Forensic Science International: Digital Investigation 52 (2025) 301858

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Source Camera Identification - Do we have a gold standard?

Samantha Klier *, Harald Baier

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

A R T I C L E I N F O

Dataset link: Articles of Source Camera Forensics classified based on the Source Camera Target Model and Problem Classes (Original data)

Keywords:
Source camera identification
Source model identification
Sensor pattern noise
Source camera target model
Problem classes of source camera forensics

A B S T R A C T

Source Camera Identification (SCI) is vital in digital forensics, yet its most prominent approach, Sensor Pattern Noise (SPN), faces new challenges in the era of modern devices and vast media datasets. This paper introduces the Source Camera Target Model (SCTM) to classify SCI approaches and formally defines three core problem classes: Verification, Identification, and Exploration. For each, we outline key evaluation metrics tailored to practical use cases. Applying this framework, we critically assess recognized SCI methods and their alignment with contemporary needs. Our findings expose significant gaps in scalability, efficiency, and relevance to modern imaging pipelines, challenging the notion of SPN as a gold standard. Finally, we provide a roadmap for advancing SCI research to address these limitations and adapt to evolving technological landscapes.

1. Introduction

Linking a media file to its origin is an important task in digital forensics and is referred to as *Source Camera Identification (SCI)* which has received considerable attention (Geradts et al., 2001; Sencar et al., 2022). For example, if illicit media content such as Child Sexual Abuse Material (CSAM) is found during an examination, a major responsibility is to track the file back to the camera (and subsequently to its owner) used to record it.

Currently, the most accepted approach to solving the SCI problem is the Sensor Pattern Noise (SPN) approach due to Lukas et al. (2006). Their concept is based on the *Photo Response Non-Uniformity (PRNU)*, i.e. a non-uniformity of the pixels introduced by a camera sensor to the recorded media file and serving as a unique fingerprint of a single device. The key advantage of the SPN approach is its outstanding classification performance, which is therefore considered the gold standard for SCI. However, since the introduction of the SPN approach in 2006 the use of devices has changed fundamentally; but, the use of SPN within digital forensics remains unchanged.

As a consequence, the contemporary challenges of SCI are not sufficiently analyzed by the digital forensics community in the scope of SPN. First, the SPN approach is designed for *verification* rather than *identification*, hence requires an origin assertion, and thus knowledge about the source to be validated. If little or no prior knowledge of the capturing device is given, the technical performance is not well understood. Second, with the daily use of smartphones, almost everyone has become an everyday photographer and film producer, leading to an enormous amount of media files to be screened during an examination (Junklewitz et al., 2021), a demand for which the SPN approach is not well prepared.

Even worse, more and more sophisticated software features are being introduced into today's digital cameras, but the impact on the capabilities of the SPN approach is unknown. For instance, Google's current Pixel smartphone series makes use of multi-frame super-resolution as described by Wronski et al. (2019), i.e. it merges several RAW frames into one single image. Consequently, such sophisticated features constitute a challenge to the commonly applied SPN approach for SCI, as it leads to a misalignment of pixels, as shown in Fig. 1. Furthermore, Artificial Intelligence-based imaging is already common for smartphones, but is also introduced to Digital single-lens reflex cameras (DSLR), e.g. to suppress unavoidable noise and lens blur (Canon, 2023). Last but not least, the simplification that a digital camera has one sensor is outdated, too (e.g. the iPhone 15 Pro contains four sensors (Apple, 2023)).

Consequently, first publications report that the SPN approach fails for certain cameras and acquisition modes or struggles in the scope of new media file formats (Iuliani et al., 2021; Baracchi et al., 2021; Al Shaya et al., 2018). This means that the digital forensics domain faces tremendous challenges in the realm of SCI. Therefore, the main objective of this paper is to shed light on the field of SCI in the era of contemporary

* Corresponding author.
E-mail addresses: samantha.klier@unibw.de (S. Klier), harald.baier@unibw.de (H. Baier).

https://doi.org/10.1016/j.fsidi.2024.301858
Received 23 April 2024; Received in revised form 5 December 2024; Accepted 10 December 2024

Available online 17 December 2024

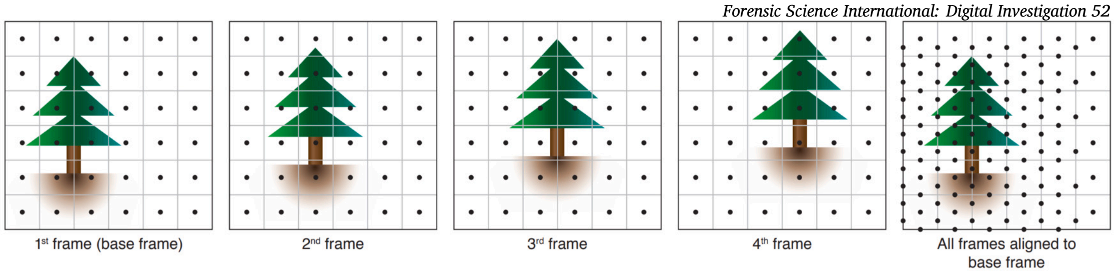

Fig. 1. Misalignment of pixels due to multi-frame usage, as shown by Wronski et al. (2019).

devices and the increasing volume of media files. Our main contributions are threefold:

- We first propose an adopted model to classify Source Camera Identification (SCI). We call it *Source Camera Target Model (SCTM)*. It is based on the classical distinction between Source Camera Identification and Source Model Identification, but the SCTM is more specific and incorporates contemporary features such as software-influenced digital imaging.
- We provide a formal definition of the problem classes *Verification*, *Identification* and *Exploration* in the scope of Source Camera Forensics (SCF). For each problem class, we derive the most important evaluation metrics and illustrate them with appropriate use cases.
- We assess the recognized literature in Source Camera Forensics (SCF) and present and discuss the results. In total, we evaluate 100 publications with respect to our SCTM. Our findings indicate that while ten articles on the SPN approach provide the necessary evaluation metrics for *Verification*, the datasets used for evaluation are entirely obsolete and observational research questions the transferability to contemporary media files. Additionally, we demonstrate that there is little research on efficiency aspects and on the camera software. Overall, there is a paucity of consideration given to the underlying use cases.

The rest of the paper is organized as follows: In Section 2 we introduce some basic aspects of camera identification techniques and discuss related work. The next Section 3 introduces our SCTM to structure the camera identification problem. In Section 4 we introduce the relevant problem classes of camera identification, that is *Verification*, *Identification* and *Exploration* followed by our literature evaluation in Section 5. Finally, Section 6 concludes our paper and points to future research.

2. Background and related work

In this section we provide a brief introduction to common camera identification techniques, starting with the SPN approach due to its dominance in the field of SCI, as proposed and enhanced by Lukas et al. (2006) and Goljan et al. (2009), respectively. Then we move on to other approaches with a focus on technical diversity rather than completeness. Finally, we introduce the Identification Granularity Model (IGM) due to Kirchner and Gloe (2015) which is minimalistic, but the only model proposed for a systematic classification of SCI approaches so far.

2.1. Sensor Pattern Noise approach

The basic idea of the Sensor Pattern Noise (SPN) approach, as proposed by Lukas et al. (2006), is that a digital camera that captured an image can be identified by the noise an imaging sensor introduced to the image by pixel non-uniformity (PNU). This PNU is due to “different sensitivity of pixels to light caused by the inhomogenity of silicon wafers and imperfections during the sensor manufacturing process”, and as such unique per sensor. Subsequently, based on their observations, Lukas et al. (2006) provide an approach to identify the source camera of an image following their scheme to approximate the PNU.

Eventually, to enable the results of the SPN approach to be used as admissible evidence in court, Goljan et al. (2009) conducted a large scale evaluation of their refined SPN approach on more than a million JPEG images.[1] Based on their evaluation that included almost 7,000 devices from 150 digital camera models, they found an incredible False Acceptance Rate (FAR) of below $2.4 \cdot 10^{-5}$ and a False Negative Rate (FNR) of less than 0.0238. With these remarkable results, they established the SPN approach as the gold standard in digital forensics to determine whether an image was captured with a given camera.

2.2. Feature-based Source Camera Identification

Even older than the SPN approach is the Feature-Based SCI which was first proposed by Kharrazi et al. (2004) in 2004 who extracted information from Color Filter Arrays (CFA), the demosaicing algorithm and color processing. Later, the set of features to extract was extended, i.e. by Gloe (2012) to up to 80 features, including additionally, e.g. wavelet statistics and measures of sharpness. After extraction, these features were used in both works to learn a Support Vector Machine (SVM) to attribute a probable source model, e.g. with an accuracy of just above 90% (Gloe, 2012), to the images examined.

Interestingly, the feature-based SCI aims to detect the source among a known set of cameras, when it is contained, rather than providing evidence that is admissible in court. Therefore, the Feature-Based SCI and SPN approach differ significantly, not only in their capabilities but also in their objectives.

2.3. Deep learning based Source Camera Identification

In contrast, rather new types of SCI approaches are data-driven and based on Convolutional Neural Networks (CNNs) which learn features that characterize a camera device or model directly from the given images instead of relying on scientifically established principles. For example, the approach of Bondi et al. (2016) combines a CNN for feature extraction with an SVM for classification. To be more precise, the CNN is trained on non-saturated patches of the training images to learn relevant features to extract, which are the input for the SVMs that attributes a camera model to the test images based on a concluding majority voting. Overall, they achieve a classification accuracy of over 93% for models from the Dresden Image Database (DIDB). Interestingly, the CNN can be used to extract features from images of unknown camera models which avoids costly re-training, as only the SVMs must be adapted to new camera models. However, Liu et al. (2021) indicate, that the accuracy may be lower than what has been reported.

Over time, many different schemes of CNN-learning have been proposed (Castillo Camacho and Wang, 2021) which, despite the model itself, differentiate mostly by patch selection and pre-processing. For example Rafi et al. (2019), who achieve a classification accuracy for models of over 99% on the DIDB, focus on data augmentation which includes e.g. compression, gamma correction, cropping and flipping of

[1] Taken from Flickr.com.

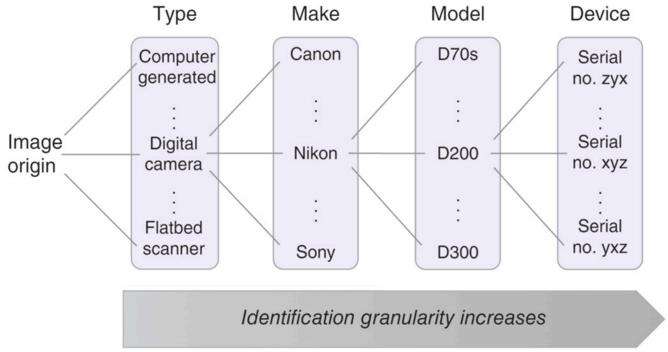

Fig. 2. Model of Source Camera Identification due to Kirchner and Gloe (2015).

the patches with the best characteristics for training and apply Empirical Mode Decomposition to remove random high-frequency noise. In contrast, Liu et al. (2021) emphasize data diversity due to representative patch selection (i.e. edge and textural patches) and use a residual prediction module which can be seen as pre-processing with an adaptive denoising filter. They report a classification accuracy for models of over 98% on the DIDB.

To sum up, just like feature-based SCI deep learning based methods are rather used to attribute a known camera model to an image instead of proving the origination from a particular device.

2.4. Metadata based Source Camera Identification

However, the most basic form of SCI is the manual analysis of Exif tags, such as the *Make* and the *Model* fields (Orozco et al., 2013), which is obviously easily subverted. In contrast, the more profound approach of Kee et al. (2011) from 2011 considers, e.g. the structure of the Exif headers, and consequently finds that 99% of manufacturers of digital cameras had a unique signature, but only 62% of individual cameras, based on 2.2 million images.[2]

Although these results are unsatisfactory for many use cases of SCI, the lightweight nature of the approach motivated Mullan et al. (2019) to study the implications of smartphone photography on the approach. In conclusion, they found a disappointing classification accuracy of only 0.65 for the source model. However, they were able to classify the operating system version with an accuracy of 0.82, just by counting how many Exif tags were set in certain areas of a JPEG's header. Consequently, their results demonstrate that there is more to identify beyond the common Make, Model and Device identification targets.

However, metadata is perceived as being unreliable due to the ease of tampering. Nevertheless, some results (Klier and Baier, 2024) suggest that they may still be of benefit to an investigation by helping investigators to prioritize.

2.5. The Identification Granularity Model

The first proposed abstract order of the source identification problem, due to Kirchner and Gloe (2015) is shown in Fig. 2 which names the *Device*, *Model*, *Make* and *Type* as attributable in a source identification task. These classes are ordered from left to right by increasing identification granularity, as Kirchner and Gloe (2015) point out, hence, we will refer to this model as Identification Granularity Model (IGM).

Undoubtedly, the identification of a specific device is fundamental (Geradts et al., 2001), and is intuitively perceived as the goal to strive for (Kirchner and Gloe, 2015) due to its status as the most *granular* identification class. However, Kirchner and Gloe (2015) show that there is also digital forensic value in the identification of the other classes presented. For instance, when higher identification granularity is hardly achievable due to lacking prior information or for pre-processing steps to reduce the amount of resource consumption.

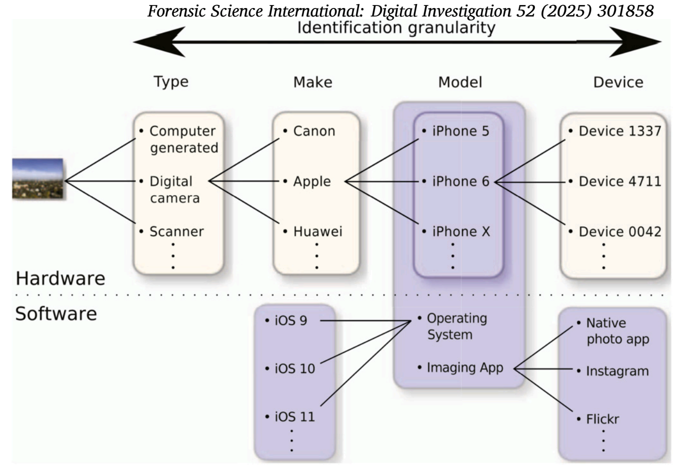

Fig. 3. Illustration of the IGM extended by software due to Mullan et al. (2019).

The IGM, which is sometimes perceived as a hierarchy, is implicitly (Gloe, 2012; Mullan et al., 2020; Gloe and Böhme, 2010; Kee et al., 2011; Mullan et al., 2020) or explicitly (Mullan et al., 2019; Marra et al., 2017; Bernacki, 2020) present in many publications, but not an important part of the respective research. However, recently Mullan et al. (2019) directly addressed the IGM, as they found that their metadata-based approach (for details see Section 2.4) to source identification on iPhones identified the software stack rather than the actual device which could not be mapped to the commonly used identification classes of the IGM.

Therefore, to be able to illustrate their findings, Mullan et al. (2019) added a vertical layer to the IGM to represent software aspects, as shown in Fig. 3. Arguably, they connected the whole software stack, beginning with the operating system (i.e. iOS) and continuing through to photo sharing platforms (i.e. Flickr) and the *Model*. This is somewhat perplexing, given that neither the operating system nor any application is linked to a specific model. Nevertheless, their primary objective was not the IGM, but rather the necessity to present their results which highlights the imperative for a considered amendment of the IGM in order to accommodate the evolving landscape of digital imagery.

3. The Source Camera Target Model

We propose the Source Camera Target Model (SCTM), which is shown in Fig. 4, and we discuss each facet of our model which is more specific than the IGM and incorporates contemporary features of software-influenced digital imaging.

3.1. Area of interest

In this paper, our focus is solely on *Source Camera Forensics (SCF)*. We differentiate this concept from any form of "Type" recognition, which is depicted in the IGM but is not within the scope of our study (indicated by the black dashed frame). Additionally, we examine the software stack, beginning with the operating system and its imaging routines, and extending to the actual application that can capture media until the media file is saved for the first time. Therefore, we consider apps that took photos or record videos, while excluding any post-processing of previously recorded media files from our research scope. For the time being, we refrain from differentiating the software stack, for example, into firmware, operating system, and applications, due to the uncertainty of the dependencies involved.

[2] Downloaded from Flickr.

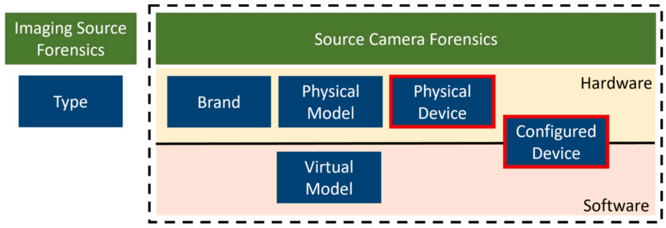

Fig. 4. The proposed Source Camera Target Model (SCTM). (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

3.2. The source camera targets

Nonetheless, the dark blue boxes represent our valid objectives for SCF, which are primarily based on the conventional categorization of "Make", "Model" and "Device". Furthermore, we adhere to the vertical separation of hardware and software, as suggested by Mullan et al. (2019). However, we enhance the model in the following manner:

1. We introduce a *Physical Model* and a *Virtual Model* whereas the first is analogous to the classical "Model" and the latter is referring to the software stack only (as defined in Section 3.1).
2. We rename the "Device" to *Physical Device* for the sake of clarity.
3. The *Configured Device* is a novel concept that combines the *Physical Device* and the *Virtual Model*, resulting in the device with which the user actually interacts.
4. We use the term *Brand* to refer to the "Make" which better captures the commonly intended meaning.

About granularity and uniqueness However, a clear order by granularity over the hardware and the software layer, as proposed by Kirchner and Gloe (2015) and Mullan et al. (2019) is unattainable, because hardware and software layer are coupled, but only loosely. On the one hand, not every operating system is available for every model, e.g. an iOS version is only available for certain iPhones. However, on the other hand, each iPhone model can be used with several versions of iOS, each of the combinations representing a new *Virtual Model*. Therefore, it is uncertain whether the *Physical Model* or this basic *Virtual Model* is more frequent to exist.

Even worse, the *Virtual Model* exists in a spectrum of granularity, since the complete software stack that is involved in the generation of the media file is considered. For example, the combination of iOS 17.1 with the native "Camera" app will be significantly more common than the combination of iOS 17.1 with "Kik Messaging & Chat App" 16.14.2 for recording media files. Therefore, we abandon a rigid order based on granularity and instead highlight only the unique identification targets (see the targets with a red frame), specifically the *Physical Device* and the *Configured Device*.

About volatility Furthermore, the software layer introduces an unseen time dependency, due to its volatility through regular and asserted updates. For example, major iOS versions are released every year, but sub-versions and updates to the "Camera" app are released more frequently. Hence, the identification of the *Virtual Model* or the *Configured Device* also provides a valuable reference to the period of time in which a media file was produced.

About the brand When we refer to the "Make" or "Manufacturer" of a device, we typically mean the brand the device was released under, such as "Apple" or "Canon". Consequently, we utilize the more precise and particular term. Moreover, there is not a single manufacturer producing a smartphone. Rather, there is an assembler, who combines components from numerous manufacturers, each of which may engage with different brands. Therefore, the actual manufacturer or even the assembler of certain camera components could also be an identification target. However, for the time being, we exclude these targets from our model, as their forensic significance is limited.

Table 1
Grouped SCF problem classes with their characteristics and crucial evaluation metrics.

	Verification	Identification	Exploration
Media Files ($\|M\|$)	≥ 1	≥ 1	≥ 1
Cameras ($\|C\|$)	$= 1$	> 1	$= 0$
Eval. Metrics	FAR, FPR FRR, FNR	TPR, REC, SEN PPV, PREC	COMP HOM
Perf. Requ.	-	Time: extraction, look up Storage: reference	scalability to $\|M\|$

4. Problem classes of Source Camera Forensics

Besides the target for SCF, the specific use case greatly influences the requirements and considerations involved. Instead of providing a descriptive list of use cases to categorize existing approaches, we will adopt a formal approach that allows us to identify problem classes without blind spots and subsequently consolidate the use cases of source camera forensics.

4.1. Formal derivation of problem classes

In the context of Source Camera Forensics (SCF), our objective is to examine a set of media files, denoted as M, in conjunction with a set of potential source cameras, denoted as C. To reveal all relevant problem classes, we generate the permutations when the number of elements in M or C is 0, 1, or > 1. However, we exclude permutations where $|M| = 0$, as an investigation cannot be carried out without any media files. Subsequently, we group the permutations according to the size of the camera set C, which signifies prior knowledge of the case and, consequently, determines the class of the problem.

Finally, we assign names to each of the groups according to their purpose and present our problem classes in Table 1. We classify them into three categories:

- *Verification* whether a specific camera was used to capture one or more media files;
- *Identification* of a source camera from a collection of relevant cameras; and
- *Exploration* when there is no prior knowledge of relevant cameras

Typically, every examination of SCF begins with a collection of media files and ends when a link between the digital evidence and a suspect is established, e.g. through the successful verification of the source camera. However, the specific path and the problem classes involved in an investigation or examination vary depending on the particular case. In Fig. 5, we present a visual representation of the relationships between these problem classes, which are defined by the available knowledge of the case and their intersections. Now we will provide a detailed discussion of these relationships.

4.2. Verification

We start our explanation with the problem class of *Verification* due to the inclusion of the most classic scenario of SCFs as introduced by Geradts et al. (2001) which involves a single media file (M_x) and a single camera (C_y), and the main objective is to obtain a highly accurate yes or no answer to the exemplary question:

Has media file M_x been captured with camera C_y?

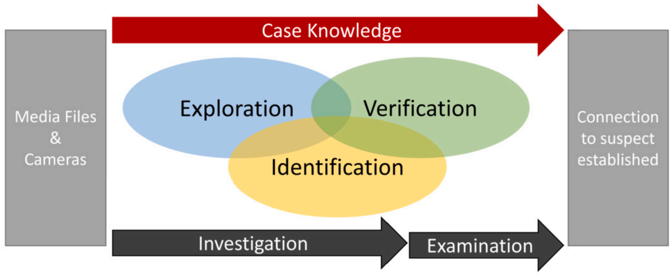

Fig. 5. Proposed scheme of SCF, starting with a set of media files and (optionally) case relevant cameras, available case knowledge determines the appropriate problem classes, endpoint of the investigation is when a connection to a suspect is established.

Thus, the *Verification* problem class is characterized by a hypothesis, that is "H = media file M_x has been captured with camera C_y." which must be refuted or verified, hence the name. Consequently, this problem class is particularly well-suited for examinations and less so for investigations. In particular, *Verification* requires a high degree of prior knowledge of the case, and thus is only applicable when a specific camera is suspected to be the source, although that camera need not be available for examination.

Performance evaluation The main objective of this problem class is to determine scientifically, with a known level of certainty, whether a camera is the source of a specific media file or not. This means that in a court setting, the assessment of the media file M_x, as the product of C_y, must stand for itself. Therefore, this requirement is similar to the scientific attribution of a fingerprint found on a crime scene to a specific individual. Consequently, certainty in this case is characterized by the likelihood that the hypothesis has been falsely accepted, as measured by the False Acceptance Rate (FAR) and the False Positive Rate (FPR) or refuted which is measured by False Rejection Rate (FRR) and False Negative Rate (FNR).

However, even in cases where there is a multitude of media files involved, the speed at which the files are processed is not a significant concern. One reason for this is that a hypothesis must be proven, for which one media file is sufficient. For instance, a murder is investigated and the case involves thousands of media files showing the perspective of the murderer. While the murderer cannot be identified from the footage, the investigators have a suspect and seized their smartphone. Consequently, it is effectual for now, to prove that the most convicting media file was captured with the suspect's smartphone. Hence, reducing the examination effort to one comparison per hypothesis, making performance considerations superfluous.

4.3. Identification

Unlike the *Verification* problem class, the *Identification* problem class is driven by findings and, hence, is investigative in nature. In this case, the investigators aim to determine the source camera of the media files based on a known set of relevant cameras C, which is a well-known classification problem in digital forensics (Goljan et al., 2009). Therefore, the main objective of *Identification* are large camera sets under the assumption that the set of cameras, although large in size, are based on a considerable amount of prior knowledge. Otherwise, the case is better served by either *Exploration* or *Verification*, as shown in Fig. 5.

Consequently, in the current stage of an investigation, it is considered successful if the number of potential source cameras is minimized to a small number or if it can be ruled out that the source camera is known, thereby increasing the case knowledge. Consequently, investigators, for example, inquire:

> Which cameras in C have probably captured the media file M_x?

As a result, the answers obtained are valuable for an investigation, but cannot be utilized as evidence for a conviction. Therefore, to firmly connect, e.g. M_x to the suspect, some form of verification has to be applied subsequently. Certainly, this division into two distinct problems, namely *Identification* and *Verification*, is in stark contrast to previous research that assumes that an *Identification* must yield a definitive and certain result by itself. A comprehensive examination of this matter will be presented in Section 5.3.

Performance evaluation Consequently, the greatest concern in this problem class must be that the source camera is known but not identified, which can prevent or at least hamper an investigation. Therefore, we mainly evaluate the true-positives (TPs) in relation to the false-negatives (FNs), hence, with a metric such as True Positive Rate (TPR), also called Recall (REC) or Sensitivity (SEN). Additionally, efficiency must be ensured, hence, the relation between false-positives (FPs) and TPs has to be favorable, which e.g. is measured by the Positive Predictive Value (PPV) or by Precision (PREC).

Lastly, in this specific problem class, there are demands on runtime and storage efficiency because of the numerous cameras and look-ups required. Therefore, any approach addressing this problem category should consider: (i) the runtime efficiency of the extraction phase, as well as, (ii) the runtime efficiency of the look up and (iii) the storage efficiency of the camera references. However, the actual constraints for each of the aspects, depend on the investigated case.

4.4. Exploration

Eventually, the *Exploration* problem class is characterized by a lack of prior case knowledge in terms of involved cameras and mostly relevant to large sets of media files. To illustrate, investigators have confiscated a server that had been utilized by a collective to disseminate CSAM, of which some is likely self-produced. Hence, they first and foremost may ask the question:

> Which media files of M have probably been captured with the same camera?

Again, we concentrate solely on investigative approaches here, which means that investigators must keep in mind that the results of *Exploration* are not intended to be a proof. Therefore, similarly to the *Identification* problem class a *Exploration* is not the end of an investigation, but rather the start.

Performance evaluation Therefore, when faced with such a set of media files, our primary focus should be to ensure that related evidence remains together. For instance, one perpetrator in the given CSAM case sexually abused three children on three different occasions, but captured all the assaults with the same camera. However, the perpetrator can only be identified while abusing one of the children. If all three assaults are grouped together, the investigation can further verify that the three assaults were committed by the same perpetrator. However, if these media files are separated, investigators can only attribute one assault to this perpetrator, leaving two cases unsolved. Vice versa, if media files are grouped together that do not belong together, this reduces the efficiency of the approach, as more media files than necessary have to be investigated further, but evidence will not be missed.

Thus, the performance evaluation resembles that of the *Identification* problem class, but in the context of clustering. Therefore, the metrics to consider are Completeness (COMP) (Rosenberg and Hirschberg, 2007) and Homogeneity (HOM) (Rosenberg and Hirschberg, 2007), which are the counter-parts of the TPR and PPV, respectively. Furthermore, the ability to scale with the number of media files is crucial in this particular problem class.

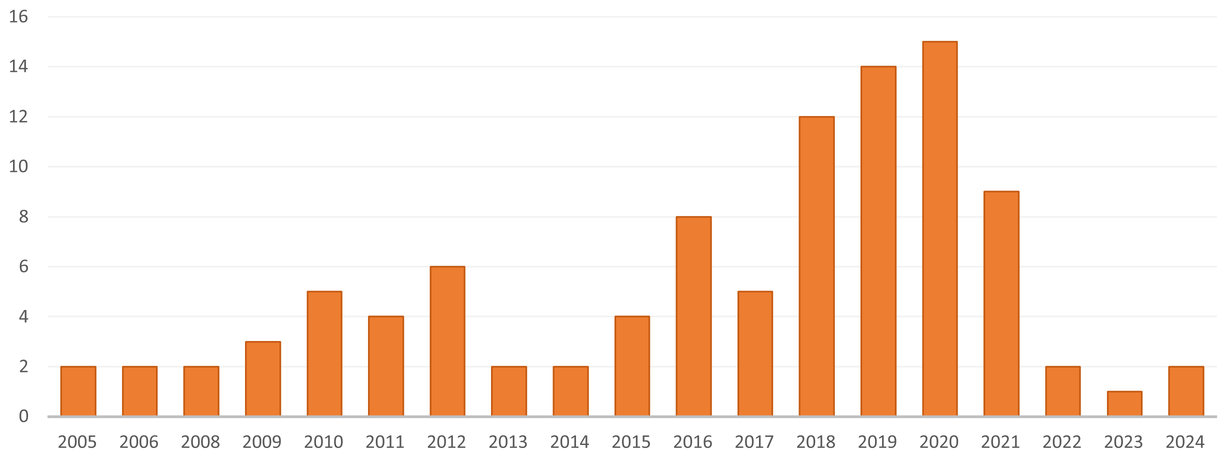

Fig. 6. Selected publications illustrated as count per year.

5. Evaluation of recognized source camera forensic approaches

This section starts with an evaluation of recognized research papers in terms of fundamental statistics. We then assess our proposed SCTM with respect to the derived problem classes from Section 4. Finally we turn to the objective of determining whether there is a gold standard in the scope of SCI.

5.1. *Considered corpora of research*

In order to conduct our assessment of SCF, we have considered research that is currently influential within the field. To this end, we have taken into account seminal works that have been incorporated into the most recent literature reviews on the topic, as well as the most relevant journal and conference proceedings. To be more precise, we consider every SCF research paper referenced in the works of Nwokeji et al. (2024), Sencar et al. (2022), Akbari et al. (2022b), Castillo Camacho and Wang (2021) and Bernacki (2020), as well, as publications from Elsevier's "Forensic Sciences International: Digital Investigation" from 2019 until September 2024, hence, also include publications from the DFRWS conferences. However, we excluded any research that focused exclusively on post-processed media files, authentication, anti-forensics, or is unpublished.

We provide our complete data basis of our upcoming analysis.[3] In addition, Table A.3 in the Appendix shows an excerpt of all articles that were successfully classified into one of the problem classes or if the main objective is to provide theoretical understanding, to which we refer as *Observational*.

5.1.1. *Fundamental statistics*

In total, we selected and classified 100 research papers, for which we show a chronology in Fig. 6 that illustrates the publication year of research that is influential for SCF today. Overall, 75 research papers address images, 20 videos and 4 both, which demonstrates a clear imbalance in favor of images. While images are easier to use for research due to their smaller size and greater availability, this finding is still alarming because videos are just as easy to capture as images and have become an integral part of many people's daily lives.

Furthermore, we find that recognized research mostly aims at the *Physical Device*, as shown in Fig. 7, which is not surprising due to its high forensic value as a unique target. However, no research has yet been conducted on the *Configured Device* which is the second unique target and is newly proposed as a legit target, which is therefore also not

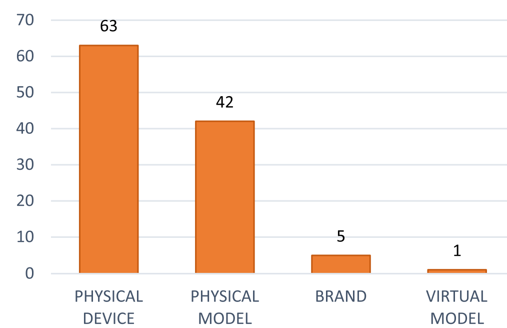

Fig. 7. Publications per Source Camera Target. (Due to papers aiming at several source camera targets, the total exceeds the amount of considered papers.)

surprising. However, the equally new *Virtual Model* has been researched once, namely by the work of Mullan et al. (2019) which we discussed in Section 2. This is also the only work that has focused on a purely software-defined target, which indicates a research gap in this area.

5.1.2. *Types of approaches*

Subsequently, the methods employed were classified in accordance with the methodology outlined in Section 2, and the correlation between these and the publication year is illustrated in Fig. 8. Accordingly, we differentiate between papers that utilize diverse types of SPN-, feature-, metadata- and CNN-based approaches, or a combination thereof. It is noteworthy that mixed and metadata approaches have received almost no attention in the literature. In contrast, the SPN approach is the most prevalent method in terms of the volume of recognized research. Furthermore, the SPN approach has been the subject of ongoing research since its inception in 2006, with a notable increase in activity in recent years (2022-2024 is probably too recent to be recognized in literature reviews). Despite the continued research into feature-based and CNN-based approaches, there is no discernible increase in activity over time. However, CNN-based approaches are still in their infancy.

5.1.3. *Used data sets*

Also, we elaborated which data sets have been used in the considered corpora of research to evaluate the approaches which is of utmost importance in SCF. Hence, Fig. 9 illustrates the correlation between the publication year and the data set employed. On the one hand, we have published forensic data sets, such as the DIDB (Gloe and Böhme, 2010), VISION (Shullani et al., 2017), Video-ACID (Hosler et al., 2019) and SOCRatES (Galdi et al., 2019), whereas more are available, such as the Qatar University Forensic Video Database (QUFVD) (Akbari et al., 2022a) or New York University Abu Dhabi - Mixed Media Dataset

[3] https://data.mendeley.com/datasets/8tzx9dwryc/2.

Year	SPN	FEATURES	CNN	METADATA	MIXED
2005	0%	2%	0%	0%	0%
2006	1%	1%	0%	0%	0%
2008	2%	0%	0%	0%	0%
2009	2%	1%	0%	0%	0%
2010	3%	2%	0%	0%	0%
2011	2%	2%	0%	0%	0%
2012	2%	4%	0%	0%	0%
2013	1%	1%	0%	0%	0%
2014	2%	0%	0%	0%	0%
2015	2%	2%	0%	0%	0%
2016	4%	2%	1%	0%	1%
2017	4%	0%	1%	0%	0%
2018	7%	1%	4%	0%	0%
2019	7%	1%	5%	1%	0%
2020	10%	1%	2%	2%	0%
2021	6%	1%	2%	0%	0%
2022	1%	0%	1%	0%	0%
2023	0%	0%	1%	0%	0%
2024	0%	1%	1%	0%	0%
Total	**56%**	**22%**	**18%**	**3%**	**1%**

Fig. 8. Publications per mean and year in percentage of grand total. Colored by allocation over time.

	DIDB	VISION	Video-ACID	SOCRatES	other	Flickr	own
2005					0%	0%	100%
2006					0%	0%	100%
2008					0%	33%	67%
2009					0%	33%	67%
2010	20%				0%	0%	80%
2011	40%				0%	0%	60%
2012	29%				0%	14%	57%
2013	50%				0%	0%	50%
2014	33%				0%	33%	33%
2015	40%				20%	20%	20%
2016	45%				0%	9%	45%
2017	50%	17%			17%	0%	17%
2018	69%	0%			15%	15%	0%
2019	27%	18%	5%	5%	23%	9%	14%
2020	15%	31%	8%	4%	27%	8%	8%
2021	15%	8%	15%	8%	31%	8%	15%
2022	0%	50%	0%	0%	50%	0%	0%
2023	100%	0%	0%	0%	0%	0%	0%
2024	25%	25%	0%	25%	0%	0%	25%
Total	30%	12%	4%	3%	15%	9%	27%

Fig. 9. Data set types used per publication year in percentage of data sets used per year. Colored per data set type and usage over time. Blank cells indicate the period preceding publication.

(NYUAD-MMD) (Taspinar et al., 2020) which, however, have been used twice or less and are summarized in the "other" category.

On the other hand, we have a conglomerate of heterogeneous data sets, either they have been created by the authors of the publications and are not published ("own") or by downloading images from Flickr[4] whereas each publication uses a different data set. However, these data sets are reproducible when their references have been published and under the condition that the images are still accessible. Furthermore, while "Flickr" may allow access to media files from up-to-date cameras, it does only provide JPEGs in their native state

The first published forensic image data set from 2010, namely the DIDB, is still prevalently used. Although, eleven publications since 2019 use the DIDB additionally to a more recent data set, three publications (Bharathiraja et al., 2023; Liu et al., 2021; Yang et al., 2019) use solely the DIDB for their evaluations. The next most used data set is VISION which publication dates back to 2017. Over all used published data sets the newest incorporated Apple Smartphones are the iPhone 8 (Akbari et al., 2022a; Hadwiger and Riess, 2021; Tian et al., 2019; Al Shaya et al., 2018) and XS max (Akbari et al., 2022a) which have been released 2017 and 2018, respectively. Hence, no available data set can be seen as contemporary.

Moreover, the scale and heterogeneity of the data sets employed are constrained. To illustrate, the DIDB is one of the most comprehensive data sets, comprising approximately 15,000 images captured by 68 digital cameras of 24 models. While the creation of such data sets represents a significant undertaking, it represents a mere fraction of the total number of cameras and models in circulation, as well as media files that may need to be examined. However, this issue can be circumvented by utilizing a data set downloaded from Flickr, though this approach has the limitation of only providing images in their native state and lacking ground truth information.

[4] https://www.flickr.com/.

It is notable that, despite the availability of published data sets, the use of evaluation with 'own' data sets has declined, but persists without clear justification from the authors.

5.2. Problem classes and research

We examine the alignment of the SCF research with our proposed SCTM and problem classes, subsequently discussing the implications for each problem class.

5.2.1. Alignment

Next, we assess the alignment of the considered approaches with the problem classes we proposed in Section 4 based on the respective evaluation metrics. Overall, from 100 research papers, only 15 evaluation results align with the problem classes of SCF and 80 approaches meet the requirement of no problem class, as shown in Fig. 10. Additionally, seven papers are a special case due to their solely observational nature, hence, do not conduct an evaluation.

Specifically, most of the 80 misaligned approaches report the FPR along with the TPR, which is inconsistent with our proposed requirements of both *Verification* (FPR, FNR) and *Identification* (TPR, Specificity (SPEC)). Nevertheless, this finding does not invalidate the approaches themselves, as they are potentially applicable to both problem classes. Rather, it demonstrates that the majority of research does not sufficiently consider the implications of the actual use case.

Similarly, clustering research primarily reports the Accuracy (ACC) of their approaches, which may be interesting for benchmarking, but is not sufficient for forensic use cases due to the lack of differentiation between different types of error, which can make a significant difference, as argued in Section 4. In conclusion, only one approach (López et al., 2020) reports the necessary metrics to qualify for the *Exploration* problem class.

5.2.2. Verification approaches

Overall, ten papers (see Table 2) provide the metrics necessary to evaluate an approach of the *Verification* problem class. These include,

Table 2
A summary of works that meet the requirements of the specified problem class.

Paper	Target(s)	Means	Media Type	Data Set(s)
VERIFICATION (10 classified, 31 candidates)				
Lukas et al. (2006)	PHYSICAL DEVICE	SPN	IMAGES	own
Chen et al. (2008)	PHYSICAL DEVICE	SPN	IMAGES	own, Flickr
Amerini et al. (2009)	PHYSICAL DEVICE	SPN	IMAGES	own
Goljan et al. (2009)	PHYSICAL DEVICE	SPN	IMAGES	Flickr
Lawgaly and Khelifi (2016)	PHYSICAL DEVICE	SPN	IMAGES	DIDB, own
Ferrara and Beslay (2020)	PHYSICAL DEVICE	SPN	VIDEOS	VISION
Mandelli et al. (2020)	PHYSICAL DEVICE	SPN	VIDEOS	VISION
Lawgaly et al. (2021)	PHYSICAL DEVICE	SPN	VIDEOS	Video-ACID
Yang et al. (2021)	PHYSICAL DEVICE	SPN	VIDEOS	VISION
Ferrara et al. (2022)	PHYSICAL DEVICE	SPN	VIDEOS	VISION
IDENTIFICATION (6 classified, 11 candidates)				
Valsesia et al. (2015)	PHYSICAL DEVICE	SPN	IMAGES	Flickr
Akbari et al. (2022a)	PHYSICAL DEVICE, PHYSICAL MODEL	CNN	VIDEOS	QUFVD
Bharathiraja et al. (2023)	PHYSICAL DEVICE	CNN	IMAGES	DIDB
Anmol and Sitara (2024)	PHYSICAL DEVICE, PHYSICAL MODEL	FEATURES	VIDEOS	VISION, SOCRatES, QUFVD
EXPLORATION (1 classified, 5 candidates)				
López et al. (2020)	PHYSICAL MODEL, BRAND	METADATA	VIDEOS	VISION, Video-ACID

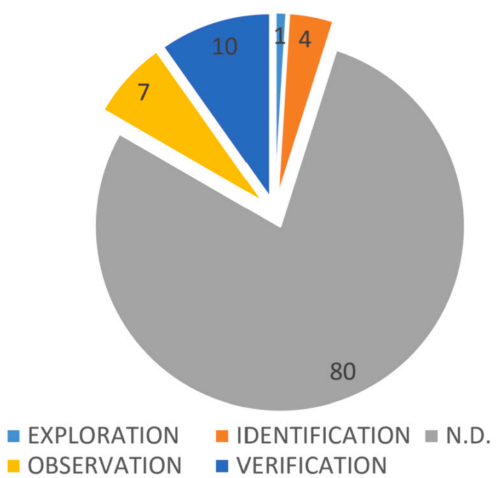

Fig. 10. Publications satisfying the requirements for the respective problem class. (Due to papers aligning with more than one problem class, the total exceeds the amount of considered papers.)

the most well-known and fundamental papers on the SPN approach, namely the work of Lukas et al. (2006) and Goljan et al. (2009). It is noteworthy that each work utilizes some form of SPN approach, targets the physical device and that images and videos are addressed in an equal number of research papers.

Undoubtedly, a substantial body of research has been conducted on the SPN approach, including very large image sets, e.g. Goljan et al. (2009) found astonishingly low FAR and FNR on the basis of more than a million images from almost 7000 individual digital cameras of 150 models. Therefore, the *Verification* of a *Physical Device* using the SPN method has been a subject of thorough investigation in the past. However, the most recent study on image *Verification* dates back to 2016 (Lawgaly and Khelifi, 2016) and employs only the DIDB along with an unpublished data set.

However, the studies carried out on the *Verification* of video files are typically more current, with their publication dates spanning from 2020 to 2022, and utilize exclusively published data sets, specifically VISION (Shullani et al., 2017) and Video-ACID (Hosler et al., 2019). However, even those data sets are many years behind the current camera market, as discussed in Section 5.1.3. Furthermore, the data sets used are considerably smaller than the large-scale test of Goljan et al. (2009) for images, as, e.g. the VISION data set contains only 35 devices of 29 models.

5.2.3. Identification approaches

Conversely, only four papers (see Table 2) align with the *Identification* problem class, although once more, one half addresses images and the other half addresses videos. However, there is diversity in terms of the targets addressed and the means employed, and the publications are considerably more recent than those of *Verification*, dating back to 2023 and 2024 for images and videos, respectively.

Although published recently, Bharathiraja et al. (2023) evaluate their approach solely on the DIDB from 2010. Furthermore, the issue of efficiency has only been addressed by Valsesia et al. (2015) and Akbari et al. (2022a), who have presented at least some efficiency metrics, including processing time per frame or video and RAM usage. However, among the unclassified papers, there are eleven approaches that take efficiency issues into account and are evaluated at least to one *Identification* metric, hence, are a candidate.

5.2.4. Exploration approaches

Even less research falls into our *Exploration* problem class, specifically only the work of López et al. (2020) (see Table 2) which addresses videos applies. However, they did not evaluate scalability or runtime efficiency, which would be the primary strengths of a metadata-based approach.

However, there are other clustering approaches that may be applicable for *Exploration*, but, they report heterogeneously divergent evaluations metrics, such as the TPR (Caldelli et al., 2010), FPR (Amerini et al., 2014), FRR (Tomioka and Kitazawa, 2011), or the Adjusted Rand Index (ARI) (Marra et al., 2017), although only the latter is a dedicated clustering metric. Arguably, the HOM and COMP we expect to evaluate are relatively new, having been published in 2007 (Rosenberg and Hirschberg, 2007), and may not yet have been widely adopted in the field of digital forensics. In total, however, only five papers would be candidates for *Exploration*.

5.3. Do we have a gold standard?

Firstly, there cannot be a single gold standard for SCF, given the considerable divergence in use cases across the field, as previously discussed in Section 4. Although this may seem apparent, it is not reflected in the corpus of existing literature on the subject.

For example, every approach for *Identification* and *Exploration* from Table 2 is more concerned of false-positives, e.g. measured in the form of *PPV* or HOM, than of false-negatives which is more reasonable when the use case is considered (see Section 4). Moreover, two out of four *Identification* approaches and nine of the eleven candidates seek to achieve a favorable FAR or FPR. This phenomenon may be attributed to the influence of the seminal works by Lukas et al. (2006) and Goljan et al. (2009). As a result, although the problem classes *Identification* or *Exploration* are targeted, the approaches try to overcome the bar set by the SPN approach. Hence, this may impede the development of approaches tailored to the specific use case. Therefore, the question nowadays must be:

“Do we have a gold standard for *Verification*, *Identification* and *Exploration*?”

5.3.1. *Verification*

Metaphorically a gold standard describes something that sets the highest standard of quality or performance. Undoubtedly, the SPN approach with the evaluation results discussed in Section 2 can be seen as such for the *Verification* of images and, hence, monopolizes the whole problem class (see Table 2). Nevertheless, the outcomes for videos are not as favorable as those for images and are not derived from similarly expansive data sets.

However, in-depth research conducted on camera hardware, shows that not just a sensor’s wafer imperfections, as initially proposed by Lukas et al. (2006), contributes to the SPN, but also e.g. the dark current and the lens optical system (Matthews et al., 2019, 2020). While these findings do not invalidate the approach as a gold standard in and of themselves, they represent a potential flaw and indicate a lack of comprehension at the hardware level.

In light of the above, it is unsurprising that the transition from digital cameras with CCD sensors to CMOS sensors occurred without significant controversy, in stark contrast to the potential for debate surrounding this technological shift. For example, Lawgaly and Khelifi (2016) identify which cameras in their data set utilize CCD or CMOS sensors, yet do not address this issue in their evaluation. Furthermore, Goljan et al. (2009) present no statistics on this issue, despite the fact that some of the authors of their earlier work (Chen et al., 2008) suspected that the CMOS sensor was the reason for the significantly inferior results of the respective camera. Additionally, the most widely used data set (see Fig. 9), is the DIDB, which contains exclusively digital cameras with CCD sensors.

Moreover, there is research available that provides insight into specific topics, namely new data formats such as HEIF[5] (Baracchi et al., 2021), the impact of compression (Chuang et al., 2011), HDR capturing mode (Al Shaya et al., 2018), pixel-binning (Taspinar et al., 2021) and smartphone cameras (Iuliani et al., 2021; Baracchi et al., 2021). In summary, they all show that each of the technologies studied is a significant hurdle for the SPN approach.

Consequently, first works demonstrate that images are falsely attributed to smartphones (Baracchi et al., 2021; Albisani et al., 2021; Al Shaya et al., 2018). Moreover, in 2021 Iuliani et al. (2021) analyzed nearly $25,000$ images from 486 devices belonging to 45 smartphone models and 114 devices belonging to 25 digital camera models,[6] demonstrating that the considered models exhibited an FPR in the range of $[0, 0.992]$, contingent on the selected resolution. In Fig. 11 we show the individually reported FPR (in %), due to Iuliani et al. (2021), in a box plot. Only 24 models show a FPR in the accustomed domain of below 10^{-5} (Goljan et al., 2009), the median is at $3.0 \cdot 10^{-3}$ which is more than a hundred times higher than what is generally considered to be neglectable. Moreover, the upper quartile is at 0.1 and twelve models, are

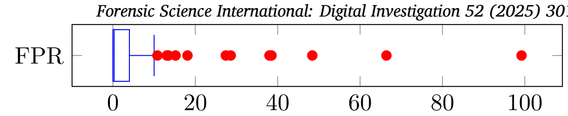

Fig. 11. FPR (in %), as individually reported by Iuliani et al. (2021) for the SPN approach. Median is at 0.3%.

even beyond this upper fence, making the approach practically unusable on certain devices.

It can thus be concluded that the SPN approach, in the absence of an adversary, represents the current standard for *Verification*. But, the whole perception of the SPN approach to be impeccable relies on antiquated data sets, which are merely unpublished. Therefore, it is highly questionable whether the SPN approach can yield the same impressive results as in previous studies, in the wild today. Consequently, it no longer constitutes a gold standard and a match for a modern camera should not be regarded as compelling evidence without further comprehensive consideration.

5.3.2. *Identification and exploration*

Once more, the most significant issue is the use of outdated data sets, which raises questions about the continued achievability of the reported TPR and PPV of ≥ 0.90 and ≥ 0.98, as presented in the studies by Valsesia et al. (2015) and Bharathiraja et al. (2023), respectively. Notably, the results reported López et al. (2020) vary considerably depending on the data set utilized. For example, the TPR is 0.81 for the VISION data set and 0.55 for the newer QUFVD. Although our expectations are different and less rigorous, this result is nevertheless a cause for concern.

Finally, the body of research is limited, with regard to the *Identification* and *Exploration* and the restricted scope and diversity of the data sets employed, raise questions about the applicability of these approaches on a larger scale today. Consequently, it can be concluded that this field of research is still in its infancy and that a standardized methodology still needs to be established.

6. Conclusion and future work

Overall, the SPN approach is widely perceived as the gold standard, but there are legitimate and profound concerns about the reliability of its results for modern media files. On the one hand, practitioners of digital forensics cannot expect robust assurances in this regard; on the other hand, research in this area is facing its greatest challenge since its inception in 2006, yet both disciplines are barely aware of the changed reality. Until we have up-to-date benchmarks based on agreed metrics and obvious constraints, we must be extremely cautious about applying the SPN approach in the wild.

Moreover, the investigative approaches to Source Camera Forensics, namely *Identification* and *Exploration*, are largely overlooked despite their relevance to law enforcement. Therefore, by distinguishing between different problem classes and clarifying the respective expectations, we encourage research in these side-lined sub-disciplines by exempting them from the strict requirements that must be placed on evidence to hold up in court. Consequently, only *Verification* approaches need to be applied.

However, SCF can no longer rest on the success of the SPN approach and needs extensive further research to catch up with the advances in digital imaging and its use. Therefore, research needs to be done on modern imaging pipelines, from hardware, as suggested by Matthews et al. (2019), to software and artifacts introduced by AI-based imaging. Certainly, we will use the leeway provided by these results to propose approaches tailored to the efficiency-driven problem classes *Identification* and *Exploration*. However, there is a huge demand for large and constantly updated datasets that must be satisfied to eventually establish a gold standard for each of the common use cases in SCF.

[5] This is the default for iPhones since iOS 11 (Apple, 2024).

[6] Downloaded from Flickr.

Table A.3
Excerpt of considered seminal works with the approach used, excluding unclassifiable works and sorted descending by date of publication.

Publication	Year	Target(s)	Means	Perf. Metrics	Effic. Metrics	Media Files	Data Set	PC
Ferrara et al. (2022)	2022	PHYS. DEVICE	SPN	FPR, FNR		VID.	VISION	VER
Akbari et al. (2022a)	2022	PHYS. DEVICE, PHYS. MODEL	CNN	FPR, TPR, PPV, ACC, F1, conf. Matrix	proc. time per patch, proc. time per frame, proc. time per video	VID.	QUFVD	ID
Lawgaly et al. (2021)	2021	PHYS. DEVICE	SPN	FPR, FNR, TPR, PCE		VID.	Video-ACID	VER
Baracchi et al. (2021)	2021	PHYS. DEVICE	SPN	FAR, TPR, ACC, PCE		IMG:	own	OBS
Iuliani et al. (2021)	2021	PHYS. DEVICE	SPN	FPR, PCE		IMG:	Flickr	OBS
Taspinar et al. (2021)	2021	PHYS. DEVICE	SPN	TPR, PCE		BOTH	NYUAD-MMD, SOCRatES	OBS
Yang et al. (2021)	2021	PHYS. DEVICE	SPN	FPR, FNR PCE	proc. time per frame, proc. time per video	VID.	VISION	VER
Ferrara and Beslay (2020)	2020	PHYS. DEVICE	SPN	FPR, FNR, PCE		VID.	VISION	VER
López et al. (2020)	2020	PHYS. MODEL, BRAND	METAD.	HOM, COMP, SIL, RI		VID.	VISION, ACID	EXP
Mandelli et al. (2020)	2020	PHYS. DEVICE	SPN	FPR, FNR, TAR, AUC	proc. time per frame	VID.	VISION	VER
Al Shaya et al. (2018)	2018	PHYS. DEVICE	SPN	PCE		IMG:	HDR	OBS
Lawgaly and Khelifi (2016)	2016	PHYS. DEVICE	SPN	FAR, FPR, FNR, TAR	CPU filtering time	IMG:	DIDB, own	VER
Valsesia et al. (2015)	2015	PHYS. DEVICE	SPN	REC, PREC	data loaded from disk, RAM usage	IMG:	Flickr	ID
Chuang et al. (2011)	2011	PHYS. DEVICE	SPN	FAR, TDR, PCE		VID.	own	OBS
Amerini et al. (2009)	2009	PHYS. DEVICE	SPN	FAR, FRR		IMG:	own	VER
Goljan et al. (2009)	2009	PHYS. DEVICE	SPN	FAR, FRR, PCE		IMG:	Flickr	OBS, VER
Chen et al. (2008)	2008	PHYS. DEVICE	SPN	FAR, FRR		IMG:	own, Flickr	VER
Lukas et al. (2006)	2006	PHYS. DEVICE	SPN	FAR, FRR, PCE		IMG:	own	OBS, VER

CRediT authorship contribution statement

Samantha Klier: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Data curation, Conceptualization. **Harald Baier:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Considered works

This section presents an excerpt of considered seminal works with the approach used in Table A.3.

Appendix B. Supplementary material

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.fsidi.2024.301858.

Data availability

Articles of Source Camera Forensics classified based on the Source Camera Target Model and Problem Classes (Original data) (Mendeley Data).

References

Akbari, Y., Al-Maadeed, S., Al-Máadeed, N., Al-Ali, A., Khelifi, F., Lawgaly, A., et al., 2022a. A new forensic video database for source smartphone identification: description and analysis. IEEE Access 10, 20080–20091.

Akbari, Y., Al-maadeed, S., Elharrouss, O., Khelifi, F., Lawgaly, A., Bouridane, A., 2022b. Digital forensic analysis for source video identification: a survey. Forensic Science International: Digital Investigation 41, 301390.

Al Shaya, O., Yang, P., Ni, R., Zhao, Y., Piva, A., 2018. A new dataset for source identification of high dynamic range images. Sensors 18, 3801.

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.

Amerini, I., Caldelli, R., Cappellini, V., Picchioni, F., Piva, A., 2009. Analysis of denoising filters for photo response non uniformity noise extraction in source camera identification. In: 2009 16th International Conference on Digital Signal Processing, IEEE, pp. 1–7.

Amerini, I., Caldelli, R., Crescenzi, P., Del Mastio, A., Marino, A., 2014. Blind image clustering based on the normalized cuts criterion for camera identification. Signal Process. Image Commun. 29, 831–843.

Anmol, T., Sitara, K., 2024. Video source camera identification using fusion of texture features and noise fingerprint. Forensic Science International: Digital Investigation 49, 301746.

Apple, 2023. iPhone 15 Pro tech specs. https://www.apple.com/iphone-15-pro/specs/. (Accessed 9 January 2024).

Apple, 2024. Using heif or hevc media on apple devices. https://support.apple.com/en-us/116944. (Accessed 2 February 2024).

Baracchi, D., Iuliani, M., Nencini, A.G., Piva, A., 2021. Facing image source attribution on iphone x. In: Digital Forensics and Watermarking: 19th International Workshop. IWDW 2020, Melbourne, VIC, Australia, November 25–27, 2020, Revised Selected Papers 19. Springer, pp. 196–207.

Bernacki, J., 2020. A survey on digital camera identification methods. Forensic Science International: Digital Investigation 34, 300983.

Bharathiraja, S., Rajesh Kanna, B., Hariharan, M., 2023. A deep learning framework for image authentication: an automatic source camera identification deep-net. Arab. J. Sci. Eng. 48, 1207–1219.

Bondi, L., Baroffio, L., Güera, D., Bestagini, P., Delp, E.J., Tubaro, S., 2016. First steps toward camera model identification with convolutional neural networks. IEEE Signal Process. Lett. 24, 259–263.

Caldelli, R., Amerini, I., Picchioni, F., Innocenti, M., 2010. Fast image clustering of unknown source images. In: 2010 IEEE International Workshop on Information Forensics and Security, IEEE, pp. 1–5.

Canon, 2023. Deep learning image processing technology. https://global.canon/en/technology/dl-iptechnology-2023.html. (Accessed 30 November 2023).

Castillo Camacho, I., Wang, K., 2021. A comprehensive review of deep-learning-based methods for image forensics. J. Imaging 7, 69.

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.

Chuang, W.H., Su, H., Wu, M., 2011. Exploring compression effects for improved source camera identification using strongly compressed video. In: 2011 18th IEEE International Conference on Image Processing, IEEE, pp. 1953–1956.

Ferrara, P., Beslay, L., 2020. Robust video source recognition in presence of motion stabilization. In: 2020 8th International Workshop on Biometrics and Forensics (IWBF), IEEE, pp. 1–6.

Ferrara, P., Iuliani, M., Piva, A., 2022. Prnu-based video source attribution: which frames are you using? J. Imaging 8, 57.

Galdi, C., Hartung, F., Dugelay, J.L., 2019. Socrates: a database of realistic data for source camera recognition on smartphones. In: ICPRAM, pp. 648–655.

Geradts, Z.J., Bijhold, J., Kieft, M., Kurosawa, K., Kuroki, K., Saitoh, N., 2001. Methods for identification of images acquired with digital cameras. In: Enabling Technologies for Law Enforcement and Security. SPIE, pp. 505–512.

Gloe, T., 2012. Feature-based forensic camera model identification. In: Transactions on Data Hiding and Multimedia Security VIII: Special Issue on Pattern Recognition for IT Security. Springer, pp. 42–62.

Gloe, T., Böhme, R., 2010. The 'Dresden image database' for benchmarking digital image forensics. In: Proceedings of the 2010 ACM Symposium on Applied Computing, pp. 1584–1590.

Goljan, M., Fridrich, J., Filler, T., 2009. Large scale test of sensor fingerprint camera identification. In: Media Forensics and Security. SPIE, pp. 170–181.

Hadwiger, B., Riess, C., 2021. The forchheim image database for camera identification in the wild. In: Pattern Recognition. ICPR International Workshops and Challenges: Virtual Event, January 10–15, 2021, Proceedings, Part VI. Springer, pp. 500–515.

Hosler, B., Mayer, O., Zhao, X., Chen, C., Shackleford, J., Stamm, M., 2019. Video-acid. https://dx.doi.org/10.21227/4dzb-h573.

Iuliani, M., Fontani, M., Piva, A., 2021. A leak in prnu based source identification—questioning fingerprint uniqueness. IEEE Access 9, 52455–52463.

Junklewitz, H., Ferrara, P., Beslay, L., 2021. Clustering and Unsupervised Classification in Forensics. Technical Report KJ-NA-30419-EN-N. European Commission: Joint Research Centre, Luxembourg (Luxembourg).

Kee, E., Johnson, M.K., Farid, H., 2011. Digital image authentication from jpeg headers. IEEE Trans. Inf. Forensics Secur. 6, 1066–1075. https://doi.org/10.1109/TIFS.2011.2128309.

Kharrazi, M., Sencar, H.T., Memon, N., 2004. Blind source camera identification. In: 2004 International Conference on Image Processing, 2004, ICIP'04, IEEE, pp. 709–712.

Kirchner, M., Gloe, T., 2015. Forensic camera model identification. In: Handbook of Digital Forensics of Multimedia Data and Devices, pp. 329–374.

Klier, S., Baier, H., 2024. Scalable image clustering to screen for self-produced csam. EAI Endorsed Transactions on Internet of Things 10.

Lawgaly, A., Khelifi, F., 2016. Sensor pattern noise estimation based on improved locally adaptive dct filtering and weighted averaging for source camera identification and verification. IEEE Trans. Inf. Forensics Secur. 12, 392–404.

Lawgaly, A., Khelifi, F., Bouridane, A., Al-Maaddeed, S., 2021. Sensor pattern noise estimation using non-textured video frames for efficient source smartphone identification and verification. In: 2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE), IEEE, pp. 19–24.

Liu, Y., Zou, Z., Yang, Y., Law, N.F.B., Bharath, A.A., 2021. Efficient source camera identification with diversity-enhanced patch selection and deep residual prediction. Sensors 21, 4701.

López, R.R., Luengo, E.A., Orozco, A.L.S., Villalba, L.J.G., 2020. Digital video source identification based on container's structure analysis. IEEE Access 8, 36363–36375.

Lukas, J., Fridrich, J., Goljan, M., 2006. Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. 1, 205–214.

Mandelli, S., Argenti, F., Bestagini, P., Iuliani, M., Piva, A., Tubaro, S., 2020. A modified Fourier-Mellin approach for source device identification on stabilized videos. In: 2020 IEEE International Conference on Image Processing (ICIP), IEEE, pp. 1266–1270.

Marra, F., Poggi, G., Sansone, C., Verdoliva, L., 2017. Blind prnu-based image clustering for source identification. IEEE Trans. Inf. Forensics Secur. 12, 2197–2211.

Matthews, R., Falkner, N., Sorell, M., 2020. Reverse engineering the raspberry pi camera v2: a study of pixel non-uniformity using a scanning electron microscope. Forensic Science International: Digital Investigation 32, 200900.

Matthews, R., Sorell, M., Falkner, N., 2019. An analysis of optical contributions to a photosensor's ballistic fingerprints. Digit. Investig. 28, 139–145.

Mullan, P., Riess, C., Freiling, F., 2019. Forensic source identification using jpeg image headers: the case of smartphones. Digit. Investig. 28, S68–S76.

Mullan, P., Riess, C., Freiling, F., 2020. Towards open-set forensic source grouping on jpeg header information. Forensic Science International: Digital Investigation 32, 300916.

Nwokeji, C.E., Sheikh-Akbari, A., Gorbenko, A., Mporas, I., 2024. Source camera identification techniques: a survey. J. Imaging 10, 31.

Orozco, A.S., González, D.A., Corripio, J.R., Villalba, L.G., Hernandez-Castro, J., 2013. Techniques for source camera identification. In: Proceedings of the 6th International Conference on Information Technology, pp. 1–9.

Rafi, A.M., Kamal, U., Hoque, R., Abrar, A., Das, S., Laganiere, R., Hasan, M.K., et al., 2019. Application of densenet in camera model identification and post-processing detection. In: CVPR Workshops, pp. 19–28.

Rosenberg, A., Hirschberg, J., 2007. V-measure: a conditional entropy-based external cluster evaluation measure. In: Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL), pp. 410–420.

Sencar, H.T., Verdoliva, L., Memon, N., 2022. Multimedia Forensics. Springer Nature.

Shullani, D., Fontani, M., Iuliani, M., Shaya, O.A., Piva, A., 2017. Vision: a video and image dataset for source identification. EURASIP J. Inf. Secur. 2017, 1–16.

Taspinar, S., Mohanty, M., Memon, N., 2020. Camera fingerprint extraction via spatial domain averaged frames. IEEE Trans. Inf. Forensics Secur. 15, 3270–3282.

Taspinar, S., Mohanty, M., Memon, N., 2021. Effect of video pixel-binning on source attribution of mixed media. In: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, pp. 2545–2549.

Tian, H., Xiao, Y., Cao, G., Zhang, Y., Xu, Z., Zhao, Y., 2019. Daxing smartphone identification dataset. IEEE Access 7, 101046–101053.

Tomioka, Y., Kitazawa, H., 2011. Digital camera identification based on the clustered pattern noise of image sensors. In: 2011 IEEE International Conference on Multimedia and Expo, IEEE, pp. 1–4.

Valsesia, D., Coluccia, G., Bianchi, T., Magli, E., 2015. Large-scale image retrieval based on compressed camera identification. IEEE Trans. Multimed. 17, 1439–1449.

Wronski, B., Garcia-Dorado, I., Ernst, M., Kelly, D., Krainin, M., Liang, C.K., Levoy, M., Milanfar, P., 2019. Handheld multi-frame super-resolution. ACM Trans. Graph. 38, 1–18.

Yang, P., Ni, R., Zhao, Y., Zhao, W., 2019. Source camera identification based on content-adaptive fusion residual networks. Pattern Recognit. Lett. 119, 195–204.

Yang, W.C., Jiang, J., Chen, C.H., 2021. A fast source camera identification and verification method based on prnu analysis for use in video forensic investigations. Multimed. Tools Appl. 80, 6617–6638.