

SOKO DEEPPFAKES:

On Discriminating Real from Synthetic (“Fake”) Images

I-Day 2026

Andreas Uhl

Multimedia Signal Processing and Security Lab, University of Salzburg, Austria

February 5th 2026





Figure: Political campaigning.



Figure: Fake War.



Figure: Fake Suffering.

Deep Fakes



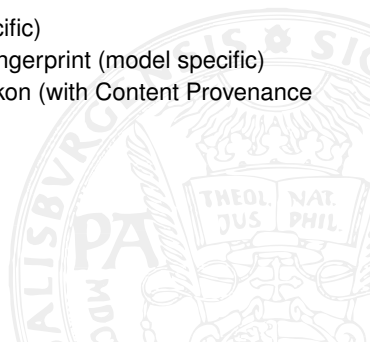
Figure: Fake Pope and how to spot this.

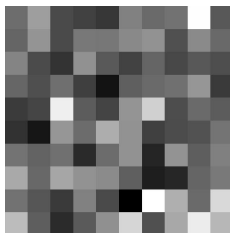
If I want to know how an image has been generated, several options can be pursued: Check if its camera generated (which one ? which model ?), check if it has been synthesized (which model ? which company ?)

1 Real images

- PRNU - Sensor Fingerprint (instance specific)
- Noiseprint - Image Processing Pipeline Fingerprint (model specific)
- Digital Signatures by Sony, Canon and Nikon (with Content Provenance and Authenticity (CP2A) support)

2 Synthetic images: “Model” Fingerprint





- PRNU: Photo-response non-uniformity
- Intrinsic property of CCD/CMOS sensors
- Noise-like pattern
- Variations in quantum efficiency among pixels
- PRNU noise residual W_I :

$$W_I = I - F(I)$$

Why PRNU?

- 1 Universality:** All imaging sensors exhibit PRNU (also in medical imaging, e.g. MRI scanners).
- 2 Generality:** The PRNU is present in every picture independently of the camera optics, camera settings, or scene content.
- 3 Robustness:** It survives lossy compression, filtering, gamma correction, and many other typical processing procedures. It even survives high quality printing and scanning.

Besides source-camera identification, investigating the spectral and spatial characteristics of the PRNU it is possible to detect whether the images have been subject to further processing, e.g. non-geometrical operations have an influence on the PRNU's signal strength so that image tampering can be detected.

Generating a Camera Fingerprint: PRNU

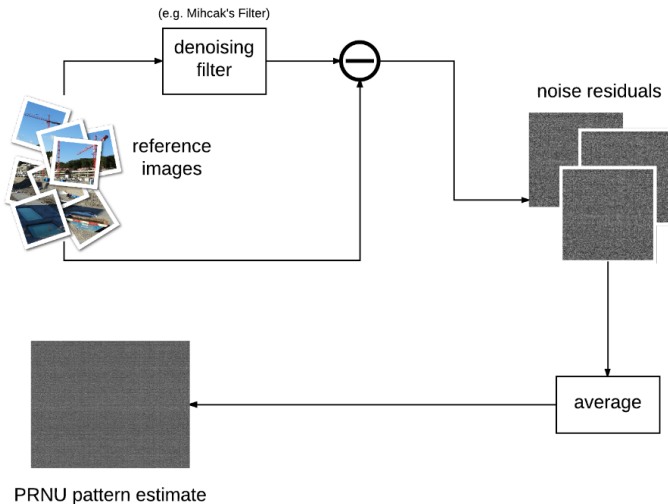


Figure: Looking at the noise is at the core of the technique!

Verifying a Camera Fingerprint: PRNU

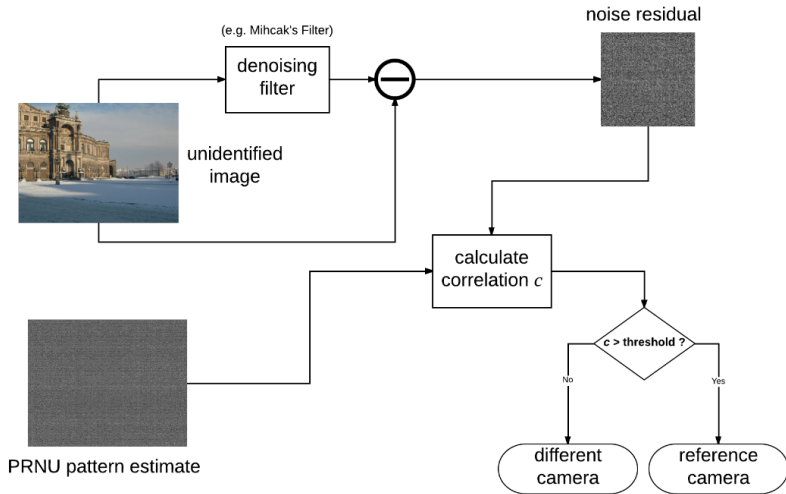


Figure: Correlation of camera fingerprint and noise residual.

Comparing Noiseprint to PRNU

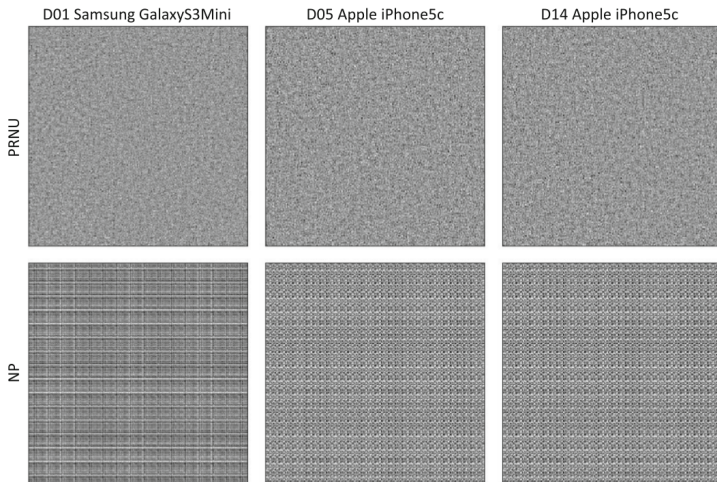


Figure: Noiseprint carries fingerprint of CFA layout with its demosaicing and the camera image formation pipeline.

Synthetic Images: Model Fingerprints

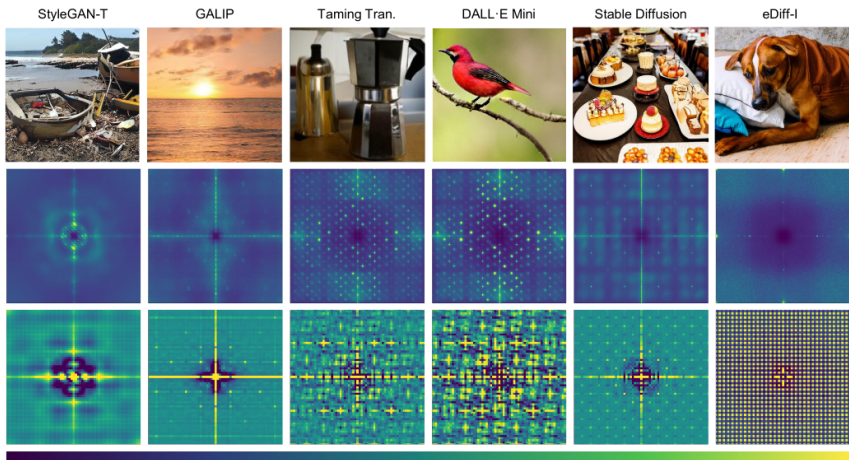


Figure: Different techniques exhibit different model fingerprints: GAN types, Diffusion types.

Comparing Synthetic Images to Real ones: Fingerprints

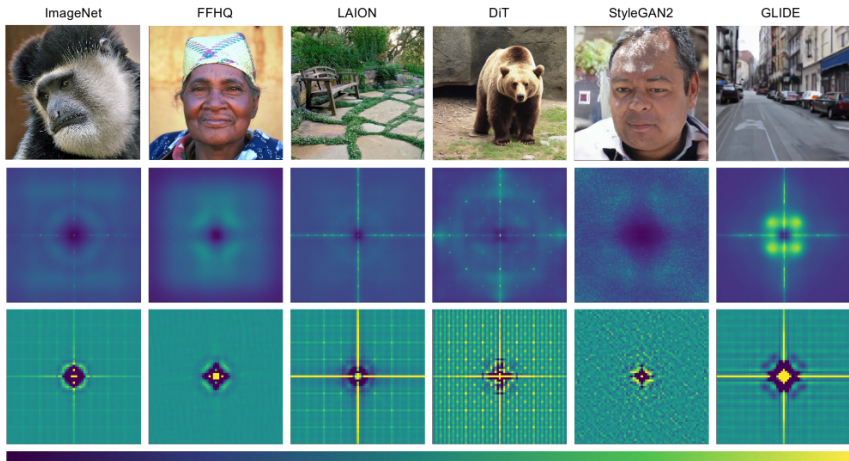


Figure: Problem: Different images, different fingerprints

Comparing Synthetic Images to Real ones: Artefacts

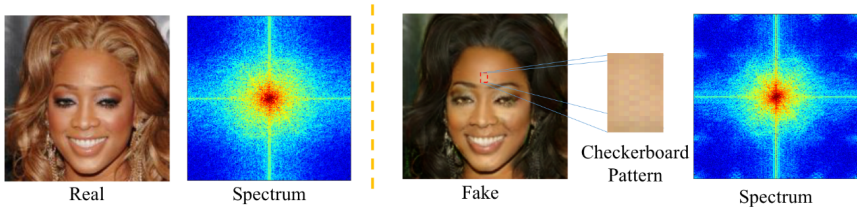


Figure: Similar look, similar style, but how do we really know if content or generation method makes the difference ?

AutoGAN: Producing Synthetic Images identical to Real ones (visually)

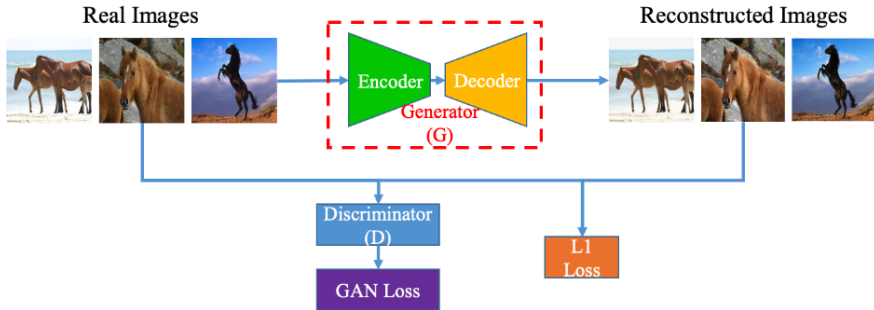


Figure: The Generator G shares important properties to real GANs.

AutoGAN Examples

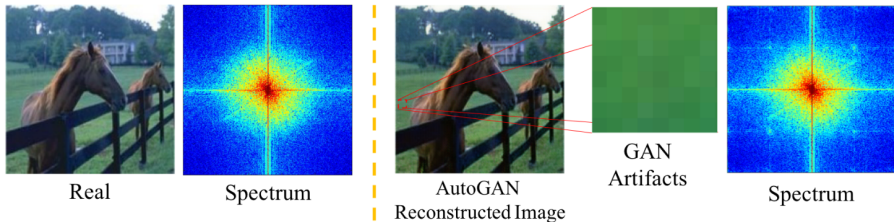


Figure: Identical content (visually), different Fourier properties.

Model Fingerprints are Content Dependent !

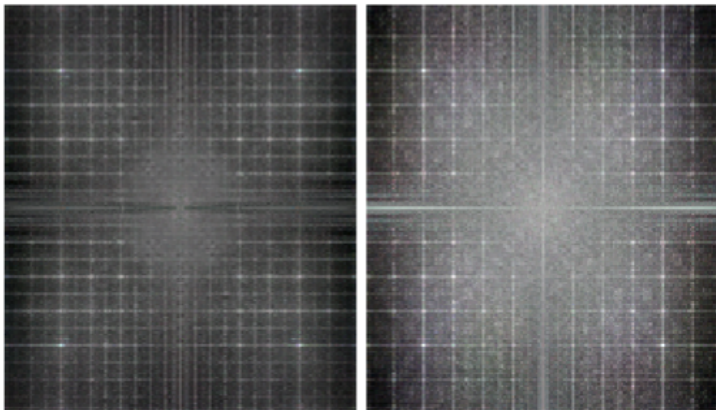


Figure: GANs: Two different subject classes (e.g. cars, planes) carry different fingerprints.

Model Fingerprints are Content Dependent !

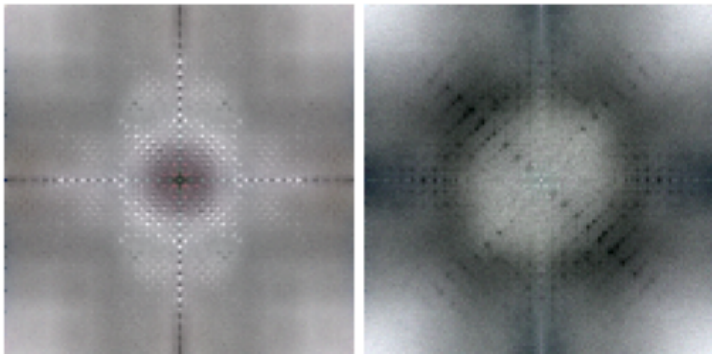


Figure: Diffusion: Two different subject classes (e.g. cars, planes) carry different fingerprints.

Content Dependency Exploited: Watermarking

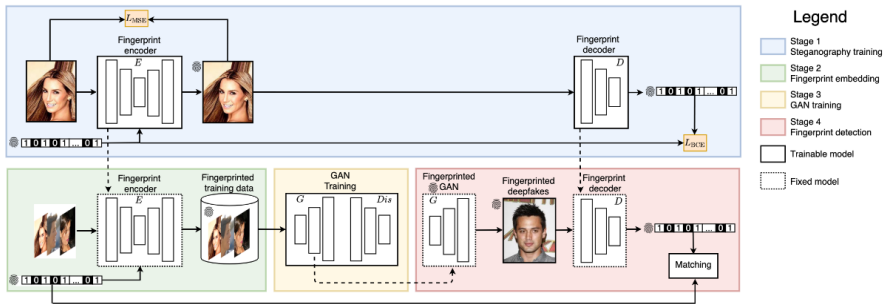


Figure: Training data for GAN carries identical watermark causes all generated images to carry that watermark.

Model Fingerprints can be Removed !

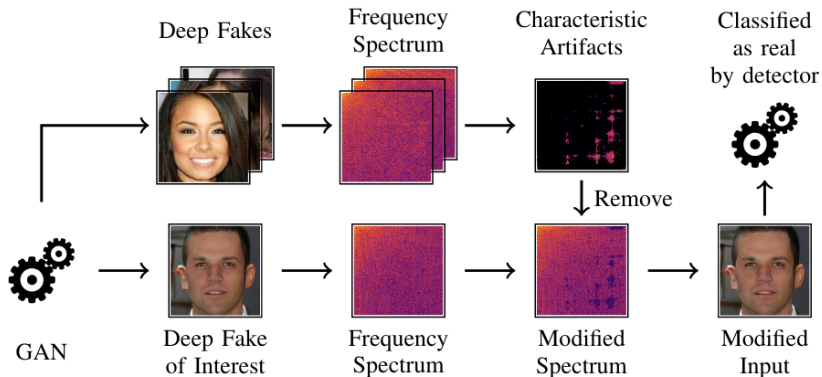


Figure: This is done in the DCT domain (which is also used for your JPEG images (cameras, smartphones)).

Removed Model Fingerprints: Synthetic Faces



(a) Original



(b) Mean



(c) Peaks



(d) Regress.



(e) Bars



(f) Original



(g) Mean



(h) Peaks



(i) Regress.



(j) Bars

Figure: Some work well, some do not (processing traces visible).

Model Fingerprint Removal is not Trivial

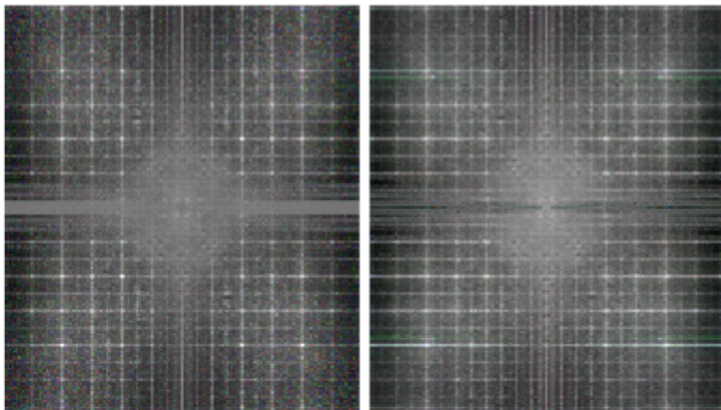


Figure: After applying the most prominent removal process, a changed model fingerprint is still contained in the data.

Conclusion

- Both natural and synthetic images carry fingerprint signals which can be used to identify the image source
- In both cases, these signals can be removed (more or less easy and effective, respectively)
- Model fingerprints in synthetic images are not yet well understood
- They are image content dependent

Local work

- Work on camera identification in a criminal case (child pornography, Swedish Forensic Institute)
- Work on biometric sensor identification in finger vein and iris recognition schemes (difference to usual data due to high correlation)
- Work on synthesizing biometric sample data (small user groups, cumbersome work to generate presentation attack instruments)

Thank you for your attention!
Any questions?

