Algorithmes de détection des attaques de présentation

Durée : 6 mois

Début : Février 2026

Contexte scientifique

L'objectif de ce projet est de développer un système capable de détecter les attaques biométriques faciales afin d'éviter l'usurpation d'identité lors de la présentation de documents officiels. Le système devra reconnaître les masques 2D et 3D, les vidéos et les photos imprimées (Fig. 1), tout en se concentrant particulièrement sur la détection de masques 3D. L'approche la plus prometteuse pour contrer ces attaques repose sur la détection du vivant. En particulier, la méthode de remote photopléthysmographie (rPPG) a montré des résultats très intéressants.

FIGURE 1 – Différentes attaques faciales.

Objectifs du stage

L'étudiant·e va étudier et adapter le modèle proposé par Jiang et al. [1] au contexte des signaux rPPG. Ensuite, une validation des résultats sera réalisée à l'aide des bases de données 3DMAD et Replay-Attack, en intra et cross-validation, suivie d'une comparaison des performances avec l'état de l'art (TS-rPPG, CFrPPG, TransRPPG).

Objectifs secondaires

Dans un second temps, on veut changer l'entrée de ce modèle afin d'exploiter des ST-maps plutôt qu'un signal unique.

Méthodologie et plan technique

Phase 1 : Compréhension de l'article et du modèle de référence.
Phase 2 : Analyse du code existant.
Phase 3 : Exploitation des signaux rPPG comme entrée du modèle.
Phase 4 : Validation expérimentale des résultats.
Phase 5 : Extension du modèle avec des ST-maps multi-régions.
Phase 6 : Comparaison des modèles rPPG et ST-maps.
Phase 7 : Rédaction du rapport final.

Résultats attendus et portée scientifique

Ce travail propose une approche robuste aux attaques de présentation rares, notamment celles impliquant des masques 3D. On prévoie d'améliorer la capacité de généralisation des modèles grâce à la détection d'anomalies et à l'exploitation de ST-maps.

Profil recherché

Étudiant·e de Master 2 ou d'école d'ingénieur (Machine Learning, IA, Mathématiques appliquées ou domaines connexes), disposant de bonnes bases en probabilités et en apprentissage automatique. Intérêt pour la biométrie, la détection du vivant (rPPG) et les méthodes de détection d'anomalies.

Compétences souhaitées :	Python, deep learning.
Laboratoire :	GIPSA-lab
Contacts :	Maria Oliver-Parera (maria.oliver.parera@gipsa-lab.grenoble-inp.fr) Patricia Ladret (patricia.ladret@gipsa-lab.grenoble-inp.fr)
Début	Février 2026
Durée	6 mois

Références

[1] Aofan Jiang, Chaoqin Huang, Qing Cao, Yuchen Xu, Zi Zeng, Kang Chen, Ya Zhang, and Yanfeng Wang. Self-supervised anomaly detection pretraining enhances long-tail ecg diagnosis. *arXiv preprint arXiv :2408.17154*, 2024.