Journal of Intelligent Manufacturing
https://doi.org/10.1007/s10845-026-02864-w

Cold spray-based secure and unique product identification with neural encoding: A full-stack framework for scalable authentication in manufacturing

Hojun Lee[1] · Changheon Han[1] · Ted Gabor[1] · Yuseop Sim[1] · Semih Akin[2] · Martin B.G. Jun[1] · Yongho Jeon[3] · Jiho Lee[1,4]

Received: 17 August 2025 / Accepted: 26 March 2026

Abstract

Constructing an effective and scalable anti-counterfeiting system against cyber-physical attacks has become an increasingly crucial problem. While mass production and digitalization across many domains profoundly transformed our society with an abundance of goods and hyper-connectivity, they have also made it harder to track products and associated information, thereby raising authentication risks. In response to such risks, leveraging random physical traces that are generated as byproducts in manufacturing processes has gained great attention as a robust and efficient replacement for existing approaches. Yet, as current methods of generating such inherently unique patterns rely on complex process setups and specific materials, they face significant limitations to be applied and scaled up as a product authentication system in various manufacturing industries. To address this issue, we propose a Physically Unclonable Identifier (PUID) that exploits the inherent randomness and process characteristics of Pulsed Cold Spray (PCS) to fabricate a unique physical identifier. In addition, we develop a complementary framework that leverages the resulting spectral features for reliable product identification. Specifically, our framework utilizes Implicit Neural Representations (INRs) and Fast Fourier Transform (FFT)-based cross-correlation as key strategies to create, register, manage, and authenticate PUIDs. Through experiments, we validate the robustness, applicability, and scalability of our approach by rapidly generating 54 PUIDs on an arbitrary substrate and successfully authenticating each one. These results highlight the significant potential of PUIDs for deployment across various industries.

Keywords Cold spray deposition · Product authentication · Implicit neural representation (INR) · Intelligent manufacturing application

✉ Semih Akin
akins@rpi.edu

✉ Yongho Jeon
princaps@ajou.ac.kr

✉ Jiho Lee
jiho.lee@unt.edu

Hojun Lee
lee1764@purdue.edu

Changheon Han
han711@purdue.edu

Ted Gabor
tgabor@purdue.edu

Yuseop Sim
sim46@purdue.edu

Martin B.G. Jun
mbgjun@purdue.edu

[1] School of Mechanical Engineering, Purdue University, 610 Purdue Mall, West Lafayette 47906, IN, USA

[2] Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute, 110 8th St, Troy 12180, NY, USA

[3] Department of Mechanical Engineering, Ajou University, 206, World cup-ro, Yeongtong-gu, Suwon 16499, Republic of Korea

[4] Department of Mechanical Engineering, University of North Texas, 1155 Union Circle, Denton 76205, TX, USA

Published online: 13 April 2026

Introduction

Preserving authenticity has been a long-standing problem since humanity began to produce and trade products. With the emergence of various electronics, digital, and manufacturing technologies, authentication has become an even more critical aspect in many different fields and applications these days as many products we consume depend on not only complicated hardware but also highly connective digital sub-components which are more vulnerable against malicious attacks (Wang et al., 2018; Elhabashy et al., 2019). As alternatives to address concerns associated with the problem, Physically Unclonable Function (PUF) that exploits inherent randomness and uncertainty during manufacturing processes (i.e., manufacturing process variation) to generate a unique physical fingerprint has gained great attention in the fields of digital security and authentication (Gao et al., 2020). When integrated with digitalized manufacturing systems, this technology can synergistically enhance security, traceability, and trust across industrial ecosystems, addressing critical vulnerabilities in Industry 4.0/5.0 (Wu et al., 2019). Notably, embedding unclonable identifiers directly into digital manufacturing workflows can provide a robust foundation for tamper-evident production and resilient supply chains in increasingly automated and interconnected industrial environments.

Traditionally, such fingerprint has been produced as a byproduct of uncontrollable deviations in semiconductor chip manufacturing processes (Maiti et al., 2011) and collected as a cost-effective unique identifier. Recently, researchers have been exploring other approaches by randomly placing nanomaterials like carbon nanotubes to introduce a distinctive electrical characteristic, which can potentially be utilized for electronic identification (Moon et al., 2019). However, majority of these approaches is unfortunately limited to electronic components and difficult to extend to other non-electronic components. Moreover, they often rely on multiple specialized processing steps in controlled environments, which is a great hurdle to satisfy scalability that manufacturing industries often require.

To tackle such a limitation in existing approaches, there have been multiple different attempts to generate PUFs on non-electronic goods for their anti-counterfeiting and authentication (Sandborn et al., 2021). As one representative example, optical PUF utilizes randomly distributed scattering particles in a transparent material to create a unique speckle pattern when a laser beam is projected onto it, making it nearly impossible to replicate (Sun et al., 2023; Murataj et al., 2024; Veinidis et al., 2025; Sandomirskii et al., 2025). These methods specifically leverage laser systems to enable the creation of unique patterns or characteristics for the authentication of non-electronic products. Yet, implementing the laser-based processes to fabricate the patterns requires precise setups involving components such as lenses, mirrors, pinholes, and diffusers, which is a big obstacle in integrating it into actual product manufacturing stages. Furthermore, no framework has been proposed to continuously manage the generated physical fingerprint as unique product identifiers (IDs).

In this work, we present a novel approach utilizing the Pulsed Cold Spray (PCS) process to efficiently form a Physically Unclonable Identifier (PUID) — a unique pattern that can be applied on many different product surfaces. In general, Cold Spray (CS) is a solid-state coating technique that propels microscale (5–50 μm) powders at high velocities (300-1200 m/s) onto a surface, where they bond through plastic deformation (Gabor et al., 2025). The process having various applications such as repairment and restoration of damaged engineering components has innate variability and uncertainty in the powder distribution even under identical process conditions (Akin et al., 2023; Yin et al., 2018). While the nature of this additive manufacturing (AM) technique often requires skilled operators to control process parameters for dense and high-quality coverage of substrates, we leverage its disadvantage as a process to obtain physically unclonable product IDs analogous to biometrics like a human iris.

While inspired by conventional PUFs, PUID significantly differs from the spin-offs of other manufacturing processes by enabling intentional pattern fabrication via surface deposition. Furthermore, our approach is applicable to a wide range of non-electronic products as well as electronic components, offering new possibilities for security tagging and anti-counterfeiting across various domains. As such, beyond the concept of PUID and its implementation, we establish a complete end-to-end framework (i.e., full-stack) that systematically captures these unique powder patterns and enable for their registration, management, and verification through an Artificial Intelligence (AI)-based digital encoding system. Notably, since AM is broadly used for high-value, low-volume components in critical sectors (e.g., aerospace (Vaz et al., 2025), defense (Joint Defense Manufacturing Council, 2021), nuclear energy (Wong & Fu, 2025)), our PUID scheme offers surface-level digital labeling to help mitigate counterfeiting, improve traceability, and protect against cyberattacks (Shi et al., 2023). Particularly, in increasingly automated and interconnected manufacturing environments, embedding physically unclonable identifiers directly into AM surfaces provides a practical path toward secure and tamper-evident production. In summary, the primary contributions of this paper are as follows:

1. PUID: a novel PCS-enabled physically unclonable pattern that can be easily fabricated on various surfaces.

2. A full framework comprised of physical and software systems to create PUIDs on surfaces and utilize them as unique characteristics for diverse authentication applications including anti-counterfeiting of products.
3. An evaluation of the proposed framework with regard to performance of the authentication process and feasibility of the digital encoding system.

The remainder of this paper is organized as follows. Section Methods details a PUID and our novel framework. A thorough analysis of the entire framework is presented in Section Evaluation, and further discussions regarding its capabilities and future extensions are covered in Section Discussion. Finally, concluding remarks are given in Section Conclusion.

Methods

Figure 1 illustrates the entire pipeline including generation, identification, and encoding of PUIDs. As visualized in Fig. 1, our framework consists of PUID acquisition and downstream tasks for product authentication applications. As the first part of the framework, we propose a method using a PCS system to deposit metal powders on substrates, creating PUIDs with unique spray patterns. For pattern identification, we formulate the problem as template matching and suggest a simple yet effective sensor-algorithm combination. Lastly, our framework includes a hybrid pattern encoding method to enhance the unclonability of PUIDs in a dedicated digital space.

PUID generation

The unclonability and uniqueness of PUID is derived from the random and sparse deposition of the as-cold sprayed particles on a target surface. For this reason, it is crucial to control the activation time on the PCS setting for the successful generation of PUID. If the activation time is too long, the particles become clustered, causing an unclear particle distribution. Conversely, if the activation time is too short, the possible variations in the particle distribution become much simpler. To address this, we regulate the opening and closing intervals of the spray nozzle, allowing the sparse deposition of particles to form a unique pattern in each attempt.

Figure 1a presents the setup and schematic of the PCS system. We assembled it to control its operation and interval timing when generating the PCS patterns. In more details, a solenoid valve (T35361647, ASCO) with an operational range of 1.3 MPa controls PCS operation. To interface the solenoid valve with the Transistor-Transistor Logic (TTL) level of a microcontroller, a relay (F-1022, OONO) was integrated into the system. Upon a momentary switch input, the microcontroller (Arduino UNO R3, Arduino) activates the relay via General-Purpose Input/Output (GPIO) for a duration of 200 ms.

During an open state of the solenoid valve, a high-pressure gas (air or nitrogen with 0.7-1.3 MPa operational range at room temperature) accelerates metallic particles to supersonic velocities. The powders propelled at high kinetic energies impact the substrate, facilitating adherent bonding (deposition). For the first substrate used for PUID fabrication, an aluminum plate (Al) with a thickness of 0.635 mm was selected. To enhance the visibility of random patterns on the substrate, copper (Cu) powder with a diameter range of 5-44 μm and a median of 36 μm was deposited on Al substrates. To generate a sparse pattern, an appropriate combination of standoff distance and nozzle pressure should be identified. In this context, building on our previous work, we set the air pressure to 1.2 MPa and the stand-off distance (i.e., the gap between the nozzle and Al substrate) to 20 mm (Han et al., 2025). This setting allows us to produce PCS patterns that are highly sparse, as only a small amount of Cu powders is able to reach critical velocity.

As summarized in Fig. 1b, we also examined different relay activation time conditions to create distinguishable individual particle arrangements. Compared to the long-duration activation spray pattern highlighted in red, the sparse spray pattern highlighted in blue demonstrates that the particle distribution can vary significantly in each attempt. Notably, a wide range of powder–substrate combinations (e.g., pure metals, polymers, composites) can be employed to fabricate such random patterns owing to the intrinsic characteristics of the PCS process. Accordingly, to evaluate the material versatility of our approach, similar patterns were also fabricated using different material systems: Polyethylene Terephthalate (PET) as the polymer substrate and tin (Sn) powders with a particle size range comparable to that of the Cu powder as the feedstock powder for the CS process. The air pressure was lowered down 0.7 MPa, while varying the stand-off distance (20–40 mm) for PET-Sn material system. Representative PCS patterns produced using the experimental setup shown in Fig. 1a are presented in Fig. 2.

To verify whether this characteristic can be leveraged to fabricate novel unique patterns, we also performed Computational Fluid Dynamics (CFD) simulations, as shown in Fig. 3. In particular, all parameters and conditions in the CFD simulation were set to be similar to those of the real particle deposition so that we can evaluate the performance of particle distributions. The Detached Eddy Simulation (DES) (Spalart, 2009) with the Shear Stress Transport (SST) k-omega turbulence model (Peng & Eliasson, 2007) captures the characteristics of the supersonic flow, while the Discrete Phase Model (DPM) (Gabor et al., 2024) simulates the behavior of spherical Cu particles injected at a flow rate of 0.00015

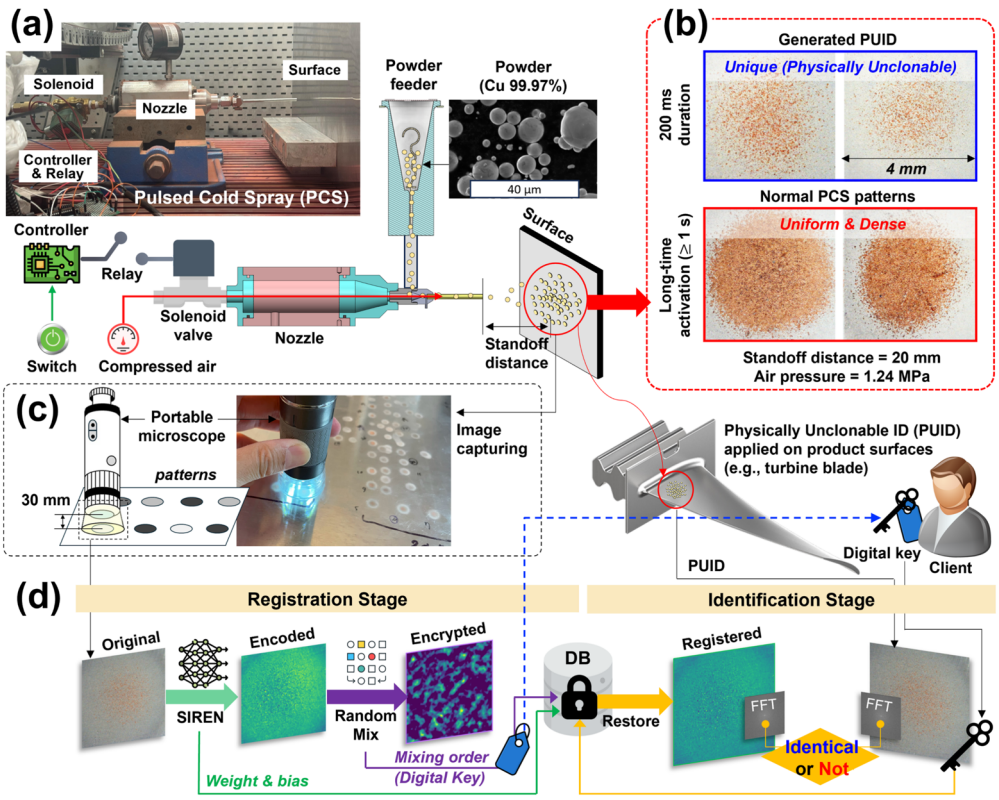

Fig. 1 Overall process flow of PUID framework: (a) System setup and schematic of our PCS system. On top of a conventional CS system consisted of a compressor, nozzle, and powder feeder, the PCS includes a solenoid valve and microcontroller to provide a pulsed gas flow for PUID fabrication. (b) Comparison between normal PCS patterns and PUIDs. While the uniform and dense deposition of particles is preferable for normal use cases such as surface repairment and restoration, we deliberately tweak parameters to obtain their sparse deposition, which enables fabrication of much more distinguishable and unpredictable pattern. (c) Capturing system of PUID on a product surface. For simplicity, a portable microscope with a built-in light source is used to consistently take an image of PUID for further digital processing such as registration of PUID in a database and verification. (d) The entire authentication algorithm of PUIDs. To register a particular PUID in a database, its template image is overfitted in SIREN model, which returns weights and biases of the neural network as an implicit representation of the image. Afterwards, we mix the weights and biases in random order and store it in a database, while the mixing order is only provided to an owner as a key of the PUID. During the identification stage, the owner must provide the key to properly retrieve the PUID template image in a database for identity verification using FFT phase correlation.

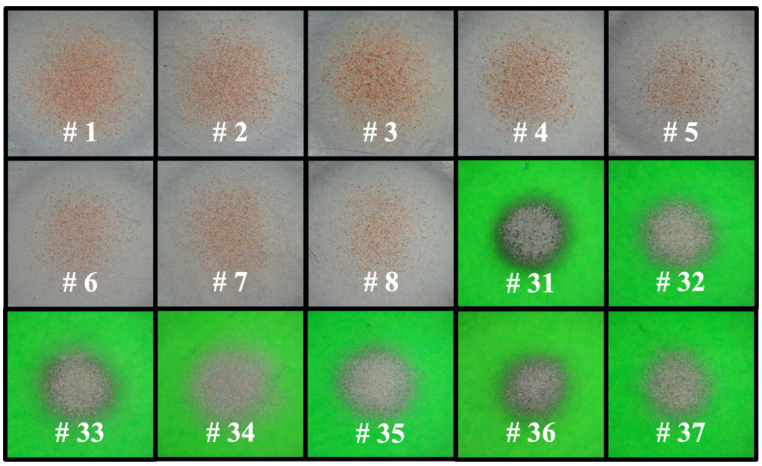

Fig. 2 Example PCS patterns physically fabricated on Aluminum (Al) and Polyethylene Terephthalate (PET) substrates using copper (Cu) and tin (Sn) powders: A unique number is assigned to each PCS pattern based on the order of their fabrication. Note that we generate all 54 patterns using the experimental setup shown in Fig. 1a.

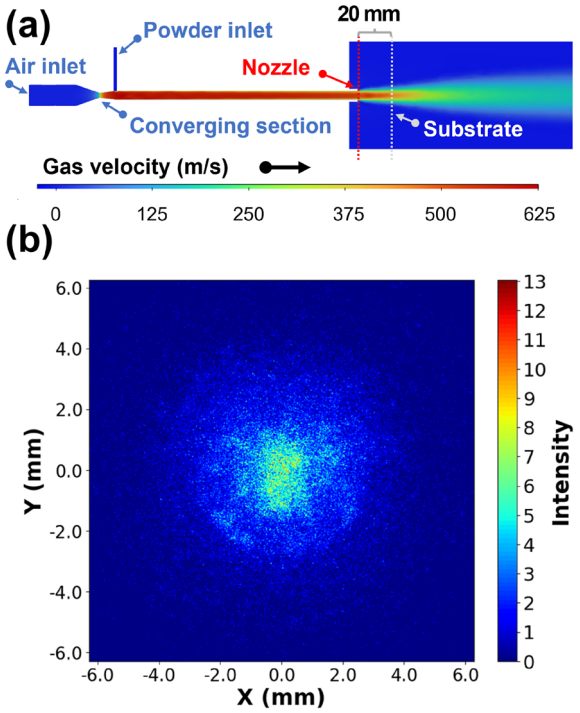

Fig. 3 CFD simulation results of the PCS setup: (a) Gas (air) velocity profile along the X-direction. After the converging section, the air velocity accelerates to supersonic speeds, causing a pressure drop below atmospheric levels. This drop creates a vacuum effect at the powder inlet, drawing the feed powder in at ambient pressure. (b) CFD simulation result of powder particle distribution on the substrate. The simulation based on our process parameters results in sparse particle deposition around the center, just like PUIDs in Fig. 1b.

kg/s. In this simulation, the particles occupy an average of 48,442 nodes within a 512 × 512 pixel cross-sectional area at the stand-off distance of 20 mm.

To quantify the number of possible particle configurations, we calculated the binomial coefficient C representing the number of ways to choose k out of n objects, as shown in Equation 1:

$$C(n,k) = \frac{n!}{k!(n-k)!} \tag{1}$$

where n and k are set as 512 × 512 and 48,442 respectively. This calculation demonstrates that over $10^{54,482}$ patterns of unique PUID far exceed the security strength of existing encryption systems (Barker, 2018). Thus, the PUID is guaranteed to securely generate unique cases.

The PCS system can achieve high productivity of creating PUIDs with a short process time of around 200 ms. Moreover, the particular CS process is versatile enough to be applied to surfaces made of various materials such as metals and polymers (Akin et al., 2023). Consequently, cryptographic pattern generation using our method is a novel technology applicable to industrial settings.

As the final step in PUID generation, we utilized a portable low-cost microscope (4K WiFi Microscope, Jiusion) to capture an image of the Al surface with as-deposited Cu particles and digitize the analog PUID. As shown in Fig. 1c, the distance between each PUID and a lens of the microscope was fixed to 30 mm, and the lighting source was set to constant brightness throughout the process. Note that the captured images were cropped, normalized, and resized to a resolution of 512 × 512 pixels so that their unique patterns can be more emphasized.

PUID identification

Since the unpredictable powder pattern is the key that ensures unclonability of PUID, it is important to utilize this information for authentication. Hence, we formulate the pattern verification as a template-matching problem similar to existing methods for biometrics (Daugman, 2009; Ali et al., 2016), where an input image $\boldsymbol{I}_\alpha(u,v) : \mathbb{Z}^2_{\geq 0} \in [0, 255]$ is compared with a stored template image $\boldsymbol{I}_\beta(u,v) : \mathbb{Z}^2_{\geq 0} \in [0, 255]$ to check for similarity or matching components. Among many different template matching techniques such as analytical feature descriptors (Lowe, 1999; Bay & Tuytelaars, 2006; Rublee et al., 2011) and Machine Learning (ML)- or Deep Learning (DL)-based embedding (Abdi & Williams, 2010; Chen et al., 2020; Khosla et al., 2020), Fast Fourier Transform (FFT) phase correlation (Kuglin, 1975) is used to verify if $\boldsymbol{I}_\alpha$ and $\boldsymbol{I}_\beta$ are identical.

Unlike many other image data produced by human activities, PUIDs themselves do not have much semantic. As shown in Fig. 4, the patterns produced by CS almost look like salt and pepper noise in the grayscale images and do not have clear separations from metal surfaces, on which they are deposited. Due to these characteristics, PUIDs are adversarial to widely used local feature-based algorithms such as Scale-Invariant Feature Transform (SIFT) (Lowe, 1999), Speeded-Up Robust Features (SURF) (Bay & Tuytelaars, 2006), and Oriented FAST and Rotated BRIEF (ORB) (Rublee et al., 2011). While this kind of methods often relies on local key-points and their associated feature descriptors, the severe noise-like patterns contain unclear local extrema and gradients. For ML- and DL-counterparts of the core analytical feature-based algorithms (Xu et al., 2024), the situation is even worse due to the uniqueness of the PUIDs, which makes challenging to gather good amount of data and build effective feature embedding for the functionality of the PUIDs as unique IDs. Given that the uniqueness of each PUID comes from idiosyncratic distributions of sprayed particles, it is very important to capture such overall distribution patterns for verification, rather than focusing on local

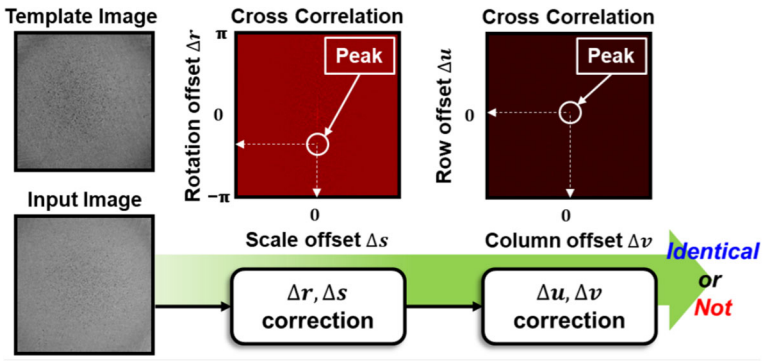

Fig. 4 Intermediate steps in FFT phase correlation-based template matching: After representing the input and template images I_α, I_β in log-polar coordinates, a cross-correlation of them is computed by applying inverse 2D Fourier transform $\mathcal{F}^{-1}$ on their normalized Cross Power Spectrum (CPS). Using a peak with the highest intensity in the cross-correlation map, rotational and scale offsets $\Delta r \in \mathbb{R}$, $\Delta s \in \mathbb{R}^+$ are estimated to transform I_α. The rotated and scaled I_α in cartesian coordinates goes through the same procedure to estimate a 2D translative offset $\Delta u \in [-u_{max}, u_{max}]$, $\Delta v \in [-v_{max}, v_{max}]$.

information. Compared to the analytical and learning-based matching algorithms, FFT phase correlation is identified as more suitable in this sense since it considers the overall phase relationship of all frequency components in the two images.

In details, FFT phase correlation is a method to estimate the relative 2D translative offset $\Delta u \in [-u_{max}, u_{max}]$, $\Delta v \in [-v_{max}, v_{max}]$ between I_α and I_β using their frequency domain representations. Based on shift theorem of the Fourier transform, we can express the relationship of I_α and I_β as following:

$$I_\alpha = I_\beta(u + \Delta u, v + \Delta v) \tag{2}$$

$$\mathcal{F}\{I_\alpha(u, v)\} = e^{-j2\pi\theta}\mathcal{F}\{I_\beta(u, v)\} \tag{3}$$

where $\mathcal{F}$ is 2D Fourier transform and $e^{-j2\pi\theta}$ (i.e., a shifted Dirac delta function) denote a phase shift between I_α and I_β in the frequency domain. To obtain the specific values of Δu and Δv, inverse 2D Fourier transform $\mathcal{F}^{-1}$ has to be applied after computing $e^{-j2\pi\theta}$ using the normalized Cross Power Spectrum (CPS):

$$e^{-j2\pi\theta} = \frac{\mathcal{F}\{I_\alpha(u, v)\} \circ \mathcal{F}^*\{I_\beta(u, v)\}}{|\mathcal{F}\{I_\alpha(u, v)\} \circ \mathcal{F}^*\{I_\beta(u, v)\}|} \tag{4}$$

$$(\Delta u, \Delta v) = \underset{(u,v)}{\text{argmax}}\{\mathcal{F}^{-1}\{e^{-j2\pi\theta}\}\} \tag{5}$$

where $\mathcal{F}^*$ represents the complex conjugate of $\mathcal{F}$ and $\circ$ is the Hadamard product. As described in Eq. 4 and Eq. 5, FFT phase correlation provides not only the estimation of Δu and Δv but also the intensity of the phase correlation between $I_\alpha(u, v)$ and $I_\beta(u, v)$, which is utilized as a similarity score of the template-matching in our method.

To estimate rotation and scale variations between $I_\alpha(u, v)$ and $I_\beta(u, v)$, we apply log-polar transform on the original two images. Their rotation $\Delta r \in \mathbb{R}$ and scaling $\Delta s \in \mathbb{R}^+$ in the original coordinate system (u, v) can be represented as linear shifts in an angular rotation and a radial direction. Afterwards, phase correlation is particularly applied on magnitude spectrum of $\mathcal{F}\{I_\alpha(r, s)\}$ and $\mathcal{F}\{I_\beta(r, s)\}$ to compute Δr and Δs since the magnitude of FFT is translation-invariant. In other words, by sequentially applying FFT phase correlation in the log-polar coordinate and the original coordinate system as outlined in Fig. 4, it is possible to verify same PUIDs in different translations, rotations, and scales.

PUID encoding

Since cold spraying involves acceleration of solid powders to a supersonic turbulent regime and collision on a substrate for their adherence, the physical patterns generated by the process are indeed unique and unclonable. Nevertheless, digitalized image templates of PUIDs I_β that we use for storage and authentication can be stolen and replicated, which potentially undermines unclonability of actual PUIDs on a substrate in many different applications. Therefore, it is necessary to encode the visual data in a safer format before storing them in a database. While there are several different classical techniques for image encoding via pixel permutation and diffusion (Kumari & Gupta, 2017), DNNs have been recently gaining more attention in some image encoding schemes thanks to their generalizability, non-linearity, and stochasticity during training processes (Lian et al., 2004; Meraouche et al., 2021; Rohhila & Singh, 2024). Most of

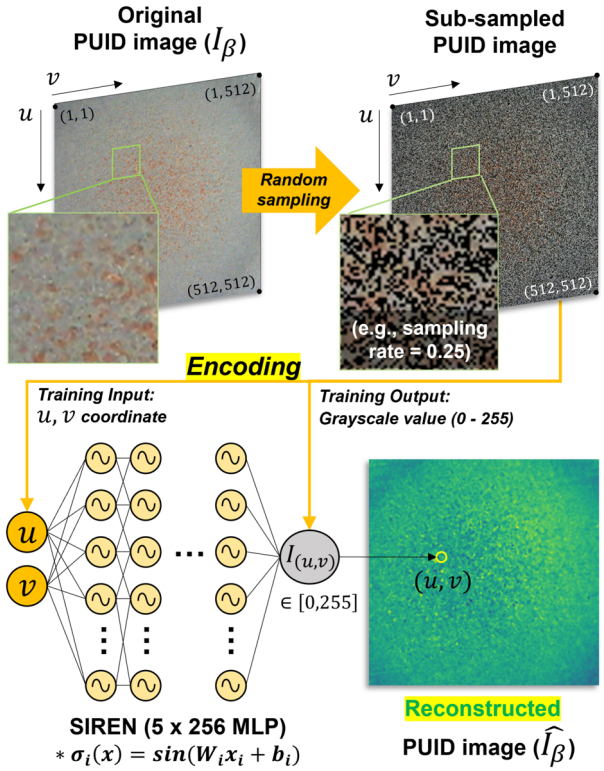

Fig. 5 Visualization of SIREN architecture and its training process: Unlike conventional NNs using non-periodic activation functions, SIREN adopts sine activation functions to add non-linearity throughout the five linear layers with 256 nodes. To overfit a PUID and create its INR, SIREN randomly sub-samples pixel coordinates and their grayscale values ($0 \sim 255$) in $\boldsymbol{I_\beta}$ as its training data and label pairs, respectively. Note that the sampling ratio is a crucial hyperparameter of SIREN to optimize quality of the reconstruction.

these methods utilize either (i) generative models like GAN as pseudo-random sequence generators for scrambling original images (Ding et al., 2021) or (ii) parameters of embedding Neural Networks (NNs) as secret keys for image encoding (Dong et al., 2024). In this work, on the other hand, we propose a two-stage approach that combines (ii) and a classical permutation technique for encoding $\boldsymbol{I_\beta}$ in a safer format. Importantly, this approach generates an encoding-related key for each step (i.e., dual encoding), and both keys are required to properly restore $\boldsymbol{I_\beta}$.

As visualized in Fig. 1d, our framework first converts each $\boldsymbol{I_\beta}$ to Implicit Neural Representations (INRs). INRs using weights $\boldsymbol{W}$ and biases $\boldsymbol{b}$ of NNs to approximate diverse signals have some relationships with attempts using NNs to solve complex differential equations like wave equations (Lagaris et al., 1998; Chen et al., 2018). Among many different approaches to form INRs, we leverage SIREN (Sitzmann et al., 2020) that shows a theoretical connection with $\boldsymbol{d}$ – dimensional Fourier series (Benbarka et al., 2022). As described in Fig. 5, SIREN is composed with linear layers, sine activation functions, and a tuned parameter initialization strategy to achieve INRs using its $\boldsymbol{W}$ and $\boldsymbol{b}$:

$$\begin{aligned} \boldsymbol{\Phi(x) = W_k(\phi_{n-1} \circ \phi_{n-2} \circ \cdots \phi_0) + b_k} \\ \boldsymbol{\phi_i(x) = sin(W_i x_i + b_i)} \end{aligned} \tag{6}$$

where $\boldsymbol{\phi_i} : \mathbb{R}^{M_i} \rightarrow \mathbb{R}^{N_i}$ is the $\boldsymbol{i^{th}}$ layer of SIREN applied on the input $\boldsymbol{x_i} \in \mathbb{R}^{M_i}$. Note that $\boldsymbol{W_i} \in \mathbb{R}^{M_i \times N_i}$ and $\boldsymbol{b_i} \in \mathbb{R}^{N_i}$ are the weight matrix and biases of the $\boldsymbol{i^{th}}$ layer while $\boldsymbol{k}$ is the total number of layers in SIREN and $\circ$ is the Hadamard product. To define a digital image in a high-dimensional parameter space of an NN, Sitzmann et al. (2020) overfits each image to an individual SIREN, providing pixel coordinates of each image as inputs and corresponding gray-scale values as outputs (i.e., coordinate-based NN).

From signal processing perspective, salt and pepper noise-like CS patterns that assure uniqueness and unclonability of PUIDs particularly enforce effective reconstruction of high spatial frequency components when transforming $\boldsymbol{I_\beta}$ into INRs. Even if oscillatory nature of sine activation functions in SIREN provides much better capability to model both low and high frequency signals than other piecewise linear activation such as ReLU and Leaky ReLU, we often encounter poor implicit representation of PUIDs due to underfitting when training SIREN with default settings. Thus, while Sitzmann et al. (2020) samples only 10% of all pixels from each test image data to efficiently generate corresponding INRs, we increase the sampling ratio to collect more pixel points during training so that SIREN can handle not only high frequency components but also high amplitude variations when encoding $\boldsymbol{I_\beta}$. After training processes of SIRENs is completed, W and b of each NN are served as the intermediate stage representation that requires an empty SIREN architecture with the specific number of nodes and layers to reconstruct each $\boldsymbol{I_\beta}$. In details, we simply have to provide pairs of $\boldsymbol{u}$ and $\boldsymbol{v}$ and reshape the outputs when reconstructing the PUID back to the image format.

After collecting W and b that represent each PUID, we stack all $\boldsymbol{W_i} \in \mathbb{R}^{M_i \times N_i}$ with $\boldsymbol{b_i} \in \mathbb{R}^{N_i}$ in the $\boldsymbol{i^{th}}$ layer and rearrange orders of all the parameters in an individual SIREN using a simple random sequence generator. Afterwards, the stacked parameters are flattened to remove any node- and layer-specific information, which become the final stage representation of a PUID image template stored in a database $\widetilde{\boldsymbol{I_\beta}} \in \mathbb{R}^{\Sigma_{i=1}^{k}(M_i+1)N_i}$. In other words, all specifications of an NN including $\boldsymbol{M_i}$ and $\boldsymbol{N_i}$ in the $\boldsymbol{i^{th}}$ layer, mixing orders of all the parameters $\boldsymbol{\delta}$, and $\widetilde{\boldsymbol{I_\beta}}$ are required to restore the original PUID image template $\boldsymbol{I_\beta}$. Note that information about $\boldsymbol{M_i}$, $\boldsymbol{N_i}$, and $\boldsymbol{\delta}$ used for mixing $\boldsymbol{W}$ and $\boldsymbol{b}$ can be also encrypted and saved in a different location for better safety. As summarized in Fig. 1d, missing any of the information can lead to failures in the restoration process. Accordingly, $\boldsymbol{M_i}$, $\boldsymbol{N_i}$, and $\boldsymbol{\delta}$ can be provided to a user as a key of each PUID on a product so that

the person can properly retrieve and decode a corresponding $\widetilde{\boldsymbol{I}}_{\boldsymbol{\beta}}$ in a database for authentication.

Evaluation

To analyze how well each PUID can be encoded and identified using SIREN and FFT phase correlation, we prepared a total of 54 unique PUIDs using our PCS system and its parameter setup described in Section PUID generation. After collecting all of the PUIDs on Al and PET substrates, four images were captured for each PUID sample using the portable low-cost microscope as shown in Fig. 1c. When preparing all 4 × 54 (i.e., 216) PUID image samples, we exactly followed the procedure mentioned in the last paragraph of Section PUID generation. After collecting and pre-processing the image samples, we randomly chose one of four images for each unique PUID sample and set it as an identification template. These 54 raw identification templates were encoded using our proposed approach. During experiments, two different authentications were initially performed by comparing the entire set of 216 PUID images with (A) the raw and (B) encoded identification templates. Note that in the case of (B), we decoded stored data to reconstruct the templates and ran FFT phase correlation for the assessments. Next, force and alcohol were deliberately applied on two randomly selected PUIDs to test their durability and robustness against potential physical damages. Specifically, we repeatably tapped two PUIDs and peeled them off 100 times, followed by 100 times rubbing of the patterns using alcohol swabs.

Identification performance on raw patterns

Before testing how well our full pipeline works on different PUIDs, we initially used their unencoded raw image templates $\boldsymbol{I}_{\beta}$ to compare performance of FFT phase correlation with those of three analytical feature descriptors, three learning-based models (ML + DL), and two other FFT-based methods (Tadmor & Tolhurst, 1993; Vurpillot et al., 2004):

- Analytical Feature Descriptor - SIFT, SURF, and ORB
- Learning-based Embedding - PCA (Abdi & Williams, 2010), SimCLR (Chen et al., 2020), and SupCon (Khosla et al., 2020)
- FFT-based method - Power Spectrum Matching (PSM) (Tadmor & Tolhurst, 1993) and Auto-Correlation (AC) (Vurpillot et al., 2004)

All verification algorithms were fine-tuned in different ways since each of them operates in a different vector space. For FFT phase correlation, as mentioned before, a single threshold value was set up based on intensity of a peak in the 2nd cross-correlation map for estimating $\Delta \boldsymbol{u}$ and $\Delta \boldsymbol{v}$. Similarly, PSM and AC also required to specify their threshold for comparing power spectrum and AC of $\boldsymbol{I}_{\alpha}$ and $\boldsymbol{I}_{\beta}$. In the case of SIFT, SURF, and ORB, we checked whether there was any projective distortion after correspondences are established between $\boldsymbol{I}_{\alpha}$ and $\boldsymbol{I}_{\beta}$. To do so, a homography matrix $\boldsymbol{H} \in \mathbb{R}^{3\times3}$ was first calculated using the correspondences to obtain a determinant of its upper half 2 × 2 sub-matrix ϵ. Then, we selected a single threshold value, considering that the value of ϵ is close to 1 when a homography transformation is close to pure rotation and translation. In the case of PCA, we simply passed the embedding of $\boldsymbol{I}_{\alpha}$ and $\boldsymbol{I}_{\beta}$ to Support Vector Machine (SVM) (Cortes & Vapnik, 1995) and checked whether they belong to the same class. For SimCLR and SupCon, a pretrained EfficientNet (Tan, 2019) was first adopted as a backbone and fine-tuned the model before building Siamese networks. Afterwards, we trained a simple binary classifier that processes latent vectors of $\boldsymbol{I}_{\alpha}$ and $\boldsymbol{I}_{\beta}$ for verification. Since we chose a single $\boldsymbol{I}_{\beta}$ for 54 individual PUID and matched with all the 216 PUID images, the total number of comparisons was 11664. Among all the cases, we should ideally get 216 True Positives ($\boldsymbol{TP}$s) and 11448 True Negatives ($\boldsymbol{TN}$s).

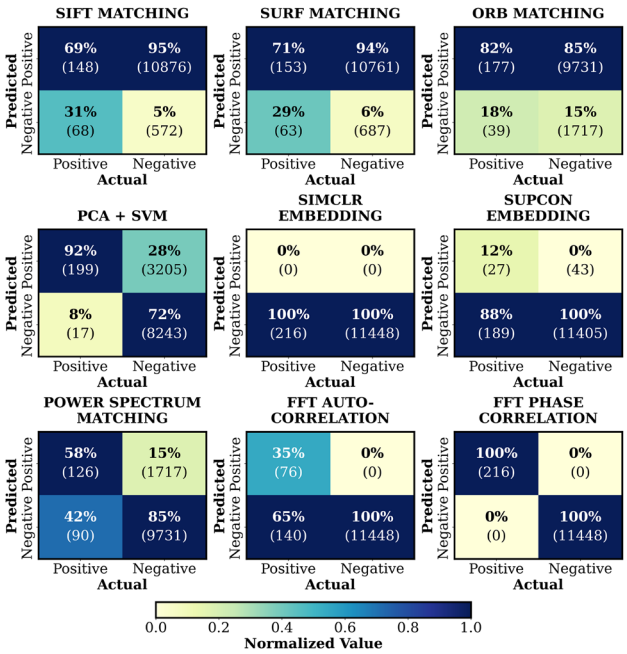

Fig. 6 2 by 2 confusion matrices $\boldsymbol{C}(i, j)$ of the six different template matching-based identifications: Since we choose one $\boldsymbol{I}_{\beta}$ for 54 distinctive PUIDs and compare them with all 4 × 54 PUID images with different camera rotations and translations $\boldsymbol{I}_{\alpha}$, each algorithm should ideally have 216 and 11448 in $\boldsymbol{C}(1, 1)$ and $\boldsymbol{C}(2, 2)$, respectively.

As visualized in Fig. 6, FFT phase correlation achieved the best verification performance without false positives and false negatives. When comparing the three local feature

descriptor-based matching algorithms with our framework, they generated a lot of False Positive ($\boldsymbol{TP}$s) cases. In the case of learning-based embedding, SimCLR and SupCon were mostly unable to recognize identical PUIDs, while PCA-based embedding with SVM captured $\boldsymbol{TP}$s much better and achieves more balanced performance. For other two FFT-based methods, PSM captured more $\boldsymbol{TP}$s and less $\boldsymbol{TN}$s than AC. The analysis comparing the different template matching approaches confirms several insights about PUIDs. First, randomness of overall particle distributions is a key element that guarantees uniqueness of each PUID and their verification process, which is supported by the huge performance gaps of SITF, SURF, and ORB from FFT-based methods in general. Note that we analyze and discuss regarding this point more detail in Section Visual comparisons of identification methods. Second, the variation of performance among FFT-based approaches indicates that phase information extracted from $\boldsymbol{I}_\alpha$ and $\boldsymbol{I}_\beta$ are far more distinguishable than magnitude spectra (i.e., PSM and AC). Third, challenges in gathering good amount of data are critical bottlenecks in constructing effective learning-based embedding models. In particular, compared to FFT phase correlation that does the perfect job in PUID identification with no learning, the learning-based methods are not the most efficient options to pinpoint uniqueness of each PUID. Moreover, the more balanced performance of PCA + SVM relative to SimCLR and SupCon further supports that DL-based algorithms suffer more from the scarcity of data, since they have way more parameters to be optimized.

Effects of encoding on identifications

As the second step of the performance assessment, we tested our entire framework including SIREN-based pattern encoding on the 54 PUID samples. Specifically, SIREN was initially trained on the corresponding PUID image templates $\widetilde{\boldsymbol{I}}_\beta$ to generate 54 different pairs of $\boldsymbol{W}$ and $\boldsymbol{b}$, while the encoded data $\boldsymbol{I}_\beta$ were used for template reconstructions whenever a verification process was necessary. Note that the reconstructed images are similar to the original 54 PUID image templates but not exactly the same as they are approximated outputs from SIREN. Nevertheless, as summarized in Fig. 7, FFT phase correlation successfully recognized different PUIDs using the decoded images without any false positive and false negative cases, which proved robustness of the algorithm for PUID authentication. On the contrary, the other eight methods failed to perfectly identify input PUID images $\boldsymbol{I}_\alpha$. Similar to the results tabulated in Fig. 6, all the three feature-based algorithms caused a lot of false positives while ORB showed slightly better performance than SIFT and SURF. In the case of SimCLR, SupCon and AC, outputs of all three approaches were very biased towards non-identical PUIDs. Lastly, PCA + SVM and PSM still maintained nice balance of capturing both $\boldsymbol{TP}$s and $\boldsymbol{TN}$s, although their performance was still incomparable with FFT phase correlation.

As described in Section PUID encoding, we tuned the pixel sampling ratio when training SIREN for our specific application. Increasing this hyperparameter affects not only the quality of the template encoding but also the computational burden during the training process. Hence, we performed a grid search with regard to the pixel sampling ratio and find its optimal value to balance both the encoding performance and computational burden. To do so, we recorded precision, recall, and F1 score along with accuracy of pattern identification:

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP} + \boldsymbol{FP}} \tag{7}$$

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP} + \boldsymbol{FN}} \tag{8}$$

$$\boldsymbol{F1} = 2 \cdot \frac{\boldsymbol{Precision} \cdot \boldsymbol{Recall}}{\boldsymbol{Precision} + \boldsymbol{Recall}} \tag{9}$$

where $\boldsymbol{TP}$, $\boldsymbol{FP}$, and $\boldsymbol{FN}$ represent true positive, false positive, and false negative. Precision in Equation 7 indicates how many of the positively identified instances are actually correct, while Recall in Equation 8 focuses on measuring how well the system detects all actual positive instances. F1-score in Equation 9 is the harmonic means of precision and recall, providing a balance between the two.

As plotted in Fig. 8, pattern identification did not work as intended when lower sampling ratios were used. For example, F1 score and recall values were below 0.7 and 0.5, respectively, when the sampling ratio was set to 0.125 similar to the number presented in Sitzmann et al. (2020). This phenomenon of miss-classifying true positive cases quickly diminished as the ratio was increased. Considering the linear increment of the training time, a sampling ratio of 0.6875 is recommended for the particular application that demands more robust pattern identification.

Robustness against potential damages

As mentioned in the beginning of Section Evaluation, we conducted experiments to evaluate whether PUIDs and their identifications are robust against potential physical damages, such as peeling off or rubbing, and chemical exposure. To do so, 100 times of taping and rubbing tests were sequentially performed on two randomly selected PCS patterns, while the patterns after each step were encoded using SIREN to

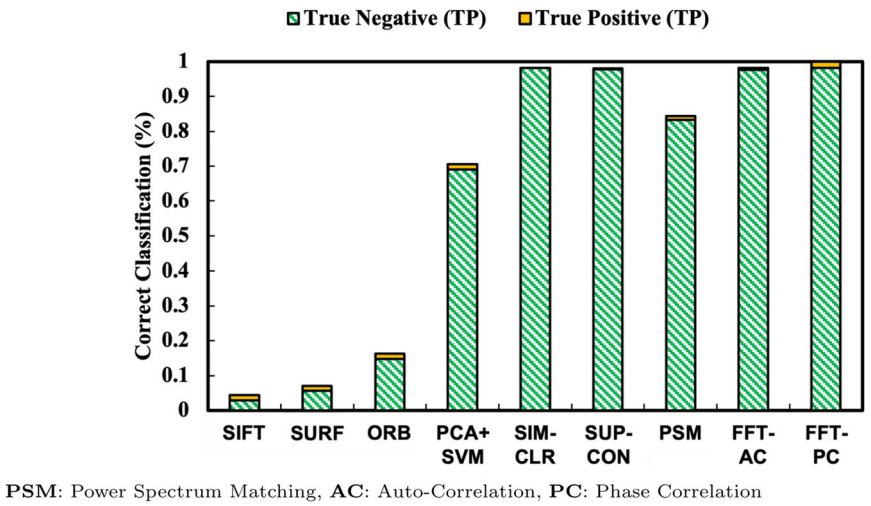

Fig. 7 Performance comparison among the nine different template matching-based identifications after SIREN-based encoding: Even though PUID templates reconstructed from SIREN $\widehat{I}_\beta$ are neural surrogate models of corresponding original images, FFT phase correlation still achieves perfect identification of the 54 PUIDs without any false positive or false negative.

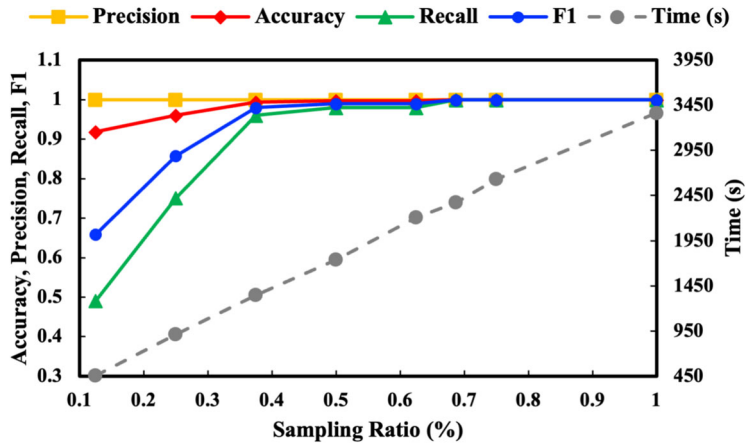

Fig. 8 Variations of identification performance and training time for SIREN-based encoding with respect to pixel sampling ratio: As the sampling ratio of SIREN increases, the training time also linearly goes up while values of all four performance metrics $\in$ **[0, 1]** reach to plateau after the ratio of 0.5.

generate templates $\boldsymbol{I}_\beta$ for comparisons. Fig. 9 summarizes the example variation of a single PCS sample after **step (a)** and **step (b)** with the corresponding confusion matrix and detached powders from the substrate. Noticeable, as shown in the (1,2) of Fig. 9, there were very few detached powders from the substrate after repeatedly attaching and detaching the scotch tape 100 times. On the contrary, there were no obvious falling off of particles in spite of rubbing the surface of the PCS pattern 100 times using alcohol swabs. In consequence, the proposed framework well maintained its identification performance without any $\boldsymbol{FP}$ and $\boldsymbol{FN}$, even under such environmental stressors.

Discussion

We present a novel approach for creating PUIDs via PCS and identifying the different salt and pepper noise-like unclonable patterns. Therefore, in this section, we first provide an additional insight about PUIDs as an identifiable pattern by visualizing how other analytical and learning-based algorithms fail while FFT phase correlation successfully carries out authentications. Then, limitations of the proposed framework are followed with suggested directions for future work.

Visual comparisons of identification methods

To further analyze how the salt and pepper noise-like PCS patterns on substrates affect different verification algorithms, we particularly visualize how feature descriptor- and learning-based approaches work in their respective operational vector space. For SIFT, SURF, and ORB, we double-check correct and incorrect matchings of key-points between a template and an input $\boldsymbol{I}_\alpha$, $\boldsymbol{I}_\beta$ based on the feature descriptors. As depicted in Fig. 10a, the key-points and correspondences (e.g., colored dots and lines) between two images of an identical PUID are inconsistent, which causes confusions during the authentication process. In particular, incorrect feature matchings causes distortions of input images when applying homography matrices on them, which leads to miss-classification of the input and template images from the same PUID. For learning-based methods such as SimCLR and SupCon in Fig. 10b, on the other hand, they mainly focus on center areas of the PUID images instead

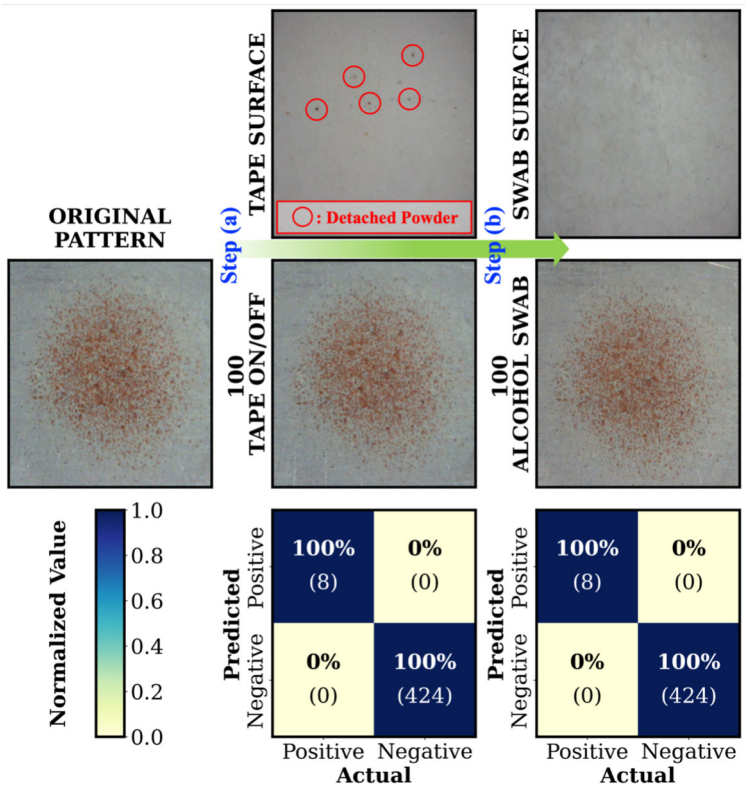

Fig. 9 Performance variation of PUID identifications after **(a)** peeling and **(b)** rubbing tests: To examine the durability and robustness of PUID identifications against potential physical damages, we repeatedly tape and peel off two randomly selected PCS samples, followed by rubbing their surfaces using alcohol swabs. Note that step **(a)** and **(b)** are proceeded subsequently, while PCS samples after 100 times of taping and rubbing are encoded using SIREN. We compare these four encoded templates (2×2) $\boldsymbol{I}_{\beta}$ with the original 216 PUID images (54×4).

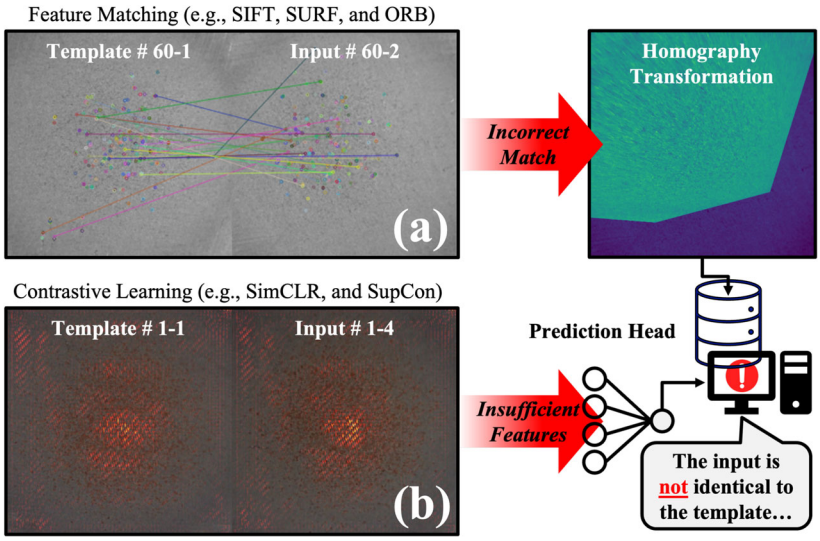

Fig. 10 Visualization of how the different pattern verification algorithms operate and their characteristics: (a) is an incorrect identification (e.g., false negative) case when analytical feature descriptors are used. (b) highlights the areas of the two PUID image samples where learning-based embedding models look at (e.g., center area) for classifications via integrate gradients technique.

of overall patterns created by the powder distributions. Note that, for highlighting the focus areas, we leverage integrated gradients to assign model predictions to their corresponding input features.

Along with their poor performances tabulated in Fig. 6, these visualizations support that both feature-based and learning-based algorithms heavily rely on a smaller portion of the patterns, causing their ineffectiveness in authentication. On the contrary, FFT phase correlation efficiently chooses the best estimate of $\boldsymbol{\Delta u}$ and $\boldsymbol{\Delta v}$, considering the phase information of spatial signals in all frequency ranges. Since the signals are induced from pixel intensity variations, which is directly related to global distribution of powders on substrates, capturing overall spraying patterns indeed crucial for PUID identifications. Note that we do not visualize how PSM and AC operate in their respective domains, since their magnitude spectra are not really interpretable. Furthermore, the results in Section Identification performance on raw patterns and Section Effects of encoding on identifications already

support that the magnitude spectrum is less distinguishable than phase information of PCS patterns.

Comparisons with PUFs

Since PUID utilizes inherent randomness of a specific manufacturing process to fabricate a unique ID, it is worth positioning our approach relative to existing approaches that also start with similar ideas of leveraging stochastic phenomena in various manufacturing processes. Table 1 summarizes representative PUF families and PUID with respect to five deployment-critical factors for manufacturing environments: 1) process complexity, 2) computational complexity, 3) sensing requirements, 4) applicability, and 5) scalability. In general, optical PUFs span a broad spectrum of fabrication processes and sensing technologies. However, their complexity, such as multi-step chemical processing and specialized optical sensing, significantly limits their in-line applicability and throughput (Nocentini et al., 2024; Park et al., 2025; Torun et al., 2021). Although electro-sprayed polymer morphologies in (Esidir et al., 2022) seem to simplify the fabrication of PUF to a single deposition step and allow optical readout, their durability and robustness across heterogeneous substrates remain insufficiently characterized for large-scale deployment. Meanwhile, electronic PUFs, such as FeFET- and memristor-based architectures, achieve strong security with negligible runtime computation (Li et al., 2025), but their reliance on advanced foundry-level fabrication increases their overall cost. In the case of electromagnetic PUFs, they leverage scattering responses or unintended near-field emissions (Ibrahim et al., 2024; Yang et al., 2023) to offer large Challenge-Response Pair (CRP) spaces, while their practical scalability is often challenged by measurement geometry, probe placement repeatability, and environmental sensitivity. Taken together, our approach stands out by offering a scalable and low-cost alternative that preserves high entropy while potentially mitigating these limitations.

Compared to the backdrop in Table 1, PUID occupies a complementary operating point by relying on CS, the well-established industrial process that is relatively low-cost but has never used for the particular purpose. Especially, PCS enables extremely fast fabrication of patterns using various powders and substrates with less than 0.5 sec, since its operation speed mainly depends on opening/closing speeds of the attached solenoid valve. Moreover, the readout of PUID only requires a low-cost microscope camera without specialized optical or spectroscopic instrumentation, while FFT phase correlation supports rapid matching in practical settings (0.07-0.1 sec). The main bottleneck to ensure high scalability of our framework is the one-time SIREN-based encoding that approximately takes 7-9.5 minutes (Fig. 8) and occupies 1 Megabyte ($\times 2$ of original PCS image) in the database per PCS sample. This computational overhead is compensated over repeated use of PUID and does not affect operational throughput, as the decoding of PUID also takes about 1.0 sec. Note that, throughout the computational experiments, we use a workstation with Intel Core i7-11700K CPU, 64GB RAM, and NVIDIA RTX A5000 GPU that is comparable to the modern high-end consumer-grade desktop. In summary, PUID is a versatile and highly applicable approach to fabricate unique IDs on various products, even though its computational complexity could be further improved for real-world applications.

Future extensions for real-world applications

There are several areas which require further research and improvements to make the best out of physical unclonability of PUIDs for real-world applications. Currently, PUIDs are directly exposed on surfaces of products without any covering to utilize the low-cost microscope camera. Even though the combination of PCS, FFT phase correlation, and SIREN-based encoding can mitigate physical spoofing, physical damage, and digital injection (Table 2), there could always be risks at sensor- and system-levels, such as snatching digitized PCS patterns during the sensing stage or directly capturing physical patterns using other cameras. To avoid these unfavorable accidents, it is necessary to consider methods that can physically conceal and protect PUIDs from direct exposure. This extra layer can be also helpful to further increase durability of PUIDs against external forces and chemical reactions. Along with this effort, research on a non-intrusive acquisition, such as electromagnetic or ultrasonic sensors, and associated robust algorithms that can capture and identify distribution of sprayed solid powers underneath the concealment is another appealing future direction of this novel approach. Lastly, there is still large room for improvement of SIREN-based encoding in terms of its size, computational complexity, and its CRP space.

Conclusion

Leveraging the heuristic nature of solid powder acceleration and adhesion in cold spray process - typically considered as manufacturing defect, this study introduced a novel approach to actively produce PUIDs, identify their unique patterns, and digitally encode them for secure storage. Based on the results, the following conclusions can be drawn:

- The PCS system enables the scalable fabrication of unique physical patterns that can be utilized for various applications such as product authentication and information security.

Table 1 Comparison of PUID with other PUF-based approaches in terms of process complexity, computational complexity, type of sensor to detect, applicability, and scalability.

PUFs	PC*	CC*	Sensor	Applicability	Scalability
Optical 1 (Torun et al., 2021)	4 Steps	Low High	Microscope Raman spectrometer	Moderate	Moderate
Optical 2 (Nocentini et al., 2024)	3 Steps	Low	CCD camera	Moderate	Moderate
Optical 3 (Park et al., 2025)	2 Steps	Low	Pulsed laser + Ultrasound transducer	Moderate	Low
Optical 4 (Esidir et al., 2022)	1 Steps	Low	Microscope	High	Moderate
Electronic 1 (Li et al., 2025)	Full Foundry	Low	Voltage comparator	Moderate	Moderate
Electronic 2 (Li et al., 2025b)	Full Foundry	Low	Voltage sensing	Moderate	Moderate
EM* 1 (Yang et al., 2023)	Full Foundry	High	Spectrum analyzer	Moderate	Low
EM* 2 (Ibrahim et al., 2024)	N/A	Low†	Near-field EM* probe	Low	Moderate
PUID (Ours)	1 Step	Low†	Microscope camera	High	Moderate

PC*: Process Complexity, **CC***: Computational Complexity, EM*: Electromagnetic, †: Requires a training stage for encoding

Table 2 Summary of potential attacks and their mitigation by each component of the proposed framework: ◯, △, and ✗ represent the degree of mitigation, from good to ineffective.

	Potential Attacks			
	Physical Spoofing	Physical Damage	Digital Injection	Sensor & System
PCS	◯	△	◯	N/A
FFT PC	◯	△	◯	✗
SIREN	N/A	N/A	◯	△

PC: Phase Correlation

- The noise-like PCS patterns that the system generates can be robustly identified using the FFT-based matching strategy, which allows PUIDs to function as identifiers like biometrics.
- The INR-based encoding only captures the core internal structures of PUIDs and approximates them in a parameter space of NNs, safely digitalizing their unpredictable patterns for effective identifications with 0% false positive and false negative.

Future work will focus on developing concealment methods to enhance the physical unclonability of PUIDs and improve their durability against structural surface damage simultaneously. Additionally, exploring alternative sensing technologies and advanced algorithms offers promising avenues for creating more effective concealed patterns and their cyber-physical safety against various malicious attacks.

Acknowledgements This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2024-00346883).

References

Abdi, H., & Williams, L. J. (2010). Principal component analysis. *Wiley Interdisciplinary Reviews: Computational Statistics, 2*(4), 433–459. https://doi.org/10.1002/wics.101

Akin, S., Nath, C., & Jun, M.B.-G. (2023). Selective surface metallization of 3D-printed polymers by cold-spray-assisted electroless deposition. *ACS Appl. Electron. Mater., 5*(9), 5164–5175. https://doi.org/10.1021/acsaelm.3c00893

Gao, Y., Al-Sarawi, S. F., & Abbott, D. (2020). Physical unclonable functions. *Nature Electronics*, *3*, 81–91. https://doi.org/10.1038/s41928-020-0372-5

Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of Intelligent Manufacturing*, *30*(3), 1111–1123. https://doi.org/10.1007/s10845-017-1315-5

Maiti, A., Kim, I., & Schaumont, P. (2011). A robust physical unclonable function with enhanced challenge-response set. *IEEE Transactions on Information Forensics and Security*, *7*(1), 333–345. https://doi.org/10.1109/TIFS.2011.2165540

Moon, D.-I., Rukhin, A., Gandhiraman, R. P., Kim, B., Kim, S., Seol, M.-L., Yoon, K. J., Lee, D., Koehne, J., & Han, J.-W. (2019). Physically unclonable function by an all-printed carbon nanotube network. *ACS Applied Electronic Materials*, *1*(7), 1162–1168. https://doi.org/10.1021/acsaelm.9b00166

Chen, T., Kornblith, S., Norouzi, M., & Hinton, G. (2020). A simple framework for contrastive learning of visual representations. In *International Conference on Machine Learning* (pp. 1597–1607). PMLR. https://doi.org/10.48550/arXiv.2002.05709

Sun, N., Chen, Z., Wang, Y., Wang, S., Xie, Y., & Liu, Q. (2023). Random fractal-enabled physical unclonable functions with dynamic AI authentication. *Nature Communications*, *14*(1), 2185. https://doi.org/10.1038/s41467-023-37588-5

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Mach. Learn., 20*(3), 273–297. https://doi.org/10.1007/BF00994018

Daugman, J. (2009). How iris recognition works. In A. Bovik (Ed.), *The Essential Guide to Image Processing* (pp. 715–739). Academic Press. https://doi.org/10.1016/B978-0-12-374457-9.00025-1

Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K.R., & Qin, Z. (2021). DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Transactions on*

Neural Networks and Learning Systems, 33(9), 4915–4929. https://doi.org/10.1109/TNNLS.2021.3062754

Dong, W., Liu, J., Chen, L., Sun, W., Pan, X., & Ke, Y. (2024). Implicit neural representation steganography by neuron pruning. *Multimedia Syst., 30*, 266. https://doi.org/10.1007/s00530-024-01476-9

Elhabashy, A. E., Wells, L. J., Camelio, J. A., & Woodall, W. H. (2019). A cyber-physical attack taxonomy for production systems: a quality control perspective. *J. Intell. Manuf., 30*(6), 2489–2504. https://doi.org/10.1007/s10845-018-1408-9

Esidir, A., Kiremitler, N. B., Kalay, M., Basturk, A., & Onses, M. S. (2022). Unclonable features via electrospraying of bulk polymers. *ACS Applied Polymer Materials, 4*(8), 5952–5964. https://doi.org/10.1021/acsapm.2c00803

Gabor, T., Akin, S., & Jun, M.B.-G. (2024). Numerical studies on cold spray gas dynamics and powder flow in circular and rectangular nozzles. *J. Manuf. Process., 114*, 232–246. https://doi.org/10.1016/j.jmapro.2024.02.005

Gabor, T., Wang, Y., Akin, S., Zhou, F., Chen, J., Jeon, Y., & Jun, M.B.-G. (2025). Design, modeling, and characterization of a pulsed cold spray system. *Surf. Coat. Technol., 131984*,. https://doi.org/10.1016/j.surfcoat.2025.131984

Gao, Y., Al-Sarawi, S. F., & Abbott, D. (2020). Physical unclonable functions. *Nature Electronics, 3*, 81–91. https://doi.org/10.1038/s41928-020-0372-5

Han, C., Gabor, T., Lee, H., Lee, J., Akin, S., & Jun, M.B.-G. (2025). Pulsed cold spray system for physical unclonable function generation. *Procedia CIRP, 137*, 176–180. https://doi.org/10.1016/j.procir.2025.02.269

Ibrahim, O. A., Sciancalepore, S., & Di Pietro, R. (2024). MAG-PUFs: Authenticating IoT devices via electromagnetic physical unclonable functions and deep learning. *Computers & Security, 143*, Article 103905. https://doi.org/10.1016/j.cose.2024.103905

Spalart, P. R. (2009). Detached-eddy simulation. *Annual Review of Fluid Mechanics*, *41*, 181–202. https://doi.org/10.1146/annurev.fluid.010908.165130

Peng, S.-H., Eliasson, P., & Davidson, L. (2007). Examination of the shear stress transport assumption with a low-Reynolds number k-omega model for aerodynamic flows. In *Proceedings of the 37th AIAA Fluid Dynamics Conference and Exhibit* (p. 3864). AIAA. https://doi.org/10.2514/6.2007-3864

Kuglin, C. D. (1975). The phase correlation image alignment method. In *IEEE International Conference on Cybernetics and Society* (pp. 163–165). IEEE.

Barker, E., & Roginsky, A. (2018). *Transitioning the use of cryptographic algorithms and key lengths* (NIST Special Publication 800-131A Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-131Ar2

Lagaris, I. E., Likas, A., & Fotiadis, D. I. (1998). Artificial neural networks for solving ordinary and partial differential equations. *IEEE Trans. Neural Networks, 9*, 987–1000. https://doi.org/10.1109/72.712178

Ali, M. M. H., Mahale, V. H., Yannawar, P., & Gaikwad, A. T. (2016). Overview of fingerprint recognition system. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1334–1338). IEEE. https://doi.org/10.1109/ICEEOT.2016.7754900

Lowe, D. G. (1999). Object recognition from local scale-invariant features. In *Proceedings of the Seventh IEEE International Conference on Computer Vision* (Vol. 2, pp. 1150–1157). IEEE. https://doi.org/10.1109/ICCV.1999.790410

Li, T., Guo, X., Müller, F., Abdulazhanov, S., Ma, X., Zhong, H., Liu, Y., Narayanan, V., Yang, H., Ni, K., & Chang, M.-F. (2025). Demonstration of high-reconfigurability and low-power strong physical unclonable function empowered by FeFET cycle-to-cycle variation and charge-domain computing. *Nat. Commun., 16*(1), 189. https://doi.org/10.1038/s41467-024-55380-x

Lowe, D. G. (1999). Object recognition from local scale-invariant features. In *Proceedings of the Seventh IEEE International Conference on Computer Vision* (Vol. 2, pp. 1150–1157). IEEE. https://doi.org/10.1109/ICCV.1999.790410

Maiti, A., Kim, I., & Schaumont, P. (2011). A robust physical unclonable function with enhanced challenge-response set. *IEEE Trans. Inf. Forensics Secur., 7*(1), 333–345. https://doi.org/10.1109/TIFS.2011.2165540

Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2021). Neural networks-based cryptography: A survey. *IEEE Access, 9*, 124727–124740. https://doi.org/10.1109/ACCESS.2021.3109635

Moon, D.-I., Rukhin, A., Gandhiraman, R. P., Kim, B., Kim, S., Seol, M.-L., Yoon, K. J., Lee, D., Koehne, J., & Han, J.-W. (2019). Physically unclonable function by an all-printed carbon nanotube network. *ACS Appl. Electron. Mater., 1*(7), 1162–1168. https://doi.org/10.1021/acsaelm.9b00166

Murataj, I., Magosso, C., Carignano, S., Fretto, M., Ferrarese Lupi, F., & Milano, G. (2024). Artificial fingerprints engraved through block-copolymers as nanoscale physical unclonable functions for authentication and identification. *Nat. Commun., 15*(1), 10576. https://doi.org/10.1038/s41467-024-54492-8

Nocentini, S., Rührmair, U., Barni, M., Wiersma, D. S., & Riboli, F. (2024). All-optical multilevel physical unclonable functions. *Nat. Mater., 23*(3), 369–376. https://doi.org/10.1038/s41563-023-01734-7

Park, T., Kim, J., Ko, R., Park, B., & Yoo, H. (2025). Light in, sound keys out: photoacoustic PUFs from stochastic nanocomposites. *Nat. Commun., 16*(1), 7323. https://doi.org/10.1038/s41467-025-62747-1

Lian, S., Chen, G., Cheung, A., & Wang, Z. (2004). A chaotic-neural-network-based encryption algorithm for JPEG2000 encoded images. In *Advances in Neural Networks – ISNN 2004* (pp. 627–632). Springer. https://doi.org/10.1007/978-3-540-28648-6_100

Rohhila, S., & Singh, A. K. (2024). Deep learning-based encryption for secure transmission digital images: A survey. *Computers & Electrical Engineering, 116*(1), Article 109236. https://doi.org/10.1016/j.compeleceng.2024.109236

Rohhila, S., & Singh, A. K. (2024). Deep learning-based encryption for secure transmission digital images: A survey. *Computers & Electrical Engineering*, *116*(1), 109236. https://doi.org/10.1016/j.compeleceng.2024.109236

Sandborn, M., Olea, C., White, J., Williams, C., Tarazaga, P. A., Sturm, L., Albakri, M., & Tenney, C. (2021). Towards secure cyber-physical information association for parts. *J. Manuf. Syst., 59*, 27–41. https://doi.org/10.1016/j.jmsy.2021.01.003

Sandomirskii, M., Petrova, E., Kustov, P., Chizhov, L., Larin, A., Bruyère, S., Yaroshenko, V., Ageev, E., Belov, P., & Zuev, D. (2025). Spectral physical unclonable functions: downscaling randomness with multi-resonant hybrid particles. *Nat. Commun., 16*(1), 5097. https://doi.org/10.1038/s41467-025-60121-9

Shi, Z., Mamun, A. A., Kan, C., Tian, W., & Liu, C. (2023). An LSTM-autoencoder based online side channel monitoring approach for cyber-physical attack detection in additive manufacturing. *J. Intell. Manuf., 34*, 1815–1831. https://doi.org/10.1007/s10845-021-01879-9

Chen, R. T. Q., Rubanova, Y., Bettencourt, J., & Duvenaud, D. K. (2018). Neural ordinary differential equations. *Advances in Neural Information Processing Systems*, *31*. https://doi.org/10.48550/arXiv.1806.07366

Spalart, P. R. (2009). Detached-eddy simulation. *Annu. Rev. Fluid Mech., 41*, 181–202. https://doi.org/10.1146/annurev.fluid.010908.165130

Sun, N., Chen, Z., Wang, Y., Wang, S., Xie, Y., & Liu, Q. (2023). Random fractal-enabled physical unclonable functions with dynamic AI authentication. *Nat. Commun., 14*(1), 2185. https://doi.org/10.1038/s41467-023-37588-5

Tadmor, Y., & Tolhurst, D. J. (1993). Both the phase and the amplitude spectrum may determine the appearance of natural images. *Vision. Res., 33*(1), 141–145. https://doi.org/10.1016/0042-6989(93)90067-7

Vurpillot, F., De Geuser, F., da Costa, G., & Blavette, D. (2004). Application of Fourier transform and autocorrelation to cluster identification in the three-dimensional atom probe. *Journal of Microscopy*, *216*(3), 234–240. https://doi.org/10.1111/j.0022-2720.2004.01413.x

Torun, N., Torun, I., Sakir, M., Kalay, M., & Onses, M. S. (2021). Physically unclonable surfaces via dewetting of polymer thin films. *ACS Applied Materials & Interfaces, 13*(9), 11247–11259. https://doi.org/10.1021/acsami.0c16846

Vaz, R. F., Garfias, A., Martorell, J., Garrido, B., Albaladejo, V., Sanchez, J., & Cano, I. G. (2025). Cold spray additive manufacturing metal knitting: Process parameters effect on aluminum components geometry. *J. Manuf. Process., 133*, 1–10. https://doi.org/10.1016/j.jmapro.2024.11.041

Veinidis, C. N., Akriotou, M., Kondi, A., Papia, E.-M., Constantoudis, V., & Syvridis, D. (2025). Complexity analysis of challenges and speckle patterns in an Optical Physical Unclonable Function. *Chaos, Solitons & Fractals, 191*, Article 115938. https://doi.org/10.1016/j.chaos.2024.115938

Vurpillot, F., De Geuser, F., da Costa, G., & Blavette, D. (2004). Application of Fourier transform and autocorrelation to cluster identification in the three-dimensional atom probe. *J. Microsc., 216*(3), 234–240. https://doi.org/10.1111/j.0022-2720.2004.01413.x

Wang, D., Bai, B., Zhao, W., & Han, Z. (2018). A survey of optimization approaches for wireless physical layer security. *IEEE Communications Surveys & Tutorials, 21*, 1878–1911. https://doi.org/10.1109/COMST.2018.2883144

Wong, B. C., & Fu, M. W. (2025). Unraveling of the statistical correlation between porosity, permeability and diffusivity of cold-sprayed Ti6Al4V. *J. Manuf. Process., 152*, 375–389. https://doi.org/10.1016/j.jmapro.2025.08.028

Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.,30*(3), 1111–1123. https://doi.org/10.1007/s10845-017-1315-5

Xu, S., Chen, S., Xu, R., Wang, C., Lu, P., & Guo, L. (2024). Local feature matching using deep learning: A survey. *Information Fusion, 107*, Article 102344. https://doi.org/10.1016/j.inffus.2024.102344

Yang, M., Ye, Z., Pan, H., Farhat, M., Cetin, A. E., & Chen, P.-Y. (2023). Electromagnetically unclonable functions generated by non-Hermitian absorber-emitter. *Science Advances*, *9*(36), eadg7481. https://doi.org/10.1126/sciadv.adg7481

Yin, S., Cavaliere, P., Aldwell, B., Jenkins, R., Liao, H., Li, W., & Lupoi, R. (2018). Cold spray additive manufacturing and repair: Fundamentals and applications. *Addit. Manuf., 21*, 628–650. https://doi.org/10.1016/j.addma.2018.04.017