

Random laser ablated tags for anticounterfeiting purposes and towards physically unclonable functions

Received: 16 February 2022

Accepted: 16 August 2024

Published online: 31 August 2024

 Check for updatesSrinivas Gandla¹, Jinsik Yoon², Cheol-Woong Yang³, HyungJune Lee⁴, Wook Park²✉ & Sunkook Kim¹✉

Anticounterfeiting tags affixed to products offer a practical solution to combat counterfeiting. To be effective, these tags must be economical, capable of ultrafast production, mass-producible, easy to authenticate, and automatable. We present a universal laser ablation technique that rapidly generates intrinsic, randomly distributed craters (in under a second) on laser-sensitive materials using a nanosecond pulsed infrared laser. The laser and scanning line parameters are balanced to produce randomly distributed craters. The tag patterns demonstrate high randomness, which is analyzed using pattern recognition algorithms and root mean square error deviation. The optical image information of the tag is digitized with a fixed bit uniformity of 0.5 without employing any debiasing algorithm. The efficacy of tags for anticounterfeiting is presented by securing the challenge associated with each tag. Statistical NIST tests are successfully performed on responses generated from both single and multiple tags, demonstrating the true randomness of the sequence of binary digits. The single(multiple) tag(s) achieved an actual encoding capacity of approximately 10^{391} (10^{518}) and a low false rate (both positive and negative) on the order of 10^{-58} (10^{-50}). Our findings introduce a laser-based method for anticounterfeiting tag generation, allowing for ultrafast and straightforward product processing with minimal fabrication and tag cost.

Counterfeiting is a serious challenge for any nation in terms of economic losses arising from counterfeit products, public health problems due to fake prescription medicines, and national security issues caused by inferior components in military appliances^{1–3}. Consequently, developing anticounterfeiting strategies has become a major concern. One such strategy is to attach anticounterfeiting tags to products. High encoding capacity anticounterfeiting tags, such as spectral and graphically encoded tags, are widely used. Unfortunately, these are prone

to cloning attacks by counterfeiters owing to their deterministic and predictable encoding mechanisms. They are thus restricted to use as “identifiers” to carry product information, rather than as “security tags” for verification. Nondeterministic encoding mechanisms with strong authentication are therefore essential for guaranteeing non-replicable code outputs.

From the past few decades, physical and chemical methods using 1D^{4–12}, 2D^{13–17}, and 3D^{18–21} based materials/structures have gained

¹Multifunctional Nano Bio Electronics Lab, Department of Advanced Materials Science and Engineering, Sungkyunkwan University, Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do 16419, Republic of Korea. ²Institute for Wearable Convergence Electronics, Department of Electronics and Information Convergence Engineering, Kyung Hee University, Deogyong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea. ³Electron Microscopy Research Laboratory, Department of Advanced Materials Science and Engineering, Sungkyunkwan University, Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do 16419, Republic of Korea. ⁴Intelligent Networked Systems Lab, Department of Computer Science and Engineering, Ewha Womans University, Ewhayeodae-gil, Seodaemun-gu, Seoul 03760, Republic of Korea. ✉ e-mail: parkwook@khu.ac.kr; seonkuk@skku.edu

significant interest to fabricate physically unclonable tags for anti-counterfeiting purposes. Among these, chemical methods for the fabrication of tags are of primary interest due to their facile, low-cost, stochastic fabrication, intrinsic complex formation of entities involved during the fabrication process, and high encoding capacity. Generally, the intrinsic/extrinsic characteristic random pattern of a physical entity is represented by an image. Therefore, image-capturing tools are of significant interest, as they can be used to read patterns for identification/verification. Similarly, luminescent (phosphorescent or fluorescent) materials, quantum dots, and lanthanide complexes that are readable upon exposure to a certain wavelength of light, using fluorescence or confocal microscopy, have been widely exploited. These offer easy detection of counterfeits^{21–25}. Other varieties of tags with high data capacity have been identified using mass-spectrometric and chemical or elemental analyses. Nevertheless, the reported tags present several individual challenges, including reliance on non-rapid fabrication strategies, complex fabrication processes, high costs of fabrication and tags, environmental stability concerns, human intervention requirements, limitations in mass production with scalability issues, and the need for algorithms to ensure a bit-uniformity of 0.5. Therefore, there is considerable room for the development of tags that can address all these issues simultaneously.

Besides, lasers, especially pulsed lasers, are strong candidates for tagging, as they fulfill the above-mentioned demands. They can generate randomly distributed marks on laser-sensitive materials. Lasers are designed to produce regular beam pulses, with moderate scanning speeds and high repetition frequencies, to interact with matter for various purposes. They can be adapted to produce unusual and random ablation patterns by tuning their laser parameters and adjusting scanning line patterns. To date, lasers have been applied to treat the surfaces of materials for sintering or nanowelding^{26,27}, crystallization²⁸, patterning^{29,30}, annealing³¹, synthesis^{32–34}, texturing³⁵, transfer, and lift-off^{36,37}. The pulsed laser beam, scanning lines with high overlapping factors, generally has an effective energy density per unit time over an effective irradiated area. Less attention is given to laser pulses separated by a distance, as this has few applications. Lasers have also been used in speckle pattern recognition for authentication and identification^{38,39}.

Here, we present a report on the utilization of laser ablation to generate random crater patterns on Si or Si/SiO₂ substrates, as well as on various products that exhibit sensitivity to a pulsed infrared (IR) laser with a wavelength of 1064 nm. Laser ablation referred to as photoablation, is the process of irradiating solid surfaces using an intense laser beam of continuous waves or pulses to remove the surface material in the irradiated zone. This generates physical marks on the surface. The time delay between successive line scans, determined by the tradeoff of laser and scanning line parameters, results in a randomly distributed craters pattern. To enable the random distribution and high data capacity of the ablated patterns, rotation and scanning line parameters were introduced. Random crater patterns were generated on a Si/SiO₂ surface as security tags for identification and verification purposes. Images of the tag's random patterns on Si/SiO₂ substrates were processed and validated through mathematical models. Merits of the presented work are 1) rapid fabrication of tags within a few seconds (see Supplementary Table S1), 2) 4-inch wafer-scale production of silicon-based tags 3) the material and fabrication costs are effectively zero, excluding the costs associated with the substrate and fabricating tool, 4) a bit uniformity of fixed 0.5 with randomness (Without employing any debiasing algorithm). With these merits, we believe the presented technique enables new opportunities in the field of tagging and counterfeit detection.

Results

Randomly distributed laser-ablated patterns

Straightforward manufacturing procedures are essential for the production of low-cost tags for anticounterfeiting purposes. Automation

of the fabrication procedure is crucial for mass production and reduces manpower requirements. Tags fabrication must be rapid to ensure no delays in production (see Supplementary Table S1)^{23,25,40–45}. The presented laser technique satisfies all these requirements. Laser-sensitive surfaces were irradiated to generate random crater patterns by laser ablation and their use as tags for anticounterfeiting purposes and emphasis on utility as a PUF was demonstrated. The concept of the random laser ablation technique is presented in Fig. 1a, b. Laser ablation was performed by a pulsed laser beam with a high scan speed of 2000 mm/s and a low repetition rate of 20 kHz. The scanning lines were rotated through up to 360° in equal steps of rotation angle (RA). The transition from a regular and predictable pattern of craters to an irregular and unpredictable pattern of craters is shown in Fig. 1a, b. The same set of scanning lines, but with a speed of 1000 mm/s, produced a visible predictable craters pattern that could be reproduced using the same laser ablation technique. A 4-inch wafer with random crater patterns engraved on it is shown in Fig. 1c, and its corresponding inset microscopic images are shown in Fig. 1d, e.

The random laser ablation approach was accomplished using a nanosecond IR laser by optimizing the laser and scanning line parameters. Unlike a continuous-wave laser, where the laser beam irradiates the solid surface and produces a continuous impression with material removed from its surface, pulsed lasers can produce both continuous and pulsed impressions. This depends on the input laser and scanning line parameters, such as laser scanning speed, repetition rate, pulse duration, and hatch distance (H_rD). The main purpose of using pulsed lasers is to avoid overheating during the irradiation process. This provides a thermal relaxation time between the pulses so that a sufficiently high temperature can be attained at a given point without affecting the surrounding material. Pulsed lasers are being used in an ever-increasing range of applications, but most research is dedicated to laser ablation techniques. Laser ablation removes portions of a target material when the incident laser photons are absorbed, their energy depending on the laser wavelength and refractive index of the material. This generates free electrons which collide with the atoms of the bulk material, and a transfer of energy occurs. Depending on the thermal conductivity of the material, this heats the surface material above its boiling point, causing vaporization^{46,47}. For high-energy laser pulses, the ejected vapor interacts with the incoming beam to form a plasma plume. Due to the pressure difference with the ambient atmosphere, this leads to a rapid expansion of the melt pool, which gets cooled and redeposited at the edge of the impression (crater) as debris⁴⁸. The distribution of craters patterns, and the size of the impressions on the surface of a material caused by laser ablation, can be tuned by laser parameters such as power, repetition rate, speed, and pulse duration, in addition to scanning line parameters including H_rD and RA. Here, using such pulsed laser tuning and choice of parameters, we apply the laser ablation technique to produce an intrinsic tag for anticounterfeiting.

Laser ablation was executed on a Si/SiO₂ substrate with a set of scanning lines rotated through 360° in equal-angle steps, for a defined H_rD and working area (Fig. 2a, b). The average laser power (P_{avg}) required to ablate the surface was first optimized. P_{avg} depends on the peak power, repetition rate, and pulse width, such that if any one of these increases, the average power increases. Sample random craters patterns obtained for different powers (40%, 50%, 60%, 70%, and 80%) are presented in Supplementary Fig. S1a. A 100% power is associated with a maximum power of 20 W. With a peak power of 10 W, repetition frequency 20 kHz, and pulse width of 20 ns, P_{avg} is 40 mW, corresponding to a laser fluence of 0.25 J/cm². The higher the average power, the larger the ablated radius. To enable high data capacity within a defined area, many craters are required. Therefore, ablated patterns with smaller radii were considered to correspond to a P_{avg} of 40 mW, which is just above the threshold laser fluence of 0.2 J/cm². The random craters patterns obtained for different frequencies (5 kHz,

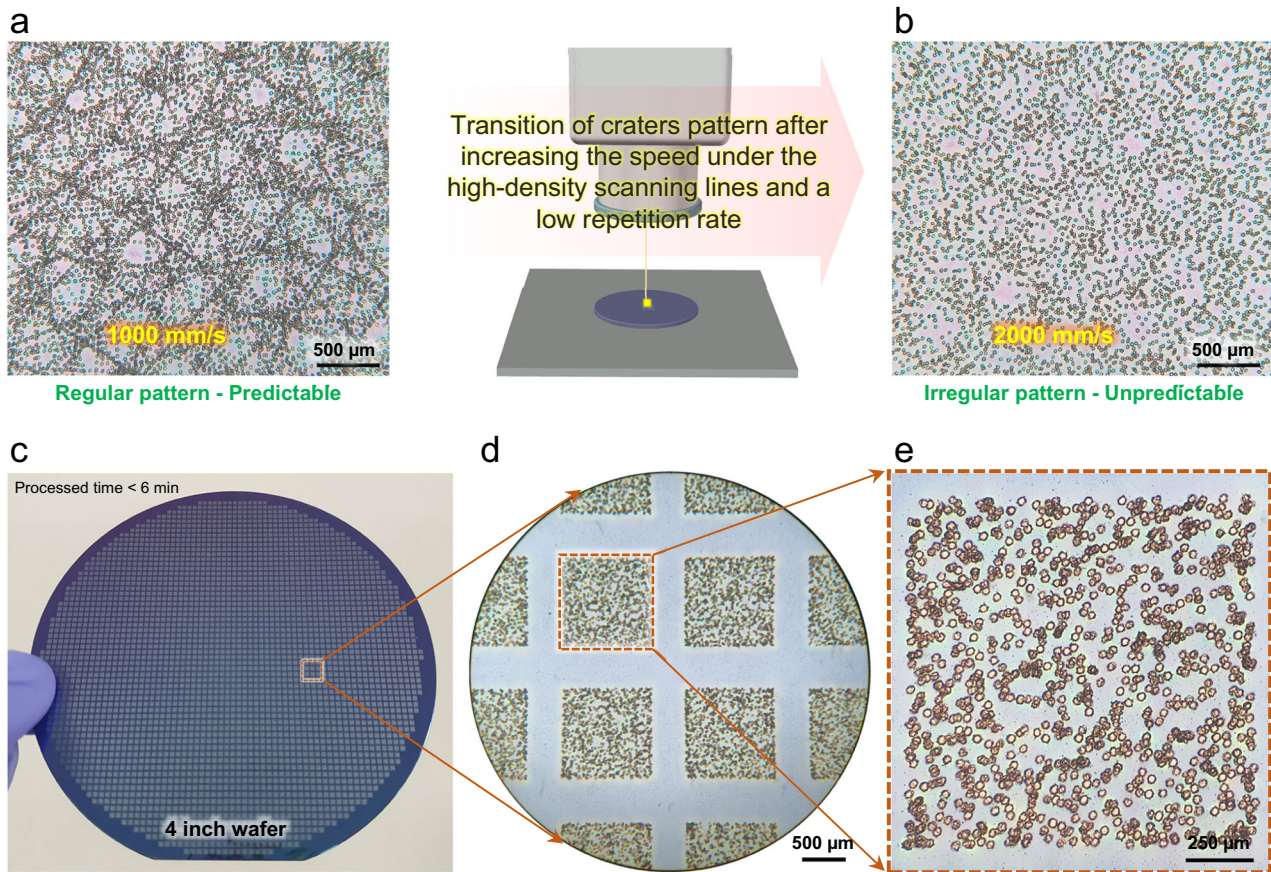


Fig. 1 | Laser-ablated random crater patterns on Si/SiO₂ 4-inch wafer substrate. Crater patterns produced at speeds (a) 1000 mm/s and (b) 2000 mm/s with H₁D 0.3 mm and RA 13°. Laser parameters: power 40 mW, pulse width 20 ns, and repetition rate 20 kHz. **a** Patterns are regular and predictable; **b** patterns are irregular and unpredictable. **c–e** Tags of 1 mm² size fabricated on a 4-inch wafer separated by a 200 μm distance, and with optical micrographs alongside it.

10 kHz, 15 kHz, 20 kHz, and 25 kHz) are presented in Supplementary Fig. S1b. With an increase in the repetition frequency, the density of the randomly ablated patterns increases. To obtain a distinguishable group of ablated patterns that enable easy image processing, crater patterns corresponding to a frequency of 20 kHz were selected. H₁D and RA parameters are tuned as per the laser-ablated pattern size. A smaller pattern size requires a smaller H₁D and RA for a high density of patterns in a unit area.

Laser ablation was first performed along with a set of scanning lines corresponding to 0° angle (Fig. 2a), followed by ablation along with the same set of scanning lines rotated through 13°. This was repeated until the completion of the 360° RA. The dotted box in Fig. 2b represents the working area. Because the laser beam is not continuous but is rather a series of continuous pulses with a well-defined gap between them, the scanning lines (Fig. 2b) correspond to a series of pulses, as shown in Fig. 2c. The pulse-to-pulse distance can be varied by changing the ratio of laser scanning speed v to repetition frequency f . The higher the speed and the lower the repetition frequency, the larger the distance between laser pulses, referred to as the bite size in micrometers (Fig. 2d). This distance can be determined using Eq. (1). The related overlapping factor can be calculated using Eq. (2).

$$\text{Bite size } (\mu\text{m}) = v(\text{mm/s})/f(\text{kHz}) \quad (1)$$

$$\% \text{Overlap} = (1 - v/(fD))100\% \quad (2)$$

where D is the circular pattern diameter. The optimized pulsed laser parameters were power 50%, repetition frequency 20 kHz, speed 2000

mm/s, and pulse width 20 ns. With these values, the distance between two successive ablated patterns was 100 μm. Using Eq. (2), the overlapping factor was −2.57%, indicating non-overlapping. A clear and significant separation of laser-ablated patterns is a crucial requirement for obtaining high randomness. This will be discussed later in this section.

The random generation of ablated craters patterns is mainly attributed to the “error” caused during the transition of laser pulses from one scanning line to another. To visually inspect the randomness, a separate case of scanning lines rotated 360° in steps of 90° was considered, as shown in Supplementary Fig. S2a–e. As the scanning lines are identical (overlap) for 0° and 180°, and 90° and 270° RAs, the ablated patterns (array of dots) corresponding to 0° and 180° RAs could have overlapped exactly (likewise for the 90° and 270° RAs). However, in all the samples fabricated at different times, the patterns have different overlapping distances (Supplementary Fig. S2c–e). A similar situation was observed in samples with scanning rotated in 45° steps (Supplementary Fig. S3a–e). This demonstrates explicitly that the variations observed in all the samples are mainly attributable to the error occurring during the transition from one scanning line to another. A slight error between successive laser pulse patterns was also observed, which would introduce additional randomness in the process.

Next, the density of the scanning lines varied with the H₁D for a fixed laser scanning speed of 2000 mm/s. This was repeated at a laser scanning speed of 1000 mm/s, as shown in Supplementary Fig. S4. The scanning line density decreased by increasing the step size of the RA, in turn, 13°, 33°, 53°, 73°, and 93° for a complete 360° RA (Fig. 2e). This set of RAs was used for H₁D of 0.03 mm, 0.07 mm, 0.1 mm, 0.3 mm, and

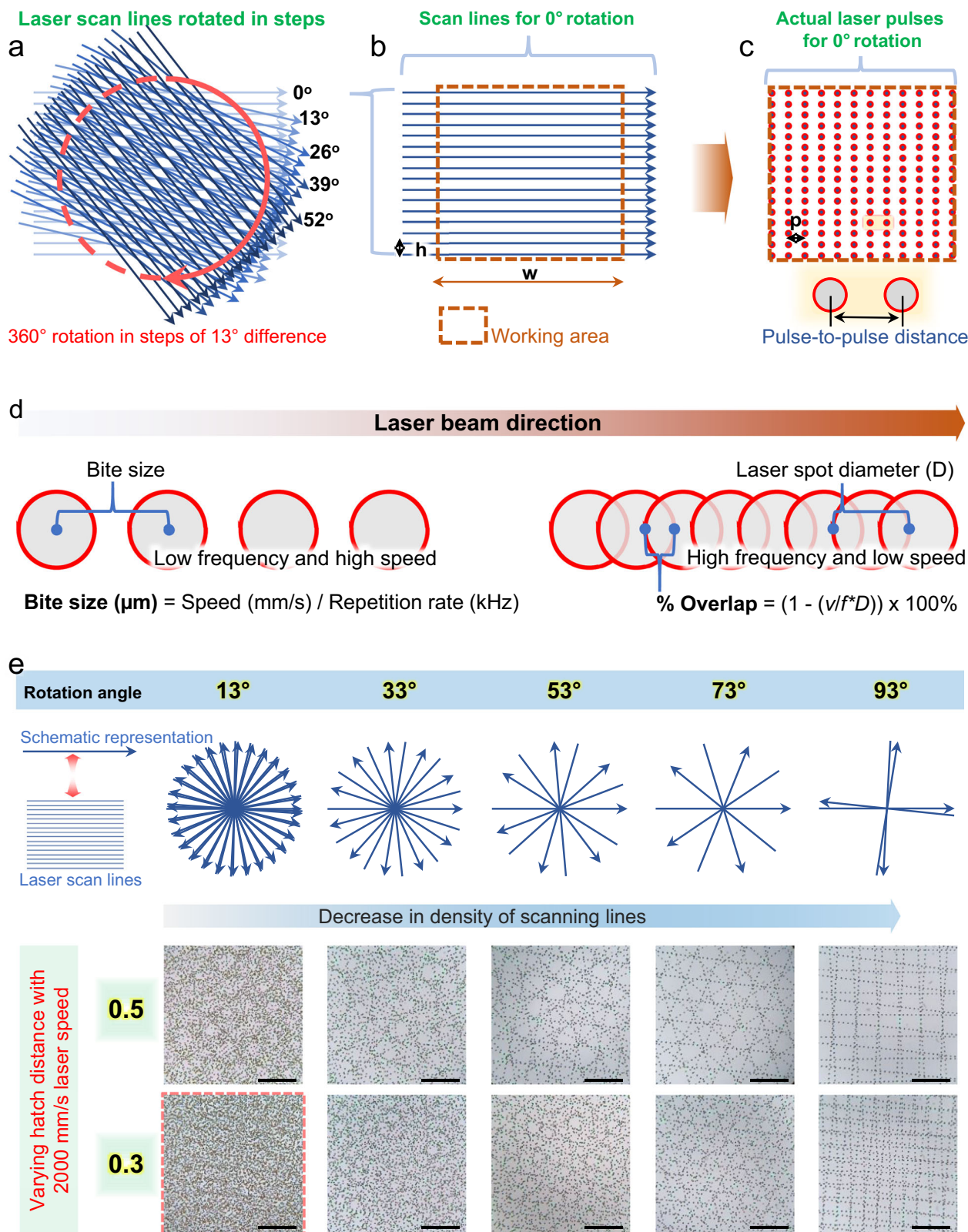


Fig. 2 | Schematic representation of laser scanning lines, beam direction with overlapping and non-overlapping beam spots, and scanning lines with varying H_tD and RAs. Scanning lines rotated 360° in steps of 13° (a) with the lines showing H_tD and (b) working area. c Lines of pulse-like impression having a definite pulse-to-pulse distance. d Pulse-to-pulse overlapping dependent parameters: diameter, bite-

size, and overlap percentage. e Laser-ablated random craters pattern samples for H_tDs 0.5 mm and 0.3 mm, and RAs 13°, 33°, 53°, 73°, and 93°. Low RAs produce higher densities of scanning lines and crater patterns. Laser parameters: power 40 mW, pulse width 20 ns, repetition frequency 20 kHz, and speed 2000 mm/s (scale bar 500 μm).

0.5 mm (Fig. 2e and Supplementary Fig. S5). As shown in Fig. 2e and Supplementary Fig. S4, as the density of scanning lines decreases, the random crater patterns tend to become more distinguishable. To be unclonable, tag patterns must be highly random and indistinguishable. Therefore, the random crater patterns achieved for the conditions of 0.3 mm H_tD and 13° RA are best suited for producing tags. Considering other H_tD, at 0.5 mm the density is not high enough, and at 0.1 mm it is unclear whether individual or group patterns are distinguishable (For distances of 0.03 mm, 0.07 mm, and 0.1 mm, see Supplementary Information Fig. S5). The patterns were nearly circular, similar to that of the irradiating laser beam. The selection of odd-numbered RAs is not limited but does not include even numbers. This is because the even-numbered RAs have the same overlapping scanning lines for the 0–180° and 180–360° ranges. For example, if the RA step is 20°, then in completing 360° rotation, the scanning lines are identical for 0–180° (0°, 20°, 40°, 60°, 80°, 100°, 120°, 140°, 160°, and 180°) and 180–360° (200°, 220°, 240°, 260°, 280°, 300°, 320°, 340°, and 360°). The optimized scanning line parameters were H_tD 0.3 mm and RA 13°.

Outline circles extraction using image processing

The process flow for extracting outline circles is shown in Supplementary Fig. S6a–d. Since the craters are of circular shapes, only circular outlines were extracted, referred to as outline circles, using a user-customized image processing program. The extracted outline circles were blue in color. The distribution of the craters in a pattern is considered random depending on the number of outline circles that exist in various forms (individual and group of outline circles with different overlapping factors and orientations). Therefore, a standard unit of area 100 μm × 100 μm, referred to as a segment, was selected for the analysis of randomness (Supplementary Fig. S6e).

Analysis of pattern randomness through RMSE value

Analysis of the random outline circle patterns was accomplished using mathematical models in MATLAB software. First, to evaluate the crater patterns created under a variety of conditions, such as 0.3 mm, 0.5 mm, and 0.7 mm H_tDs, with 13°, 33°, 53°, 73°, and 93° RAs, the number of outline circles produced per unit area was analyzed, as shown in Fig. 3a. Approximately 800 segments were tested in each condition. The smallest number of 0.588 (per unit area) was obtained for 0.7 mm H_tD and 93° RA, and the largest number of 6.539 for 0.3 mm H_tD and 13° RA. In addition, to analyze whether the distribution was uniform, the root mean square error (RMSE) value of the distribution was calculated using the following Eq. (3) (Fig. 3b):

$$RMSE = \sqrt{\frac{\sum (P_i - \bar{P})^2}{n}} \quad (3)$$

where P_i , \bar{P} and n are the variable probability of analyzed outline circles patterns, variable probability of uniform distribution, and variable number of distributions, respectively. A low RMSE value indicates that the distribution is very uniform. The RMSE analysis yielded a lowest value of 0.013 for 0.3 mm H_tD and 13° RA, and a highest value of 0.068 for 0.7 mm H_tD and 93° RA. This analysis confirmed that the outline circles number per unit area is more uniform when more outline circles are present. When the outline circles were close to each other, they were either separated or overlapped with other outline circles to form objects (Fig. 3c). An object composed of an isolated single outline circle does not have a specific direction; therefore, the object's orientation value is zero. However, for an object composed of multiple overlapping outline circles, the orientation has a specific value. If the number of outline circles per unit area is large, such as for 0.3 mm H_tD, several overlapped outline circles exist, so the probability of uniform distribution of object orientation is relatively low. Figure 3c shows the analysis of the object orientation distribution for 0.3 mm H_tD with various RA. The number of elements of the orientation distribution was

set to six (with a step size of 30°). The RMSE values of the outline circles patterns created under 0.1 mm, 0.3 mm, 0.5 mm, and 0.7 mm H_tD and 13°, 33°, 53°, 73°, and 93° RA are shown in Fig. 3e. Analysis of the randomly distributed outline circles for 0.3 mm H_tD confirmed that the distribution had a very low RMSE value of approximately 0.004, regardless of the RA. Most of the objects obtained with 93° RA were separated individually; thus, the RMSE value was expected to be low. Even at 13° RA, in which several outline circles overlapped, the RMSE value was equally low. These results show that the orientation of an object is random even if outline circles overlap, confirmed by the low RMSE values of approximately 0.004 obtained for all analyzed conditions. Consequently, object orientation can always be considered random. The ratio of objects to the total outline circles was analyzed. In general, the smaller the H_tD and RA, the larger the number of overlapping outline circles and, consequently, the smaller the object/outline circles ratio. From this analysis, a low objects/outline circles ratio of 61% for 0.3 mm H_tD and 13° RA and a high ratio of 88% for 0.7 mm H_tD and 93° RA was obtained (Supplementary Fig. S7).

Based on object orientation analysis, it is difficult to predict the fabricated position of craters/outline circles when they overlap. Additionally, we analyzed whether the position could be forecast even when the outline circles were separated. Several linear trend lines at various angles could be constructed by combining numerous outline circles. Among these, a few straight trend lines connecting several outline circles were evident. The direction angles of these straight trend lines were analyzed. Figure 3d shows the distribution of the trend line angles for outline circles created with 0.3 mm H_tD and various RA. As the supplied RA increased, the trend line angle distribution showed a characteristic convergence to specific values. These converged values indicated that the direction of the linear trend lines for these outline circle patterns was limited and unevenly distributed. Conversely, for low RAs of 13° and 33°, the directions of the straight trend lines were quite diverse and uniformly distributed. The RMSE values of the trend line distribution for a range of H_tDs and RAs were analyzed, as shown in Fig. 3f. This shows that independent of H_tD, RMSE values range between 0.02 and 0.13 for RAs of 13° and 93° respectively. Therefore, the trend lines for 0.3 mm H_tD and 13° RA can be considered uniformly distributed, while the craters are randomly distributed. The average diameter of the outline circles produced under a wide range of H_tD and RAs was measured to be approximately 28 μm (Supplementary Fig. S8a). The distribution of outline circles for 0.3 mm H_tD and 13° RA had an average size of approximately 27 μm (Supplementary Fig. S8b). In summary, the crater patterns created under 0.3 mm H_tD and 13° RA exhibited high randomness. A total of 16 laser-ablated crater samples are shown in Fig. S9.

Challenge-response pair generation

The analyses of pattern randomness from object orientation and trend lines confirm that the craters are randomly distributed, and therefore suitable for generating challenge-response pairs. The challenge-response generation mechanism is shown in Fig. 4. First, the challenge to be loaded onto the tag image is set as a 64-bit sequence of 8 × 8 size. In each challenge, an equal number of zeros (32) and ones (32) is distributed, therefore, the average value of the challenge sequence is equal to 0.5 (Fig. 4a). After applying the challenge sequence with the tag image, thirty-two different areas corresponding to the white pixel, the bit '1', are only considered for response sequence generation, while the region corresponding to the black pixel, representing the bit '0' are discarded (Fig. 4b). Starting from the top left white areas, craters trend lines are extracted in each case, sequentially. The extracted inclined trend line angles are categorized into elements. In a total of 180°, from –90° to 90°, the trend lines arbitrarily lying in between 8 elements (with 22.5° each) constitute a distribution of trend lines per white area (Fig. 4ci). This means the probability of trend lines lying in between –90° to –67.5° (element 1),

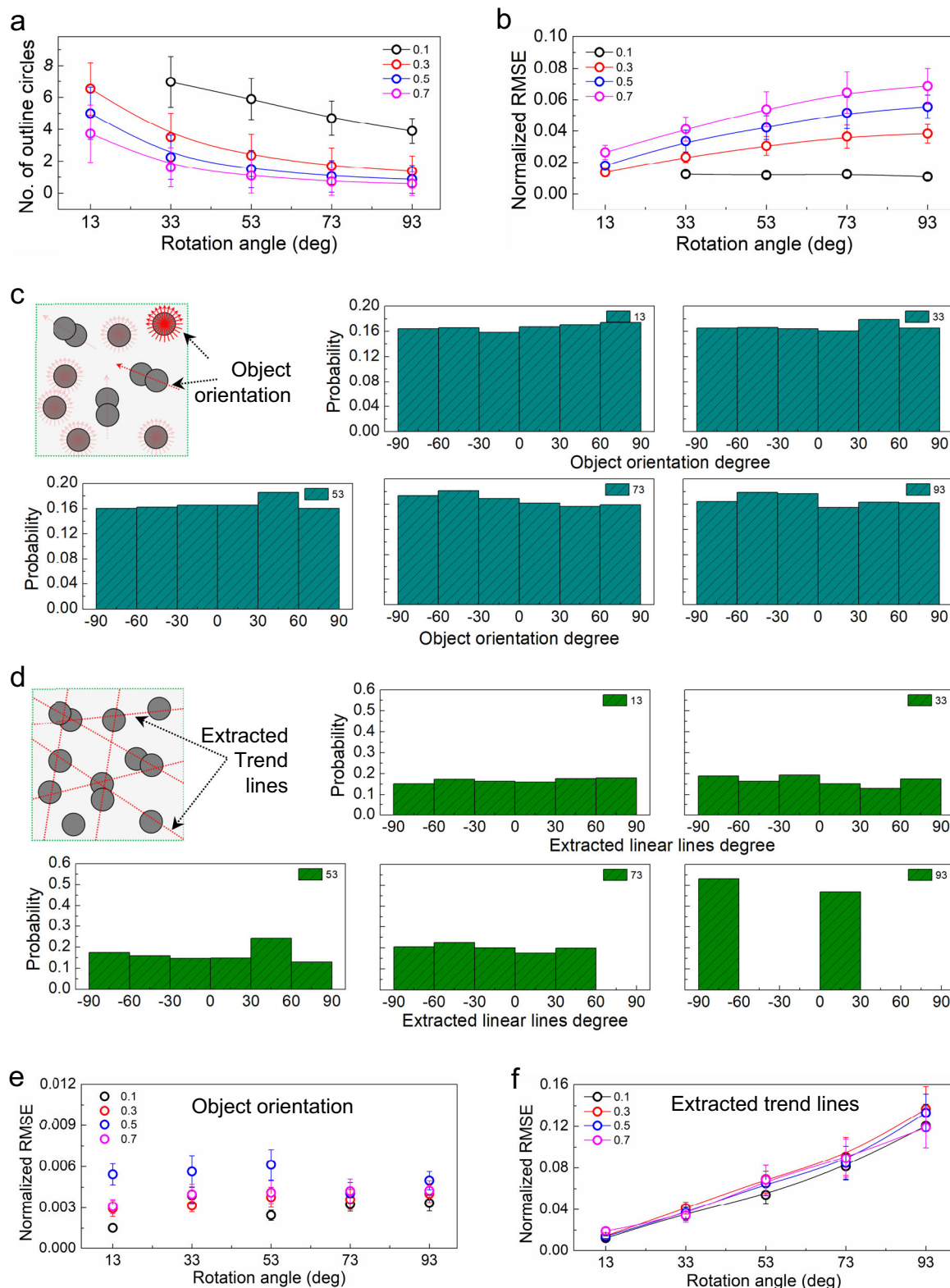


Fig. 3 | Analysis of uniform distribution and randomness of outline circle patterns. a, b The number of outline circles per unit area of 0.01 mm² and their uniform distribution for various H₂Ds and RAs. **c, d** Object orientation and

extracted trend line distribution for RAs 13°, 33°, 53°, 73°, and 93° with 0.3 mm H₂D. **e, f** RMSE of object orientation and extracted trend line distribution for RAs 13°, 33°, 53°, 73°, and 93° with H₂Ds 0.1 mm, 0.3 mm, 0.5 mm, and 0.7 mm.

−67.5° to −45° (element 2), −45° to −22.5° (element 3), and so on to 67.5° to 90° (element 8) is plotted for each white area. So, for each area, there are 8 elements considered as a single distribution. Accordingly, by merging a total of 32 areas, a combined distribution

with a total of 256 elements (32 distributions) can be obtained (Fig. 4cii). Then, starting from the left to the end of the right each element is assigned with an increasing integer (starting from ‘0’). Note that it is impossible to predict which element has the biggest or

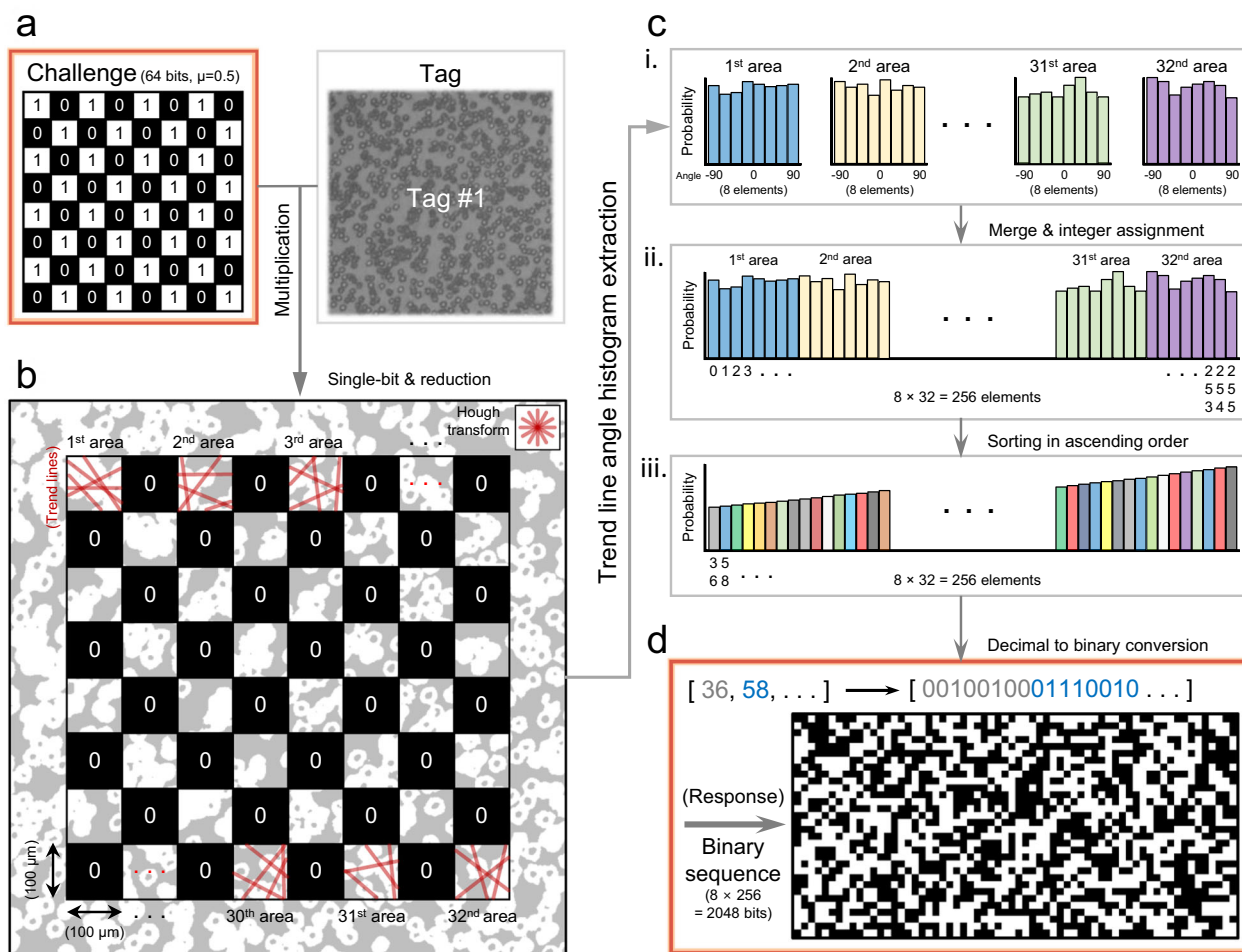


Fig. 4 | Laser ablated tags for challenge-response pair generation. **a** The challenge of a 64-bit sequence of 8×8 size with multiplication operation of tag. The challenge consists of 64 bits (the number of 0's and 1's are equal to 32) with 0.01 mm^2 size. **b** The tag with challenge after multiplication. **c** Extraction of trend lines distribution of craters in a pattern; (i) the probability of trend lines lying

between -90° to 90° is divided into 8 elements with 22.5° each; (ii) merging and integer assignment; (iii) ascending the elements with an increase in the probability values. **d** Conversion of integers to 8-bit binary digits for the generation of a response, a binary sequence of 2048 bits corresponding to the 32 white areas of the input challenge.

smallest probability. As the probability distribution throughout the 256 elements is random, the elements of the distribution are sorted from the smallest to the biggest probability value (Fig. 4ciii). By this approach, the integers are made random in sequential order. As the maximum integer 255 can be represented by an 8-bit binary notation to '1111111', all the integers randomly arranged in Fig 4ciii are converted to 8-bit binary digits. As a result, by merging all the 8-bit binary digits associated with integers, a single stream (1D form) of 2048 ($=8 \times 256$) bit sequence is obtained which is presented as a 2D form (Fig. 4d). Even if the position of '1' in the challenge sequence is partially switched, the distribution order of the trend lines extracted from each area of the challenge shuffles unpredictably, therefore, diverse challenge-response pairs can be generated.

Performance of responses from a single tag

To use tags as a potential candidate for anticounterfeiting, tag responses to different challenges need to be different. For that, 36 different challenges were separately overlapped with a single tag image, and their corresponding 36 responses composed of 2048 bits each are compared (Fig. 5a). A total bit-sequence of 36 responses obtained from one tag is shown in Supplementary Fig. S10. For better visibility of bits, the total 73728 ($=36 \text{ rows} \times 2048 \text{ columns}$) bits are reconstructed closer to a square shape ($36 \times 2048 = 256 \times 288 = 73728$)

to fit Supplementary Fig S10. To evaluate the extracted responses, first, uniformity was analyzed using the following Eq. (4):

$$\text{Bit uniformity} = \frac{1}{l} \sum_{i=1}^l B_i \quad (4)$$

where B_i is the i -th bit of the bit sequence B , and l is the sequence length. The response generated by every challenge is a sequence in which all integers from 0 to $2^n - 1$ are converted into n bits. Therefore, the ratio of 0s to 1s in the bit sequence response is always one-to-one, and the bit uniformity is fixed at 0.5. Next, to evaluate uniqueness characteristics, the hamming distance (HD) distributions between different challenges are analyzed. The HD is a constant that compares bit sequences, and it is equivalent to checking how many bits in the same position occupy different cases. The HD was calculated using the following Eq. (5):

$$\text{Hamming distance (HD)} = \frac{1}{l} \sum_{i=1}^l B_{1i} \oplus B_{2i} \quad (5)$$

(Inter – hamming distance (Inter – HD),
if B_1 and B_2 are different responses)

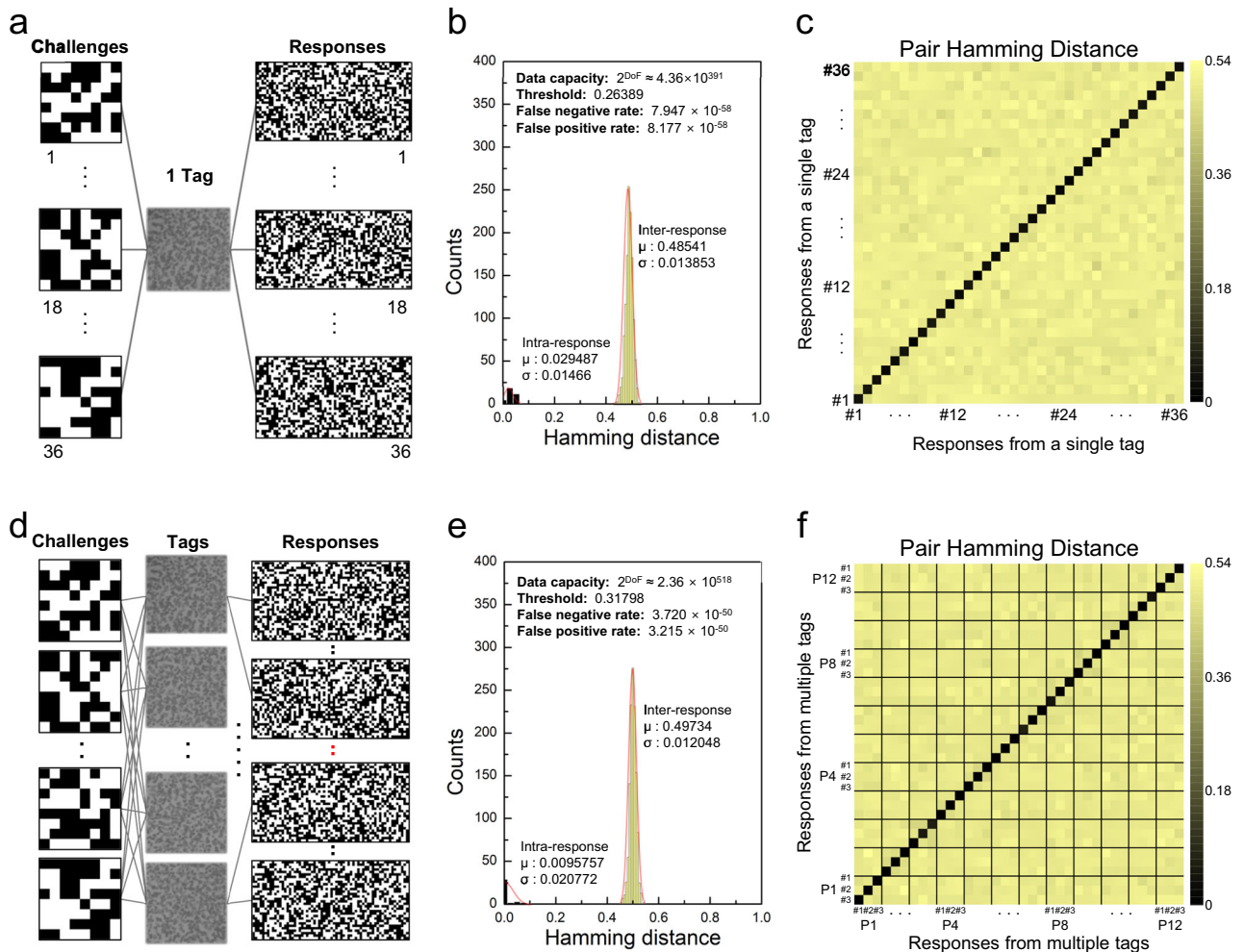


Fig. 5 | Responses from single and multiple tags correspond to multiple challenges. **a** 36 responses from a single tag and 36 challenge pairs. **b** Gaussian distributions of inter- and intra-HD: The inter-HD distribution between 1260 combinations of response pairs and intra-HD distribution between 36 response pairs of same-bit sequences. **c** The equivalent representation of **b** as a heatmap.

d Responses extracted from different challenges individually multiplied with each tag image. **e** Gaussian distributions of inter- and intra-HD (36 responses from 12 tags and 3 challenge pairs): The inter-HD distribution between 1260 combinations of response pairs and intra-HD distribution between 36 response pairs of same-bit sequences. **f** The equivalent representation of **e** as a heatmap.

$$(Intra - \text{hamming distance}(Intra - HD), \text{ if } B1 \text{ and } B2 \text{ are an equivalent response})$$

where, $B1_i$ and $B2_i$ are the i -th bits of the bit sequences $B1$ and $B2$, and l is the length of the sequences. An exclusive OR operation on bit sequences returns 0 if the $B1_i$ and $B2_i$ are equal, and 1 if they are different. Additionally, when $B1$ and $B2$ yield different responses, the result approaches an inter-HD close to 0.5, and, in equivalent response cases, an intra-HD close to 0 can be obtained. The inter-HD distribution plotted by comparing a pair of responses among 36 responses extracted from a single tag image is shown in Fig. 5b. The pair-wise hamming distance of the 36 responses in the form of a heat map is shown in Fig. 5c. Based on the analyzed pattern randomness through RMSE results, high randomness is achieved with 0.3 H_tD and 13° RA. However, comparative experiment was performed for 0.3 H_tD with 33° , 53° , 73° , and 93° RAs. As expected, the results for 0.3 H_tD and 13° RA condition are better as inter-HD is close to 0.5 with a low value (0.0139) of standard deviation (STD). The average and STD for all the RAs are summarized in Supplementary Fig. S11.

In general, to infer the data capacity of a bit sequence, the capacity can be calculated as 2^l using the bit sequence length (l) of the response^{49,50}, and, thus, the single tag has a nominal encoding capacity

of $2^{2048} (\approx 3.23 \times 10^{616})$. However, the capacity is only available in case all bits of the response are ideally distributed. Therefore, many systems consider the independent bit elements of a bit sequence, called degrees of freedom (DoF), to estimate the encoding capacity of a sequence that is not theoretically impeccable. The data capacity is estimated with 2^{DoF} ^{16,20,51,52}, and the DoF is calculated using the following Eq. (6):

$$\text{Degree of freedom}(DoF) = \mu(1 - \mu) / \sigma^2 \quad (6)$$

where μ and σ are the average and standard deviation values of the inter-HD distribution. The DoF of the single tag produced under 13° RA condition showed the highest value, and the estimated DoF is $1301 (\approx 0.4854 \times (1 - 0.4854) / (0.0139)^2)$ (Supplementary Information Fig. S11). Therefore, the data capacity of a single tag is estimated to be $4.36 \times 10^{391} (\approx 2^{1301})$ which means that the bit sequence response is distributed most randomly. To evaluate whether the degree of randomness according to the manufacturing conditions is random, the NIST (National Institute of Standards and Technology) statistical tests are additionally performed (Supplementary Table S2). The NIST test (NIST SP 800-22) consists of a total of 15 tests, but only 7 tests are conducted^{52,53} because the sequence length of the response is short (Table 1). The responses extracted from the 33° , 53° , 73° , and 93° RAs

Table 1 | NIST statistical tests for binary sequences generated from single (left) and multiple (right) tags

Statistical test	p-value rotation angle 13°	Proportion (p-value ≥ 0.01)	Result	Statistical test	p-value rotation angle 13°	Proportion (p-value ≥ 0.01)	Result
Frequency	1.0	144/144	Passed	Frequency	1.0	144/144	Passed
Block frequency	0.932342	142/144	Passed	Block frequency	0.447847	144/144	Passed
Run	0.929568	143/144	Passed	Run	0.906185	143/144	Passed
Longest run	0.210191	144/144	Passed	Longest run	0.015976	144/144	Passed
Serial	0.833228	144/144	Passed	Serial	0.983848	144/144	Passed
	0.459577	144/144	Passed		0.768684	144/144	Passed
Approximate entropy	0.959097	144/144	Passed	Approximate entropy	0.999181	143/144	Passed
Cumulative sums	0.999999	144/144	Passed	Cumulative sums	0.999999	144/144	Passed
	0.999999	144/144	Passed		0.999999	144/144	Passed

passed only five tests except for the block frequency and longest run test, confirming that the degree of randomness is insufficient (Supplementary Table S3). Nonetheless, the responses extracted under the 13° RA pass all seven tests, and through these results, the fact that responses with significant randomness can be extracted only under the 13° RA condition is confirmed. Even though the binary sequence extracted from the single tag image is unique and random, it will be problematic to utilize whenever the responses cannot be reproduced in the re-extraction process. Therefore, to evaluate reproducibility, the hamming distance between the equivalent responses, the intra-HD distribution, is analyzed (Fig. 5b). The intra-HD distribution has a very low average and standard deviation values of 0.029487 and 0.01466. In the case that different responses are compared, the average value is 0.48541, and, thus, the false positive and negative rates will also be quite low. To confirm the false rate, the intra- and inter-HD distributions are fitted to Gaussian plots, and the rates are calculated successfully. As a result, the false positive and negative rates are measured to 8.177×10^{-58} and 7.947×10^{-58} , and the results mean that the tag responses exhibit outstanding reproducibility.

In summary of a single tag case, diverse responses extracted by exploiting a single tag image and different challenges exhibited great characteristics of uniqueness, reproducibility, false rate, and randomness proven by hamming distance distributions and NIST statistical tests.

Performance of responses from multiple tags

The responses extracted by combining multiple challenges separately with a single tag image are verified by the hamming distance and NIST test. In addition, whether the responses extracted from multiple tags images have uniqueness, reproducibility, false rate, and randomness are also evaluated. In this test, 12 tags obtained for already proven 0.3 H₁D and 13° RA condition were utilized. The responses using different challenges individually multiplied with each tag image were extracted (Fig. 5d). Among these, 36 responses corresponding to a pair of 12 tag images and 3 challenges were collected, and the binary sequences also have a bit uniformity of 0.5. The total bit-sequence of 36 responses from 12 tags is shown in Supplementary Fig. S12. First, to validate the uniqueness, the inter-HD distribution is extracted (Fig. 5e). The inter-HD average and standard deviation values of the responses from multiple tags are more ideal than the responses from a single tag. The paired-wise hamming distance of the 36 responses in the form of a heat map is shown in Fig. 5f. Thus, the degree of freedom (DoF) is further increased compared to the DoF when a single tag is utilized. The overwhelming DoF value means that the responses extracted from multiple tags are more diverse and unique than responses from a single tag. The DoF of the responses from the multiple tags is $1722 \approx 0.4973 \times (1 - 0.4973) / (0.0120)^2$, and it means that the data capacity is estimated to be $2.36 \times 10^{518} \approx 2^{1722}$. The encoding capacity is about 10^{120} times higher than that of a single tag.

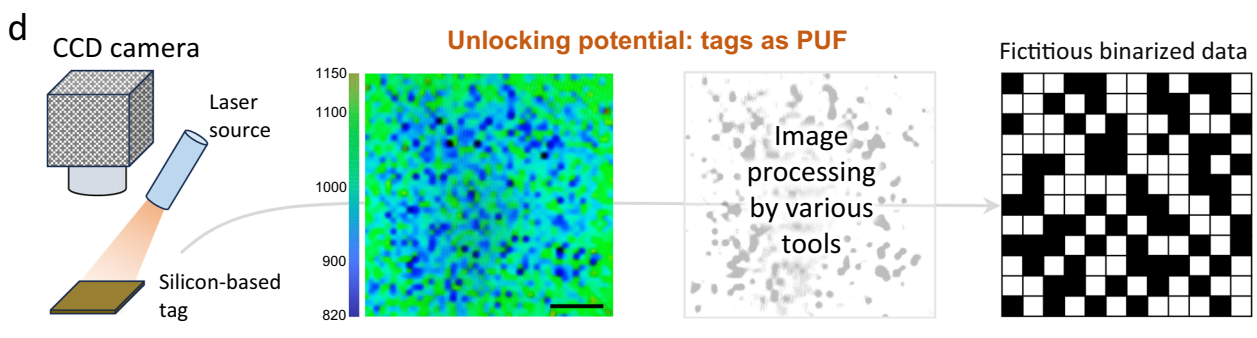
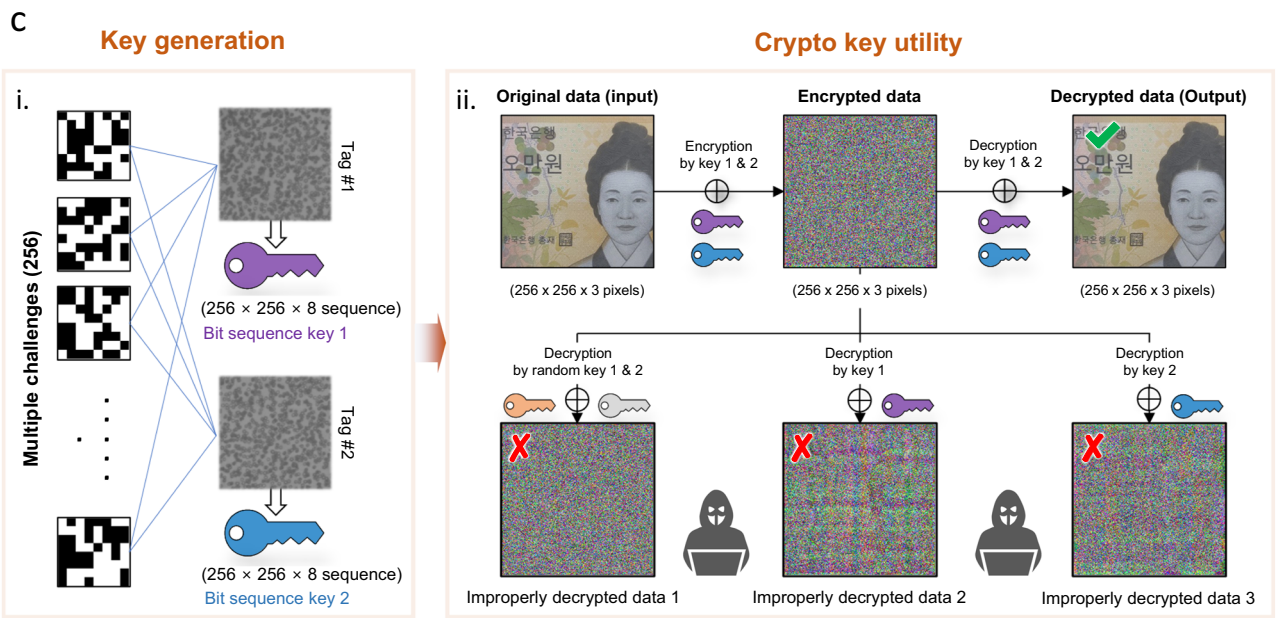
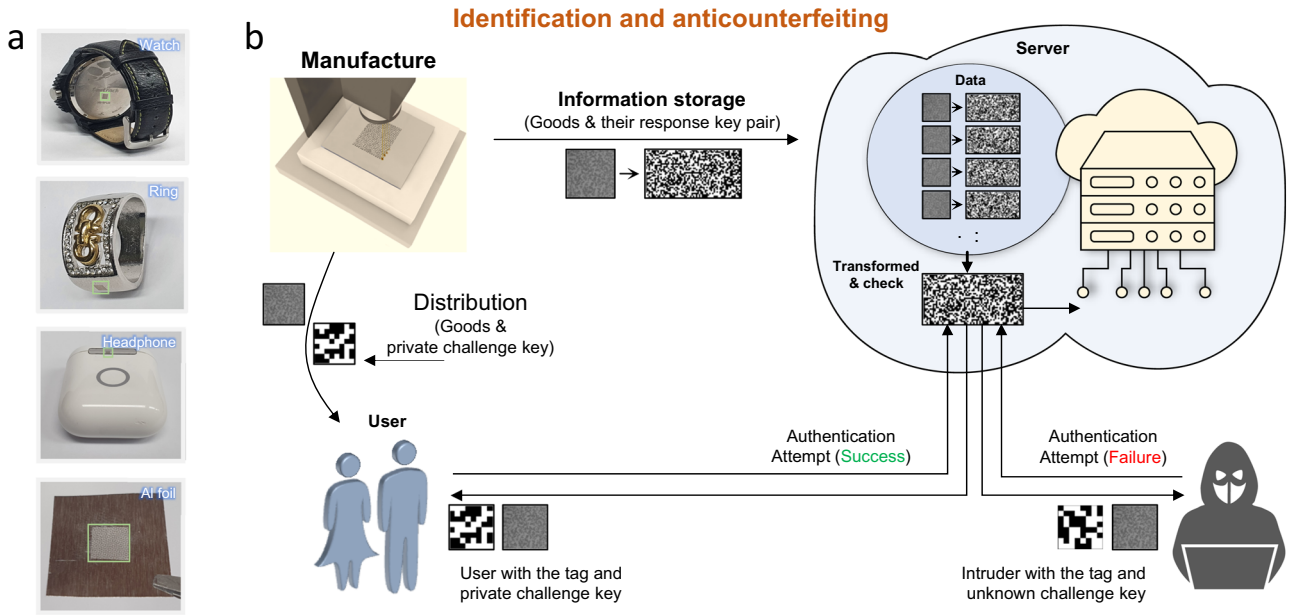
Subsequently, seven NIST statistical tests are conducted, and the responses pass all the NIST tests (Table 1). The result of the NIST test indicates that not only responses extracted from a single tag are random, but also binary sequences extracted from multiple tags are quite random. Similarly, the intra- and inter-HD distributions are measured to evaluate reproducibility and uniqueness (Fig. 5e, f). The intra-HD distribution has a low average and standard deviation values of 0.0095757 and 0.020772. To calculate the false positive and negative rate, the intra- and inter-HD distributions are Gaussian fitted, and the false positive and negative rates are 3.215×10^{-50} and 3.720×10^{-50} . The false rates are quite low even though the standard deviation of the intra-HD is slightly large.

In summary of multiple tags case, diverse responses extracted by exploiting 12 tags and a total of 3 different challenges exhibited uniqueness, reproducibility, false rate, and randomness similar to those responses extracted from a single tag.

Anticounterfeiting, crypto key generation, unclonability and stability

Physical tags relying only on optical images without utilizing additional intrinsic characteristics may be prone to clonable and therefore can only be usable as identification tags. However, authentication protocols involving private keys (challenges at the end-user/retailer/dealer) can prevent fake/unregistered tags associated with products. By this, the physical tags with private challenge keys can be used for anticounterfeiting purposes. Besides, the physical tags with keys generated from intrinsic characteristics can be coined as PUF tags^{20,54–56}. The utility of these tags for anticounterfeiting, crypto key generation, and PUF applications is shown in Fig. 6.

The possibility of the tags on real-world products for identification and/or anticounterfeiting applications is shown in Fig. 6a. The product's tag microscopic images are shown in Supplementary Fig. S13. Note that the background of microscopic images is unclear compared to the silicon background, this can be improvised by fabricating the tags on a polished flat surface. The tags can be either attached or can be fabricated intrinsically onto the products. The tag for anticounterfeiting applications is shown in Fig. 6b. The manufacturer fabricates tags and assigns an identifiable private challenge key to it. Afterward, the tag and its corresponding response information are registered in the data server, while the tag and its associated private challenge key are distributed to the user/retailer/dealer (Fig. 6b). During the authentication process, the data server verifies the product authenticity, brought up by either an authentic individual or intruder, by doing the multiplication operations of the tag's optical pattern with the private challenge. If an intruder attempts to verify by entering a random unregistered challenge or no challenge, the data server will authenticate the product as failure/unauthentic or unregistered. Through the process of distributing the private challenge keys associated with the product tags to the users, the tags/products can be authenticated securely.



In addition, let's understand the complexity involved from the intruder's side. If an intruder lacks encoding hardware and starts with only the response bits, he/she needs to iterate $\binom{N}{8} \binom{N-8}{8} \binom{N-16}{8} \binom{N-24}{8} \dots \binom{8}{8} \times (8!)^{N/8}$ times where N is the total number of elements as illustrated in Fig. 4d to c. Even if this can be tracked

down, there is another level of uncertainty in the reversed trend line extraction from Fig. 4c to b, leading to the additional complexity of the combinations to find out the correct unmasked areas as in Fig. 4b. Therefore, it is almost impossible to simulate a series of timely complex procedures for all possible challenge bits within a limited timeframe.

Fig. 6 | Tags for various purposes. **a, b** identification, authentication, **c** cryptography, and **d** PUF. **a** Direct intrinsic creation of tags on real-world products for identification application. **b** Overall schematic illustrating how products with anticounterfeiting tags and their associated private challenge keys are distributed to the users and how the authentication of products is executed by comparing the responses generated during the verification process with the responses stored in the database. **c** Key generation preparation for encryption and decryption in blockchain cryptography system: Crypto keys (1 and 2) generation by combining

256 challenges with the tags (1 and 2) separately; The generated sequence keys are successfully used to encrypt the image data without any sign of original input. Using the same keys decryption is possible while the randomly selected keys fail to decrypt the data to its original data. **d** The schematic illustrates the idea of using tags as PUF: The setup shows the PL imaging process, and then the obtained PL image (scale bar 250 μm) can be processed by various image processing tools, followed by binarization for efficient storage in the database.

The strategy towards the crypto key generation is shown in Fig. 6c. Random responses extracted by loading various challenges (private keys) onto the tags have yielded promising results, indicating that bit sequences can be a powerful method for encrypting and decrypting data. To encrypt and decrypt a 256×256 color image, a random $256 \times 256 \times 8$ -bit sequence key is generated by overlapping 256 challenges individually with two tags separately (as shown in Fig. 6ci). While the DoF of the bit sequence key extracted by an individual tag is 1301, the DoF is increased to 1722 by utilizing multiple tags. Therefore, encryption and decryption processes are attempted by applying a more random bit sequence key using two tags. Since the generated crypto keys are of a specific size that can only cover a single channel of color image data, the pristine crypto keys are applied directly to the red channel, while 90° and 180° rotated keys are used for the green and blue channels (Supplementary Fig. S14). This process can result in the construction of a key capable of encrypting and decrypting color image data.

To encryption of color image data, which has a size of $256 \times 256 \times 3$, with the generated crypto keys 1 and 2 using bit exclusive OR operation, is successfully executed (Fig. 6cii), and the encrypted data has been transformed to such a degree that recognizing the signs of pristine image characteristics is difficult. To restore the encrypted data, four key conditions are tested. In the first test, random keys 1 and 2 generated using a programming tool are used for the decryption process but fail to decrypt the original data. In the second and third tests, even though the decryption procedures are conducted using individual keys separately for complete decryption, both attempts failed. In the last test, the keys used for encryption are applied, and the encrypted data can be successfully restored to the original data. It has been verified that the bit sequences obtained from tags 1 and 2 can be successfully applied for data encryption and decryption.

Furthermore, stability assessments of the tags under harsh conditions (60°C , and underwater environments) were conducted for 40 repetitions. The results revealed that their intra-HD values remained close to an ideal value of 0, with approximately 0.036 and 0.021 for the responses from single and multiple tags, respectively (Supplementary Fig. S15).

Coming to the clonability of these tags, the duplication of tags may be possible to some extent by physical replication of 3D patterns using molding techniques, therefore, encapsulation of tags by PDMS elastomer has been utilized. Note that the efficient removal of silicon-based elastomers from the silicon-based tags is extremely difficult due to the presence of similar chemical composition constituents. Moreover, the Si used in this study is crystalline, and the crater pattern created on it can be extremely difficult to replicate on another crystalline Si sample. However, the possibility of creating physical patterns may still exist through sophisticated techniques. Therefore, it is essential to utilize the intrinsic characteristics of silicon such as photoluminescence (PL). By utilizing the Si PL, the clonability of PL imaging which means the clonability of the tag can be made extremely difficult. This means, that even if the physical device has been reproduced by sophisticated technique the intrinsic PL features remain unpredictable from the original optical images. PL imaging is a promising characterization tool as it

provides fast, contactless, and spatial-resolved imaging. Especially for Si, it has been widely used in the photovoltaic industry for the inspection of defects. The intensity of PL corresponding to physically similar-looking craters can vary at different locations due to variations in defect levels. These defect levels are associated with whether a single crater spot is ablated once or multiple times. The details of PL mapping are provided in the experimental section. The potential use of tags as PUF is schematically and pictorially illustrated in Fig. 6d. The PL image obtained by a BTI imaging tool is evident which shows different PL intensities at different locations. The PL image can be simplified using various image processing tools to convert it into its binarized form, which can then be stored in the database for authentication purposes. Thus, these tags hold promise for applications in anticounterfeiting, crypto key generation, and PUF technologies.

Discussion

The successful demonstration of pulsed laser-ablated random crater patterns on a 4-inch Si/SiO₂ wafer presents a potential step forward in the development of rapid processing of tags. By optimizing laser parameters, such as scanning line density, repetition rate, and speed, it was possible to transform predictable regular patterns into unpredictable irregular patterns. The process of digitalizing the tags crater pattern has an enabling feature with a bit uniformity of fixed 0.5. The uniqueness and reproducibility, evaluated through inter- and intra-HD for both the single tag and multiple tags cases, demonstrated impressive results. In the case of a single tag, the false positive and negative rates are on the order of approximately 10^{-58} . While in the case of multiple tags, the false positive and negative rates were approximately 10^{-50} . With the enabling challenge-response pair, digitalization, possibility of unclonability, and encryption and decryption factors, these tags have the potential to be used for identification, anticounterfeiting, and cryptography. The laser ablation technique offers numerous benefits, including rapid fabrication, facile processing, intrinsic tagging, user-friendly automation, and economy, and can be readily accessed by small- to large-scale product-based companies. This proposed technique can enable the development of a new variety of smart PUF tags.

Methods

Laser-irradiated random crater patterns

Initially, a Si/SiO₂ substrate was used to validate the random crater patterns created using a nanosecond pulsed infrared laser ($\lambda = 1064$ nm, INYA-20, In Lasers, Inc.) with a wavelength of 1064 nm. The laser parameters used to create random speckle patterns on Si/SiO₂ substrates were laser power 50%, frequency 20 kHz, speed 2000 mm/s, and pulse width 20 ns. Note, that a thin layer of PDMS was coated on Si/SiO₂ substrate to avoid duplication by molding.

Imaging

The crater patterns were photographed as color images with a size of 4800×3600 pixels by utilizing the cellSens (imaging software, Olympus) program connected with a charge-coupled device camera (DP73, Olympus), $4\times$ magnification objective lens (UPlanFL N, Olympus), and optical microscope (IX71, Olympus).

Extraction of outline circles and analysis

MATLAB software has proceeded using a laptop with Intel(R) Core(TM) i3-1005G1 CPU @ 1.2 GHz and 8GB RAM for analysis. All captured images were converted into single-bit images through the 'rgb2gray' and 'graythresh' functions. To automatically divide the entire pattern into the desired area, after checking the pixel resolution (0.73 μm per pixel) of the image, the area is divided into segments according to the resolution. By applying the 'imfindcircles' functions with 0.9 applied 'sensitivity' option to the transformed image, the center points and size of outline circles were obtained. In this step, the diameter of the outline circles was limited from 19 to 36.5 μm through the 'imfindcircle' option. To elicit the orientation of the detected object, the 'orientation' option of the 'regionprops' function was applied. Also, to extract the trend line angle data, 'hough' with a 2-degree interval applied the 'theta' option and 'houghpeaks' functions with 30% of the maximum value of the hough transform matrix applied the 'threshold' option was used. To check the number of outline circles according to the area, the center point of each outline circle was replaced with '1' for mapping, and then all the numbers of the corresponding region matrix were added through the 'sum' function. For the ratio of objects to total outline circles analysis, we simply adopted the function 'bwlabel' and the pattern map was transformed into a labeled matrix, and the number of objects could be checked by finding the maximum value in the matrix. To obtain the RMSE value of distributions, 'immse' and 'sqrt' functions were applied with analyzed data and uniform distribution.

Challenge-response pair generation

All crater pattern images were cropped to $1 \times 1 \text{ mm}^2$ size and converted into single-bit images through 'rgb2gray' and 'graythresh' functions. The challenge signal consisted of a 64-bit sequence, and, to multiply the image and challenge signal, the single-bit size of the signal was set to $0.1 \times 0.1 \text{ mm}^2$, thus, $0.8 \times 0.8 \text{ mm}^2$ area in the center of the image obtained and analyzed. Also, the images were compressed from 0.73 to 1.56 μm per pixel to shorten calculation time by the 'imresize' function. To extract distributions of trend line direction angles, the 'hough' function with a 2-degree interval applied the 'theta' option. After running the function, in total hundreds of trend lines were extracted from each area, and the distribution was constructed by dividing into 8 bins (elements) of 22.5 degrees from -90 to 90 degrees. To count the number of trend lines assigned to each element of distribution, the 'histc' function was exploited. After assigning integers to elements in order, the 'sort' function was applied for the ascending order sorting process. Then, the 'de2bi' function was used for converting decimal integers to binary bits, and, finally, by combining all bitwise elements into a group, a bit sequence response could be obtained.

False positive and negative rate calculation

The mean and standard deviation values of the two distributions on a histogram obtained by inter and intra-analysis were extracted. The rough distribution graphs were transformed to smoothly fitted distribution graphs by applying the extracted two values into the Gaussian distribution formula. The two improved distributions have a contact point between 0 and 1, and the positive and negative false rate was calculated based on the point of intersection. Especially, in the case of the image cross-correlation process, the worst value was set as the false rate between the obtained false positive and negative rates.

Data encryption and decryption process

To generate a bit sequence key, 256 challenges were applied to a single tag image, and a $256 \times 256 \times 8$ size key could be obtained. The binary sequence keys were converted into 8-bit unsigned integers by the 'bin2dec' function because color images consisted of 8-bit unsigned integers, thus, the keys transformed from $256 \times 256 \times 8$ bits to

256×256 pixels. Also, for generating 8-bit unsigned integer random keys to tamper encoded data, the 'randi' function is utilized. Finally, the 'bitxor' function was simply exploited to encrypt and decrypt original color image data.

Large area photoluminescence

BT Imaging R3 equipment was used to characterize the photoluminescence of the tag. Light source flux (photon flux) of $2.5 \times 10^{18} \text{ cm}^{-2} \text{ s}^{-1}$ with an exposure time of 10 s for over a size of 4-inch wafer was used for imaging.

Data availability

All raw data generated during the current study are available from the corresponding author upon request.

References

1. Yoon, B. et al. Recent functional material based approaches to prevent and detect counterfeiting. *J. Mater. Chem. C* **1**, 2388 (2013).
2. Clark, F. Rise in online pharmacies sees counterfeit drugs go global. *Lancet* **386**, 1327–1328 (2015).
3. Blackstone, E. A., Fuhr, J. P. & Pociask, S. The health and economic effects of counterfeit drugs. *Am. Heal. Drug Benefits* **7**, 216–224 (2014).
4. Paunescu, D., Fuhrer, R. & Grass, R. N. Protection and Deprotection of DNA-High-Temperature Stability of Nucleic Acid Barcodes for Polymer Labeling. *Angew. Chem. Int. Ed.* **52**, 4269–4272 (2013).
5. Mullard, A. DNA tags help the hunt for drugs. *Nature* **530**, 367–369 (2016).
6. Lin, C. et al. Submicrometre geometrically encoded fluorescent barcodes self-assembled from DNA. *Nat. Chem.* **4**, 832–839 (2012).
7. Gooch, J., Goh, H., Daniel, B., Abbate, V. & Frascione, N. Monitoring Criminal Activity through Invisible Fluorescent "Peptide Coding" Taggants. *Anal. Chem.* **88**, 4456–4460 (2016).
8. Duong, B. et al. Printed Multilayer Microtaggants with Phase Change Nanoparticles for Enhanced Labeling Security. *ACS Appl. Mater. Interfaces* **6**, 8909–8912 (2014).
9. Duong, B., Liu, H., Ma, L. & Su, M. Covert thermal barcodes based on phase change nanoparticles. *Sci. Rep.* **4**, 5170 (2015).
10. Dejneka, M. J. et al. Rare earth-doped glass microbarcodes. *Proc. Natl Acad. Sci.* **100**, 389–393 (2003).
11. Nicewarner-Peña, S. R. et al. Submicrometer Metallic Barcodes. *Science* **294**, 137–141 (2001).
12. Zhang, Y. et al. Multicolor Barcoding in a Single Upconversion Crystal. *J. Am. Chem. Soc.* **136**, 4893–4896 (2014).
13. Demirok, U. K., Burdick, J. & Wang, J. Orthogonal Multi-Readout Identification of Alloy Nanowire Barcodes. *J. Am. Chem. Soc.* **131**, 22–23 (2009).
14. Lee, J. et al. Universal process-inert encoding architecture for polymer microparticles. *Nat. Mater.* **13**, 524–529 (2014).
15. Smith, A. F., Patton, P. & Skrabalak, S. E. Plasmonic Nanoparticles as a Physically Unclonable Function for Responsive Anti-Counterfeit Nanofingerprints. *Adv. Funct. Mater.* **26**, 1315–1321 (2016).
16. Hu, Z. et al. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol.* **11**, 559–565 (2016).
17. Zheng, Y. et al. Unclonable Plasmonic Security Labels Achieved by Shadow-Mask-Lithography-Assisted Self-Assembly. *Adv. Mater.* **28**, 2330–2336 (2016).
18. Goorden, S. A., Horstmann, M., Mosk, A. P., Škorić, B. & Pinkse, P. W. H. Quantum-secure authentication of a physical unclonable key. *Optica* **1**, 421 (2014).
19. De Cremer, G. et al. Optical Encoding of Silver Zeolite Microcarriers. *Adv. Mater.* **22**, 957–960 (2010).

20. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical One-Way Functions. *Science* **297**, 2026–2030 (2002).
21. Bae, H. J. et al. Biomimetic Microfingerprints for Anti-Counterfeiting Strategies. *Adv. Mater.* **27**, 2083–2089 (2015).
22. Carro-Temboury, M. R., Arppe, R., Vosch, T. & Sørensen, T. J. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* **4**, e1701384 (2018).
23. Leem, J. W. et al. Edible unclonable functions. *Nat. Commun.* **11**, 328 (2020).
24. Im, H. et al. Chaotic Organic Crystal Phosphorescent Patterns for Physical Unclonable Functions. *Adv. Mater.* **33**, 2102542 (2021).
25. Liu, Y. et al. Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication. *Nat. Commun.* **10**, 2409 (2019).
26. Lee, D., Paeng, D., Park, H. K. & Grigoropoulos, C. P. Vacuum-Free, Maskless Patterning of Ni Electrodes by Laser Reductive Sintering of NiO Nanoparticle Ink and Its Application to Transparent Conductors. *ACS Nano* **8**, 9807–9814 (2014).
27. Han, S. et al. Fast Plasmonic Laser Nanowelding for a Cu-Nanowire Percolation Network for Flexible Transparent Conductors and Stretchable Electronics. *Adv. Mater.* **26**, 5808–5814 (2014).
28. Korkut, C. et al. Laser Crystallization of Amorphous Ge Thin Films via a Nanosecond Pulsed Infrared Laser. *Cryst. Growth Des.* **21**, 4632–4639 (2021).
29. Chae, H. et al. Laser-Processed Nature-Inspired Deformable Structures for Breathable and Reusable Electrophysiological Sensors toward Controllable Home Electronic Appliances and Psychophysiological Stress Monitoring. *ACS Appl. Mater. Interfaces* **11**, 28387–28396 (2019).
30. Gandla, S. et al. Ultrafast prototyping of large-area stretchable electronic systems by laser ablation technique for controllable robotic arm operations. *IEEE Trans. Ind. Electron.* <https://doi.org/10.1109/TIE.2021.3073355> (2021).
31. Jin, H. M. et al. Laser Writing Block Copolymer Self-Assembly on Graphene Light-Absorbing Layer. *ACS Nano* **10**, 3435–3442 (2016).
32. Strong, V. et al. Patterning and Electronic Tuning of Laser Scribed Graphene for Flexible All-Carbon Devices. *ACS Nano* **6**, 1395–1403 (2012).
33. Hawes, G. F., Yilman, D., Noremborg, B. S. & Pope, M. A. Supercapacitors Fabricated via Laser-Induced Carbonization of Biomass-Derived Poly(furfuryl alcohol)/Graphene Oxide Composites. *ACS Appl. Nano Mater.* **2**, 6312–6324 (2019).
34. Gandla, S. et al. Highly Linear and Stable Flexible Temperature Sensors Based on Laser-Induced Carbonization of Polyimide Substrates for Personal Mobile Monitoring. *Adv. Mater. Technol.* **5**, 2000014 (2020).
35. Samanta, A., Wang, Q., Shaw, S. K. & Ding, H. Roles of chemistry modification for laser textured metal alloys to achieve extreme surface wetting behaviors. *Mater. Des.* **192**, 108744 (2020).
36. Shin, W. et al. Shear-Assisted Laser Transfer of Metal Nanoparticle Ink to an Elastomer Substrate. *Material* **11**, 2511 (2018).
37. Park, K. I. et al. Highly-Efficient, Flexible Piezoelectric PZT Thin Film Nanogenerator on Plastic Substrates. *Adv. Mater.* **26**, 2514–2520 (2014).
38. Yeh, C.-H., Sung, P.-Y., Kuo, C.-H. & Yeh, R.-N. Robust laser speckle recognition system for authenticity identification. *Opt. Express* **20**, 24382 (2012).
39. Cowburn, R. Laser surface authentication – reading Nature’s own security code. *Contemp. Phys.* **49**, 331–342 (2008).
40. Wali, A. et al. Biological physically unclonable function. *Commun. Phys.* **2**, 39 (2019).
41. Hu, Y. et al. Flexible and Biocompatible Physical Unclonable Function Anti-Counterfeiting Label. *Adv. Funct. Mater.* **31**, 2102108 (2021).
42. Torun, N., Torun, I., Sakir, M., Kalay, M. & Onses, M. S. Physically Unclonable Surfaces via Dewetting of Polymer Thin Films. *ACS Appl. Mater. Interfaces* **13**, 11247–11259 (2021).
43. Park, J. et al. Disordered Heteronanostructures of MoS₂ and TiO₂ for Unclonable Cryptographic Primitives. *ACS Appl. Nano Mater.* **4**, 2076–2085 (2021).
44. Kim, J. H. et al. Nanoscale physical unclonable function labels based on block copolymer self-assembly. *Nat. Electron.* **5**, 433–442 (2022).
45. Kayaci, N. et al. Organic Light-Emitting Physically Unclonable Functions. *Adv. Funct. Mater.* **32**, 2108675 (2022).
46. Herrmann, R. F. W., Gerlach, J. & Campbell, E. E. B. Ultrashort pulse laser ablation of silicon: an MD simulation study. *Appl. Phys. A Mater. Sci. Process.* **66**, 35–42 (1998).
47. Bäuerle, D. *Laser Processing and Chemistry* (Springer Berlin Heidelberg, 2011) <https://doi.org/10.1007/978-3-642-17613-5>.
48. Nammi, S., Vasa, N. J., Balaganesan, G. & Mathur, A. C. Pulsed Laser Assisted Micro-Scribing of Metal thin Films in Air and Underwater Using UV, Visible and Near-IR Wavelengths. *Procedia Manuf.* **5**, 684–695 (2016).
49. Zhang, T. et al. Random Nanofracture-Enabled Physical Unclonable Function. *Adv. Mater. Technol.* **6**, 2001073 (2021).
50. Gu, Y. et al. Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels. *Nat. Commun.* **11**, 516 (2020).
51. Li, Q. et al. Intrinsic Random Optical Features of the Electronic Packages as Physical Unclonable Functions for Internet of Things Security. *Adv. Photonics Res.* **3**, 2100207 (2022).
52. Kim, M. S. et al. Revisiting silk: a lens-free optical physical unclonable function. *Nat. Commun.* **13**, 247 (2022).
53. Bassham, L. E. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=906762 (2010).
54. Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).
55. Babaei, A. & Schiele, G. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors* **19**, 3208 (2019).
56. Gao, Y., Al-Sarawi, S. F. & Abbott, D. Physical unclonable functions. *Nat. Electron.* **3**, 81–91 (2020).

Acknowledgements

This study was supported by the SKKU Research Fellowship Program of Sungkyunkwan University and the National Research Foundation of Korea (2021M3H4A1A02056037, 2018R1A6A1A03025708, 2021R1A2C2012680 and RS-2024-00448809). The authors thank Prof. Stefaan De Wolf and Dr. Anil Reddy Pininti from King Abdullah University of Science and Technology, Saudi Arabia for conducting photoluminescence imaging.

Author contributions

S.G. and J.Y. contributed equally to this research. S.G. and S.K. designed the work. S.G. carried out experiments. S.G., C.-W.Y. and S.K. analyzed the experimental data and J.Y. and W.P. contributed to analyzing the image processing. S.G. and J.Y. wrote the paper. H.J.L. provided valuable insights during the revision process.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41467-024-51756-1>.

Correspondence and requests for materials should be addressed to Wook Park or Sunkook Kim.

Peer review information *Nature Communications* thanks Yansong Gao and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2024