifier une personne. Elle est largement utilisée dans les smartphones et les systèmes de surveillance.

Afin d'illustrer la diversité des modalités biométriques existantes, la figure 1.1 présente un aperçu visuel des principales techniques utilisées en identification. On y retrouve notamment les empreintes digitales, les traits du visage, l'iris, la démarche, la reconnaissance vocale, l'analyse de la paume, la signature dynamique, ainsi que l'ADN. Chacune de ces modalités repose sur des caractéristiques uniques, plus ou moins faciles à acquérir, à falsifier, ou à traiter, ce qui influence leur usage selon les contextes d'application.



Figure 1.1 : Modalités biométriques utilisées pour l'identification biométrique
Par exemple :visage, empreintes, iris, voix, démarche, paume, signature, et ADN [1].

1.2.2 Utilisation de la biométrie dans les domaines de la sécurité et de l'identification

Les systèmes biométriques sont largement intégrés dans des dispositifs de sécurité à différents niveaux .

Dans le domaine du contrôle aux frontières, les systèmes biométriques, tels que la reconnaissance faciale et les empreintes digitales, facilitent le passage des voyageurs tout en renforçant la sécurité[2]. Les institutions financières intègrent la biométrie pour sécuriser les transactions et simplifier l'accès aux services, réduisant ainsi les risques de fraude[3].

Dans les infrastructures sensibles, la biométrie est utilisée pour restreindre l'accès aux zones sécurisées, assurant que seules les personnes autorisées peuvent y accéder[4].

Enfin, dans le secteur médical, la biométrie joue un rôle crucial dans l'identification des patients et la protection des données médicales, réduisant les erreurs d'identification et assurant un accès sécurisé aux dossiers médicaux[5].

1.2.3 Importance de la fiabilité et des risques liés à l'usurpation d'identité

Bien que les systèmes biométriques offrent des avantages significatifs en matière de sécurité, ils présentent également des vulnérabilités techniques et éthiques qu'il convient de considérer. Parmi les menaces techniques, les attaques de présentation — telles que l'utilisation de photos, de vidéos ou de masques 3D — peuvent tromper les dispositifs de reconnaissance faciale. La figure 1.2 illustre un exemple de ce type d'attaque, à l'aide d'un masque 3D[6].

De plus, l'émergence des deepfakes, générés par intelligence artificielle, représente une menace croissante, car ils peuvent imiter fidèlement un visage ou une voix, rendant la détection de falsifications plus difficile[8]. Ces manipulations sophistiquées peuvent être utilisées pour contourner les systèmes de vérification d'identité à distance, compromettant ainsi la fiabilité des authentifications biométriques.

Les préoccupations éthiques sont également importantes, notamment en ce qui concerne la collecte, le stockage et la protection des données biométriques sensibles. Une mauvaise gestion de ces données peut entraîner des violations de la vie privée et des risques de piratage[9].



Figure 1.2 : Masque 3D[7]

Par ailleurs, la fiabilité des systèmes biométriques peut être affectée par des conditions environnementales défavorables, telles qu'une mauvaise luminosité, des angles de prise de vue inadéquats ou des changements physiques chez l'utilisateur, ce qui peut compromettre l'exactitude de l'identification[10].

La Table 1.1 montre que l'authentification biométrique se distingue par une sécurité et une commodité élevées par rapport aux méthodes traditionnelles telles que les mots de passe ou les jetons physiques.

Table 1.1 : Comparaison des méthodes d'authentification[11]

Caractéristique	Authentification Bio-métrique	Mots de Passe/PIN	Authentification Basée sur un Jeton
Sécurité	Élevée (traits uniques)	Moyenne (devinable)	Moyenne (peut être volé)
Commodité	Très élevée	Basse (mémoire nécessaire)	Basse (nécessite un jeton physique)
Risque de Perte	Aucun	Élevé	Élevé
Évolutivité	Élevée	Élevée	Moyenne

1.3 Traitement d'images pour la reconnaissance faciale

Le traitement d'images est une composante essentielle de la reconnaissance faciale. Il englobe un ensemble de techniques permettant d'analyser, de transformer et d'interpréter des images numériques afin d'en extraire des informations pertinentes. Dans ce contexte, ces méthodes facilitent la détection des visages, l'extraction de caractéristiques distinctives et leur comparaison avec des données enregistrées pour l'identification ou l'authentification des individus.

1.3.1 Description du processus de reconnaissance faciale

La reconnaissance faciale repose sur un enchaînement structuré d'étapes, intégrant le traitement d'images et l'intelligence artificielle :

- **Acquisition** : La première étape consiste à capturer une image du visage à l'aide d'une caméra ou d'un capteur. La qualité de cette acquisition dépend de facteurs tels que l'éclairage, l'orientation du visage et la résolution de l'appareil[12].

- **La détection du visage** : Une fois l'image capturée, le système identifie les zones contenant un visage comme l'illustre la figure 1.3. Des algorithmes spécialisés, tels que les cascades de Haar [13] ou les réseaux de neurones convolutifs, sont utilisés pour localiser précisément les visages dans l'image [14].

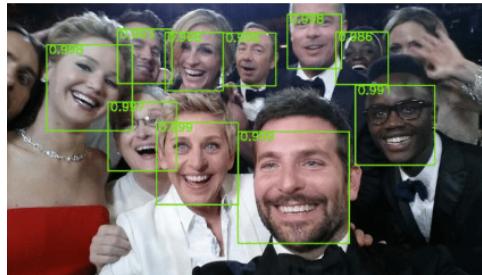


Figure 1.3 : Détection de visage

- **Le prétraitement** : Cette étape vise à normaliser l'image pour améliorer la qualité des données avant l'analyse. Les opérations courantes incluent le redimensionnement, l'alignement du visage, la conversion en niveaux de gris et la réduction du bruit. Ces techniques permettent de minimiser les variations dues à l'environnement ou à la position de l'utilisateur [14].
- **L'extraction des caractéristiques** : Le système extrait des vecteurs numériques représentant les traits distinctifs du visage, appelés "empreintes faciales", la figure 1.4 illustre cette approche. Des méthodes telles que les descripteurs de caractéristiques locales (par exemple, les histogrammes de gradients orientés) ou les réseaux de neurones profonds sont utilisés pour obtenir ces représentations [14].

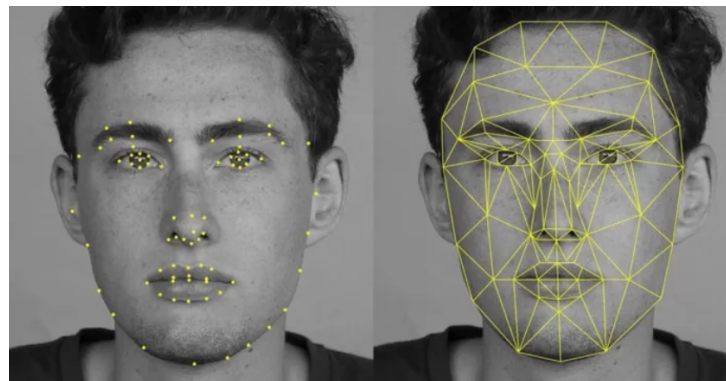


Figure 1.4 : Représentation des points et vecteurs constituant l'empreinte faciale [15]

- **La comparaison et la décision** : Les empreintes faciales extraites sont comparées à celles stockées dans une base de données pour déterminer une correspondance. Des mesures comme la distance euclidienne, sont utilisées pour évaluer la similarité des visages. Si la similarité estimée dépasse un certain seuil, le système réussi à confirmer l'identité de l'individu [16].

1.3.2 Évolution des méthodes : des traditionnelles vers les modernes

La reconnaissance faciale a connu une évolution significative, passant des méthodes traditionnelles à des approches modernes exploitant l'apprentissage profond. Cette section présente quelques méthodes parmi les plus caractéristiques des deux paradigmes :

— Méthodes traditionnelles

1. **Eigenfaces (Analyse en Composantes Principales - PCA)** : Introduite par Turk et Pentland, cette méthode projette les images de visages dans un espace de caractéristiques de plus faible dimension,

appelé "espace des visages". Elle capture les principales variations entre les visages, facilitant ainsi leur classification[17] .

2. **Fisherfaces (Analyse Discriminante Linéaire - LDA)** : Cette technique maximise la séparabilité entre différentes classes de visages en projetant les données dans un espace où la variance entre les classes est accentuée, tout en minimisant la variance intra-classe [18].
3. **Descripteurs SIFT et HOG** : Ces descripteurs extraient des caractéristiques locales invariantes aux changements d'échelle, de rotation et d'éclairage. SIFT détecte des points d'intérêt et les décrit par des vecteurs de gradient, tandis que HOG [19] capture la distribution des orientations des gradients dans des régions localisées de l'image comme le montre la figure ci-dessous[20] .



Figure 1.5 : Exemple d'application de la méthode HOG[20].

— Avancées modernes

1. **Apprentissage profond avec Réseaux de Neurones Convolutifs** : Les CNN permettent d'apprendre automatiquement des représentations hiérarchiques des visages à partir de vastes ensembles de données. Des architectures avancées telles que FaceNet ou DeepFace ont démontré une précision remarquable, même dans des conditions de lumière, de pose ou d'expression variées[21].
2. **Reconnaissance 3D** : Contrairement aux approches 2D, la reconnaissance 3D capture la structure tridimensionnelle du visage, offrant une meilleure robustesse aux variations de pose et d'éclairage. Elle est particulièrement efficace pour distinguer des visages très similaires, comme ceux des jumeaux identiques [22].
3. **Transformers** : Inspirés des progrès dans le traitement du langage naturel, les Transformers ont été adaptés à la vision par ordinateur via des modèles comme Vision Transformer. Ils permettent de capturer des relations globales dans l'image, offrant une meilleure compréhension contextuelle que les CNN traditionnels. Ces architectures récentes surpassent parfois les CNN dans des tâches complexes, tout en conservant une grande flexibilité et une capacité de généralisation élevée[23].

La Table 1.2 résume les performances des méthodes traditionnelles et les approches modernes en reconnaissance faciale.

Table 1.2 : Comparaison des performances des méthodes traditionnelles et les approches modernes en reconnaissance faciale

Critère	Méthodes traditionnelles	Avancées modernes
Précision	Moyenne	Élevée
Robustesse aux variations	Faible	Forte
Complexité computationnelle	Faible	Élevée
Données requises	Modérées	Importantes
Facilité de mise en œuvre	Simple	Complexe

1.3.3 Techniques de prétraitement des images biométriques

L'efficacité des systèmes de reconnaissance faciale dépend en grande partie de la qualité des images traitées et des techniques avancées de prétraitement. Les principales techniques incluent :

- **Le redimensionnement** : ajuste toutes les images à une taille spécifique, ce qui garantit une cohérence des données d'entrée. Cette uniformité est cruciale pour de nombreux modèles d'apprentissage profond qui exigent une taille d'entrée constante. De plus, le redimensionnement réduit la complexité des calculs et accélère l'entraînement [24].
- **La normalisation des pixels** : consiste à transformer les valeurs des pixels d'une image pour les placer sur une échelle standardisée (généralement entre 0 et 1, ou centrée avec un écart-type de 1 (blanchiment)). Cela améliore la stabilité et la vitesse de convergence des réseaux de neurones [24].
- **L'alignement facial** : repositionne automatiquement le visage selon un axe standard (par exemple, en alignant les yeux) afin de réduire les erreurs liées à l'orientation. Cette étape est souvent réalisée à l'aide de réseaux convolutifs détectant les points clés du visage [25].
- **Le nettoyage des données** : vise à améliorer la qualité de l'ensemble de données en supprimant ou en corrigeant les erreurs (images floues, mal étiquetées, de mauvaise qualité, etc.). Cela permet d'éviter le surapprentissage ou l'introduction de biais dans les modèles [26].
- **L'augmentation des données** : génère de nouvelles images à partir des images existantes via des transformations telles que la rotation, le zoom, le retournement, le cisaillement ou l'ajustement de la luminosité. Cette méthode renforce la diversité de l'ensemble d'apprentissage et améliore la généralisation des modèles [27], la figure 1.6 illustre ce processus.



Figure 1.6 : Processus d'augmentation de données[28]

1.4 Détection de vivacité et lutte contre les fraudes

La reconnaissance faciale est devenue une composante essentielle des systèmes d'authentification biométrique. Toutefois, elle reste vulnérable aux attaques dites de présentation, où un imposteur tente de tromper le système en utilisant des représentations artificielles telles que des photos, des vidéos ou des masques.

1.4.1 Définition et rôle de la détection de vivacité dans la reconnaissance faciale

La détection de vivacité est une technique qui permet de vérifier que l'image capturée par le système provient bien d'une personne réelle physiquement présente devant la caméra, et non d'un support frauduleux. Elle joue un rôle crucial dans la protection contre les attaques de présentation, en garantissant que seuls les individus authentiques peuvent accéder aux services sécurisés [29].

1.4.2 Problèmes liés aux attaques de présentation

Les attaques de présentation, ou "spoofing", consistent à usurper une identité en présentant au système de reconnaissance faciale une fausse représentation du visage d'une personne autorisée. Plusieurs techniques sont utilisées par les fraudeurs, allant des supports les plus simples aux plus sophistiqués.

- **Photo numérique ou imprimée** : L'utilisation de photographies statiques affichées sur écran ou imprimées sur papier peut suffire à tromper des systèmes peu robustes. La figure 1.7 illustre une attaque typique de ce genre.



Figure 1.7 : Spoofing à base de l'utilisation de photos numériques [30]

- **Masque photo découpé** : Il s'agit d'une photographie imprimée, souvent modifiée par des découpes au niveau des yeux ou de la bouche pour simuler une certaine vivacité. Ce type de fraude est illustré en figure 1.8.

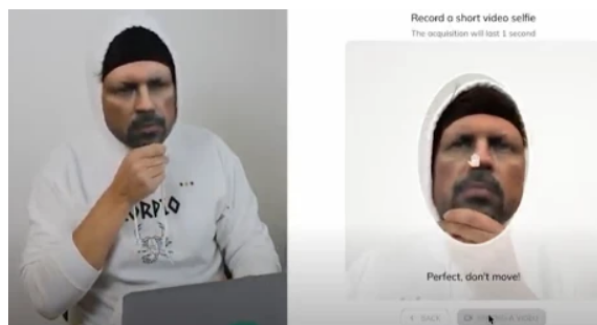


Figure 1.8 : Spoofing à base de l'utilisation d'un masque photo [30]

- **Vidéos préenregistrées** : Des séquences vidéo montrant la personne cible peuvent être diffusées pour simuler des mouvements naturels (clignement, légers déplacements), rendant la détection de vivacité plus difficile [31].
- **Masques 3D** : Fabriqués en silicone, latex ou d'autres matériaux souples, ces masques reproduisent les traits du visage avec une fidélité impressionnante. Ils peuvent tromper les systèmes qui ne prennent pas en compte la profondeur ou les micro-expressions [30].
- **Deepfakes** : Générés par des réseaux de neurones, ils permettent de créer des vidéos hyperréalistes dans lesquelles le visage d'une personne est superposé à celui d'une autre, rendant la détection encore plus complexe [32].

Face à ces menaces de plus en plus sophistiquées, la détection de vivacité s'impose comme une contre-mesure indispensable pour garantir l'intégrité et la fiabilité des systèmes de reconnaissance faciale.

1.4.3 Aperçu des méthodes utilisées pour la détection de vivacité

Diverses approches ont été développées pour détecter la vivacité d'un visage . Elles se divisent principalement en deux catégories[29] :

- **Méthodes actives** : requièrent une interaction de l'utilisateur, comme cligner des yeux, tourner la tête ou suivre un objet à l'écran. Ces actions permettent de vérifier la présence d'une personne réelle en temps réel.
- **Méthodes passives** : n'exigent aucune action de l'utilisateur et analysent des caractéristiques naturelles du visage, telles que la texture de la peau, les micro-mouvements ou les reflets, pour déterminer la vivacité.

Parmi les techniques spécifiques utilisées pour la détection de vivacité **l'analyse des micro-mouvements involontaires du visage**, comme les clignements des yeux ou les contractions musculaires, permet de distinguer un visage réel d'une représentation artificielle, car ces mouvements sont difficiles à reproduire avec des artefacts[33] .

L'analyse de la texture de la peau joue également un rôle crucial en examinant les détails cutanés pour détecter des anomalies indiquant une surface artificielle, comme une photo ou un écran[33].

De plus, certaines solutions utilisent des techniques telles que la spectroscopie pour **analyser les propriétés optiques de la peau**, permettant de différencier la peau humaine des matériaux synthétiques[33].

1.5 Défis du développement d'une solution de reconnaissance faciale intelligente

Le développement d'une solution d'intelligence artificielle pour la reconnaissance faciale exige de surmonter plusieurs défis techniques, éthiques et pratiques. Ces obstacles sont cruciaux à considérer pour garantir la fiabilité, l'équité et la sécurité du système.

1.5.1 Contraintes techniques affectant les systèmes biométriques de reconnaissance faciale

La variabilité des conditions d'acquisition constitue un obstacle majeur, des changements d'éclairage, des angles de vue différents, des expressions faciales variées ou la présence d'accessoires tels que lunettes ou masques peuvent altérer la qualité des images capturées, rendant la reconnaissance moins fiable.

La qualité des données est également cruciale ; des images floues ou de faible résolution, souvent issues de caméras de surveillance, peuvent entraîner des erreurs d'identification, augmentant les taux de faux positifs ou de faux négatifs [34].

Les limitations des capteurs, notamment leur sensibilité aux conditions environnementales et leur résolution parfois insuffisante, affectent également la précision de la reconnaissance .

Enfin, **les algorithmes de reconnaissance faciale**, en particulier ceux basés sur l'apprentissage profond, requièrent des ressources computationnelles importantes, ce qui peut poser problème pour les dispositifs embarqués ou les applications en temps réel [28].

1.5.2 Contraintes spécifiques liés aux biais algorithmiques et à l'équité dans la reconnaissance faciale

Les systèmes de reconnaissance faciale sont confrontés à des biais algorithmiques susceptibles d'entraîner des discriminations envers certains groupes de personnes. Ces biais peuvent provenir de plusieurs sources, notamment des données d'entraînement non représentatives de la diversité de la population.

En effet, si les ensembles de données utilisés pour entraîner les modèles ne reflètent pas la diversité en termes d'âge, de genre ou d'origine ethnique, les performances du système peuvent varier significativement entre les groupes. Par exemple, un modèle entraîné principalement sur des visages d'un groupe ethnique spécifique sera moins précis pour identifier des visages issus d'autres groupes [35].

Des études ont montré que certains systèmes de reconnaissance faciale présentent des taux d'erreur plus élevés pour les femmes et les personnes à la peau foncée. Par exemple, une étude du MIT Media Lab a révélé que certains systèmes commerciaux avaient un taux d'erreur allant jusqu'à 34,7% pour les femmes à peau foncée, contre seulement 0,8 % pour les hommes à peau claire [36].

La figure 1.9 explique comment les ensembles de données utilisés pour l'entraînement des systèmes de reconnaissance faciale présentent souvent une répartition déséquilibrée en termes de genre et de teinte de peau

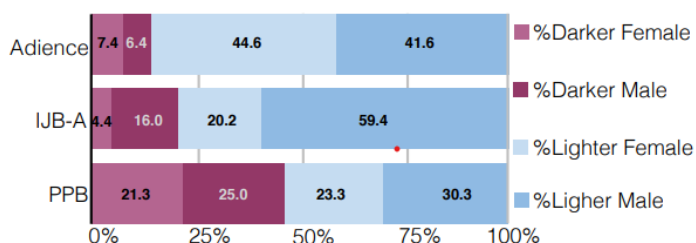


Figure 1.9 : Exemples de données faciales avec répartitions biaisées.[37].

Les erreurs d'identification peuvent avoir des impacts graves, notamment en matière de sécurité publique, de surveillance ou d'accès à des services. Par exemple, des personnes faussement identifiées pourraient faire l'objet d'arrestations injustifiées ou se voir refuser l'accès à des lieux ou à des services [38].

Ces biais soulignent la nécessité d'une vigilance accrue dans le développement et le déploiement des technologies de reconnaissance faciale, afin de garantir l'équité et de prévenir les discriminations.

La confidentialité des données biométriques est désormais une question centrale. La collecte et le traitement de ces données sensibles doivent respecter des normes strictes pour éviter les dérives, comme la surveillance non consentie ou les violations de vie privée.

Face à ces constats, le projet présenté dans ce mémoire vise à répondre aux besoins suivants :

- Renforcer la précision et la robustesse du système face aux variations environnementales ;
- Intégrer un module de détection de vivacité, pour distinguer un visage réel d'une attaque ;

1.6 Conclusion

Ce chapitre a permis d'établir les bases essentielles à la compréhension des systèmes de vérification biométrique. En mettant en évidence les principes de la biométrie, les étapes du traitement d'images pour la reconnaissance faciale et les méthodes de détection de vivacité, nous avons montré comment ces éléments interagissent pour renforcer la sécurité des systèmes d'authentification. Les défis techniques soulignent la nécessité de solutions robustes. Ces considérations serviront de socle à la conception de notre propre solution, qui sera abordée dans le chapitre suivant.

Chapitre 2

Conception et implémentation de la solution :
Méthodologie adoptée et outils utilisés

2.1 Introduction

Ce deuxième chapitre s'intéresse à la mise en œuvre pratique d'une solution d'authentification biométrique sécurisée. L'objectif est de présenter l'architecture globale du système développé, en détaillant les modules de détection de visage, de détection de vivacité et de vérification faciale. Ce chapitre décrit également les outils utilisés, les choix méthodologiques adoptés, ainsi que les jeux de données exploités pour l'entraînement et les tests. Chaque composant de la solution est étudié en profondeur afin de justifier son intégration et d'évaluer sa contribution à l'efficacité globale du système.

2.2 Architecture Globale de la Solution

L'architecture de la solution a été pensée selon une approche modulaire, assurant une intégration cohérente des divers composants.

1. **Module de détection de visage** : Se base sur le modèle RetinaFace pour localiser les visages dans une image.
2. **Module de détection de vivacité** : Implémente les modèles CDCN++ et MiniFASNetV1SE pour vérifier si le visage détecté est bien réel ou qu'il s'agit d'une attaque.
3. **Module de vérification faciale** : Emploie les modèles ArcFace et Facenet512 pour identifier l'individu en comparant les caractéristiques faciales extraites à du visage présenté et jugé comme réel référence donnée en vue de l'authentification d'un utilisateur.

2.3 Présentation l'organigramme principal de la solution proposée

Le schéma de la figure 2.1 représente le flux global du processus de vérification biométrique intégrant la détection de visage, la détection de vivacité, la vérification faciale, et la gestion du nombre de tentatives autorisées via des compteurs assurant la sécurité.

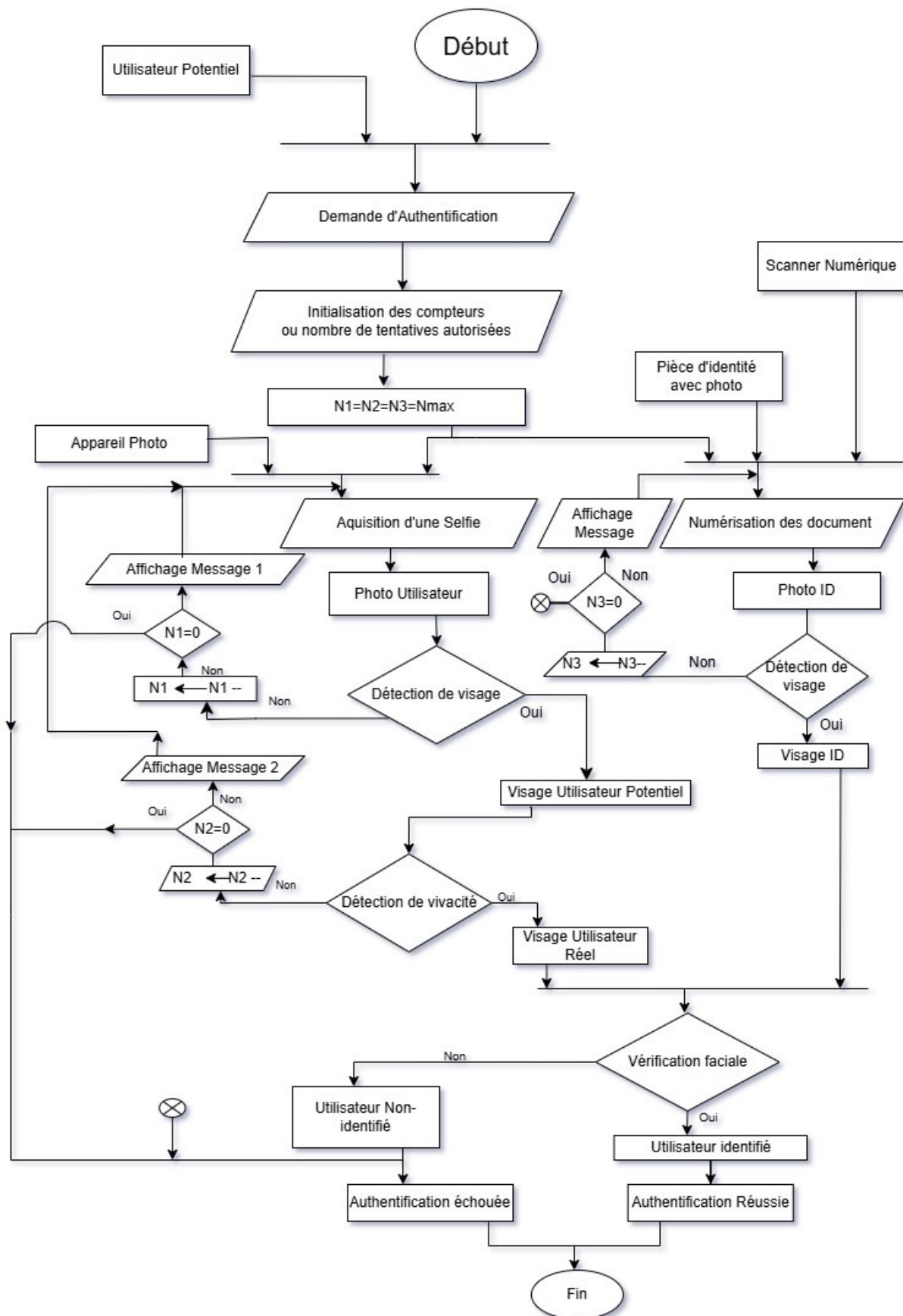


Figure 2.1 : Processus général de la solution de vérification biométrique proposée.

Le processus commence lorsqu'un utilisateur potentiel tente d'accéder à un système nécessitant une authentification. Le système initie une demande d'identification, ce qui déclenche l'initialisation de plusieurs compteurs :

- N1: Nombre de tentatives autorisées pour la prise de selfie en cas d'absence de visage.
- N2: Nombre de tentatives autorisées pour la prise de selfie en cas de détection d'une tentative d'attaque (visage non vivace).
- N3: Nombre de tentatives autorisées pour la numérisation d'une pièce d'identité en cas d'absence de visage sur la partie scannée.

Ensuite, l'utilisateur doit fournir deux types de données : une pièce d'identité avec photo (faciale) et une photo instantanée du visage de l'utilisateur présumé (un selfie).

Pour la photo d'identité, l'utilisateur scanne un document à l'aide d'un scanner numérique. Le système tente alors d'extraire le visage présent sur la pièce d'identité. Suite à chaque échec, un message d'information s'affiche invitant l'utilisateur à présenter une pièce d'identité valide et à tenir compte du nombre de tentatives restantes.

Par ailleurs, l'utilisateur est invité à prendre un selfie via une caméra ou un appareil photo intégré. Si la photo n'est pas correcte (visage non détecté ou de mauvaise qualité), un message d'erreur s'affiche, par exemple : "Visage non détecté, il vous reste N1 tentatives possibles", et le système autorise plusieurs essais, contrôlés par le compteur N1. Dès qu'une photo comportant une zone faciale est détectée, la suite du processus de traitement est enclenchée.

Dès que le visage est détecté sur le Selfie, le système passe à l'estimation de la vivacité du visage pour détecter les tentatives d'attaques par présentation. Si le test de vivacité échoue, le système permet plusieurs tentatives (gérées par N2) avant de considérer l'utilisateur comme fake.

Si la vivacité du visage est confirmée, une vérification faciale est effectuée en comparant les caractéristiques du visage réel aux caractéristiques du visage scanné (pièce d'identité). En cas de similarité insuffisante, l'utilisateur ne peut être identifié, entraînant le rejet de la demande d'authentification (opération échouée). En cas de similarité avérée, l'utilisateur est identifié et sa demande d'authentification est accordée (opération réussie).

2.4 RetinaFace : Procédure de la détection des visage

2.4.1 Présentation du modèle RetinaFace

Développé par l'équipe InsightFace, RetinaFace [39] est un détecteur de visages à un seul étage qui intègre plusieurs tâches en une seule passe : la détection de visages, l'alignement 2D des points clés. IL utilise des techniques d'apprentissage multi-tâches supervisées et auto-supervisées pour améliorer la précision de la localisation faciale[39].

2.4.2 Architecture globale

L'architecture de RetinaFace repose sur les éléments suivants :

1. **Réseau de base** : Il traite l'image d'entrée pour en extraire des caractéristiques hiérarchiques à différents niveaux de profondeur. Ces caractéristiques sont ensuite utilisées pour détecter les visages, prédire les boîtes englobantes et localiser les points clés du visage, comme le montre la figure 2.2 .
2. **Feature Pyramid Network** : C'est une technique qui améliore la détection des objets de différentes tailles, notamment les petits visages, en combinant les détails des couches peu profondes avec les informations globales des couches profondes du réseau[40].
3. **Modules de Contexte** : Ces modules enrichissent les cartes de caractéristiques avec du contexte visuel, ce qui améliore la détection des visages dans des conditions difficiles comme les occlusions ou les faibles résolutions[41].

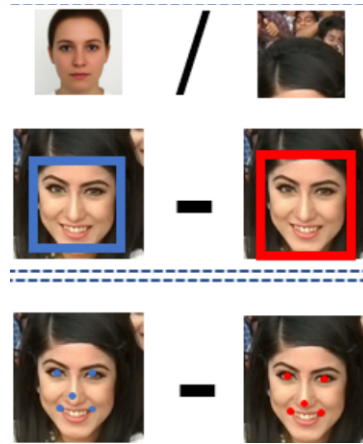


Figure 2.2 : Principe de traitement par Retina Face [39]

4. **Têtes de Prédiction Multi-tâches** : permettent au modèle d'effectuer plusieurs tâches à la fois, comme la classification, la détection des boîtes englobantes, la localisation de points clés comme l'explique la figure suivante.

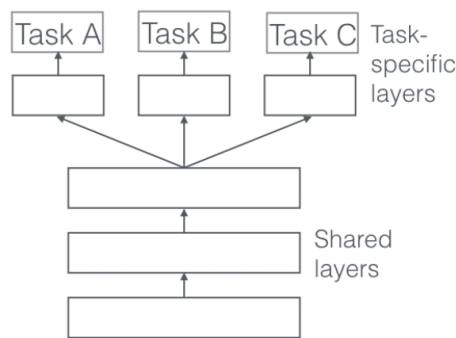


Figure 2.3 : Prédiction multi-tâches [28]

2.4.3 Principe de détection faciale par Retina Face

La classification consiste à déterminer si une région spécifique de l'image contient un visage ou non. Le modèle attribue une probabilité à chaque région, indiquant la présence ou l'absence d'un visage. Cette étape est cruciale pour filtrer les zones non pertinentes et se concentrer sur les régions d'intérêt[42].

Une fois qu'une région est identifiée comme contenant un visage, le modèle prédit les coordonnées précises de la boîte englobante qui entoure le visage. Cela implique de déterminer les positions exactes des coins de la boîte, permettant ainsi de localiser le visage avec précision dans l'image[43].

La localisation de points clés vise à identifier des éléments spécifiques sur le visage, tels que les yeux, le nez et les coins de la bouche.

2.4.4 Présentation de l'organigramme de la détection du visage

L'organigramme de la figure 2.4 représente le processus de détection de visage considéré pour notre solution, se basant sur le modèle Retina Face. Tout commence avec la présentation en entrée d'une photo à évaluer (selfie ou photo d'identité). Une première étape de prétraitement est effectuée afin de normaliser l'image pour la rendre exploitable

par l'algorithme. Ensuite, une vérification est réalisée pour détecter la présence de zones faciales. Si aucune zone de visage n'est trouvée, le processus s'arrête. En revanche, si un visage est détecté, les caractéristiques faciales comme les yeux, le nez et la bouche sont extraites. Les points clés de ces zones sont identifiés avec des scores de confiance. Ces points sont ensuite utilisés pour valider et filtrer la zone faciale à retenir (visage dominant). Une vérification est faite pour savoir si les yeux repérés sont correctement alignés. Dans le cas contraire, un alignement du visage est effectué via une rotation géométrique suivant un angle déterminé. Une fois l'alignement validé, l'image est recadrée autour du visage selon un rectangle englobant minimal. Le processus se termine alors avec succès lorsque le visage est correctement détecté, aligné et isolé du reste de l'image.

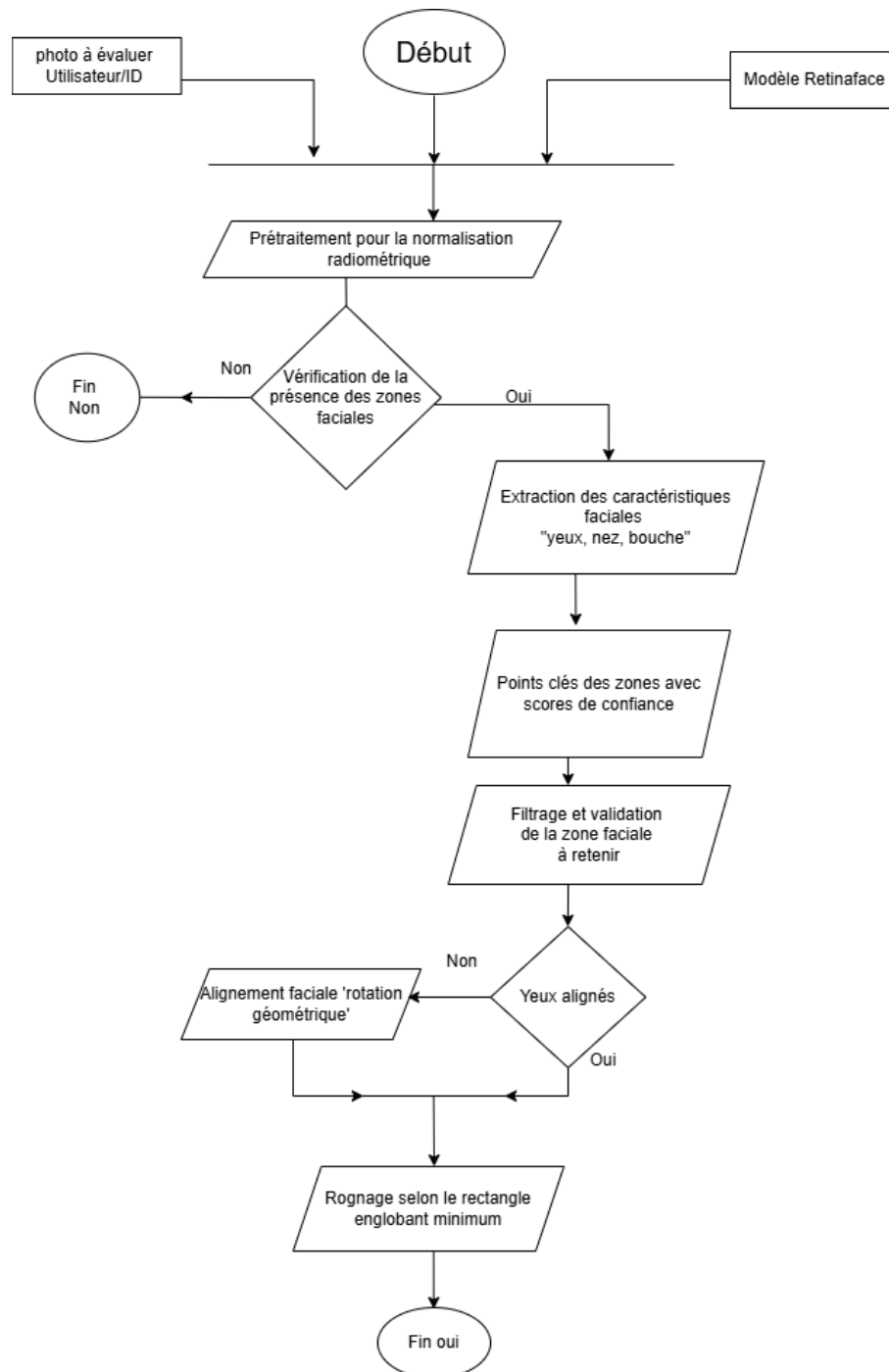


Figure 2.4 : Principe de la détection de visage considérée

2.5 Procédure de détection de vivacité

Cette section présente les méthodes utilisées pour détecter la vivacité d'un visage. L'objectif est de vérifier que l'image transmise correspond à une personne réelle et non à une tentative de fraude.

Deux modèles sont étudiés : CDCN++ et MiniFASNetV1SE.

2.5.1 Présentation du modèle CDCN++

CDCN++ [44] est une version améliorée du modèle CDCN, conçu pour la détection de la fraude faciale (face anti-spoofing). Cette méthode repose sur une nouvelle opération de convolution appelée Central Difference Convolution (CDC), qui améliore la capacité du réseau à extraire des caractéristiques fines et invariantes, essentielles pour détecter les subtilités entre les visages authentiques et les attaques[44].

2.5.2 Architecture globale du CDCN++

CDC est une version améliorée de la convolution classique. Elle prend en compte à la fois l'intensité des pixels et leurs variations locales, contrairement à la convolution traditionnelle, qui fait simplement une somme pondérée des pixels voisins, ce qui permet de capturer davantage de détails fins et de textures dans l'image, la figure ci-dessous explique simplement ce processus.

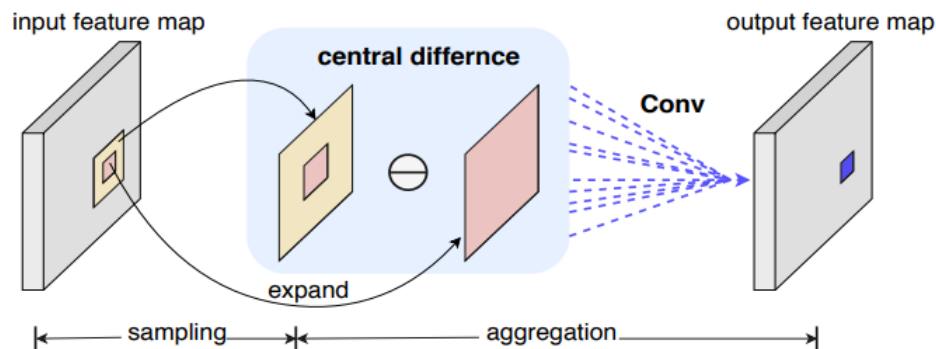


Figure 2.5 : Central Difference Convolution [44]

CDCN++ est entraîné en utilisant des cartes de profondeur comme supervision, ce qui permet au modèle d'apprendre à distinguer les visages réels des attaques en se basant sur des informations structurelles tridimensionnelles. Cette supervision en profondeur renforce la capacité du modèle à généraliser à des scénarios variés et à détecter efficacement les tentatives de spoofing[44].

2.5.3 Présentation du modèle MiniFASNetV1SE

Le MiniFASNetV1SE est une version améliorée du modèle MiniFASNetV1, spécifiquement conçue pour la détection passive — sans interaction utilisateur — des attaques par usurpation faciale. Cette version intègre des modules Squeeze-and-Excitation (SE) [45], apportant une amélioration structurelle au réseau de base pour renforcer sa capacité à distinguer les visages réels des tentatives d'usurpation.

2.5.4 Architecture globale de MiniFASNetV1SE

MiniFASNetV1SE est un modèle léger de réseau de neurones convolutifs, conçu pour fonctionner efficacement sur des appareils à ressources limitées[46]. Il utilise :

- Des blocs convolutionnels peu profonds pour extraire les caractéristiques importantes de l'image ;
- Des modules SE qui ajustent automatiquement l'importance des canaux, en mettant l'accent sur les informations les plus pertinentes pour repérer les attaques ;
- Des techniques de normalisation et des fonctions d'activation pour améliorer la rapidité et la performance de l'apprentissage [46] ;
- Des blocs de MaxPooling pour réduire la taille des données tout en gardant l'essentiel [46].
- Des couches entièrement connectées assurent la classification entre un visage réel et une tentative de falsification.

2.5.5 Présentation d l'organigramme de détection de vivacité

Le schéma proposé décrit une architecture hybride pour la détection de vivacité, combinant deux modèles complémentaires : MiniFASNetV1SE et CDCN++. Lorsqu'un visage utilisateur potentiel est capturé, il est simultanément traité par les deux réseaux.

Du côté de MiniFASNet, l'image subit d'abord un prétraitement comprenant une normalisation spatiale et un ajustement radiométrique (lumière et contraste). Ensuite, une analyse texturale est effectuée pour détecter d'éventuelles irrégularités typiques des tentatives de spoofing. En l'absence de telles irrégularités, une analyse fréquentielle est appliquée pour détecter des composantes artificielles. Si aucune anomalie n'est relevée, le processus entre dans un module d'analyse faciale SE : chaque canal est compressé (squeeze) pour calculer une moyenne globale par canal RGB, puis excité (excitation) via une transformation non linéaire permettant d'adapter dynamiquement les poids des canaux RGB selon leur importance dans la reconnaissance des caractéristiques faciales. Ces poids recalibrés sont ensuite utilisés dans une classification binaire (via Softmax) basée sur l'estimation d'une probabilité de vivacité, notée par P1.

De son côté, le modèle CDCN++ applique un prétraitement différent de normalisation spatiale et de conversion de couleur (RGB vers niveaux de gris), suivi par l'extraction des caractéristiques locales à l'aide de convolutions différentielles centrales. Une analyse fréquentielle spatiale est ensuite menée pour détecter des composantes artificielles.

Si aucune anomalie n'est détectée, une régression de profondeur et une normalisation sont effectuées afin de générer une carte de profondeur. Si cette carte contient des incohérences, le visage est déclaré fake et rejeté. Dans le cas contraire, une classification binaire est conduite, fournissant une deuxième estimation de la probabilité de vivacité, notée P2.

Finalement, les deux scores partiels (P1 et P2) sont fusionnés par une moyenne pondérée, donnant un score final P . Si ce score dépasse un seuil de tolérance défini expérimentalement, le visage est reconnu comme réel ; sinon, il est considéré comme fake, issu d'une tentative d'usurpation.

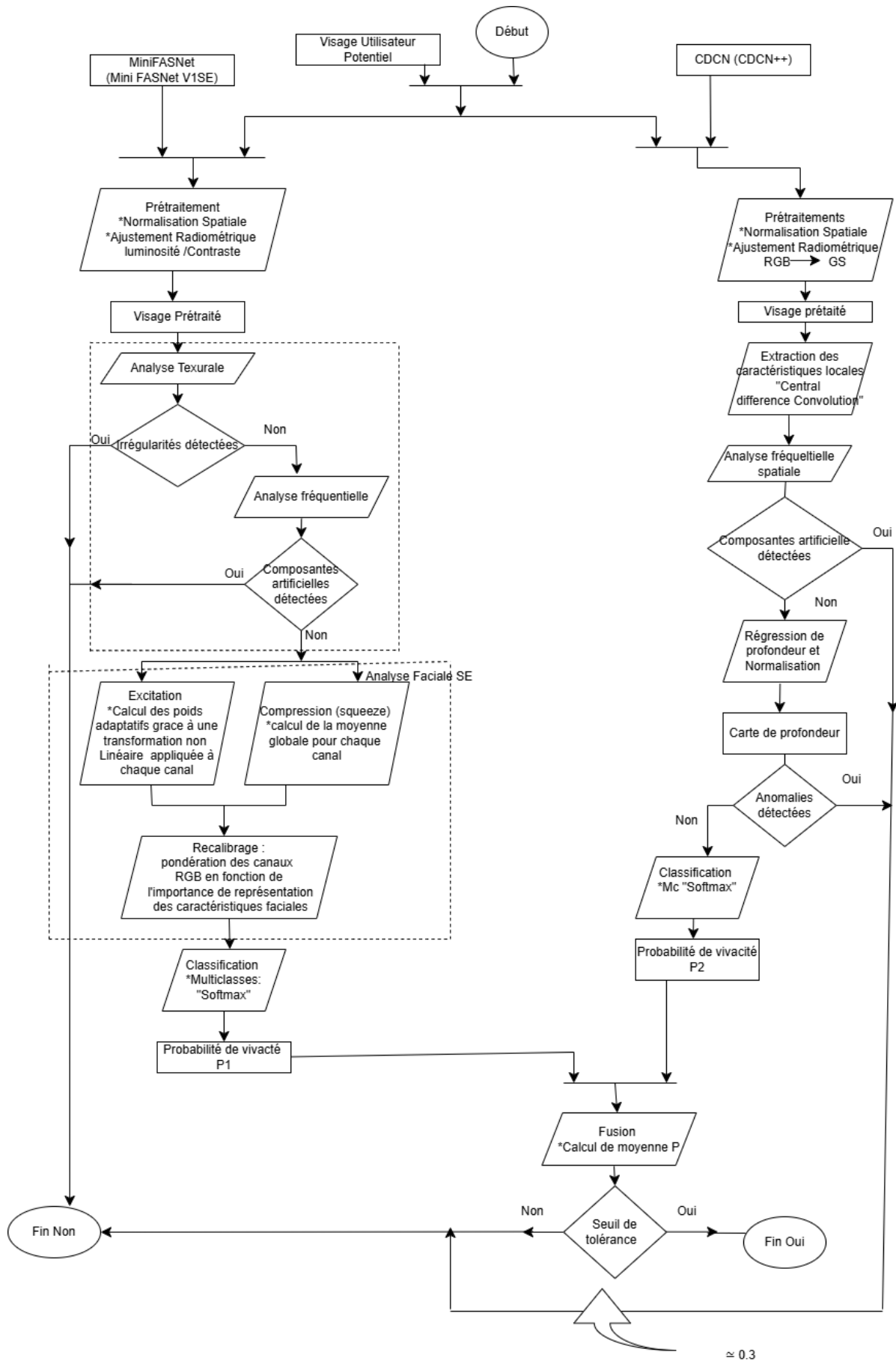


Figure 2.6 : Principe de la détection de vivacité considérée

2.6 Procédure de vérification faciale

Cette section présente les méthodes utilisées pour comparer la vérification faciale. Deux modèles sont utilisés : ArcFace et FaceNet512.

2.6.1 Présentation de la méthode ArcFace

ArcFace [48] est une méthode de reconnaissance faciale. Elle repose sur une fonction de perte appelée *Additive Angular Margin Loss* (AAML), qui vise à maximiser la séparabilité entre les classes en ajoutant une marge angulaire additive entre les caractéristiques des différentes identités. Cette approche permet d'obtenir des représentations faciales plus discriminantes, améliorant ainsi la performance globale du système de reconnaissance [48].

2.6.2 Architecture globale d'ArcFace

Après les couches convolutionnelles, une séquence composée de BN-Dropout-FC-BN est utilisée :

- **Batch Normalization (BN)** : Normalise les sorties pour accélérer l'apprentissage et le stabiliser [47].
- **Dropout** : Désactive aléatoirement certaines connexions pour éviter le surapprentissage [47].
- **Fully Connected (FC)** : Transforme les caractéristiques en un vecteur d'embedding de 512 dimension, qui représente l'identité de la personne dans un espace mathématique [48].
- **Batch Normalization finale** : Pour encore mieux stabiliser les vecteurs d'embedding.

Pour renforcer la discrimination entre les classes, ArcFace introduit une normalisation L2 des vecteurs d'embedding et des poids de la dernière couche FC, projetant ainsi tous les vecteurs sur une hypersphère de rayon. Cette projection permet de comparer les vecteurs uniquement en fonction de l'angle entre eux, facilitant l'application de la fonction de perte angulaire [48].

2.6.3 Principe de fonctionnement

La fonction de perte AAML, au cœur du modèle ArcFace, introduit une innovation majeure dans la reconnaissance faciale en imposant une contrainte géométrique stricte sur les représentations des visages. Contrairement à la fonction softmax traditionnelle, qui ne garantit pas une séparation optimale entre les classes, cette approche projette les vecteurs d'embedding sur une hypersphère normalisée, où la similarité entre les visages est mesurée uniquement par l'angle entre les vecteurs [48], la figure suivante en donne une représentation visuelle.

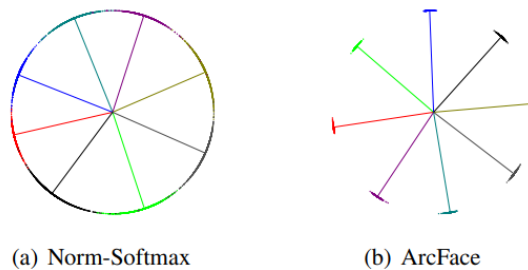


Figure 2.7 : Comparaison de la Distribution des Caractéristiques 2D sous Norm-Softmax et ArcFace[48]

Concrètement, pour chaque échantillon d'entraînement, le modèle ArcFace calcule l'angle θ entre le vecteur d'embedding normalisé de l'image et le vecteur de poids normalisé associé à la classe cible. Une marge angulaire additive

m est ensuite ajoutée à cet angle, ce qui revient à augmenter la distance géodésique entre les centres des classes sur la surface d'une hypersphère unitaire. Cette modification de la fonction de perte se traduit par une pénalisation plus forte des erreurs de classification, renforçant ainsi la compacité intra-classe (les échantillons d'une même identité sont rapprochés) et la séparation inter-classe (les identités différentes sont mieux distinguées). Ce mécanisme permet au modèle de produire des représentations faciales plus discriminantes, améliorant considérablement la fiabilité du système de reconnaissance[48].

Mathématiquement, cette approche peut être formulée comme suit [48] :

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N \log \left(\frac{e^{s \cdot \cos(\theta_{y_i} + m)}}{e^{s \cdot \cos(\theta_{y_i} + m)} + \sum_{j \neq y_i} e^{s \cdot \cos(\theta_j)}} \right)$$

où :

- N est le nombre d'échantillons dans le lot d'entraînement,
- θ_{y_i} est l'angle entre le vecteur d'embedding et le poids de la véritable classe,
- m est la marge angulaire additionnelle (généralement 0,5),
- s est le facteur d'échelle (généralement 64),
- θ_j est l'angle entre le vecteur d'embedding de l'échantillon i et le poids de la classe j.

2.6.4 Présentation du modèle FaceNet512

FaceNet512 [50] est un modèle de reconnaissance faciale avancé, conçu pour générer des embeddings de visages de 512 dimensions [49], offrant ainsi une représentation plus riche et plus discriminante des caractéristiques faciales. Cette augmentation de la dimensionnalité permet une meilleure différenciation entre les individus, ce qui est particulièrement utile dans des applications nécessitant une précision élevée, comme la vérification d'identité et la détection de fraudes.

2.6.5 Architecture globale de FaceNet512

FaceNet repose sur une architecture de réseau de neurones convolutifs conçue pour apprendre directement une représentation vectorielle d'un visage, sans passer par une étape de classification traditionnelle. L'objectif principal du réseau est de projeter chaque visage dans un espace euclidien où la distance entre deux vecteurs reflète leur similarité d'identité : deux visages d'une même personne seront proches, tandis que ceux de personnes différentes seront éloignés[50].



Figure 2.8 : La structure du modèle FaceNet512[50]

La particularité de FaceNet réside dans sa fonction de perte triplet loss comme le montre la figure ci-dessus, qui s'appuie sur un apprentissage considérant des triplets d'images : l'ancre, la positive et la négative. Cette perte force l'embedding de l'image ancre à être plus proche de celui d'une image positive (même identité) que de celui d'une image négative (identité différente), avec une marge définie. La figure 2.10 met en évidence ce mécanisme[50].

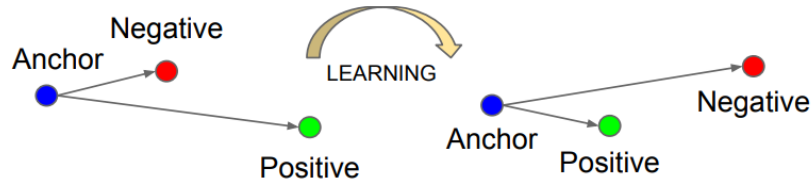


Figure 2.9 : Triplet Loss : apprentissage par similarité et dissimilarité[50].

2.6.6 Présentation de l'organigramme d'extraction des caractéristiques

Ce flowchart montre le processus d'extraction des caractéristiques à partir d'une image faciale. L'objectif est de générer un vecteur de caractéristiques en combinant deux outils afin d'obtenir une représentation plus robuste et discriminante du visage.

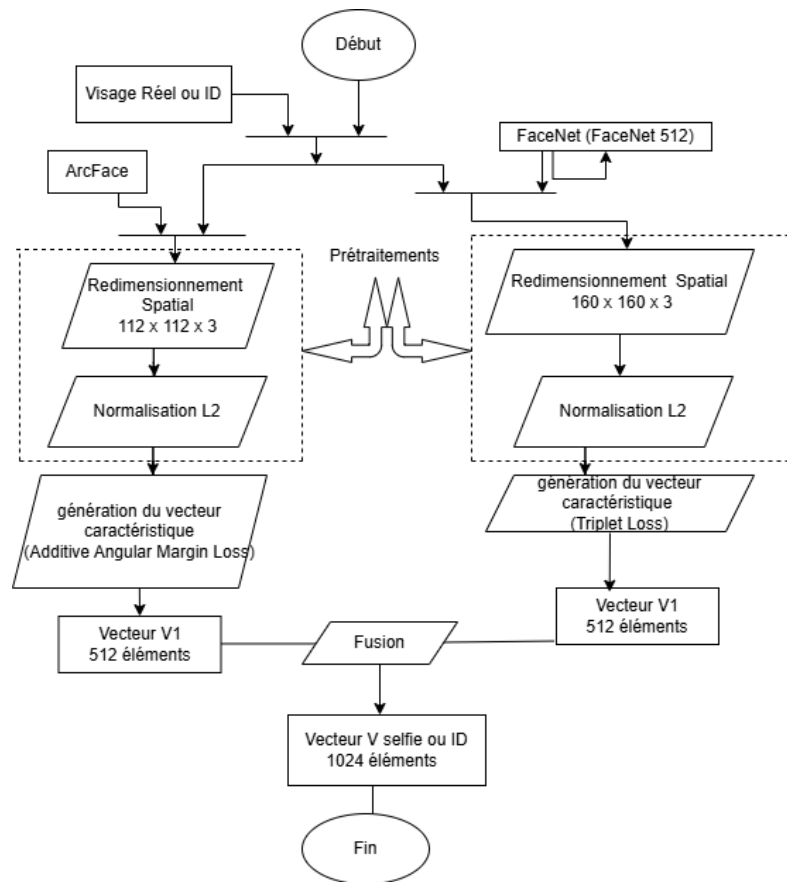


Figure 2.10 : Principe de l'extraction des caractéristiques considérée

Le processus d'extraction des caractéristiques commence par la saisie de visages réel et extrait de l'ID, qui est ensuite traité par deux pipelines parallèles : l'un utilisant le modèle ArcFace, l'autre FaceNet.

Dans les deux cas, une étape de prétraitement est appliquée, cela comprend un redimensionnement spatial de l'image ($112 \times 112 \times 3$ pour ArcFace, $160 \times 160 \times 3$ pour FaceNet) suivi d'une normalisation L2 des pixels.

Chaque pipeline génère un vecteur de caractéristiques facial d'une dimension de 512 éléments, mais suivant des approches bien distinctes tel qu'il a été précédemment décrit : ArcFace utilise une fonction AAML, tandis que FaceNet emploie la Triplet Loss. Les deux vecteurs obtenus sont ensuite fusionnés pour produire un vecteur final d'une dimension estimée à 1024 éléments, représentant de façon enrichie le visage traité. Ce vecteur combiné peut alors être utilisé pour des tâches de comparaison, d'identification en vue de la vérification biométrique.

2.6.7 Présentation de l'organigramme de la vérification faciale

Le schéma suivant représente le processus de vérification faciale intégré à notre solution. Il consiste à comparer le visage réel de l'utilisateur avec le visage extrait à partir de la photo présente sur une pièce d'identité numérisée.

Le processus commence par l'acquisition de deux images faciales : le visage réel de l'utilisateur et le visage de l'ID.

Pour chacune de ces images, un algorithme de reconnaissance faciale extrait un vecteur de caractéristiques représentant numériquement les traits du visage. Ces deux vecteurs sont ensuite comparés à l'aide d'une mesure de similarité, la distance cosinus, afin de produire un score de similarité noté S .

Ce score est ensuite comparé à un seuil de tolérance prédéfini. Si le score dépasse ce seuil, les deux visages sont considérés comme appartenant à la même personne et la vérification est validée ; dans le cas contraire, l'identification présumée est rejetée.

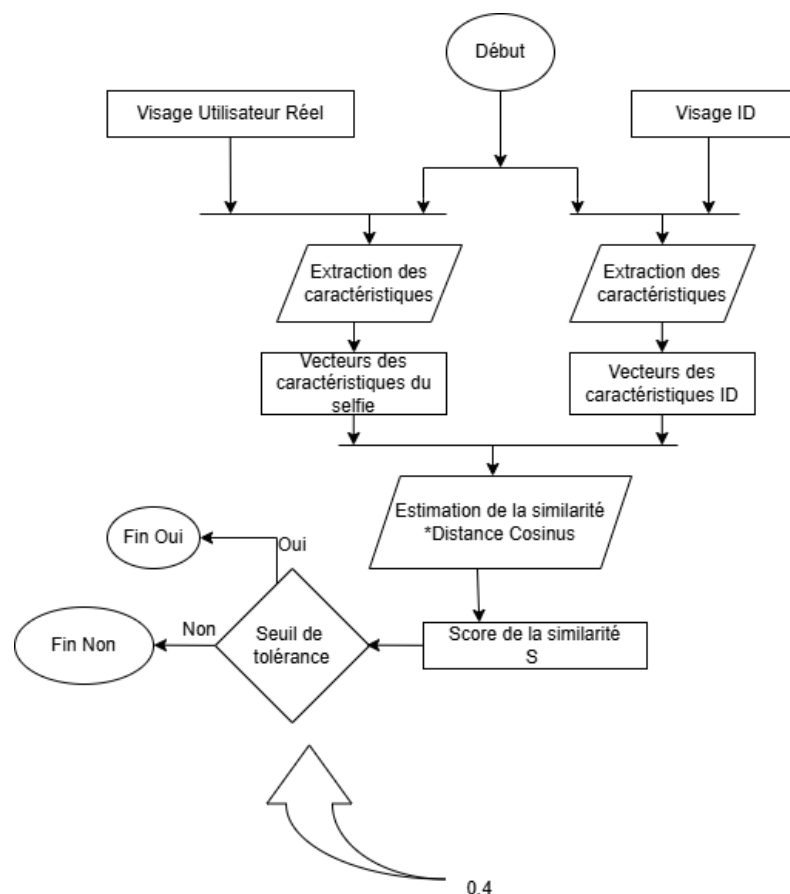


Figure 2.11 : Principe de la vérification faciale considérée

2.7 Interface homme-machine en mode développeur

L'ensemble du système de vérification biométrique a été encapsulé dans une API Web RESTful développée à l'aide du framework FastAPI. Cette API offre une architecture claire, extensible et facilement intégrable dans des systèmes tiers.

2.7.1 Point d'entrée principal : /verify

Ce point d'entrée permet de soumettre une paire d'images – une photo d'identité et un selfie – afin de lancer toute la chaîne de traitement biométrique, incluant la détection de visage, la validation de vivacité, et la comparaison faciale.

- **Méthode HTTP** : POST
- **URL** : /verify

2.7.2 Données d'entrée

L'API attend deux fichiers image (format JPEG ou PNG) envoyés dans le corps de la requête :

- **id_image** : photo extraite de la pièce d'identité.
- **selfie** : photo en temps réel prise par l'utilisateur.

2.7.3 Réponse : format JSON

La réponse renvoyée par l'API contient plusieurs éléments d'analyse et de diagnostic :

- **similarity** : score de similarité (souvent entre 0 et 1) entre les visages extraits des deux images.
- **same_person** : booléen indiquant s'il s'agit de la même personne (true ou false).
- **liveness_score** : score global de vivacité, combinant les résultats des tests effectués pour vérifier que le visage du selfie est bien associé à un vivant (et non à une image falsifiée).
- **visual_outputs** : liste d'images générées illustrant les étapes clés du traitement (par exemple : visages détectés, redimensionnés, cartes de chaleur, etc.), utiles pour le débogage ou l'explication du processus. Une vue d'ensemble est donnée dans la figure suivante. Plus de détails sera fournis dans le chapitre N°3.

2.8 Conclusion

Ce chapitre a permis de traduire les concepts théoriques en une solution concrète, intégrant des modules avancés de détection de visage, de vivacité, et de vérification faciale. L'architecture modulaire et les choix technologiques ont été guidés par les exigences de précision, de rapidité et de robustesse face aux tentatives de fraude. Grâce à une démarche méthodique, chaque étape du processus d'authentification a été pensée pour améliorer la fiabilité et la sécurité, tout en assurant une expérience utilisateur fluide. Les performances de ces modules seront analysées en détail dans le chapitre suivant.

Chapitre 3

Résultats expérimentaux, analyse critique et voies
d'amélioration

Introduction

Ce chapitre présente l'évaluation expérimentale du système de vérification biométrique développé. L'objectif principal est de tester la solution afin de vérifier sa fiabilité et sa capacité à distinguer les utilisateurs légitimes des tentatives d'usurpation.

Pour cela, nous avons utilisé deux types de données : des images de cas réels et d'autres issues des cas d'attaques. Différents indicateurs de performance ont été analysés, tels que les scores de vivacité, les scores de similarité et les taux d'erreur.

Les résultats obtenus sont visualisés à l'aide de graphiques, comparés aux seuils de décision, puis interprétés afin d'identifier les points forts du système, ses limites actuelles et les pistes d'amélioration envisageables.

3.1 Approche d'évaluation expérimentale

Afin d'analyser les performances du système développé, une démarche d'évaluation a été mise en place. Celle-ci repose sur une méthodologie définie et sur l'utilisation de critères quantitatifs permettant de mesurer le comportement du système dans différents contextes d'usage.

3.1.1 Méthodologie d'évaluation

Les modèles ont été initialement entraînés sur des bases publiques (**CASIA-WebFace**, **Replay-Attack** et **OULU-NPU**), sont testés indépendamment, préparées pour simuler des conditions d'usage réelles et des scénarios d'attaque.

Les données issues de la combinaison des deux sources sont organisés en **165 dossiers**, chacun correspondant à un individu :

- **110 dossiers** contiennent des images réelles :
 - Une à deux photos d'identité (fichiers nommés ID_1, ID_2);
 - Plusieurs selfies (jusqu'à 13), capturés dans des conditions d'éclairage et des contextes variés.
- **55 dossiers** sont dédiés à des tentatives d'usurpation :
 - Deux images imprimées sont utilisées l'une comme ID et l'autre comme selfie.;
 - Ces dossiers simulent des attaques par présentation.

Cette structure permet d'analyser séparément le comportement du système face à des entrées authentiques et à des intrusions simulées, obtenues en créant des paires d'images à partir du jeu de données global de sorte à simuler plusieurs scénarios possibles.

Les figures 3.1 et 3.2 représente un aperçu de l'organisation des données et un extrait de la base de données représentant un même individu à l'ordre.

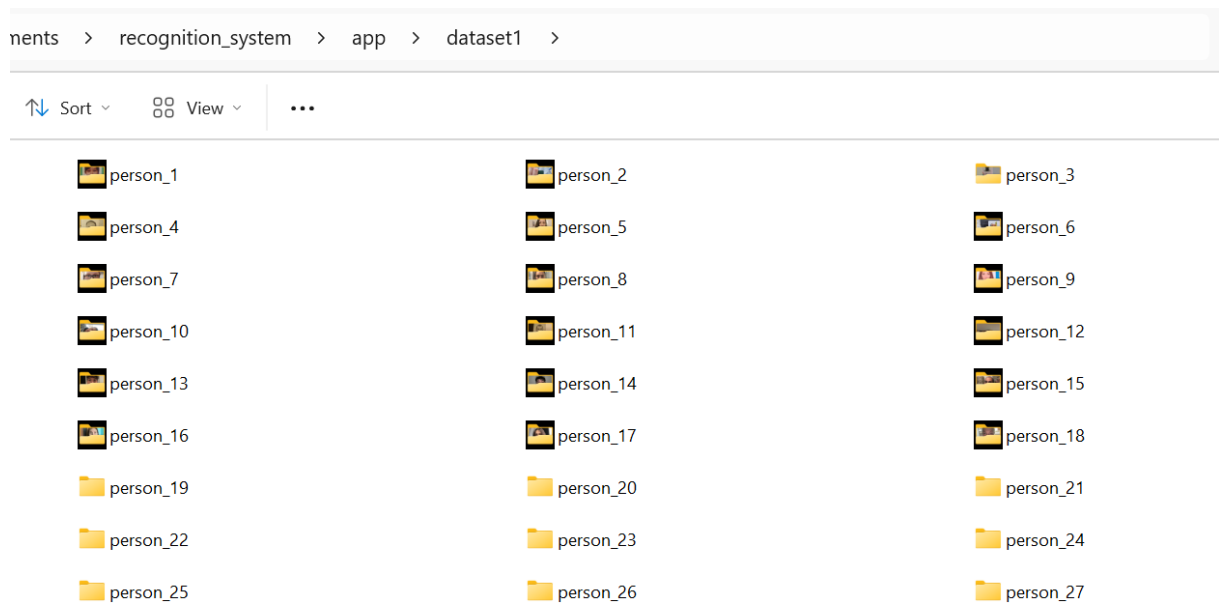


Figure 3.1 : Aperçu de l'organisation des données

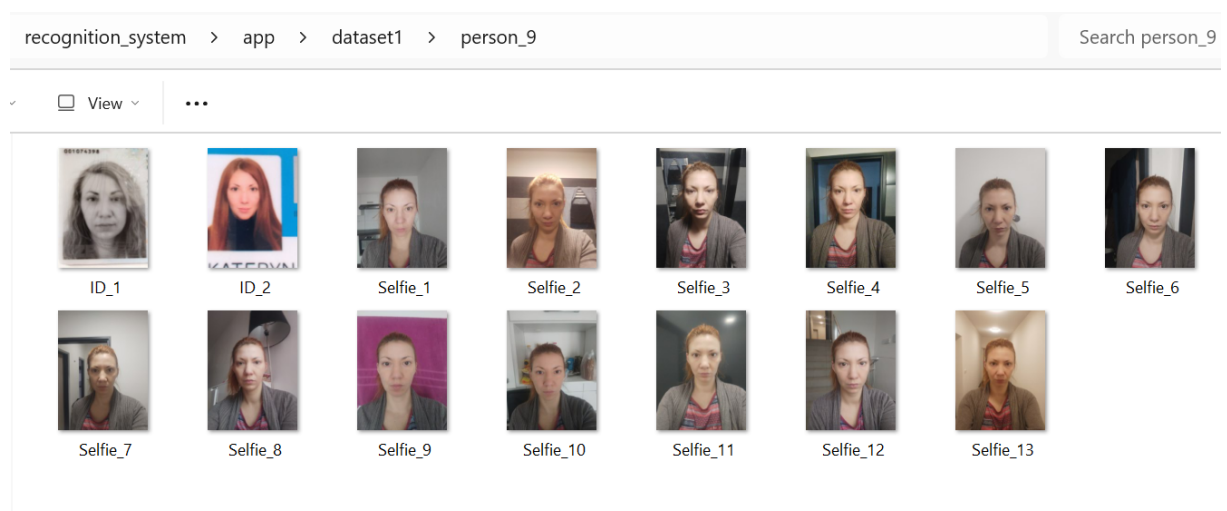


Figure 3.2 : Extrait de la base de données représentant un même individu.

3.1.2 Critères d'évaluation utilisés

Avant d'analyser les performances, il est important de préciser les ****règles de décision**** appliquées pour valider une image comme authentique (selfie réel) ou comme attaque (faux selfie). Une image est considérée comme « vivante » si elle satisfait à l'une des deux conditions suivantes :

- Le score moyen pondéré, noté `avg_score`, calculé à partir des résultats des modèles MiniFASNet (40%) et CDCN++ (60%), est supérieur ou égal à 0,30 ;
- `mini_score` $\geq$ 0,3 **ou** `cdcn_score` $\geq$ 0,4.

Ces règles de décision permettent d'équilibrer rigueur et souplesse dans la validation biométrique.

Les indicateurs de performance utilisés pour évaluer la fiabilité globale du système sont les suivants :

- **Score de similarité** : mesure la correspondance entre l'image d'identité et le selfie, basée sur les embeddings extraits par les modèles ArcFace et FaceNet. Le seuil de similarité appliqué est fixé à 0,40.

- **Taux de faux positifs (FAR)** : pourcentage de cas où une attaque est incorrectement acceptée comme étant une image authentique ;
- **Taux de faux négatifs (FRR)** : pourcentage de cas où une image authentique est rejetée à tort ;
- **Score ACER (Average Classification Error Rate)** : moyenne des taux de FAR et FRR. Cet indicateur permet d’avoir une vue globale sur la robustesse du système face aux erreurs de classification.

Ces métriques offrent une base fiable pour interpréter les résultats expérimentaux présentés dans les sections suivantes, et permettent de juger si la solution proposée répond aux exigences de sécurité tout en assurant une bonne expérience utilisateur.

3.2 Environnement de test

Les tests expérimentaux de la solution biométrique ont été réalisés dans un environnement local, sur une machine de développement standard, afin de simuler des conditions proches d’un déploiement réel.

3.2.1 Configuration matérielle

- **Processeur** : Intel Core i7
- **Mémoire vive** : 16 Go RAM
- **Carte graphique** : non utilisée (traitement effectué sur CPU)
- **Système d’exploitation** : Windows 11 (64 bits)

Cette configuration permet d’évaluer le fonctionnement du système sans dépendre d’une accélération GPU, en mettant l’accent sur la portabilité et la performance sur des machines courantes.

3.2.2 Configuration logicielle

- **Environnement Python** : Virtual environment (venv)
- **Langage** : Python 3.x
- **Frameworks et bibliothèques** :
 - **FastAPI** : pour exposer l’API de vérification biométrique
 - **PyTorch** : pour le modèle CDCN++ de détection de vivacité
 - **TensorFlow** : utilisé via certaines dépendances DeepFace
 - **OpenCV** : pour le traitement des images (lecture, redimensionnement, conversion)
 - **DeepFace** : pour l’extraction d’embeddings faciaux à partir de modèles *ArcFace* et *Facenet512*

3.2.3 Durée moyenne de traitement

Le temps de traitement complet d’une vérification est généralement inférieur à **1 seconde**, ce qui comprend :

- La détection du visage avec *RetinaFace* ;
- L’évaluation de la vivacité (*MiniFASNETVISE* + *CDCN++*) ;
- La comparaison d’embeddings (*ArcFace* + *Facenet512*).

Les tests ont été exécutés via des scripts Python interactifs et appels d’API directs.

3.3 Etapes du pipeline de la vérification biométrique

Cette section illustre le fonctionnement interne du système de vérification biométrique en présentant les différentes étapes du traitement, depuis la réception des images jusqu'à la prise de décision et en prévoyant plusieurs scénarios.

3.3.1 Présentation du processus global

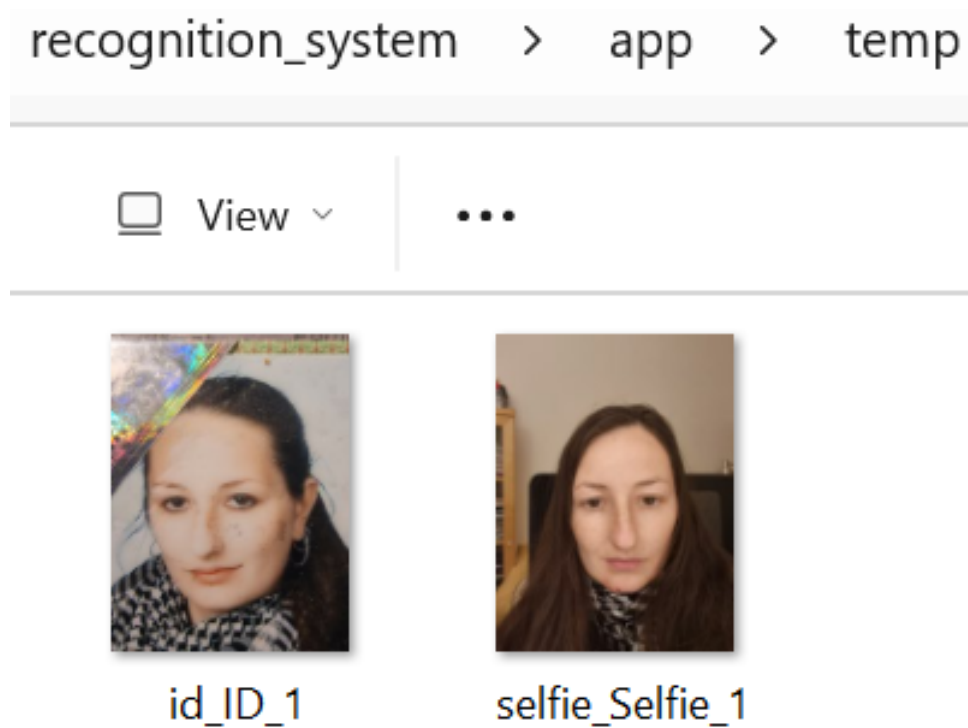


Figure 3.3 : Images d'entrée (Dossier Temp <– ID+Selfie).

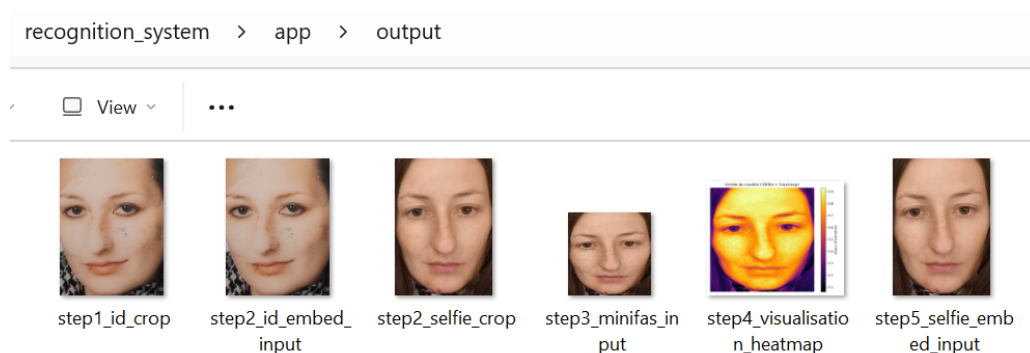


Figure 3.4 : Résultats intermédiaires du traitement (Dossier Output)

Les captures d'écran ci-dessus présentent :

- L'appel de l'API via Swagger, avec envoi d'une image ID et d'un selfie.
- Le dossier temporaire contenant les images d'entrée brutes.
- Les résultats des étapes intermédiaires : détection et recadrage des visages, images transformées pour la reconnaissance et la détection de vivacité (MiniFASNETV1SE et CDCN++), ainsi que les représentations finales utilisées pour la vérification faciale.

3.3.2 Analyse détaillée du processus global

Cette visualisation permet de percevoir l'impact de chaque composant dans la chaîne de traitement biométrique. Les figures suivantes isolent ces résultats pour une meilleure interprétation des étapes incluses dans le processus de vérification biométrique :



Figure 3.5 : Résultat de détection du visage sur l'image ID

Il s'agit du visage extrait à partir de l'image ID. Ce visage est détecté et recadré automatiquement, puis redimensionné pour alimenter les modèles d'extraction d'embeddings (ArcFace ou Facenet512). Cette représentation sera ensuite utilisée dans la comparaison biométrique avec le selfie.



Figure 3.6 : Résultat de détection du visage sur l'image Selfie

Visage extrait à partir du selfie acquis par l'utilisateur, destiné à la détection de vivacité et à l'identification.

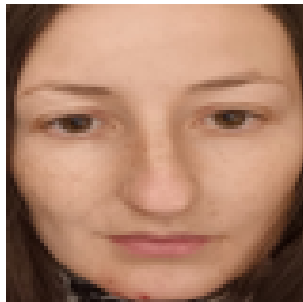


Figure 3.7 : Résultat du redimensionnement spatial exigé par MiniFASNetV1SE (80x80)

Cette image est utilisée comme entrée du modèle MiniFASNETV1SE pour une première évaluation de vivacité.

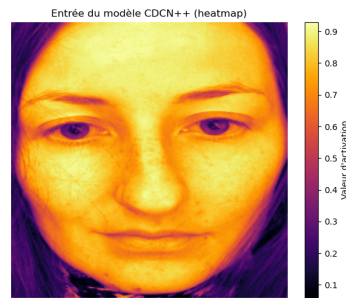


Figure 3.8 : Heatmap générée en vue de l’analyse spatio-texturale réalisée par CDCN++

Représentation visuelle des zones d’attention du modèle CDCN++, qui détecte les textures typiques d’un vrai visage.

La figure 3.9 montre un cas de vérification réussie exécutée via l’interface Swagger de l’API. Après l’envoi d’une image d’identité (ID_1.jpg) et d’un selfie (Selfie_1.jpg) :

- le système détecte un visage vivant (`is_alive = true`) avec un score de vivacité de 0,413 ;
- la similarité calculée est de 0,756, dépassant le seuil de 0,4 ;
- l’utilisateur est correctement reconnu comme étant la bonne personne (`same_person = true`).

Cet exemple illustre le bon fonctionnement de la chaîne de traitement et donne un aperçu clair de la forme que prennent les résultats retournés à travers l’API développée.

id_image * required
string(binary)

selfie * required
string(binary)

Execute **Clear**

Responses

Curl

```
curl -X 'POST' \
  'http://localhost:8000/verify' \
  -H 'accept: application/json' \
  -H 'Content-Type: multipart/form-data' \
  -F 'id_image=@ID_1.jpg;type=Image/jpeg' \
  -F 'selfie=@Selfie_1.jpg;type=Image/jpeg'
```

Request URL

`http://localhost:8000/verify`

Server response

Code **Details**

200

Response body

```
{
  "similarity": 0.756,
  "same_person": true,
  "threshold": 0.4,
  "liveness_score": 0.413,
  "is_alive": true
}
```

Download

Figure 3.9 : Exemple d’exécution via l’API développée pour la vérification biométrique

3.3.3 Détection de visage avec nécessité d’alignement

Afin de mieux comprendre le rôle du module RetinaFace et l’étape d’alignement des visages, nous présentons ci-dessous une séquence illustrant le processus de détection faciale, le calcul de l’angle entre les yeux, et l’alignement géométrique du visage avant l’extraction des caractéristiques.

Les captures suivantes montrent :

- les fichiers générés automatiquement (image originale et image alignée),

- les messages du terminal indiquant l'angle détecté par RetinaFace,
- et l'appel de l'API avec le résultat de la vérification.

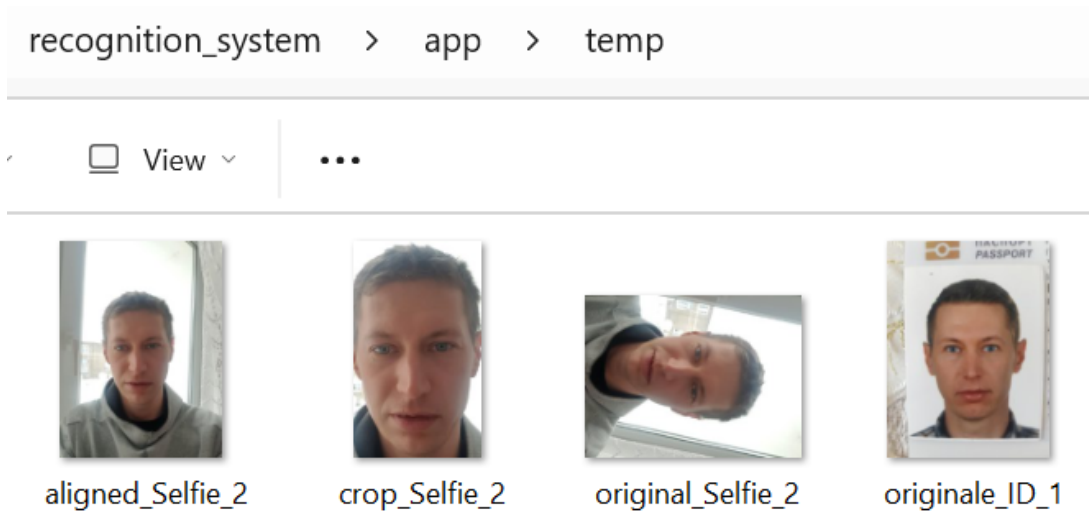


Figure 3.10 : Images avant et après la détection du visage avec alignement des yeux (`crop_...`).

La figure 3.10 montre, de gauche à droite :

- **aligned_Selfie_2** : Selfie après détection du visage et alignement géométrique basé sur les yeux.
- **crop_Selfie_2** : Visage détecté et automatiquement rogné sans correction de l'orientation.
- **original_Selfie_2** : Selfie d'origine tel que soumis à l'entrée du système.
- **originale_ID_1** : Photo d'identité issue d'un document officiel (passeport).

Comme illustré dans la figure 3.11, l'angle entre les yeux détecté par RetinaFace est utilisé pour corriger l'orientation du visage avant traitement. Ensuite, la figure 3.12 montre l'appel de l'API `/verify` avec les images prétraitées, retournant les scores de vivacité et de similarité.

```
INFO: __main__: [Alignement] Angle entre les yeux : -95.15°
INFO: __main__: [Alignement] Rotation appliquée pour redresser le visage.
INFO: __main__: [Alignement] Visage final sauvegardé : C:\Users\surf\Documents\recognition_system\app\temp\crop_Selfie_222.jpg
INFO: 127.0.0.1:55101 - "POST /verify HTTP/1.1" 200 OK
```

Figure 3.11 : Cas de détection d'une déviation (-95.15°) dans la position des yeux nécessitant un alignement automatique.

id_image * required
string(\$binary) ID_1.jpg

selfie * required
string(\$binary) Selfie_222.jpg

Responses

Curl

```
curl -X 'POST' \
  'http://localhost:8000/verify' \
  -H 'accept: application/json' \
  -H 'content-type: multipart/form-data' \
  -F 'id_image=@ID_1.jpg;type=image/jpeg' \
  -F 'selfie=@Selfie_222.jpg;type=image/jpeg'
```

Request URL

http://localhost:8000/verify

Server response

Code	Details
200	Response body <pre>{ "similarity": 0.744, "same_person": true, "threshold": 0.4, "liveness_score": 0.3798, "is_alive": true }</pre> Response headers <pre>content-length: 95 content-type: application/json date: Thu, 12 Jun 2025 22:05:19 GMT server: uvicorn</pre>

Figure 3.12 : Résultat de l'appel de l'API /verify après prétraitement : le système a appliqué la détection et l'alignement, et retourne les scores de vivacité et de similarité.

3.3.4 Cas de détection d'une attaque par présentation

Ce qui suit montre un exemple concret où le système bloque une tentative de vérification, car l'image soumise ne correspond pas à un visage réel. Il s'agit d'un selfie imprimé (donc non réel), détecté automatiquement par le filtre de vivacité.

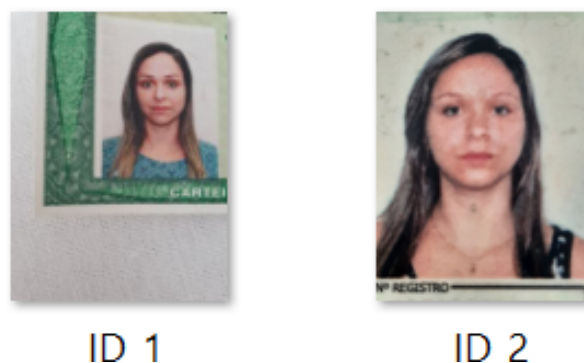


Figure 3.13 : Images utilisées dans la tentative d'usurpation d'identité par présentation d'un faux selfie (image scannée)

La figure 3.14 illustre une tentative d'authentification qui a échoué dès l'étape de détection de vivacité. Bien que deux images représentant la même personne aient été soumises (ID_1.jpg et ID_2.jpg), le selfie est jugé "non authentique", avec un score de 0,252, inférieur au seuil de tolérance défini..

— L'API retourne une erreur HTTP 400 avec le message "Visage non vivant détecté".

— Aucun calcul de similarité n'est effectué, car le processus est bloqué dès cette étape.
Ce cas démontre le rôle essentiel du filtre de vivacité pour protéger l'accès au module de reconnaissance faciale.

id_image * required
string(\$binary) ID_1.jpg

selfie * required
string(\$binary) ID_2.jpg

Responses

Curl

```
curl -X 'POST' \
  'http://localhost:8000/verify' \
  -H 'accept: application/json' \
  -H 'Content-Type: multipart/form-data' \
  -F 'id_image=@ID_1.jpg;type=image/jpeg' \
  -F 'selfie=@ID_2.jpg;type=image/jpeg'
```

Request URL

http://localhost:8000/verify

Server response

Code	Details
400	Error: Bad Request

Response body

```
{  
  "detail": "Visage non vivant détecté (score: 0.252)"  
}
```

Figure 3.14 : Echec d'authentification suite à la non détection de la vivacité du selfie

3.4 Analyse de la distribution des différents scores calculés

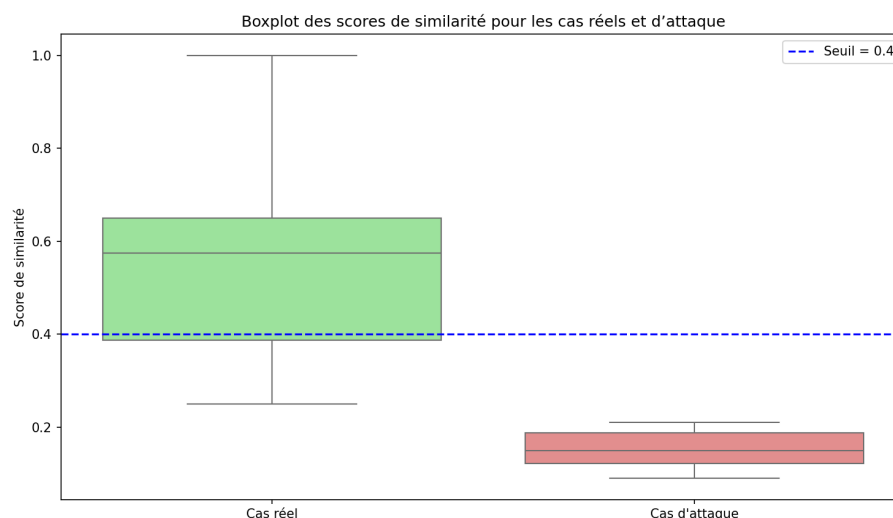
Cette section présente les résultats obtenus à travers différents indicateurs, en commençant par l'analyse des scores de similarité.

3.4.1 Analyse des scores de similarité – Cas réels et attaques

Afin d'évaluer la capacité du système à distinguer les visages authentiques des imposteurs, nous avons analysé la distribution des scores de similarité entre les images d'identité et les selfies. une représentation visuelle a été utilisée : boxplot comparatif.

La figure 3.15 montre une séparation relativement nette :

- **Cas réels** : médiane à 0,57, intervalle interquartile [0,40 ; 0,67]
- **Cas d'attaque** : médiane à 0,15, intervalle interquartile [0,08 ; 0,22]



3.4.2 Analyse des scores de vivacité – Cas réels et attaques

Afin d'évaluer la capacité du système à distinguer les visages authentiques des imposteurs, nous avons analysé la distribution des **scores de vivacité**. Deux représentations visuelles ont été utilisées : un *boxplot* comparatif et un *histogramme* superposé, mettant en évidence la séparation entre les cas réels et les attaques.

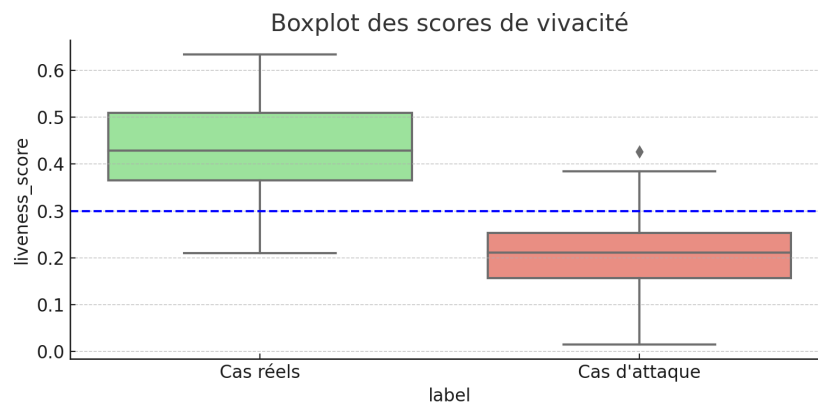


Figure 3.17 : Boxplot des scores de vivacité pour les cas réels (en vert clair) et les cas d'attaque (en rouge).

La figure montre une séparation relativement nette :

- **Cas réels** : médiane à 0,45, intervalle interquartile [0,37 ; 0,52]
- **Cas d'attaque** : médiane à 0,20, intervalle interquartile [0,15 ; 0,26]

Le seuil de 0,3 est bien positionné pour distinguer les deux groupes. Toutefois, on observe une zone de chevauchement autour de cette valeur, ce qui peut générer des cas ambigus (faux positifs ou négatifs).

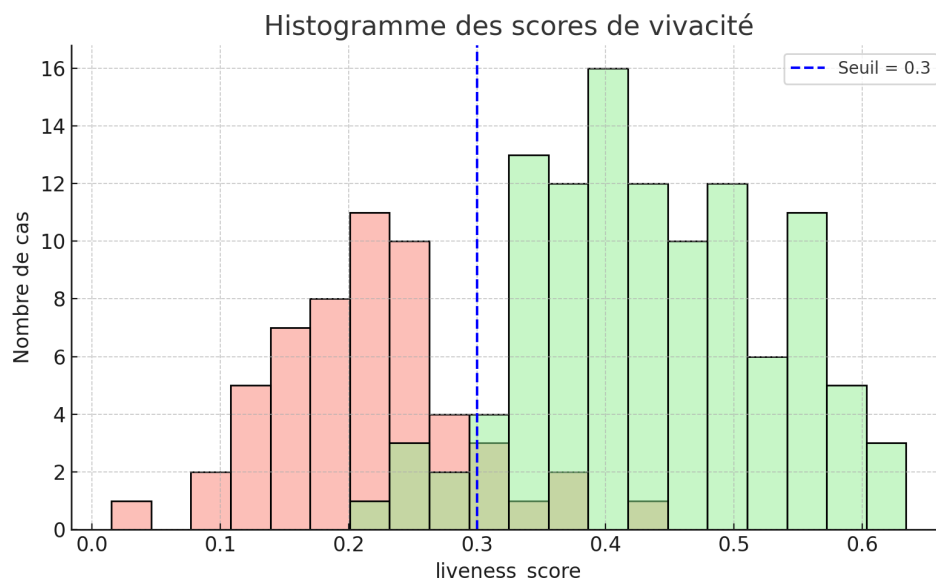


Figure 3.18 : Histogramme des scores de vivacité – Répartition des cas réels (vert clair) et des attaques (rouge).

La figure confirme cette tendance :

- Les cas réels sont majoritairement concentrés dans l'intervalle [0,35 ; 0,6], avec un pic autour de 0,45.

— Les cas d’attaque sont plus nombreux sous le seuil de 0,3, notamment entre 0,1 et 0,25. Quelques cas dépassent néanmoins le seuil.

Le tableau 3.1 présente les principales mesures statistiques (médiane, IQR, extrêmes) des scores de vivacité, permettant de comparer objectivement les distributions selon le type de cas.

Table 3.1 : Résumé statistique des scores de vivacité pour les cas réels, les attaques et le total

Catégorie	Médiane	IQR	Min – Max	Nombre total
Cas réels	0,4285	[0,365 ; 0,509]	[0,210 ; 0,634]	110
Cas d’attaque	0,2110	[0,157 ; 0,253]	[0,015 ; 0,427]	55
Total	0,3740	[0,252 ; 0,473]	[0,015 ; 0,634]	165

À partir du seuil de décision fixé à 0,3, le tableau 3.2 illustre les performances du système de détection de vivacité en termes de taux d’erreurs.

Table 3.2 : Taux d’erreur de classification pour les scores de vivacité (seuil = 0,3)

Type d’erreur	Nombre de cas	Taux (%)
Faux positifs	6	10,91
Faux négatifs	6	5,45
ACER	-	8,18

Ces résultats montrent que le système atteint une précision globale de 91,82%, avec un ACER de 8,18%, ce qui reflète une fiabilité satisfaisante dans la détection de vivacité. Le taux de faux positifs (10,91%) et celui de faux négatifs (5,45%) indiquent un bon équilibre dans les performances du système, capable de distinguer les visages réels des tentatives d’usurpation dans la majorité des cas testés.

3.4.3 Interprétation de la courbe ROC et évaluation globale

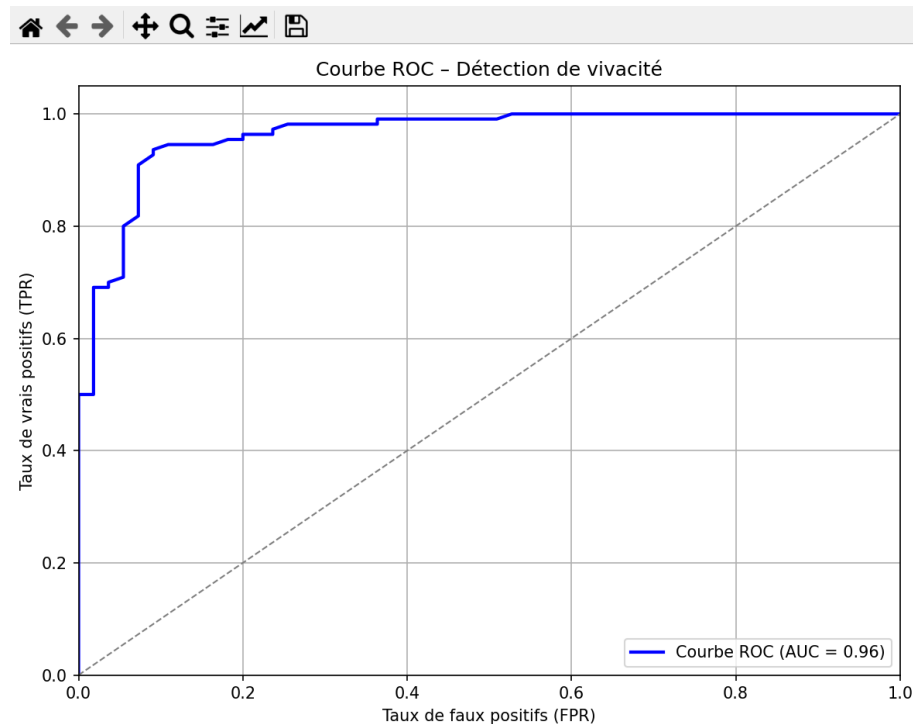


Figure 3.19 : Courbe ROC pour la détection de vivacité (AUC = 0,96)

La courbe ROC présentée ci-dessus permet d'évaluer la capacité du module de vivacité à distinguer efficacement les visages réels des tentatives d'usurpation.

On observe que la courbe s'approche fortement du coin supérieur gauche du graphique, ce qui témoigne d'une bonne performance globale. La valeur de l'AUC est de **0,96**, ce qui indique une capacité discriminante très élevée.

Plus précisément :

- Un TPR élevé est maintenu même pour de faibles FPR, traduisant une capacité à reconnaître correctement les visages réels tout en limitant les erreurs d'acceptation.
- L'éloignement net par rapport à la diagonale (aléatoire) confirme que le modèle apprend bien à distinguer les deux classes.

Ces résultats confirment la stabilité et la fiabilité du module de vivacité dans des conditions de test variées. Ils viennent compléter les analyses précédentes basées sur les distributions et les scores statistiques.

3.4.4 Analyse critique

- Le système biométrique montre des performances robustes pour distinguer les visages vivants des tentatives d'usurpation.
- Les scores de vivacité des attaques sont majoritairement **inférieurs à 0,3**, tandis que ceux des utilisateurs légitimes sont largement **supérieurs à 0,3**, avec une médiane autour de **0,5**.
- Le critère de vivacité basé sur des images statiques s'est révélé **discriminant**, grâce à :
 - une bonne qualité des données ;
 - un calibrage affiné des modèles ;
 - un nettoyage rigoureux des jeux de données.

- Les boxplots et histogrammes montrent une **séparation claire** entre réels et attaques, avec une faible zone tampon autour du seuil.
- Le modèle MiniFASNet + prétraitement s’est montré **efficace** contre les attaques imprimées et numériques.
- Quelques **erreurs de classification** subsistent près du seuil, souvent dues à des visages flous, mal cadrés ou sombres.
- Pour la **similarité faciale**, les scores séparent bien réels et imposteurs ; la combinaison ArcFace + FaceNet renforce la fiabilité.
- **Limites identifiées** :
 - seuil fixe : possibilité d’amélioration via une stratégie adaptative ;
 - pas d’analyse dynamique (mouvements, clignements) → d’où la vulnérabilité aux attaques vidéo ou 3D.
- **En résumé** :
 - L’architecture proposée est efficace en contexte réel.
 - Les seuils utilisés (0,3 pour vivacité, 0,4 pour similarité) sont **globalement pertinents**.
 - Le taux de faux positifs reste faible, assurant un bon niveau de sécurité.

3.5 Analyse des erreurs et interprétation et des limites

L’analyse détaillée des résultats expérimentaux, appuyée par les courbes de distribution cumulée, révèle une performance globalement satisfaisante du système biométrique. Toutefois, certaines erreurs subsistent, en particulier autour des seuils de décision.

3.5.1 Faux négatifs (utilisateurs légitimes rejetés)

Parmi les **110 cas réels**, **6 utilisateurs ont été rejetés à tort**, soit un taux de faux négatifs de **5,45 %**. Ces erreurs sont principalement liées à des conditions de capture non optimales, comme le montrent les distributions des scores de vivacité et de similarité.

Une analyse fine de l’ensemble des cas réels permet de dégager les causes récurrentes suivantes, comme illustré en figure 3.20 :

- **Faible similarité (< 0,4)** : **18,18 %** des images réelles présentent une similarité insuffisante, généralement causée par du flou, un mauvais éclairage ou un cadrage défaillant.
- **Mauvais cadrage probable (similarité < 0,3)** : **11,82 %** des cas relèvent d’un défaut d’alignement ou d’un visage partiellement hors champ.
- **Vivacité borderline (entre 0,28 et 0,32)** : **1,82 %** des cas se situent dans une zone d’incertitude autour du seuil de vivacité.
- **Vivacité insuffisante (< 0,3)** : dans **5,45 %** des cas, la vivacité est si faible que le système rejette directement l’entrée sans effectuer la reconnaissance.

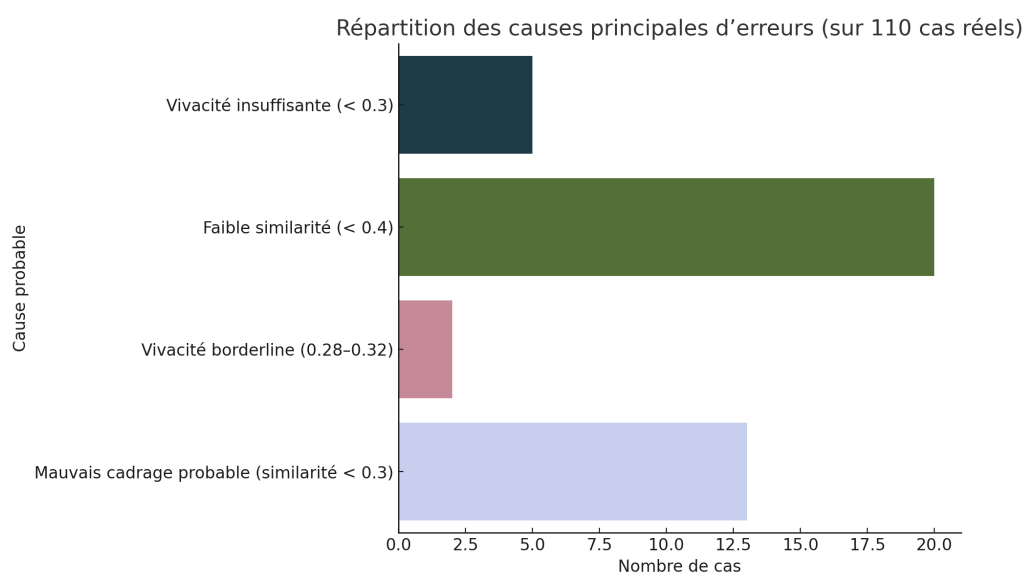


Figure 3.20 : Répartition des causes principales d'erreurs dans les cas réels

Le graphique met en évidence les erreurs liées à la qualité de capture (similarité ou vivacité insuffisante), représentant les principaux motifs de rejet des utilisateurs légitimes.

Ces résultats mettent en évidence l'influence critique de la qualité des images sur les performances du système. Un prétraitement rigoureux (alignement, filtrage des images floues ou mal exposées) reste essentiel pour en améliorer la fiabilité.

3.5.2 Faux positifs (attaques acceptées)

Le taux de faux positifs s'élève à **18,6 %**, ce qui indique que certaines attaques ont réussi à contourner le système. Ces erreurs concernent principalement des images d'attaque bien éclairées et en haute résolution.

Les causes identifiées incluent :

- **Vivacité anormalement élevée** : certaines images d'attaque obtiennent un score supérieur au seuil fixé, les faisant passer pour authentiques.
- **Faible similarité mais vivacité suffisante** : l'image est reconnue comme vivante, mais ne correspond pas à l'identité cible.
- **Absence de dynamique** : le traitement étant basé sur des images statiques, le système est plus vulnérable aux attaques visuellement convaincantes.

3.5.3 Limites du système

Malgré les performances globalement satisfaisantes, certaines limites structurelles méritent encore d'être soulignées :

- **Dépendance à la qualité de capture** : des images floues ou mal éclairées peuvent affecter aussi bien la reconnaissance que la vivacité.
- **Traitement purement statique** : l'absence de vidéo ou d'interaction empêche la détection de certaines attaques dynamiques ou sophistiquées (deepfakes, masques 3D).
- **Seuils fixes et non adaptatifs** : les seuils actuels sont constants, alors qu'un ajustement dynamique basé sur la qualité ou le contexte pourrait accroître la fiabilité.

- **Accès limité aux bases de données adaptées** : le manque d'accès à des jeux de données publics ou privés suffisamment riches et pertinents, notamment pour les cas dynamiques ou spécifiques à certaines situations d'usage, a restreint les possibilités d'entraînement sur des scénarios réalistes.

En somme, les résultats obtenus témoignent de performances satisfaisantes, tout en rappelant l'intérêt de poursuivre l'optimisation, notamment via des approches dynamiques ou multimodales.

3.6 Interface Homme Machine en mode Utilisateur

3.6.1 Objectifs

L'objectif de l'interface utilisateur est de permettre aux utilisateurs de tester le système d'authentification biométrique de manière simple et intuitive. Cette interface constitue un outil de démonstration qui permet de :

- Charger une image d'identité (photo issue d'un document officiel).
- Charger un selfie (image faciale acquise en conditions réelles)
- Lancer la procédure de vérification biométrique complète (détection de visage, détection de vivacité, reconnaissance faciale).
- Afficher un journal des étapes avec des messages d'état bien détaillés.
- Indiquer clairement la décision finale (authentification réussie ou échouée).

3.6.2 Présentation de l'interface

L'interface a été réalisée à l'aide de la bibliothèque Tkinter de Python. Elle se présente sous la forme d'une fenêtre interactive avec plusieurs boutons d'action :

- **Charger Image ID** : permet d'importer une image d'identité.
- **Charger Selfie** : permet d'importer un selfie récent.
- **Lancer Vérification** : démarre l'ensemble du processus biométrique.
- **Réinitialiser** : réinitialise tous les champs et compteurs.



Figure 3.21 : Interface graphique de l'application de vérification biométrique

3.6.3 Fonctionnement de l'interface de vérification

L'interface de vérification biométrique s'appuie sur une séquence interactive en plusieurs étapes que l'utilisateur suit pour initier et compléter un processus d'authentification.

1. Chargement des images L'utilisateur commence par importer une image d'identité et un selfie récent. Cette opération est réalisée via les boutons **Charger Image ID** et **Charger Selfie**, comme illustré ci-dessous :

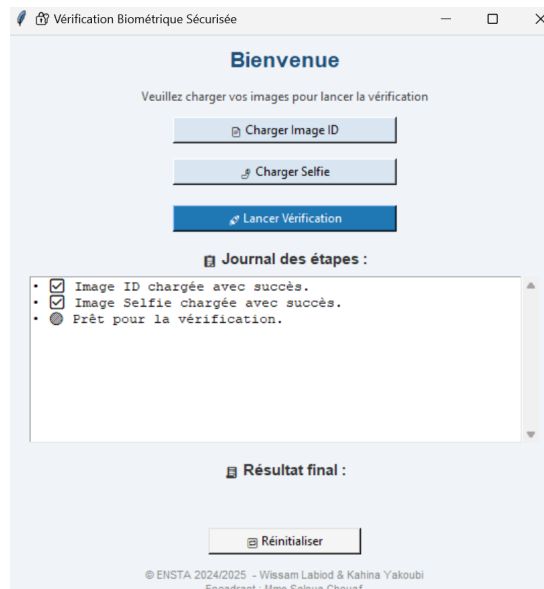


Figure 3.22 : Interface graphique après chargement réussi des deux images

2. Lancement de la vérification Une fois les images chargées, l'utilisateur clique sur **Lancer Vérification**. Cela déclenche automatiquement trois étapes de traitement successives :

1. **Détection de visage** : les deux images sont analysées pour localiser les visages.
2. **Détection de vivacité** : le selfie est analysé pour vérifier qu'il ne s'agit pas d'un artefact (photo, vidéo ou deepfake).
3. **Vérification faciale** : les visages extraits sont comparés à l'aide d'embeddings afin d'évaluer la correspondance.

Chaque étape est soumise à un nombre de tentatives limité, fixé selon un compromis entre convivialité et sécurité :

- **Image ID** : 2 tentatives sont autorisées.
- **Selfie** : jusqu'à 3 tentatives possibles (en raison des variations d'éclairage, angle, etc.).
- **Détection de vivacité** : 1 seule tentative pour éviter les attaques par répétition.
- **Vérification faciale** : une seule tentative est permise. En cas d'échec, aucune nouvelle tentative n'est autorisée.

Des messages explicites informent l'utilisateur à chaque étape du processus, que ce soit en cas de succès ou d'échec. Les figures suivantes illustrent les scénarios les plus courants rencontrés lors de l'exécution :



Figure 3.23 : Cas 1 : Authentification réussie (toutes les étapes validées)

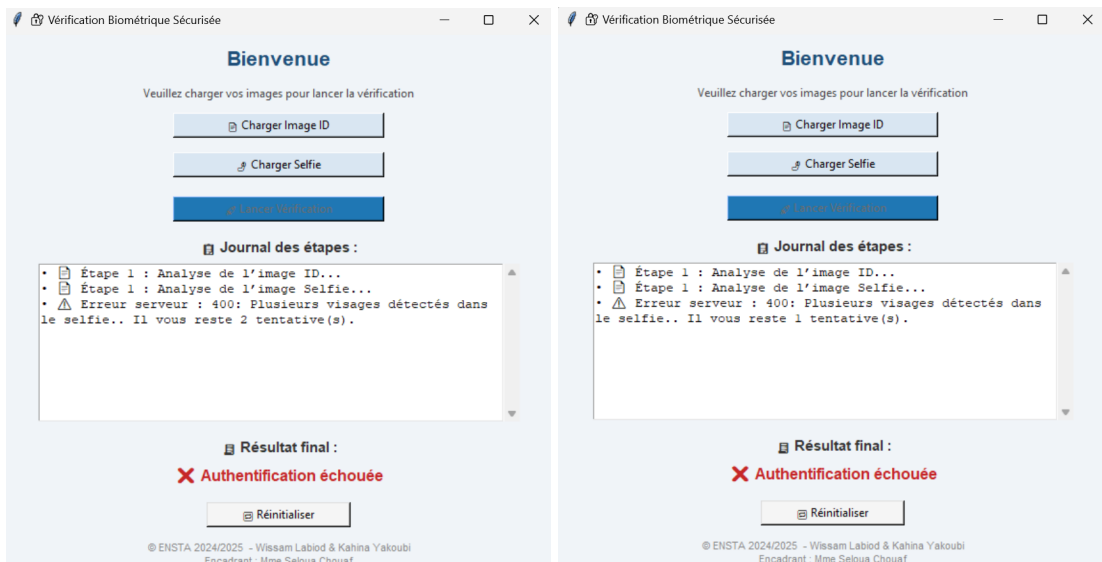


Figure 3.24 : Cas 2 : Plusieurs visages détectés dans le selfie – tentatives échouées

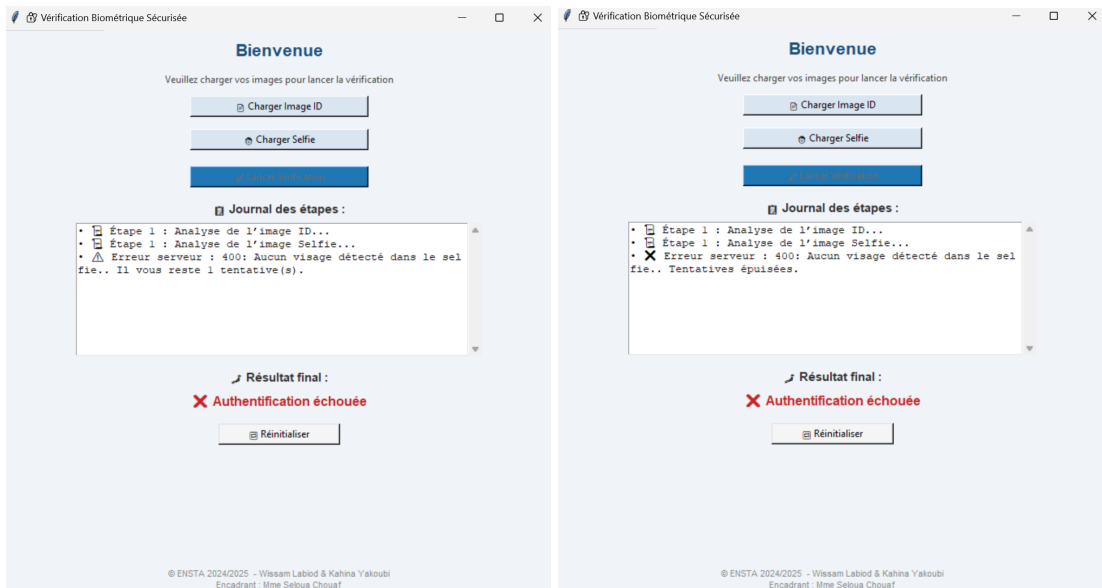


Figure 3.25 : Cas 3 : Aucun visage détecté dans le selfie – tentatives épuisées

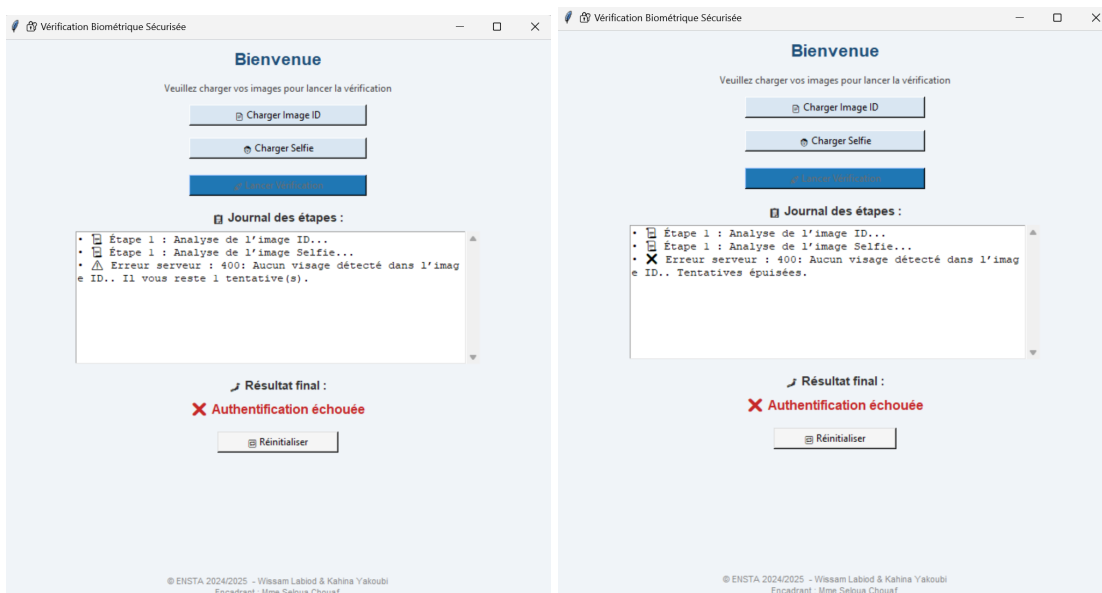


Figure 3.26 : Cas 4 : Aucun visage détecté dans l'image ID

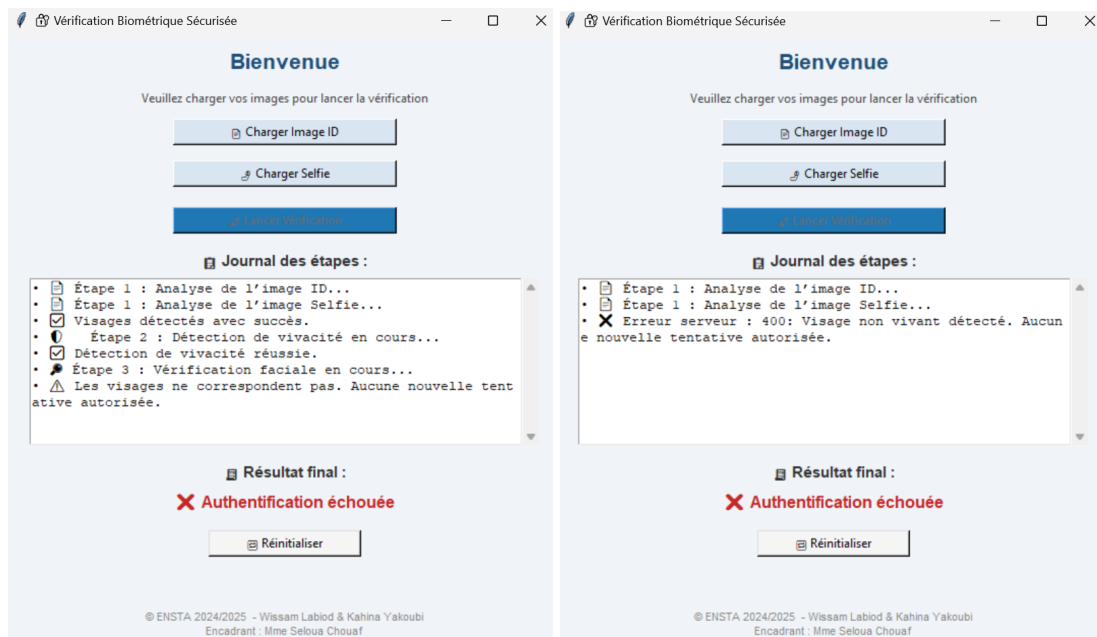


Figure 3.27 : Cas 5 : Échec de correspondance ou visage non vivant détecté

Ces scénarios permettent d'illustrer les limites de robustesse, les erreurs fréquentes, ainsi que la capacité du système à informer clairement l'utilisateur.

3.7 Perspectives d'amélioration et travaux futurs

L'analyse des performances du système biométrique développé a permis d'identifier plusieurs pistes concrètes d'amélioration, aussi bien sur le plan technique que fonctionnel.

3.7.1 Amélioration de la détection de vivacité

- Recalibrage des seuils ou adoption d'un système **adaptatif**, en fonction de la qualité d'image ou de la diversité des utilisateurs ;
- Évaluation de **nouveaux modèles légers ou multi-modaux**, combinant texture, mouvement, profondeur ou spectre IR ;
- Possibilité d'introduire une **supervision active** dans le processus (détection de réactions à des consignes).

3.7.2 Optimisation des performances et du code

- **Réduction de la taille des modèles** pour une exécution plus rapide via quantization ou distillation de connaissances ;
- **Traitement asynchrone dans l'API FastAPI**, pour améliorer la réactivité du système et gérer plusieurs requêtes en parallèle ;
- Préparation à un **déploiement distribué ou embarqué**, selon le cas d'usage visé.

3.7.3 Robustesse et diversité

- Améliorer la **tolérance aux variations** (âge, expression, pose) en enrichissant les jeux de données et en renforçant le prétraitement (nettoyage, alignement) ;
- **Intégration d'un module de qualité d'image**, capable de rejeter automatiquement les captures non exploitables.

3.7.4 Sécurité des données et expérience utilisateur

- Chiffrement systématique des **embeddings faciaux** et des données traitées ;
- Implémentation d'un **retour visuel ou vocal en temps réel** pour guider l'utilisateur lors de la capture (ex : cadrage, mouvement requis) ;
- Conformité renforcée avec les **règlements sur la protection des données**, notamment en limitant la conservation locale des images.

3.7.5 Développement d'une interface utilisateur embarquée

— Développement d'une application mobile embarquée tenant compte des scénarios dictés par les organigrammes d'authentification, permettant à l'utilisateur de faire une demande d'accès via capture selfie ou scan d'identifiant, et de recevoir des messages de validation ou de rejet.

— L'interface a été développée avec succès, mais reste à relier aux dispositifs d'acquisition pour permettre la capture en direct du selfie et la numérisation de la pièce d'identité, au lieu de sélectionner manuellement les fichiers depuis un emplacement local.

3.7.6 Reprise du mode dynamique basé sur vidéo

Une version complémentaire à la solution proposée a été testée, intégrant une analyse **dynamique** à partir d'une **courte vidéo selfie**. Le principe était d'extraire plusieurs frames de la vidéo, d'évaluer la vivacité sur chacune (via le modèle *CDCN++*) puis d'en calculer un embedding moyen des visages vivants détectés, afin d'en améliorer la robustesse.

Cependant, cette approche a été **abandonnée** en raison de performances insatisfaisantes :

- Qualité faible des frames extraites (flou, mauvaise exposition, bruit) ;
- Instabilité de la détection de visage sur certaines images ;
- Lourdeur du traitement et complexité à calibrer les seuils dans un flux d'images non uniforme.

Les figures 3.28 et 3.29 illustrent quelques cas rencontrés lors des expériences menées avec des vidéos, montrant les limites de robustesse ou d'interprétation.

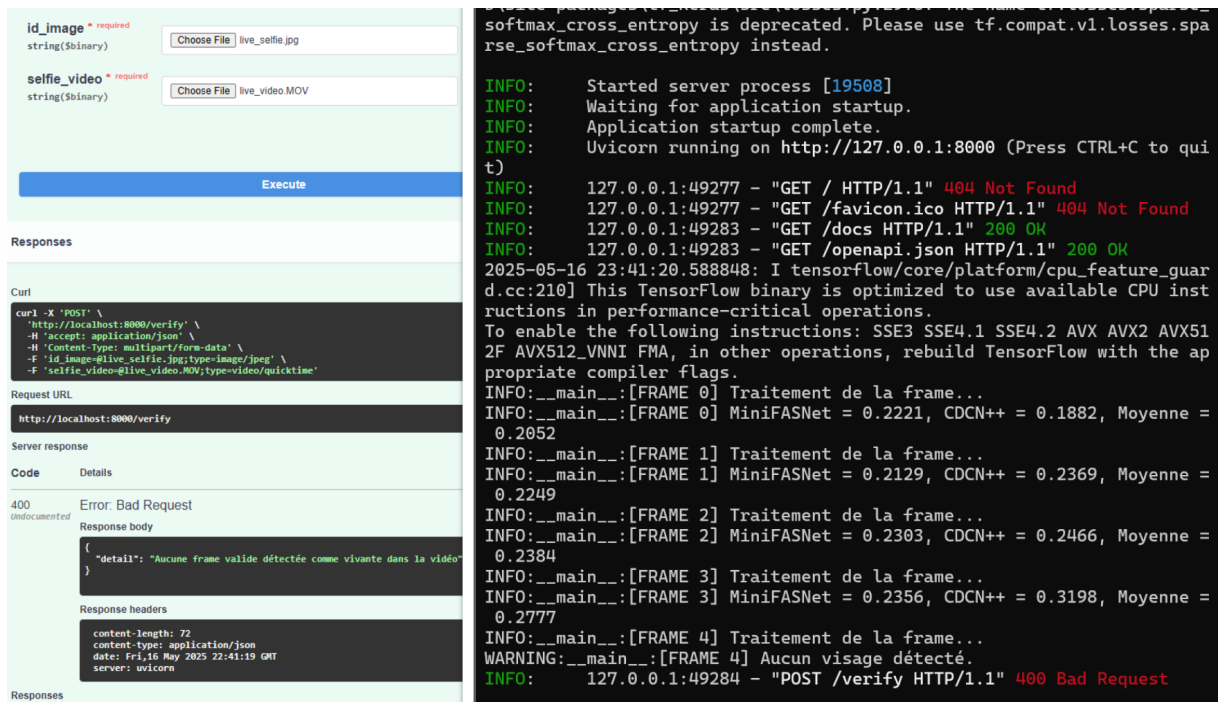


Figure 3.28 : Limites de détection de visage observées pour la solution exécutée en mode dynamique

Dans cet exemple, les images extraites de la vidéo ne contenaient pas de visage exploitable. Le système rejette donc l'entrée sans procéder à la comparaison ou à l'analyse de vivacité.



Figure 3.29 : Similarité faible malgré une vivacité confirmée, observée pour la solution exécutée en mode dynamique

Bien que les frames extraites aient été jugées authentiques (score de vivacité supérieur au seuil), la identification faciale a échoué. Cela est probablement dû à une qualité dégradée des images extraites (flou, bruit, ou mauvaise pose), ce qui a conduit à un score de similarité très faible malgré qu'il s'agisse de la même personne.

Une analyse des frames extraites a permis de mieux comprendre certaines erreurs observées. Comme illustré à la figure 3.30, les images extraites automatiquement présentent parfois des orientations incorrectes ou une qualité insuffisante (flou, cadrage partiel, etc.), ce qui compromet l'efficacité des modules de vivacité et de reconnaissance.

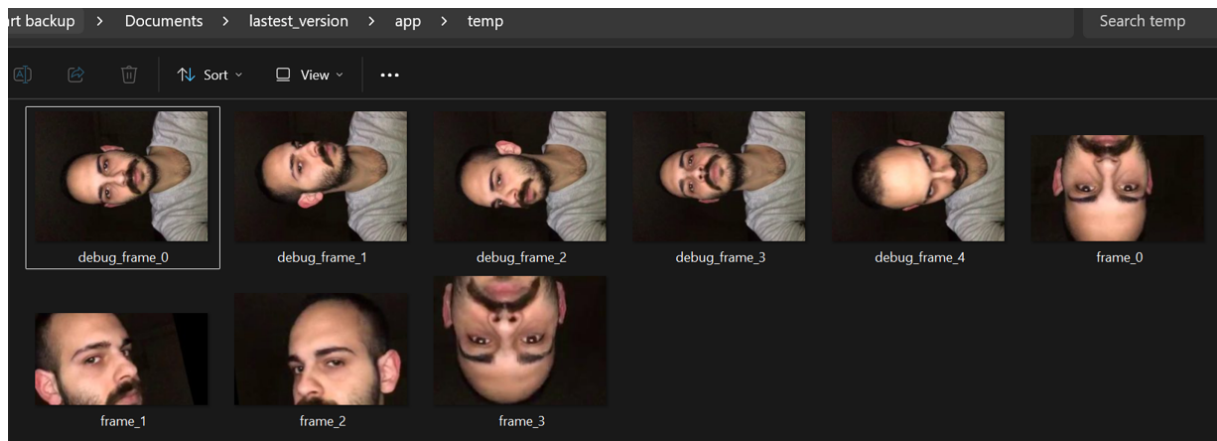


Figure 3.30 : Exemple d’illustration des frames extraits d’une vidéo et présentant des problèmes potentiels

On remarque que certaines images sont mal orientées ou de faible qualité, ce qui nuit à l’analyse de vivacité et à la reconnaissance faciale.

Malgré cela, cette approche dynamique reste prometteuse pour détecter des micro-mouvements impossibles à simuler par des attaques statiques. Pour y parvenir, les améliorations suivantes sont envisageables :

- Utiliser des **algorithmes de sélection de frames optimales** (en fonction de la netteté, de la présence d’un visage, etc.);
- Intégrer des méthodes d’**analyse de séquences** ou de tracking vidéo (optical flow, réseaux RNN/CNN 3D);
- Compléter la vivacité passive par des **actions guidées** (tourner la tête, cligner des yeux...).

3.8 Conclusion

Ce chapitre a permis de valider expérimentalement la solution de vérification biométrique proposée. Les résultats montrent une **bonne capacité de filtrage des attaques** via la détection de vivacité, en particulier grâce au seuil fixé à 0,3, qui rejette plus de 80 % des tentatives d’usurpation.

Les courbes cumulées et les statistiques résument une **séparation notable** entre les scores des cas réels et des attaques, malgré une zone de chevauchement expliquant certains faux positifs/négatifs.

Des **limitations techniques** ont été relevées, notamment liées à la qualité des images issues de vidéos, affectant la similarité. Cela justifie le besoin de renforcer le système avec des filtres de qualité ou des approches multi-modalité. Les résultats obtenus confirment la pertinence de l’architecture mise en place, tout en ouvrant la voie à plusieurs champs d’amélioration tel qu’il a été amplement discuté à la fin de ce chapitre.

Conclusion Générale

Dans un contexte où la sécurisation des identités numériques constitue un enjeu majeur, ce mémoire s'inscrit dans une démarche visant à concevoir une solution fiable de vérification biométrique reposant sur la reconnaissance faciale et la détection de vivacité.

L'étude met en évidence la complémentarité de ces deux composantes pour répondre aux défis actuels de l'authentification, notamment face à des attaques par présentation de plus en plus sophistiquées.

Le travail s'est appuyé sur une revue approfondie des fondements théoriques de la biométrie, des techniques de traitement d'images et des approches modernes en apprentissage profond, constituant un socle conceptuel solide pour guider la conception d'un système modulaire performant.

Ce système intègre plusieurs modèles avancés, tels que RetinaFace pour la détection faciale, CDCN++ et Mini-FASNetV1SE pour la détection de vivacité, ainsi que ArcFace et FaceNet pour l'identification. Son architecture a été pensée pour garantir à la fois robustesse, précision et applicabilité en conditions réelles.

Les résultats expérimentaux obtenus démontrent l'efficacité de la solution, notamment en termes de réduction des faux positifs et de capacité à distinguer les visages réels des attaques, bien que certaines limites existent face à des cas extrêmes de falsification et à la variabilité des conditions de capture.

Au-delà des aspects techniques, cette étude met également en lumière les défis éthiques liés à l'usage de la reconnaissance faciale, notamment en matière de respect de la vie privée et de la considération des biais algorithmiques. Ces enjeux doivent être intégrés plus systématiquement dans le développement de futures solutions afin d'assurer une approche plus équitable et transparente.

Ainsi, ce travail ouvre plusieurs perspectives prometteuses, telles que l'intégration de modèles plus légers pour une exécution optimisée sur des terminaux mobiles, l'enrichissement des bases d'entraînement pour améliorer l'équité du système, ou encore l'adaptation à d'autres modalités biométriques. Une autre piste intéressante serait d'intégrer des commandes sonores à l'interface utilisateur, afin d'assister les personnes malvoyantes dans le processus d'authentification.

Par ces avancées, cette recherche constitue une contribution concrète au développement de technologies d'intelligence artificielle éthiques, sécurisées et adaptées aux exigences du monde numérique actuel.

Références bibliographiques

- [1] IDEMIA, “Qu’est-ce que la biométrie? Toutes les réponses!,” *IDEMIA*, 2025. Disponible : <https://www.idemia.com/fr/biometrie>.
- [2] Laxton Group, “Technologie biométrique pour un contrôle efficace des frontières dans l’UE,” *Laxton Group*, 2025. Disponible : <https://www.laxtongroup.com/eu-border-biometrics>.
- [3] HID Global, “La biométrie dans le secteur bancaire et financier,” *HID Global*, 2025. Disponible : <https://www.hidglobal.com/solutions/biometrics-finance>.
- [4] L. Mansouri, “Optimisez la sécurité de votre entreprise avec le contrôle d’accès biométrique,” *Access Protection*, 2025. Disponible : <https://www.accessprotection.fr/contrôle-accès-biometrique>.
- [5] Mike, “La biométrie utilisée dans les soins de santé pour identifier avec précision les patients,” *HFSecurity*, 2023. Disponible : <https://www.hfsecurity.com/healthcare-biometrics>.
- [6] Alice Biometrics, “Le rôle de la biométrie dans la cybersécurité : Menaces et solutions,” *Alice Biometrics*, 2023. Disponible : <https://alicebiometrics.com/cybersecurity-threats>.
- [7] A. Terekhin, “Presentation Attacks : What Liveness Detection Systems Protect From Every Day,” *Regula Forensics*, 2025. Disponible : <https://www.regulaforensics.com/blog/presentation-attacks>.
- [8] iProov, “Comment les deepfakes menacent les systèmes de vérification d’identité à distance,” *iProov*, 2024. Disponible : <https://www.iproov.com/blog/deepfake-threat>.
- [9] DATUREX GmbH, “Données biométriques et éthique : la protection des données en ligne de mire,” *DATU-REX*, 2024. Disponible : <https://www.daturex.com/ethics-biometrics>.
- [10] FasterCapital, “Systèmes de reconnaissance faciale,” *FasterCapital*, 2025. Disponible : <https://www.fastercapital.com/face-recognition>.
- [11] Didit, “Authentification biométrique : avantages et risques,” *Didit*, 2025. Disponible : <https://www.didit-security.com/biometric-authentication>.
- [12] Proax, “Vision Industrielle : Matériel, Logiciel et Applications,” *Proax*, 2024. Disponible : <https://www.proax.com/industrial-vision>.
- [13] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” *IEEE CVPR*, vol. 1, pp. I-511–I-518, 2001.
- [14] T. Rousseau and L. Lopez, “Les différents visages de la reconnaissance faciale : fonctionnement et attaques,” *RiskInsight – Blog cybersécurité de Wavestone*, 2024. Disponible : <https://riskinsight.wavestone.com/face-recognition-faces>.
- [15] Backprop Lab, “Face Recognition Pipeline Clearly Explained,” *Medium*, 2020. Disponible : <https://medium.com/backproplab/face-recognition-pipeline>.
- [16] Shaip, “Qu’est-ce que la reconnaissance faciale? Comment ça fonctionne?,” *Shaip*, 2024. Disponible : <https://www.shaip.com/what-is-face-recognition>.
- [17] V. Kshirsagar, M. R. Baviskar, and M. E. Gaikwad, “Face recognition using Eigenfaces,” *Proc. ICCRD*, vol. 2, pp. 302–306, Mar. 2011.

- [18] A. Singh, “Linear Discriminant Analysis (LDA) : Maximizing Class Separability for Supervised Learning,” *Medium*, 2024. Disponible : <https://medium.com/@abhaysingh/lda-class-separability>.
- [19] N. Dalal and B. Triggs, “Histograms of Oriented Gradients for Human Detection,” *Proc. IEEE CVPR*, 2005.
- [20] Danyang, “Comparison of HOG and SIFT,” *Medium*, 2023. Disponible : <https://medium.com/@danyang/hog-vs-sift>.
- [21] IA School, “Convolutional Neural Network (CNN), qu’est-ce que c’est?,” *IA School*, 2025. Disponible : <https://www.iaschool.fr/cnn-definition>.
- [22] FACIA, “3D Face Recognition : The Definitive Guide to Improve Digital Security,” *FACIA*, 2023. Disponible : <https://facia.ai/3d-face-recognition-guide>.
- [23] Daniella, “Vision Transformer : nouvel horizon en traitement image,” *Innovatiana*, 2024. Disponible : <https://innovatiana.com/vision-transformer>.
- [24] Aïcha, “Classification d’images : de la théorie à la pratique,” *Innovatiana*, 2024. Disponible : <https://innovatiana.com/classification-images>.
- [25] Bruno, “Why is Face Alignment Important for Face Recognition?,” *Analytics Vidhya*, 2024. Disponible : <https://www.analyticsvidhya.com/face-alignment>.
- [26] Astera, “Outils de nettoyage des données : un moyen d’améliorer la fiabilité des données,” *Astera*, 2025. Disponible : <https://www.astera.com/data-cleaning-tools>.
- [27] LinkedIn Learning, “Quelles sont les meilleures pratiques et outils pour le prétraitement et l’augmentation des données d’image?,” *LinkedIn Learning*, 2025. Disponible : <https://www.linkedin.com/learning/image-preprocessing-augmentation>.
- [28] J. Robert, “Reconnaissance faciale : Décryptage de son fonctionnement,” *DataScientest*, 2023. Disponible : <https://datascientest.com/face-recognition-explained>.
- [29] Didit, “Biométrie, détection de vivacité et plus encore,” *Didit*, 2024. Disponible : <https://www.didit-security.com/liveness-biometrics>.
- [30] Unissey, “Quelles sont les attaques par biométrie faciale les plus courantes,” *Unissey*, 2023. Disponible : <https://unissey.com/face-biometrics-attacks>.
- [31] Alice Biometrics, “Détection des attaques par présentation faciale,” *Alice Biometrics*, 2023. Disponible : <https://alicebiometrics.com/presentation-attacks>.
- [32] K. Yasar, N. Barney and I. Wigmore, “What is Deepfake Technology?,” *TechTarget*, 2025. Disponible : <https://www.techtarget.com/what-is-deepfake-technology>.
- [33] Cyber Sécurité, “Qu’est-ce qu’un LIVENESS – Détection de Vivacité?,” *Cyber Sécurité*, 2025. Disponible : <https://www.cybersecurite.fr/liveness-detection>.
- [34] FasterCapital, “Traitement d’images par ordinateur,” *FasterCapital*, 2025. Disponible : <https://www.fastercapital.com/computer-vision>.
- [35] Ada Tech School, “Les biais algorithmiques : comment le code peut être discriminant?,” *Ada Tech School*, 2025. Disponible : <https://www.adatechschool.com/algorithmic-bias>.
- [36] A. Kabbalan et al., “Reconnaissance faciale dans l’espace public,” *Mines Paris PSL*, 2022.
- [37] J. Buolamwini and T. Gebru, “Gender Shades,” *Bias in ML, PMLR*, pp. 77–91, 2018. Disponible : <http://proceedings.mlr.press/v81/buolamwini18a.html>.
- [38] Amnesty International France, “Reconnaissance faciale : neuf questions pour comprendre,” *Amnesty International France*, 2024. Disponible : <https://www.amnesty.fr/tech-et-libertes/biometrie>.
- [39] J. Deng et al., “RetinaFace : Single-stage Dense Face Localisation in the Wild,” *arXiv*, 2019. Disponible : <https://arxiv.org/abs/1905.00641>.

- [40] T.-Y. Lin et al., “Feature Pyramid Networks for Object Detection,” *arXiv*, 2016. Disponible : <https://arxiv.org/abs/1612.03144>.
- [41] M. Najibi et al., “SSH : Single Stage Headless Face Detector,” *arXiv*, 2017. Disponible : <https://arxiv.org/abs/1708.03979>.
- [42] GeeksforGeeks, “What is Image Classification?,” *GeeksforGeeks*, 2024. Disponible : <https://www.geeksforgeeks.org/what-is-image-classification>.
- [43] RunComfy, “ComfyUI Node : Face Bounding Box,” *RunComfy*, 2024. Disponible : <https://www.runcomfy.com/comfyui-face-bounding-box>.
- [44] Z. Yu et al., “Central Difference Convolutional Networks for Face Anti-Spoofing,” *arXiv*, 2020. Disponible : <https://arxiv.org/abs/2003.04092>.
- [45] J. Hu et al., “Squeeze and Excitation Networks,” *arXiv*, 2017. Disponible : <https://arxiv.org/abs/1709.01507>.
- [46] A. Grignola, “Qu’est-ce qu’un CNN?,” *DataBird*, 2024. Disponible : <https://databird.com/what-is-cnn>.
- [47] Shubham, “Batch Normalization and Dropout : A Combined Regularization Approach,” *LearnOpenCV*, 2025. Disponible : <https://learnopencv.com/batchnorm-dropout>.
- [48] J. Deng et al., “ArcFace : Additive Angular Margin Loss for Deep Face Recognition,” *arXiv*, 2018. Disponible : <https://arxiv.org/abs/1801.07698>.
- [49] D. Agarwal, “Creating a Face Recognition System with MTCNN, FaceNet, and Milvus,” *Medium*, 2025. Disponible : <https://medium.com/@devrajarwal/face-recognition-mtcnn-facenet>.
- [50] F. Schroff, D. Kalenichenko and J. Philbin, “FaceNet : A Unified Embedding for Face Recognition and Clustering,” *arXiv*, 2015. Disponible : <https://arxiv.org/abs/1503.03832>.
- [51] C. Jekel, “512 vs 128 FaceNet embeddings on Tinder dataset,” *Jekel.com*, 2025. Disponible : <https://jekel.com/facenet-embeddings-tinder>.