Article	Année	Modeles	Accuracy	DataSets	Points Forts	Limites
AILearn: An Adaptive Incremental Learning Model for Spoof Fingerprint Detection	2020	AILearn (Apprentissage Incrémental basé sur Ensemble Learning) - Handcrafted features : LBP, LPQ, BSIF - Deep features : ResNet-50	Meilleurs résultats : - LivDet2011 : Jusqu'à 93.19% (DigitalPersona - ResNet-50) - LivDet2013 : Jusqu'à 99.02% (Biometrika - ResNet-50) - LivDet2015 : Jusqu'à 94.87% (Biometrika - ResNet-50)	LivDet 2011, LivDet 2013, LivDet 2015 - Empreintes réelles ("Live") et falsifiées ("Spoof") - Capteurs : Biometrika, DigitalPersona, ItalData, Sagem - Différents matériaux de falsification : gélatine, latex, playdoh, silicone, etc.	- Apprentissage incrémental : Adaptation aux nouvelles données sans réentraîner tout le modèle -Séparation des données en Known Fake (KF) et New Fake (NF) pour une meilleure robustesse -Utilisation combinée de caractéristiques locales (LBP, LPQ, BSIF) et profondes (ResNet-50) -Amélioration significative sur les nouvelles attaques (NF) sans perte majeure sur KF -Comparé aux modèles existants, AILearn maintient la stabilité et améliore la plasticité	-Légère perte de précision sur KF lors de l'intégration des nouvelles données (NF) -Les caractéristiques manuelles (LBP, LPQ, BSIF) sont parfois moins performantes que ResNet-50 -Nécessité d'optimiser l'intégration des caractéristiques locales et profondes pour maximiser les performances
Deep Learning Approaches for Fingerprint Spoofing Detection Using Visual Data	2024 - Thomas Micheal-	CNNs : - ResNet - VGG - Inception Hybrid Model : - CNN + LSTM (RNN)	ResNet: 95.6% VGG: 94.1% Inception: 96.3% Hybrid CNN-LSTM: 97.1%	Source des données : - Images de vraies et fausses empreintes digitales collectées sous différentes conditions. Types d'empreintes : - Vraies empreintes digitales de divers	Performances élevées : - Les CNNs surpassent les méthodes classiques de détection d'empreintes falsifiées. - Le modèle hybride (CNN + LSTM) exploite à la fois les caractéristiques spatiales et temporelles, améliorant la robustesse. Techniques avancées de traitement d'image : - Data augmentation (rotation, translation, bruit)	Besoin de larges bases de données : - La performance dépend fortement de la diversité et de la quantité des données utilisées pour l'entraînement. Sensibilité aux conditions environnementales : - Les variations extrêmes de luminosité ou d'humidité peuvent affecter la fiabilité. Complexité et coût

				individus. - Fausses empreintes fabriquées avec des matériaux comme : - Silicone - Gélatine - Latex Conditions de collecte : - Variabilité des conditions d'éclairage - Différents capteurs utilisés (optique et capacitif) - Variabilité des températures et humidités	pour améliorer la généralisation du modèle. - Normalisation et réduction du bruit pour une meilleure extraction de caractéristiques. Détection en temps réel : - Possibilité d'intégrer ces modèles dans des systèmes de reconnaissance biométrique en temps réel.	computationnel : - Les modèles profonds nécessitent des ressources importantes en calcul et en stockage. Risques d'attaques adversariales : - Nécessité de renforcer les modèles contre des attaques sophistiquées qui pourraient tromper le système.
Enhancing Fingerprint Liveness Detection Accuracy Using Deep Learning: A Comprehensive Study and Novel Approach	2023	- Proposé : ResNet50 + Attention, ResNet34 + Attention - Comparés : VGG19, DenseNet121, InceptionV3, Xception	- 97.78% (ResNet50 + Attention) - 95.81% (ResNet34 + Attention) - Inférieur pour VGG19, DenseNet121, InceptionV3, Xception	- LivDet 2021 : 5000 images réelles, 3000 fausses (580 dpi) - ATVS : 4800 images réelles, 4000 fausses (520 dpi)	- Utilisation d'un modèle d'attention séquentielle (Spatial & Channel) pour améliorer l'apprentissage des caractéristiques - Différentes stratégies de pooling testées (Max, Average, Stochastique) → Pooling stochastique donne les meilleurs résultats - Surpasse les modèles CNN classiques en termes de précision - Augmentation de données	- Coût computationnel élevé dû à l'utilisation de ResNet50 avec attention (50 couches) - Dépendance aux paramètres d'entraînement : le taux d'apprentissage et le dropout ont un impact majeur - Besoin d'un dataset varié pour améliorer la généralisation - Possible sur-

					utilisée pour améliorer la robustesse du modèle	apprentissage si le modèle n'est pas bien régularisé
Enhancing Fingerprint Authentication: A Systematic Review of Liveness Detection Methods Against Presentation Attacks	2024	CNN, ResNet, Transformer, IoT-based Multimodal, MCNNs, Edge Descriptor, LBP, RNN, Hybrid Deep Learning	Varie selon le modèle : - Adversarial Liveness Detector (CNNs + Data Augmentation) : 97.77% (LivDet 2021) - LFLDNet (Lightweight ResNet + Transformer) : 95.27% (LivDet 2015) - IoT-Based Multimodal (ECG + Fingerprint) : 99.28% - MFFFLD (MCNNs Fusion de Features) : Supérieur à 97% sur plusieurs benchmarks - Edge Direction Descriptor (SVD + Log-Gabor) : 93.83% (LivDet 2011, 2013) - Low-Rank LBP + LDP : 96.04% (LivDet 2013) - BiRi-PAD (Histogramme des bifurcations de crêtes) : 98.65% (LivDet 2013, 2015) - MFAS (Micro-behavioral Fingerprint Analysis System) : 100% (détection des empreintes légitimes, gummy, et forcées)	LivDet (2011-2021), NUAA, Public Benchmark (13,000 images)	- Amélioration significative de l'accuracy grâce à des approches hybrides et multimodales - Techniques matérielles innovantes pour détecter la vitalité (films COF, transpiration, structures de peau) - Algorithmes avancés de Machine Learning et Deep Learning - Détection efficace contre des attaques sophistiquées (masques, matériaux fins, attaques par marion	- Certains modèles souffrent d'un manque de généralisation sur de nouveaux capteurs et environnements - Problèmes de confidentialité des données dans les systèmes hardware-based - Complexité et coût élevé des modèles multimodaux - Sensibilité aux attaques émergentes (ex. : spoofing ultra-fin)

			- FinAuth (Caractéristiques des touchers de doigts) : 96.04% - CFD-PAD (Channel-Wise Feature Denoising) : 97.5% (LivDet 2017) - Sweat-responsive COF film (détection basée sur la transpiration) : 100% (différenciation empreintes réelles vs fausses)			
Fingerprint Liveness Detection Using Deep Learning	2022	SVM, CNN, CNN+SVM	CNN: 98.16% (Green Bit), 90.00% (Crossmatch), 85.67% (Digital Persona)	LivDet2015	- Comparaison de plusieurs modèles (SVM, CNN, CNN+SVM) - Utilisation d'un dataset de référence - Prétraitement avancé des images (Canny, transformation par ondelettes, extraction de caractéristiques) - Forte amélioration de la précision avec CNN	- SVM seul montre une faible précision (~51%) - CNN+SVM n'apporte pas une amélioration significative par rapport à CNN seul - Nécessité d'un gros volume de données pour l'entraînement CNN
Fingerprint Spoof Detection: Temporal Analysis of Image Sequence	2019	CNN-LSTM (MobileNet-v1 + Bi-LSTM)	99.25% (connus) 86.20% (cross-matériaux) @ FDR = 0.2%	26,650 images live (685 sujets), 32,910 images spoof (7 matériaux, 14 variantes)	- Analyse temporelle pour détecter des indices dynamiques (perspiration, changement de couleur, distorsion de la peau). - Utilisation de minutiae-based local patches pour améliorer la détection. - Amélioration des performances par rapport à l'état de l'art.	- Peut nécessiter du temps d'entraînement élevé. - Certains doigts vivants peuvent ne pas montrer ces phénomènes (peau sèche). - Certaines empreintes falsifiées peuvent imiter les distorsions de la peau réelle.

Fingerprint Liveness Detection Using Convolutional Neural Network Based Hybrid Model	2022	Xception, InceptionV3, SVM avec LPQ, LBP, BSIF	- ATVS-FFp-DB : → SVM seul : 89.8% (BSIF), 85.6% (LPQ), 87.5% (LBP) → Xception seul : 82.9% → InceptionV3 seul : 77.86% → Proposed CNN Model (Hybrid) : 99.6% - SOCOFing : → SVM seul : 83.7% (BSIF), 81.8% (LPQ), 80.5% (LBP) → Xception seul : 71.43% → InceptionV3 seul : 71.19% → Proposed CNN Model (Hybrid) : 99.35%	ATVS-FFp-DB, SOCOFing	- Intégration de CNN et de descripteurs de texture - Haute précision avec combinaison des méthodes - Amélioration significative par rapport aux modèles existants	- Performance variable selon le dataset - Dépendance aux descripteurs de texture - Complexité computationnelle
La reconnaissance automatique des empreintes digitales	2016	EFinger (Min Distance, Image Mapping, Quad Tree)	Variable : Min Distance (~3s pour 40 empreintes), Image Mapping (~6,44 min), Quad Tree (~1,8s)	Base de données contenant 40 empreintes	Méthode Min Distance rapide, Quad Tree rapide pour certaines comparaisons	Quad Tree moins performant en précision, Image Mapping très lent avec grande base
		Réseaux de neurones (MLP avec Backpropagation)	100%	100 images (50 entraînement, 50 test)	Apprentissage efficace, précision très élevée	Nécessite un bon prétraitement des images, pas testé sur de plus grandes bases de données
		Algorithme basé sur minuties et recherche de coordonnées dans SQLite		Base de 82 personnes	Rapide et optimisé pour recherche d'empreintes	Dépend fortement de la qualité des minuties extraites

LIVDET 2021 FINGERPRINT LIVENESS DETECTION COMPETITION-INTO THE UNKNOWN	2021	Deep Learning, Hybride, Hand-crafted	Jusqu'à 99.75% (*megvii_ensemble*)	Green Bit, Dermalog	- Meilleure précision avec les modèles Deep Learning. - Introduction du test ScreenSpoof pour des attaques plus réalistes. - Comparaison entre méthodes consensuelles et semi-consensuelles. - Bonne compacité des features (megvii_single : 64 dimensions).	- Réduction de performance face aux attaques "never-seen-before" (ex. ScreenSpoof). - Modèles Deep Learning nécessitant plus de données d'entraînement. - Déséquilibre entre FNMR et FMR pour certains modèles.
Patch-based Fake Fingerprint Detection Using a Fully Convolutional Neural Network with a Small Number of Parameters and an Optimal Threshold	2025	Fully Convolutional Neural Network (FCN) basé sur le module Fire de SqueezeNet	98.65% (ACE moyen de 1.35%)	LivDet 2011, 2013, 2015	- Classification en trois classes (live, fake, background) sans prétraitement - Utilisation de patchs pour éviter la réduction de taille des empreintes - Nombre réduit de paramètres (~2.0 MB) - Détection optimisée par seuil optimal	- Performances variables selon le type de capteur - Détection plus difficile pour les matériaux inconnus - Sensible à la qualité des empreintes
Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems	2023	DenseNet-121, DenseNet-121 (Keras), NasNetMobile (Keras)	- DenseNet-121 : APCER 0.14%, BPCER 0.18% - DenseNet-121 (Keras) : APCER 1.55%, BPCER 3.64% - NasNetMobile : APCER 3.22%, BPCER 9.04%	Nouveau dataset PAD avec 7500 images de quatre doigts, 14 000 images de doigts segmentés, 10 000 empreintes synthétique	- Développement d'un dataset PAD conforme aux normes FIDO et ISO - Utilisation de CNN avancés pour la détection des attaques par présentation - Comparaison des performances des modèles sur des attaques connues et inconnues	-Faible performance sur les attaques par impression photo (APCER 79.01%) - Dataset encore en cours de collecte - Besoin de plus de données pour améliorer la généralisation aux attaques inconnues
Etude d'un système	2005	- Algorithmes basés sur les	EER entre 0.063 et 0.126 selon la méthode	- BDS0, BDS1, BDS2, BDS3,	- Approche multi-algorithmes permettant une	- Performances inférieures aux méthodes

complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage		minuties (extraction classique et extraction directe) - Filtrage spatial directionnel avec filtres de Gabor et Log-Gabor - Masquage fréquentiel directionnel		BDS4 (bases synthétiques) - Base d'empreintes réelles acquises via le capteur étudié	analyse comparative des performances - Prise en compte des distorsions dues à l'acquisition (facteur d'échelle, alignement) - Tests sur des bases synthétiques et réelles pour évaluer la robustesse	de l'état de l'art - Tests limités sur une seule base réelle, manquant de diversité - Absence d'implémentation matérielle du système final
RFDforFin: Robust Deep Forgery Detection for GAN-generated Fingerprint Images	2023	- CNNDetection [43] (ResNet-50) - LNP-based Classifier [28] (extraction de bruit haute fréquence) - DCTAnalysis [13] (analyse des artefacts en domaine fréquentiel avec DCT) - RFDforFin (Proposé) (fusion de caractéristiques des crêtes et artefacts FFT)	- 100% (original) - 99.5% (après attaque anti-forensic SDN++)	- PolyU-HRF (réel, 1480 images) - L3-SF (faux, 1480 images générées avec CycleGAN)	-Approche spécialisée pour la détection des empreintes GAN-générées (contrairement aux méthodes générales). - Architecture en deux flux : 1) *Ridge stream* : extrait les variations en niveaux de gris le long des crêtes d'empreintes. 2) *Generation artifact stream* : analyse les artefacts des GANs en utilisant FFT. -Faible complexité : 94.8K paramètres (contre 23.5M pour CNNDetection). -Meilleure robustesse aux attaques anti-forensic (SpectralGAN++, SDN++).	-Vulnérabilité variable aux attaques anti-forensic : bien que robuste, la performance diminue légèrement après correction des spectres (SpectralGAN++ et SDN++). -Chaque flux individuellement est moins efficace : Le *ridge stream* seul a une accuracy plus faible. -Spécifique aux empreintes digitales : moins généralisable aux autres types d'images deepfake.
Revolutionizing Biometric Security: Advanced Deep	2025	CNN-GAN (ResNet-50 pour extraction de caractéristiques,	92.8%	SOCOFing (6000 empreintes, 600 sujets)	Haute précision, robustesse aux attaques inconnues, temps d'inférence rapide (6	Sensible à la qualité des images d'entrée, erreurs dues au bruit et distorsions, amélioration

Learning Strategies for Fingerprint Anti-Spoofing in High-Risk Applications		CycleGAN pour génération de données)			ms), amélioration avec données synthétiques	possible via techniques adaptatives