ADVANCED MATERIALS TECHNOLOGIES
www.advmattechnol.de

Unclonable MXene Topographies as Robust Anti-Counterfeiting Tags via Fast Laser Scanning and Siamese Neural Networks

Lin Jing, Huachun Si, Tianle Chen, Li-Yin Hsiao, Haochen Yang, Joshua M. Little, Kerui Li, Shuo Li, Qian Xie,* and Po-Yen Chen**

An ideal anti-counterfeiting technology is desired to be unclonable, nondestructive, mass-producible, and accompanied with fast and robust authentication under various external influences. Although multiple anti-counterfeiting technologies have been reported, few meet all of the above-mentioned features. Herein, a mechanically driven patterning process is reported to produce higher dimensional $Ti_3C_2T_x$ MXene topographies in a scalable yet unclonable manner, which can be used as anti-counterfeiting tags. By using a high-speed confocal laser microscopy, the complex topographies can be extracted within one minute and then reconstructed into 3D physical unclonable function (PUF) keys. Meanwhile, a Siamese neural network model and a feature-tracking software are built to achieve a pick-and-check strategy, enabling highly accurate, robust, disturbance-insensitive tag authentication in practical exploitations. The 3D PUF key-based anti-counterfeiting technology features with several advances, including ultrahigh encoding capacities ($\approx 10^{144\,000}$-$10^{7\,800\,000}$), fast processing times (<1 min), and high authentication accuracy under various external disturbances, including tag rotations (≈0°–360°), tag dislocation(s) in *x*(*y*) directions (≈0%–100%), tag shifts in *z*-direction (≈0%–28%), tag tilts (≈0°–5°), differences in contrasts (20%–60%) and laser power (6.0–9.0 µW). The anti-counterfeiting technology promises information security, encoding capacity, and authentication efficiency for the manufacturer-distributor-customer distribution processes.

1. Introduction

Physical unclonable function (PUF) possesses abundant complexity and stochastic fashion, which plays a vital role for highly secure anti-counterfeiting technologies.[1] To date, most of the PUF-based anti-counterfeiting technologies are equipped with security tags containing disordered graphics, including biometric fingerprints,[2–4] fluorescence label,[5–8] physically responsive pattern (e.g., light, heat, humidity, etc.).[9–11] Besides the environmental instability challenges,[5,12–16] most of these PUF-based anti-counterfeiting technologies suffer from fluctuating authentication results under various external disturbances during the pattern extraction processes (e.g., tag dislocations, tag shifts, tag tilts, different equipment settings). When these PUF-based anti-counterfeiting technologies are implemented in practical scenarios, these influences are inevitable and substantially impair the tag authentication accuracy. Therefore,

L. Jing, L.-Y. Hsiao, K. Li, S. Li
Department of Chemical and Biomolecular Engineering
National University of Singapore
4 Engineering Drive 4, Singapore 117585, Singapore
E-mail: lin.jing@ntu.edu.sg

H. Si, Q. Xie
School of Metallurgic Engineering
Anhui University of Technology
59 Hudong Road, Ma'anshan 243002, P.R. China
E-mail: xieqian@ahut.edu.cn

T. Chen, H. Yang, J. M. Little, P.-Y. Chen
Department of Chemical and Biomolecular Engineering
University of Maryland
College Park, MD 20740, USA
E-mail: checp@nus.edu.sg

P.-Y. Chen
Maryland Robotics Center
College Park, MD 20740, USA

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/admt.202300568

DOI: 10.1002/admt.202300568

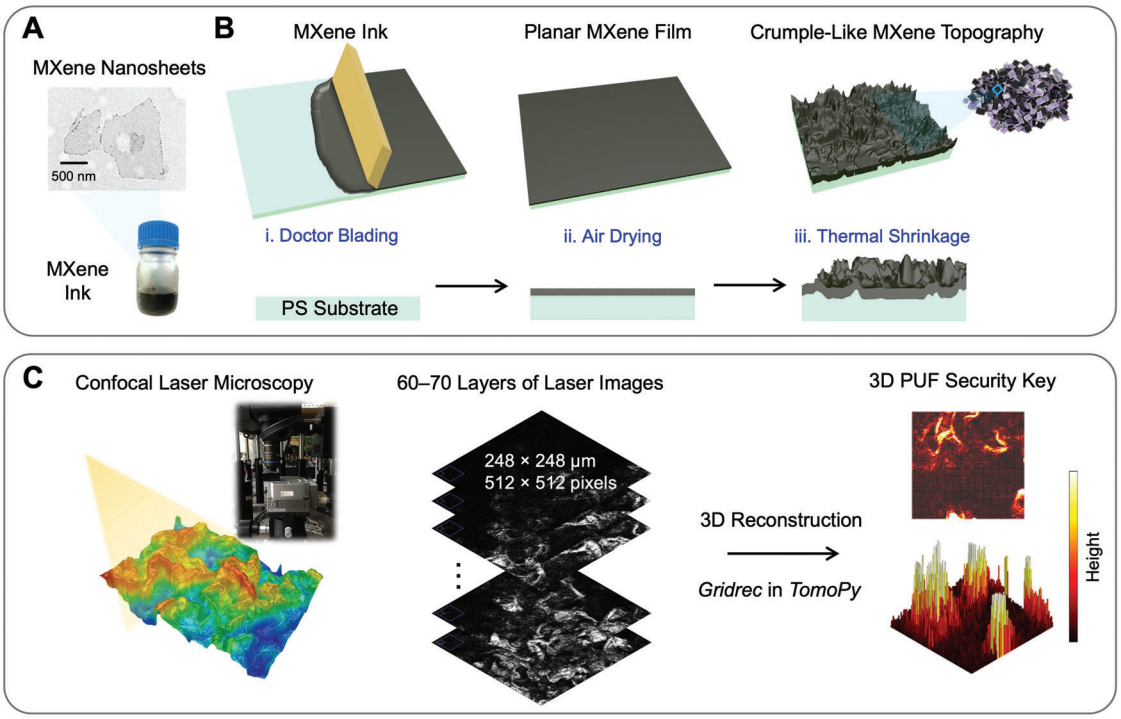

Figure 1. Schematic illustration of higher dimensional, complex MXene topographies fabricated through a mechanically driven patterning process for anti-counterfeiting applications. A,B) Simple and scalable fabrication of higher dimensional MXene topographies through doctor blading followed by thermal contraction. C) High-speed laser confocal scanning of a complex MXene topography followed by reconstruction into a 3D PUF key via a Gridrec algorithm.

challenges remain in developing a highly accurate, robust, disturbance-insensitive PUF-based anti-counterfeiting technology even under various external disturbances.

One emerging approach is to create 3D structure-based PUF tags for anti-counterfeiting technologies, which provide additional degrees of freedom to increase encoding capacities and maintain high authentication accuracy. To date, few anti-counterfeiting technologies based on 3D or higher dimensional PUF tags have been reported, which may be due to multiple technological difficulties.[17–21] First, conventional fabrication processes for the 3D PUF tags with rich, accessible structural information are highly sophisticated with low scalability.[17–19] Second, conventional approaches to extract 3D information involve electron imaging (e.g., scanning electron microscopy (SEM))[22,23] or contact tapping (e.g., atomic force microscopy (AFM)),[24] which are normally time-consuming and require professional equipment training. Third, to authenticate 3D PUF keys, an efficient and robust strategy is required to process and compare these higher dimensional, complex security tags under various external disturbances (e.g., tag dislocations/shifts/tilts).

Recently, stochastic out-of-plane crumpling of ultra-thin materials emerges as an efficient approach to increasing the structural dimensions from 2D to 3D, leading to diverse applications where high specific areas and complex topographies are demanded.[25–30] Herein, a mechanically driven patterning process was developed to produce higher dimensional, complex $Ti_3C_2T_x$ MXene topographies in a scalable yet unclonable manner, which were able to serve as the 3D PUF-based tags for anti-counterfeiting applications. By using a high-speed confocal laser microscopy to scan a MXene tag, its complex topography was extracted in a layer-by-layer fashion within one minute and then reconstructed into a 3D PUF key. Meanwhile, a Siamese neural network (SNN) model and a feature-tracking software are built to achieve a pick-and-check strategy, enabling highly accurate, robust, disturbance-insensitive tag authentication in practical exploitations. Compared with prior arts, the 3D PUF key-based anti-counterfeiting technology features with several advances, including ultrahigh encoding capacities ($\approx 10^{144\,000}$–$10^{7\,800\,000}$), fast processing times (<1 min), and high authentication accuracy under various external disturbances, including tag rotations (≈0°–360°), tag dislocation(s) in $x(y)$ directions (≈0%–100%), tag shifts in z-direction (≈0%–28%), tag tilts (≈0°–5°), differences in contrasts (20%–60%) and laser power (6.0–9.0 μW). Our anti-counterfeiting technology based on 3D PUF keys demonstrates unequaled encoding capacities, promising tag scalability, fast and robust authentication under practical exploitations, which imply their broad and practical applications in consumer industries.

2. Results and Discussion

Figure 1A demonstrates a mechanically driven and scalable patterning process to generate higher dimensional, complex $Ti_3C_2T_x$ MXene topographies by harnessing mechanical instabilities during substrate contraction. $Ti_3C_2T_x$ MXene nanosheets were first prepared by etching $Ti_3C_2T_x$ MAX crystals in the lithium fluoride (LiF) and hydrochloric acid (HCl) solution followed by ultrasonic exfoliation (see more details in Experimental Section). Figure S1, Supporting Information shows the X-ray diffraction and X-ray

photoelectron spectroscopy results, indicating that $Ti_3C_2T_x$ MAX crystals were fully transformed into $Ti_3C_2T_x$ MXene nanosheets after the etching and exfoliation processes. As shown in the transmission electron microscope (TEM) images in the inset of Figure 1A, the as-exfoliated MXene nanosheets were with the average dimensions of ≈500 × 500 nm^2.

As shown in Figure 1B, the MXene dispersion was uniformly coated onto a thermally responsive polystyrene (PS) substrate (i.e., shrink film) by doctor blading at the areal loading of 0.32 mg cm^{-2} (more details in Experimental Section). The PS substrate was pretreated with oxygen plasma to enhance surface hydrophilicity prior to the doctor-blading step. After air drying, a planar MXene layer (with a thickness of ≈1.0 µm) was obtained, and the MXene-coated shrink film was then heat-treated at 135 °C for 10 min to induce the thermal contraction of the underlying PS substrate. By harnessing mechanical instabilities, the upper-layer MXene coating exhibited spatially homogeneous, crumple-like topographies (with a characteristic wavelength of ≈20 µm), as shown in the top-down and tilt-view SEM images in Figure S2, Supporting Information. The MXene-coated PS substrate was further cut into small tags with demanded sizes (3 × 3 mm^2 here) for further use (details in the Experimental Section).

Attributing to the mechanical instabilities during thermal contraction, the higher dimensional MXene topographies exhibited chaosmetric features based on a random generation of isotropic crumples, which are ideal candidates for PUF-based security keys targeting anti-counterfeiting applications. To thoroughly extract the stochastic x, y, and z information, the as-produced MXene topographies were scanned by a laser confocal microscope in a layer-by-layer fashion at high speed (see more details in Experimental Section). Laser confocal imaging employs a single, collimated laser beam as a source of illumination that is directed at a specific point on the sample. The reflected light is then focused through a small aperture, known as a pinhole, which serves as both a second point of focus and a filter to eliminate out-of-focus scattered light. If the light scattered by the sample does not pass through the pinhole, it is not captured by the detector. In other words, only the light signals focused on each layer height were collected.[31] Typically, 60–70 layers of laser scanning images were extracted across the z-direction for a complex MXene topography, typically covering the region of 248 × 248 µm^2 (512 × 512 pixels) in the x–y plane, which took less than 60 seconds (as shown in Figure 1C). It can be observed that the metallic nature of MXene renders its sharp laser imaging that can reveal its full structural information, which is better than other 2D materials or polymers we tested (Figure S3, Supporting Information). Thereafter, by adopting the *Gridrec* algorithm in *TomoPy*, the collected laser images were reconstructed into a 3D PUF-based security key containing comprehensive structural information, enabling highly secure anti-counterfeiting (see more details in Note S1, Supporting Information).[32]

It should be noted that laser confocal imaging exhibits several advantages over conventional SEM and AFM approaches. 1) Ambient working environment. Unlike SEM to be conducted mostly in vacuum, laser confocal imaging can be done in an ambient environment to save energy and time. 2) Facile sample preparation. No sample pretreatment is needed for laser confocal imaging, whereas specific treatments such as conductive coating and flat substrate mounting are necessary for SEM and AFM, respectively. 3) Faster imaging process. Laser confocal imaging is fast and takes less than 1 minute. However, SEM and AFM normally take 5–10 min or more because of extra time needed for evacuation, calibration, and scanning. 4) Larger area imaging. Laser confocal imaging can easily scan a large area at the centimeter scale with high resolution, whereas the length scale of AFM imaging is limited to below 100 µm. SEM imaging is mainly for the areas at the micro- or nano-scale. 5) Less training is required. For mature laser confocal imaging setup (e.g., *Keyence VK-X3000 Series*), minimal training is required since it provides fool-proof operation system. For SEM and AFM, on the other hand, it takes much more operating experience to obtain high-quality images. 6) Relatively cheap setup. The cost of a commercial setup of laser confocal imaging (e.g., *Keyence VK-X3000 Series*) is below US$50,000. However, the costs of commercial setups of SEM and AFM can generally exceed US$100 000.

To efficiently authenticate the 3D PUF-based security keys with multi-layer structural information, a customized Siamese neural network (SNN) model was developed (as shown in Figure S4, Supporting Information),[33,34] which contains 12 depthwise-separable convolutional layers as the body and 2 convolutional layers on the edges (see more details in Note S2, Supporting Information). SNN has particular strength in dealing with the input data with varying qualities and still provide highly accurate, robust decision-making capabilities.[35] For example, SNN has been adopted by the daily-used Face ID systems to authorize the mobile phone access to the user with changing characteristics (e.g., wearing hats, scarves, glasses, or makeup, as well as different facial expressions).[36] Therefore, SNN is highly suitable for authenticating 3D PUF-based security keys during practical exploitations, where many external disturbances exist.

Adopting the SNN model to authenticate 3D PUF keys creates an important synergy for anti-counterfeiting applications, enabling highly accurate, robust tag authentication to decrease the false-negative and false-positive rates originating from various human or machine factors. **Figure 2** illustrates how a SNN-based authentication software was trained and then utilized to identify 3D PUF-based security keys.[34] First, by using a fast laser microscopy to capture a batch of MXene tags with chaosmetric features, a set of 3D PUF keys were collected as the training data, to improve the accuracy and robustness of a SNN model against human and machine instabilities. To be specific, both negative training dataset (i.e., FAKE tags consisting of distinctive 3D PUF keys that were not stored in the database, 630 pairs in total) and positive training dataset (i.e., REAL tags consisting of the same 3D PUF keys but under various disturbances of tag rotations, tag dislocation(s) in the x(y) directions, tag shifts in the z-direction, tag tilts, differences in contrast and laser power, 350 pairs in total) were used (see more details in Note S3, Supporting Information).[37]

With the training dataset, the SNN model functions by considering each 3D PUF key as a centroid in a dissimilarity space (Figure 2). Then, the SNN model was used to calculate the mathematical distance (D) between any of two 3D PUF keys. A larger D indicates that the two 3D PUF keys perform higher dissimilarity and vice versa. There are two goals for the training of a SNN model, i) to maximize the D between the REAL and FAKE tags and ii) to minimize the D between the REAL tag and its counterparts under disturbances. These training processes are done by

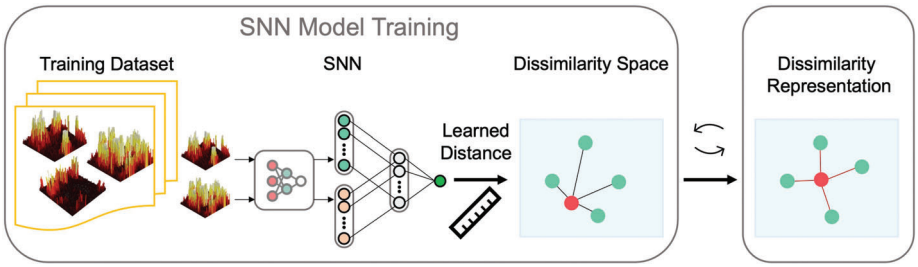

Figure 2. Schematic illustration of the training and testing processes of a Siamese neural network (SNN) model. The dissimilarity vector value (abbreviated as the *D* value) was used to quantify the structural difference between two 3D PUF keys. Two goals were set to train a SNN model: *i*) to minimize the *D* values between REAL tags and *ii*) to maximize the *D* values between REAL and FAKE tags.

adjusting multiple parameters of a SNN model (e.g., number of layers, activation function, normalization function for each layer, *m* value of contrast loss function),[38–40] and 8 train–test cycles were conducted to achieve the abovementioned two goals in this work.

To further test the accuracy and robustness of the as-trained SNN model, the MXene tags were authenticated in various practical scenarios with diverse influential factors, as schematically illustrated in **Figure 3**A. These influential factors include (*1*) tag dislocations in the *x*(*y*) directions (shifting the 3D PUF keys in the *x*–*y* plane: 2% and 4% in the *x*-direction, 2% and 4% in *y* direction), 2) tag rotations (rotating the 3D PUF keys in the *x*–*y* plane: 0°, 2°, 4°, 6°, 8°, 10°), 3) tag shifts in the *z*-direction (shifting the 3D PUF keys in the *z* direction: 0%, 7%, 14%, 21%, and 28%), 4) tag tilts (0°, 3.3°, 3.7°, 4.3°, 5.0°), 5) differences in contrasts (20%, 30%, 40%, 50%, 60%) and *6*) laser power (6.0, 6.5, 7.0, 7.5, 8.0, 9.0 μW). As shown in Figure S5, Supporting Information, the real-time optical images were obviously different upon the variations (1) and (4)–(6). By comparing the REAL tags in the original database and the counterparts captured under various influences (Note S4, Supporting Information), the scattering plots of *D* are shown in Figure 3A. Figure 3B further summarizes them in the box plot, where the *D* values between the REAL and FAKE tags in the database were high, with the $D_{avg.}$ of 761.6 and the D_{max} of 1803.6. In comparison, the *D* values between the REAL tags in the database and the counterparts under various influences are relatively low, with an average *D* (D_{avg}) of 65.2 and a maximum *D* (D_{max}) of 228.0. By setting a threshold *D* slightly above 228.0, the 3D PUF key-based anti-counterfeiting system was able to achieve 0% false-positive rates (100% authentication accuracy, indicating that no "FAKE" ones are recognized as "REAL") and 0% false-negative rates (high authentication robustness, indicating no "REAL" ones are recognized as "FAKE" upon certain external influences), as shown in the green shaded area in Figure 3B. The high authentication accuracy and robustness of 3D PUF keys were attributed to their multi-layer data format accompanied with a well-trained SNN model, which largely preserved most of the structural information to achieve outstanding comparison accuracy.

To highlight the advantages of 3D PUF keys, the same batch of MXene tags were examined by SEM, and the captured SEM images were reconstructed as 2D PUF keys. To train another SNN model using 2D PUF keys, similar negative (i.e., FAKE tags consisting of distinctive 2D PUF keys that were not stored in the database), and positive training datasets (i.e., REAL tags consisting of the same 2D PUF keys but under the variations (1)–(6) were used (more details in Note S5, Supporting Information). Compared to the highly accurate and robust 3D PUF-based system, the 2D PUF one was significantly affected by various human/machine factors. As shown in the red shaded area in Figure 3B, to ensure a 0% false-positive rate (no "FAKE" ones are recognized as "REAL"), a threshold *D* of 223.2 was selected, while 28.2% false-negative rate was observed, meaning that 28.2% of the "REAL" 2D PUFs will be mis-authenticated as "FAKE" under various influences, especially upon tag rotations, tag dislocations in the *x*(*y*) directions, and tag tilts. The use of 3D PUF keys led to high authentication robustness and accuracy, which could avoid multiple attempts of tag authentication.

Among various influences, the tag dislocations in the *x*(*y*) directions as well as the tag rotations were the scenarios that happened most frequently during the tag authentication processes. Although 3D PUF-based anti-counterfeiting system allowed some percentages of tag dislocations (<4%) and tag rotations(<10%), the *D* values easily exceeded the threshold *D* of 228.0 when the *x*(*y*) shifts were larger than 7% and the rotation angles were larger than 12° (more relevant details can be seen in Figure S6, Supporting Information).

To tackle these challenges, a feature-tracking software was built to achieve a pick-and-check strategy, enabling highly accurate, robust, disturbance-insensitive tag authentication in practical exploitations. As shown in **Figure 4**A, after an MXene tag was fabricated, its entire topography (across 3 × 3 mm^2) was scanned and extracted by using a fast laser confocal microscopy, and a large-area, mother 3D PUF key was then stored in the database. After the MXene tag was distributed, the authentication mechanism consisted of two basic steps: i) pick and ii) check. Regarding the first pick step, the user used the fast laser microscopy to scan any smaller sub-region of an MXene tag, and a 3D PUF key was constructed. Afterward, the scale invariant feature transform (SIFT) algorithm was adopted to match the captured 3D PUF key with the mother 3D PUF key that was stored in the database (detailed in Note S6, Supporting Information).[41–43] If not matched, this MXene tag was determined as "FAKE". If matched, this MXene tag was allowed to proceed with the next check step, and the SNN model was used to authenticate the captured 3D PUF key. The pick-and-check strategy ensured that any tag shifts or tag rotations caused by human or machine factors were able to be corrected, which substantially prevented information loss or distortion due to imprecise tag positioning.

As shown in Figure 4B, five sub-regions (#1 to #5, with *x*(*y*) shifts >100%) were randomly selected and scanned, and the SIFT algorithm was able to match precisely with the mother 3D

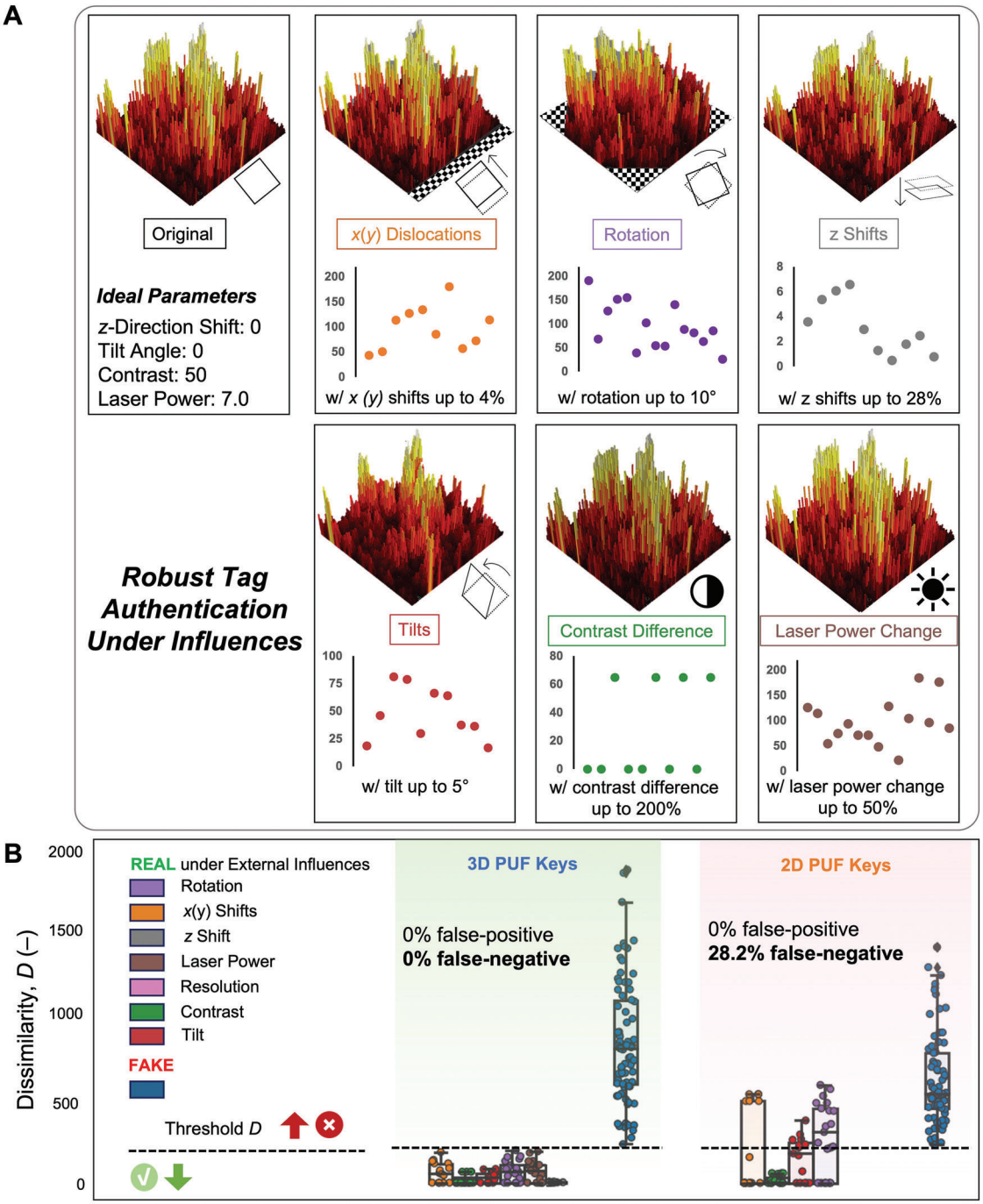

Figure 3. 3D PUF key-based anti-counterfeiting technology with highly accurate, robust tag authentication under external influences. A) The synergy between 3D PUF keys and SNN model led to an anti-counterfeiting technology with highly accurate, robust tag authentication against 1) tag dislocations in the $x(y)$ directions, 2) tag rotations, 3) tag shifts in the z-direction, 4) tag tilts, 5) differences in contrasts and 6) laser power. B) Box plots representing the D values between "REAL" and "FAKE" tags. The "REAL" cases included the scenarios of extracting the PUF keys under various external influences.

PUF key from the database. Similarly, five sub-regions (#6 to #10, with rotations >180°) were selected and scanned, and the SIFT algorithm could also match with the large-area 3D PUF key. The SIFT algorithm with precise locating capabilities made the 3D PUF-based anti-counterfeiting technology more dislocation- and rotation-insensitive. After the first pick step, the customer-captured 3D PUF key was compared with the mother 3D PUF key using the SNN algorithm.

By realizing the pick-and-check strategy, the D values between the customer-captured and mother 3D PUF keys were in the low ranges of ≈0–10 (with $x(y)$ shifts) and ≈0–50 (with rotations), as shown in the scattering plots in Figure 4B. As shown in

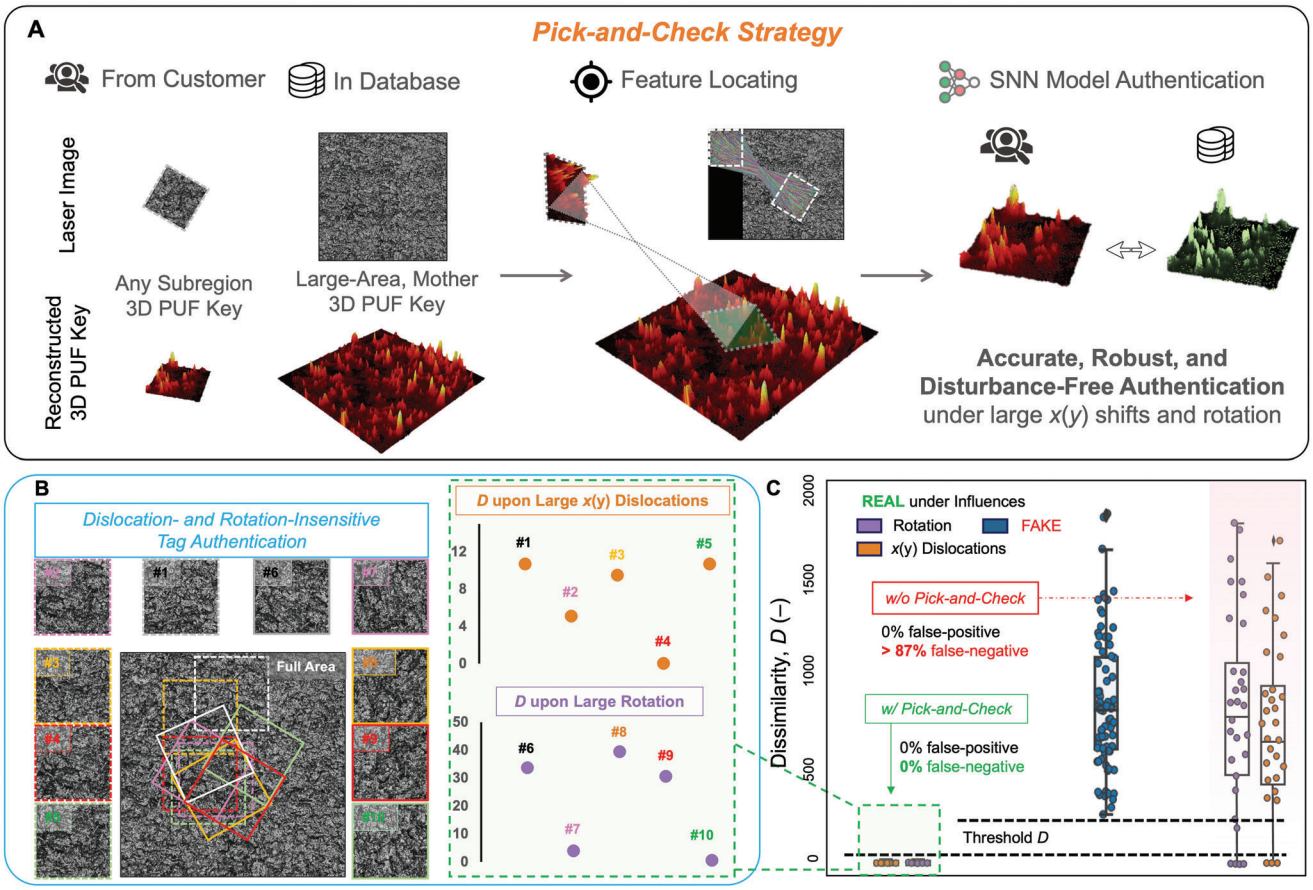

Figure 4. Pick-and-check strategy enabled highly accurate, robust, and disturbance-free tag authentication in practical exploitations with large $x(y)$ dislocations and rotations. A) The pick-and-check strategy consisted of two steps: 1) matched the 3D PUF key (that was extracted from the customer side) with the large-area, mother 3D PUF key (that was stored in the manufacturer's database), 2) authenticated the customer-captured 3D PUF key via the SNN-based software. B) With the pick-and-check strategy, our anti-counterfeiting technology reached sufficiently lower D values than the threshold D value (228) even under large $x(y)$ shifts and rotations, enabling dislocation- and rotation-insensitive tag authentications. C) The box plot compared the D values of our anti-counterfeiting technology with and without the pick-and-check strategy, and the former exhibited higher tolerance against large $x(y)$ shifts and rotations, demonstrating top authentication accuracy with 0% false-positive and 0% false-negative rates.

Figure 4C, these D values were much lower than the threshold D of 228.0, ensuring 0% false-positive rates and high authentication robustness. This is because the disturbance factors (e.g., $x(y)$ shift, rotations) will be canceled first during the "pick" step by calibrating the location and angle with the help of SIFT algorithm. Then, during the "check" process, there will be nearly no difference between the extracted PUF key and its corresponding original PUF key, which is why the D values derived by SNN model will be much lower and close to 0.

On the other hand, if the pick-and-check strategy was not applied, the D values increased to 619.9 under the $x(y)$ shifts up to 100% and to 827.1 under the rotation up to 180°, both of which were much higher than the threshold D of 228.0. In this case, to maintain a 0% false-positive rate, the anti-counterfeiting system was required to compromise with a false-negative rate of over 87%, which was not acceptable for practical applications, as over 34 attempts of pattern extraction are to be repeated to make the false-negative rate fall below 1%. Therefore, it is reasonable to conclude that the pick-and-check strategy substantially improved the overall robustness of 3D PUF-based anti-counterfeiting technology, which saved the efforts/time involved in the authentication process, while ensuring top authentication accuracy (high validation precision with both 0% false-positive and 0% false-negative rates).

In addition, unlike most current PUF systems that are vulnerable to light,[5,12] heat,[13,14] physical stress,[15,16] the MXene-based PUF tags in this work possess excellent environmental stabilities upon exposure to various conditions such as low (−20 °C) and high temperatures (150 °C), 0% and 90% RH conditions, UV light, as well a highly acidic (6.0 M HCl) and alkaline (6.0 M NaOH) solutions (Figure S7, Supporting Information).

To further quantitatively analyze the robustness of our anti-counterfeiting technology, we further exposed our tags to several mechanical and thermal treatments and evaluate the authentication accuracy after that. As shown in **Figure 5**A below, our 3D MXene-based PUF tags experienced several thermal and mechanical treatments separately, including high-temperature heating (120 °C for 12 h), water stirring (600 rpm for 12 h), water flushing (for 3 min), and water soaking (for 12 h), and hand rubbing (for 1 min). After these treatments, the PUF keys were

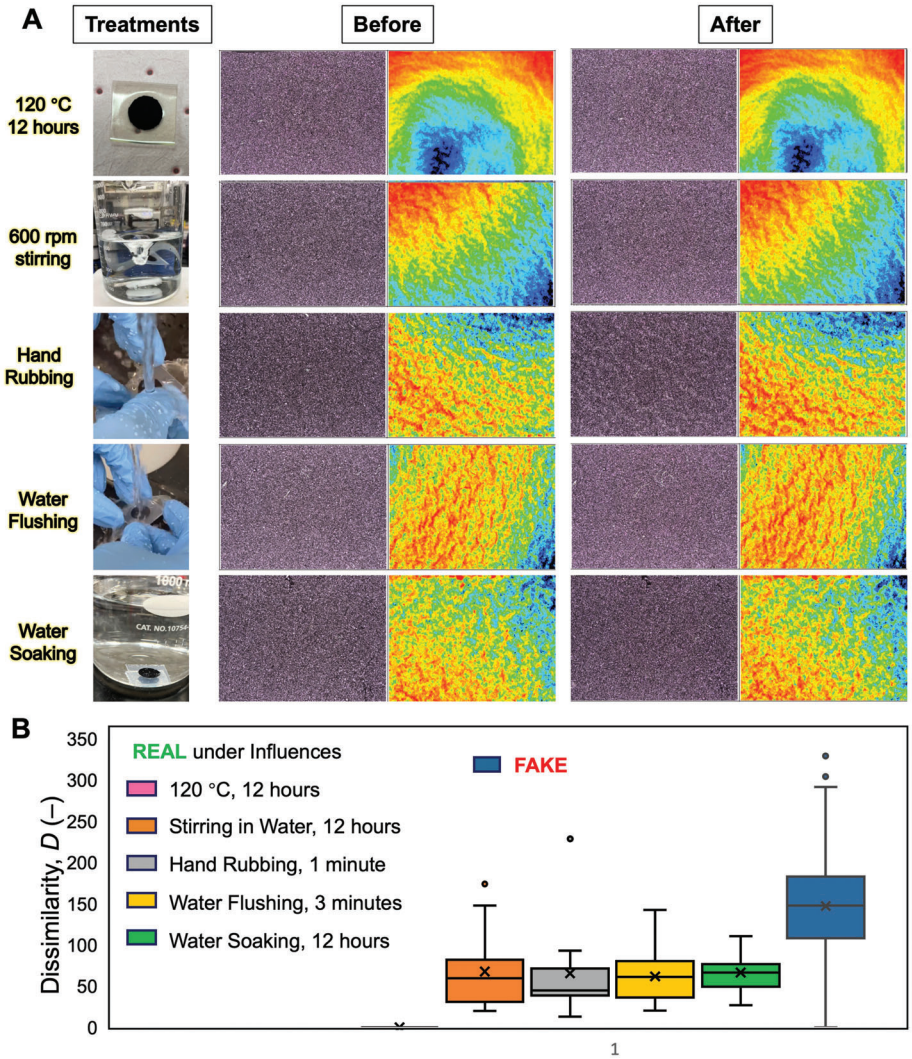

Figure 5. 3D PUF key-based anti-counterfeiting technology demonstrates high authentication robustness even under various thermal and mechanical treatments. A) 3D crumple anti-counterfeiting tags under high-temperature heating (120 °C for 12 h), water stirring (600 rpm, 12 h), water flushing (3 min), and water soaking (12 h), as well as hand rubbing (1 min). Before and after these treatments, the confocal laser images of 3D MXene-based PUF tags were obtained using Keyence VK series, and little topographical differences were observed. B) Box plots representing the *D* values between the same PUF tags before and after thermal and mechanical treatments (the REAL group) and the *D* values between different PUF tags (the FAKE group).

extracted using Keyence VK series. Figure 5A shows the representative confocal laser images and Note S8, Supporting Information includes the rest of confocal laser images. Finally, the *D* values between the same PUF tags before and after treatments (the REAL group) were calculated using our SNN model, and a D_{avg} value of 44.2 was shown in the box plots of Figure 5B. In comparison, the *D* values between different PUF tags (the FAKE group) were much higher with a D_{avg} value of 147.7. By setting a threshold *D* value of 68.0, a false-positive rate of 8.5% and a false-negative rate of 6.1% were achieved. It should be noted that tag authentication accuracy and robustness could be improved by conducting repetitive authentication processes. For example, if we repeat the authentication process twice, the false-positive rate and false-negative rate were able to significantly drop to 0.7% and 0.4%, respectively.

Besides authentication speed and robustness, our 3D PUF-based anticounterfeiting technology also featured higher security (encoding capacity), as summarized in **Table 1**. The higher uniqueness of the crumple-like topographies originates from its potential to encode higher density of information, which leads to its higher encoding capacity (i.e., the number of distinct patterns).[44,45] In this work, the structural information of 3D PUF keys contributes to significant encoding capacities ranging from $10^{144\,000}$ to $10^{7\,864\,320}$ (depending on the layer number in the *z*-direction, detailed calculations are supplied in Note S7, Supporting Information), which are much higher than the state-of-the-art PUF systems.[2,5,7,15,45,46]

Furthermore, by using a confocal laser microscopy, the processing time was further shortened to less than 1 min. Our strategy includes the potential for using other convenient reading platforms, such as optical microscopy and optical cameras on cell phones, to authenticate our PUF tags. This will make them highly accessible to many end-users. Figure S8, Supporting Information shows a proof-of-concept demonstration using a handheld

Table 1. Comparison between our anticounterfeiting technology in this work and the state-of-the-art PUF systems in terms of encoding capacity, processing speed, authentication robustness upon disturbances like tag rotation, tag shift, and upon environmental factors like thermal and mechanical stresses, etc.

PUF systems	Encoding Capacity	Processing Speed	Robustness Upon Rotation	Robustness Upon Shift	Environmental Stability
Polymer wrinkle (Ref. [2])	10^{175}	40 min	Not demonstrated	Robust under tag rotations (≈0°–360°)	Not demonstrated
Fluorescent tags (Ref. [5,7,15,45])	$\approx 10^{25}$–10^{202}	≈2–5 min	Not demonstrated except Ref. [5].	Not demonstrated	Not demonstrated
Raman tag (Ref. [46])	$\approx 10^{15\,051}$	20 min	Not demonstrated	Not demonstrated	Not demonstrated
This work	$\approx 10^{144\,000}$–$10^{7\,800\,000}$	<60s	Robust under tag rotations (≈0°–360°)	Robust under $x(y)$ shifts (≈0%–100%)	Robust under 120 °C, rubbing, water flushing, etc.

optical microscope to read our PUF tags, and the corresponding authentication results are presented. It can be observed that this optical imaging approach also exhibits sufficient authentication accuracy and robustness, indicating its potential for everyday anti-counterfeiting applications. Upon comparison with other PUF tags (i.e., #1, #2, #3 representing three different PUF tags), all the authentication results displayed high dissimilarity (D) values of >300. In contrast, when the same PUF tag was subjected to various disturbances (i.e., #1-1, #1-2, #1-3, #1-4 representing the same PUF tags under different focal distances, brightness, or contrasts), much lower D values of <100 were demonstrated.

More importantly, the pick-and-check strategy developed in this work addressed the long-standing positioning challenge for graphic PUF authentication, contributing to a robust and accurate authentication under various disturbances of rotation, dislocation, shift, tilt, contrast, etc. The unequaled combination of high encoding capacity, processing speed, authentication robustness, and environmental stability of our 3D PUF key anticounterfeiting technology stands itself out while comparing with the state-of-the-art PUF systems, pushing it one step further to practical applications.

3. Conclusion

In this work, crumple-like $Ti_3C_2T_x$ MXene topographies were fabricated in a scalable yet unclonable fashion through a mechanically driven patterning process, and the resulting MXene patterns were utilized as the anti-counterfeiting tags. The complex MXene topographies were extracted in a layer-by-layer manner via a confocal laser microscopy, and the stacks of laser images were then reconstructed into 3D PUF keys, showing high potentials for anti-counterfeiting applications. To enable the robust authentication of 3D PUF keys, a SNN model accompanied with a feature tracking software was constructed. Compared to the state-of-the-art PUF-based technologies, this work demonstrated multiple critical advances, including ultrahigh encoding capacities, fast processing times, and high authentication accuracy and robustness, all of which were promising and ready to be adopted for the manufacturer-distributor-customer distribution processes.

Electronic supplementary information (ESI) available: Experimental section, material characterization, 2D and 3D PUF key training and testing sets, SNN model, SIFT algorithms, additional results, illustrative notes. Source code used in this work is freely available for non-commercial use at https://github.com/aljay-jing/3D-SNN.

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

L.J. and H.S. contributed equally to this work. The authors acknowledge the financial support provided by the Start-Up Fund of the University of Maryland, College Park (KFS No.: 2957431 to P.-Y.C.). Fundings for this research were provided by MOST-AFOSR Taiwan Topological and Nanostructured Materials Grant under Grant No. FA2386-21-1-4065 (KFS No.: 5284212 to P.-Y.C.), and Energy Innovation Seed Grant from Maryland Energy Innovation Institute (MEI^2) (KFS No.: 2957597 to P.-Y.C.). L.J. acknowledges the support from the Ministry of Education Academic Research Fund R-279-000-579-112 and Professor Xiaonan Wang from the Department of Chemical and Biomolecular Engineering, National University of Singapore.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: April 13, 2023
Published online:

[1] R. Arppe, T. J. Sørensen, *Nat. Rev. Chem.* **2017**, *1*, 0031.
[2] H. J. Bae, S. Bae, C. Park, S. Han, J. Kim, L. N. Kim, K. Kim, S. H. Song, W. Park, S. Kwon, *Adv. Mater.* **2015**, *27*, 2083.
[3] C. Park, H. J. Bae, J. Yoon, S. W. Song, Y. Jeong, K. Kim, S. Kwon, W. Park, *ACS Omega* **2021**, *6*, 2121.

[4] S. Wang, E. Toreini, F. Hao, *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2823.
[5] Y. Liu, F. Han, F. Li, Y. Zhao, M. Chen, Z. Xu, X. Zheng, H. Hu, J. Yao, T. Guo, W. Lin, Y. Zheng, B. You, P. Liu, Y. Li, L. Qian, *Nat. Commun.* **2019**, *10*, 2409.
[6] H. Nam, K. Song, D. Ha, T. Kim, *Sci. Rep.* **2016**, *6*, 30885.
[7] P. Kumar, J. Dwivedi, B. K. Gupta, *J. Mater. Chem. C* **2014**, *2*, 10468.
[8] H. Zhou, J. Han, J. Cuan, Y. Zhou, *Chem. Eng. J.* **2022**, *431*, 134170.
[9] T. Ma, T. Li, L. Zhou, X. Ma, J. Yin, X. Jiang, *Nat. Commun.* **2020**, *11*, 1811.
[10] J. Zhang, S. Xu, Z. Wang, P. Xue, W. Wang, L. Zhang, Y. Shi, W. Huang, R. Chen, *Angew. Chem., Int. Ed.* **2021**, *60*, 17094.
[11] X. Le, H. Shang, S. Wu, J. Zhang, M. Liu, Y. Zheng, T. Chen, *Adv. Funct. Mater.* **2021**, *31*, 2108365.
[12] B. Duong, H. Liu, C. Li, W. Deng, L. Ma, M. Su, *ACS Appl Mater Interfaces* **2014**, *6*, 8909.
[13] S. Johansen, M. Radziwon, L. Tavares, H. G. Rubahn, *Nanoscale Res. Lett.* **2012**, *7*, 262.
[14] M. Radziwon, S. Johansen, H. G. Rubahn, *Procedia Eng.* **2014**, *69*, 1405.
[15] Y. Geng, J. Noh, I. Drevensek-Olenik, R. Rupp, G. Lenzini, J. P. F. Lagerwall, *Sci. Rep.* **2016**, *6*, 26840.
[16] R. Cowburn, *Contemp. Phys.* **2008**, *49*, 331.
[17] R. Platel, L. Vaure, E. Palleau, S. Raffy, F. Guérin, D. Lagarde, R. Cours, C. Marcelot, B. Warot-Fonrose, C. Nayral, F. Delpech, L. Ressier, *J. Colloid Interface Sci.* **2021**, *582*, 1243.
[18] H. Tan, G. Gong, S. Xie, Y. Song, C. Zhang, N. Li, D. Zhang, L. Xu, J. Xu, J. Zheng, *Langmuir* **2019**, *35*, 11503.
[19] H. Wang, H. Wang, Q. Ruan, Y. S. Tan, C. W. Qiu, J. K. W. Yang, *ACS Nano* **2021**, *15*, 10185.
[20] J. Yang, D. Lei, D. Chen, J. Li, H. Jiang, Q. Ding, Q. Luo, X. Xue, H. Lv, X. Zeng, M. Liu in *2020 IEEE International Electron Devices Meeting (IEDM)*, IEEE, San Francisco, CA, USA **2020**.
[21] J. Li, C. He, H. Qu, F. Shen, J. Ye, *J. Mater. Chem. C* **2022**, *10*, 7273.
[22] K. Hagita, T. Higuchi, H. Jinnai, *Sci. Rep.* **2018**, *8*, 5877.
[23] R. Podor, X. Le Goff, T. Cordara, M. Odorico, J. Favrichon, L. Claparede, S. Szenknect, N. Dacheux, *Mater. Charact.* **2019**, *150*, 220.
[24] A. Glia, M. Deliorman, M. A. Qasaimeh, *Adv. Sci.* **2022**, *9*, 2201489.
[25] P. Y. Chen, M. Liu, T. M. Valentin, Z. Wang, R. Spitz Steinberg, J. Sodhi, I. Y. Wong, R. H. Hurt, *ACS Nano* **2016**, *10*, 10869.
[26] K. Li, M. Gao, Z. Li, H. Yang, L. Jing, X. Tian, Y. Li, S. Li, H. Li, Q. Wang, J. S. Ho, G. W. Ho, P. Y. Chen, *Nano Energy* **2020**, 104875.
[27] L. Jing, L. Y. Hsiao, S. Li, H. Yang, P. L. P. Ng, M. Ding, T. V. Truong, S. P. Gao, K. Li, Y. X. Guo, P. Valdivia y Alvarado, P. Y. Chen, *Mater. Horiz.* **2021**, *8*, 2065.
[28] P. Y. Chen, M. Zhang, M. Liu, I. Y. Wong, R. H. Hurt, *ACS Nano* **2018**, *12*, 234.
[29] L. Jing, K. Li, H. Yang, P. Y. Chen, *Mater. Horiz.* **2020**, *7*, 54.
[30] K. Li, T. H. Chang, Z. Li, H. Yang, F. Fu, T. Li, J. S. Ho, P. Y. Chen, *Adv. Energy Mater.* **2019**, *9*, 1901687.
[31] D. B. Hovis, A. H. Heuer, *J Microsc* **2010**, *240*, 173.
[32] B. Dowd, G. Campbell, R. Marr, V. Nagarkar, S. Tipnis, L. Axe, D. Siddons, *Proceedings of SPIE - The International Society for Optical Engineering*, SPIE, San Jose, CA, USA **1999**.
[33] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam, *ArXiv* **2017**.
[34] L. Nanni, A. Rigo, A. Lumini, S. Brahnam, *Appl. Sci.* **2020**, *10*, 4176.
[35] S. Pan, C. Zhu, X. M. Zhao, L. P. Coelho, *Nat. Commun.* **2022**, *13*, 1.
[36] N. D. Palo, https://towardsdatascience.com/how-i-implemented-iphone-xs-faceid-using-deep-learning-in-python-d5dbaa128e1d (accessed: March 2023).
[37] J. Li, K. Lim, H. Yang, Z. Ren, S. Raghavan, P. Y. Chen, T. Buonassisi, X. Wang, *Matter* **2020**, *3*, 393.
[38] D. Ulyanov, A. Vedaldi, V. Lempitsky, *ArXiv* **2016**.
[39] S. Ioffe, C. In Szegedy, *International Conference on Machine Learning*, IEEE, Lille, France **2015**.
[40] R. Hadsell, S. Chopra, Y. LeCun in *2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06)*, IEEE, New York, NY, USA **2006**.
[41] D. G. Lowe, *Int J Comput Vis* **2004**, *60*, 91.
[42] Z. Hossein-Nejad, H. Agahi, A. Mahmoodzadeh, *Pattern Anal Appl* **2021**, *24*, 669.
[43] M. Bansal, M. Kumar, M. Kumar, *Multimed Tools Appl.* **2021**, *80*, 18839.
[44] R. Arppe-Tabbara, M. Tabbara, T. J. Sørensen, *ACS Appl Mater Interfaces* **2019**, *11*, 6475.
[45] M. R. Carro-Temboury, R. Arppe, T. Vosch, T. J Sørensen, *Sci Adv.* **2018**, *4*, e1701384.
[46] Y. Gu, C. He, Y. Zhang, L. Lin, B. D. Thackray, J. Ye, *Nat. Commun.* **2020**, *11*, 516.