Thème de recherche	**Détection des deepfakes audio adverses**
Poste (H/F)	Doctorant
Référence de l'offre	SN/NE/PhD/PEPR2/072024
Département de Recherche	Sécurité Numérique (SN)
Date de publication	04/07/2024
Date d'embauche	Poste à pourvoir de suite
Durée du contrat	Durée de la thèse

Description

La conception de solutions fiables et robustes pour la détection des deepfakes est une bataille permanente contre les acteurs malveillants. Une fois qu'une nouvelle stratégie ou un nouvel algorithme d'attaque est identifié et que la solution de détection est correctement mise à jour, les acteurs malveillants peuvent concevoir de nouvelles attaques pour surmonter le nouveau détecteur. Les attaques deviennent naturellement de plus en plus sophistiquées et de nature adverse. Même si les attaques deepfake actuellement connues sont déjà adverses, à quelques exceptions notables près, elles ont été étudiées dans un scénario purement biométrique, alors qu'elles peuvent être conçues pour cibler à la fois les systèmes biométriques et le détecteur d'usurpation.

Cette thèse étudiera une nouvelle génération d'attaques adverses conçues pour tromper à la fois un système de biométrie vocale et un détecteur d'usurpation. En commençant par une sélection de détecteurs à l'état de l'art, nous concevrons des techniques de post-traitement pour supprimer les distorsions et les artefacts dans les signaux audios générés artificiellement (parole synthétique / convertie). Ce travail exposera la vulnérabilité des solutions existantes à des attaques plus adverses. En s'appuyant sur les concepts d'apprentissage adversarial, la deuxième étape consistera à concevoir des approches de détection qui capturent les caractéristiques des signaux de la parole que même les approches de synthèse et de conversion à l'état de l'art ne modélisent pas bien et qui ne peuvent pas être supprimées ou atténuées. Étant donné que l'apprentissage adversarial est généralement très exigeante en termes de calcul et peut aboutir à des modèles encore plus complexes que ceux utilisés actuellement, nous sommes également intéressés à étudier les techniques comme la distillation des connaissances, les réseaux enseignant-étudiant ou le `gradient flow preservation pruning', pour réduire la complexité des modèles. Le but est d'apprendre des modèles efficaces et moins complexes qui sont plus adaptés aux applications pratiques.

Le candidat retenu rejoindra le groupe "Sécurité audio et vie privée" au sein du département "Sécurité numérique" d'EURECOM. Vous travaillerez sous la supervision des Profs. Nicholas Evans et Massimiliano Todisco et avec le Prof. Driss Matrouf au Laboratoire d'Informatique Avignon (LIA), et il y aura des opportunités de collaboration internationale, par exemple avec les membres du comité d'organisation d'ASVspoof. Le poste est financé par le Programme prioritaire de recherche et d'équipement (PEPR) en cybersécurité de l'Agence nationale de la recherche (ANR).

[1] "ASVspoof 5 Evaluation Plan", Hector Delgado, Nicholas Evans, Jee-weon Jung, Tomi Kinnunen, Ivan Kukanov, Kong Aik Lee, Xuechen Liu, Hye-jin Shim, Md Sahidullah, Hemlata Tak, Massimiliano Todisco, Xin Wang, Junichi Yamagishi, ASVspoof consortium, 2024 https://www.asvspoof.org/file/ASVspoof5___Evaluation_Plan_Phase2.pdf

Prérequis

- Niveau d'études / diplôme : Maîtrise
- Domaine / spécialité : Informatique, Intelligence Artificielle, Traitement de la parole, Détection de Deepfake
- Technologies / langages / systèmes : apprentissage automatique, apprentissage profond, Python et PyTorch
- Autres compétences / spécialités : solides compétences en mathématiques, en analyse, en résolution de problèmes, en communication et en rédaction.
- Autres éléments importants : un excellent parcours académique, la maîtrise de l'anglais.

Dossier de candidature
Les candidatures doivent être accompagnées de :

- Curriculum Vitae détaillé,
- Liste des publications en précisant les trois publications les plus importantes,
- Document de deux pages présentant les perspectives de recherches et d'enseignement du candidat,
- Noms et adresses de trois références.

Le tout est à adresser à secretariat@eurecom.fr sous la référence **SN/NE/PhD/PEPR2/072024**

A propos d'EURECOM
EURECOM est une grande école d'ingénieurs et un centre de recherche en sciences du numérique fondé en 1991 sous la forme d'un GIE, dans la technopole internationale de Sophia Antipolis. L'Institut Mines-Télécom est membre fondateur du GIE. Les activités d'enseignement et de recherche sont organisées autour de 3 thématiques porteuses : sécurité numérique, systèmes de communication et Data Science.

L'institution accueille 150 salariés, chercheurs et administratifs et 400 étudiants internationaux dans ses locaux situés sur le Campus Sophia Tech, le plus grand campus en sciences et technologies de l'information des Alpes Maritimes. EURECOM bénéficie d'un environnement géographique privilégié sur la Côte d'Azur, entre mer et montagne, au cœur d'un écosystème dynamique et pluridisciplinaire qui encourage l'innovation scientifique et technologique de haut niveau.

Avantages sociaux
- Environnement international et multiculturel
- Salaire attractif - Épargne salariale
- Retraite par capitalisation (100% employeur)
- Accord d'Intéressement
- Mutuelle d'entreprise (contrat familial - hauts niveaux de garanties) - 60% employeur
- Prime annuelle de performance
- Titres-restaurant (60% employeur)

EURECOM fait partie des meilleures écoles d'ingénieurs européennes en sciences des technologies numériques. Elle est située au cœur de la Côte d'Azur, au sein de la Silicon Valley européenne (Tech Park Sophia-Antipolis). Les équipes de recherche d'EURECOM évoluent dans un environnement international et multiculturel.

EURECOM mène une politique dynamique en termes **d'inclusion et de qualité de vie au travail**. Nous nous engageons pour la diversité et accordons la même considération à toutes les candidatures, sans discrimination. Nous recherchons avant tout la compétence et l'esprit d'équipe.

Tous nos postes sont ouverts aux **personnes en situation de handicap.** EURECOM est doté d'un référent handicap afin d'accompagner, de conseiller, d'organiser les éventuels aménagements et de prendre des engagements positifs en faveur d'une intégration personnalisée.

EURECOM, dans le cadre de son **plan d'égalité femmes/hommes**, encourage la mixité dans ses équipes. Notre plan d'action en faveur de cette mixité prévoit que nous encouragions les candidatures masculines pour les postes administratifs, postes traditionnellement occupés par des femmes, et les candidatures féminines dans les postes en informatique et recherche, postes traditionnellement occupés par des hommes.

EURECOM mène des actions positives dans le cadre de sa **politique RSE**. Un référent RSE pilote la politique d'EURECOM en matière de RSE et de transition énergétique (bornes de recharge électrique, panneaux solaires, tri sélectif…).

Site web EURECOM : https://www.eurecom.fr/fr/eurecom/presentation
EURECOM en VIDEO : https://www.youtube.com/watch?v=uIlFcgNijnM
Expériences collaborateurs :
https://www.youtube.com/watch?v=gITWTVRgLpc
https://www.youtube.com/watch?v=BHv9zIduzuQ
https://www.youtube.com/watch?v=hvbzzCBups8