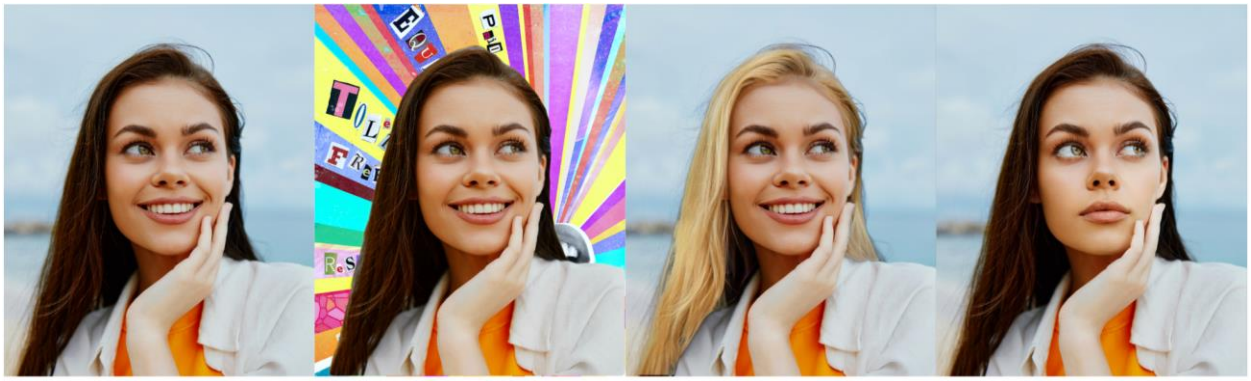
Mitek Systems/ID R&D — Research Intern Project



Original | Background Changed | Hair Color Filter | Expression Filter

Project Description

Research of Black-Box Adversarial Attacks on Computer Vision Systems

Paid: 1200 euro/month

Project abstract

When someone attempts to fool a face recognition system by the using digital image transformations (color distortions, compression, geometric transforms, filters, etc), it's known as a "spoofing" attack. Facial liveness detection aims to defend against these attacks by verifying that the presented image is not a transformed image or video but is an alive, original photo of face.

Each transformation incorporates numerous parameters that can't feasibly be iterated over within a practical time frame. To fortify the final ensemble and enhance its resilience, it's crucial to scrutinize all transforms that could potentially pose a threat.

In this project, we propose the construction of a Reinforcement Learning system designed to emulate real-world scenarios for evading machine learning systems.

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

Propose a structure for a reinforcement learning system that can simulate real-world scenarios of attempts to evade facial liveness systems. Using the reinforcement learning system, simulate different image transformations, taking into consideration the multiple parameters each transformation can have. Evaluate the performance of the system in detecting these transformations.

Optimize and Iterate: continuously refine the reinforcement learning system, iterating over different transformations and making adjustments to improve detection effectiveness.

Prepare a presentation to communicate your findings, showing how the reinforcement learning system 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>