BIOMETRICS: TYPES, ACCURACY, AND COMPARISONS

UNDERSTANDING PHYSIOLOGICAL & BEHAVIORAL AUTHENTICATION TECHNOLOGIES

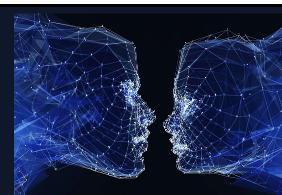
AGENDA

- BIOMETRICS OVERVIEW
- TYPES OF BIOMETRICS
- BIOMETRICS ACCURACY & SELECTION
- SUMMARY

We use biometrics everyday. Logging into your computer, smartphone, etc. Voice recognition is used on phone systems for verification.
There are many types of biometric security, and I am going to focus on the most common.

BIOMETRICS OVERVIEW

WHAT ARE BIOMETRICS?



- Automated recognition of individuals based on unique biological or behavioral characteristics
- Two main categories:
  - Physiological (body traits): Fingerprint, Face, Iris, Vein, Hand Geometry, Heat Signature
  - Behavioral (patterns of behavior): Voice, Signature, Gait, Keystroke
- Why biometrics? More secure and convenient than passwords/PINs

Speaker note: Biometrics are now standard in smartphones, border control, banking, and workplaces.

HISTORY OF BIOMETRICS

While the initial instances of biometrics date back to the Babylonian empire, the first biometric identification system wasn't developed until the 1800s. A Parisian, Alphonse Bertillon, created a method of classifying and comparing criminals based on their body measurements. While imperfect, Bertillon's system was the catalyst of using physical characteristics as a means of authenticating identity.

In the 1880s, fingerprints started being used regularly as a way to identify criminals and to sign contracts. It became commonplace knowledge that people had unique fingerprints, which are symbolic of one's identity. Though it is not 100% certain who first began using fingerprints for identification, we know that Edward Henry developed the Henry Classification System fingerprint standard.

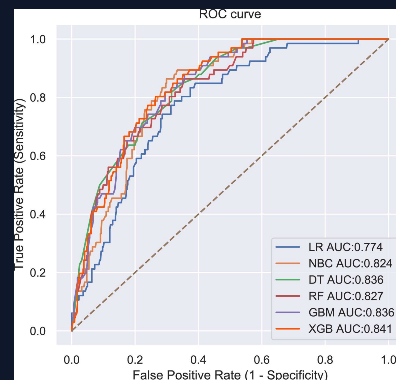
WHERE ARE BIOMETRICS USED MOST?

Area	Common Biometric Used	Typical Purpose / Example
Personal Devices	Fingerprint, Facial	Unlocking smartphones, tablets, and laptops
Apps & Accounts	Fingerprint, Facial	Logging into apps (email, password managers, social media)
Banking & Finance	Fingerprint, Facial, Voice	Mobile banking login, approving payments, phone banking
Payments	Fingerprint, Facial	Mobile payments (Apple Pay, Google Pay)
Travel & Airports	Facial	Airport check-in, security screening, boarding gates
Border Control	Facial, Fingerprint, Iris	Passport control and identity verification
Workplace Access	Fingerprint, Facial	Building entry, restricted areas
Time & Attendance	Fingerprint, Facial	Clocking in/out at work or school
Healthcare	Fingerprint, Facial	Patient identification, medical record access
Government Services	Fingerprint, Facial	National IDs, voter registration, public services
Retail & Stores	Facial	Loss prevention, loyalty programs, self-checkout
Smart Homes	Voice	Identifying users for smart assistants (Alexa, Google Assistant

Most people use biometrics daily without noticing, especially through their phones.

KEY ACCURACY METRICS EXPLAINED

- False Acceptance Rate (FAR): % of impostors incorrectly accepted (security risk)
- False Rejection Rate (FRR): % of legitimate users incorrectly rejected (usability issue)
- Equal Error Rate (EER / CER): Point where FAR = FRR → single number for overall accuracy (Lower EER = more accurate system)
- Other factors: Spoofing resistance, user acceptance, cost, environmental sensitivity



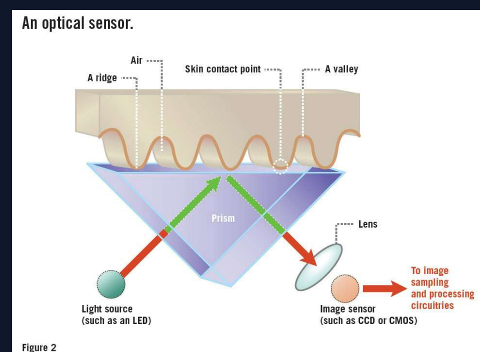
Much like measurements for flu test kits, metrics on how good biometric devices are focused on three main numbers:
FAR – false positives
FRR – false negatives
EER – combination of the two numbers
We will talk about these in terms on the various types of biometrics.

The most common biometrics are
1.) Fingerprints/Palm Prints – different technologies for the two of these
2.) Facial Recognition
3.) Iris recognition
4.) voice recognition

FINGERPRINT RECOGNITION

- How it works: Scans ridges & valleys on fingertips (optical or capacitive sensors)
- Typical EER: 1–2%
- Pros: Cheap, fast, high user acceptance
- Cons: Affected by cuts, dirt, moisture; medium spoofing risk (gels/latex)
- Best for: Smartphones, laptops, office access

How Fingerprint Recognition Works Video



Theoretical attacks target the fact that fingerprints are surface patterns:
- Systems without physiological sensing may only check ridge patterns
- Older or low-cost sensors may lack strong liveness checks

FACIAL RECOGNITION

- How it works: Analyzes facial landmarks, distances, and texture using AI/deep learning
- Typical EER: 0.1–2% (modern systems often <1%)
- Pros: Completely contactless, very convenient, works at a distance
- Cons: Sensitive to lighting, angles, masks, aging; lower spoofing resistance (photos/videos)
- Best for: Airports, surveillance, phone unlock

How Facial Recognition Works Video

Speaker note: Accuracy has improved dramatically with AI but still struggles in poor lighting.

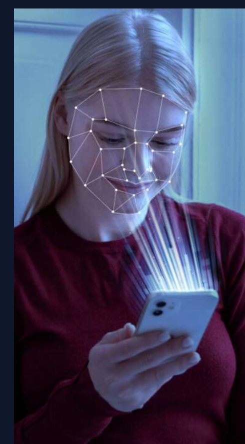
At a high level, attacks attempt to present non-live facial representations to a camera-based system:

- Flat visual representations
- Replayed or synthesized motion
- Artificial 3D facial forms

These exploit systems that rely only on 2D imagery or weak depth cues. Modern research shows these risks are real and evolving, especially with AI-generated media.

IPHONE FACIAL RECOGNITION

- The TrueDepth camera is a front-facing 3D sensing system developed by Apple
- It creates a detailed 3D map of a user's face, not just a photo
- Primary uses:
  - Face ID biometric authentication
  - Animoji / Memoji
  - Portrait-mode selfies
  - Augmented Reality (AR) applications
- Key hardware components:
  - Dot Projector – projects thousands of invisible infrared dots onto the face
  - Infrared Camera – reads the dot pattern and captures depth data
  - Flood Illuminator – emits infrared light so it works in low-light or darkness
  - Front RGB Camera – captures the regular selfie image
- Why it matters:
  - Uses depth + infrared, making it much more secure than 2D facial recognition

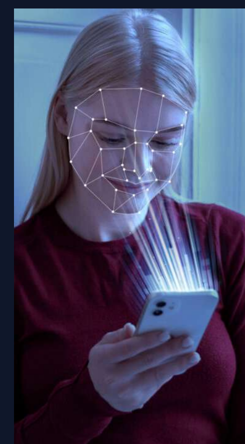


Memoji are personalized, animated, or static avatar stickers created on Apple devices

IPHONE FACIAL RECOGNITION

- Step-by-step process:
  1. Flood Illuminator activates - Infrared light illuminates the face (even in total darkness)
  2. Dot Projector emits IR dots - Over 30,000 invisible dots are projected onto facial features
  3. Infrared Camera captures the pattern - Reads how the dots deform across the face's contours
  4. 3D depth map is created - A precise model of facial geometry is generated
  5. Neural Engine processes the data - Converts the depth map into a mathematical representation
  6. Secure comparison happens on-device - Data is checked against the enrolled face inside the Secure Enclave

- Security advantages:
  - Works in darkness, bright light, hats, glasses
  - Resistant to photos and masks
  - Facial data never leaves the device

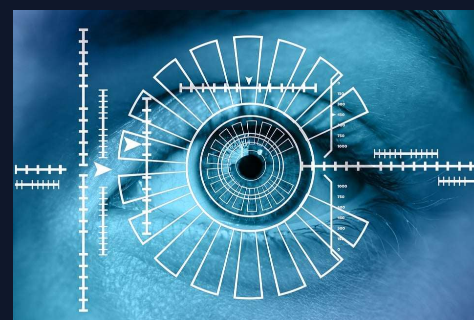


Memoji are personalized, animated, or static avatar stickers created on Apple devices

IRIS RECOGNITION

- How it works: High-resolution camera captures the unique patterns in the colored part of the eye
- Typical EER: 0.01–0.1% (often cited as one of the most accurate)
- Pros: Extremely stable over lifetime, very hard to spoof
- Cons: Requires user to look at camera; higher hardware cost
- Best for: High-security environments (borders, data centers, military)

How Iris Recognition Works Video



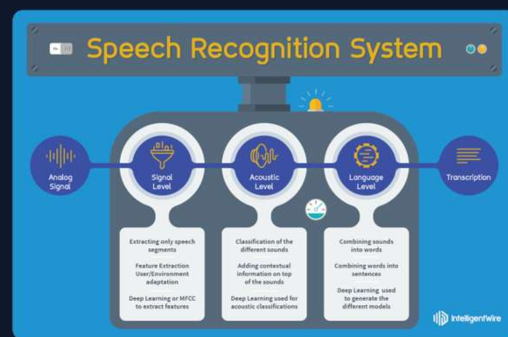
Researchers classify iris spoofing as presentation attacks, meaning non-live artifacts are presented to a sensor.
High-level categories studied in the literature include:

- Image-based presentations (non-live visual representations)
- Textured contact lenses that alter iris appearance
- Synthetic or artificial iris patterns
- Post-mortem eye scenarios (mostly theoretical / lab-based)

These are studied for defensive evaluation, not because they are easy or common in real deployments.

VOICE RECOGNITION

- How it works: Analyzes pitch, tone, cadence, and spectrogram patterns
- Typical EER: 2–5%
- Pros: Natural, works over phone/remote, low cost
- Cons: Heavily affected by noise, colds, aging, or emotional state
- Best for: Call centers, voice assistants, hands-free access



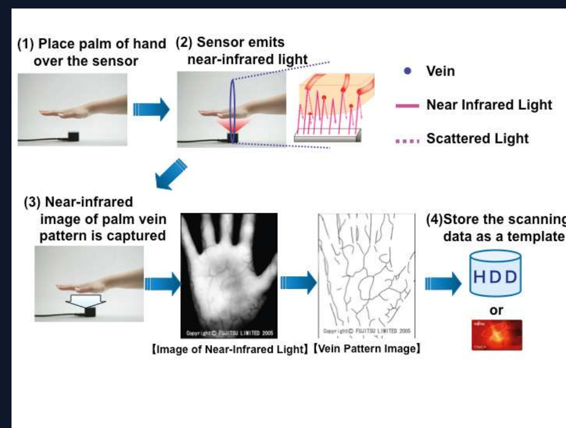
Voice systems are vulnerable in theory because:

- Sound can be recorded, replayed, or synthesized
- Some systems authenticate on spectral similarity alone

This has driven the adoption of voice liveness detection and behavioral modeling.

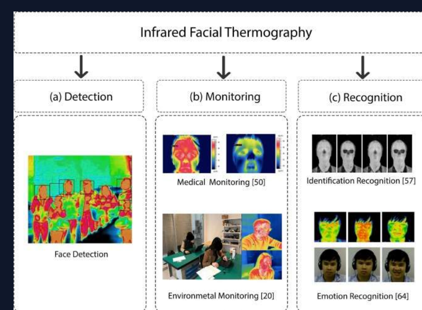
PALM VEIN / FINGER VEIN RECOGNITION

- How it works: Near-infrared light scans unique blood vessel patterns beneath the skin
- Typical EER: 0.01–0.1% (extremely low false rates)
- Pros: Very hard to spoof (internal feature), unaffected by surface dirt/cuts
- Cons: Less common, requires specialized scanner
- Best for: Banking ATMs, secure facilities



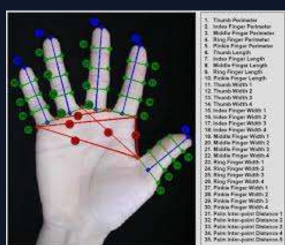
FACIAL HEAT MAPS – THERMAL INFRARED

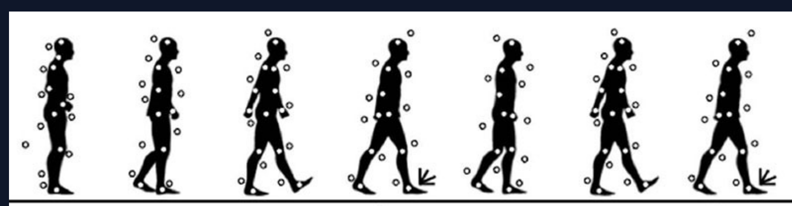
- How it works: Uses infrared cameras to capture heat patterns emitted by facial blood vessels, tissue, and skin temperature distribution (creates a unique "thermal signature")
- Typical Accuracy: Recognition rates: 88–95%+ in studiesEER: Often 0.1–1% in controlled tests (comparable or better than visible light in challenging conditions)
- Pros:
  - Works in complete darkness / total darkness
  - Less affected by lighting, makeup, or skin tone
  - Harder to spoof with photos/videos (live heat required)
  - Stable vascular patterns
- Cons:
  - Sensitive to ambient temperature, exercise, alcohol, or illness (affects heat patterns)
  - Higher hardware cost (thermal cameras)
  - Lower resolution than visible light cameras
- Best for: Night-time surveillance, border control, high-security access, medical/emotion detection



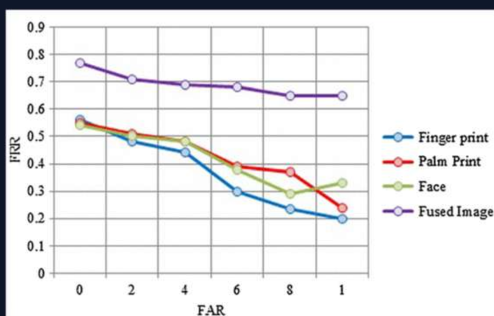
OTHER NOTABLE BIOMETRICS

- Hand Geometry: Shape/size of hand – moderate accuracy, easy to use
- Behavioral (Gait, Signature, Keystroke): Convenient for continuous authentication but generally lower accuracy than physiological traits
- Multimodal Systems: Combine 2+ biometrics (e.g., face + fingerprint) → dramatically higher accuracy (often >99.5%)





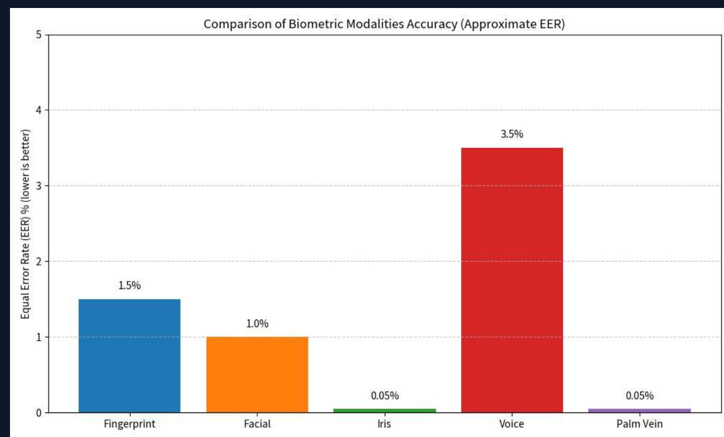
BIOMETRICS ACCURACY & SELECTION



Speaker note: Biometrics are now standard in smartphones, border control, banking, and workplaces.

BIOMETRICS ACCURACY COMPARISON

- Approximate Equal Error Rate (EER) – Lower is Better
  - Iris & Palm Vein: ~0.05% (highest accuracy)
  - Facial: ~1.0%
  - Fingerprint: ~1.5%
  - Voice: ~3.5%



EER is the composite number of false positives and false negatives

BIOMETRICS ACCURACY COMPARISON

Modality	Typical EER	Spoof Resistance	User Acceptance	Cost	Environmental Sensitivity
Iris	0.01–0.1%	High	Medium	High	Low-Medium
Palm Vein	0.01–0.1%	Very High	Medium-High	Medium	Low
Face (Visible)	0.1–2%	Low-Medium	Very High	Low	High (light)
Face (Thermal/Heat Map)	~0.1–1%	Medium-High	High	Medium-High	Medium (temp)
Fingerprint	1–2%	Medium	High	Low	Medium
Voice	2–5%	Low	High	Very Low	High

HOW TO CHOOSE THE RIGHT BIOMETRIC

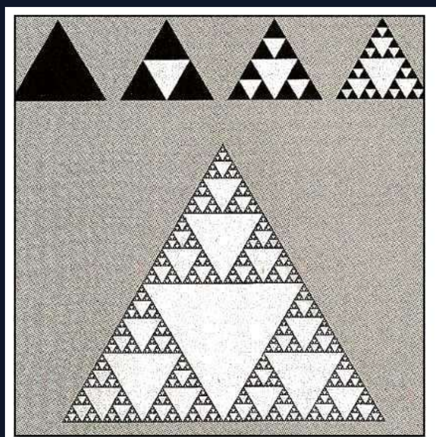
- High-security needs → Iris or Vein
- Convenience & cost → Fingerprint or Face
- Remote/phone use → Voice or Face
- Best practice: Use multimodal (multiple biometrics) for maximum security and usability

Factor	Ask This
Security	How bad is a false accept?
Accuracy	How reliable must it be?
Convenience	How fast and easy for users?
Environment	Where will it operate?
Cost	What hardware is acceptable?
Privacy	What data risks are allowed?

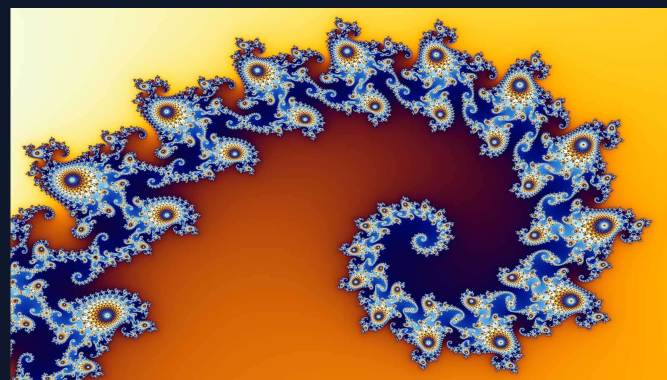
SUMMARY

Biometrics are being used everywhere today and will only increase. The most likely scenario

FUTURE TRENDS IN BIOMETRICS

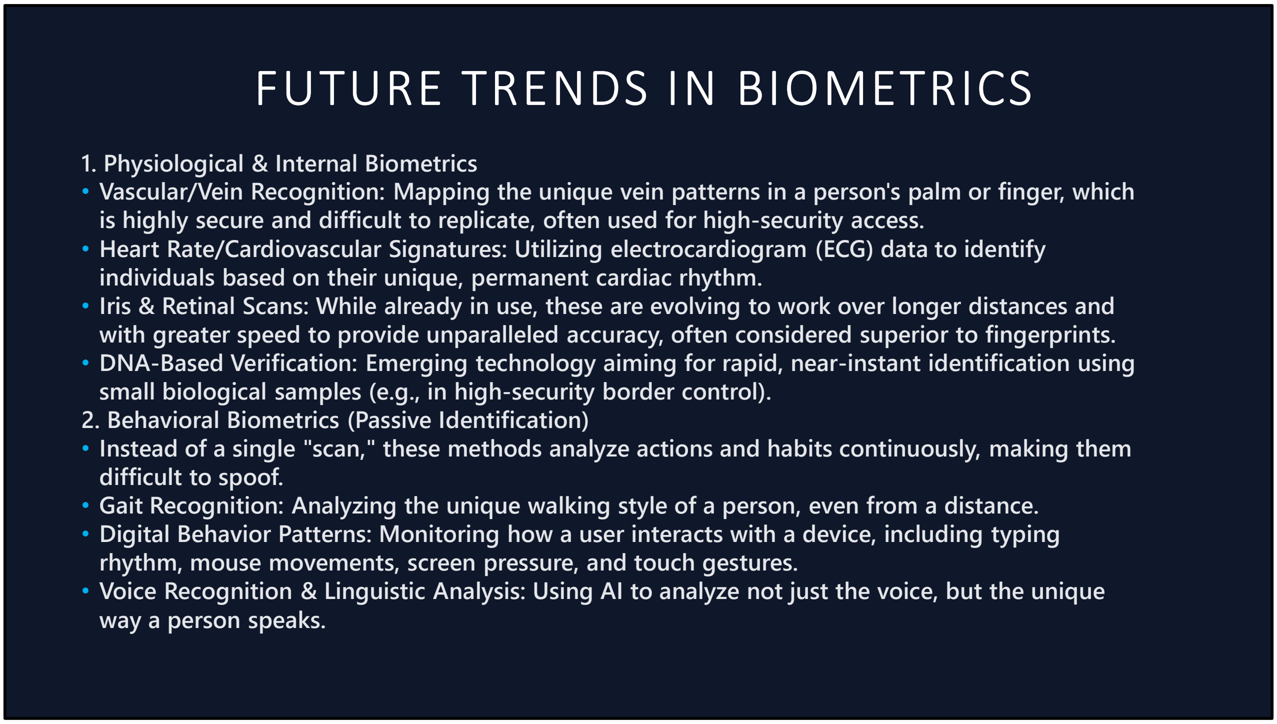


The Sierpiński gasket—a simple fractal produced by breaking up a triangle into successively smaller ones



Fractal geometry is the geometry of repeating patterns.

Fractal geometry is the study of complex, never-ending geometric patterns that repeat themselves at different scales, known as self-similarity. Unlike Euclidean geometry (lines, circles), fractals are often irregular, infinitely complex, and possess fractional dimensions, frequently modeling natural structures like coastlines, trees, and clouds.



DNA based verification could give a lot more data than just who you are.
Are there fractal patterns that people will be able to spoof in the future?

FUTURE TRENDS IN BIOMETRICS

3. Advanced AI-Driven Systems

- Multimodal Fusion: Combining two or more biometric methods—such as face + iris, or voice + gait—to create a more secure, multilayered identity profile.
- Continuous Authentication: Instead of logging in once, systems continuously monitor the user to ensure they are the same person throughout a session, reducing fraud in financial apps.
- Liveness Detection (Anti-Spoofing): AI-powered technology that ensures a "live" person is present, preventing deepfakes, masks, or synthetic photos from bypassing security.
- Subconscious/Brain Wave Authentication: Research into using electroencephalogram (EEG) patterns in response to specific stimuli for identification.

4. Key Future Trends

- Contactless/Touchless: Driven by a desire for hygiene and speed, technologies like facial and palm recognition are replacing fingerprints.
- Edge Biometrics: Processing biometric data directly on a device rather than on a central server, enhancing privacy.
- Interoperable "Digital Identities": Moving toward systems where a person's biometric template can be used securely across different platforms, such as travel, finance, and government services.

Privacy Challenge: While convenient, these technologies raise concerns about permanent data theft, as biometrics (like your retina) cannot be changed if leaked.

Could someone grow or print an eye to fake a retinal scan?

CONCLUSION & KEY TAKEAWAYS

- Biometrics offer superior security and convenience over traditional passwords
- Iris and Vein currently lead in accuracy and spoof resistance
- Fingerprint and Face dominate everyday use due to balance of cost and usability
- Accuracy continues to improve rapidly with AI and multimodal approaches
- The more data points, the less vulnerable the system is.
- Future trend: Contactless + continuous authentication

ADDITIONAL RESOURCES

The Alan Turing Institute – Biometrics
History of Biometrics