



# 위조지문 공격에 대응하는 차세대 생체인증 보안

UBio-X LiveGuard가 제시하는 위조지문 방어력의 새로운 기준

White Paper 2026  
UNION biometrics Co., Ltd.



## 목차

---

- 1 Executive Summary: 핵심 요약
- 2-3 Background: 위조지문은 이미 현실의 산업 리스크가 되었다
- 4 기존 지문인증의 한계: 패턴은 복제될 수 있다
- 5 UBio-X LiveGuard의 핵심 차별성: 세계 최초 심박 신호 기반 위조지문 탐지
- 6 인증 프로세스: 지문 패턴과 심박 신호를 동시에 분석하다
- 7 공인 시험으로 검증된 위조지문 방어 성능
- 8 보안성과 사용성의 균형
- 8 산업 현장에서의 의미
- 9 차세대 지문인증의 기준: 인식률을 넘어 위조 방어력으로
- 10 Reference

# Executive Summary: 핵심 요약

지문인식은 오랫동안 빠르고 편리한 생체인증 방식으로 활용되어 왔다. 금융, 출입통제, 근태관리, 공공 서비스, 의료기관, 데이터센터 등 다양한 산업 영역에서 지문인식은 사용자의 신원을 확인하는 핵심 인증 수단으로 자리 잡았다. 그러나 생체인증의 활용 범위가 넓어질수록 공격자는 더 이상 비밀번호나 카드만을 노리지 않는다. 이제 공격의 대상은 인증 수단 그 자체, 즉 사람의 생체정보로 이동하고 있다.

특히 위조지문 공격은 지문 패턴만 확인하는 기존 인증 구조의 한계를 직접적으로 겨냥한다. 실리콘, 젤라틴, 라텍스, 전도성 고무와 같은 재질은 지문의 외형적 패턴을 모방할 수 있으며, 일부 지문인식 장비는 이를 실제 손가락으로 오인할 수 있다. 고보안 환경에서 단 한 번의 인증 우회는 정보 유출, 부정 출입, 근태 조작, 금융 피해, 규제 위반으로 이어질 수 있다.

이러한 위협에 대응하기 위해 지문인식 보안은 단순히 “등록된 지문과 일치하는가”를 확인하는 수준을 넘어야 한다. 앞으로의 지문인증은 “입력된 지문이 실제 살아있는 사람의 손가락에서 나온 것인가”를 함께 검증해야 한다. 즉, 지문의 모양뿐 아니라 살아있는 생체 반응까지 확인하는 복합 생체인증 구조가 필요하다.

UBio-X LiveGuard는 이러한 보안 요구에 대응하기 위해 개발된 위조지문 방어형 생체인증 단말기다. 특히 UBio-X LiveGuard는 세계 최초 심박 신호 기반 위조지문 탐지 기술을 통해, 지문 패턴 인식만으로는 구별하기 어려운 위조지문을 살아있는 손가락의 생체 신호 분석으로 판별한다. 지문 위·변조를 방지하기 위해 지문 패턴과 심박 신호를 함께 검증함으로써, 실제 살아있는 손가락만을 정확하게 식별하는 것이 핵심이다.

본 백서는 위조지문 공격 사례와 연구 결과를 바탕으로, 지문인식 보안이 단순한 인식을 중심으로 위조 방어력 중심으로 이동해야 하는 이유를 설명한다. 또한 UBio-X LiveGuard의 K-NBTC 위조 생체인식 지문 성능 시험 결과를 통해, 다양한 위조지문 재질과 등록·인증 시나리오에서 검증된 방어 성능을 살펴본다.

UBio-X LiveGuard는 해당 시험에서 위조 생체인식 지문 방어력 성능평가 1등급, 우수 평가를 획득했다. 이는 차세대 지문인식 시스템의 기준이 단순한 인증 속도와 편의성을 넘어, 위조된 생체정보를 식별하고 차단하는 방어력으로 확장되고 있음을 보여준다.

## UBio-X LiveGuard

얼굴인식 단말기에 심박 신호 기반 복합 지문 인증을 탑재한  
차세대 멀티모달 생체인증 단말기

# 01 Background: 위조지문은 이미 현실의 산업 리스크가 되었다



생체인증은 오랫동안 “가장 개인적이고, 가장 복제하기 어려운 인증 수단”으로 인식되어 왔다. 특히 지문인식은 빠른 인증 속도와 높은 사용 편의성 덕분에 금융 거래, 출입통제, 근태관리, 공공 서비스, 의료기관, 교육기관 등 다양한 산업 현장에 널리 도입되어 왔다.

그러나 지문인식의 활용 범위가 확대되면서 공격자들은 지문 자체를 공격 대상으로 삼기 시작했다. 문제는 지문이 비밀번호처럼 쉽게 변경하거나 재발급할 수 있는 정보가 아니라는 점이다. 한 번 유출된 지문 정보는 사용자가 임의로 바꿀 수 없으며, 고위 권한자나 시설 관리자, 금융 사용자, 연구원, 공공기관 담당자의 지문이 노출될 경우 장기적인 인증 리스크로 이어질 수 있다.

실제로 인도에서는 공개된 토지·등기 기록에서 확보한 지문과 Aadhaar 정보를 이용해 위조지문을 만들고, 이를 Aadhaar Enabled Payment System 기반 금융 거래에 악용한 사건이 발생했다. 공격자는 복제된 지문을 통해 피해자들의 계좌에서 약 35 lakh 루피를 인출한 것으로 알려졌으며, 수사 과정에서 수백 개의 복제 지문과 생체인식 장비가 압수되었다(Dilshad, 2026). 이 사례는 위조지문이 실험실 수준의 가능성이 아니라 실제 금융 피해로 이어질 수 있는 공격 수단임을 보여준다.

공공·국경 보안 영역에서도 지문 기반 인증 우회는 현실적인 문제로 나타났다. 일본에서는 한 중국인 여성이 지문을 외과적으로 변형해 일본 입국 심사의 생체인식 절차를 우회한 사례가 보도되었다(Heussner, 2009).

이는 공격자가 반드시 타인의 지문을 복제하지 않더라도, 지문 기반 인증 체계가 생체의 진위 여부를 충분히 검증하지 못할 경우 공공 보안 절차가 우회될 수 있음을 보여준다.

또한 독일에서는 Chaos Computer Club 소속 해커가 고해상도 사진만을 이용해 당시 독일 국방장관 Ursula von der Leyen의 지문을 재현했다고 발표했다(Hern, 2014). 이 사례는 지문 정보가 더 이상 물리적으로 접촉한 표면에서만 유출되는 것이 아니라, 고해상도 이미지, 공개 사진, 미디어 자료를 통해서도 노출될 수 있음을 보여준다.

기술 연구에서도 위조지문 공격 가능성은 반복적으로 검증되고 있다. 상용 지문 스캐너 5종을 대상으로 한 연구에서는 왁스, 라텍스, 실리콘, 접착제 등 다양한 위조 재질을 이용한 실험에서 5개 장비 중 4개가 최소 하나 이상의 위조 재질에 취약한 것으로 확인되었다(Kauba et al., 2020). Cisco Talos의 실험에서도 연구진은 위조지문을 제작해 스마트폰, 노트북, 자물쇠 등 다양한 지문 인증 장치를 우회할 수 있음을 확인했다(Ventura et al., 2020).

이러한 사례들이 말하는 핵심은 단순하다. 지문인식 기술의 위험은 지문 자체가 아니라, 지문 패턴만을 신뢰하는 인증 구조에서 발생한다. 지문의 모양은 복제될 수 있다. 따라서 차세대 지문인증은 지문의 모양뿐 아니라, 그 지문이 실제 살아있는 사람의 손가락에서 입력된 것인지까지 확인해야 한다.

지문은 더 이상 복제 불가능한 정보로만 볼 수 없습니다.  
고해상도 이미지, 유출된 생체정보, 인공 재질을 활용한 위조지문 공격은  
이미 현실의 보안 위협이 되고 있습니다.  
이제 인증 보안은 단순히 지문의 모양이 일치하는지를 확인하는 단계를 넘어,  
그 지문이 실제 살아있는 사람의 손가락에서 입력된 진짜 생체 신호인지까지  
검증해야 합니다.

”

## 02 기존 지문인증의 한계: 패턴은 복제할 수 있다

기존 지문인증은 주로 입력된 지문 이미지와 등록된 지문 데이터의 패턴 일치 여부를 비교하는 방식으로 작동한다. 이 방식은 정상 사용자의 빠른 인증에는 효과적이지만, 위조지문 공격에는 구조적인 한계를 가질 수 있다.

실리콘, 젤라틴, 라텍스, 접착제, 전도성 고무와 같은 재질은 지문의 융선과 골, 즉 외형적 패턴을 비교적 정교하게 재현할 수 있다. 만약 인증 장비가 입력된 지문의 패턴만 확인하고 실제 생체 반응을 충분히 검증하지 못한다면, 위조된 재질이 실제 손가락으로 오인될 가능성이 있다.

특히 고보안 산업군에서는 이러한 위험이 단순한 인증 실패에 그치지 않는다. 금융기관에서는 부정 거래로, 데이터센터와 연구소에서는 중요 정보 유출로, 제조시설에서는 생산 보안 침해로, 근태관리 환경에서는 대리 출근이나 근태 조작으로 이어질 수 있다. 공공기관과 의료기관에서는 개인정보와 민감정보 보호 문제로 확대될 수 있다.

따라서 지문인식 보안의 기준은 더 이상 빠른 인증 속도와 높은 인식률에만 머물러서는 안 된다. 이제 중요한 질문은 “정상 사용자를 얼마나 빠르게 인식하는가”가 아니라 “위조된 생체정보를 얼마나 정확하게 구분하고 차단하는가”다.



## 03 UBio-X LiveGuard의 핵심 차별성: 세계 최초 심박 신호 기반 위조지문 탐지

UBio-X LiveGuard는 위조지문 공격에 대응하기 위해 지문 패턴 인식과 심박 신호 분석을 결합한 복합 생체인증 기술을 적용했다. 핵심은 단순히 지문 모양이 등록된 정보와 일치하는지를 확인하는 것이 아니라, 입력된 손가락에서 살아있는 사람의 생체 신호가 감지되는지를 함께 분석하는 것이다.

위조지문은 지문의 외형적 패턴을 흉내 낼 수 있다. 하지만 살아있는 손가락에서 발생하는 심박 기반 생체 신호까지 동일하게 재현하기는 어렵다. UBio-X LiveGuard는 바로 이 차이에 주목한다. 지문 패턴만으로는 구별하기 어려운 위조지문을 심박 신호 분석을 통해 판별함으로써, 실제 살아있는 손가락만을 정확하게 식별한다.

이는 기존 지문인증의 기준을 근본적으로 확장한다. 기존 방식이 “지문 패턴의 일치 여부”를 중심으로 했다면, UBio-X LiveGuard는 “지문 패턴의 일치 여부”와 “살아있는 생체 신호의 존재 여부”를 함께 검증한다.

즉, 지문의 모양과 생체 반응을 동시에 확인하는 이중 검증 구조다.

이러한 구조는 위조지문 공격에 대한 방어력을 크게 강화한다. 공격자가 실리콘, 젤라틴, 라텍스, 전도성 고무 등으로 지문 패턴을 재현하더라도, 실제 손가락에서 발생하는 심박 신호가 확인되지 않으면 인증을 통과하기 어렵다. 따라서 UBio-X LiveGuard는 단순한 지문인식 단말기가 아니라, 위조지문 공격을 전제로 설계된 차세대 생체인증 보안 장치라고 할 수 있다.

특히 이 기술은 고보안 환경에서 중요한 의미를 갖는다. 데이터센터, 연구소, 금융기관, 공공기관, 의료기관, 제조시설처럼 인증 우회가 심각한 피해로 이어질 수 있는 곳에서는 단순한 편의성보다 위조 방어력이 더욱 중요하다. UBio-X LiveGuard는 심박 신호 기반 라이브니스 검증을 통해 지문인증의 신뢰 수준을 한 단계 높이며, 생체인증 보안의 새로운 기준을 제시한다.

### KISA 위조 지문 방어력 성능 시험 1등급

한국인터넷진흥원 K-NBTC(바이오인식정보시험센터)의 위조 바이오인식(지문) 방어력 성능시험에서 최고 등급인 1등급을 획득했습니다.

인증 등급 : 위조 바이오인식(지문) 방어력 1등급

인증 시간 : <1초



## 04 인증 프로세스: 지문 패턴과 심박 신호를 동시에 분석하다

UBio-X LiveGuard의 위조지문 탐지는 네 단계의 인증 흐름으로 이해할 수 있다.

### 1. 지문 패턴 인식 단계:

센서가 손가락의 융선 패턴을 스캔하고, 등록된 지문 데이터와의 일치 여부를 확인한다. 이 단계는 기존 지문인식의 기본 구조에 해당하며, 사용자의 신원 확인을 위한 1차 판단 기준이 된다.

### 2. 심박 신호 감지 단계:

단말기는 IR 및 Green/Red 광원을 통해 손끝의 혈류 반응을 측정한다. 살아있는 손가락에서는 혈류 변화에 따른 반사율 변화가 나타날 수 있지만, 실리콘, 젤라틴, 전도성 고무, 필름, 종이와 같은 위조 재질에서는 이러한 생체 반응을 재현하기 어렵다.

### 3. 데이터 융합 분석 단계:

UBio-X LiveGuard는 지문 데이터와 심박 데이터를 별도로 판단하는 데 그치지 않고, 두 정보를 동시에 분석해 위조 여부를 판별한다. 이 과정은 지문의 모양과 살아있는 생체 신호를 함께 검증하는 구조로, 패턴 기반 인증의 한계를 보완한다.

### 4. 인증 결과 전송 및 보안 저장 단계:

인증 결과는 단말기로 전송되며, 보안 영역에 암호화 저장되는 구조를 통해 인증 데이터의 무결성과 안전성을 강화한다. 이는 단말기 단위의 인증 기능을 넘어, 실제 출입통제·근태관리·고보안 인증 환경에서 안정적으로 운영될 수 있는 보안 구조를 제공한다.

지문 패턴 인식



센서가 손가락의 융선(ridge) 패턴을 정밀하게 스캔

심박 신호 감지(PPG)



IR 및 Green/Red 광원으로 혈류 반사율 변화 측정

데이터 융합 분석



지문 + 심박 데이터를 동시에 분석하여 위조 여부 판별

인증 결과 전송



단말기로 결과 전송 및 보안 영역에 암호화 저장

## 05 공인 시험으로 검증된 위조지문 방어 성능

위조지문 대응 기술의 신뢰성은 단순한 기능 설명이나 내부 테스트만으로 입증되기 어렵다. 위조지문 공격은 사용되는 재질, 지문 품질, 센서 방식, 등록 및 인증 절차에 따라 결과가 달라질 수 있기 때문이다. 따라서 금융, 공공기관, 데이터센터, 연구소와 같은 고보안 산업군에서 지문인식 기반 인증을 도입하기 위해서는 다양한 위조 재질과 실제 공격 시나리오를 반영한 객관적 시험 결과가 필요하다.

UBio-X LiveGuard는 한국인터넷진흥원 생체인식시험센터(K-NBTC)의 위조 생체인식 지문 성능 시험을 통해 위조지문 방어 성능을 검증받았다. 해당 시험에서 UBio-X LiveGuard는 위조 생체인식 지문 방어력 성능평가 1등급, 우수 평가를 획득했다. 이는 위조지문 공격에 대응하기 위한 방어 성능이 공인 시험 환경에서 확인되었음을 의미한다(K-NBTC, 2025).

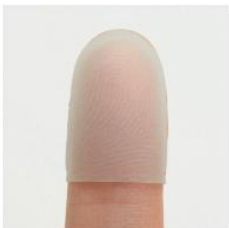
시험은 실제 위조지문 공격에 사용될 수 있는 다양한 재질을 대상으로 진행되었다. 사용된 위조지문 시료는 종이, OHP, 실리콘 A, 실리콘 B, 실리콘 C, 실리콘 D, 젤라틴, 전도성 고무, 점토로 구성되었다. 각 시료는 두께, 색상, 수분 함량이 서로 다르게 설정되어, 단일 재질이 아닌 여러 형태의 위조지문 공격 가능성을 반영했다.

또한 시험은 정상 사용 환경과 위조 공격 환경을 모두 포함해 구성되었다. 실제 지문을 등록하고 실제 지문으로 인증하는 정상 시나리오뿐 아니라, 실제 지문을 등록한 뒤 위조지문으로 인증을 시도하는 시나리오, 위조지문을 등록한 뒤 다시 위조지문으로 인증을 시도하는 시나리오까지 포함되었다. 이는 인증 단계뿐 아니라 등록 단계에서 위조 생체정보가 시스템에 유입될 가능성까지 함께 검증하기 위한 구조다.

이러한 시험 결과는 UBio-X LiveGuard의 보안적 의미를 분명하게 보여준다. 지문인식 시스템의 신뢰성은 인증 단계에서만 결정되지 않는다. 최초 등록 단계에서 위조 생체정보가 입력되면 이후 인증 체계 전체가 흔들릴 수 있다. 따라서 등록과 인증 전 과정에서 위조지문을 탐지하고 차단하는 성능은 생체인증 보안의 핵심 요소다.

### 다양한 위조 지문 시도를 감지합니다

실리콘, 젤라틴, 전도성 고무 등 위조된 지문에서는 탐지되지 않는 혈류 반응을 감지합니다.



실리콘



젤라틴



전도성 고무



필름



종이

## 06 보안성과 사용성의 균형

위조지문 방어 기술은 공격 차단 능력만큼 정상 사용자 인증 성능도 중요하다. 위조지문을 강하게 차단하더라도 실제 사용자의 지문 등록이나 인증이 자주 거부된다면, 출입통제, 근태관리, 금융 인증, 공공 서비스 등 실제 운영 환경에서 불편과 지연이 발생할 수 있다.

UBio-X LiveGuard는 위조지문 방어 기능을 적용하면서도 정상 사용자의 인증 흐름을 안정적으로 유지하도록 설계되었다. 실제 지문을 등록하고 실제 지문으로 인증하는 정상 사용 시나리오에서도 안정적인 등록 및 인증 성능을 보였으며, 이는 보안성과 사용성의 균형을 함께 고려한 결과라고 할 수 있다.

특히 출입통제나 근태관리처럼 하루에도 여러 번 반복적으로 사용되는 인증 환경에서는 보안 기능이 운영 효율성을 저해하지 않아야 한다. UBio-X LiveGuard는 위조지문 방어 성능을 강화하면서도 정상 사용자의 인증 경험을 유지함으로써, 고보안 환경과 일상 운영 환경 모두에 적용 가능한 생체인증 보안 모델을 제시한다.

## 07 산업 현장에서의 의미

지문인식 기반 인증은 이미 금융, 출입통제, 근태관리, 공공 서비스, 의료기관, 연구소, 데이터센터 등 다양한 산업군에서 활용되고 있다. 그러나 지문 패턴만을 중심으로 인증을 수행하는 구조에서는 위조지문 공격이 인증 신뢰를 흔드는 위험 요소가 될 수 있다.

UBio-X LiveGuard의 심박 신호 기반 위조지문 탐지 기술은 이러한 산업 환경에서 중요한 의미를 갖는다. 지문 패턴은 복제될 수 있지만, 살아있는 손가락의 생체 신호까지 동일하게 재현하기는 어렵다. 따라서 UBio-X LiveGuard는 지문 패턴과 심박 신호를 함께 검증함으로써, 위조지문 공격에 대한 실질적인 방어력을 제공한다.

금융기관에서는 계정 도용과 부정 거래를 방지하는 데 기여할 수 있으며, 데이터센터와 연구소에서는 고권한 구역 출입 통제를 강화할 수 있다. 제조시설과 물류센터에서는 근태 조작과 대리 인증을 방지할 수 있으며, 공공기관과 의료기관에서는 민감정보 접근 통제의 신뢰성을 높일 수 있다.

결국 위조지문 방어 기술은 단순한 단말기 기능이 아니라, 인증 체계 전체의 신뢰성을 높이는 보안 인프라다. 특히 생체정보가 한 번 유출되면 쉽게 변경할 수 없다는 점을 고려할 때, 위조지문을 사전에 탐지하고 차단하는 기술은 앞으로의 생체인증 환경에서 필수적인 보안 요소가 될 것이다.

## 08 차세대 지문인증의 기준: 인식률을 넘어 위조 방어력으로

그동안 지문인식 기술은 빠른 인증 속도, 높은 인식률, 사용자 편의성을 중심으로 평가되어 왔다. 그러나 생체인증이 고보안 산업군으로 확대되면서 단순한 인식 성능만으로는 충분하지 않게 되었다. 이제 지문인식 시스템은 지문이 등록된 정보와 일치하는지를 확인하는 것을 넘어, 입력된 지문이 실제 살아있는 사람의 생체 입력인지, 위조된 생체정보인지 구분할 수 있어야 한다.

UBio-X LiveGuard는 세계 최초 심박 신호 기반 위조지문 탐지 기술을 통해 이러한 변화에 대응한다. 지문 패턴 인식만으로는 구별하기 어려운 위조지문을 심박 신호 분석으로 판별하고, 실제 살아있는 손가락만을 정확하게 식별한다. 이는 지문인증의 기준을 “누구의 지문인가”에서 “실제 살아있는 사람의 지문인가”로 확장하는 기술적 전환이다.

또한 UBio-X LiveGuard는 K-NBTC의 공인 시험에서 위조 생체인식 지문 방어력 성능평가 1등급, 우수 평가를 획득함으로써, 위조지문 방어 성능이 차세대 생체인증의 핵심 평가 기준이 되고 있음을 보여준다.

앞으로의 생체인증은 “얼마나 빠르게 인식하는가”를 넘어 “위조된 생체정보를 얼마나 정확히 구분하는가”를 기준으로 평가되어야 한다. UBio-X LiveGuard는 심박 신호 기반 라이브니스 검증과 공인 시험으로 확인된 위조지문 방어 성능을 바탕으로, 고보안 산업군에서 지문인증의 신뢰성을 높이는 새로운 기준을 제시한다.



### UBio-X LiveGuard

얼굴인식 단말기에 심박 신호 기반 복합 지문 인증을 탑재한  
차세대 멀티모달 생체인증 단말기

## 09 Reference

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



2026 UNION biometrics Co., Ltd. All Right Reserved.

---

#### Address

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

#### Contact

Email: [onlinemarketing@unionbiometrics.com](mailto:onlinemarketing@unionbiometrics.com)