Comparative Analysis of Copy Detection Patterns and Physical Unclonable Functions in Authentication Systems: A Mobile Phone Perspective

Roman Chaban, Ethan Icet, Olga Taran, Slava Voloshynovskiy
Department of Computer Science, University of Geneva
Stochastic Information Processing Group
Geneva, Switzerland
roman.chaban@unige.ch, ethan.icet@gmail.com, taran.olga@gmail.com, svolos@unige.ch

***Abstract*—In this paper, we perform a comparative analysis of Copy Detection Patterns (CDP) and Physical Unclonable Functions (PUFs) within the context of anti-counterfeiting technologies, examining their effectiveness against machine-learning based attacks and their functioning across different mobile imaging devices. In the evaluation involving both iPhone 12 Pro and Samsung Galaxy S20, we assess the authentication performance of CDP and PUFs integragted in printed labels produced on industrial printer. Our approach includes the creation of machine-learning based counterfeits to challenge the resilience of each authentication method. The outcomes, quantified via Receiver Operating Characteristic analysis, reveal the robustness of CDP and PUFs against counterfeiting, underscoring CDP's consistency across mobile devices and highlighting PUFs's sensitivity to the variations in mobile imaging quality. This research not only provides insights into the operational strengths and vulnerabilities of CDP and PUFs but also proposes recommendations for enhancing the practical applications of these technologies in protection against counterfeit goods.**

I. Introduction

In the realm of anti-counterfeiting technologies, Copy Detection Patterns (CDP) have emerged as a novel and effective method for protecting goods [1]. CDP have been the focus of extensive research in recent years, leading to various authentication and identification strategies, including template-less methods [1], or using a template of digital [2], synthetic [3] or potentially physical template as reference, which we explore in this study. CDP offer several advantages: they are cost-effective, scalable to any production volume, are applicable in numerous industries, and well-recognized for their resistance to counterfeiting [1]. Nonetheless, some recent studies have shown vulnerabilities of CDP, challenging their perceived security through successful forgery attacks [4] [5] or due to the variability caused by manufacturing parameters [6].

Parallel to CDP, Physical Unclonable Functions (PUFs) is another well-established countermeasure against counterfeiting [7] [8]. PUFs operate on the principle of comparing an incoming probe with a reference stored in an enrollment database, leveraging the unique microstructure for example, paper substrate, making the replication physically infeasible. This study aims at conducting a comparative analysis between CDP and PUFs, particularly focusing on the clonability of CDP and the inherent copy-proof nature of PUFs. More detailed comparison is presented in Table I.

TABLE I: The comparative analysis of CDP- and PUF-based authentication systems (the best characteristic in **bold**).

Characteristic	CDP	PUFs
Nature	Additive	Inherently non-additive
Cost of Clonability	Low	**High**
Sensitivity to Wear & Tear	**Low**	High
Enrollment Needs	**Flexible**	Requires individual
Verification Capability	Compatible with mobile phones	Compatible with mobile phones
Robustness to Environment	**High**	Medium
Requirements to Substrate	**Low**	High
Application Scope	**Broad**	Specific
Key Advantages	Scalable, adaptable	High security
Key Limitations	Cloning vulnerability	Wear sensitivity

Our investigation is driven by a hypothesis that while CDP cloneability presents a potential vulnerability, albeit with a certain degree of difficulty, PUFs offer an inherently more secure method due to their reliance on unique physical characteristics [9]. This study intends to evaluate the effectiveness of these two security features in authenticating goods, examining their strengths, weaknesses, and potential for coexistence or superiority in specific contexts. Though it is worth mentioning that the enrollment process contrasts with the main advantage of CDP-based authentication system – cost-effectiveness. We believe that there is a huge potential in research to workaround the enrollment necessity for robust and high-accuracy applications, especially in the domain of synthetic CDP [10].

In addition, it is important to highlight the risks of using sophisticated machine learning models which may tackle many authentication aspects but at the same time, they inherently impose critical vulnerabilities linked to the explainability and can be exploited with machine learning countermeasures like adversarial attacks [11] and cloneability [4].

Finally, this research also explores the influence of various acquisition devices on the authentication process. By assessing whether different devices can be used interchangeably or if a consistent methodology should be maintained across both

S. Voloshynovskiy is a corresponding author.

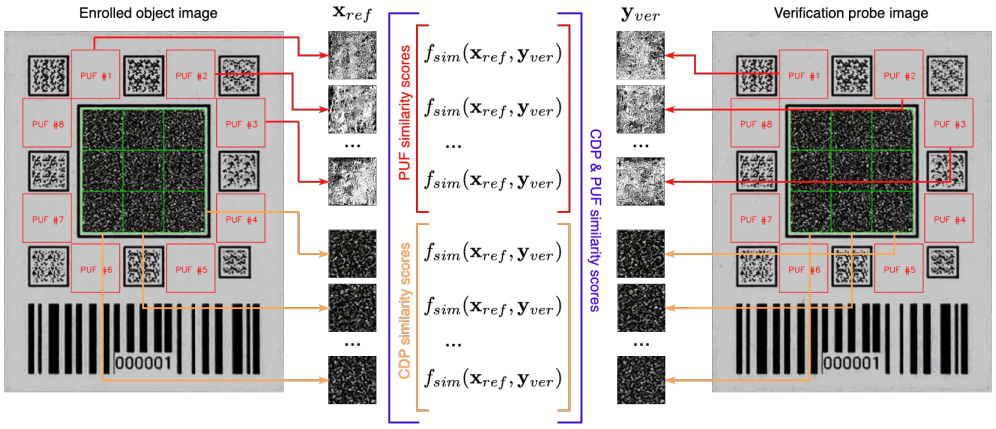

Fig. 1: The illustrative example of a layout of $\mathbf{x}_{ref}$ and $\mathbf{y}_{ver}$, which comprises CDP (green squares) in the center and PUFs (red squares). The barcode serves as the identifier and the synchromarkers (8 smaller printed elements) are used for the pixel-precision alignment.

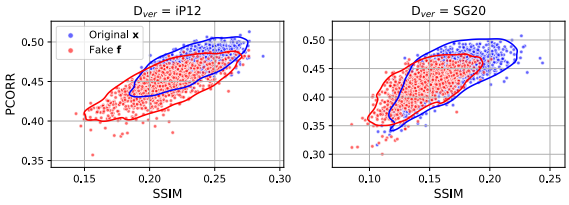

Fig. 2: The distributions of $f_{sim}(\mathbf{y}, \mathbf{t})$ depicting the mere separability between originals $\mathbf{x}$ and fakes $\mathbf{f}$.

enrollment and verification stages, we aim to provide insights into the optimization of anti-counterfeiting strategies. Through this comprehensive analysis, we seek to determine the most effective approach based on CDP, PUF or their joint use for goods protection, contributing to the ongoing discourse on anti-counterfeiting technologies.

In conclusion, our analysis demonstrates that, under machine learning-based attacks, CDP authentication based on physical template not only maintains a higher degree of robustness to imaging device variability but also achieves enhanced performance levels in comparison to PUFs. While PUFs are inferior in terms of performance, we unveil its comparative advantages through the benchmarks and address them for the specific use-cases.

II. Dataset

In this work, we utilize the previously published dataset known as *Indigo 1x1 mobile* [12], which employs CDP printed on Invercote G $220\mathrm{g}/\mathrm{m}^2$ printing substrate. CDP digital template $\mathbf{t}$ is 228×228 pixels in size, where half of the pixels are black and the other half are white, arranged in a completely random structure. This randomness is determined by a unique identifier encoded in a barcode as shown in Fig. 1, which also serves as a seed for the generation of CDP pattern.

The total amount of unique CDPs is 1440 which were printed using the industrial digital offset printer HP Indigo 5500. CDP dataset comprises both original $\mathbf{x}$ and fake $\mathbf{f}$. Fake CDP $\mathbf{f}$ were created by scanning the original CDP $\mathbf{x}$ using a scanner at 2400 PPI and estimating their original digital representation $\hat{\mathbf{t}}$ via a specially trained U-Net estimator [4]. An average probability of bit-error between $\mathbf{t}$ and $\hat{\mathbf{t}}$ $P_{\mathrm{BER}} \approx 0.06$. Then estimated CDP $\hat{\mathbf{t}}$ were printed using exactly the same parameters. As a result the fakes $\mathbf{f}$ are hardly distinguishable from the original CDP both perceptually and statistically as shown in Fig. 2 in terms of similarity metric $f_{sim}(\mathbf{y}, \mathbf{t})$, where f_{sim} can be either Pearson correlation (PCORR) or Structural Similarity Index Measure (SSIM) [13]. Consequently, we are presented with two physical instances of CDP within the dataset: the original $\mathbf{x}$ and the fake $\mathbf{f}$. However, from the perspective of PUFs authentication, they can be simply treated as two distinct physical subsets effectively yielding 1440×2 unique physical instances.

Each CDP was captured using two mobile phones, the iPhone 12 Pro (iP12) and the Samsung Galaxy Note 20 Ultra (SG20), with a special application designed to obtain demosaiced, and uncompressed images. The cameras of both phones, being the default wide cameras, provided an effective approximate resolution of 600 PPI from an approximate distance about 13cm from the acquisition surface. With such an approach, we achieved the highest possible image quality for these phones. As a result, it effectively yielded 6 photos per CDP. All obtained CDP $\mathbf{y}$ were aligned with respect $\mathbf{t}$ using SIFT descriptors [14] with an additional pixel-precision alignment using auxiliary synchromarkers which can be seen in Fig. 1. Since the acquisition was done over a long period by a human, we have conducted mostly automatic and sometimes manual quality control to eliminate CDP which were unsatisfactory for the authentication (blurred, low contrast, etc.).

III. Methodology

Given the dataset at our disposal, we divided it into two principal subsets to facilitate our study. The first subset is designated for **enrollment** or **reference** $\mathbf{x}_{ref}$. CDP included in the enrollment serve as references for training our classifier and for assessing the similarity of incoming probe $\mathbf{y}_{ver}$, which can be either original $\mathbf{x}_{ver}$ or fake $\mathbf{f}_{ver}$. The second subset is termed the **verification** subset. This subset is utilized

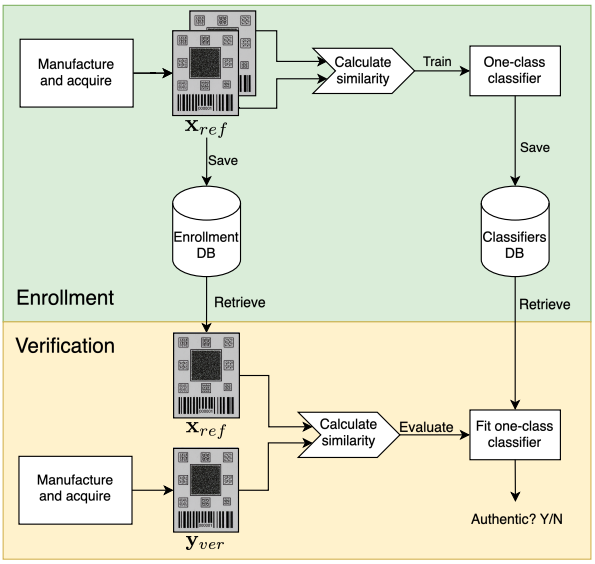

Fig. 3: The diagram depicting the processes of $\mathbf{x}_{ref}$ enrollment and verification of $\mathbf{y}_{ver}$.

for comparing incoming CDP $\mathbf{y}_{ver}$ against $\mathbf{x}_{ref}$ from the enrollment subset.

To assess the similarity we selectively extract the security features from the image of CDP label as shown in Fig. 1. This approach is coherent throughout both enrollment and verification stages. By comparing two security features from the enrollment database, we compute similarity scores. These similarity scores are instrumental in training our classifier of choice, the isolation forest [15] [1]. The enrollment process is well-illustrated in Fig. 3 (green part).

As shown in Fig. 3 (yellow part), during the verification stage, the dataset encompasses both original $\mathbf{x}_{ver}$ and fake $\mathbf{f}_{ver}$ (counterfeit) CDP. This allows for a comprehensive examination where the incoming CDP probe, denoted as $\mathbf{y}_{ver}$, can either be an original $\mathbf{x}_{ver}$ or a fake $\mathbf{f}_{ver}$. The verification process thus hinges on the comparison of $\mathbf{y}_{ver}$ against the reference $\mathbf{x}_{ref}$ from the enrollment database. In scenarios, where $\mathbf{y}_{ver}$ matches the statistics of the reference CDP $\mathbf{x}_{ref}$, it is classified as original $\mathbf{x}$. Conversely, should $\mathbf{y}_{ver}$ represent a counterfeit $\mathbf{f}$, it is identified as an anomaly and rejected.

To extract a visually perceivable microstructure from a feature-poor we came up with a straightforward solution after many approaches and trials. Ultimately, for current case the most effective solution is converting to grayscale followed by histogram equalization. The resulting eight PUFs of 90×90 pixels are shown in Fig. 1.

Distinctively, in contrast to previous studies where CDP of the same size was treated as a whole, this study relies on different approach to balance the information obtained via PUFs and CDP. This is achieved by splitting CDP into nine blocks, resulting in non-overlapping blocks of 76×76 pixels. As for CDP we did not apply any pre-processing.

[1]Training size $\approx$ 20% of dataset, $N_{\text{estimators}}$=200, contamination=0.02, random state is fixed.

Furthermore, our research explores three distinct authentication scenarios: utilizing only PUFs, only CDP, or a combination of both to calculate the similarity scores. The experimental logic of these approaches is shown in detail in Fig. 3.

IV. Experiment and Results

In our investigation, we have concluded numerous experiments to gain a wider perspective on the most optimal approach. However, for the sake of simplicity and to present the results in a clear way we proceed with the following setups, which answer the key research questions.

First of all, Fig. 4 presents four different scenarios using one device for the enrollment D_{ref} and another for verification D_{ver}. The reference subset acquired with D_{ref} was used to fit the PCA model using CDP and PUFs from originals $\mathbf{x}_{ref}$ and both PCORR and SSIM as similarity metrics. In total, we have two scenarios when $\mathrm{D}_{ref} = \mathrm{D}_{ver}$ and two when $\mathrm{D}_{ref} \neq \mathrm{D}_{ver}$. For Fig. 4 we proceeded with both security features and similarity metrics to assess the separability of original and fake distributions.

We observe the expected behavior for the case $\mathrm{D}_{ref} = \mathrm{D}_{ver}$ where the distribution of $\mathbf{x}_{ver}$ completely overlaps with those of $\mathbf{x}_{ref}$. On the other hand, the superior imaging quality of iP12 is very noticeable in comparison to SG20, since for SG20 we observe a small overlap between $\mathbf{x}_{ver}$ and $\mathbf{f}_{ver}$. As for $\mathrm{D}_{ver} \neq \mathrm{D}_{ref}$ case, we observe that distributions of $\mathbf{x}_{ref}$ and $\mathbf{x}_{ver}$ have much smaller overlap and still being clustered from fakes $\mathbf{f}_{ver}$. Fig. 4 additionally confirms that distributions of $\mathbf{y}_{ver}$ at the verification stage are strongly conditioned by D_{ref} as we can see on plots where D_{ref} = SG20 or D_{ref} = iP12.

To evaluate which combination of security features and similarity metrics yields the best authentication accuracy we proceeded with the classification model of choice: isolation forest. In this experiment we considered using nine combinations of metrics and security features. The corresponding ROCs are shown in Fig. 5, where each ROC represents a different combination of parameters used to form a set of features for the training and testing of the model. For each subfigure, the choices of D_{ref} and D_{ver} correspond to Fig. 4.

The first notable result is the inferior performance of the model using only the features obtained from PUFs (blue, orange, and green ROCs). On average, $\mathrm{AUC}_{\mathrm{PUFs}} < \mathrm{AUC}_{\mathrm{CDP}}$ regardless of the similarity metrics. This observation can be explained by PUFs origin nature (printing substrate) which micro-structure is feature-poor comparatively to many other materials. However, it can be mitigated by using a higher quality imaging system as shown in $\mathrm{D}_{ref} = \mathrm{D}_{ver}$ = iP12 case, where $\mathrm{AUC} \approx 1.00$ for any scenario.

Another observation is that $\mathrm{AUC}_{\mathrm{PUFs\&CDP}} > \mathrm{AUC}_{\mathrm{CDP}} > \mathrm{AUC}_{\mathrm{PUFs}}$ regardless of used metrics. This result is explainable primarily by the increase of effective information from security features we use for the similarity estimation.

More importantly, following the results obtained with $\mathrm{D}_{ref} = \mathrm{D}_{ver}$ = iP12 we can state that the proper mobile phone selection for the enrollment is the key factor in creating a robust and accurate system, which can achieve good

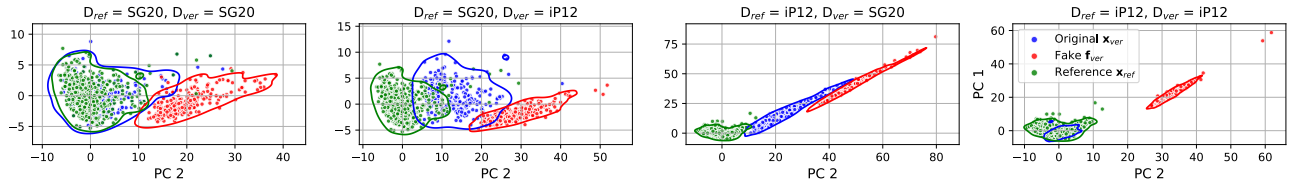

Fig. 4: The scatter plots of PCA($f_{sim}(\mathbf{x}_{ref}, \mathbf{y}_{ver})$) using PUFs & CDP and both metrics.

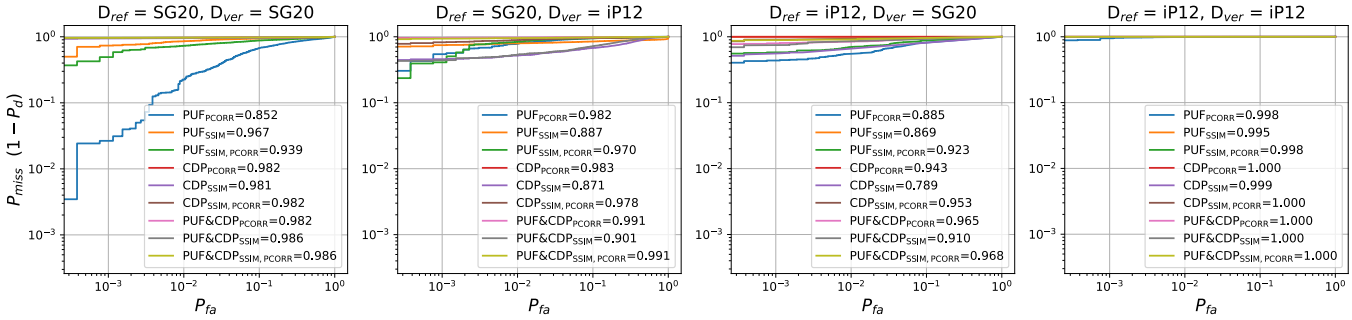

Fig. 5: ROC curves of isolation forest output trained on D_{ref} subset. Legend indicates the combination of parameters with the respective AUC value.

performance using only PUFs as a security feature, while for $\mathrm{D}_{ref} = \mathrm{D}_{ver} =$ SG20 even using information-rich CDP cannot achieve theoretically satisfactory AUC > 0.99.

At last, for the best-case scenario which is using both CDP and PUFs it is also beneficial to use both SSIM and PCORR. Given this, it is possible to extend the list of similarity metrics [16] or try to incorporate some more recent approaches based on deep classifiers [17].

Following the insights we obtained through ROCs and respective AUC it is necessary to assess the actual accuracy of the model in terms of probability of miss P_{miss} and of false acceptance P_{fa}. Concerning Fig. 5 we proceeded with both similarity metrics to train and test the isolation forest. The results are shown in Fig. 6. Note, that AUC values may differ from the ones in Fig. 5 since this time we fine-tuned the model hyper-parameters.

For real-world applications, the measures of P_{miss} and P_{fa} are the best assessments of model performance. Note that since we train the one-class classifier we cannot rely on P_{fa} to forecast the system robustness against fakes and fine-tune it. Thus, in contrast to AUC which is computed by finding the optimal threshold between two classes, in the current scenario we completely rely on the arbitrary threshold of the classifier which was established during the training phase. It is motivated by high standards of the security domain related to the protection of physical goods, where the nature of the potential fake is inherently unknown.

Based on the mentioned constraints we can analyze the results shown in Fig. 6. Notably the previously noticed dynamics between CDP and PUFs is the most pronounced for $\mathrm{D}_{ref} = \mathrm{D}_{ver} =$ SG20 case, where CDP completely outperforms PUFs with $P_{fa} = 0$, but with a small increase in P_{miss}. As for $\mathrm{D}_{ref} = \mathrm{D}_{ver} =$ iP12 such difference between security features is negligible. As expected, a combination of both PUFs and CDP for both mobile phones in $\mathrm{D}_{ref} = \mathrm{D}_{ver}$ case increases the classification accuracy and these results are relatively correlated to ROCs and AUC.

The $\mathrm{D}_{ref} \neq \mathrm{D}_{ver}$ scenarios demonstrate the potential to fine-tune the classifier's decision threshold θ in order to obtain a higher accuracy when the verification device differs from the one used during enrollment. In device mismatch scenarios we still observe a certain degree of separability between $\mathbf{x}_{ver}$ and $\mathbf{f}_{ver}$ and AUC > 0.92 is an indicator of this. Setting the threshold to default $\theta = 0$ yields $P_{miss} > \approx 0.9$ in the majority of the cases, but at the same time $\mathbf{f}_{ver}$ are still classified properly at $P_{fa} = 0$ in any given scenario.

V. Key Observations

Following the main experimental results, we can briefly highlight the most important findings concisely:

1) Device consistency ($\mathrm{D}_{ref} = \mathrm{D}_{ver}$) yields the most accurate authentication, whereas device mismatch ($\mathrm{D}_{ref} \neq \mathrm{D}_{ver}$) still permits clear separation of $\mathbf{x}_{ver}$ from $\mathbf{f}_{ver}$ despite smaller overlaps.
2) Imaging quality of iP12 is the key factor of a superior authentication accuracy over SG20, and generally iP12 as an enrollment device enhances the performance.
3) PUFs features alone show inferior performance compared to CDP or CDP & PUF, limited by the microstructure content, albeit improvable with high-quality imaging, speficially with iP12.
4) An enrollment device has a bigger impact on the final accuracy, than the one used for the enrollment in the scenarios of device mismatch.

VI. Conclusions and Future Work

In this work, we explored the capabilities and limitations of two pivotal anti-counterfeiting technologies: CDP and PUFs.

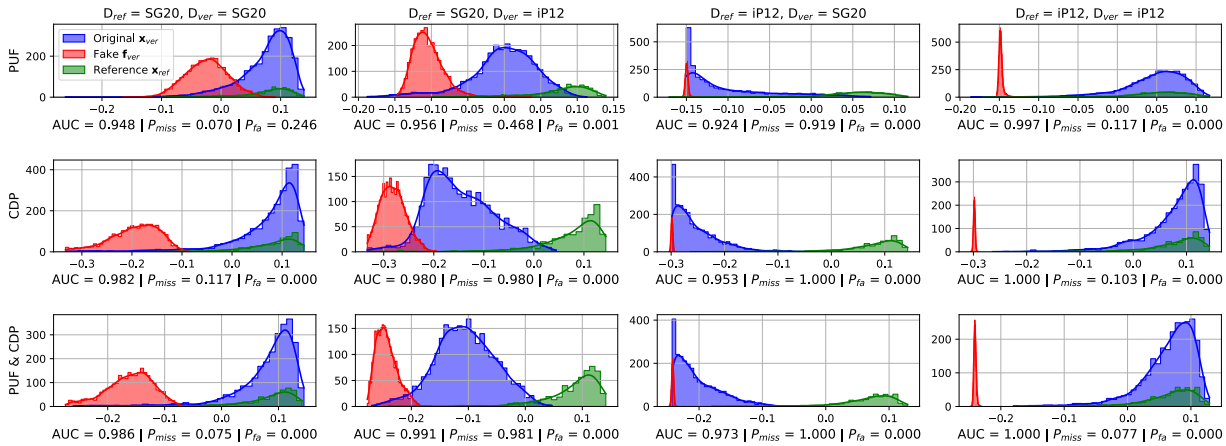

Fig. 6: The histograms of isolation forest decision function output. The Y-axis label indicates the security features used for the similarity estimation. Three performance measures AUC, P_{miss}, and P_{fa} are shown under each plot.

Our comparative analysis revealed the key similarities and differences between authentication methods.

A significant insight from our investigation is the importance of consistency between the devices used for enrollment and verification processes. The study demonstrated that even though devices like the iPhone 12 Pro and the Samsung Galaxy 20 Ultra differ in imaging quality, a combination of CDP and PUFs markedly improves authentication fidelity.

The challenges posed by the need for an extensive enrollment database and the deployment of sophisticated machine learning models are strongly conditioned by the protection against high-quality machine learning fakes of CDP. Such an approach must balance leveraging the strengths of both digital and physical template-based authentication systems to engineer solutions that are not only secure but also pragmatically viable for a widespread application.

Future investigations should focus on creating new similarity metrics specific to a security feature of choice, improving the manufacturing and enrollment strategies of both CDP and PUFs, and creating a generalized classification system to facilitate the authentication process which may offer robustness to imaging devices used for verification.

In conclusion, our findings advocate for a methodological pivot towards a non-trainable system with elementary preprocessing techniques to construct a robust authentication framework. The proposed framework shows remarkable resilience to variations in imaging devices and excels in performance though is tied to excessive enrollment needs.

References

[1] J. Picard, "Digital authentication with copy-detection patterns," *Electron. Imaging*, vol. 5310, 06 2004.

[2] O. Taran, J. Tutt, T. Holotyak, R. Chaban, S. Bonev, and S. Voloshynovskiy, "Mobile authentication of copy detection patterns: how critical is to know fakes?" in *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2021, pp. 1–6.

[3] Y. Belousov, B. Pulfer, R. Chaban, J. Tutt, O. Taran, T. Holotyak, and S. Voloshynovskiy, "Digital twins of physical printing-imaging channel," in *2022 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2022, pp. 1–6.

[4] R. Chaban, O. Taran, J. Tutt, T. Holotyak, S. Bonev, and S. Voloshynovskiy, "Machine learning attack on copy detection patterns: are 1x1 patterns cloneable?" in *IEEE International Workshop on Information Forensics and Security (WIFS)*, December 2021.

[5] E. Khermaza, I. Tkachenko, and J. Picard, "Can copy detection patterns be copied? evaluating the performance of attacks and highlighting the role of the detector," in *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2021, pp. 1–6.

[6] R. Chaban, O. Taran, J. Tutt, Y. Belousov, B. Pulfer, T. Holotyak, and S. Voloshynovskiy, "Printing variability of copy detection patterns," in *2022 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2022, pp. 1–6.

[7] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[8] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.

[9] T. Holotyak, S. Voloshynovskiy, O. Koval, and F. Beekhof, "Fast physical object identification based on unclonable features and soft fingerprinting," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 1713–1716.

[10] B. Pulfer, Y. Belousov, J. Tutt, R. Chaban, O. Taran, T. Holotyak, and S. Voloshynovskiy, "Anomaly localization for copy detection patterns through print estimations," in *2022 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2022, pp. 1–6.

[11] O. Taran, S. Bonev, T. Holotyak, and S. Voloshynovskiy, "Adversarial detection of counterfeited printable graphical codes: towards "adversarial games" in physical world," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020.

[12] R. Chaban and S. Voloshynovskyy, "Research data snf it-dis: Information-theoretic analysis of deep identification systems," Jun 2023.

[13] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[14] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, pp. 91–110, 2004.

[15] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 Eighth IEEE International Conference on Data Mining*, 2008, pp. 413–422.

[16] J. Tutt, O. Taran, R. Chaban, B. Pulfer, Y. Belousov, T. Holotyak, and S. Voloshynovskiy, "Authentication of copy detection patterns: A pattern reliability based approach," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3124–3134, 2024.

[17] Y. Belousov, G. Quétant, B. Pulfer, R. Chaban, J. Tutt, O. Taran, T. Holotyak, and S. Voloshynovskiy, "A machine learning-based digital twin for anti-counterfeiting applications with copy detection patterns," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3395–3408, 2024.