Mitek Systems/ID R&D — Research Intern Project

Project Description

Static photo detection

Paid: 1200 euro/month

Project Abstract

When someone attempts to fool a face recognition system by presenting a photo, video, mask, or other facsimile of a real person's face, it's known as a "spoofing" attack. Facial liveness detection aims to defend against these attacks by verifying that the presented face is not a static image or video but belongs to a live, present individual.

One of the modules working in our Attack Detector is designed to catch an attept to demonstrate a static object like printed photo insead of the face. The algorithm takes 2 photos made with some time interval. When injecting, an attacker often uses a static image, slightly changing it over time (by moving/scaling/applying filters). In this project, it is proposed to improve our current developments and create a model that will accurately determine whether the presentation is a static picture.

Qualifications and Educational Preferences

- Experience in computer vision, machine learning, image processing

- Good Python3 programming skills.
- Good written and spoken English
- Experience in one or more deep learning frameworks: Tensorflow, Pytorch.
- Familiarity with Linux/Docker/Git
- A willingness to learn and strong communication skills

What You Will Do

Design and implement an algorithm which takes two RGB images with face as input and returns a score representing a probability that the presented object is an alive face or a printed photo of the face. You will be provided with training dataset, evaluation dataset, workstation for algorithm training, and full supervision on what approach to be implemented as well as guidance on each step.

The algorithm will be based on the machine learning approach including CNNs (Convolutional Neural Networks), ViT (Visual Transformers), but not limited ones.

Prepare a presentation to communicate your findings, showing how your algorithm enhances the ability of facial recognition systems to defend against spoofing attacks.

About Company

ID R&D (a Mitek Systems company) is a cutting-edge machine learning company that has recently opened its office in Barcelona. We are committed to pushing the boundaries of AI and biometrics. We encourage our team members to engage in scientific publications based on their work and actively participate in challenges. In fact, our teams were rated in the top 10 for Kaggle Deepfake detection, showcasing our expertise and dedication to excellence.

You can find more information on our latest Tech developments on our website: www.idrnd.ai and on our LinkedIn profile: www.linkedin.com/company/idr&d.

Contacts:

If you are interested in this project, write to Oscar Cabo<ocabo@miteksystems.com> or Olga Kozyukhina <olga.kozyukhina@idrnd.net>

Abstract	Our Injection Attack Detector detector takes 2 photos with some interval. When injecting, an attacker often uses a static image, slightly changing it over time (by moving/ scaling/ applying filters). In this project, it is proposed to improve our current developments and create a model that will accurately determine whether the injection is a static picture.
Extended abstract:	Link to pdf
Academic Supervisor:	<Denis Kondranin?>
Supervisor e-mail:	<e-mail?>
Company:	Mitek Systems
Contact Person:	Olya Kozyukhina, Oscar Cabo
Contact e-mail:	olga.kozyukhina@idrnd.net ocabo@miteksystems.com
Confidential:	Yes
Date:	TBD <we're flexible, minimum 3-month duration>