IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 August 2022, accepted 13 September 2022, date of publication 26 September 2022, date of current version 11 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3209241

RESEARCH ARTICLE

Counterfeit Detection and Prevention in Additive Manufacturing Based on Unique Identification of Optical Fingerprints of Printed Structures

AHMET TURAN EROZAN[1], MICHAEL HEFENBROCK[2], DENNIS R. E. GNAD[1], MICHAEL BEIGL[2], JASMIN AGHASSI-HAGMANN[3], (Member, IEEE), AND MEHDI B. TAHOORI[1], (Fellow, IEEE)

[1]Chair of Dependable Nano Computing, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany
[2]TECO, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany
[3]Institute of Nanotechnology, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany

Corresponding author: Mehdi B. Tahoori (mehdi.tahoori@kit.edu)

This work was supported in part by Ministry of Science and Arts, BW, Germany, under Graduate School Modellierung, Entwurf, Realisierung und Automatisierung von Gedruckter Elektronik und ihren Materialien (MERAGEM).

ABSTRACT Printed Electronics (PE) based on additive manufacturing has a rapidly growing market. Due to large feature sizes and reduced complexity of PE applications compared to silicon counterparts, they are more prone to counterfeiting. Common solutions to detect counterfeiting insert watermarks or extract unique fingerprints based on (irreproducible) process variations of valid components. Commonly, such fingerprints have been extracted through electrical methods, similar to those of physically unclonable functions (PUFs). Hence, they introduce overhead to the production resulting in additional costs. While such costs may be negligible for application domains targeted by silicon-based technologies, they are detrimental to the ultra-low-cost PE applications. In this paper, we propose an optical unique identification, by extracting fingerprints from the optically visible variations of printed inks in the PE components. The images can be obtained from optical cameras, such as cell phones, thanks to large feature sizes of PE, by trusted parties, such as an end user wanting to verify the authenticity of a particular product. Since this approach does not require any additional circuitry, the fingerprint production cost consists of merely acquisition, processing and saving an image of the circuit components, matching the requirements of ultra-low-cost applications of PE. To further decrease the storage costs for the unique fingerprints, we utilize image downscaling resulting in a compression rate between 83–188×, while preserving the reliability and uniqueness of the fingerprints. The proposed fingerprint extraction methodology is applied to four datasets and the results show that the optical variation printed inks is suitable to prevent counterfeiting in PE.

INDEX TERMS Printed electronics, additive manufacturing, low-cost, optical fingerprint, anti-counterfeiting, security, authentication, identification.

I. INTRODUCTION

Additive manufacturing enables Printed Electronics (PE) as a promising candidate to enable applications where ultra-low-cost, on-demand fabrication, and/or mechanical flexibility are required. PE provides these features owing to its additive and point-of-use manufacturing as well as the usage of various substrate types [1]. Therefore, several envisioned applications such as smart packaging [2], in-situ monitoring for logistics [3], health monitoring patches [4], [5], smart cards [6], smart labels [7], pharmaceuticals [8] and disposable food sensors [9] can benefit from the features of PE.

Counterfeiting is a major problem in the supply chain, such as in the domain of integrated circuits and systems, automotive parts, software, cosmetic, jewellery, health-care diagnosis systems, and drugs, just to name a few [10], [11], [12], [13]. Since PE has a huge market, projected to grow from $29B in 2017 to $73B in 2027 [14], [15], the counterfeiting of PE components has been expected to rise, and technology-specific, low-cost measures have to be taken [16].

The associate editor coordinating the review of this manuscript and approving it for publication was Gustavo Callico.

Due to large feature sizes of printed components and their reduced complexity compared to silicon-based counterparts, they are more prone to counterfeiting.

Physically Unclonable Functions (PUFs), which generate biometric fingerprints from manufacturing variation, have been utilized to prevent counterfeiting [13], [17], [18]. Electrical PUFs and optical PUFs are two distinctive examples in various fields [18], [19], [20]. Recently, the optical PUFs have received an increasing interest since they can generate the fingerprint based on visual inspection and image processing without adding a physical overhead to the product [18], [19], [20], [21]. This is beneficial for low-cost applications where adding an additional physical tag is infeasible for economic reasons. On the other hand, it is important to develop an image processing based fingerprint extraction methodology which generates fingerprints while considering their storage costs, particularly for high volume products.

On the other hand, one can use PE, thanks to its conformity and non-toxicity, for counterfeiting detection and prevention in various domains such as disposable personalized medicine and brand identification. Imagine that a brand close has a smart PE tag with a unique non-reproducible fingerprint. The potential buyer can take an optical photo with a cellphone camera and send it to the cloud service of the brand make to authenticate it. The unique fingerprint is checked against the database of fingerprints of all legitimate fabricated products to validate its authenticity. Another example is the usecase of personalized disposable medicine. The physician can prescribe a personalized smart medicine to a patent. At the hospital or pharmacy, the unique fingerprint can be checked with the manufacturer's database to authenticate the disposable medical device. The patient herself can validate to ensure that this smart medicine is meant for her and not someone else. In all such scenarios, the parties who issue authentication queries are trusted.

In this work, we propose an approach based on additive manufacturing to provide low-cost unique identification in the form of optical fingerprints from printed structures for counterfeit detection. This is meant for ultra-low-cost PE where typical hardware implementation of authentication protocols [22], [23] becomes too costly for PE realization. The proposed methodology extracts fingerprints from the optically visible variations of printed inks used during manufacturing process of PE circuits, so that no additional circuitry is required for fingerprint generation. Furthermore, we have examined downscaling compression to reduce the size of the fingerprints, resulting in significantly lower storage cost. The methodology is applied to four datasets to examine the optical variation of printed inks. The results show that the optical variation in PE is sufficient to extract unique and reliable fingerprints for anti-counterfeiting of PE. Moreover, we achieve at least a $83\times$ compression rate without compromising uniqueness metrics. The contributions of this work are summarized as follows:

- We propose a robust image processing methodology to extract fingerprints,
- We use an image downscaling algorithm to reduce the storage cost of fingerprints,
- We evaluate the proposed methodology on four real datasets.
- We examine the suitability of the optical variability of the printed inks,
- We examine the downscaling compression to determine the optimal compression rate which satisfies uniqueness metrics.

The paper is organized as follows: Section II provides preliminary information on PE technology and related works. The proposed optical fingerprint is explained in Section III, while the evaluation results are given in Section IV. Section V concludes the paper.

II. PRELIMINARIES

A. PRINTED ELECTRONICS

Printed Electronics (PE) has received a great interest since it enables new application areas where mechanical flexibility, lightweight, large area, low-cost and on-demand fabrication are of interest [1], [25], [26], [27]. The current market driver applications are radio frequency identification (RFID) tags [28], [29], [30], [31], sensor arrays [32], [33], [34], photo-voltaic cells [35], batteries [36], [37] and displays [38], [39]. In addition, some envisioned applications are dynamic newspapers, smart labels, smart cards, ingestible health care diagnosis devices, energy harvesters and smart clothing [25], [26], [27].

Several additive printing processes are used to manufacture PE circuits instead of photolithography-based subtractive processes which are complex, expensive and environmentally hazardous [40]. These additive printing processes are screen printing, flexography printing, offset printing, gravure printing and inkjet printing [1], [15], [25], [41]. Several materials are printed on a flexible substrate to construct PE circuits and systems. Single or multiple printing processes can be used depending on the target application. Some of these processes such as inkjet printing enable a highly demanding feature: customized fabrication, more specifically, personalized fabrication [25], [41], which allows users to select their own material and substrate, and fabricate fully custom designs without profound expertise or sophisticated and extremely expensive manufacturing tools.

Several printed transistors such as p-type organic-based thin film transistors (OTFTs) [42], organic field-effect transistors (OFETs) [43], some n-type organic transistors [44], [45], and inorganic oxide semiconductor based transistors [46] are proposed to build functional PE circuits. Organic transistors generally suffer from low field effect mobility and high supply voltage requirement, and this makes them unsuitable for low-power applications [15]. On the other hand, inorganic oxide semiconductor based transistors such as Electrolyte-gated Transistor (EGT) are investigated since they provide high field effect mobility, and requires low supply voltage ($\leq$ 1 V) when combined with electrolyte

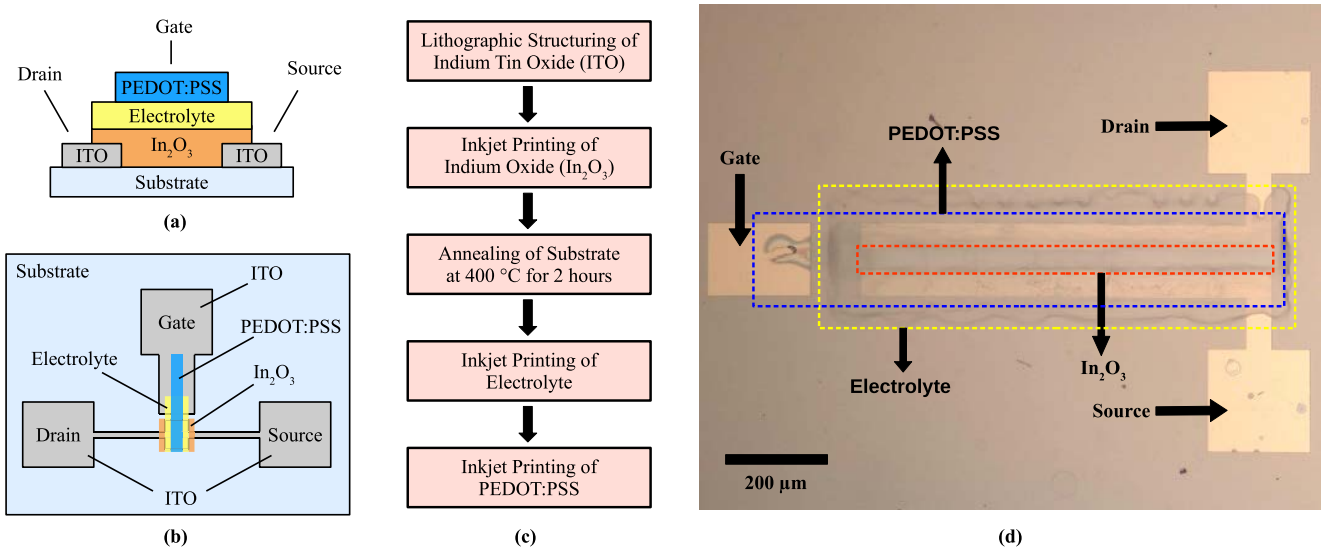


FIGURE 1. Description of Electrolyte-gated transistor technology a) Cross-sectional view of EGT on substrate [24]. b) Top view of EGT on substrate [24]. c) Flow of fabrication process of EGT [19]. d) Photo of a fabricated EGT [19].

gating [46], [47], [48], [49], which make EGT a promising candidate that can be utilized in PE application requiring small supply voltages powered by printed batteries and/or printed energy harvesters [37], [50].

Since the fabrication process of EGTs is based on inkjet printing, EGTs have high intrinsic variation resulting from the random dispersion of the ink on the substrate. In inkjet-printing, all devices are printed individually by multiple additive process steps, where each step can vary on its own. These processes and systematic variations originating from the ink, droplet forming, the attachment of droplets on the substrate, and manufacturing tools are random and uncontrollable. These variations do not only affect the electrical behavior of EGTs but are also optically visible which can be exploited for an optical unique identifier (UID), fingerprint, or PUF. In the context of this work, our aim is to extract fingerprints from optically visible variations of printed devices used in the PE applications. More specifically, we use EGTs to evaluate the proposed fingerprint due to its promising features mentioned above. However, it should be noted that the proposed fingerprint extraction method is applicable to any printed structure.

In the fabrication process of EGTs, the channel material, indium oxide (In_2O_3) semiconductor, is inkjet printed to form the channel between drain and source electrodes which use patterned indium tin oxide (ITO) as material. Then, on the top of the channel, the electrolyte is inkjet printed as gate dielectric. At last, PEDOT:PSS is inkjet printed on the top of the electrolyte as a top-gate in a way that it covers the channel area [24]. Figure 1 shows the structure, the fabrication process, and the photo of the EGTs. As elaborated in Section III, patterned ITO electrodes (e.g., drain) can be used to align transistor images since it has less optically visible variation than printed inks (e.g., electrolyte) while the entropy of the proposed fingerprints are harvested from the optical image of printed inks of EGTs.

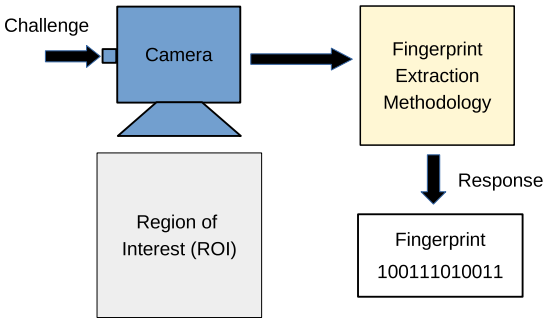


FIGURE 2. Overview of proposed optical PUF.

B. RELATED WORKS

PUFs have become common in the last decade to provide secret fingerprints [51]. They extract digital fingerprints from intrinsic manufacturing process variations. The inherent and uncontrollable variations ensure unpredictable fingerprints. Therefore, the fingerprints are utilized as a key for security purposes such as authentication and cryptography [17], [18], [51], [52], [53]. Several electrical PUFs have been proposed to secure integrated circuits and embedded systems. The most common electrical PUFs include SRAM PUF [54], Arbiter PUF [55], and Ring Oscillator PUF [56]. Furthermore, Printed memory PUF [19] and Printed Differential Circuit PUF [57] have been proposed in the context of PE.

On the other hand, recent research has also focused on optical PUFs for their advantages. Since Optical PUFs extracts randomness from optical variations, contrary to electrical PUFs, they require no additional circuitry in the product. Moreover, they provide a high number of response bits. These advantages result in low-cost per piece, which make them beneficial for cost-limited applications [58], particularly for ultra-low-cost PE applications.

In [20], a camera based optical PUF, which exploits the surface patterns of injection moulded plastic components is presented to further reduce authentication cost while other

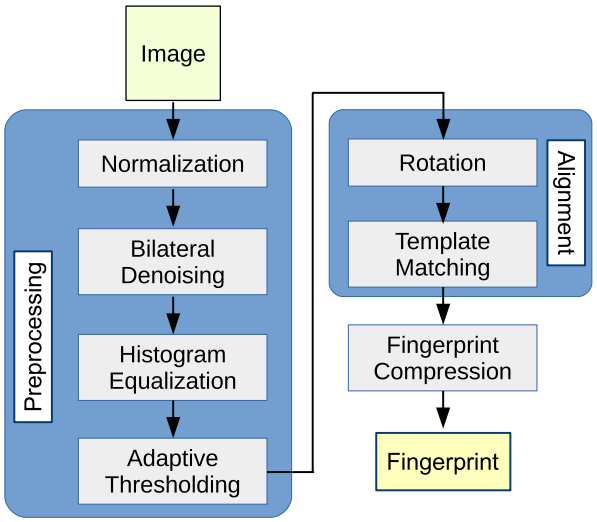


FIGURE 3. Proposed fingerprint extraction methodology composed of preprocessing, alignment, and fingerprint compression.

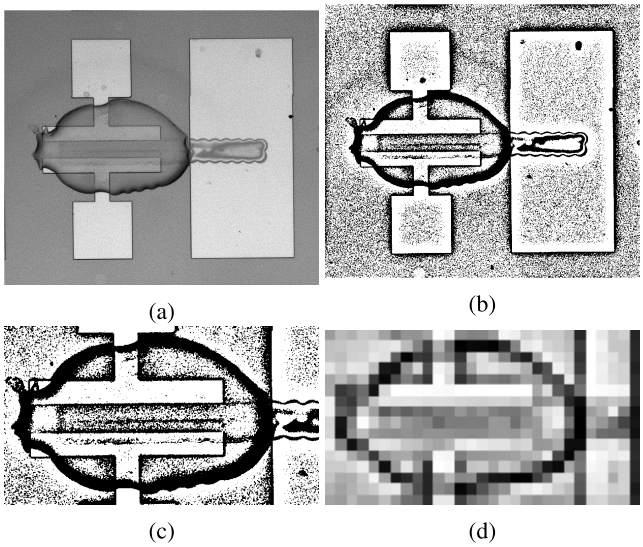


FIGURE 4. A printed transistor image (a) original, (b) preprocessed, (c) aligned (d) downscaled (downscaling factor = 22).

optical PUFs in the literature mainly use costly imaging methods (e.g., laser). The method pre-processes the image under examination and then uses the correlation coefficient to compare it to a database of stored imagines for identification. Naturally, this requires large amounts of memory for stored images resulting in high storage cost. For instance, the binary image size of a component is 1800 × 1800 corresponding to ∼0.386 MB in the memory, and for high volume produced components, it increases proportionally (e.g., for 1 billion components, required memory is ∼368 TB), which harms its low-cost feature. The high memory usage of this method makes its utilization infeasible in ultra-low-cost PE applications. To the best of authors' knowledge, our paper presents the first work extracting fingerprints from optically visible variations of PE inks with the objective of low memory usage in the literature, which can be used for counterfeiting detection in PE and other products equipped with smart PE sensors.

III. PROPOSED OPTICAL FINGERPRINT

The electrical hardware fingerprints, aka PUFs, introduce exorbitant overhead which is infeasible for ultra-low-cost PE applications. For instance, the electrical PUF proposed for PE in [19] containing three transistors and two resistors allocates ∼3.5 mm^2 to generate one bit. In addition to the PUF circuitry, a secure access mechanism and protocol to interact with the PUF needs to be implemented in the hardware, such as controlled PUF (CPUF) [59]. However the overhead of such schemes for their hardware realizations in PE, even in resource-constrained settings [60], become simply too costly and inapplicable for the intended use cases.

Since the feature size of PE devices are large enough (e.g., 10 μm), one can capture the optically visible variations of printed inks with a low-cost camera integrated to a microscope so that an optical unique fingerprint can extract multiple bits from one printed transistor, meaning that without any hardware overhead, a multi-bit fingerprint can be generated. Therefore, the ultra-low-cost feature of PE can be preserved, while providing unique device-specific fingerprints to prevent counterfeiting and overbuilding. In such scenario, the person who is initiating the query (e.g., the customer who wants to authenticate the legitimacy of a brand product in a retail store or the pharmacy trying to authenticate the smart medical device or the patient who wants to verify this is the right medicine for her) is assumed to be trusted. Therefore, the communication channel to the fingerprint server and the process to check the queried fingerprint across the inventory of valid fingerprints (from all non-counterfeit products) are also assumed to be trusted. Therefore, the question is whether the device for which the optical fingerprint is taken is counterfeit or not.

There are several challenges to extract reliable fingerprints. In electrical PUFs, external conditions such as supply voltage fluctuation and temperature may cause bit flips resulting in PUF unreliability. However, in optical fingerprints, the sources of unreliability are insufficient optical precision (different relative positioning), dust, camera noise and non-uniform illumination. We consider these challenges while developing the fingerprint extraction methodology of the proposed optical fingerprinting.

A. METHODOLOGY OVERVIEW

The flow for extraction and processing of the proposed optical fingerprinting is illustrated in Figure 2. It starts from the image acquisition using an optical camera integrated to a microscope. The preprocessing steps are applied to the acquired image to remove the effect of environmental conditions such as illumination and camera noise. After that, the images are aligned with respect to a reference. These steps are performed to ensure that the generated keys are reliably extracted. Last, to reduce the size of generated fingerprint, image downscaling is applied. The response is the fingerprint consisting multiple bits.

After components are manufactured, the fingerprints of these components are extracted using the proposed method,

and stored in a database. In the authentication phase, the extracted fingerprint of the examined component is compared with the fingerprints of all printed components which are stored in a secure database. The validity of the printed component is verified based on the correlation of its fingerprint with the pre-stored fingerprint.

The details of each step of the fingerprint extraction methodology is elaborated in the following subsections. All steps described in this section are performed in *python* using the *scikit − image* open source library [61].

B. IMAGE ACQUISITION

The images are acquired by a camera integrated into a microscope. The acquisition should be carried out with a trusted device in the real usage to secure the verification of products. The acquired transistor image has a size of $\sim 800 \times 800$. An example transistor image is shown in Figure 4a.

C. PREPROCESSING

To increase the reliability of the proposed optical fingerprinting method with respect to noise and illumination differences, we apply the following preprocessing steps respectively:

- **Normalization** is used to scale the pixel values to the range of $[0, 1]$ to reduce the effect of global lighting conditions, i.e. systematic shifts in the pixel value range.
- **(Bilateral) Denoising** [62] is an edge-preserving filtering. While basic filters perform a weighted sum of close pixels, bilateral filtering also considers their values. Through this, the pixels in the neighbourhood of a target pixel only have a strong influence if they also have a similar value before filtering. This is especially noticeable on sharp edges e.g. transitions from black to white. Here, black and white pixels would average to grey, where for bilateral filtering, the black pixels are not considered for white values (and vice versa) which leads to the preservation of the contrast after filtering.
- **Histogram equalization** [63] tries to achieve a more equal distribution of the pixel value intensities in an image. For this, the images cumulative frequency histogram of the pixel values is used to transform the values of all pixels according to their rank in intensity. This leads to increased contrasts in the image while also decreasing the effect of global lighting conditions.
- **Adaptive thresholding** binarizes the image by comparing the weighted neighbourhood of a pixel to a threshold value. If this threshold is exceeded, the pixel is declared black, else white is assigned.

The preprocessed version of the transistor image is shown in Figure 4b.

D. ALIGNMENT CORRECTION

The alignment used in the methodology is chosen to ensure the reproducibility of the extracted keys, hence improve their reliability. Following the preprocessing, the alignment of the images is applied to provide same relative positioning which increases the reliability of the fingerprint extraction with respect to shifts and rotations. For this purpose, first, a reference line, which is top edge of drain electrode (upper), is identified through a Hough Line Transform [64]. The images are then rotated such that the reference lines form the same angle to a horizontal line. Through this, an invariance to rotation is achieved. Then, a template matching [65] is performed on the rotated images to identify the position of the drain electrode, which will serve as a reference point to locate the region of the image containing electrolyte (region of interest i.e. ROI), which contains the most optically visible variation. The aligned version of the transistor image is given in Figure 4c, where the ROI is a 2-dimensional matrix containing bits, which then can be used as a fingerprint.

E. FINGERPRINT COMPRESSION

Since the extracted fingerprint after alignment has high resolution, it requires high storage area causing high storage cost. The local averaging based image downscaling is applied to reduce the size of the ROI to lower the storage cost. An example downscaled image with a downscaling factor of 22 is depicted in Figure 4d Moreover, the downscaling reduces the entropy of the image, which results in worse uniqueness (inter correlation), while on the positive side, mitigates the errors caused from misalignment, dust, camera noise and illumination differences which improves the reliability (intra correlation). This trade-off will be evaluated, to optimize the downscaling factor.

IV. EVALUATION

In this section, we explain the metrics to evaluate the proposed optical fingerprinting. Moreover, we describe the datasets which are used to validate the methodology. Finally, we report and discuss the results obtained using the proposed methodology applied to described datasets as well as security implications of the proposed fingerprinting.

A. EVALUATION METRICS

To evaluate the quality of the proposed method, we employ metrics for inter (uniqueness) and intra (reliability) correlation, and the *uniformity* metric to estimate the randomness between different responses. The uniqueness represents the correlation between the fingerprints of different EGTs, and it should be low. The reliability represents the correlation between the fingerprints of same EGT, and it should be high. Therefore, the fingerprints of different EGTs are distinguishable from the keys of same EGTs with a threshold. It should be noted that, in this work, fast normalized cross-correlation [65] is used to calculate uniqueness and reliability. We have used the fast normalized cross-correlation to provide a baseline quantity that is used for the uniqueness and reliability of the fingerprint keys. The use of other metrics may improve the figure of merits of the proposed method but the main focus of this work is to show that the optical variation of printed components provide sufficient entropy to utilize as an optical fingerprinting. For that, the *uniformity* also plays an

important role, which looks at Hamming distances between individual extracted fingerprints as described in [66].

The uniqueness of the optical fingerprinting reflects the visible variability of printed inks. The reliability of the optical fingerprint suffers from misalignment, dust, camera noise, improper illumination and shape degradation over time.

The figure of merit (FoM) for the distinguishability is the difference between the minimum value of the reliability and the maximum value of the uniqueness, and is given by:

$$\mathrm{FoM}(I) = \min_{\{(i,j)\,|\,i=j,\ i,j\in I\}} C(i,j) - \max_{\{(i,j)\,|\,i\neq j,\ i,j\in I\}} C(i,j),$$

where the set I thereby denotes the multiset[1] of all transistor images. The first summand represents the intra correlation (reliability) between images of the same device i.e. $i = j, i, j \in I$, while the second summand denotes the inter correlation (uniqueness) between images of different devices i.e. $i \neq j, i, j \in I$.

B. DATASET

We have used the optical images of fabricated EGTs to validate the methodology. The entire dataset is composed of four subsets, each containing EGTs of a certain width (see Table 2). The layout designs of transistors in the same datasets are same so that the process variation is the only source of entropy for the extracted bits. Moreover, the images of each EGT are acquired two times to evaluate the reliability of the methodology in the context of camera noise, dust, illumination and the material degradation over time. In this regard, the images are acquired using the same camera integrated into a microscope, which is used by several researchers, with a time difference of 120 days between acquisitions to achieve randomness in the illumination and position of the setup that are uncontrollably changed by other users between acquisitions.

V. RESULTS AND DISCUSSION

The intra (reliability) and inter (uniqueness) correlation distributions of four datasets are given in Figure 5. The results show a high intra correlation, and thus high reliability, and a lower inter correlation, and thus high uniqueness. By that, with a certain threshold, the extracted bits are distinguishable meaning that the FoM is positive.

The raw amount of extracted bits from dataset-A, dataset-B, dataset-C, and dataset-D are 273000 (350 × 780), 217000 (350 × 620), 161000 (350 × 460), and 150500 (350 × 430) respectively. The entropy of the extracted bits can be increased using postprocessing methods while sacrificing the amount of bits [67], [68]. It should be noted that these lengths are achieved using only one printed transistor in the optical fingerprint while the existing printed electrical PUF provides 1-bit using 3 transistors and 2 resistors [19]. To achieve an equal number of bits (e.g., 150500) using the printed electrical PUF, an area of $\sim 0.5\,\mathrm{m}^2$ is required due to the large feature sizes ($\geq 10\,\mu$m) of printing techniques, which is clearly infeasible.

Our mean hamming distance across all datasets is 72316 with a minimum of 40901 (from dataset-D) and maximum of 115912 (from dataset-A). That means, in the case of a larger data set, at least 2^{40901} key combinations are available. Even given a certain amount of correlation between the pixels, and postprocessing needed for reliability reasons, the value for the minimum hamming distance would still leave enough space for quite a large dataset, hence providing unique keys.

This comparison proves that the optical fingerprints provide extremely larger number of bits with no hardware overhead and component cost while introducing a delay resulting from the execution of the fingerprint extraction method. However, the time required to extract the fingerprint is negligible and can be in the range of milliseconds as the process of the counterfeiting verification does not have a strict time constraint.

A. DOWNSCALING

To examine the relation between FoM and downscaling factor, we extracted FoM results with respect to several downscaling factors, as depicted in Figure 6. We summarize the results from those figures in Table 2 in terms of pixel compression rates and respective storage sizes, and determine the sweet spot for the downscaling factor in which the FoM is maximized. The last downscaling factors that still result in FoM > 0 are listed for the respective datasets, and are within the range of 28–41. These downscaling factors result in the decrease of the amount of fingerprint pixels by factors of 784–1681 across our four datasets. Since keeping black and white color levels did not lead to useful results, we downscale the pictures using interpolation, resulting in new grayscales to appear, increasing the storage need to more than one bit per pixel, but still reducing the required storage space. Like that, the reduced pixel images result in needed storage space for grayscale downscaled pictures in a range of 1152–3276 bit per image at maximum for the evaluated datasets when the last downscaling factor still results in a FoM > 0. In summary, the minimum achieved data compression rate is 83–188×, depending on the dataset.

Using our method, the storage need is reduced significantly compared to existing image-based fingerprint extraction methods [20], [21] where the whole ROI is stored as the fingerprint and compared for authentication. Please note again that, in Figure 6, the FoM of all datasets increases while the downscaling factor is increased from 1 to around 8, because the downscaling eliminates the high resolution details resulting in lower maximum inter correlation (better reliability) and higher minimum intra correlation (better uniqueness). Thus, the distinguishability of the fingerprints become better, resulting in an increased FoM with a specific downscaling factor, as we also integrated in Table 2. However, Figure 6 also shows that after a certain downscaling factor, the FoM is decreasing, since the downscaled images start losing their

[1]The elements of I are not unique since there are multiple images i of the same transistor in I. We all denote them with the same repeated element.

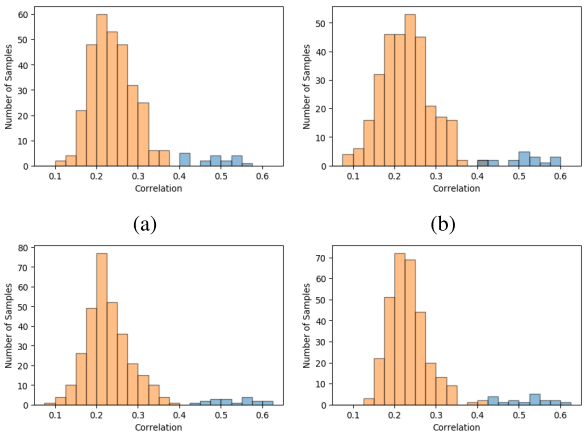


FIGURE 5. Intra and inter (pearson) correlation distribution of (a) Dataset-A, (b) Dataset-B, (c) Dataset-C, and (d) Dataset-D before downscaling (downscaling factor = 1).

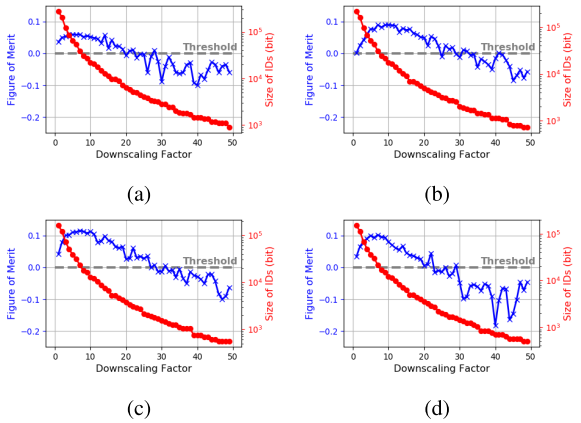


FIGURE 6. Figure of Merit (FoM) of (a) Dataset-A, (b) Dataset-B, (c) Dataset-C, and (d) Dataset-D with respect to downscaling factor (FoM: difference between minimum value of intra correlation and maximum value of inter correlation).

distinctive features, leading to higher maximum inter correlation (worse reliability) and lower minimum intra correlation (worse uniqueness). Therefore, the fingerprints are less distinguishable while reaching better compression rates. The trade-off between distinguishability and compression rate should be considered, and the downscaling rate should be selected according to targeted application specifications.

B. BENEFIS OF PRINTED ELECTRONICS

One of the major benefits of image fingerprints over all typical electrical PUFs is that in printed electronics based on additive manufacturing, the electrical properties of the printed circuits degrade over time and they are subject to environmental variations, far more than silicon devices [69]. That makes obtaining high reliability of typical electrical PUFs in printed electronics very challenging. However the optical features of printed structures are not subject to such variations. This makes image fingerprints intrinsically more reliable and robust to environmental variations. This also further motivates the need for an image fingerprint (i.e., non-electrical) in printed electronics, particularly based on additive processes, as opposed to conventional silicon VLSI. The main source of variations in image fingerprint, however, comes from variations in taking optical image (such as lighting, alignment, etc) which can be corrected with conventional image pre-processing methods.

C. DISCUSSION OF SECURITY IMPLICATIONS

As explained in Section I, the target of this work is to countermeasure counterfeiting and overbuilding of PE components. This can also enable counterfeit detection and prevention in other sectors by equipping the products with smart PE labels based on this fingerprinting scheme. In most prominent attack scenarios, the attacker has to clone the part of the component where the fingerprint is extracted from the optical fingerprint, such that the cloned component can be verified. Several cloning attacks have been performed on electrical PUFs [58], [70], [71]. Such attacks do not apply to optical fingerprints, which are directly visible to an attacker.

One specific attack is to use more precise subtractive tools (e.g. laser) than additive printing to clone the edge shape of ROI since ROI is the entropy source of the fingerprint. In terms of reproducibility, the shape of printed objects come from sub-manufacturing, i.e., uncontrollable variations and dispersion of inks on the substrate. Although the feature sizes reported in this work seem large, but assuming the attacker has printing devices with similar or even slightly higher resolution, it is impossible to generate the exact same shapes using additive manufacturing and printing techniques. This can be achieved by either fabricating the component using subtractive methods or reshaping already printed inks. However, such a costly fine-grained cloning attack has to be done in large volume to be economically viable for the attacker. However, using such costly precise processes defeats the purpose of ultra low-cost PE products, hence rendering such an attack economically unfit. Furthermore, regardless of economical suitability, in both ways, an attacker cannot imitate the thickness and smoothness of the edges (see Figure 4c), since the thickness and smoothness of ROI results from the random dispersion of inks, which is specific to additive manufacturing. Moreover, an additional step can be performed during the pre-processing to detect any sharp edges caused by subtractive processes directly.

D. DISCUSSION OF USAGE IN SUPPLY CHAIN TRACKING

We envision various application and use cases for which the identification of printed devices is necessary. For instance, in many application domains for fast-moving consumer goods (FMCG) market, such as identification and tracking [72], quality monitoring [73], and brand authentication [74], it can be envisioned that such a setup is available.

In addition to the usage of this fingerprinting scheme in PE applications for an anti-counterfeiting purpose, the proposed approach can be used for supply chain tracking thanks to its point-of-use fabrication feature. In the supply chain, each party can print a structure as a fingerprint (FP_i), which is a part of namely a *Super fingerprint*, along with

TABLE 1. Definition of datasets.

	# of EGTs	Width (μm)	Length (μm)	Image size of ROI after alignment
Dataset-A	18	600	60	350x780
Dataset-B	18	400	60	350x620
Dataset-C	18	200	60	350x460
Dataset-D	18	100	60	350x430

TABLE 2. Dataset compression results from Figure 6.

	FoM > 0, last downscaling factor	FoM > 0 storage size	FoM > 0 storage decrease	max(FoM) downscaling factor	max(FoM) storage size
Dataset-A	28×	3276 bit	83×	6×	39200 bit
Dataset-B	41×	1152 bit	188×	9×	17360 bit
Dataset-C	31×	1440 bit	112×	6×	23100 bit
Dataset-D	29×	1560 bit	96×	6×	21700 bit

formerly printed structures ($iFP_0, iFP_1, \ldots, iFP_{i-1}$). When the end-user or any party in the chain receives the product, it has a Super fingerprint consisting of multiple optical fingerprints, printed by each previous party in the supply chain. This way, the chain can be uniquely tracked down.

The advantage of using such optical fingerprint in supply chain tracking is that it can be printed using low-cost tools (e.g., inkjet-printer), which results in ultra-low-cost overhead while providing sufficient resolution in the range of 10 μm, and intrinsic visual features to sustain the unclonability of the optical fingerprints as discussed in Section V-C.

Additionally, as already stated in the introduction, this fingerprinting scheme can be used as smart printed label to prevent counterfeiting in other products such as brand clothes, smart personalized medicine and so on. This can also be used to prevent illegal recycling or refurbishing, as any item that is sold in the retail store, the fingerprint of the sold item can be tagged as "sold" in the database and even if the used item is tried to be sold as new or the smart tag is ripped and used in counterfeit products, it appears in the database as a "used" item and hence cannot be authenticated.

VI. CONCLUSION

The growing market of Printed Electronics (PE) bring about the counterfeiting of PE components. Unique and non-reproducible hardware fingerprints are commonly utilized to prevent counterfeiting. However, typical electrical PUFs which require extra circuitry and associated overhead to produce are infeasible in low-cost PE applications. In this paper, we present an image-based fingerprint extraction methodology from the optical variation of printed inks in the PE components. Therefore, no extra circuitry is required to obtain such a fingerprint. Moreover, we utilize an image downscaling technique to compress the extracted fingerprints to reduce the storage cost of the fingerprints. The methodology is applied to four datasets for evaluation. The results show that the optically visible variations of the printed inks are suitable to utilize in fingerprint extraction for anti-counterfeiting of PE, and the downscaling compression reduces the storage cost of the extracted fingerprints by 83×, while maintaining adequate PUF metrics. This approach shows the applicability of additive manufacturing to develop smart sensors to prevent counterfeiting in several sectors such as consumer brands, FMCG and disposable smart medicine.

REFERENCES

[1] V. Subramanian, D. Soltman, S. K. Volkman, Q. Zhang, J. B. Chang, A. de la Fuente Vornbrock, D. C. Huang, L. Jagannathan, F. Liao, B. Mattis, S. Molesa, and D. R. Redinger, "Printed electronics for low-cost electronic systems: Technology status and application development," in *Proc. ESSDERC 38th Eur. Solid-State Device Res. Conf.*, Sep. 2008, pp. 17–24.

[2] D. Schaefer and W. M. Cheung, "Smart packaging: Opportunities and challenges," *Proc. CIRP*, vol. 72, pp. 1022–1027, Jan. 2018.

[3] P. Ferreira, R. Martinho, and D. Domingos, "Iot-aware business processes for logistics: Limitations of current approaches," in *Proc. INForum*, 2010, pp. 611–622.

[4] H. Mora, D. Gil, R. M. Terol, J. Azorín, and J. Szymanski, "An IoT-based computational framework for healthcare monitoring in mobile environments," *Sensors*, vol. 17, no. 10, p. 2302, Oct. 2017.

[5] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, "SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors," in *Proc. IEEE 14th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Oct. 2012, pp. 238–243.

[6] J. Marques, B. Pahl, and C. Kallmayer, "Thermoplastic packaging and embedding technology for ID-cards," in *Proc. Microelectron. Packag. Conf. (EMPC) Eur.*, Sep. 2013, pp. 1–5.

[7] L. W. Ferreira and C. Decker, "A survey on organic smart labels for the Internet-of-Things," in *Proc. 7th Int. Conf. Netw. Sens. Syst. (INSS)*, Jun. 2010, pp. 161–164.

[8] E. N. Mambou, S. Nlom, T. G. Swart, K. Ouahada, A. Ndjiongue, and H. C. Ferreira, "Monitoring of the medication distribution and the refrigeration temperature in a pharmacy based on Internet of Things (IoT) technology," in *Proc. 18th Medit. Electrotech. Conf. (MELECON)*, Apr. 2016, pp. 1–5.

[9] F. Farabullini, F. Lucarelli, I. Palchetti, G. Marrazza, and M. Mascini, "Disposable electrochemical genosensor for the simultaneous analysis of different bacterial food contaminants," *Biosensors Bioelectron.*, vol. 22, no. 7, pp. 1544–1549, Feb. 2007.

[10] W. Burns, "Who launches taskforce to fight counterfeit drugs," *Bull. World Health Org.*, vol. 84, pp. 689–690, Jan. 2006.

[11] H. H. Cheung and S. H. Choi, "Implementation issues in RFID-based anti-counterfeiting systems," *Comput. Ind.*, vol. 62, no. 7, pp. 708–718, Sep. 2011.

[12] *Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, SAS Committee, Washington, DC, USA, 2012.

[13] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Jul. 2014.

[14] R. Das and X. He. (2020). *Flexible, Printed and Organic Electronics 2020–2030: Forecasts, Technologies, Markets*. [Online]. Available: http://www.idtechex.com/en/research-report/flexible-printed-and-organic%-electronics-2020-2030-forecasts-technologies-markets/687

[15] J. S. Chang, A. F. Facchetti, and R. Reuss, "A circuits and systems perspective of organic/printed electronics: Review, challenges, and contemporary and emerging design approaches," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 1, pp. 7–26, Mar. 2017.

[16] A. T. Erozan, M. Hefenbrock, M. Beigl, J. Aghassi-Hagmann, and M. B. Tahoori, "Reverse engineering of printed electronics circuits: From imaging to netlist extraction," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 475–486, 2020.

[17] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[18] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Cham, Switzerland: Springer, 2010, pp. 3–37.

[19] A. T. Erozan, G. C. Marques, M. S. Golanbari, R. Bishnoi, S. Dehm, J. Aghassi-Hagmann, and M. B. Tahoori, "Inkjet-printed EGFET-based physical unclonable function—Design, evaluation, and fabrication," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2935–2946, Dec. 2018.

[20] B. Wigger, T. Meissner, A. Förste, V. Jetter, and A. Zimmermann, "Using unique surface patterns of injection moulded plastic components as an image based physical unclonable function for secure component identification," *Sci. Rep.*, vol. 8, no. 1, p. 4738, Dec. 2018.
[21] V. Costa, A. Sousa, and A. Reis, "Cork as a unique object: Device, method, and evaluation," *Appl. Sci.*, vol. 8, no. 11, p. 2150, Nov. 2018.
[22] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, pp. 1–41, Nov. 2017.
[23] P. Syverson and I. Cervesato, "The logic of authentication protocols," in *International School on Foundations of Security Analysis and Design*. Cham, Switzerland: Springer, 2000, pp. 63–137.
[24] G. C. Marques, S. K. Garlapati, D. Chatterjee, S. Dehm, S. Dasgupta, J. Aghassi, and M. B. Tahoori, "Electrolyte-gated FETs based on oxide semiconductors: Fabrication and modeling," *IEEE Trans. Electron Devices*, vol. 64, no. 1, pp. 279–285, Jan. 2017.
[25] P. Rosa, A. Câmara, and C. Gouveia, "The potential of printed electronics and personal fabrication in driving the Internet of Things," *Open J. Internet Things (OJIOT)*, vol. 1, no. 1, pp. 16–36, 2015.
[26] C. Dagdeviren, "Conformal piezoelectric energy harvesting and storage from motions of the heart, lung, and diaphragm," *Proc. Nat. Acad. Sci. USA*, vol. 111, no. 5, pp. 1927–1932, 2014.
[27] C. Steiger, A. Abramson, P. Nadeau, A. P. Chandrakasan, R. Langer, and G. Traverso, "Ingestible electronics for diagnostics and therapy," *Nature Rev. Mater.*, vol. 4, no. 2, pp. 83–98, Feb. 2019.
[28] Y. J. Chan, C. P. Kung, and Z. Pei, "Printed RFID: Technology and application," in *Proc. IEEE Int. Wkshp Radio-Frequency Integr. Technology: Integr. Circuits Wideband Comm Wireless Sensor Netw.*, Nov. 2005, pp. 139–141.
[29] V. Subramanian, P. C. Chang, D. Huang, J. B. Lee, S. E. Molesa, D. R. Redinger, and S. K. Volkman, "All-printed RFID tags: Materials, devices, and circuit implications," in *Proc. 19th Int. Conf. VLSI Design Held Jointly With 5th Int. Conf. Embedded Syst. Design (VLSID)*, Jan. 2006, p. 6.
[30] V. Subramanian, P. C. Chang, J. B. Lee, S. E. Molesa, and S. K. Volkman, "Printed organic transistors for ultra-low-cost RFID applications," *IEEE Trans. Compon. Packag. Technol.*, vol. 28, no. 4, pp. 742–747, Dec. 2005.
[31] L. Yang and M. M. Tentzeris, "Design and characterization of novel paper-based inkjet-printed RFID and microwave structures for telecommunication and sensing applications," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Jun. 2007, pp. 1633–1636.
[32] K. C. Honeychurch and J. P. Hart, "Screen-printed electrochemical sensors for monitoring metal pollutants," *TrAC Trends Anal. Chem.*, vol. 22, no. 7, pp. 456–469, 2003.
[33] S. Laschi, I. Palchetti, and M. Mascini, "Gold-based screen-printed sensor for detection of trace lead," *Sens. Actuators B, Chem.*, vol. 114, no. 1, pp. 460–465, Mar. 2006.
[34] B. Li, "Inkjet printed chemical sensor array based on polythiophene conductive polymers," *Sens. Actuators B, Chem.*, vol. 123, no. 2, pp. 651–660, 2007.
[35] F. C. Krebs, "Fabrication and processing of polymer solar cells: A review of printing and coating techniques," *Solar Energy Mater. Solar Cells*, vol. 93, no. 4, pp. 394–412, Apr. 2009.
[36] R. Hahn and H. Reichl, "Batteries and power supplies for wearable and ubiquitous computing," in *Dig. Papers. 3rd Int. Symp. Wearable Comput.*, Oct. 1999, pp. 168–169.
[37] M. Hilder, B. Winther-Jensen, and N. Clark, "Paper-based, printed zinc–air battery," *J. Power Sources*, vol. 194, no. 2, pp. 1135–1141, 2009.
[38] A. C. Arsenault, D. P. Puzzo, I. Manners, and G. A. Ozin, "Photonic-crystal full-colour displays," *Nature Photon.*, vol. 1, no. 8, p. 468, 2007.
[39] J. Heikenfeld, P. Drzaic, J.-S. Yeo, and T. Koch, "A critical review of the present and future prospects for electronic paper," *J. Soc. Inf. Display*, vol. 19, no. 2, pp. 129–156, Feb. 2011.
[40] K. Flamm, "Measuring Moore's Law: Evidence from price, cost, and quality indexes," in *Measuring and Accounting for Innovation in the Twenty-First Century*. Cambridge, MA, USA: Nat. Bureau Econ. Res., 2018, pp. 403–470. [Online]. Available: https://www.nber.org/books-and-chapters/measuring-and-accounting-innovation-twenty-first-century/measuring-moores-law-evidence-price-cost-and-quality-indexes
[41] V. Subramanian, D. Soltman, S. K. Volkman, Q. Zhang, J. B. Chang, A. de la Fuente Vornbrock, D. C. Huang, L. Jagannathan, F. Liao, B. Mattis, S. Molesa, and D. R. Redinger, "Printed electronics for low-cost electronic systems: Technology status and application development," in *Proc. ESSDERC 38th Eur. Solid-State Device Res. Conf.*, Sep. 2008, pp. 17–24.
[42] C. D. Dimitrakopoulos and P. R. L. Malenfant, "Organic thin film transistors for large area electronics," *Adv. Mater.*, vol. 14, no. 2, pp. 99–117, 2002.
[43] H. Sirringhaus, "25th anniversary article: Organic field-effect transistors: The path beyond amorphous silicon," *Adv. Mater.*, vol. 26, no. 9, pp. 1319–1335, Jan. 2014.
[44] L.-L. Chua, J. Zaumseil, J.-F. Chang, E. C.-W. Ou, P. K.-H. Ho, H. Sirringhaus, and R. H. Friend, "General observation of n-type field-effect behaviour in organic semiconductors," *Nature*, vol. 434, no. 7030, p. 194, 2005.
[45] S. Kyung, J. Kwon, Y.-H. Kim, and S. Jung, "Low-temperature, solution-processed, 3-D complementary organic FETs on flexible substrate," *IEEE Trans. Electron Devices*, vol. 64, no. 5, pp. 1955–1959, May 2017.
[46] G. C. Marques, D. Weller, A. T. Erozan, X. Feng, M. Tahoori, and J. Aghassi-Hagmann, "Progress report on 'from printed electrolyte-gated metal-oxide devices to circuits,'" *Adv. Mater.*, vol. 31, Jun. 2019, Art. no. 1806483.
[47] S. K. Garlapati, N. Mishra, S. Dehm, R. Hahn, R. Kruk, H. Hahn, and S. Dasgupta, "Electrolyte-gated, high mobility inorganic oxide transistors from printed metal halides," *ACS Appl. Mater. Interfaces*, vol. 5, no. 22, pp. 11498–11502, 2013.
[48] P. K. Nayak, M. N. Hedhili, D. Cha, and H. N. Alshareef, "High performance In_2O_3 thin film transistors using chemically derived aluminum oxide dielectric," *Appl. Phys. Lett.*, vol. 103, no. 3, Jul. 2013, Art. no. 033518.
[49] A. T. Erozan, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, "Inkjet-printed true random number generator based on additive resistor tuning," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 1361–1366.
[50] Y. Qi, N. T. Jafferis, K. Lyons, C. M. Lee, H. Ahmad, and M. C. McAlpine, "Piezoelectric ribbons printed onto rubber for flexible energy conversion," *Nano Lett.*, vol. 10, no. 2, pp. 524–528, 2010.
[51] M. Rostami, J. B. Wendt, M. Potkonjak, and F. Koushanfar, "Quo Vadis, PUF?: Trends and challenges of emerging physical-disorder based security," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–6.
[52] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
[53] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[54] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.
[55] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148–160.
[56] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.
[57] L. Zimmermann, A. Scholz, M. B. Tahoori, J. Aghassi-Hagmann, and A. Sikora, "Design and evaluation of a printed analog-based differential physical unclonable function," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 11, pp. 2498–2510, Nov. 2019.
[58] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek, "Optical PUFs reloaded," *Eprint. Iacr. Org.*, May 2013.
[59] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," in *Proc. 18th Annu. Comput. Secur. Appl. Conf.*, Dec. 2002, pp. 149–160.
[60] U. Kocabaş, A. Peter, S. Katzenbeisser, and A.-R. Sadeghi, "Converse PUF-based authentication," in *Proc. Int. Conf. Trust Trustworthy Comput.* Cham, Switzerland: Springer, 2012, pp. 142–158.
[61] S. van der Walt, J. L. Schönberger, J. Nunez-Iglesias, F. Boulogne, J. D. Warner, N. Yager, E. Gouillart, and T. Yu, "Scikit-image: Image processing in Python," *PeerJ*, vol. 2, p. e453, Jun. 2014, doi: 10.7717/peerj.453.
[62] C. Tomasi and R. Manduchi, "Bilateral filtering for gray and color images," in *Proc. 6th Int. Conf. Comput. Vis.*, Jan. 1998, pp. 839–846.
[63] S. M. Pizer, E. P. Amburn, J. D. Austin, R. Cromartie, A. Geselowitz, T. Greer, B. T. H. Romeny, J. B. Zimmerman, and K. Zuiderveld, "Adaptive histogram equalization and its variations," *Comput. Vis., Graph., Image Process.*, vol. 39, pp. 355–368, Sep. 1987.

[64] R. O. Duda and P. E. Hart, "Use of the Hough transformation to detect lines and curves in pictures," *Commun. ACM*, vol. 15, no. 1, pp. 11–15, Jan. 1972.
[65] K. Briechle and U. D. Hanebeck, "Template matching using fast normalized cross correlation," *Proc. SPIE*, vol. 4387, pp. 95–102, Mar. 2001.
[66] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design With FPGAs*. Cham, Switzerland: Springer, 2013, pp. 245–267.
[67] J. S. Liberty, A. Barrera, D. W. Boerstler, T. B. Chadwick, S. R. Cottier, H. P. Hofstee, J. A. Rosser, and M. L. Tsai, "True hardware random number generation implemented in the 32-nm soi power7+ processor," *IBM J. Res. Develop.*, vol. 57, no. 6, pp. 1–4, 2013.
[68] J. Von Neumann, "13. various techniques used in connection with random digits," *Appl. Math. Ser.*, vol. 12, nos. 36–38, p. 5, 1951.
[69] G. C. Marques, F. von Seggern, S. Dehm, B. Breitung, H. Hahn, S. Dasgupta, M. B. Tahoori, and J. Aghassi-Hagmann, "Influence of humidity on the performance of composite polymer electrolyte-gated field-effect transistors and circuits," *IEEE Trans. Electron Devices*, vol. 66, no. 5, pp. 2202–2207, May 2019.
[70] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, "Cloning physically unclonable functions," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2013, pp. 1–6.
[71] S. B. Dodo, R. Bishnoi, S. M. Nair, and M. B. Tahoori, "A spintronics memory PUF for resilience against cloning counterfeit," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 11, pp. 2511–2522, Nov. 2019.
[72] K. Domdouzis, B. Kumar, and C. Anumba, "Radio-frequency identification (RFID) applications: A brief introduction," *Adv. Eng. Inform.*, vol. 21, no. 4, pp. 350–355, 2007.
[73] J. A. Cavallo, M. C. Strumia, and C. G. Gomez, "Preparation of a milk spoilage indicator adsorbed to a modified polypropylene film as an attempt to build a smart packaging," *J. Food Eng.*, vol. 136, pp. 48–55, Sep. 2014.
[74] M. Peris and L. Escuder-Gilabert, "Electronic noses and tongues to assess food authenticity and adulteration," *Trends Food Sci. Technol.*, vol. 58, pp. 40–54, Dec. 2016.

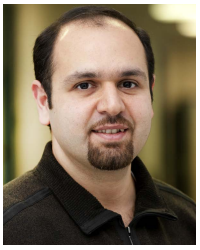
AHMET TURAN EROZAN received the B.S. degree in electronics and communication engineering from Istanbul Technical University, Istanbul, Turkey, in 2013, the M.S. degree from Yildirim Beyazit University, Ankara, Turkey, in 2015, and the Ph.D. degree in computer science from the Karlsruhe Institute of Technology, (KIT), Karlsruhe, Germany, in 2020. His research interests include hardware security, circuits and systems, and emerging computing technologies.

MICHAEL HEFENBROCK received the Ph.D. degree in computer science from the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, in 2022. His current research interests include machine learning and optimization and their application to problems in design automation.

DENNIS R. E. GNAD received the B.Eng. degree in computer engineering from Hochschule Pforzheim University, in 2011, and the M.Sc. and Ph.D. degrees in computer science from the Karlsruhe Institute of Technology (KIT), in 2015 and 2020, respectively. He is currently a Postdoctoral Researcher at KIT, with the research focus on various topics related to security in hardware.

MICHAEL BEIGL received the M.Sc. and Ph.D. degrees from the University of Karlsruhe (currently KIT), Germany. He is currently a Professor in pervasive computing systems at KIT and the Head of the TECO Research Laboratory. Previously, he was a Professor at the TU Braunschweig, from 2006 to 2010, a Visiting Associate Professor at Hide Tokuda Laboratories, Keio University, Japan, in 2005, and the Research Director of the TECO, KIT, from 2001 to 2005. He has been heading the Smart Data Innovation Laboratory (SDIL), National Competence Center for Big Data AI, and the State Competence Center for Big Data AI in Baden-Württemberg, the Smart Data Solution Center (SDSC-BW), since 2014. His research interests include blending human with computing, with specific interest in sensing systems, and blending artificial and human intelligence.

JASMIN AGHASSI-HAGMANN (Member, IEEE) received the Graduate degree in physics from Aachen University (RWTH), and the Ph.D. degree in theoretical physics from Karlsruhe University. In 2007, she joined Infineon Technologies, Munich, Germany, and in 2011, Intel, Germany, as a Device Expert for low power CMOS technologies. In 2013, she became a Full Professor in electrical engineering at Offenburg University. Since 2021, she has been a Full Professor in electronic devices and systems in future technologies at the Institute of Nanotechnology, KIT, Germany, focusing on printed electronics. She has authored and coauthored more than 60 publications in this field.



MEHDI B. TAHOORI (Fellow, IEEE) received the B.S. degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2000, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, USA, in 2002 and 2003, respectively. In 2003, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Northeastern University, where he became an Associate Professor, in 2009. He was a Visiting Professor at the VLSI Design and Education Center (VDEC), The University of Tokyo, Japan, in 2015. From 2002 to 2003, he was a Research Scientist with Fujitsu Laboratories of America, Sunnyvale, CA, USA. He is currently a Professor and the Chair of Dependable Nano-Computing at KIT. He was a recipient of the U.S. National Science Foundation Early Faculty Development (CAREER) Award, in 2008. He has received a number of best paper nominations and awards at various conferences and journals. He is a recipient of European Research Council (ERC) Advanced Grant. He was the Program Chair of VLSI Test Symposium in (VTS), in 2021and 2018, and the General Chair of European Test Symposium (ETS), in 2019. He is also the Deputy Editor-in-Chief of *IEEE Design and Test* magazine. He was the Editor-in-Chief of *Microelectronic Reliability* journal.