Real or fake?

Guidelines and tools to identify deepfakes

Deepfakes are images or videos that have been tampered with using artificial intelligence (AI) to simulate events that never actually happened.

To detect them, look carefully at:

The medium

What is it like?

Look for red flags, especially around the face.

Visual defects

- **Lighting and skin tone**: suspicious changes.
- **Face and neck**: obvious differences.
- **Outlines**: blurry or not very sharp.
- **Shadows**: inconsistent with the ambient lighting.

Strange movements

- **Facial expressions**: fake or unnatural.
- **Blinking**: infrequent.
- **Wrong perspective**: the AI-generated area does not match the rest of the video.
- **Objects going past in front of the face**: causing distortions.

Quality

- **Sound**: distorted or background noise.
- **Cuts**: interruptions to the image sequence.
- **Duration**: they are usually short videos to reduce possible errors.

Voice

- **Modulation**: strange variations.
- **Synchronization**: mismatches between the person's lips and their voice.

Be wary. Deepfakes are not easy to detect. Look further.

The message

What is it saying?

Analyse it and question it.

The people appearing in the video

- **Are they famous**?
- Is the way they are behaving **consistent with what you know**?
- Are they **talking or gesticulating** as they normally would?

El tema

- **Is the content consistent?** Does it fit with what you know?
- **What emotion does it arouse in you?** Be wary of images or videos that appeal to emotions such as fear or anger in order to go viral.

What is it like?

- **Origin**: who made it and where was it published? Are the sources cited?
- **Date and place**: when and where was it made?
- **Comments and replies**: have any users commented on it or questioned it?

Question what you know about deepfakes:

They can appear not only on news sites or social media but also in fake WhatsApp voice messages or manipulated video calls.

The source

Who else has shared it?

Check the source and look for other official sources.

- **Check**: use fact-checking sites and tools to trace the source of the information.
- **Verify**: if you have received a suspicious private message from one of your contacts, check with the sender through a separate trusted channel.
- **Research** the author of the content.
- **Compare** the video or image with other videos of the same person.
- **Compare** the information with that contained in other media, official and academic sources.

What tools can you use?

Fact Check Explorer | TinEye | Google Images | InVID | Wayback Machine | Library Guide Fake News: Fact-checking tools

Check and protect yourself

Before sharing content or responding to suspicious requests, **check the information**.

Protect your devices with additional authentication mechanisms besides biometric systems.

Sources:

Deepfake Lab. (2023). *Deep fake Lab: Unraveling the mystery around deepfakes*. https://deepfakelab.theglassroom.org

Hoe-Lian, D, [Dion]. (2024). He looks very real: Media, knowledge, and search-based strategies for deepfake identification. *Journal of the American Society for Information Science and Technology*, 75(6), 643–654. https://doi.org/10.1002/asi.24867

INCIBE. (2023.). *Bulos y noticias falsas (fake news)*. https://www.incibe.es/ciudadania/tematicas/bulos-fake-news

Lyon, B. [Brian] & Tora, M. [Matt]. (2023). Exploring deepfakes: Deploy powerful AI techniques for face replacement and more with this comprehensive guide (1st ed.). Packt Publishing Ltd.

Maldita Tecnología. (2023). *Cómo detectar un 'deepfake' y en qué se diferencian estos vídeos manipulados de otras contenidos generados con inteligencia artificial*. Maldita.es. https://maldita.es/malditatecnologia/20231026/detectar-deepfakes-diferencia-contenidos-inteligencia-artificial

Universitat Oberta de Catalunya