

Contents lists available at [ScienceDirect](https://www.sciencedirect.com)

## Forensic Science International: Digital Investigation

journal homepage: [www.elsevier.com/locate/fsidi](http://www.elsevier.com/locate/fsidi)DFRWS EU 2026 - Selected Papers from the 13th Annual Digital Forensics Research Conference Europe  
Boon or Bane: Source Camera Identification meets AI-generated imagesSamantha Klier<sup>\*</sup> , Harald Baier 

Research Institute CODE, Faculty for Computer Science, University of the Bundeswehr Munich, Munich, Germany

## ARTICLE INFO

## Keywords:

Source Camera Identification  
Media Forensics  
AI-generated image detection  
AI image fingerprints

## ABSTRACT

Linking an image to its origin is a fundamental task in digital forensics often addressed through Source Camera Identification (SCI) based on Sensor Pattern Noise (SPN). However, recent advances in AI-enhanced smartphone photography challenge the reliability of SPN. On the other hand, noise-based identification approaches have been successfully transferred to AI-generated images. Therefore, we investigate whether the noise patterns of AI-generated images interfere with those of modern smartphones and analyze the implications for standard procedures. Our empirical evaluation reveals that the noise in AI-generated images is not predominantly additive, contradicting prior assumptions. Furthermore, we show that fingerprints of AI image generators can identify corresponding images only when the prompted resolution matches. Additionally, the standard PCE threshold leads to high false-positive rates — 61 % for Adobe Firefly Image 4 and 100 % for ChatGPT 5 — when comparing AI images to smartphone fingerprints. We demonstrate that simple center-cropping effectively eliminates these false positives without reducing true-positive identification performance. Our findings highlight the need for updated forensic methodologies due to the influence of software on imaging pipelines.

## 1. Introduction

Linking a digital artifact to its origin is an important task in digital forensics. This is of particular interest in the scope of finding the source of incriminated media files like pictures of Child Sexual Abuse Material (CSAM). Back in 2006, [Lukas et al. \(2006\)](#) demonstrated that camera sensors introduce unique noise patterns into captured images due to inherent hardware imperfections. This discovery led to the development of the so-called Sensor Pattern Noise (SPN) approach for Source Camera Identification (SCI). The refined version of this method proposed by [Goljan et al. \(2009\)](#) has since become the standard technique in digital forensics for verifying whether an image originates from a specific imaging sensor ([Klier and Baier, 2025](#)).

However, roughly twenty years have passed since the seminal works of [Lukas et al. \(2006\)](#) and [Goljan et al. \(2009\)](#). Recent works on the topic have raised concerns that the introduction of AI-based imaging techniques to digital cameras, and smartphones in particular, undermines its reliability ([Klier and Baier, 2025](#)). For example, [Albisani et al. \(2021\)](#) provided a contemporary smartphone data-set and demonstrated that an unacceptable amount of false-positives occur, likely due to patterns introduced by the native software of the smartphones.

On the other hand, Artificial Intelligence (AI)-generated visual content is becoming increasingly widespread. Although such generators

lack a physical image sensor, they still exhibit characteristic noise patterns that can be used to link an image to its source, as demonstrated by [Marra et al. \(2019\)](#) and [Corvi et al. \(2023\)](#).

In this paper we address the question whether the noise patterns of AI-generated images and the noise patterns of images captured by modern smartphones interfere with one another. In particular, we examine the implications of unintentionally comparing software-enhanced real images with photorealistic AI-generated images through established SCI methods.

## 1.1. Contributions

The key contributions of our work are as follows:

- We present an empirical analysis showing no evidence that the noise in AI-generated images is primarily additive in nature, contrary to assumptions made in prior work (see Section 3.2).
- We empirically demonstrate that AI fingerprints can reliably identify images originating from a specific AI model only, when the generation resolution is identical (see Section 4.1); moreover, comparing real-images from smartphones with the threshold commonly used for SCI can lead to false-positives.

<sup>\*</sup> Corresponding author.

E-mail addresses: [samantha.klier@unibw.de](mailto:samantha.klier@unibw.de) (S. Klier), [harald.baier@unibw.de](mailto:harald.baier@unibw.de) (H. Baier).

<https://doi.org/10.1016/j.fsidi.2026.302064>

- We conduct an empirical study demonstrating that matching AI-generated images to smartphone fingerprints yields a False Positive Rate (FPR) of 100 % for ChatGPT 5 and 61 % for Firefly Image 4 (see Section 4.2). This highlights the substantial risk of incorrectly attributing AI-generated images to specific cameras when applying standard forensic procedures.
- We show that center-cropping of images effectively prevents such false-positives (see Section 4.3).

## 1.2. Structure of paper

The rest of this article is structured as follows: after this introduction we review related work in the scope of our paper in Section 2. We then explain our methodology in Section 3 and present our results in Section 4. Section 5 discusses the limitations and implications of our study and Section 6 concludes our paper and points to future work.

## 2. Related work

In this section, we first introduce the SPN approach, which is the quasi standard for SCI in digital forensics. We then present related work that applies a noise-based approach on AI generated images.

### 2.1. Camera identification with Sensor Pattern Noise (SPN)

The basic idea of the SPN approach is to identify a digital camera, which captured an image, by specific noise that is introduced due to hardware imperfections of the sensor. The SPN approach was proposed and later refined by Lukas et al. (2006) and Goljan et al. (2009).

#### 2.1.1. Procedure

The procedure of SPN applies a denoising filter (denoted as  $F$ ) to an image (denoted as  $I$ ), yielding a denoised image version. This version is then subtracted from the original image to obtain the noise residual  $N(I)$ , as shown in Equation 1. Subsequently, a so-called *camera fingerprint* is calculated by averaging the noise residuals from several images of the same camera. Finally, the noise residual of an image can be compared to the *camera fingerprint* to verify whether it captured the image.

$$N(I) = I - F(I) \quad (1)$$

Here, a common noise filter can be used, such as the Wiener Filter (Goljan et al., 2009), which is a standard operation in image processing. However, for the generation of the *camera fingerprint*, so-called *flat* images should be used which, e.g. depict a bright blue sky to ensure a uniform lighting of the pixels (Chen et al., 2008). Subsequently, the comparison between the noise residual of an image and a *camera fingerprint* is based on their cross-correlation of which the Peak to Correlation Energy (PCE) (Goljan et al., 2009) is calculated. Therefore, the PCE is a single value that expresses the fitting of an image's noise residual to a camera's fingerprint. Generally, a PCE value of  $> 60$  is considered a match (Goljan et al., 2009).

#### 2.1.2. Smartphones

However, this common threshold of 60 leads to false-positives among smartphone cameras from the same model or brand, especially for images captured in the bokeh mode which are heavily processed by the camera software, as found by Albisani et al. (2021). In conclusion, they attributed the false-positives to diagonal correlation patterns of the affected noise residuals, likely introduced by the native software of the smartphone.

## 2.2. AI generated images and noise

We now review related work in the scope noise patterns of AI generated images.

### 2.2.1. Noise patterns of GANs

Marra et al. (2019) extracted noise fingerprints of Generative Adversarial Networks (GANs), by following the procedure of the basic SPN approach. However, they propose to treat the noise introduced by the GANs as additive, instead of multiplicative. This is explained by the fact that the noise of a camera sensor depends on the lightning, which cannot be assumed for an AI model. However, Marra et al. (2019) do not further study the 'additive assumption' to provide evidence of their claim. Nevertheless, their noise extractions converge to stable quasi-periodic patterns unique to each GAN.

Finally, this finding is verified by computing correlations between noise residuals of AI generated images and fingerprints of the respective models which yielded correlations close to zero for mismatched GANs, but significantly positive for matching ones. In conclusion, Marra et al. (2019) report an Area Under-Receiver Operating Curve (AU-ROC) value of 0.990 for Cycle-GANs and 0.998 for Pro-GANs, indicating almost perfect accuracy in telling apart images from the evaluated GANs. Unfortunately, the collisions with the only two tested physical digital single-lens reflex cameras are not discussed in detail.

### 2.2.2. Noise patterns of Diffusion Models

Corvi et al. (2023) studied noise-based fingerprints of Diffusion Models and, overall, confirmed the applicability of the previous results for GAN. Additionally, they consider cropped and resized images and train a classifier to detect specific image generator models, but achieve mixed results. In particular, AU-ROC results are significantly better than Precision and the performance depends strongly on the specific AI model type, whereas identification of Diffusion Models is particularly difficult. Therefore, they analyzed the Fourier Transform of the averaged noise residuals of 1000 images per model, as shown in Fig. 1. They conclude, that while most Diffusion Models still have quasi-periodical patterns, these are more subtle.

## 3. Methodology

This section explains our underlying methodology. We first introduce the used data sets in Section 3.1 and then address key questions arising from related work in Section 3.2. Subsequently we explain our experimental setup in Section 3.3.

### 3.1. Used data sets

With respect to *real images from smartphones* we resort to the PRNU Modern Devices data set (Albisani et al., 2021) due to its known problem devices, as presented in Section 2.1. A summary of the data set,<sup>1</sup> is shown in Table 1.

For *AI generated images*, the Synthbuster (Bammey, 2023) data set from 2023 is commonly used. However, all images have a quadratic aspect ratio which is also the case for many other data sets (Cozzolino et al., 2024) while the available resolutions are very small, e.g. for the ADM AI images are only available with a resolution of  $256 \times 256$ . In contrast, smartphone images are mostly captured and processed in portrait or landscape mode and with much higher resolutions. This is problematic, as in conventional photography, a different aspect ratio is often obtained by simple cropping, while AI models obtain different aspect ratios by changing the dimensions of the latent grid. Consequently, this may lead to noise patterns that depend on the resolution.

Therefore, we generate our own data set<sup>2</sup> which takes these points into account, the statistics are shown in Table 2. The data set contains predominantly photorealistic images, respectively generated by OpenAI's *ChatGPT 5* and Adobe's *Firefly Image 4*. The prompts included

<sup>1</sup> Prnu Modern Devices data set is available here. <https://cloud.digfor.code.unibw-muenchen.de/s/BEEzsMnZLFCXw9S>

<sup>2</sup> Our data set of AI generated images is available here.

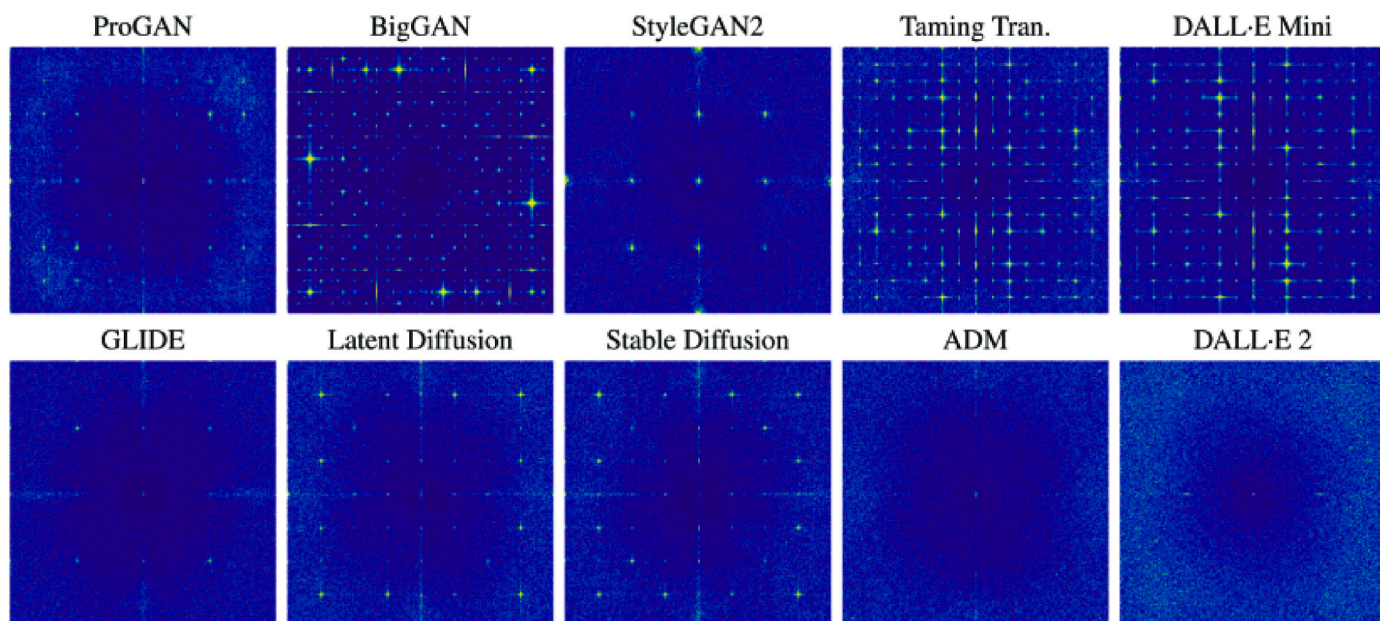


Fig. 1. Spectral Amplitudes of noise residuals per image generator model, due to Corvi et al. (Corvi et al., 2023). GANs in the top and Diffusion Models in the bottom row.

Table 1

Summary of the used real-image dataset, captured with smartphones, from Albisani et al. (2021).

PRNU Modern Devices	
Publication	2021
Smartphone Models	17
Smartphones	22
Images	550
Image Types	flat, nat, bokeh

Table 2

Overview of our self-crafted text-to-image-generated dataset, showing the number of images used for reference calculation and for test, respectively for each resolution and model.

ChatGPT 5		
Resolution	Fingerprint Images	Test Images
2048 x 2048	3	13
2304 x 1792	3	20
1792 x 2304	3	18
	<b>Total</b>	<b>51</b>
Firefly Image 4		
Resolution	Fingerprint Images	Test Images
1024 x 1024	3	21
1536 x 1024	3	65
1024 x 1536	3	13
	<b>Total</b>	<b>99</b>

common scenes of everyday life, but also content suitable to disturb public order, and few non-photorealistic images. Examples are shown in Fig. 2.

### 3.2. Preliminary considerations

#### 3.2.1. Spectral observations

Albisani et al. (2021) observed diagonal correlation patterns in those smartphones that produce false-positives when the SPN is applied. Therefore, we consider the spectral amplitude of C02 (Huawei P20 pro)

of the PRNU Modern Devices data set, and compare it to the findings of Corvi et al. (2023) (see Section 2.2). Hence, we calculate a basic fingerprint<sup>3</sup> by simply adding the pixel values of all flat images in grayscale and divide them by the amount of available images without normalization and convert it to the frequency domain.

An excerpt of the resulting spectral amplitudes is shown in Fig. 3. Therefore, weak periodical patterns, similar to those of Diffusion Models (compared to Fig. 1), can be observed. Consequently, supporting the importance of the raised research question in this paper.

#### 3.2.2. Additive and multiplicative noise

While Marra et al. (2019) generally followed the noise pattern approach of Lukas et al. (2006), they treated the noise as additive, instead of multiplicative (see Section 2.2), due to not being sensor-based. While the physics of sensor-based imaging does not apply to AI generated images, the underlying models may still have learned that noise in images should be multiplicative. Therefore, we run an empirical test to find out whether the noise of AI generated images is indeed more additive than the noise of real images. Therefore, we statistically test whether there is a correlation between noise and signal which would be indicative for a multiplicative effect.

In Fig. 4 Spearman's correlation coefficient for all AI generated images and all smartphone captured real images are shown. Please note, that all results are significant ( $p < 0.0001$ ). Consequently, both groups show a significant mean correlation coefficient of approximately  $-0.5$  which means that there is an inverse correlation between noise and pixel intensity. Therefore, darker areas have higher noise which is the expected result for sensor-based imaging, but apparently, this is also the case for the AI generated images. However, there are many exceptions to this general trend in both groups, hence, the noise has multiplicative and additive components. In conclusion, there is no indication that the noise of AI images is less multiplicative than the noise of smartphone images.

<sup>3</sup> This fingerprint calculation is not analogous to the approach of Lukas et al. (2006) or Goljan et al. (2009), as their refinements to the naive approach impair visual comparison with the results of Corvi et al. (2023).



Fig. 2. Examples from our data set, top row was generated by ChatGPT 5, bottom row by Firefly Image 4. Respectively, a normal, a disturbing and a non-photorealistic scene are shown.

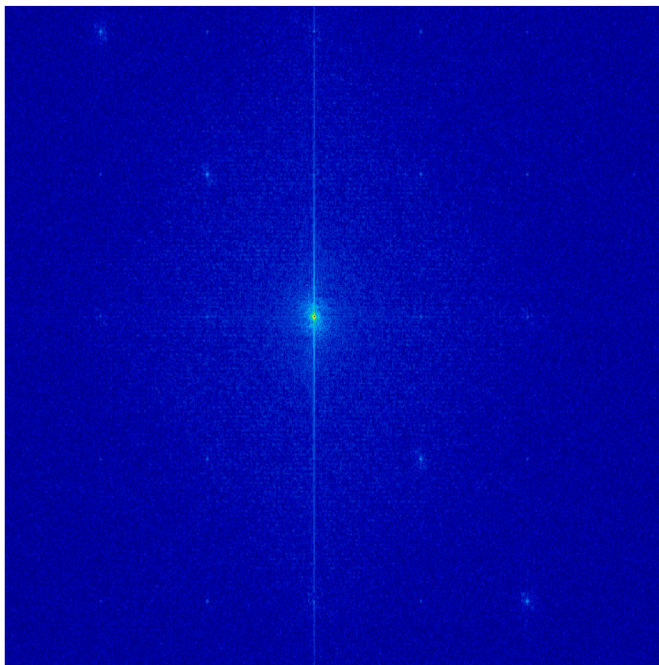


Fig. 3. Excerpt of the spectral amplitudes of a problem device's basic fingerprint, here a Huawei P20 pro (C02).

### 3.3. Experimental setup

For the upcoming experiments, we follow the commonly applied SPN approach for SCI, as proposed by Goljan et al. (2009), and use their Matlab code.

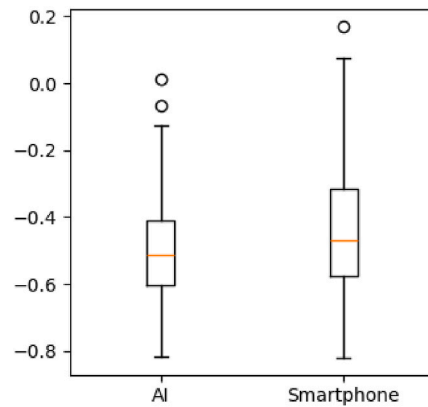


Fig. 4. Spearman's correlation coefficients between noise and pixel intensity for AI and smartphone images.

#### 3.3.1. Fingerprints

Therefore, the fingerprints are calculated per smartphone, as usual, with the dedicated flat images. However, the fingerprints for the AI models are calculated per generated resolution, by three<sup>4</sup> randomly selected photorealistic images.

#### 3.3.2. Comparison

Subsequently, the test images are compared against the calculated fingerprints. For images and fingerprints with diverging resolutions, we follow the procedure of Goljan et al. (2009). Therefore, we add a zero padding where necessary and allow the maximal shifting in the detection algorithm to find the highest match.

In SCI, the cross-correlation is calculated between the noise residual ( $Noise_x$ ) of the test image ( $I_x$ ) and the fingerprint, but multiplied by the pixel-intensity of test image itself due to the assumption of handling multiplicative noise, as shown in Equation (2). In contrast, Marra et al.

<sup>4</sup> prior tests showed that the following results are not sensitive to the amount of images selected for fingerprinting.

(2019) proposed to treat the noise of AI generated images as additive, as shown in Equation (3). Due to the findings presented in Section 3.2, we stick to the conventional calculation of the cross-correlation (Equation (2)).

$$C_m = \text{crosscorr}(\text{Noise}_x, I_x\text{-Fingerprint}) \quad (2)$$

$$C_a = \text{crosscorr}(\text{Noise}_x, \text{Fingerprint}) \quad (3)$$

### 3.3.3. Evaluation

For the evaluation, we exclude the images that were used for the fingerprint calculations. Therefore, we use all *nat* and *bokeh* images from the PRNU Modern Devices data set (see Table 1) and test them against the AI fingerprints. Vice-a-Versa, we use all AI generated test images (see Table 2) and match them against the smartphone fingerprints. Each comparison yields a PCE value, which in turn is evaluated.

## 4. Results

In this Section we present the results of our origin interference study of AI generated images to real smartphone images.

### 4.1. AI fingerprints and smartphone images

First, we compare the smartphone test images to the AI fingerprints. Therefore, in Fig. 5 boxplots of the PCE values per AI fingerprint are shown (Firefly Image 4 in Fig. 5a, ChatGPT 5 in Fig. 5b). Here, the dashed red line marks the commonly applied PCE threshold of 60. Please note, that the y-axis is scaled logarithmically. Additionally, we report the median PCE values and standard deviations in Table 3.

Overall, the results for both AI models are similar. Favorably, images from the same AI model are clearly distinguishable from the other groups, when the generated resolutions match. Therefore, this result is consistent with previous findings (see Section 2.2). However, the PCE values of matches are extraordinarily high with a median  $> 60,000$ , especially for ChatGPT 5 with a median PCE value of  $> 500,000$ . Therefore, these findings are analyzed in detail in Section 4.3. However, images generated by the same AI model, but with a different resolution do not clearly stand out against images from other sources, such as smartphones. Moreover, when applying the common threshold of 60, a non-negligible amount of false positives, especially from smartphone images are obtained.

### 4.2. Smartphone fingerprints and AI images

Next, we compare our AI test images to the smartphone fingerprints and show the resulting PCE values in Fig. 6 (Firefly Image 4 in Fig. 6a, ChatGPT 5 in Fig. 6b). Again, the red dashed line denotes the common PCE threshold of 60.

Consequently, a substantial proportion of AI-generated images exceed the common threshold when compared against smartphone fingerprints. Notably, the results for ChatGPT 5 are the most concerning, as all test images produce false positives across all smartphones, yielding an FPR of 1.0. In contrast, Firefly Image 4 exhibits a lower FPR of 0.61, which remains alarming. Also, no smartphone is exempt from false-positives. However, device C10 (Xiaomi Mi Note 10) stands out, exhibiting the highest PCE values, exceeding 100 continuously. In contrast, the devices previously identified as problematic by Albisani et al. (2021)—C02–C08 (various Huawei P models), C14–C15 (Samsung S9 series), and C19–C22 (various Apple iPhones)—do not stand out.

### 4.3. Extraordinarily high PCE values

#### 4.3.1. Observations

As presented in Section 4.1 the correct matches between AI fingerprints and their test images with corresponding resolution, are

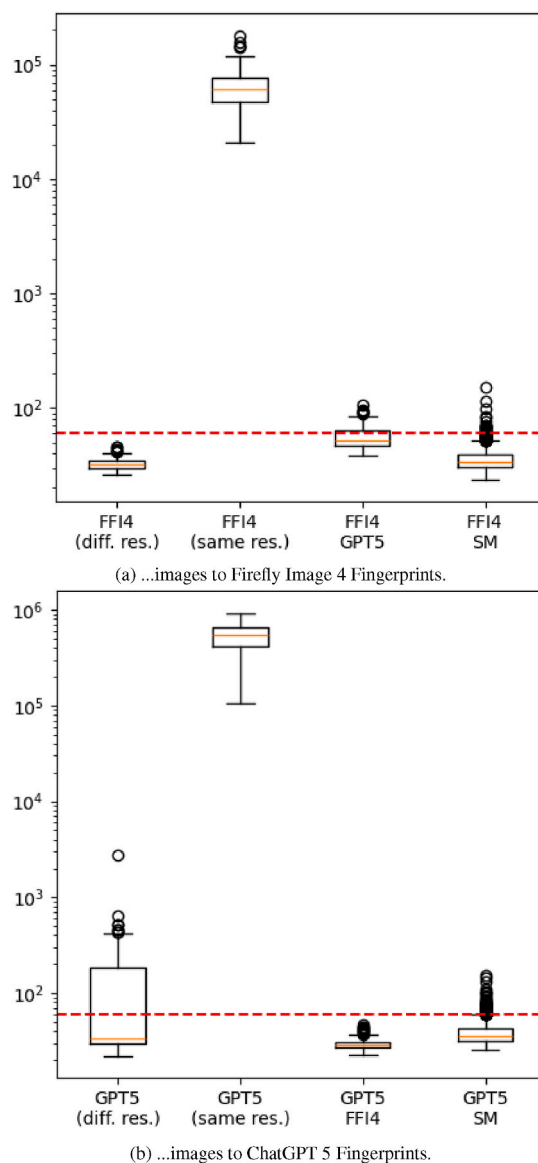


Fig. 5. PCE values of test images matched against AI fingerprints, red line indicates the common threshold of 60. (For interpretation of the references to colour in this figure legend, the reader is referred to the Web version of this article.)

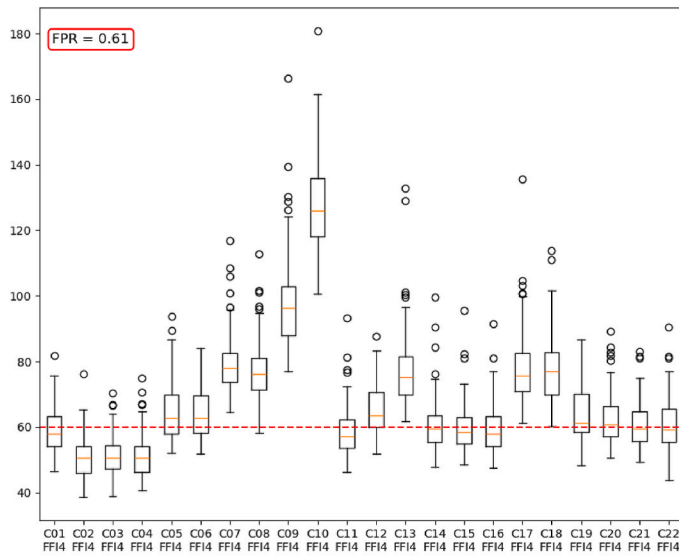
Table 3

Median PCE values and standard deviation, per group.

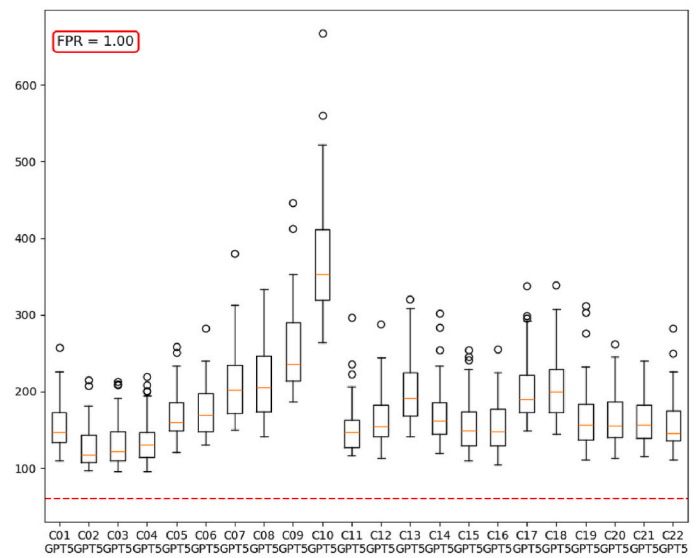
Fingerprint	Test Images	Median	Std. Dev.
FireflyImage4	FFI4 (same res.)	60, 604.73	29, 495.41
	FFI4 (diff. res.)	31.68	3.92
	GPT 5	52.21	13.39
	Smartphones	33.96	8.83
GPT 5	GPT5 (same res.)	549, 325.02	186, 171.55
	GPT5 (diff. res.)	33.79	299.28
	FFI4	28.45	3.64
	Smartphones	35.57	12.13

extraordinarily high. Therefore, we analyzed the peak region of the cross-correlation. First, we located the peak, as shown in Fig. 7. Curiously, for all matching images from both AI models, the peak occurs at the tip of the corner.

Therefore, we visually analyzed the results of the cross-correlation in the peak area. An example for Firefly Image 4 is shown in Fig. 8 and

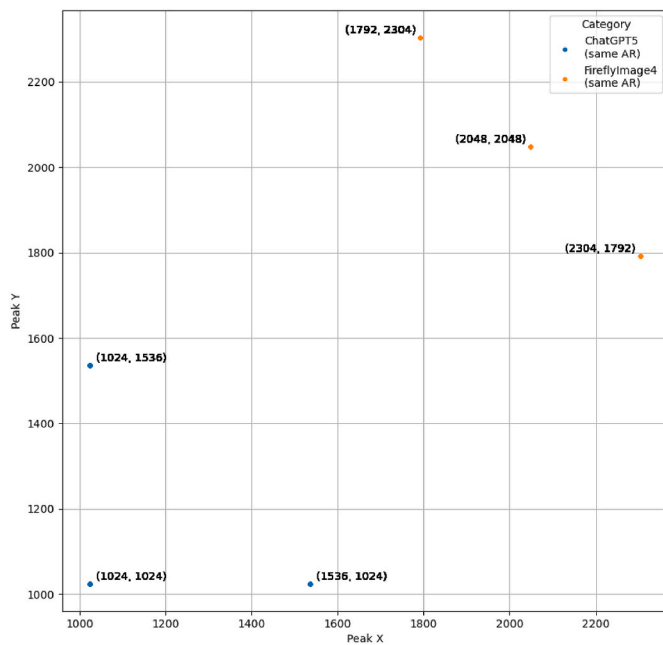


(a) Firefly Image 4 images.



(b) ChatGPT 5 images.

**Fig. 6.** PCE values of AI generated images matched against smartphone fingerprints and FPR for a threshold of 60 (red line). (For interpretation of the references to colour in this figure legend, the reader is referred to the Web version of this article.)

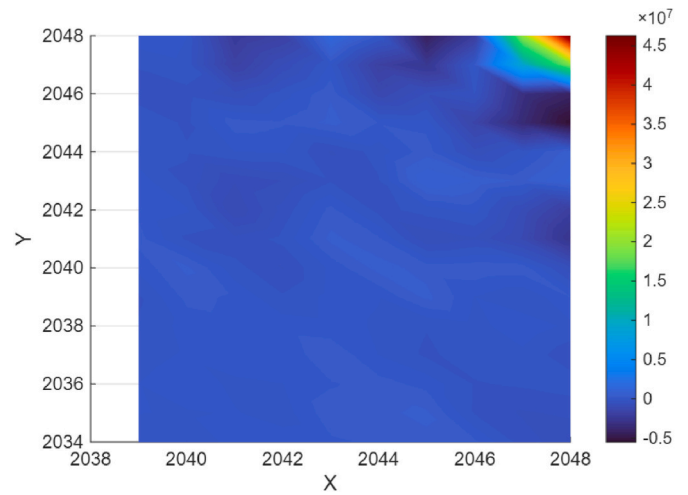


**Fig. 7.** Location of peak in cross-correlation, respectively the last pixel of each image.

illustrates the immense difference between the corner pixels (magnitude of  $10^7$ ) and the surrounding area (magnitude of  $10^0$ ). Therefore, the question arises whether the reported results apply, when the images are cropped.

**4.3.2. Cropping**

Consequently, we repeated the experiments described in the previous sections using center-cropped images at a resolution of  $512 \times 512$  for fingerprint calculation and testing. Therefore, we report the median PCE values of AI fingerprints to the test images, in **Table 4** (analogous to **Table 3**). In conclusion, the median PCE values decrease, but are still extraordinarily high for the matches. Also, the standard deviation declines which is favorable, as it indicates more stable results. Finally, the



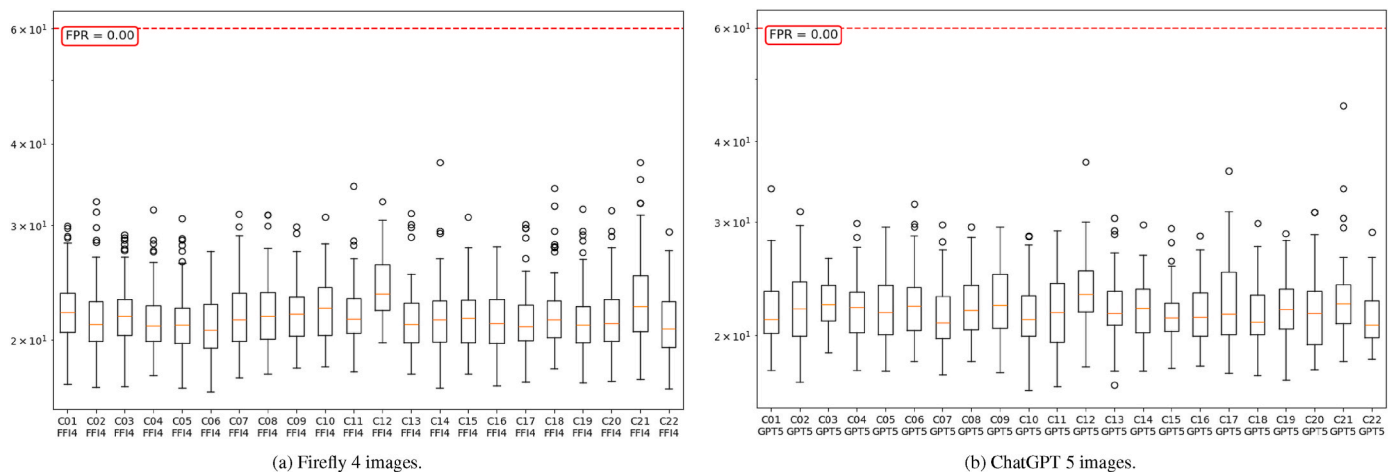
**Fig. 8.** The peak area of the cross-correlation between the Firefly Image 4 fingerprint and a matching image, respectively in a resolution of  $2048 \times 2048$ .

**Table 4**

Median PCE values and standard deviation of cropped images, per group.

Fingerprint	Test Images	Median	Std. Dev.
FireflyImage4	FF14 (same res.)	3,413.79	1,909.94
	FF14 (diff. res.)	22.51	2.67
	GPT 5	22.02	3.33
	Smartphones	22.22	3.26
GPT 5	GPT5 (same res.)	85,059.58	31,774.13
	GPT5 (diff. res.)	22.18	13.35
	FF14	21.63	2.44
	Smartphones	21.82	3.24

FPR for AI images matched against smartphone fingerprints with the common threshold drops to 0.0 for all devices and AI models, as show in **Fig. 9** (analogous to **Fig. 6**).



**Fig. 9.** PCE values of cropped AI generated images matched against cropped smartphone fingerprints and FPR for a threshold of 60 (red line). (For interpretation of the references to colour in this figure legend, the reader is referred to the Web version of this article.)

## 5. Limitations & Discussion

In this section we shortly address the limitations of our work and discuss important aspects like noise types, PCE thresholds and resolution aspects.

### 5.1. Limitations

The main limitation of this work is the respectively small data set size. Furthermore we consider the narrow diversity of images and the outdated smartphone models as issues to be addressed by subsequent work. Therefore, the presented results illustrate a possible (in our perception a highly probable) outcome, however, they should be validated and generalized by follow-up studies.

### 5.2. Noise types

However, an interesting aspect to consider is whether the noise is additive or multiplicative in nature. While our dataset provides no empirical evidence that the noise in AI-generated images is primarily additive, the distinction between these two types, could still be valuable. Differentiating them thoroughly may enhance noise-based approaches, since additive noise could be software-induced, whereas multiplicative noise could be more hardware or training set related.

### 5.3. PCE threshold

The most important implication of our noise pattern tests in Section 4.1 and 4.2, is that a PCE value of  $> 60$  does no longer reliably verify the origin of an image which is consistent with the findings for certain smartphone models of [Albisani et al. \(2021\)](#). Otherwise, a smartphone image could easily be mistaken as AI-generated and vice-versa. Therefore, such misclassifications can have severe consequences, e.g. someone may generate artificial CSAM to accuse another person of child abuse which could be falsely-verified to stem from the accused' smartphone, when following the standard scheme. However, when images correctly match an AI fingerprint, the PCE values are extraordinarily high.

### 5.4. Resolution and crop

[Goljan et al. \(2009\)](#)'s approach mitigates simple crop operations, yet, is unable to detect an image from the same AI model when it was generated with a different resolution. Therefore, the resolution at the time of generation plays a critical role for AI generated images, as it does not equate to a simple crop operation.

## 6. Conclusion and future work

This work studied to which extent the noise patterns of smartphone and AI generated images interfere with one another. We also addressed the implications on standard processes in digital forensics.

Therefore, we demonstrated that both types of images can exhibit similar quasi-periodic noise patterns, and that the noise in AI-generated images is not predominantly additive in nature, as previously suggested.

Favorably, in our evaluation we found that Diffusion Models can be identified with the standard SPN procedure which yields extraordinary high PCE values for correct matches. However, images generated by the same model, but in a different resolution cannot be identified.

Conversely, we found that the fingerprints of ChatGPT-5 and Firefly Image 4 resulted in false detection rates of 100 % and 61 %, respectively, for smartphone images, when the common PCE threshold of 60 is applied. This finding is alarming for the use of the SPN approach in practice.

However, the false-positives depend on an anomaly in the corner of the AI generated images. Consequently, we demonstrated that the false-positives disappear, while the decisiveness for true-positives remains, when the images are center cropped.

For future work, this anomaly warrants further investigation, as it may improve the identification of AI-generated content—either broadly or for the specific model involved. Moreover, future research should explore how AI fingerprints can be computed to recognize generated content independently of the prompted resolution. Finally, it may be valuable for SCI to investigate methods for disentangling different noise sources to better distinguish between software- and hardware-related features.

## References

- [Albisani, C., Iuliani, M., Piva, A., 2021. Checking PRNU usability on modern devices. In: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing \(ICASSP\). IEEE, pp. 2535–2539.](#)
- [Bammey, Q., 2023. Synthbuster: towards detection of diffusion model generated images. IEEE Open J. Signal Processing 5, 1–9.](#)
- [Chen, M., Fridrich, J., Goljan, M., Lukás, J., 2008. Determining image origin and integrity using sensor noise. IEEE Trans. Inf. Forensics Secur. 3, 74–90.](#)
- [Corvi, R., Cozzolino, D., Zingarini, G., Poggi, G., Nagano, K., Verdoliva, L., 2023. On the detection of synthetic images generated by diffusion models. In: ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing \(ICASSP\). IEEE, pp. 1–5.](#)
- [Cozzolino, D., Poggi, G., Corvi, R., Nießner, M., Verdoliva, L., 2024. Raising the bar of ai-generated image detection with clip. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4356–4366.](#)
- [Goljan, M., Fridrich, J., Filler, T., 2009. Large scale test of sensor fingerprint camera identification. In: Media Forensics and Security. SPIE, pp. 170–181.](#)

Klier, S., Baier, H., 2025. Source camera identification-do we have a gold standard? *Forensic Sci. Int.: Digit. Invest.* 52, 301858.  
Lukas, J., Fridrich, J., Goljan, M., 2006. Digital camera identification from sensor pattern noise. *IEEE Trans. Inf. Forensics Secur.* 1, 205–214.

Marra, F., Gagnaniello, D., Verdoliva, L., Poggi, G., 2019. Do gans leave artificial fingerprints?. In: *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. IEEE, pp. 506–511.