Research topics	**Detection of adversarial audio deepfakes**
Position (M/F)	PhD studentship
Reference offer	SN/NE/PhD/PEPR2/072024
Research Department	Digital Security (SN)
Publication date	04/07/2024
Start date	Sept./Oct. 2024
Duration	Duration of the thesis

Description

The design of reliable, robust solutions for the detection of deepfakes is a continuous arms race with the fraudsters. Once a new deepfake attack is identified and the detection solution is appropriately updated, the fraudster can design new attacks to overcome the new detector. Attacks are naturally becoming more sophisticated and adversarial in nature. Those seen thus far are typically designed to overcome a single classifier, perhaps an automatic speaker verification sub-system or a deepfake detection sub-system. We aim to explore and improve upon the resilience of spoofing robust speaker verifications systems to attacks which are designed to manipulate both sub-systems.

This thesis will study a new generation of adversarial attacks designed to fool both a voice biometric system and a deepfake spoofing detector. Starting with a selection of state-of-the-art detectors, we will design post-processing techniques to suppress the distortions and artefacts in speech signals that are generated using text-to-speech (TTS) and voice conversion (VC) algorithms. This work will establish the vulnerability of existing solutions to more adversarial attacks. Building on the concepts of adversarial training, the second stage will be to design alternative detection approaches that detect speech attributes that even state-of-the-art TTS and VC approaches do not model well and which cannot be removed or attenuated through adversarial post-processing. Since adversarial training is typically highly demanding in terms of computation and may result in even more complex models than those used currently, we are also interested to study knowledge distillation and other model complexity reduction techniques, e.g. in the form of teacher-student networks or gradient flow preservation pruning, to reduce complexity and to help learn efficient models suited to practical applications.

The successful candidate will join the Audio Security and Privacy Group within EURECOM's Digital Security Department. You will work under the supervision of Profs. Nicholas Evans and Massimiliano Todisco and with Prof. Anthony Larcher at the Laboratoire d'Informatique de l'Université du Mans (LIUM), and there will be opportunities for international collaboration, e.g. with members of the ASVspoof organising committee. The position is funded by the French National Research Agency (ANR) Cybersecurity Priority Research and Equipment Programme (PEPR).

[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

Requirements

- Education Level / Degree : Master's degree
- Field / specialty: Computer Science, Artificial Intelligence, Speech Processing, Deepfake Detection
- Technologies / languages / systems: machine learning, deep learning, Python and PyTorch
- Other skills / specialties: strong mathematics, analytical, problem solving, communications and writing skills
- Other important elements: an excellent academic track record, proficiency in English

Application

The application must include:

- Detailed curriculum,
- Motivation letter of two pages also presenting the perspectives of research and education,
- Name and address of three references.

Applications should be submitted by e-mail to secretariat@eurecom.fr with the reference:
SN/NE/PhD/PEPR2/072024

About EURECOM

EURECOM is a major Engineering School and a Research Center in digital sciences founded in 1991 as a consortium in the international technology park of Sophia Antipolis. The IMT is a founding member of the GIE. Teaching and research activities are organized around 3 promising fields: digital security, communication systems and Data Science.

EURECOM has a staff of 150 (researchers and support teams) and welcomes 400 international students on the Campus Sophia Tech, the largest information science and technology campus of the region. EURECOM enjoys a privileged geographical environment on the French Riviera (Côte d'Azur), between sea and mountains, at the heart of a dynamic and multidisciplinary ecosystem that promotes high-level scientific and technological innovation.

Social advantages

- International and multicultural environment
- Attractive salary - Corporate saving plans
- Private retirement plan (executive, employer participation of 100%)
- Employee profit sharing policy
- Company health insurance (mutuelle) with high levels of guarantees for the whole family (employer participation of 60%)
- Restaurant vouchers (employer contribution of 60%)

EURECOM is one of Europe's leading engineering schools specializing in digital technologies. It is located in the heart of the Côte d'Azur, in Europe's Silicon Valley (Tech Park Sophia-Antipolis). EURECOM's research teams work in an international, multicultural environment.

EURECOM has a dynamic policy in terms of **inclusion and quality of life at work**. We are committed to diversity and give equal consideration to all applicants, without discrimination. Above all, we look for competence and team spirit.

All our positions are open to **people with disabilities**. EURECOM has set up a disability advisor to provide support and advice, organize accommodation and make positive commitments to personal integration.

As part of its **gender equality plan**, EURECOM encourages gender diversity within its teams. As part of our gender equality action plan, we encourage male applications for administrative positions, traditionally held by women, and female applications for IT and research positions, traditionally held by men.

EURECOM is taking positive action as part of its **CSR policy**. A CSR representative oversees EURECOM's CSR and energy transition policies (electric charging stations, solar panels, waste sorting, etc.).

Web site EURECOM: https://www.eurecom.fr/fr/eurecom/presentation
EURECOM in VIDEO: https://www.youtube.com/watch?v=uIlFcgNijnM
Employee experience:
https://www.youtube.com/watch?v=gITWTVRgLpc
https://www.youtube.com/watch?v=BHv9zIduzuQ
https://www.youtube.com/watch?v=hvbzzCBups8