ADVANCED MATERIALS TECHNOLOGIES
www.advmattechnol.de

Iris-Inspired Microparticles with a Two-Factor Authentication Security Feature for Wet-Phase Enhanced Anti-Counterfeiting Strategies

Cheolheon Park, Minhyuk Lee, Hyeli Kim, Daewon Lee, Jangho Choi, Yeongjae Choi, and Wook Park**

This article presents an iris-mimicking polymeric microparticle with randomly generated silica film cracks to be utilized as a wet-phase micro security taggant. The microparticles are designed to replicate the capillary patterns in the human iris, providing high data capacity and stability, making them ideal for authentication. Furthermore, the microparticles integrate a QR code within the pupillary zone of the iris, enabling pupillary authentication to enhance two-factor identification and elevate overall security levels an unprecedented feature absent in conventional iris recognition systems. The resulting artificial iris-mimicking microparticles have high coding efficiency and unique characteristics and can be authenticated in the wet phase, making them suitable for use as micro security taggants.

1. Introduction

In the complex terrain of contemporary cybersecurity, counterfeiting poses challenges to multiple aspects of modern society,[1–7] including finances, public health, and social trust. To mitigate this risk, there is a growing need for highly secure technologies, such as unique device identifiers, trusted mutual authentication, and encrypted data transmission.[8–25] Encryption keys, such as physical unclonable functions (PUFs), which generate a hardware-based security key using unpredictable micro or nanostructures, are emerging as alternatives to software-based security systems. Previously, PUFs were mainly applied to dry-state goods, such as official documents, luxury products, and electronic devices. However, the need for PUFs has expanded to wet-state goods, following the broadened use of liquors, wet-phase cosmetics, medicines, and vaccines in modern society. Dry-phase PUFs can be applied to the carriers of liquid-state goods; however, they do not directly assign encryption to the goods themselves. By simply replacing or contaminating the liquid goods, the effectiveness of PUFs can be compromised and potentially exploited. Given that the majority of previously introduced PUFs only function under dry-state conditions and degrade or lose functionality in wet environments, the development of wet-phase PUFs is essential.

In this research, we developed artificial iris microparticles that mimic the unique characteristics of the human iris and exist only in a wet state (**Figure 1**). Iris recognition stands out among biometric authentication methods owing to its distinctive and stable data capacity, as well as its unparalleled level of security, making duplication impossible. Inspired by the distinctive features of the iris, we created a micro security taggant by applying polymeric microparticle fabrication and silica layer coating. This taggant generates random crack patterns ranging from nanometers to several micrometers, mirroring the pattern of capillaries in the human iris. By utilizing the high programmability of the fabrication process, we could precisely designate the region for these random crack patterns, emulating the shape of the iris. Additionally, we were able to incorporate a non-random code in the region without crack patterns within an identical taggant. Consequently, we introduced an additional security code by

C. Park
Bio-MAX Institute
Seoul National University
1 Gwanak-ro Gwanak-gu, Seoul 08826, Republic of Korea
M. Lee, H. Kim, W. Park
Department of Electronic Engineering
Kyung Hee University
Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea
E-mail: parkwook@khu.ac.kr
D. Lee
Department of Electronics Engineering
Myongji University
116, Myongji-ro, Yongin-si 17058, Republic of Korea
J. Choi, Y. Choi
School of Materials Science and Engineering
Gwangju Institute of Science and Technology (GIST)
Gwangju 61105, Republic of Korea
E-mail: yeongjae@gist.ac.kr
W. Park
Institute for Wearable Convergence Electronics
Kyung Hee University
Yongin 17104, Republic of Korea

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/admt.202400566

DOI: 10.1002/admt.202400566

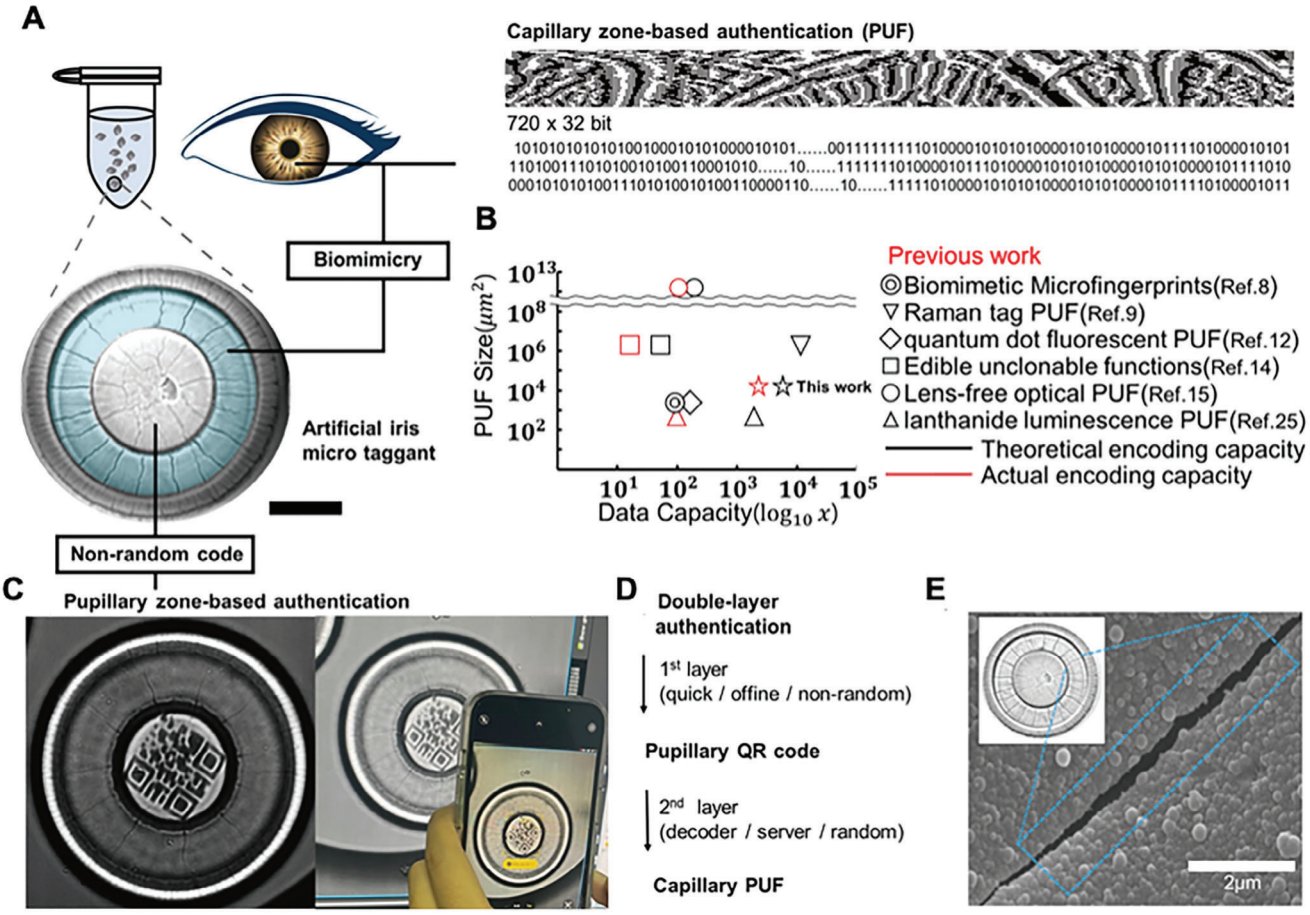

Figure 1. Artificial iris-mimicking microparticle. A) Comparison of the area of the artificial iris-mimicking microparticle with the real iris and binary code from the iris recognition algorithm. B) Comparison of the data capacity between PUFs presented in other papers and artificial iris-mimicking microparticles. C) Pictures of a particle with a QR code on it and a particle recognizing the QR code. D) Two-factor authentication algorithm. E) SEM image of artificial iris-mimicking microparticle can identify cracks in the particle (scale bar: 2 μm).

embedding a QR code into the pupillary zone of the iris, providing support for dual identification. Artificial iris microparticles can authenticate information via a QR code in the pupil area, with each particle possessing a unique code through a random pattern in the iris area. This taggant boasts high coding efficiency, compatibility with existing biometric decoders, and exceptional security features, including two-factor authentication for wet phase decoding.

The proposed artificial iris-mimicking microparticles and iris recognition share the same authentication process (Figure 1A). The microparticles resemble the iris, being divided into a capillary zone and a pupillary zone. The capillary zone, characterized by random patterns of capillaries, is used for feature extraction during authentication. Our artificial iris-mimicking microparticles replicate these capillary patterns by forming cracks in the capillary zone. These cracks are stable and persist even through hydration and dehydration cycles. Consequently, the microparticles can be authenticated in a wet environment, making it possible to store them in liquid form. The authentication procedure for the artificial iris-mimicking microparticles involves several steps. First, the iris region is segmented from the captured image; then, it is normalized. Next, feature extraction is performed, followed by encoding of the extracted features into a binary code. The resulting code is subsequently compared to a database to complete the authentication process. The binary code generated from the authentication process has a sequence of 32×720 bits, resulting in an encoding capacity of 2^{23040} ($\approx 5.3839 \times 10^{6935}$):

$$\text{Encoding capacity} = C^s \tag{1}$$

Alternatively, the encoding capacity can be determined using the concept of degrees of freedom and represents the independently operating bits within the bit sequence. In this calculation, the encoding capacity of the artificial iris-mimicking microparticles is found to be 2^{4588} ($\approx 1.3354 \times 10^{1381}$):

$$\text{Degrees of Freedom} = \frac{\mu(1-\mu)}{\sigma^2} \tag{2}$$

Despite being comparable to other PUFs, the proposed system reduces the volume occupied by the authentication application (Figure 1B). This makes the microparticles suitable for

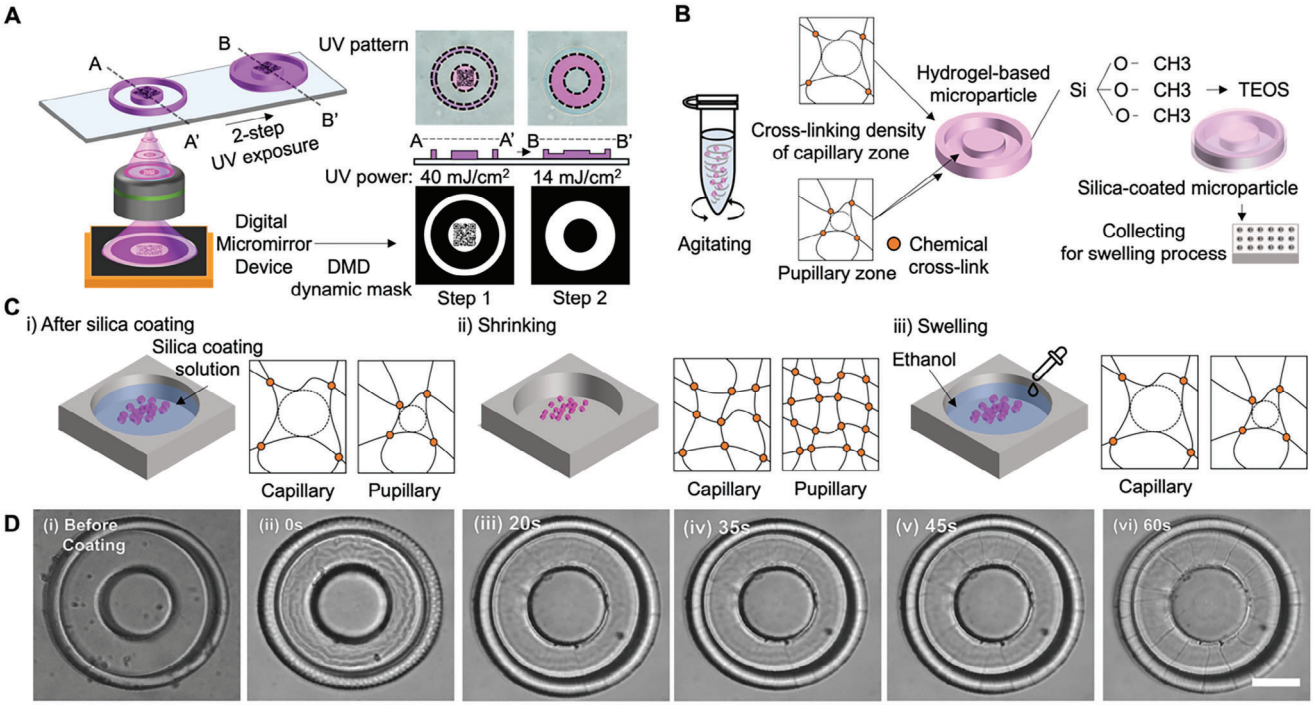

Figure 2. Fabrication of artificial iris-mimicking microparticle. A) Fabrication of polymeric microparticles with two heights using DMD dynamic mask. B) Process of silica coating and appearance of particles immediately after silica coating. C) Crack generation process after changing the cross-linking densities. D) Crack generation process according to swelling time (scale bar: 50 μm).

authenticating small objects, such as micro devices or limited amounts of drugs. The original iris recognition process does not take advantage of the pupillary zone. To address this issue, our system incorporates a QR code into the pupillary zone to enable two-factor identification (Figure 1C). This additional step of pupillary authentication provides basic information and can be performed in environments without an authentication database or communication (Figure 1D). Consequently, this two-factor identification provides an added level of security.

2. Fabrication

The manufacturing process of artificial iris particles can be divided into three steps: synthesis of polymeric microparticles using maskless photolithography,[18,19,26] addition of a silica layer to the surface of the fabricated polymer particles, and crack patterning of silica-coated particles through hydration–dehydration (**Figure 2**).[20] In the first step, shape and height differences between the capillary and pupillary zones are introduced during the photopatterning of polymeric particles by controlling crosslinking density through light irradiation time. The capillary zone is fabricated with a low height and high elastic modulus, whereas the pupillary zone is fabricated with a greater height. The photolithography process facilitates real-time changes to the ultraviolet (UV) pattern, offering high degrees of programmability and freedom (Figure 2A). In the second step, a silica layer is introduced onto the surface of the polymer particles, generating a core-shell structure with a hard silica layer on the surface and a hydrogel with a high elastic modulus inside (Figure 2B). Finally, in the third step, the silica-coated particles are sprayed onto a well-plate, and crack patterning is performed through hydration-dehydration. Dehydration is performed first, followed by hydration. The silica layer shrinks on the surface while the hydrogel inside expands, causing cracking in the capillary zone where the most mismatched strain occurs (Figure 2C). The cracks form randomly from the pupillary zone rim to the outer ring (Figure 2D).

The phenomenon of cracks not being generated in the areas of microparticles that were created with a longer UV exposure time can be rationalized based on the Flory–Rehner theory,[21–23] which describes the swelling behavior of crosslinked polymers in a solvent. The Flory–Rehner theory provides a relationship between the equilibrium swelling ratio (Q) of a crosslinked polymer network and the crosslinking density (ρ) within the network. This theory is based on the assumption that the polymer network behaves as an ideal elastic network and considers the number of crosslinks and the interaction between the solvent molecules and the polymer chains. According to the Flory–Rehner theory, the equilibrium swelling ratio (Q) can be expressed as

$$Q = \frac{V_s}{V_0} \propto \frac{1}{\rho}, \tag{3}$$

where V_s is the swollen volume of the hydrogel (microparticles in this case), V_0 is the initial volume of the hydrogel (microparticles), ρ is the actual crosslinking density within the hydrogel (microparticles).

A longer UV exposure time during fabrication leads to a higher crosslinking density within the microparticles. Based on the Flory–Rehner theory, when the crosslinking density (ρ) increases, the equilibrium swelling ratio (Q) decreases (Note S1,

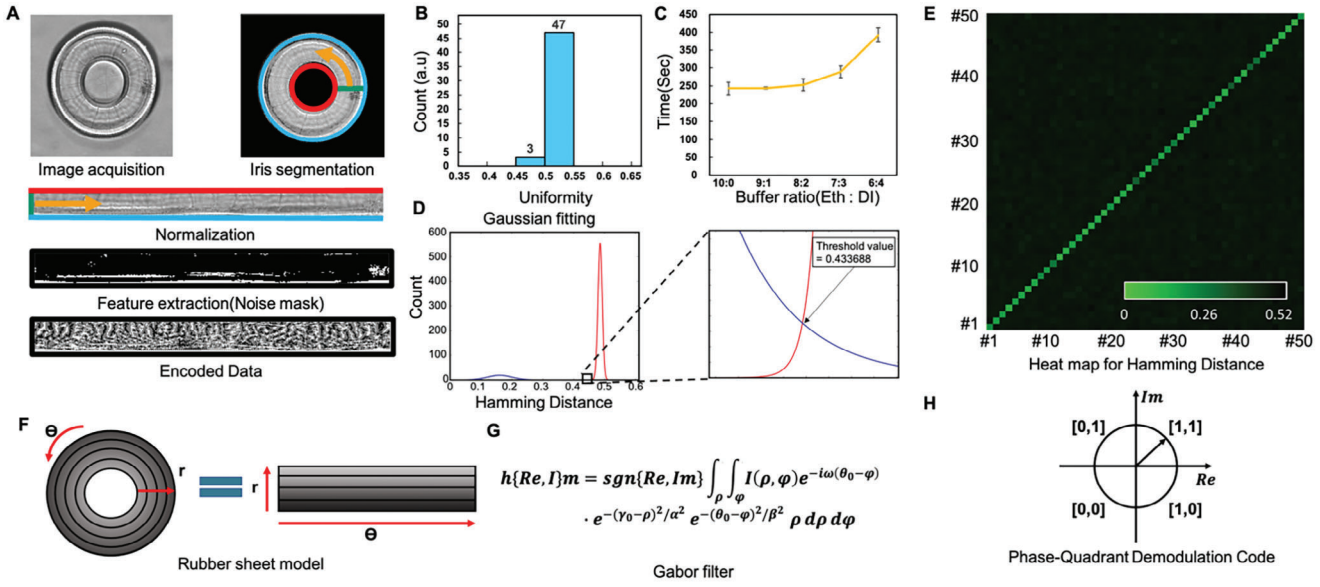

Figure 3. Authentication system of iris-mimicking microparticles. A) Process of authentication of iris-mimicking microparticles. B) Histogram showing the uniformity values of 50 iris-mimicking microparticles. C) Graph depicting the swelling time of artificial iris-mimicking microparticles as a function of the ratio of ethanol and DI water. D) Graph of a Gaussian fit based on the Hamming distance value obtained by comparing 50 different particles. E) Heatmap based on Hamming distance values. F) Schematic of rubber sheet model. G) The formula for the Gabor filter. H) Phase-quadrant demodulation code.

Supporting Information). In other words, a higher crosslinking density results in reduced swelling of the microparticles in ethanol. With lower swelling, the pressure exerted by the solvent (ethanol) on the silica layer is reduced in the areas with higher crosslinking density. This reduced pressure likely prevents the formation of cracks in those regions because the stress caused by swelling is diminished. In contrast, the areas with lower crosslinking densities within the microparticles have higher equilibrium swelling ratios and experience greater pressure from the solvent during ethanol-induced swelling. This increased pressure can lead to the formation of random cracks in the silica layer in these regions. Therefore, the difference in crosslinking density within the microparticles, induced by the variation in UV exposure time, is the key factor contributing to the selective generation of cracks in the silica layer during ethanol-induced swelling. The cross-linking density of the relatively weakly UV-irradiated capillary zone and the cross-linking density of the pupillary zone and the outer line of the artificial iris are approximately shown in Figure 2C. The change in cross-linking density during the silica coating process and iris patterning is roughly shown in Figure 2C,D, and detailed data can be found in Figure S1 (Supporting Information).

2.1. Analysis of Iris-Mimicking Microparticle

The artificial iris-mimicking microparticles developed in this study undergo the same authentication process as iris recognition (**Figure 3**).[24,27] Iris recognition technology is based on the unique pattern of the iris, which serves as a biometric identifier. In iris recognition, an image of the iris is captured and computer algorithms are used to extract features from the iris pattern (Figure 3A; Note S2, Supporting Information), such as the distance between features, their relative size, and orientation. These extracted features are then compared to a database of known iris patterns to determine a match.

Similarly, the authenticity of our artificial iris-mimicking microparticles was determined based on the cracks, which are distinctive patterns found in the donut-shaped capillary zone (Figure 3A; Note S2.1, Supporting Information). First, the iris area was separated from the particle image and normalized to 32×360 through a rubber sheet model (Figure 3F; Note S2.2, Supporting Information). In the normalized image, a Gabor filter (Figure 3G) was used to extract the crack characteristics. The extracted bit was then encoded into two bits through phase-quadrature demodulation code (Figure 3H), yielding a bit sequence of 32×720 (Note S2.3, Supporting Information). Bit uniformity is a metric that determines the distinguishability of a PUF. It is defined as the ratio of ones to zeros in a binary key and is considered ideal when it is equal to 50%. This suggests that PUFs produced using the same method can be differentiated. The formula for computing bit uniformity is as follows:

$$\text{Bit uniformity} = \frac{1}{s}\sum_{l=1}^{s} K_l \tag{4}$$

K_l is the lth binary bit of the key and s is the total size of the key. In our study, the average bit uniformity of the keys of the 50 artificial iris-mimicking microparticles produced was 0.5147, which indicates that these particles can be uniquely distinguished (Figure 3B).

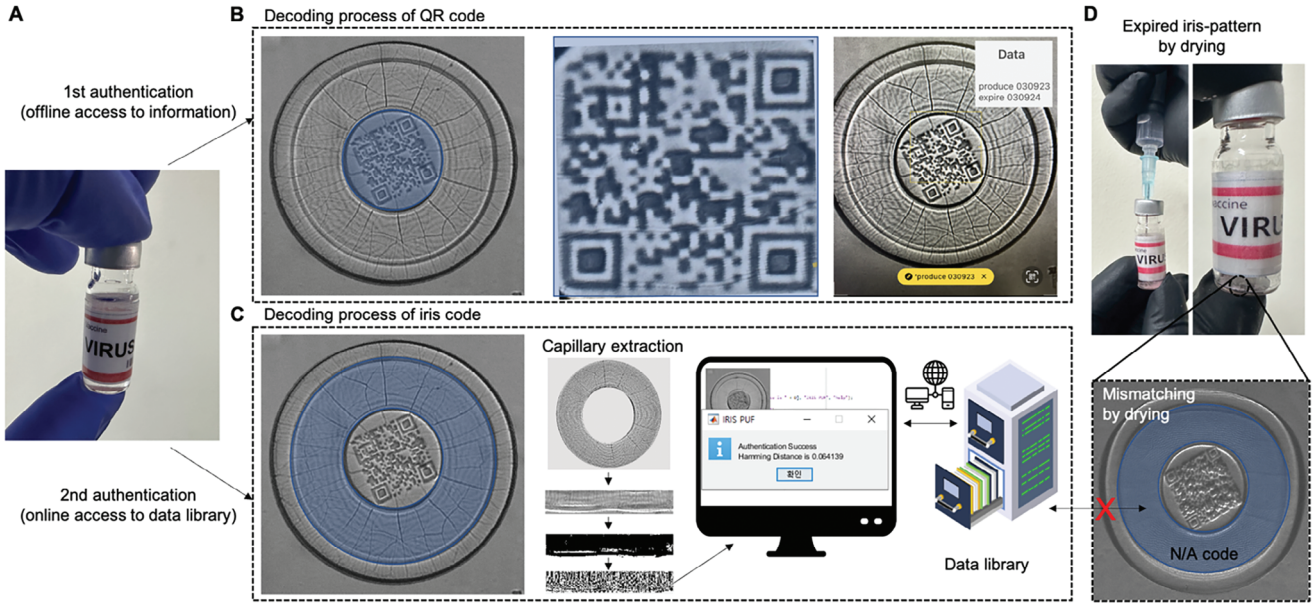

Figure 4. Application of wet-phase authentication. A) Artificial iris registered in the data library in the vial filled with virus; iris regions can be masked for authentication by matching against data libraries. B) QR codes in the pupillary zone allow for offline access to information. C) Decoding of iris code and iris code authentication through comparison with the data library of the server. D) After using the vial, the remaining artificial iris particles in the vial do not match the data in the library (Note S3; Figure S2, Supporting Information).

The Hamming distance in a PUF represents the number of bit positions where two responses of the PUF differ. In other words, the Hamming distance between two PUF responses is the difference between them.[28] A lower Hamming distance indicates similarity, whereas a higher Hamming distance indicates dissimilarity. The formula for the Hamming distance is

$$\text{Hamming Distance} \quad (\text{HD}) = \frac{\#\left(K_i \neq K_j\right)}{s} \tag{5}$$

K_i and K_j are the ith and jth binary bits of the key, respectively, and s is the total size of the key. The heatmap in Figure 3E shows the Hamming distances of the 50 artificial iris-mimicking microparticles, which demonstrates that each particle can be uniquely distinguished, consistent with the bit uniformity value. The mean of the inter-hamming distance with Gaussian fitting is 0.1896 with a standard deviation of 0.0389, and the mean of the intra-hamming distance with Gaussian fitting is 0.4855 with a standard deviation of 0.0069.

2.2. Wet-Phase Authentication

The developed micro taggant can be used for two-factor authentication in the wet phase (**Figure 4**). In the final stage of authentication, the PUF must establish communication with the server that stores the code, which renders the authentication information unknown until after communication occurs. To overcome this challenge, we integrated a non-communication authentication method into the PUF as a two-factor authentication system. This objective was achieved by inserting a QR code into the pupillary zone, which was not previously utilized for iris recognition. We introduced not only two-factor authentication, but also wet-phase authentication to address the limitations of conventional authentication systems, including PUFs, which are primarily used in the dry phase. To date, there have been no reported cases of PUFs that directly tag expensive liquids, such as drugs or cosmetics, and are able to confirm reuse or duplication of the contents without modification.

To verify the applicability of our two-factor authentication system for microparticles in the wet phase, we initiated an authentication process within a vial containing liquid medicine (Figure 4A). The QR code in the pupillary zone was generated through UV irradiation after inserting the QR code image into the digital micromirror device (DMD) of the maskless lithography system (Figure 4B). The QR code serves as the first part of authentication, providing manufacturing information for liquid goods, and this step can be completed without requiring an external connection for authentication. The artificial iris particles were fabricated and patterned with cracks (Figure 4C). As the second step of authentication, the cracks underwent iris authentication through detection under a microscope and were matched with the data library, thereby enhancing the security level of authentication. Notably, the artificial iris particles retained their patterns in the vial even after the cracks were introduced. However, upon drying fully, the cracks resulting from over-swelling contracted and became undetectable (Figure 4D and S2, Supporting Information). The artificial iris particles underwent a change in volume when the solvent was dried or underwent a transformation in properties from their original state. Consequently, variations in contraction between the silica layers resulted in alternative shapes, sizes, and thicknesses of cracks. This characteristic implies that any illicit activities, such as tampering with drugs during the distribution process, could prevent authentication.

3. Discussion

We developed a novel PUF based on a biomimetic iris for use with iris recognition, a biometric authentication method commonly used on human irises. Our artificial iris particles are generated by inducing unique and random cracking patterns, a consequence of mismatched strain during the manufacturing process. These distinctive cracking patterns, inherently unreplicable, form the basis for an authentication mechanism within the PUF. Additionally, an extra layer of authentication is provided by the incorporation of a QR code in the pupillary zone. Our proposed artificial iris particles, when in a wet state, exhibit unique crack patterns that serve as authentication features. This characteristic provides a unique security feature not available in other platforms, as the authentication codes cannot be matched with the database unless liquid is introduced. It is expected that the application of deep learning algorithms, which are commonly used in iris recognition systems to analyze patterns and process large amounts of data, will further enhance the security and data storage capabilities of our proposed artificial iris-mimicking microparticles.

4. Experimental Section

Photolithography: Before photolithography, a polydimethylsiloxane-coated glass slide with a 45 µm spacer was prepared, and the photocurable polymer was spread over it. The DMD (Texas Instruments) was then used to pattern the UV light from the UV source (Lightningcure LC8, Hg-Xe lamp, Hamamatsu) into the desired shape.[10,29] Artificial pupil particles were produced by two steps of photolithography using a 7:3 volume ratio of poly(ethylene glycol) diacrylate (PEGDA, Mn≈700, Aldrich) and 3-(trimethoxysilyl)propyl acrylate (TMASPA, Aldrich) was used as a alkoxysilane-grafted photocurable resin with 10 vol% of Irgacure 1173 (BASF) as the photoinitiator. The height difference between two regions was created by adjusting the UV irradiation time on the two masks. A pupillary zone surrounding the capillary zone and an outer area were produced with a dose of 40 mJ cm^{-2}, and the capillary zone was produced with a dose of 14 mJ cm^{-2}. The resulting particles were harvested by centrifugation, and silica coating was performed to produce a multilayer structure.

Silica Coating: The coating solution used consisted of tetraethyl orthosilicate (TEOS, 98%, Aldrich), ethyl alcohol anhydrous (99%, Daejung), deionized (DI) water, and ammonium hydroxide (25%–28%, Daejung), with a volume ratio of 25:4:1. In this experiment, 0.1 ml of TEOS was injected into a mixture of 20 ml of ethanol, 3.2 ml of DI water, and 0.8 ml of ammonium hydroxide and vortexed every 20 min until a total of 0.4 ml had been injected (total of 80 min). Subsequently, the coating solution was used to perform washing and 0.1 ml of TEOS was again injected into a mixture of 20 ml of ethanol, 3.2 ml of DI water, and 0.8 ml of ammonium hydroxide and vortexed every 20 min until a total of 0.4 ml had been injected (total of 80 min).[30]

Supporting Information

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

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (NRF-2022R1C1C2006949, NRF-2018R1A6A1A03025708, NRF-2021R1A2C2012680, NRF-2022M3C1A3081366, NRF-2022R1C1C1010938).

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Y.C. and W.P. contributed equally to this work. C.P. and M.L. performed conceptualization. M.L., H.K., and C.Y. performed the methodology. C.P., M.L., D.L., and J.C. performed an investigation. C.P., C.Y., and W.P. performed supervision. C.P., M.L., C.Y., and W.P. Wrote—original draft. C.P., M.L., D.L., C.Y., and W.P. Wrote—reviewed and edited the manuscript.

Data Availability Statement

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

Keywords

Biomimetics, iris mimicking, wet-phase authentication

Received: April 11, 2024
Revised: July 8, 2024
Published online: July 31, 2024

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, *IEEE Access* **2019**, *7*, 82721.
[2] T. M. Fernández-Caramés, P. Fraga-Lamas, *IEEE Access* **2018**, *6*, 32979.
[3] M. Frustaci, P. Pace, G. Aloi, G. Fortino, *IEEE Internet Things J.* **2018**, *5*, 2483.
[4] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, H. Tenhunen, *IEEE J. Biomed. Heal. Informatics* **2018**, *22*, 1711.
[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, *IEEE Internet Things J.* **2017**, *4*, 1125.
[6] A. Mosenia, N. K. Jha, *IEEE Trans. Emerg. Top. Comput.* **2017**, *5*, 586.
[7] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, *IEEE Internet Things J.* **2017**, *4*, 1250.
[8] 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.
[9] Y. Gu, C. He, Y. Zhang, L. Lin, B. D. Thackray, J. Ye, *Nat. Commun.* **2020**, *11*, 516.
[10] T. Ma, T. Li, L. Zhou, X. Ma, J. Yin, X. Jiang, *Nat. Commun.* **2020**, *11*, 1811.
[11] 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.
[12] M. Xie, G. Lin, D. Ge, L. Yang, L. Zhang, J. Yin, X. Jiang, *ACS Mater. Lett.* **2019**, *1*, 77.
[13] J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, *Nat. Commun.* **2020**, *11*, 328.
[14] M. S. Kim, G. J. Lee, J. W. Leem, S. Choi, Y. L. Kim, Y. M. Song, *Nat. Commun.* **2022**, *13*, 247.
[15] W. H. Grover, *Sci. Rep.* **2022**, *12*, 7452.
[16] H. Kim, G. Kwon, C. Park, J. You, W. Park, *Micromachines* **2022**, *13*, 168.
[17] B. W. Reichardt, F. Unger, U. Vazirani, *Nature* **2013**, *496*, 456.
[18] S. E. Chung, W. Park, H. Park, K. Yu, N. Park, S. Kwon, *Appl. Phys. Lett.* **2007**, *91*, 041106.

[19] C. Park, H. J. Bae, J. Yoon, S. W. Song, Y. Jeong, K. Kim, S. Kwon, W., Park, *ACS Omega* **2021**, *6*, 2121.
[20] J. B. Kim, P. Kim, N. C. Pégard, S. J. Oh, C. R. Kagan, J. W. Fleischer, H. A. Stone, Y.-L. Loo, *Nat. Photonics* **2012**, *6*, 327.
[21] R. G. M. van der Sman, *Food Hydrocoll.* **2015**, *48*, 94.
[22] C. G. Lopez, W. Richtering, *Soft Matter* **2017**, *13*, 8271.
[23] N. Boon, P. Schurtenberger, *Phys. Chem. Chem. Phys.* **2017**, *19*, 23740.
[24] J. Daugman, *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 21.
[25] M. R. Carro-Temboury, R. Arppe, T. Vosch, T. J. Sørensen, *Sci. Adv.* **2018**, *4*, 1701384.
[26] Y. Choi, C. Park, A. C. Lee, J. Bae, H. Kim, H. Choi, S. w Song, Y. Jeong, J. Choi, H. Lee, S. Kwon, W. Park, *Nat. Commun.* **2021**, *12*, 4724.
[27] L. Masek, *Report*, School of Computer Science and Software Engineering, The University of Western Australia, Perth Australia **2003**.
[28] B. W. Waggener, W. M. Waggner, *Pulse Code Modulation Techniques*, Springer Science & Business Media, Tiergartenstrasse 17, Heidelberg **1995**.
[29] S. Han, H. J. Bae, J. Kim, S. Shin, S.-E. Choi, S. H. Lee, S. Kwon, W. Park, *Adv. Mater.* **2012**, *24*, 5924.
[30] L. N. Kim, M. Kim, K. Jung, H. J. Bae, J. Jang, Y. Jung, J. Kim, S. Kwon, *Chem. Commun.* **2015**, *51*, 12130.