Jan Čech
Center for Machine Perception
Department of Cybernetics, Faculty of Electrical Engineering
Czech Technical University in Prague

Master's Thesis Review

Prague, January 23, 2024

Title: Synthetic Image Detection
Author: Nela Petrželková
Date received: January 9, 2024

The thesis presents an experimental study on detecting synthetic images of faces, a.k.a. "deep fakes". Due to the remarkable progress of recent image generators, it is virtually impossible for a human to distinguish synthetic images from real photos. The study reveals several interesting insights and findings that were not obvious at the beginning of the research and have not been described in the literature. It was found that a simple model of a standard ResNET-50 architecture trained on a specific image generator achieves near perfect accuracy in separating synthetic and real images, and the model also handles common image distortion (reduced resolution, compression). Partial manipulations, when a synthetic image is blended into a real one, are precisely localized with a standard YOLO architecture. However, it was found that the model is vulnerable to adversarial attacks, and the model does not generalize to generators unseen during the training. As tested, failure to generalize to newer generators also occurs for state-of-the-art models, which indicates that the problem is far from being solved despite active research in recent times.

The problem is certainly not trivial. Nela performed an extensive set of quantitative experiments. She collected her own dataset running the recent diffusion model generator (Stable diffusion – Realistic Vision), trained several recognition models, and tested them in a cross-generator setting and over various image distortions. She experimented with adversarial attacks on the model, both in preparing and defending the attacks. She implemented partial image manipulations using the inpainting method and trained another model for localization. This is a regular research topic, and Nela handled it very well. We are about to submit the main results of the thesis to an international conference.

Nela worked on her thesis systematically. We were meeting regularly, usually once a week. Nela was always well prepared, having her experiments well documented and organized. Nela was very proactive in asking meaningful questions and proposing her own solutions to the challenges she encountered. Nela easily reads scientific papers and is able to run third-party models and adapt related codes. She is indisputably competent in recent deep machine learning techniques for both image synthesis and image analysis. She was working hard and dedicated many hours to the project. She was willing to prepare additional/optional experiments that exceed the thesis assignment, in order to provide a comprehensive view of the problem.

I have been working with Nela for more than three years. I was also her bachelor thesis advisor. Although her bachelor thesis (on face image editing) was defended as A–excellent, I can clearly confirm that Nela made further professional progress afterwards. I believe she is now a competent engineer and a promising researcher.

It was a pleasure for me to work with Nela. I believe Nela presented an outstanding thesis with original research results and therefore I suggest assessment

A – excellent.

Ing. Jan Čech, Ph.D.
Thesis Advisor