République Tunisienne
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Sfax

École nationale d'électronique
et des télécommunications de Sfax

Ingénieur en :
Ingénierie des données et Systèmes
Décisionnels

N° d'ordre : IDSD-2024/2025-N° 33

Projet De Fin D'Année

présenté à

L'École Nationale d'Électronique et des Télécommunications de Sfax

en vue de l'obtention du

Diplôme National d'Ingénieur en :
Ingénierie des données et Systèmes Décisionnels

par

Khaoula BOUGHATTAS

Vers une authentification fiable : Système de classification pour la détection des empreintes digitales réelles et falsifiées

Soutenu le 19/04/2025, devant la commission d'examen :

Mme. Sonda AMMAR	Encadrante
Mme. Nassira ACHICH	Examinatrice

REMERCIEMENTS

Au terme de ce projet de fin d'année, je souhaite exprimer ma profonde gratitude à toutes les personnes qui ont contribué, de près ou de loin, à la réussite de ce travail.

Je remercie tout particulièrement mon encadrante, **Mme Sonda AMMAR**, pour sa disponibilité, son accompagnement bienveillant, ses conseils constructifs et sa rigueur scientifique tout au long de ce projet. Son soutien m'a permis d'approfondir mes compétences et de mener cette expérience dans les meilleures conditions.

Je tiens également à adresser mes sincères remerciements à **Mme Nassira ACHICH**, qui assurera l'évaluation de ce travail. Son regard critique et ses remarques lors de la soutenance seront, sans nul doute, une source précieuse d'enrichissement.

Mes remerciements s'étendent à l'ensemble du corps enseignant de **l'ENET'Com** pour la qualité de la formation reçue, ainsi qu'aux membres de l'administration pour leur disponibilité et leur professionnalisme.

Je n'oublie pas de remercier ma famille, en particulier mes parents, pour leur soutien moral constant, leur patience et leur confiance en moi. Leur présence silencieuse mais essentielle m'a accompagné à chaque étape de mon parcours.

Enfin, un grand merci à mes collègues, amis et camarades de promotion pour leur entraide, leur bonne humeur et leur esprit collaboratif tout au long de cette aventure académique.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

AFIS Automated Fingerprint Identification System

Accuracy Exactitude, proportion de prédictions correctes

Adam Algorithme d'optimisation pour l'apprentissage

Cross-Entropy Loss Fonction de perte utilisée pour la classification

CUDA Compute Unified Device Architecture (plateforme de calcul parallèle)

ConvNeXt Architecture de réseau neuronal convolutif inspirée des Transformers

CNN Convolutional Neural Network (Réseau de neurones convolutifs)

ECG Electrocardiogram

F1-Score Moyenne harmonique entre la précision et le rappel

Fake Empreintes falsifiées

FCN Fully Convolutional Network

FFT Fast Fourier Transform

GELU Gaussian Error Linear Unit (fonction d'activation)

Intra-capteur Evaluation sur le même capteur que l'entraînement

Inter-capteur Evaluation sur un capteur différent de celui utilisé pour l'entraînement

ImageNet Large-scale visual recognition dataset (ensemble de données pour la reconnaissance visuelle à grande échelle)

LSTM Long Short-Term Memory (a type of Recurrent Neural Network)

LayerNorm Normalisation de couche (une technique de normalisation des réseaux de neurones)

LivDet International Fingerprint Liveness Detection Competition (used for benchmarking fingerprint detection methods)

Live Empreintes authentiques (réelles)

Mevii$_{ensemble}$ A specific ensemble of models for testing fingerprint liveness detection, mentioned in the context of the LivDet competition

PAD Presentation Attack Detection (Détection d'attaque par présentation)

Precision Proportion des vraies prédictions positives sur toutes les prédictions positives

Recall Sensibilité, capacité du modèle à capturer les vraies positives

ResNet Residual Network (a type of CNN)

RTV Room Temperature Vulcanizing (caoutchouc à prise ambiante)

SVD Singular Value Decomposition

SVM Support Vector Machine

VGG Visual Geometry Group (a type of CNN)

PyTorch Librairie d'apprentissage automatique pour le calcul de gradients

Checkpoint Sauvegarde du modèle lors de la meilleure performance sur la validation

Early Stopping Arrêt prématuré pour éviter le surapprentissage

GANs Generative Adversarial Networks

INTRODUCTION GÉNÉRALE

À l'ère du numérique, la biométrie occupe une place centrale dans les systèmes d'authentification. Parmi les différentes modalités, l'empreinte digitale est l'une des plus utilisées en raison de sa stabilité, son unicité et sa facilité d'intégration. Cependant, malgré son efficacité, elle reste vulnérable aux attaques par présentation (ou "presentation attacks"), qui consistent à tromper le système à l'aide de fausses empreintes réalisées avec divers matériaux.

Face à cette problématique, ce projet a pour objectif de concevoir un système de détection d'empreintes falsifiées, combinant à la fois des méthodes classiques d'extraction de descripteurs et les approches récentes d'apprentissage profond. Pour cela, le modèle ConvNeXt Tiny a été utilisé en tant que classificateur principal.

Le travail repose sur l'exploitation de la base de données LivDet2015, qui offre une diversité de capteurs et de matériaux de falsification, rendant l'analyse plus réaliste et pertinente. Le développement de l'outil a été réalisé en `Python`, avec `PyTorch` et `Streamlit` et d'autres bibliothèques.

Ce rapport s'articule autour de deux axes principaux :

— Une première partie théorique abordant le contexte géneral et la problématique.

— Une deuxième partie dédiée à la réalisation du système, de classification pour la détection des empreintes digitales réelles et falsifiées .

Ce projet illustre ainsi comment les avancées en intelligence artificielle peuvent renforcer la sécurité des systèmes biométriques face aux nouvelles menaces.

Chapitre

1 CLASSIFICATION DES EMPREINTES DIGITALES : CONTEXTE, PROBLÉMATIQUES ET APPROCHES DE DEEP LEARNING

Sommaire

Introduction

À l'ère numérique, où la sécurité devient un enjeu majeur, les systèmes biométriques, notamment ceux reposant sur les empreintes digitales, jouent un rôle clé. Leur force réside dans l'unicité et la permanence des empreintes, mais ces systèmes font face à des attaques de plus en plus ingénieuses, telles que les moulages ou les empreintes synthétiques.

Ce projet de fin d'année se donne pour mission de repousser ces vulnérabilités. Il propose de concevoir un système innovant basé sur le Deep Learning, capable de distinguer les empreintes authentiques des imitations, assurant ainsi une fiabilité inébranlable face aux menaces modernes.

1.1 Contexte et problématique

1.1.1 Les empreintes digitales

1.1.1.1 Historique de l'identification par empreintes digitales

L'utilisation des empreintes digitales pour l'identification humaine remonte à l'Antiquité, notamment en Chine ou à Babylone. Cependant, ce n'est qu'au XIX^{e} siècle qu'elles sont intégrées dans un cadre scientifique rigoureux, grâce aux travaux de Galton et Henry. Ce dernier développe un système de classification adopté par Scotland Yard. L'ère moderne commence avec l'automatisation via l'AFIS dans les années 1980, marquant l'avènement d'une reconnaissance numérique rapide et globale.

1.1.1.2 Caractéristiques biométriques

Les empreintes digitales sont l'un des traits biométriques les plus fiables, car elles présentent des propriétés uniques, permanentes et faciles à acquérir. Leur formation débute au stade fœtal, entre la 10^{e} et la 16^{e} semaine de gestation, sous l'influence combinée de facteurs génétiques et environnementaux, ce qui leur confère une variabilité interindividuelle irréductible.

Elles sont composées de **crêtes papillaires** (ou dermatoglyphes), formant un motif régulier de sillons et de crêtes qui recouvrent la peau des doigts. Ces crêtes s'organisent selon trois grands **motifs globaux** :

— les **boucles** (*loops*) : motif le plus fréquent, représentant environ 60–65% des empreintes ;

— les **tourbillons** (*whorls*) : structures concentriques ou spiralées (30–35%) ;

— les **arches** (*arches*) : motif le plus simple et le plus rare, présent dans environ 5% des cas.

FIGURE 1.1 – Structure des crêtes papillaires.

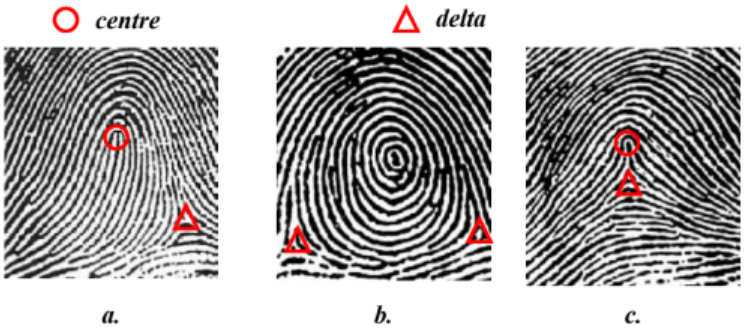


FIGURE 1.2 – Motifs globaux des empreintes : boucle, tourbillon, arche.

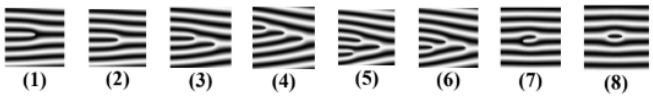
Au-delà des motifs globaux, l'identification fine repose sur l'analyse des **minuties**, des détails locaux très discriminants. Les minuties les plus courantes incluent :

— les **terminaisons** : fin d'une crête ;

— les **bifurcations** : division d'une crête en deux branches ;

— les **îlots**, **points** ou **traverses** : crêtes isolées ou éléments singuliers.

Ces minuties sont extraites puis représentées sous forme d'un **gabarit biométrique** (*template*), structure de données numérique contenant leurs positions, orientations et types. Ce template sert ensuite de référence pour les opérations de vérification ou d'identification.



1.	terminaison	**9.**	boucle double
2.	bifurcation simple	**10.**	pont simple
3.	bifurcation double	**11.**	pont jumeau
4.	bifurcation triple I	**12.**	intervalle
5.	bifurcation triple II	**13.**	point isolé
6.	bifurcation triple III	**14.**	traversée
7.	crochet	**15.**	croisement
8.	boucle simple	**16.**	tête bêche

FIGURE 1.3 – Principaux types de minuties.

La richesse structurelle et l'invariance temporelle des empreintes en font un outil idéal pour la biométrie. Toutefois, leur exactitude dépend fortement de la qualité d'acquisition et des performances des algorithmes d'analyse, notamment en présence de bruit, de distorsion, ou d'empreintes partielles.

1.1.1.3 Applications et implications

Les empreintes digitales sont omniprésentes dans les applications de sécurité, l'administration, les enquêtes criminelles ou les services numériques. Toutefois, leur utilisation massive soulève des questions de sécurité des données et de respect de la vie privée.

1.1.2 Défis et limitations de la biométrie par empreintes digitales

1.1.2.1 Défis techniques

Malgré leur fiabilité, plusieurs limites persistent :

— **Qualité de capture** affectée par l'état de la peau, la présence de sueur, de cicatrices ou encore le flou de l'image, particulièrement critique dans les systèmes sans contact [17] ;

— **Variabilité intra/interindividuelle** rendant l'appariement incertain, notamment dans les environnements à forte humidité ou avec des doigts secs ;

— **Captures partielles et distorsions** liées aux déformations élastiques lors du contact avec le capteur ou à l'angle de prise de vue dans les systèmes sans contact ;

— **Manque de standardisation** entre capteurs optiques, capacitifs, ultrasoniques ou photo-vidéo, ce qui nuit à l'interopérabilité et à la portabilité des modèles.

1.1.2.2 Attaques par falsification (spoofing)

Les attaques de présentation visent à tromper les capteurs avec des empreintes artificielles :

— **Physiques** : moulages en latex, ecoflex, playdoh, colle bois [17] ;

— **Imprimées ou projetées** : impressions couleur haute résolution sur papier photo brillant ;

— **Synthétiques** : empreintes générées par GANs, comme celles produites avec StyleGAN-ADA, atteignant des scores visuellement réalistes [17].

La détection de vitalité (mouvement, transpiration, structure de la peau) est une réponse technique essentielle. Toutefois, les performances diminuent face aux attaques inconnues ou sophistiquées, comme celles conformes aux niveaux de difficulté définis par la norme FIDO [17].

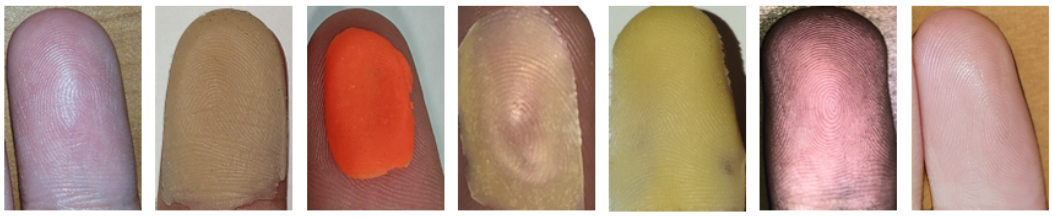


FIGURE 1.4 – Exemples d'attaques de spoofing.

1.1.2.3 Enjeux de sécurité et d'éthique

— **Irréversibilité** : une empreinte volée est difficile à remplacer, rendant le compromis biométrique critique ;

— **Fuites de données** : la centralisation de données sensibles requiert un chiffrement fort et des protocoles de gestion d'accès stricts ;

— **Vie privée et biais** : des biais algorithmiques ou des défauts de généralisation sur certaines populations peuvent introduire des discriminations, en contradiction avec le RGPD et les principes éthiques de l'IA.

1.2 Objectif

Ce projet vise à répondre à la problématique suivante : *comment concevoir un système de classification fiable, basé sur des architectures de Deep Learning, pour détecter efficacement les empreintes digitales falsifiées ?*

Pour ce faire, l'étude se donne pour objectifs :

— d'implémenter et de comparer plusieurs architectures CNN ;

— d'évaluer leur robustesse face à divers types d'attaques de spoofing ;

— de proposer un modèle performant, généralisable à des contextes réels.

1.3 État de l'art

La *Presentation Attack Detection* (PAD) pour les empreintes digitales cherche à différencier les empreintes authentiques des falsifications, qu'elles soient physiques (ex. moulages) ou numériques (ex. générées par des GANs). Ce domaine a considérablement évolué, passant des descripteurs manuels à des approches hybrides, multimodales, et basées sur des réseaux neuronaux profonds.

1.3.1 Descripteurs manuels et hybridation

Les descripteurs classiques tels que LBP, LPQ, et BSIF sont efficaces en termes de rapidité, mais restent sensibles aux variations environnementales. Le modèle AILearn [1] combine apprentissage incrémental et ResNet-50, atteignant jusqu'à 99.02% de précision sur LivDet2013. D'autres approches hybrides, comme CNN+SVM [5], fusionnent des techniques de texture et d'apprentissage profond, atteignant des précisions proches de 99.6%.

1.3.2 Apprentissage profond

Les architectures CNN (ResNet, VGG, Inception) ont largement surpassé les méthodes traditionnelles. Le modèle hybride CNN+LSTM [2], qui combine convolution et réseaux récurrents, atteint 97.1% de précision. Toutefois, la complexité computationnelle et la dépendance à des bases de données massives restent des défis majeurs.

1.3.3 Modules d'attention

L'ajout de mécanismes d'attention, qu'ils soient spatiaux ou par canal (ex. ResNet+Attention) [3], permet d'améliorer les performances jusqu'à 97.78%. Le pooling stochastique a également montré son efficacité, bien que la régularisation des modèles reste un point délicat.

1.3.4 Méthodes multimodales

La fusion des empreintes digitales avec des signaux complémentaires comme l'ECG, les images thermiques, ou l'analyse comportementale (ex. transpiration) [4] permet d'atteindre des scores proches de 100%. Des systèmes comme MFAS [4] et les dispositifs IoT offrent une haute précision, bien qu'ils nécessitent souvent un matériel spécialisé.

1.3.5 Contre les empreintes synthétiques

Face aux attaques basées sur les GANs, des modèles spécialisés comme RFDforFin [8] utilisent des techniques avancées comme le FFT et le flux de crêtes, atteignant des taux de précision de 100% sur certaines bases. Ce modèle réduit la complexité à 94.8K paramètres, contre 23.5M pour un ResNet-50 traditionnel.

1.3.6 Analyse temporelle

L'analyse dynamique des empreintes par des architectures CNN-LSTM [6], utilisant des réseaux comme MobileNet-v1 couplés à des Bi-LSTM, permet de capturer des indices subtils

de vie, tels que la perspiration et les variations de texture, avec des précisions atteignant 99.25%. D'autres méthodes, comme celles basées sur l'analyse comportementale des doigts (ex. FinAuth) ou la transpiration (Sweat-COF [4]), atteignent des taux de réussite de 100%.

1.3.7 Réseaux neuronaux légers et compacts

Des réseaux neuronaux plus légers, comme le FCN FireNet [16], utilisent des modules compacts (2MB) pour une détection rapide et efficace, même sans prétraitement, atteignant 98.65%. D'autres modèles comme LFLDNet [4] sont spécifiquement conçus pour l'intégration sur des systèmes embarqués à ressources limitées.

1.3.8 Méthodes statistiques et basées sur la texture

Des approches comme l'Edge Direction Descriptor, BiRi-PAD, ou Low-Rank LBP [4] s'appuient sur des analyses de texture avancées (SVD, bifurcations, histogrammes) et atteignent des performances allant jusqu'à 98.65%. Bien que rapides et efficaces, ces méthodes peuvent souffrir de limitations en termes de généralisation.

1.3.9 Compétitions et benchmarks

Les compétitions *LivDet* (2011–2021) demeurent des références incontournables dans le domaine. L'édition 2021 a introduit le benchmark ScreenSpoof pour tester la robustesse des systèmes face à des attaques inédites. Les ensembles comme *megvii_ensemble* ont atteint des précisions de 99.75 % [7], mais ces résultats chutent face aux attaques dites "never-seen-before".

1.3.10 Comparaison des approches

TABLE 1.1 – Comparaison des approches récentes de détection d'empreintes falsifiées

Méthode / Réf.	**Modèle / Approche**	**Base de données**	**Accuracy**	**Forces**	**Limites**
AILearn [1]	ResNet-50 + LBP, LPQ, BSIF	LivDet2011–15	99.02%	Incrémental, robustesse aux NF	Perte sur KF
Thomas [2]	CNN+LSTM	Propriétaire	97.1%	Spatio-temporel	Besoins computationnels
Qureshi [3]	ResNet+Attention	LivDet, ATVS	97.78%	Attention multicanal	Sensible aux paramètres
Jamal [4]	ECG + empreintes	Multibases	99.28%	Multimodalité, IoT	Coût matériel, vie privée
RFDforFin [8]	FFT + Ridge Streams	PolyU-HRF	100% / 99.5%	Anti-GAN, léger	Cas spécifiques
Hybrid [5]	CNN + SVM + descripteurs	ATVS-FFp-DB, SOCOFing	99.6%	Fusion texture + CNN	Variable selon dataset
MFAS [4]	Analyse comportementale	Données captives	100%	Détection de gestes forcés	Intrusif
FCN-Fire [16]	Fire Module FCN	LivDet 2011–15	98.65%	Léger, embarquable	Sensibilité matérielle
BiRi-PAD [4]	Histogrammes bifurcations	LivDet	98.65%	Texture, non-apprentissage	Moins robuste aux nouvelles attaques
LivDet2021 [7]	Ensemble CNNs	LivDet2021	99.75%	Bon sur test connu	Faible généralisation

1.3.11 Perspectives

Les travaux futurs devront s'orienter vers plusieurs axes novateurs :

— Développement de jeux de données synthétiques diversifiés, générés par des GANs, pour contrer les attaques émergentes et toujours plus complexes.

— Conception de modèles ultra-légers (TinyML) adaptés aux dispositifs embarqués, afin de rendre la détection biométrique plus accessible et efficace sur des plateformes à faibles ressources.

— Intégration de la détection multimodale, combinant thermographie, électrocardiographie et analyse comportementale, pour renforcer la fiabilité des systèmes biométriques face aux tentatives de falsification.

— Élaboration de benchmarks multicapteurs, capables de simuler des conditions environnementales réelles, pour tester et valider les performances des systèmes dans des scénarios variés et réalistes.

1.4 Solution adoptée

L'architecture retenue pour cette étude est **ConvNeXt**, un réseau neuronal convolutif de nouvelle génération proposé par Liu et al. en 2022. Conçu comme une modernisation des CNN classiques (notamment ResNet), ConvNeXt adopte plusieurs concepts inspirés des transformers tout en conservant une structure purement convolutive.

Parmi ses spécificités :

— Utilisation de **convolutions depthwise separables**, réduisant la complexité tout en améliorant les performances ;

— Intégration de la **normalisation LayerNorm** plutôt que BatchNorm, facilitant l'apprentissage profond ;

— Adoption de **kernels plus larges** (`7x7`) dans les couches initiales pour mieux capter le contexte spatial ;

— Design modulaire permettant une **scalabilité** sur différentes tailles de modèles (Tiny, Small, Base, Large).

Dans le cadre de cette étude, nous utilisons la variante *ConvNeXt-Tiny*, qui offre un excellent compromis entre précision, rapidité d'exécution, et consommation mémoire. Cette architecture sera entraînée sur des données d'empreintes digitales authentiques et falsifiées pour évaluer sa capacité de détection dans des contextes réalistes.

1.5 Technologies et environnement de développement

Ce projet a été développé dans un environnement optimisé pour l'apprentissage profond, avec une attention particulière portée à la compatibilité GPU, la gestion des données biométriques, et l'évaluation rigoureuse des performances du modèle.

1.5.1 Outils et bibliothèques essentiels

— **Python 3.10** : Langage de développement principal.

— **PyTorch & Torchvision** : Framework d'apprentissage profond pour la création, l'entraînement et l'évaluation des modèles.

— **Timm** : Accès au modèle `ConvNeXt Tiny` préentraîné.

— **Scikit-learn** : Calcul des métriques de classification et matrices de confusion.

— **Matplotlib & Seaborn** : Visualisation des performances.

— **Pillow (PIL)** : Lecture et traitement des empreintes digitales.

— **TQDM** : Affichage dynamique de la progression de l'entraînement.

1.5.2 Infrastructure matérielle

— **Machine** : HP Victus – Ryzen 5 5600H, 16 Go RAM.

— **Accélération GPU** : NVIDIA RTX 3050 (4 Go VRAM) via CUDA.

— **OS** : Windows 11.

1.5.3 Environnement logiciel

— **IDE** : Jupyter Notebook.

— **Gestion des packages** : `pip`, `conda`.

— **Dataset** : LivDet2015 – structure organisée par capteur et par classe.

— **Checkpoints** : Un fichier `.pth` enregistré par capteur dans `checkpoints/`.

Conclusion

La biométrie par empreintes digitales, bien que largement utilisée, demeure vulnérable aux attaques par présentation, notamment celles générées artificiellement. Ce chapitre a exposé les fondements, les limites actuelles et les enjeux liés à cette technologie. L'état de l'art met en évidence l'efficacité croissante des approches basées sur le Deep Learning, en particulier les modèles CNN, attentionnels et hybrides. Dans ce contexte, ce projet vise à développer un système de classification robuste, capable de détecter des empreintes falsifiées, même face à des attaques inconnues ou sophistiquées.

Chapitre

2

DEPLOIEMENT DU SYSTÈME DE CLASSIFICATION POUR DES EMPREINTES DIGITALES RÉELLES ET FALSIFIÉES

Sommaire

Introduction

La vérification de l'authenticité des empreintes digitales est un enjeu clé des systèmes biométriques, face à des techniques de contrefaçon de plus en plus sophistiquées. Ce projet vise à concevoir un système automatique de détection d'empreintes falsifiées, en s'appuyant sur des modèles d'apprentissage profond.

Nous explorons l'architecture *ConvNeXt Tiny*, appliquée à la base LivDet2015, afin d'évaluer sa capacité à distinguer les empreintes réelles des fausses. L'objectif est d'obtenir un modèle performant, robuste aux attaques inconnues, tout en restant léger pour un déploiement potentiel.

2.1 Modélisation et Classification

2.1.1 Choix du modèle

Le modèle choisi est **ConvNeXt Tiny**, une architecture CNN inspirée des Transformers, conçue pour offrir des performances élevées tout en restant légère et efficace. Elle est bien adaptée à la classification d'images biométriques comme les empreintes digitales.

Pourquoi ConvNeXt ?

— Architecture moderne inspirée des Transformers, avec des convolutions efficaces.

— Moins de paramètres que ResNet50, tout en maintenant de bonnes performances.

— Bon compromis entre performance, temps d'entraînement et complexité.

— Prise en charge de l'apprentissage par transfert (pré-entraînement sur ImageNet).

— Adaptabilité au fine-tuning sur des jeux de données spécifiques comme LivDet2015.

2.1.2 Architecture du modèle

ConvNeXt Tiny s'organise en quatre étapes principales :

— **Patchify Stem** : une convolution 4×4 avec stride 4 segmente l'image en patches.

— **Blocs ConvNeXt** : empilement de convolutions *depthwise* 7×7, normalisation `LayerNorm`, MLP avec activation `GELU`.

— **Hiérarchie** : 4 stades avec résolution décroissante et profondeur croissante.

— **Tête** : `Global Average Pooling` + couche linéaire à 2 classes (`live`, `fake`).

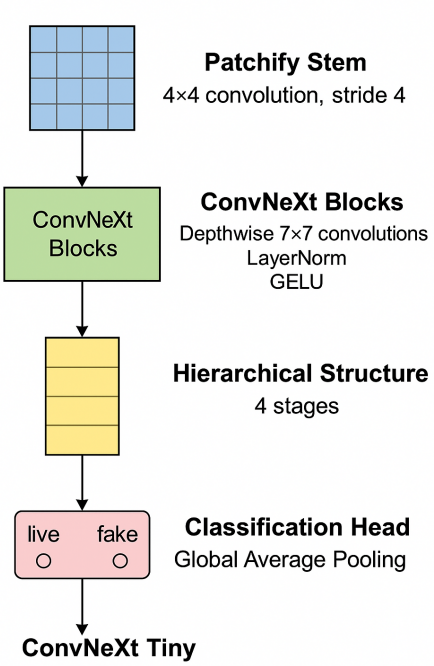


FIGURE 2.1 – Architecture simplifiée de ConvNeXt Tiny

2.1.3 Description de la base de données LivDet2015

LivDet2015 est un benchmark de référence pour l'évaluation des systèmes de détection d'attaques par présentation (PAD), avec un protocole expérimental rigoureux et reproductible.

a) Organisation

La base est composée de deux sous-ensembles :

— **Training/** : utilisé pour l'apprentissage supervisé.

— **Testing/** : utilisé pour l'évaluation sur des empreintes partiellement inédites.

Les données sont collectées via cinq capteurs :

— **CrossMatch**, **Digital Persona**, **Green Bit**, **Hi-Scan**, **Time Series** (ce dernier contient des données dynamiques).

Chaque capteur fournit des empreintes de deux types :

— `Live/` : empreintes authentiques.

— `Fake/` : empreintes falsifiées fabriquées avec divers matériaux.

b) Chiffres

Le jeu contient environ **10 205 images**, réparties entre l'entraînement et le test, selon la répartition suivante :

TABLE 2.1 – Distribution des images dans LivDet2015

Subset	Capteur	Live	Fake
Training	CrossMatch	1510	2070
	Digital Persona	1000	1000
	Green Bit	1000	1000
	Hi-Scan	1000	1000
	Time Series	130	4495
Testing	CrossMatch	394	1484
	Digital Persona	1000	1500
	Green Bit	1000	1500
	Hi-Scan	1000	1500

c) Matériaux de spoofing

Les empreintes falsifiées sont réalisées à partir de matériaux variés, chacun posant des défis spécifiques :

— **Ecoflex / Liquid Ecoflex** : silicone souple et réaliste.

— **Gelatine / Gelatin** : biomatériau semi-solide répandu.

— **Latex** : polymère moulable.

— **RTV** : caoutchouc à prise ambiante.

— **Wood Glue** : colle séchée à fort contraste.

— **OOMOO** : silicone à durcissement rapide.

— **Playdoh** : pâte souple, peu réaliste.

— **Body Double** : silicone pour moulage corporel.

d) Intérêt pour la recherche

— Présence de matériaux inédits en test (e.g. RTV, Liquid Ecoflex) permettant l'évaluation en *zero-shot*.

— Hétérogénéité des capteurs renforçant la robustesse inter-domaine.

— Données dynamiques (`Time Series`) exploitables pour des architectures hybrides (CNN + RNN).

2.1.4 Hyperparamètres et entraînement

L'entraînement a été effectué en utilisant PyTorch avec le modèle `ConvNeXt Tiny` pré-entraîné sur ImageNet, sur l'ensemble des capteurs de LivDet2015. Voici la configuration adoptée :

— **Fonction de perte** : Cross Entropy Loss (adaptée à la classification binaire).

— **Optimiseur** : Adam.

— **Taux d'apprentissage** : 1×10^{-4}.

— **Nombre d'époques** : 50 (avec early stopping).

— **Batch size** : 32.

— **Taille des images** : 224×224 pixels.

— **Split validation** : 20% de l'ensemble d'entraînement.

— **Environnement** : GPU (NVIDIA RTX 3050) via PyTorch CUDA.

Stratégies supplémentaires :

— **Early Stopping** : arrêt si la validation stagne plus de 3 époques.

— **Learning Rate Scheduler** : réduction du taux d'apprentissage si la loss ne diminue plus.

— **Checkpoint** : sauvegarde du modèle avec la meilleure précision sur validation.

2.1.5 Détails sur l'entraînement

Le processus d'entraînement comprend plusieurs étapes clés :

1. **Prétraitement des images** : Les images sont transformées pour correspondre aux dimensions d'entrée du modèle (`224x224` pixels) et normalisées. Une conversion en niveau de gris est effectuée avant l'entraînement pour adapter le format des images de manière cohérente pour les différentes empreintes.
2. **Création du Dataset** : Le dataset personnalisé `LivDetBinaryDataset` permet de charger et d'organiser les images en fonction de leur label (`Live` ou `Fake`), provenant de différents matériaux et capteurs. Chaque image est associée à un label correspondant (0 pour les empreintes réelles et 1 pour les empreintes falsifiées).
3. **Entraînement avec Early Stopping** : L'entraînement se poursuit jusqu'à un maximum de 50 époques, avec un suivi de la validation via la stratégie d'Early Stopping. Cette stratégie arrête l'entraînement si la perte de validation n'a pas diminué pendant 3 époques consécutives.
4. **Checkpoint** : Le modèle est sauvegardé après chaque époque si la perte de validation s'améliore, ce qui permet de récupérer la meilleure version du modèle pour une évaluation future.

2.2 Évaluation du modèle

2.2.1 Métriques de performance

Afin d'évaluer rigoureusement les performances du modèle **ConvNeXt Tiny**, plusieurs métriques standards issues de la matrice de confusion ont été utilisées :

— **Exactitude (Accuracy)** : proportion de prédictions correctes.

— **Précision (Precision)** : proportion de vraies prédictions positives sur toutes les prédictions positives.

— **Rappel (Recall)** : capacité du modèle à capturer les vraies positives (sensibilité).

— **F1-Score** : moyenne harmonique entre précision et rappel.

Remarque : Le modèle a été entraîné séparément sur chaque capteur (environnement indépendant) et ensuite évalué à la fois sur les données de son capteur d'origine (*intra-capteur*) et sur celles des autres capteurs (*inter-capteur*) afin d'évaluer sa robustesse à la généralisation inter-domaine.

2.2.2 Résultats de validation

Les performances sur les ensembles de validation montrent une convergence rapide et efficace :

TABLE 2.2 – Performances sur l'ensemble de validation (par capteur)

Capteur	Loss Entraînement	Loss Validation	Accuracy
GreenBit	0.0005	0.0006	100.00%
CrossMatch	0.0938	0.0276	98.88%
Digital Persona	0.0130	0.0037	99.75%
Hi_Scan	0.0344	0.0177	99.50%

2.2.3 Résultats de test intra-capteur

L'évaluation directe du modèle sur les données du même capteur que l'entraînement donne :

TABLE 2.3 – Performances du modèle (test sur le même capteur)

Capteur	Accuracy	Precision	Recall	F1 Score	Test Loss
GreenBit	90.08%	0.9311	0.9013	0.9160	–
CrossMatch	98.00%	1.00	0.97	0.99	0.0695
Digital Persona	89.00%	0.92	0.89	0.90	0.5908
Hi_Scan	94.00%	0.96	0.94	0.95	0.2160

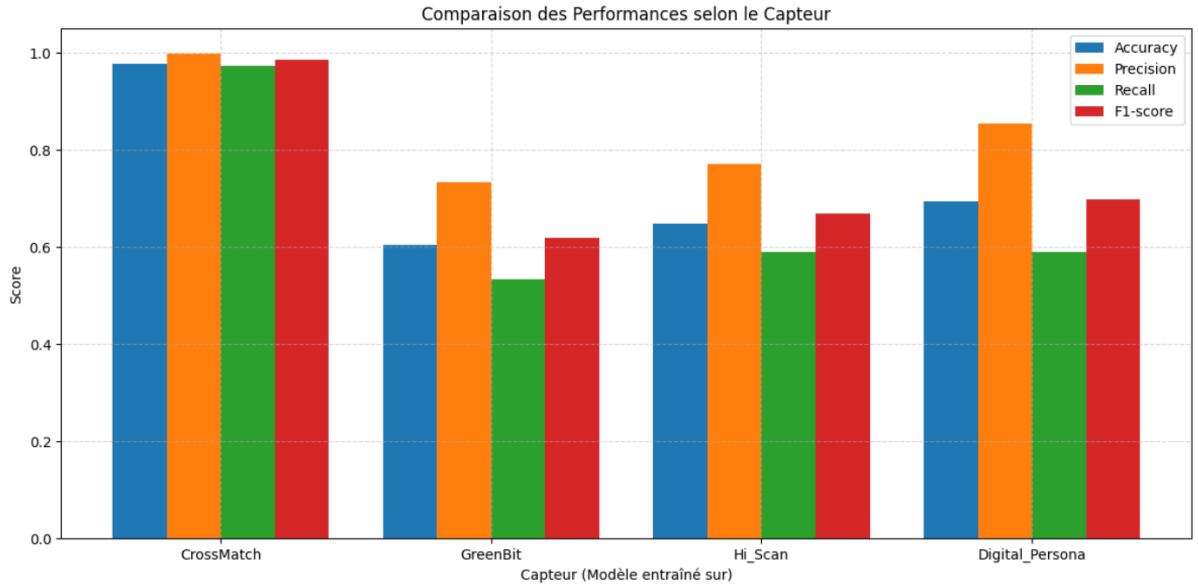


FIGURE 2.2 – Comparaison des Performances selon le Capteur

2.2.4 Évaluation inter-capteur (généralisation)

Nous avons ensuite testé chaque modèle sur les capteurs *non utilisés durant l'entraînement* afin de mesurer sa capacité à généraliser :

TABLE 2.4 – Test croisé entre capteurs (modèle entraîné sur CrossMatch)

Testé sur	Accuracy	Precision	Recall	F1 Score
CrossMatch	97.77%	0.9986	0.9731	0.9857
GreenBit	60.44%	0.7342	0.5340	0.6183
Hi_Scan	64.88%	0.7704	0.5907	0.6687
Digital Persona	69.36%	0.8542	0.5900	0.6979

TABLE 2.5 – Test croisé (modèle entraîné sur GreenBit)

Testé sur	Accuracy	Precision	Recall	F1 Score
GreenBit	90.08%	0.9311	0.9013	0.9160
CrossMatch	78.61%	0.7861	1.0000	0.8802
Hi_Scan	60.04%	0.6003	0.9993	0.7501
Digital Persona	60.00%	0.6000	1.0000	0.7500

TABLE 2.6 – Test croisé (modèle entraîné sur Hi_Scan)

Testé sur	Accuracy	Precision	Recall	F1 Score
Hi_Scan	94.08%	0.9580	0.9427	0.9503
GreenBit	91.60%	0.9743	0.8833	0.9266
CrossMatch	43.76%	0.9682	0.2942	0.4513
Digital Persona	70.56%	0.6851	0.9427	0.7935

TABLE 2.7 – Test croisé (modèle entraîné sur Digital Persona)

Testé sur	Accuracy	Precision	Recall	F1 Score
Digital Persona	88.76%	0.9183	0.8920	0.9050
GreenBit	52.20%	0.9935	0.2047	0.3394
CrossMatch	28.83%	1.0000	0.0946	0.1729
Hi_Scan	54.36%	0.9812	0.2440	0.3908

2.2.5 Interprétation et analyse critique

Les résultats montrent clairement que :

— Les performances sont très élevées dans un contexte **intra-capteur**, prouvant que le modèle apprend efficacement à détecter les empreintes falsifiées pour un capteur donné.

— En revanche, les performances chutent lors de tests **inter-capteurs**, ce qui met en évidence un manque de **généralisation cross-domain**. Cela s'explique par les différences dans les caractéristiques des images produites par chaque capteur (résolution, texture, conditions optiques...).

— Le modèle entraîné sur `Hi_Scan` montre la meilleure robustesse inter-capteurs.

— Le modèle entraîné sur `Digital_Persona` ne généralise pas bien sur les autres, malgré d'excellentes performances internes.

2.3 Interface graphique (GUI)

2.3.1 Objectif

Une interface graphique simple et interactive a été développée pour permettre aux utilisateurs de charger une empreinte digitale et d'obtenir instantanément un diagnostic sur son authenticité (*Live* ou *Fake*). Cette interface permet une interaction fluide avec le modèle de classification pour une identification rapide.

2.3.2 Technologies utilisées

— **Streamlit** : Framework Python pour créer des interfaces web interactives.

— **PyTorch** : Bibliothèque de deep learning utilisée pour charger et exécuter le modèle de classification.

— **TorchVision** : Outils pour les transformations d'images, notamment le redimensionnement et la normalisation.

— **PIL** : Pour la gestion des images, permettant de charger et de manipuler des fichiers image (.png, .bmp).

— **CUDA (GPU RTX 3050)** : Accélération des calculs pour traiter plus rapidement les images et les prédictions.

2.3.3 Architecture

L'application, gérée via le fichier `app.py`, suit les étapes suivantes pour chaque image chargée :

— **Chargement du modèle** : Un modèle pré-entraîné, `ConvNeXt-Tiny`, est utilisé pour la classification des empreintes digitales.

— **Prétraitement de l'image** : L'image est redimensionnée, normalisée, et transformée en tensor pour l'entrée dans le modèle.

— **Prédiction** : Le modèle effectue une prédiction binaire pour déterminer si l'empreinte est *Live* ou *Fake*.

— **Affichage des résultats** : Les résultats de la prédiction, accompagnés du score de confiance, sont affichés dans l'interface avec un message indiquant l'authenticité de l'empreinte.

2.3.4 Interface utilisateur

L'interface utilisateur permet de :

— Importer une image d'empreinte digitale depuis un fichier local.

— Afficher l'image chargée pour permettre à l'utilisateur de vérifier visuellement l'empreinte.

— Lancer l'analyse et afficher le résultat, soit *Live* ou *Fake*, accompagné d'un pourcentage de confiance.

FIGURE 2.3 – Capture de l'interface utilisateur montrant l'upload d'une empreinte digitale et le résultat de la prédiction.

2.4 Perspectives futures

— **Adaptation de domaine** : Améliorer les performances en *CrossSensor* en ajustant le modèle aux spécificités de chaque capteur.

— **Enrichissement des données** : Utiliser l'augmentation de données pour diversifier les conditions de prise et améliorer la généralisation du modèle.

— **Entraînement multi-capteurs** : Développer un modèle capable d'intégrer les données de plusieurs capteurs pour une meilleure robustesse et polyvalence.

— **Déploiement sur mobile** : Permettre l'intégration en temps réel sur des appareils mobiles tout en optimisant la consommation d'énergie et la performance.

— **Apprentissage actif** : Mettre en place un apprentissage continu avec des données en temps réel pour améliorer la réactivité du modèle face à de nouvelles attaques.

— **Réseaux adversariaux (GANs)** : Utiliser les GANs pour générer des empreintes digitales synthétiques réalistes et renforcer l'entraînement du modèle.

Conclusion

Ce projet a abouti à un système performant de détection de fausses empreintes digitales, avec un modèle ConvNeXt Tiny offrant une bonne précision en mode Intersensor. L'interface Streamlit facilite son utilisation et peut être étendue pour d'autres fonctionnalités.

CONCLUSION GÉNÉRALE

Ce travail a permis de proposer une approche de classification des empreintes digitales réelles et falsifiées, en utilisant un modèle ConvNext, dans le but de lutter contre les attaques par falsification. L'analyse des résultats a montré une excellente performance en intra-capteur, où le modèle a su détecter efficacement les empreintes falsifiées. Cependant, une baisse significative des performances a été observée lors des tests inter-capteurs, ce qui soulève un défi majeur en termes de généralisation cross-domain, dû aux différences de caractéristiques entre les capteurs.

L'entraînement du modèle sur le capteur Hi Scan a montré une meilleure robustesse inter-capteurs, tandis que le modèle formé sur Digital Persona n'a pas généralisé efficacement sur d'autres capteurs. Ces résultats mettent en évidence la nécessité de travailler sur la généralisation des modèles pour améliorer leur robustesse face à la variation des caractéristiques des capteurs .

Ce travail ouvre ainsi des perspectives intéressantes pour la mise en place de modèles plus adaptatifs et généralisables, notamment grâce à des techniques d'apprentissage multimodal et l'amélioration de la diversité des données d'entraînement, afin de mieux faire face à la variabilité des capteurs dans des scénarios réels.

BIBLIOGRAPHIE

[1] W. El Atrache, A. Maalouf, S. Yahia *et al.*, *AILearn : An Adaptive Incremental Learning Model for Spoof Fingerprint Detection*, 2020. Disponible sur : https://ieeexplore.ieee.org/document/10126178

[2] T. Michael, *Deep Learning Approaches for Fingerprint Spoofing Detection Using Visual Data*, 2024.

[3] A. Qureshi, R. Khan *et al.*, *Enhancing Fingerprint Liveness Detection Accuracy Using Deep Learning : A Comprehensive Study and Novel Approach*, 2023.

[4] M. Jamal, I. Al-Garadi *et al.*, *Enhancing Fingerprint Authentication : A Systematic Review of Liveness Detection Methods Against Presentation Attacks*, 2024.

[5] R. Singh, A. Sharma *et al.*, *Fingerprint Liveness Detection Using Convolutional Neural Network Based Hybrid Model*, 2022.

[6] S. Akhtar, A. Mian *et al.*, *Fingerprint Spoof Detection : Temporal Analysis of Image Sequence*, 2019.

[7] Y. Ding, D. Maltoni *et al.*, *LIVDET 2021 : Fingerprint Liveness Detection Competition – Into the Unknown*, 2021.

[8] H. Wang, J. Li *et al.*, *RFDforFin : Robust Deep Forgery Detection for GAN-generated Fingerprint Images*, 2023.

[9] S. Purnapatra, C. Miller-Lynch, S. Miner, Y. Liu, K. Bahmani, S. Dey, S. Schuckers, *Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems*, 2023.

[10] Y. Liu, H. Jin *et al.*, *Patch-based Fake Fingerprint Detection Using a Fully Convolutional Neural Network with a Small Number of Parameters and an Optimal Threshold*, 2025.

[11] D. Zhou, X. Meng *et al.*, *Revolutionizing Biometric Security : Advanced Deep Learning Strategies for Fingerprint Anti-Spoofing in High-Risk Applications*, 2025.

[12] T. Karras, M. Aittala, J. Hellsten, S. Laine, J. Lehtinen, T. Aila, *Training Generative Adversarial Networks with Limited Data*, NeurIPS, 2020.

[13] S. Schuckers, G. Cannon, N. Tekampe, *FIDO Biometric Requirements*, FIDO Alliance, 2021. Disponible sur : https://fidoalliance.org/specs/biometric/requirements/

[14] G. Huang, Z. Liu, L. van der Maaten, K. Q. Weinberger, *Densely Connected Convolutional Networks*, CVPR, 2017.

[15] B. Zoph, V. Vasudevan, J. Shlens, Q. V. Le, *Learning Transferable Architectures for Scalable Image Recognition*, CVPR, 2018.

[16] Y. Liu, H. Jin, X. Zhao, *Patch-based Fake Fingerprint Detection Using a Fully Convolutional Neural Network with a Small Number of Parameters and an Optimal Threshold*, 2025.

[17] S. Purnapatra, C. Miller-Lynch, S. Miner, Y. Liu, K. Bahmani, S. Dey, S. Schuckers, *Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems*, 2023.

[18] T. Karras, M. Aittala, J. Hellsten, S. Laine, J. Lehtinen, T. Aila, *Training Generative Adversarial Networks with Limited Data*, in Advances in Neural Information Processing Systems (NeurIPS), 2020.

[19] S. Schuckers, G. Cannon, N. Tekampe, *FIDO Biometric Requirements*, FIDO Alliance, 2021. Disponible sur : https://fidoalliance.org/specs/biometric/requirements/

VERS UNE AUTHENTIFICATION FIABLE : SYSTÈME DE CLASSIFICATION POUR LA DÉTECTION DES EMPREINTES DIGITALES RÉELLES ET FALSIFIÉES

Khaoula BOUGHDIRI

Résumé :

Ce projet vise à développer un système de classification intelligent permettant de différencier les empreintes digitales réelles des empreintes falsifiées. En s'appuyant sur des techniques de Deep Learning, notamment l'architecture ConvNeXt, et en exploitant la base de données de référence LivDet2015, le modèle a été entraîné sur différents capteurs pour garantir sa robustesse face aux attaques par présentation. L'évaluation rigoureuse montre une performance globale satisfaisante, démontrant la capacité du système à résister aux tentatives de contrefaçon biométrique.

Mots-clés : Biométrie, Empreinte digitale, Classification binaire, Deep Learning, ConvNeXt, LivDet2015, Falsification.

Abstract :

This project aims to develop an intelligent classification system capable of distinguishing between real and spoofed fingerprints. Using Deep Learning techniques, particularly the ConvNeXt architecture, and leveraging the benchmark LivDet2015 dataset, the model was trained on multiple sensors to ensure robustness against presentation attacks. The evaluation results demonstrate strong performance, highlighting the model's potential for reliable biometric authentication.

Key-words : Biometrics, Fingerprint, Binary Classification, Deep Learning, ConvNeXt, LivDet2015, Spoofing.