F

Facial Recognition: How It Works, Accuracy, Privacy, and Security

Facial recognition compares a facial template with one or more enrolled templates. The result is a similarity score and decision threshold, not proof of identity by itself.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Facial recognition uses an image or video to create a mathematical representation of facial features and compare it with enrolled templates. A result is normally a similarity score evaluated against a threshold, not an absolute statement that two people are the same.

Detection, verification, and identification

- **Face detection** locates a face in an image. It does not identify the person.
- **Verification (one-to-one)** asks whether a captured face matches one claimed identity, such as a device owner.

- **Identification (one-to-many)** searches a gallery for possible matches and is more likely to require human review and strong governance.
- **Face analysis** may estimate attributes or quality but should not be confused with identity matching.

How the matching pipeline works

1. **Capture:** a camera obtains an image or video under particular lighting, angle, resolution, and compression.
2. **Quality and alignment:** software finds the face and normalizes pose, scale, and landmarks.
3. **Template creation:** an algorithm converts features into a numeric representation.
4. **Comparison:** the probe template is compared with an enrolled template or a gallery.
5. **Decision:** policy applies a threshold and may require another factor or human review.

A template is not an ordinary photograph, but it is sensitive biometric data and may support recognition or correlation. It needs protection, retention limits, and a deletion process.

Accuracy and decision thresholds

A **false match** incorrectly links different people. A **false non-match** fails to recognize the enrolled person. Tightening a threshold usually reduces false matches while increasing false non-matches. The appropriate balance depends on whether the system unlocks a personal device, admits someone to a building, deduplicates records, or generates an investigative lead.

Performance can change with image quality, aging, pose, expression, lighting, camera, occlusion, demographic group, gallery size, and operational workflow. A laboratory accuracy figure does not guarantee performance in a different population or environment.

Security threats

- **Presentation attack:** a photo, screen, mask, replay, or synthetic media is presented to a sensor.

- **Injection attack:** manipulated media bypasses the physical sensor and enters the processing pipeline.
- **Morphing:** one image is blended from multiple people to support identity fraud.
- **Template or account theft:** enrollment records, administrative access, or recovery paths are compromised.
- **Poisoned enrollment:** the wrong person or poor evidence becomes the trusted reference.

NIST discusses presentation attacks and face morphing in its current overview of facial-recognition security.

Privacy and governance questions

- What is the specific purpose and legal basis, and is a less intrusive method adequate?
- Were people clearly informed, and can they use a practical alternative where required?
- Are original images, templates, candidate lists, audit records, and derived attributes retained only as needed?
- Which provider, employee, or agency can search, export, or share the data?
- How are accuracy, demographic effects, appeals, human review, deletion, and misuse audited?

Security controls

- combine high-risk verification with another independent factor as part of multi-factor authentication, and protect account recovery;
- use tested presentation-attack detection and protect the sensor-to-matcher path;
- encrypt templates, separate identifiers, restrict administrator access, and log searches and exports;
- test the intended population and environment at documented thresholds;

- treat identification results as leads requiring corroboration, not automatic adverse decisions;
- maintain incident response and notification procedures for biometric compromise.

Facial recognition FAQ

Can a face be changed like a password?

Not easily. That makes template protection, revocable representations, and alternative factors especially important.

Does liveness detection stop every spoof?

No. It reduces selected presentation attacks and must be tested against the sensor, attack types, accessibility needs, and operating environment.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com