Next-Generation Biometric Security Against Fingerprint Spoofing

UBio-X LiveGuard Sets a New Standard for Liveness-Based Protection

White Paper 2026
UNION biometrics Co., Ltd.

Contents

Executive Summary

Fingerprint recognition has long been adopted as a fast, convenient, and highly personal biometric authentication method. It is now widely used across finance, access control, workforce management, public services, healthcare, education, and data center environments, where accurate user verification is essential.

However, as fingerprint-based authentication expands across industries, fingerprint spoofing has become a practical security risk. Conventional fingerprint authentication systems mainly verify whether the entered fingerprint pattern matches the registered template. This creates a structural limitation: if the fingerprint pattern can be replicated, the system may not be able to distinguish a fake fingerprint from a real human finger.

Spoof fingerprints made from materials such as silicone, gelatin, latex, wax, or conductive rubber can imitate the external pattern of a fingerprint. In high-security environments, even a single successful spoofing attempt can lead to unauthorized access, attendance manipulation, financial fraud, data leakage, or compliance violations. Therefore, the security standard for fingerprint authentication must evolve beyond recognition speed and matching accuracy.

Next-generation fingerprint security must verify not only the shape of the fingerprint, but also whether the fingerprint is being entered by a living human finger. In other words, liveness detection is becoming a critical requirement for reliable biometric authentication.

UBio-X LiveGuard addresses this challenge with heartbeat signal-based fingerprint spoofing detection technology. By analyzing both fingerprint patterns and heartbeat signals during the authentication process, UBio-X LiveGuard helps detect fake fingerprints and authenticate only real, living fingers.

This white paper explains why fingerprint authentication must move beyond recognition accuracy toward spoofing defense. It also examines the certified spoof fingerprint defense performance of UBio-X LiveGuard, based on testing against various spoof fingerprint materials and authentication scenarios.

UBio-X LiveGuard

Next-Generation Multimodal Biometric Authentication with Face and Heartbeat-Based Fingerprint Recognition

01 Background: Fingerprint Spoofing Has Become a Real-World Industrial Risk

Biometric authentication has long been regarded as one of the most personal and difficult-to-replicate methods of authentication. In particular, fingerprint recognition has been widely adopted across various industrial environments, including financial transactions, access control, workforce management, public services, healthcare institutions, and educational facilities, due to its fast authentication speed and high user convenience.

However, as the use of fingerprint recognition has expanded, attackers have begun to target fingerprints themselves. The key issue is that fingerprints cannot be easily changed or reissued like passwords. Once fingerprint information is exposed, users cannot simply replace it at will. If the fingerprints of high-privilege users, facility administrators, financial users, researchers, or public-sector personnel are compromised, the risk can persist over the long term.

In India, for example, attackers reportedly used fingerprints and Aadhaar information obtained from publicly available land and registry records to create fake fingerprints, which were then abused for financial transactions through the Aadhaar Enabled Payment System. The attackers are known to have withdrawn approximately 35 lakh rupees from victims' accounts using replicated fingerprints, and investigators seized hundreds of cloned fingerprints and biometric devices during the investigation (Dilshad, 2026).

This case shows that fake fingerprints are not merely a laboratory-level possibility, but a real attack method that can lead to actual financial damage.

Fingerprint-based authentication bypass has also emerged as a practical issue in public and border security. In Japan, a Chinese woman was reportedly able to bypass biometric immigration screening by surgically altering her fingerprints (Heussner, 2009).

This demonstrates that even when attackers do not directly replicate another person's fingerprint, public security procedures can still be bypassed if fingerprint-based authentication systems fail to sufficiently verify whether the biometric input comes from a real, living person.

In Germany, a hacker affiliated with the Chaos Computer Club also claimed to have reproduced the fingerprint of then German Defense Minister Ursula von der Leyen using only high-resolution photographs (Hern, 2014). This case shows that fingerprint information is no longer exposed only through physical contact with surfaces, but can also be obtained from high-resolution images, public photographs, and media materials.

Technical studies have also repeatedly demonstrated the feasibility of fingerprint spoofing attacks. In one study involving five commercial fingerprint scanners, researchers tested various spoof materials, including wax, latex, silicone, and adhesive. The study found that four out of the five devices were vulnerable to at least one type of spoof material (Kauba et al., 2020). In a separate experiment conducted by Cisco Talos, researchers also created fake fingerprints and confirmed that they could bypass various fingerprint authentication devices, including smartphones, laptops, and locks (Ventura et al., 2020).

The key message from these cases is clear. The risk of fingerprint recognition technology does not come from fingerprints themselves, but from authentication structures that rely only on fingerprint patterns. The shape of a fingerprint can be replicated. Therefore, next-generation fingerprint authentication must verify not only the fingerprint pattern, but also whether the fingerprint is being entered by a real, living human finger.

Fingerprints are no longer beyond replication.
As spoofing threats become real, authentication must go beyond pattern matching
and verify the true liveness of every fingerprint input.

02 The Weakness of Fingerprint Authentication: Patterns Are Replicable

Conventional fingerprint authentication systems mainly operate by comparing the pattern of an input fingerprint image with the registered fingerprint data. While this method is effective for fast authentication of legitimate users, it can have structural limitations against fingerprint spoofing attacks.

Materials such as silicone, gelatin, latex, adhesive, and conductive rubber can reproduce the ridges and valleys of a fingerprint — in other words, its external pattern — with a relatively high level of precision. If an authentication device only checks the fingerprint pattern and does not sufficiently verify live biometric responses, a spoof material may be mistaken for a real human finger.

In high-security industries, this risk does not stop at a simple authentication failure. In financial institutions, it can lead to fraudulent transactions. In data centers and research facilities, it can result in the leakage of critical information.

In manufacturing facilities, it can compromise production security, while in workforce management environments, it can enable proxy attendance or attendance manipulation. In public institutions and healthcare organizations, it can further escalate into issues involving the protection of personal and sensitive information.

Therefore, the standard for fingerprint recognition security can no longer remain limited to fast authentication speed and high recognition accuracy. The focus must shift from how quickly a legitimate user can be recognized to how accurately forged biometric information can be distinguished and blocked.

03 Core Strength of UBio-X LiveGuard: World's Forst Heatbeat Signal-Based Fingerprint Spoofing Detection

UBio-X LiveGuard applies a multi-layered biometric authentication technology that combines fingerprint pattern recognition with heartbeat signal analysis to defend against fingerprint spoofing attacks. The core concept is not simply to verify whether the shape of a fingerprint matches the registered data, but to also analyze whether live biometric signals are detected from the input finger.

A spoof fingerprint may be able to imitate the external pattern of a fingerprint. However, it is difficult to replicate the heartbeat-based biometric signals generated by a living human finger. UBio-X LiveGuard focuses on this difference. By using heartbeat signal analysis to identify spoof fingerprints that are difficult to distinguish through fingerprint pattern recognition alone, it accurately verifies only real, living fingers.

This fundamentally expands the standard of conventional fingerprint authentication. While traditional methods focus on whether the fingerprint pattern matches, UBio-X LiveGuard verifies both whether the fingerprint pattern matches and whether live biometric signals are present.

In other words, it is a dual-verification structure that simultaneously checks both the fingerprint pattern and the biometric response.

This structure significantly strengthens defense against fingerprint spoofing attacks. Even if an attacker reproduces a fingerprint pattern using materials such as silicone, gelatin, latex, or conductive rubber, authentication becomes difficult to pass if the heartbeat signal generated by a real finger is not detected.

Therefore, UBio-X LiveGuard is not simply a fingerprint recognition terminal, but a next-generation biometric security device designed with fingerprint spoofing attacks in mind. This technology is especially meaningful in high-security environments. In data centers, research facilities, financial institutions, public agencies, healthcare organizations, and manufacturing facilities, where authentication bypass can lead to serious consequences, spoofing defense is more important than simple convenience.

Through heartbeat signal-based liveness verification, UBio-X LiveGuard raises the level of trust in fingerprint authentication and presents a new standard for biometric security.

KISA Spoof Fingerprint Defense Performance Test – Grade 1

UBio-X LiveGuard has achieved the highest rating (Grade 1) in the Spoof Fingerprint Defense Performance Test conducted by K-NBTC (Korea National Biometric Test Center) of the Korea Internet & Security Agency.

Certification : Spoof Fingerprint Defense Performance – Grade 1
Certification Period : < 1 year

KISA Korea Internet & Security Agency

K-NBTC Korea National Biometric Test Center

CERTIFICATE

Certificate No. : KISA-FD-2025-001
Company : UNION biometrics Co., Ltd. Representative : SHIN, YO-SIK
Location : 127, Beobwon-ro, Songpa-gu, Seoul, Korea
Certified Product : UBio-X LiveGuard
Category : Biometric/Spoof Detection Anti-Spoof Device | Grade 1
Period of Validity : 2025.04.29 ~ 2026.04.28
Test Organization : Korea National Biometric Test Center K-NBTC

Test organization is to certify that the above product is appropriately qualified for the criteria of biometric system certification.

April 29, 2025

Korea Internet & Security Agency

04 Authentication Process: Simultaneous Analysis of Fingerprint Patterns and Heatbeat Signals

The fingerprint spoofing detection process of UBio-X LiveGuard can be understood as a four-step authentication flow.

1. Fingerprint Pattern Recognition:

The Sensor Scans the finger's ridge patterns and compares it with the registered fingerprint data to verify the user's identity

2. Heartbeat Signal Detection:

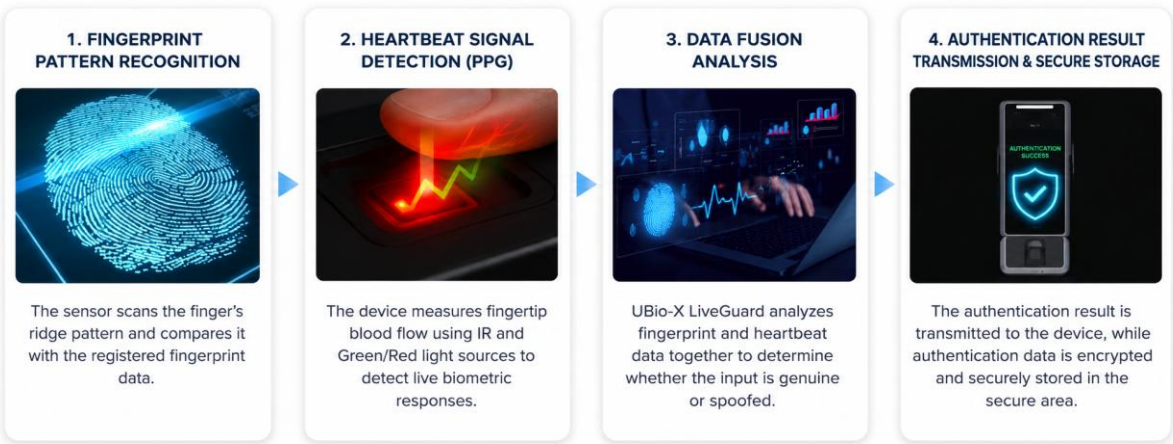
The device measures blood flow responses at the fingertip using IR and green/red light sources. In a living finger, changes in blood flow may cause variations in reflected light. However, spoof materials such as silicone, gelatin, conductive rubber, film, and paper cannot easily reproduce these biometric responses.

3. Data Fusion Analysis:

UBio-X LiveGuard analyzes fingerprint and heartbeat data together to determine whether the input is genuine or spoofed.

4. Authentication Result Transmission and Secure Storage:

The authentication result is transmitted to the device, while authentication data is encrypted and securely stored to protect integrity and security..



05 Fingerprint Spoofing Defense Performance Verified by Certified Testing

The reliability of fingerprint spoofing defense technology cannot be proven through feature descriptions or internal testing alone. The results of fingerprint spoofing attacks can vary depending on the spoof material, fingerprint quality, sensor type, and registration and authentication procedures. Therefore, to adopt fingerprint recognition-based authentication in high-security industries such as finance, public institutions, data centers, and research facilities, objective test results that reflect various spoof materials and real-world attack scenarios are required.

UBio-X LiveGuard verified its fingerprint spoofing defense performance through the spoof biometric fingerprint performance test conducted by the Korea National Biometric Test Center (K-NBTC) of the Korea Internet & Security Agency. In this test, UBio-X LiveGuard received Grade 1, Excellent, in the spoof biometric fingerprint defense performance evaluation. This means that its defense performance against fingerprint spoofing attacks was confirmed in an official testing environment (K-NBTC, 2025).

The test was conducted using various materials that could be used in real fingerprint spoofing attacks. The spoof fingerprint samples included paper, OHP film, silicone A, silicone B, silicone C, silicone D, gelatin, conductive rubber, and clay. Each sample was configured with different thickness, color, and moisture content to reflect multiple types of spoof fingerprint attack possibilities, rather than a single material type.

The test also included both normal user environments and spoofing attack environments. It covered not only the normal scenario of registering and authenticating with a real fingerprint, but also scenarios in which a real fingerprint was registered and authentication was attempted with a spoof fingerprint, as well as scenarios in which a spoof fingerprint was registered and then used again for authentication. This structure was designed to verify not only the authentication stage, but also the possibility of forged biometric information entering the system during the registration stage.

These test results clearly demonstrate the security significance of UBio-X LiveGuard. The reliability of a fingerprint recognition system is not determined only at the authentication stage. If forged biometric information is entered during the initial registration stage, the entire authentication system can be compromised. Therefore, the ability to detect and block spoof fingerprints throughout both registration and authentication is a core requirement for biometric authentication security.

Detects Various Fingerprint Spoofing Attempts

UBio-X LiveGuard reliably detects various types of fake fingerprints crafted from different materials.

Paper | Gelatin | Conductive Rubber | Silicone | OHP Film

06 Balancing Security and Usability

Fingerprint spoofing defense technology must not only block attacks, but also maintain reliable authentication performance for legitimate users. Even if a system strongly blocks spoof fingerprints, frequent rejection of real users during fingerprint registration or authentication can cause inconvenience and delays in real-world environments such as access control, workforce management, financial authentication, and public services.

UBio-X LiveGuard is designed to maintain a stable authentication flow for legitimate users while applying fingerprint spoofing defense. In normal use scenarios, where a real fingerprint is registered and authenticated with a real fingerprint, it demonstrated stable registration and authentication performance. This shows that the technology is designed to balance both security and usability.

In authentication environments such as access control and workforce management, where users authenticate multiple times a day, security functions must not interfere with operational efficiency. By strengthening fingerprint spoofing defense while preserving the authentication experience for legitimate users, UBio-X LiveGuard presents a biometric security model that can be applied to both high-security environments and daily operational settings

07 Industrial Impact and Practical Value

Fingerprint recognition-based authentication is already used across various industries, including finance, access control, workforce management, public services, healthcare institutions, research facilities, and data centers. However, in authentication structures that rely mainly on fingerprint patterns, fingerprint spoofing attacks can become a risk factor that undermines authentication trust.

UBio-X LiveGuard's heartbeat signal-based fingerprint spoofing detection technology carries significant value in these industrial environments. While fingerprint patterns can be replicated, it is difficult to reproduce the biometric signals generated by a living human finger. By verifying both fingerprint patterns and heartbeat signals, UBio-X LiveGuard provides practical defense against fingerprint spoofing attacks.

In financial institutions, it can help prevent account takeover and fraudulent transactions. In data centers and research facilities, it can strengthen access control for high-privilege areas. In manufacturing facilities and logistics centers, it can help prevent attendance manipulation and proxy authentication. In public institutions and healthcare organizations, it can enhance the reliability of access control for sensitive information.

Ultimately, fingerprint spoofing defense technology is not merely a device-level feature, but a security infrastructure that strengthens the reliability of the entire authentication system. Considering that biometric information cannot be easily changed once exposed, the ability to detect and block spoof fingerprints in advance will become an essential security requirement in the future biometric authentication environment.

08 New Standard for Fingerprint Authentication: From Recognition Accuracy to Spoofing Defense

Fingerprint recognition has traditionally been evaluated by speed, accuracy, and user convenience. However, as biometric authentication expands into high-security industries, recognition performance alone is no longer enough.

Today, fingerprint systems must verify not only whether a fingerprint matches registered data, but also whether it comes from a real, living person. UBio-X LiveGuard addresses this need with the world's first heartbeat signal-based fingerprint spoofing detection technology, identifying spoof fingerprints that are difficult to detect through pattern recognition alone.

This shifts the standard of fingerprint authentication from simply identifying "whose fingerprint it is" to verifying "whether it is a real, living fingerprint." With Grade 1, Excellent, certification from K-NBTC, UBio-X LiveGuard demonstrates that spoofing defense is becoming a core requirement for next-generation biometric security.

Based on heartbeat signal-based liveness verification and certified spoof fingerprint defense performance, UBio-X LiveGuard presents a new standard for trusted fingerprint authentication in high-security industries.

UBio-X LiveGuard

Next-Generation Multimodal Biometric Authentication with Face and Heartbeat-Based Fingerprint Recognition

09 Reference

Dilshad, M. (2026, February 12). *When thumbprints aren't safe: Scamsters clone fingerprints from tehsil records to siphon bank funds*. The Times of India. https://timesofindia.indiatimes.com/city/agra/when-thumbprints-arent-safe-scamsters-clone-fingerprints-from-tehsil-records-to-siphon-bank-funds/articleshow/128219392.cms

Heussner, K. M. (2009, December 10). *Surgically altered fingerprints help woman evade immigration*. ABC News. https://abcnews.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505

Hern, A. (2014, December 30). *Hacker fakes German minister's fingerprints using photos of her hands*. The Guardian. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

Kauba, C., Debiasi, L., & Uhl, A. (2020). *Enabling fingerprint presentation attacks: Fake fingerprint fabrication techniques and recognition performance*. arXiv. https://doi.org/10.48550/arXiv.2012.00606

Korea-National Biometric Test Center. (2025, April 29). *위조 생체인식(지문) 성능 시험 결과보고서: UBio-X LiveGuard* (Certification No. KISA-BD-2025-002). Korea Internet & Security Agency.

Rascagneres, P., & Ventura, V. (2020, April 8). *Fingerprint cloning: Myth or reality?* Cisco Talos Blog. https://blog.talosintelligence.com/fingerprint-research/

Address

12F, Daemyung Valeon bldg.,
127, Beobwon-ro, Songpa-gu,
Seoul, 05836, Republic of Korea

Contact

Email: onlinemarketing
@unionbiometrics.com