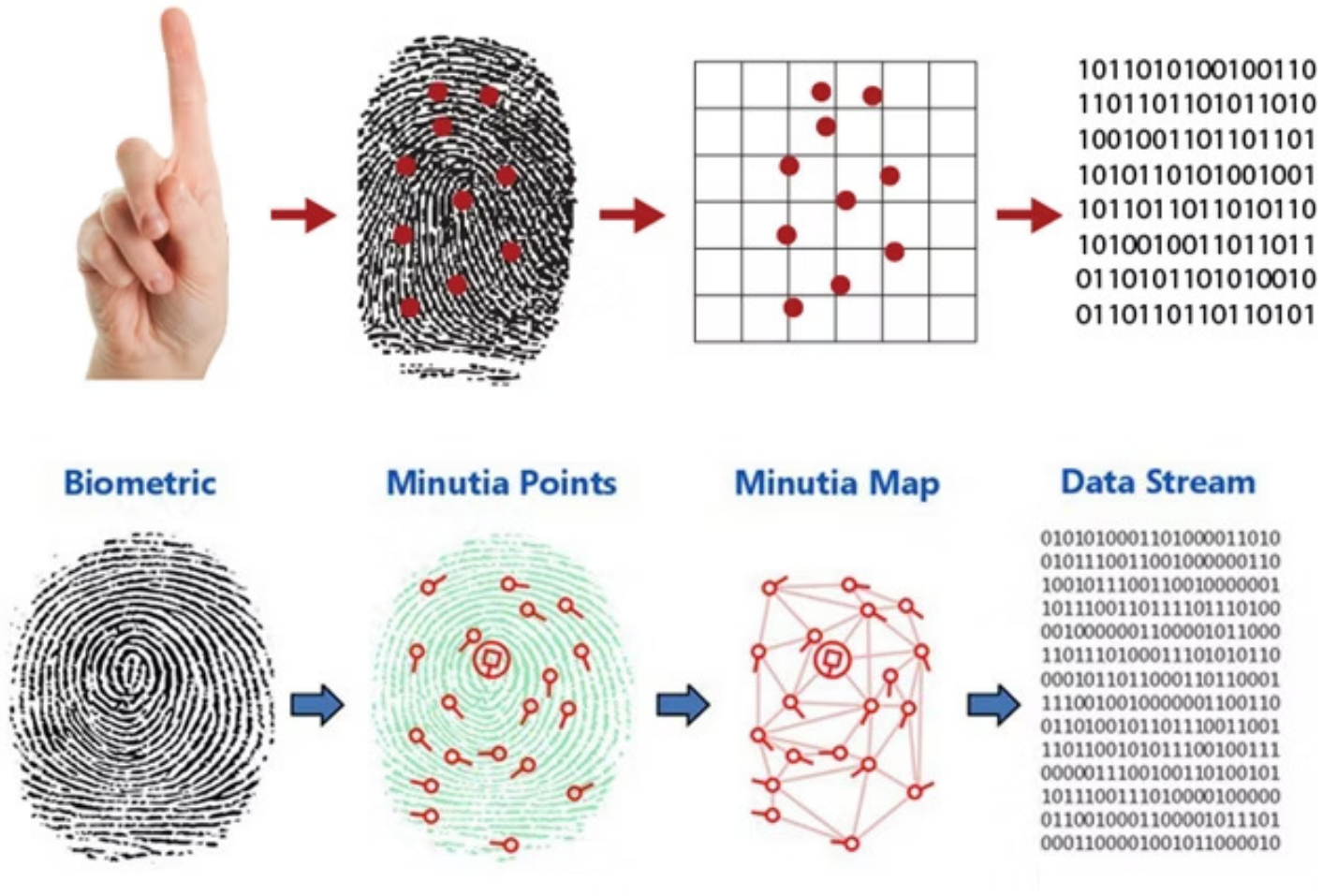
Che cos’è il Biometric Spoofing?

Il Biometric Spoofing è l’atto di imitare le caratteristiche biologiche uniche di una persona per ingannare un sistema di sicurezza e ottenere accesso non autorizzato. Ad esempio, creare una copia falsa della tua impronta digitale per sbloccare il telefono fingendosi te.

Il processo si basa su tre fasi principali: gli hacker prendono di mira elementi biometrici, utilizzano tecniche di spoofing per creare repliche false e cercano di ingannare il sistema di sicurezza per ottenere accesso non autorizzato.



An optical sensor.

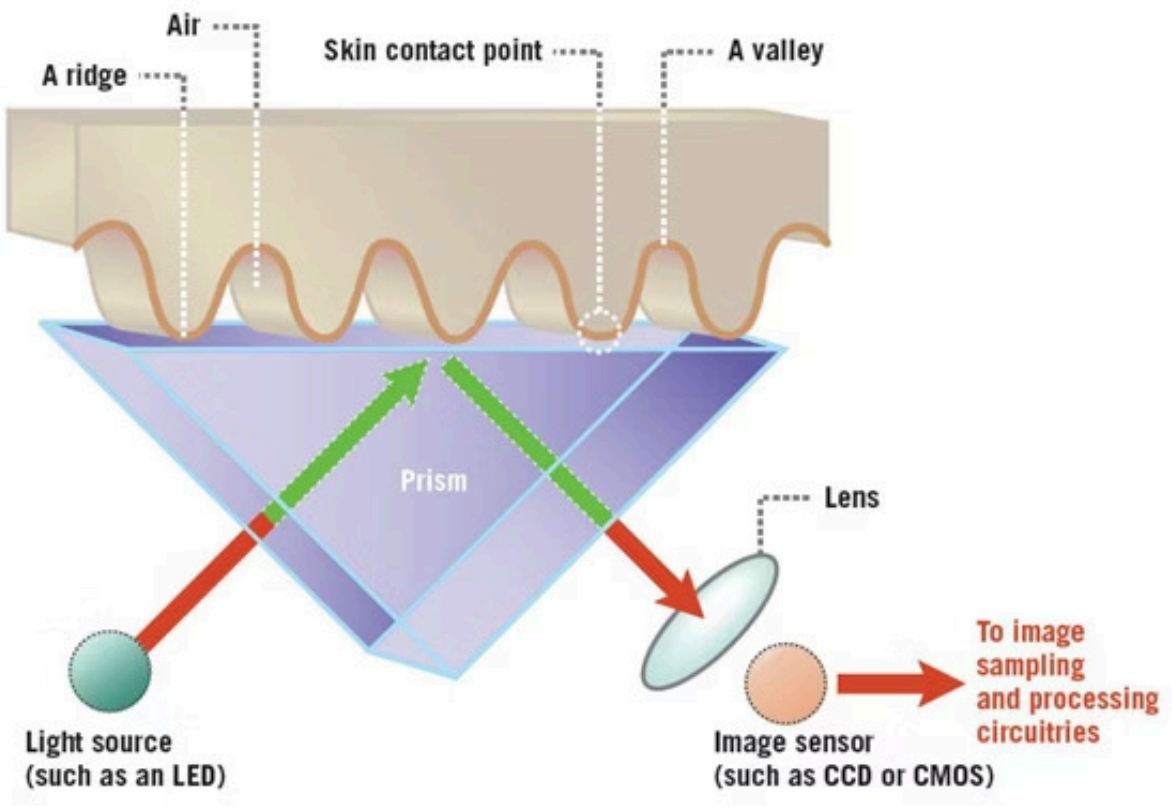


Figure 2

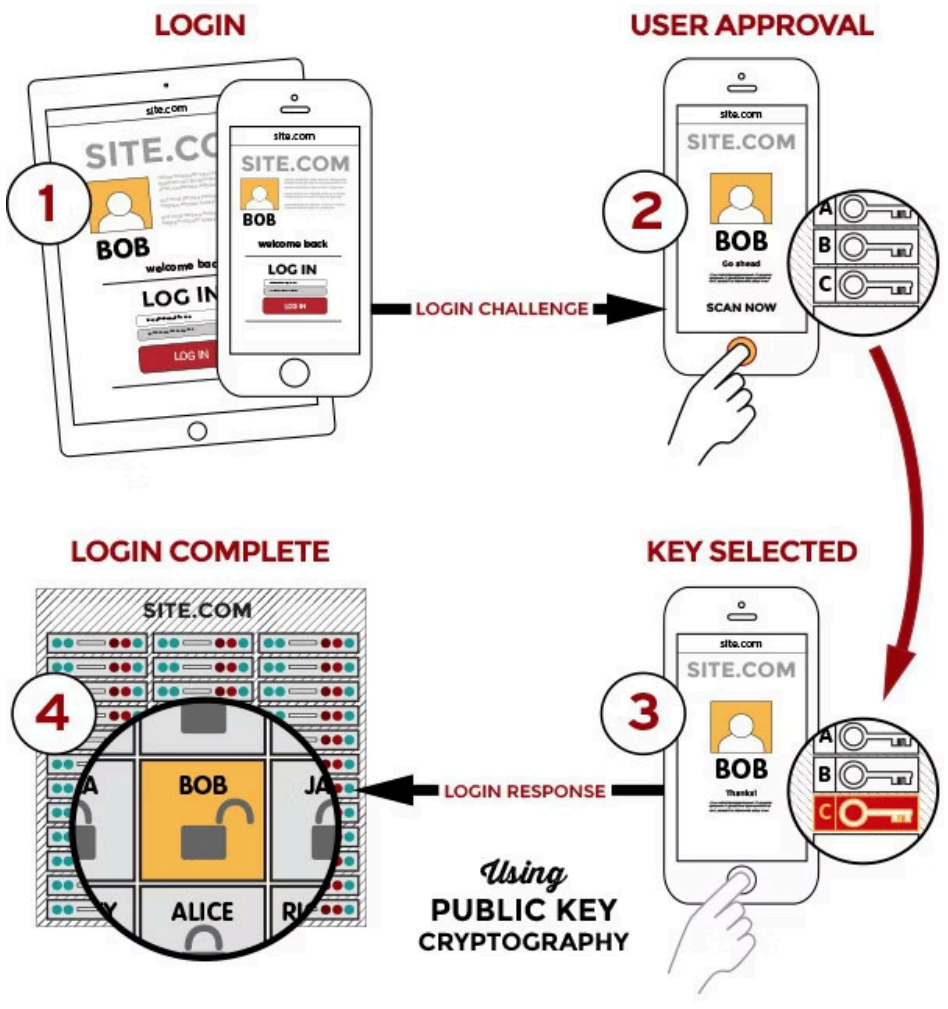
L’Esperimento del “Gummy Bear” Bio-Spoofing

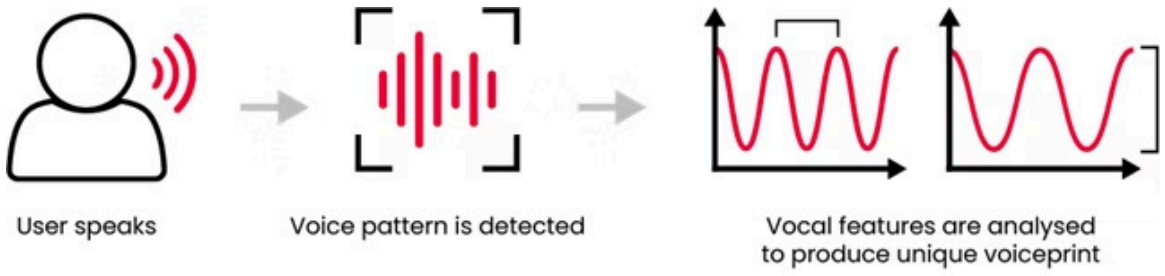
Gummy Bear Spoofing

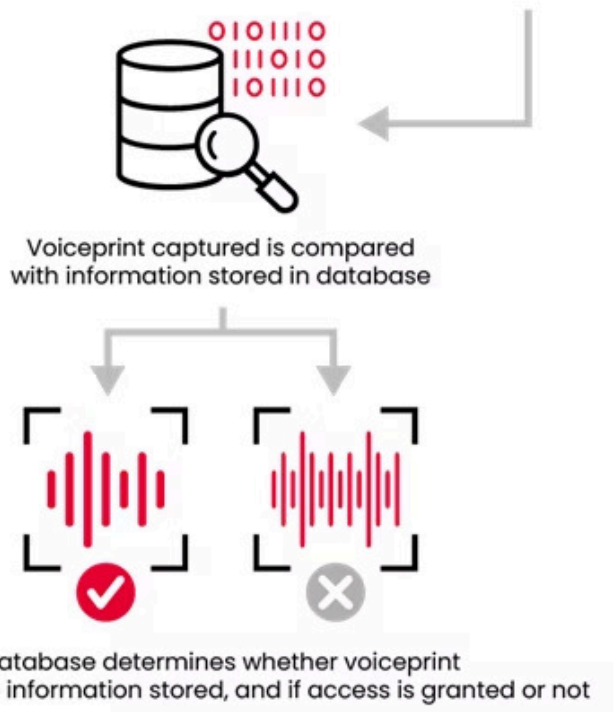
Nel 2002, il ricercatore giapponese Tsutomu Matsumoto ingannò un sensore di impronte digitali usando una caramella **Gummy Bear** per realizzare una copia di un’impronta prelevata da un bicchiere.

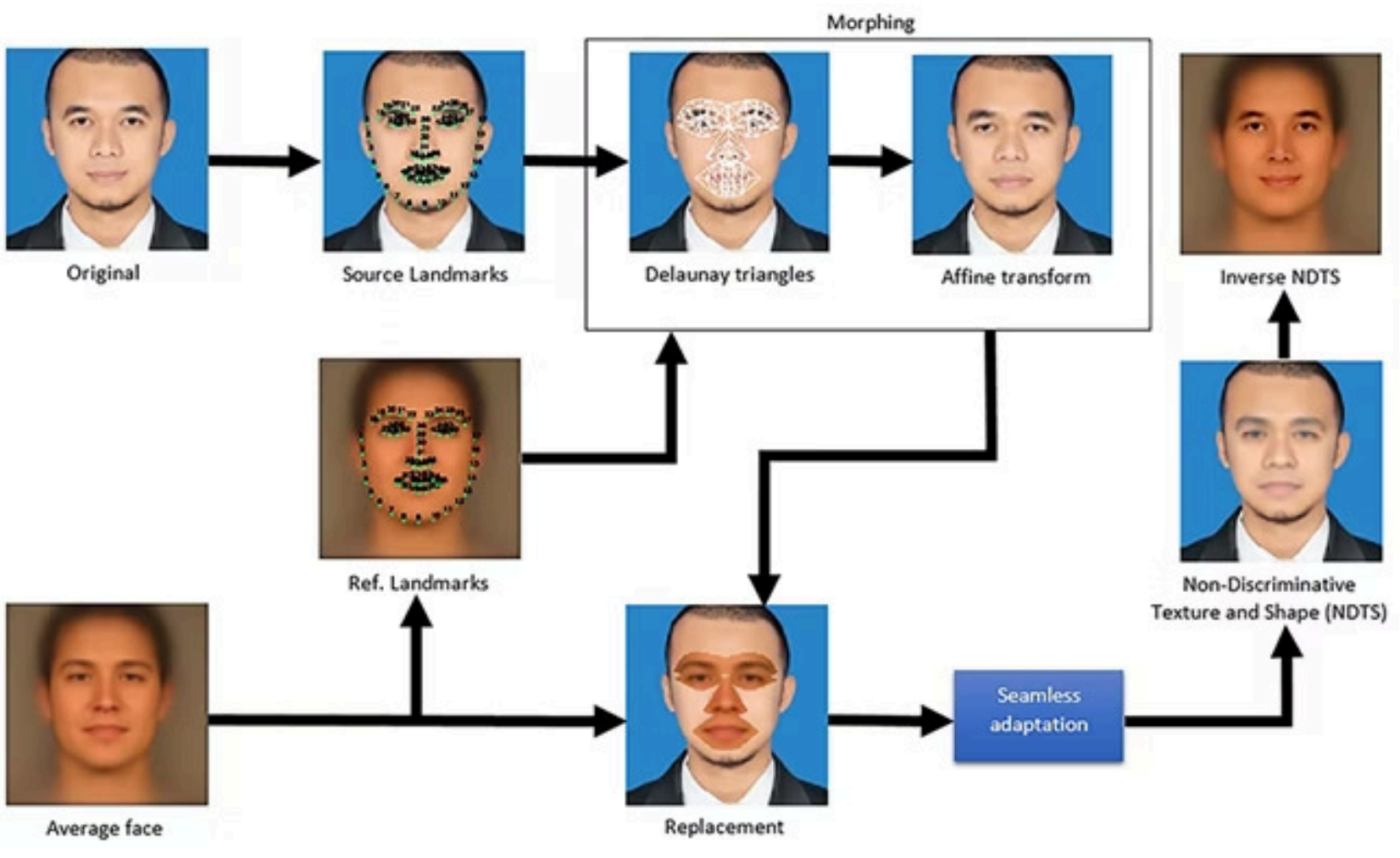
Risultati

La sua impronta digitale artificiale riuscì a ingannare il sensore 4 volte su 5, dimostrando che i sistemi biometrici possono essere elusi con metodi semplici.


LOGIN
USER APPROVAL
site.com
SITE.COM
BOB
welcome back
LOG IN
1
2
LOGIN CHALLENGE
Go ahead
SCAN NOW
A
B
C
LOGIN COMPLETE
KEY SELECTED
4
3
BOB
ALICE
LOGIN RESPONSE
Thanks!
Using
PUBLIC KEY
CRYPTOGRAPHY


User speaks
Voice pattern is detected
Vocal features are analysed
to produce unique voiceprint


Voiceprint captured is compared
with information stored in database
Database determines whether voiceprint
matches the information stored, and if access is granted or not


Morphing
Original
Source Landmarks
Delaunay triangles
Affine transform
Inverse NDTS
Ref. Landmarks
Non-Discriminative
Texture and Shape (NDTS)
Seamless
adaptation
Average face
Replacement

Fasi del Biometric Spoofing

Raccolta dei Dati

Gli hacker ottengono informazioni biometriche della vittima, come impronte digitali, caratteristiche facciali o dati vocali, da oggetti fisici, tracce digitali o direttamente dalla vittima.

Creazione della Replica

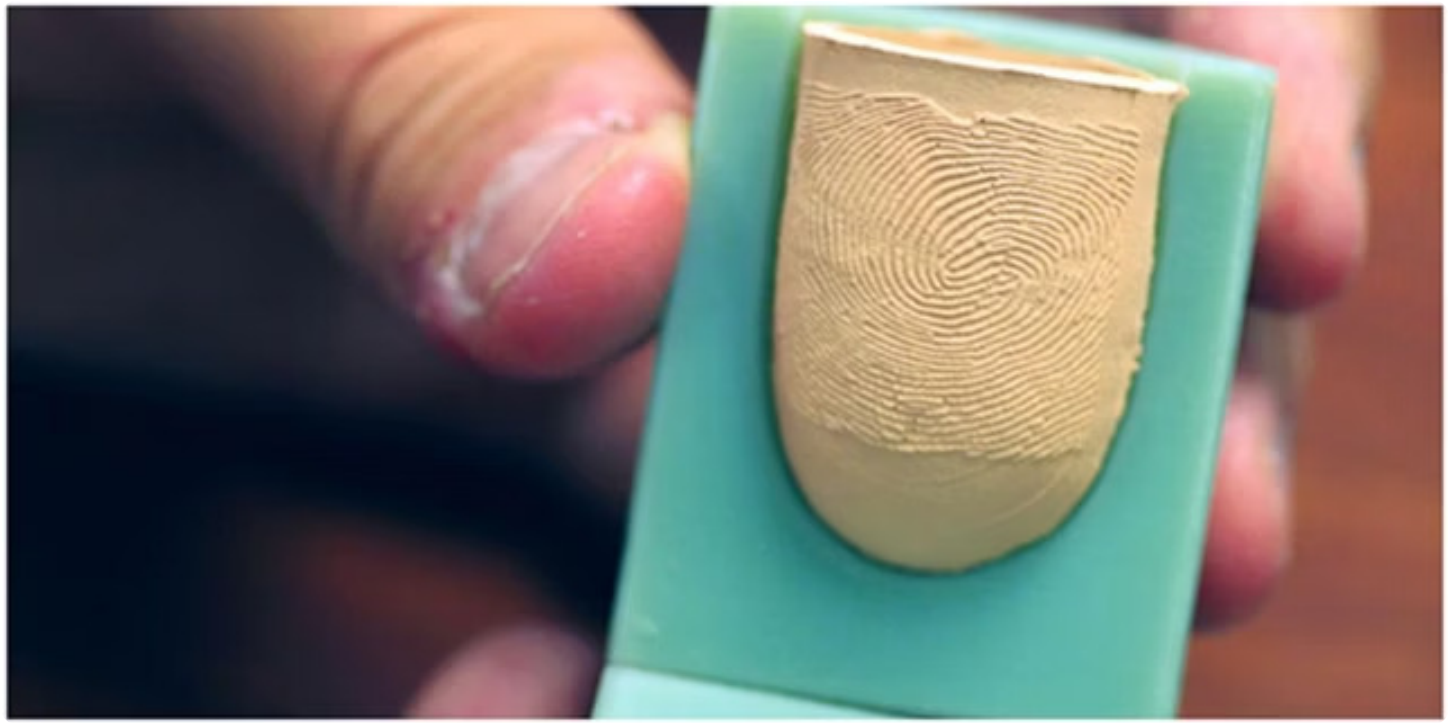
Utilizzando le informazioni raccolte, viene realizzata una replica della caratteristica biometrica: stampi in silicone o gelatina per impronte digitali, software avanzati per clonazione digitale o vocale.

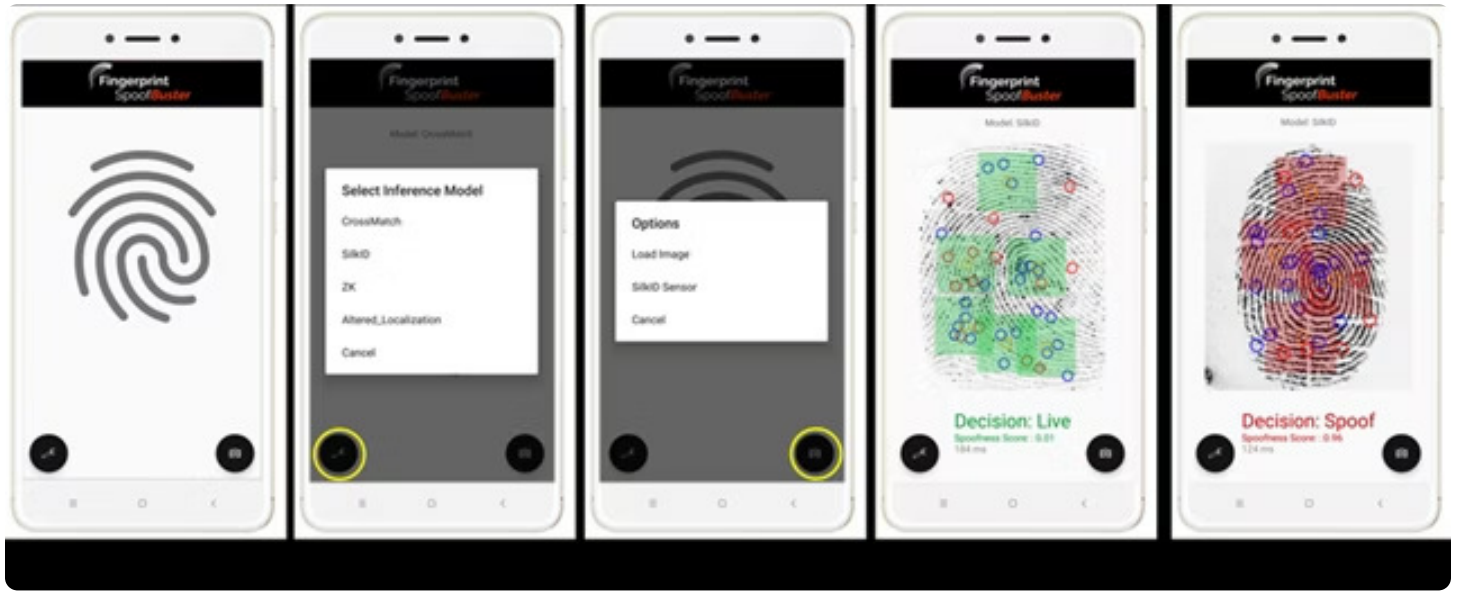
Tentativo di Inganno

L'hacker presenta i dati biometrici falsi al sistema di sicurezza. Se il sistema viene ingannato, concede l'accesso.

Accesso Non Autorizzato

Nei casi più avanzati, i criminali possono bypassare altri livelli di sicurezza, rendendo l'attacco ancora più pericoloso.




Fingerprint SpoofBuster
Select Inference Model
CrossMatch
SilkID
ZK
Altered_Localization
Cancel
Options
Load Image
SilkID Sensor
Cancel
Decision: Live
Decision: Spoof

Attacchi di Presentazione e le loro Conseguenze

Riconoscimento Facciale

- Print Attack: Foto stampata
- Replay Attack: Video preregistrato
- 3D Mask Attack: Maschere 3D
- Deepfake Attack: IA crea volto falso

Riconoscimento Impronte Digitali

- Impronte false: Stampi in silicone
- Impronte latenti: Recupero da superfici
- Impronte stampate 3D: Modelli tridimensionali

Riconoscimento dell'Iride

- Immagini digitali: Schermo
- Lenti a contatto: Disegni di iride
- Occhi artificiali: Protesi oculari

Come Difendersi dal Biometric Spoofing?

Rilevamento della vivacità

Verifica se il tratto biometrico appartiene a un essere umano vivo (es. movimenti involontari degli occhi).

Multi-Factor Authenticati on

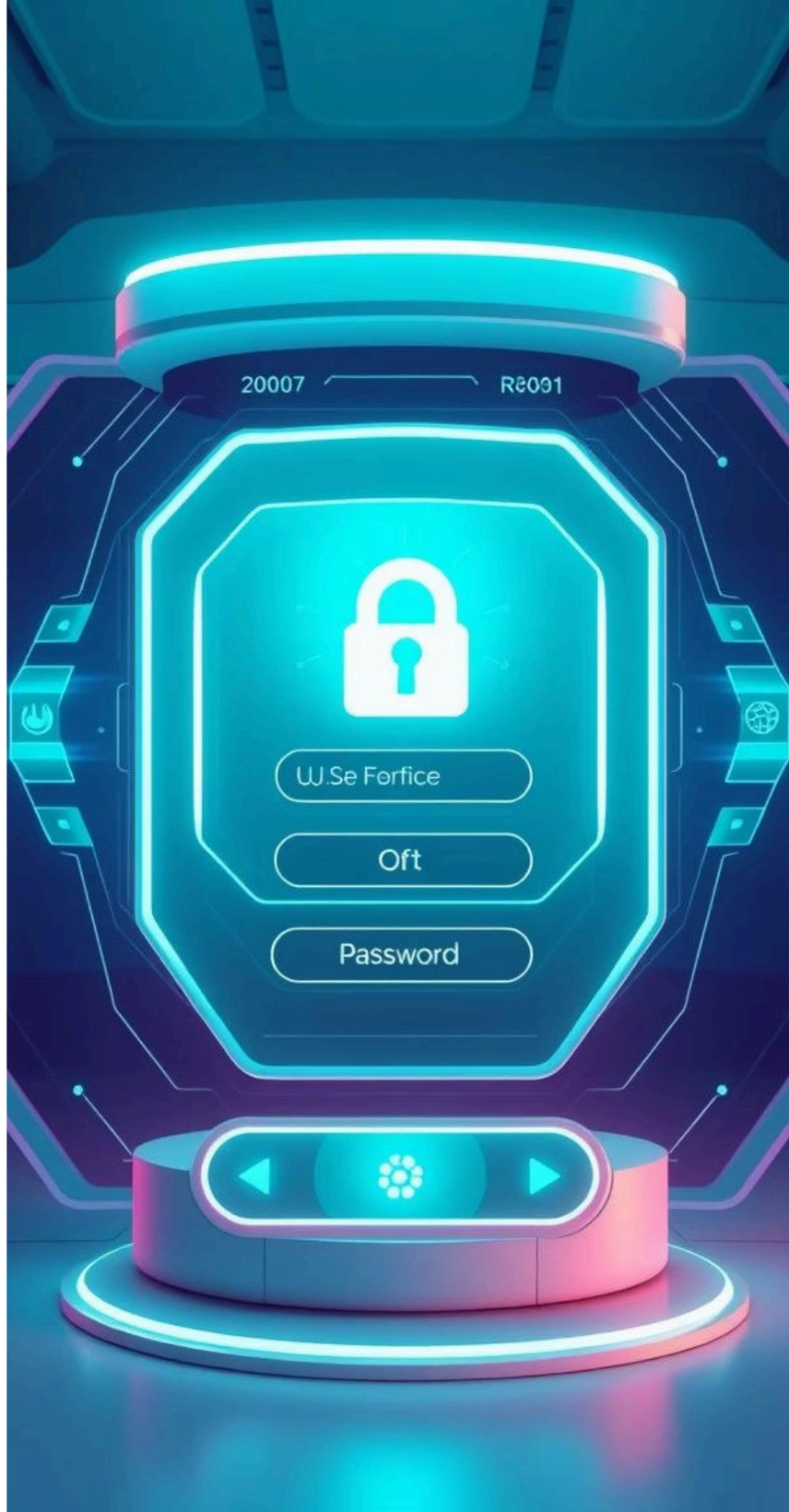
Combinare biometria con password o PIN per una maggiore sicurezza.

Sensori avanzati

Lettori di impronte digitali capaci di rilevare la pressione o il calore corporeo.

AI contro i deepfake

Software in grado di riconoscere video o voci sintetiche create con intelligenza artificiale.



Conclusione

Il Biometric Spoofing è una minaccia concreta che sfrutta le vulnerabilità dei sistemi biometrici per ottenere accesso non autorizzato. Sebbene le tecnologie di sicurezza stiano migliorando, è fondamentale adottare metodi di autenticazione multipli per garantire una protezione efficace contro questi attacchi.