ALTERED FACE RECOGNITION USING MACHINE LEARNING

- Face recognitions is a well known task of machine learning
- This task becomes more complicated the more degrees of freedom are considered, such as
  - Age, facial hair, hairstyle, glasses or tattoos
- Tuning parameters and adapting the Transformer structure heavily influence learning process and therefore the detection
- The contents of the thesis are
  - Improving the learning process and structure of a Transformer
  - Evaluating the influence of parameters, such as
    - Sample size, image count and age span
  - Reference paper: ViTAE v2
  - Existing Dataset: MORPH Face Recognition Dataset

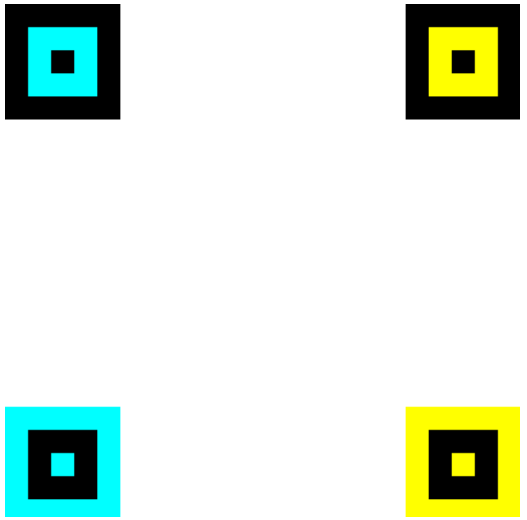
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer*in: MF
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

OBJECT RECOGNITION THROUGH VISIBLE COLOR PATTERN

- Plug and Play solution for "discovering" offline objects in images and videos
- Develop a robust method that uses visible color patterns to make objects discoverable for digital devices (video, image).
- In the Thesis
  - n ≥ 4 different color patterns are to be created, which can be robustly recognized by neural /deep learning
  - Post-processing (dewarping, rotation, etc.) of the recognized space enclosed by the color patterns for further use (OCR or similar)
  - A good starting point is for example



ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer*in: JH
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

ADVERSARIAL ROBUSTNESS OF OPTICAL CHARACTER RECOGNITION (OCR)

- Misinformation is spread on social media by posting images containing text. Automatic systems need to use OCR to detect such posts.
- Smartphone banking apps offer automatic scanning of invoices. Relevant information can be tampered with by an attacker.
- Most OCR systems using DNNs are vulnerable to adversarial examples which are indistinguishable to the human eye.
- The goal of the thesis is to
  - Conceptualize and implement a method which detects such adversarial examples
    - Evaluate the concept on common OCR attack methods
  - A good starting point is for example https://www.sciencedirect.com/science/article/abs/pii/S2214212622000552

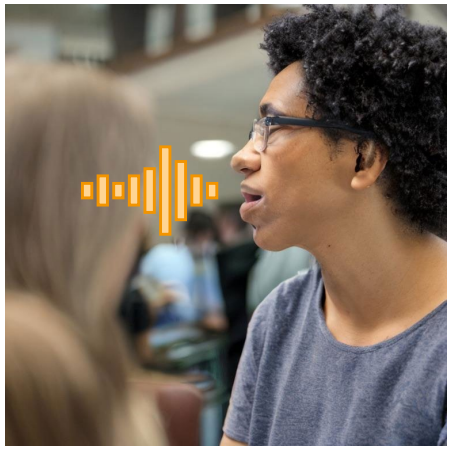
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer*in: SB
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

ROBUSTNESS OF AUDIO DEEPFAKE DETECTION METHODS

- New synthesis methods can be used to alter the spoken information contained in audio recordings and video soundtracks
- Current state-of-the-art detection methods can achieve high accuracies but their robustness against common audio post-processing (e.g., compression, band-pass filtering), operations have not been investigated
- The goals of this thesis are:
  - To analyze the robustness of state-of-the-art detection methods on post-processed audio deepfakes
  - To provide an implementation of a classification system that can improve the robustness
- Earlier work regarding the detection of audio deepfakes:
  - https://ui.adsabs.harvard.edu/link_gateway/2022arXiv220316263M/EPRINT_PDF



Stable Diffusion

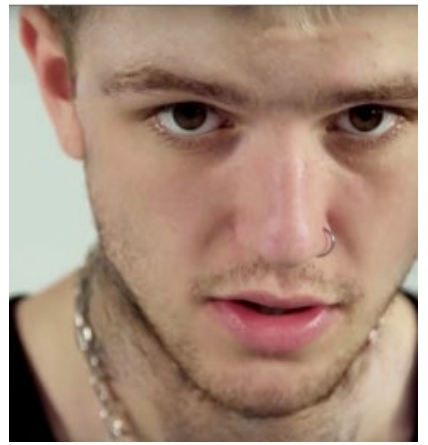
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: RF, SZ
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

DETECTING SYNTHETIC IMAGE CONTENT CREATED BY „INPAINTING“

- Detail in digital images can be enhanced or created using ML-based image synthesis methods in terms of „inpainting“. Such enhancements can be applied for malicious purposes such as forging digital evidence or distributing fake news
- Current methods for identifying inpainting feature varying detection performance with respect to different image inpainting algorithms
- The goals of this thesis are:
  - To analyze the shortcomings of current detection algorithms for “inpainting”
  - To improve the forgery detection performance by exploiting common characteristics of a selection of synthesis algorithms
- Earlier work regarding the detection of splicing boundaries:
  - https://openaccess.thecvf.com/content_CVPR_2020/papers/Li_Face_X-Ray_for_More_General_Face_Forgery_Detection_CVPR_2020_paper.pdf



https://www.reddit.com/r/LilPeep/comments/j4c1uz/tattooless_peep_using_the_nvidia_image_inpainting/

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: RF, SZ
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

DETECTING SYNTHETIC IMAGES CREATED BY „FULL IMAGE SYNTHESIS“

- Digital images can be created using ML-based image synthesis. In contrast to „inpainting“ *full* images can be synthesized from scratch in a photorealistic appearance. Such enhancements can be applied for malicious purposes such as making up digital evidence or fake news
- Current methods for “full image synthesis” identification feature varying detection performance with respect to different image synthesis algorithms
- The goals of this thesis are:
  - To analyze the shortcomings of current detection algorithms for “full image synthesis”
  - To implement a detection method exploiting characteristics of a selection of synthesis algorithms to improve the forgery detection performance
- Earlier works regarding the annotation of synthetically generated images:
  - https://arxiv.org/pdf/2211.00680v1.pdf

openai.com

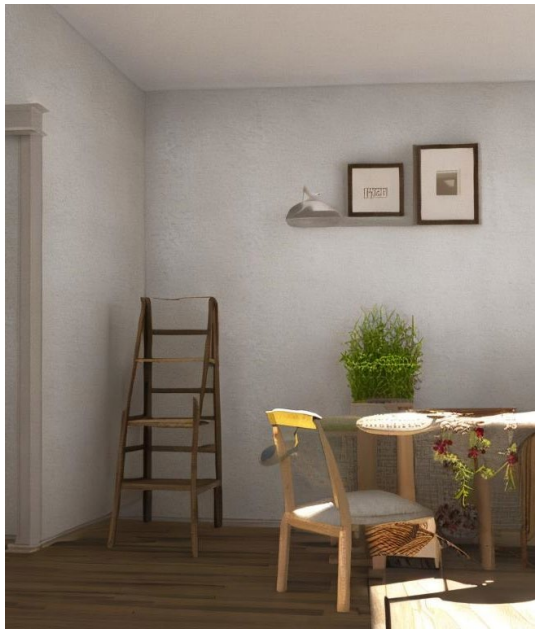
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: RF, SZ
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

RECOGNIZING ROOMS/LOCATIONS INSIDE BUILDINGS BASED ON REFERENCE DATA

- There exist several solutions for recognizing objects in images and videos as well as techniques to match visual data. For some use-cases training an ML-based solution is challenging as training data is scarce.
- Training an ML-based classifier on 3D synthesized data to estimate the facial landmarks of human faces has shown to outperform state-of-the-art methods
- The goals of this thesis are:
  - To analyze whether synthesizing training data in 3D space can improve the performance of methods trying to match the interior of a room
  - To evaluate the transferability on real data
- Requirements: Knowledge in 3D modelling and/or game engines
- Earlier works regarding the transfer of synthesized image data:
  - https://openaccess.thecvf.com/content/ICCV2021/papers/Wood_Fake_It_Till_You_Make_It_Face_Analysis_in_the_ICCV_2021_paper.pdf



Stable Diffusion

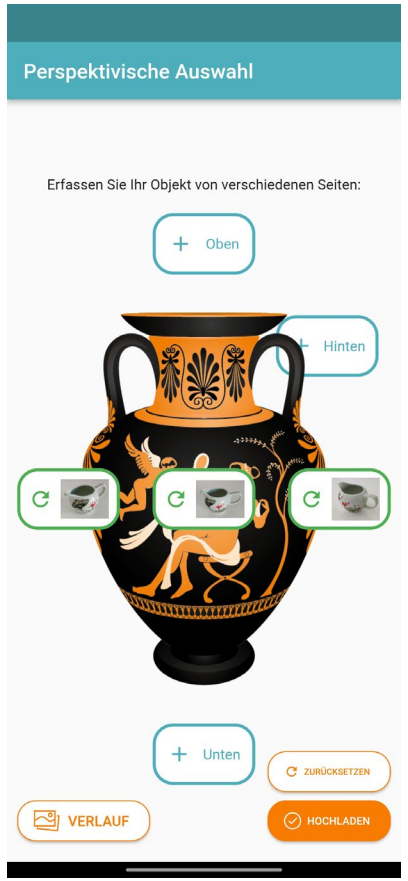
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: RF, SZ
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

DEEP ANALYSIS OF ARCHAEOLOGICAL OBJECTS

- Automatic identification of archaeological objects helps prevent illicit trafficking of cultural assets in trade and at customs. The identification of materials and textures can be used to determine the origin of unknown antiques and verify the results of object recognition by appearance.
- Proper deep neural networks are required to train a model to recognize different materials and textures. The available datasets for training are limited because labeling antiques poses a high resource demand for archaeological experts.
- The goal of this thesis is to
  - develop or adapt a deep neural network model to analyze the surface of archaeological objects
  - implement the recognition model
  - evaluate the developed model with available datasets
- Related work:
  - https://library.imaging.org/ei/articles/34/8/IMAGE-273



ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: HL
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

INVISIBLE IMAGE TAG

- Like 2D-barcodes, digital watermark can be used to link images to further resources. Compared to barcodes, an invisible digital watermark neither requires additional space nor obscures the image, as it can be embedded into the image itself.
- A digital watermark used for image tagging must be robust against possible distortions introduced by smartphone scanning, and detection must be fast to ensure a good user experience.
- The goal of this thesis is to
  - develop or adapt a watermarking algorithm for image tagging
  - implement the watermarking algorithm
  - evaluate the performance of implemented algorithm using various smartphones

Martin Steinebach / Betreuer: HL
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

IMAGE MANIPULATION DETECTION

- Digital images are subject to manipulation. Powerful image editing tools make it possible to manipulate images without specialized skills. Therefore, image forensics is needed to verify the integrity and authenticity of digital images.
- Different types of manipulations leave different traces, which can not be easily detected by a single method. Moreover, such traces can be weakened or even eliminated by post-processing.
- The goal of this thesis is to
  - develop or improve a deep learning based or classical forensic algorithm for specific image manipulations
  - implement the forensic algorithm
  - evaluate the implemented algorithm using different datasets
- Related Work:
  - https://www.sciencedirect.com/science/article/pii/S1051200417301938

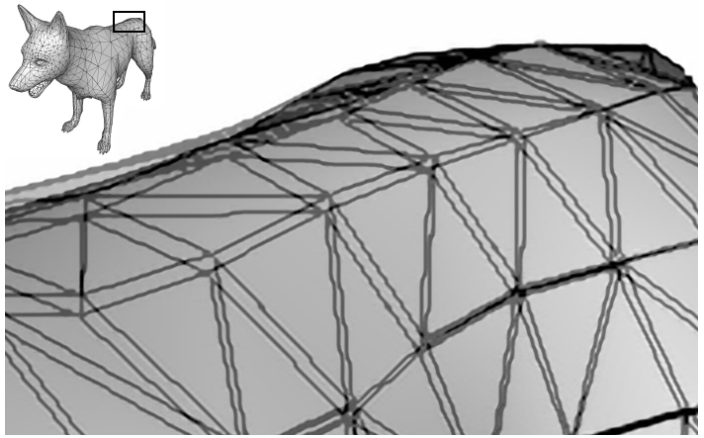
ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer: HL
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT

3D-MODEL WATERMARK

- Decentralized production becomes more important with 3D printers
- 3D models are sent to the printers and printed/manufactured on-site
- Sharing the print data, or scanning a 3D model and duplicating it, is possible and that is where this process fails to progress
- The goal of this thesis
  - Is to design a digital watermarking technique for 3D models with the following properties
    - Written for G Code
    - Watermark extractable after 3D printing and scanning
    - watermark is imperceptible to a person
  - Implement the designed watermark and evaluate it
  - A good starting point is e.g. https://arxiv.org/abs/2109.07202



ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Martin Steinebach / Betreuer*in: WB
Martin.Steinebach@sit.fraunhofer.de, Tel: 06151/869 349

Fraunhofer SIT