Detecting Synthetically Generated Videos

Preamble

Adversarial state and non-state actors use AI-generated deepfake video as instruments of strategic deception, psychological influence and narrative manipulation. Below are the ten pointers that offer an evidence-based technique to identify such fabricated video footage.

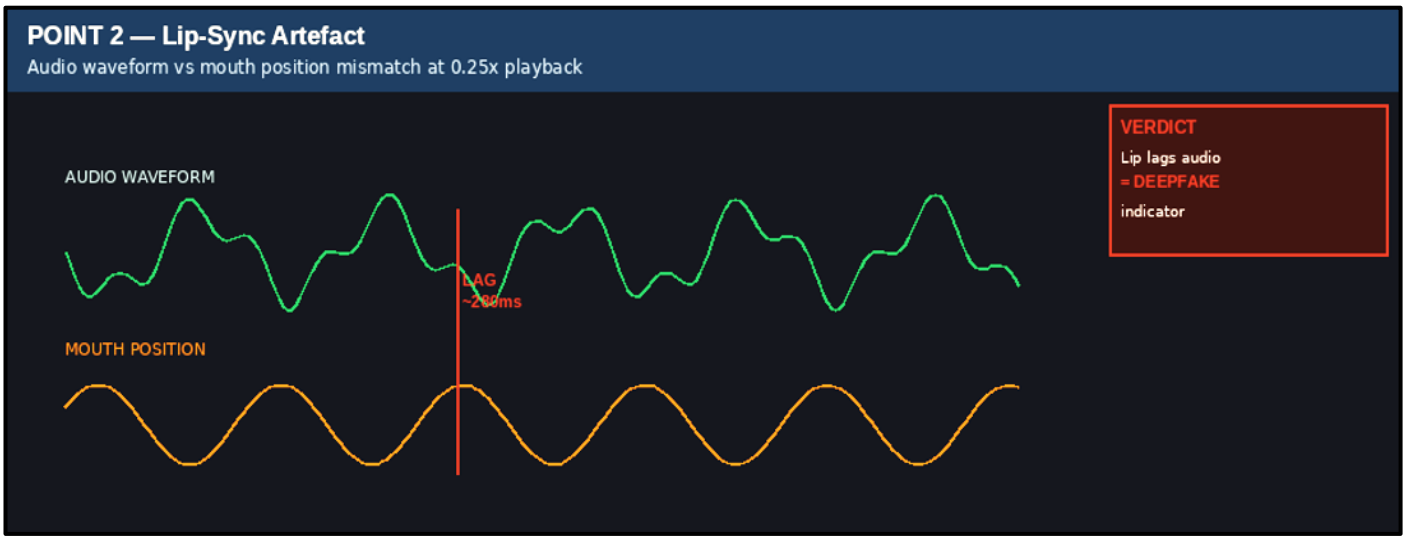
Ten-Point Advisory

1. **Scrutinise Facial Micro-Expressions and Blink Patterns**.

Videos that employ deepfake technologies, including DeepFaceLab, FaceSwap and Wav2Lip, are often characterised by an unnatural rate of blinking, which includes either too many, too few or no blinks at all. The problem occurred more commonly among older versions of technology; the latest generation of deepfakes created in 2025 has been fixed. Check any dubious video at 0.25x speed for unnatural blinks.

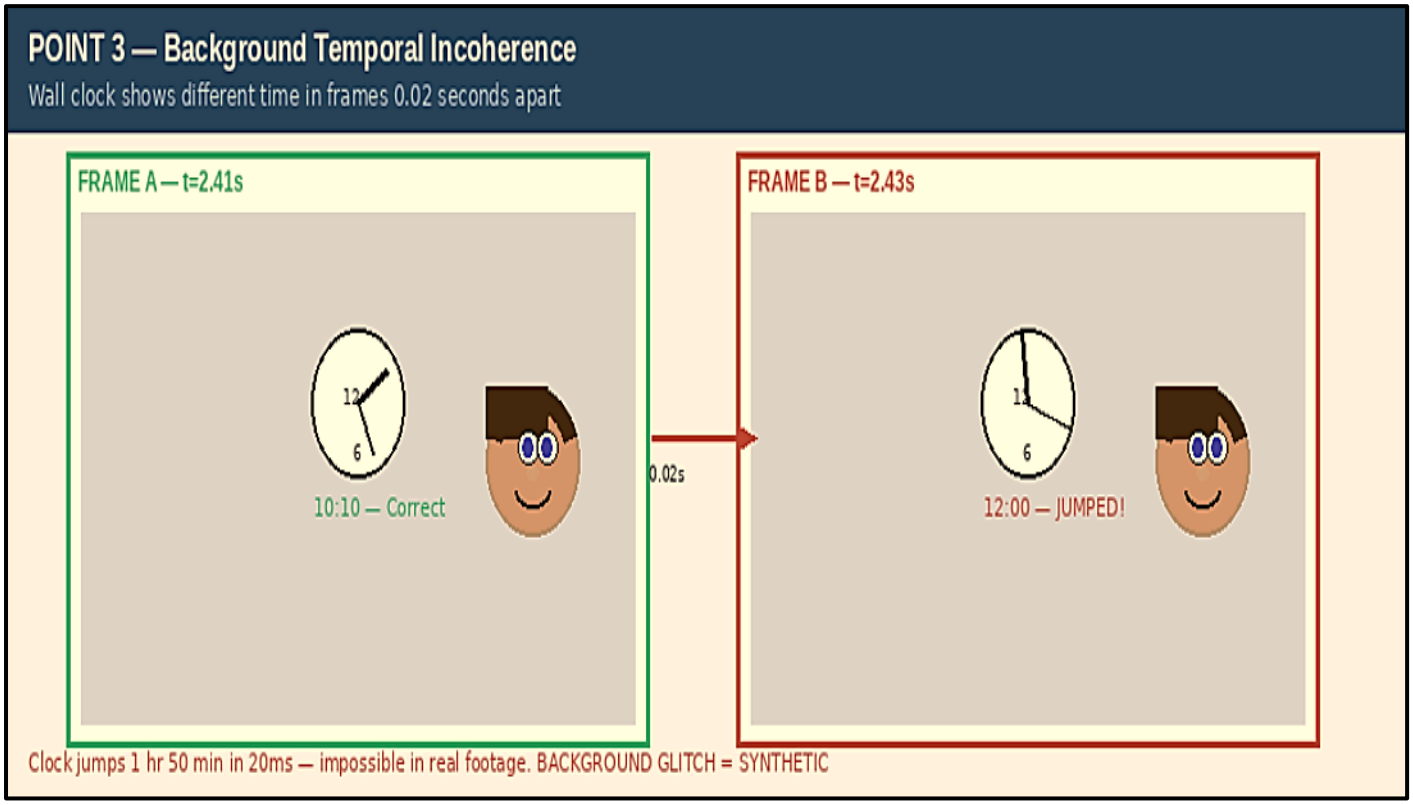
2. **Examine Lip Synchronisation Against the Audio Track**.

The lip-sync artifacts are created by generative models on bilabial sounds (b, p, m) and labiodental sounds (f, v). Play at 0.25x speed and analyse the lip movements for perfect synchronisation with the sound produced. A noticeable delay of around 200–300 ms or override; wherein lip movements do not sync with speaking sounds, is a key indicator of deepfakes.



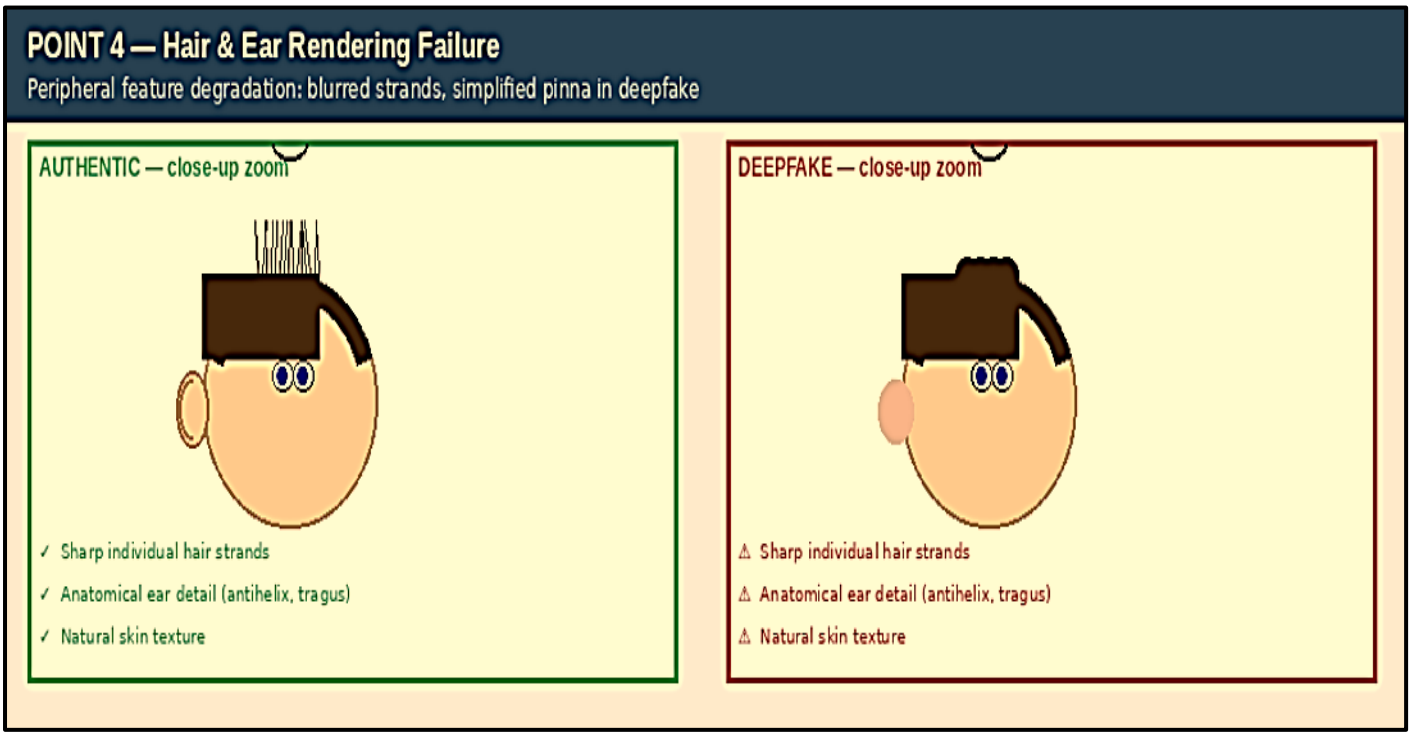
3. **Analyse Background Consistency and Temporal Coherence**.

Maintaining spatial coherence is another challenge faced by AI-created videos. Background objects such as clocks, signboards, furniture corners, texts on walls can shimmer, distort or change from frame to frame. It is an acknowledged temporal incoherence issue to have a clock showing different time just after 0.02 seconds which is impossible in real videos.



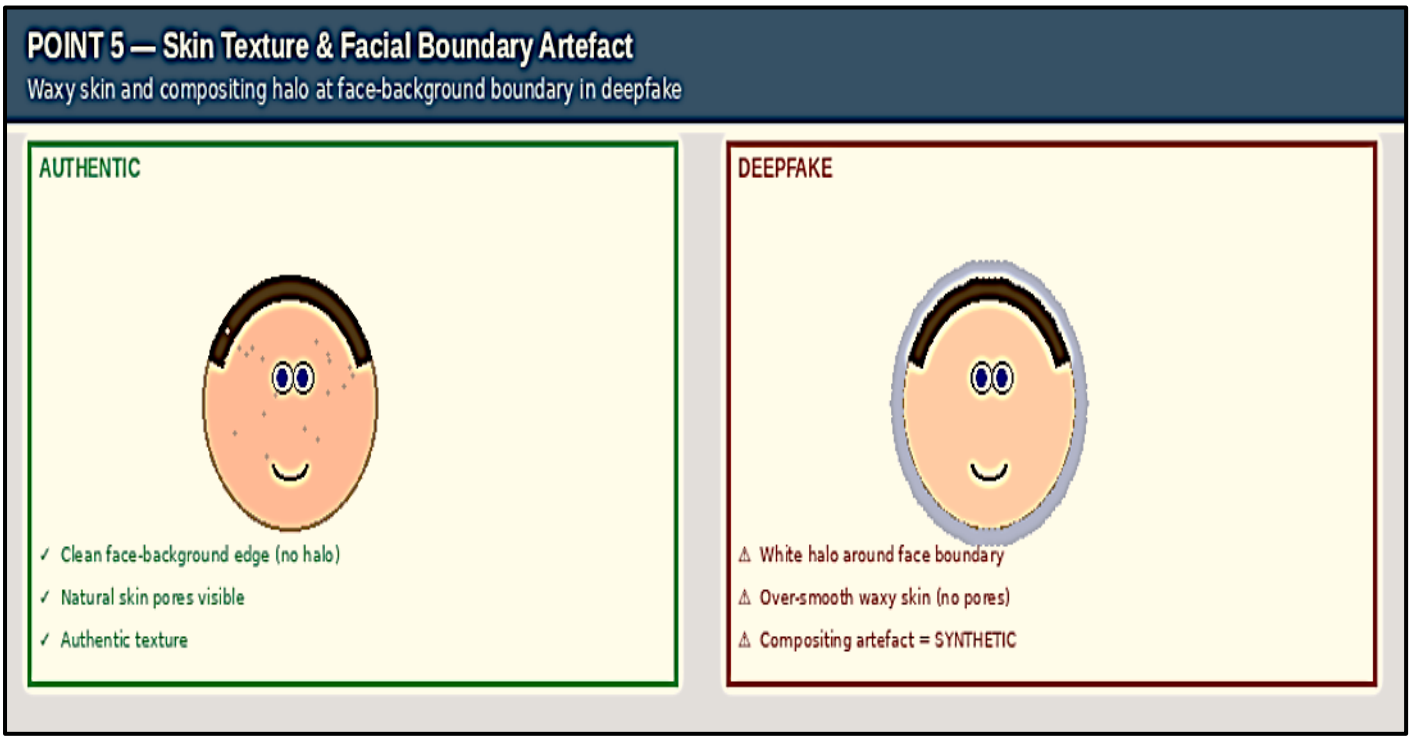
4. **Check Hair, Ear and Jewellery Rendering**.

The fine details, such as hairs, earrings, eyeglasses and the edge of collars, pose the greatest challenge to computer-generated images. Inspect these areas by zooming in as far as possible. Any blurring, hair smudging together and stylised ears are a sure sign of deepfakes.



5. **Verify Skin Texture and Facial Boundary Artefacts**.

A face created using AI usually displays an abnormal wax-like appearance or a bright circle around the place where the face borders the neck, hair or background. The presence of such compositing artifacts shows that the face was created independently of the background image.

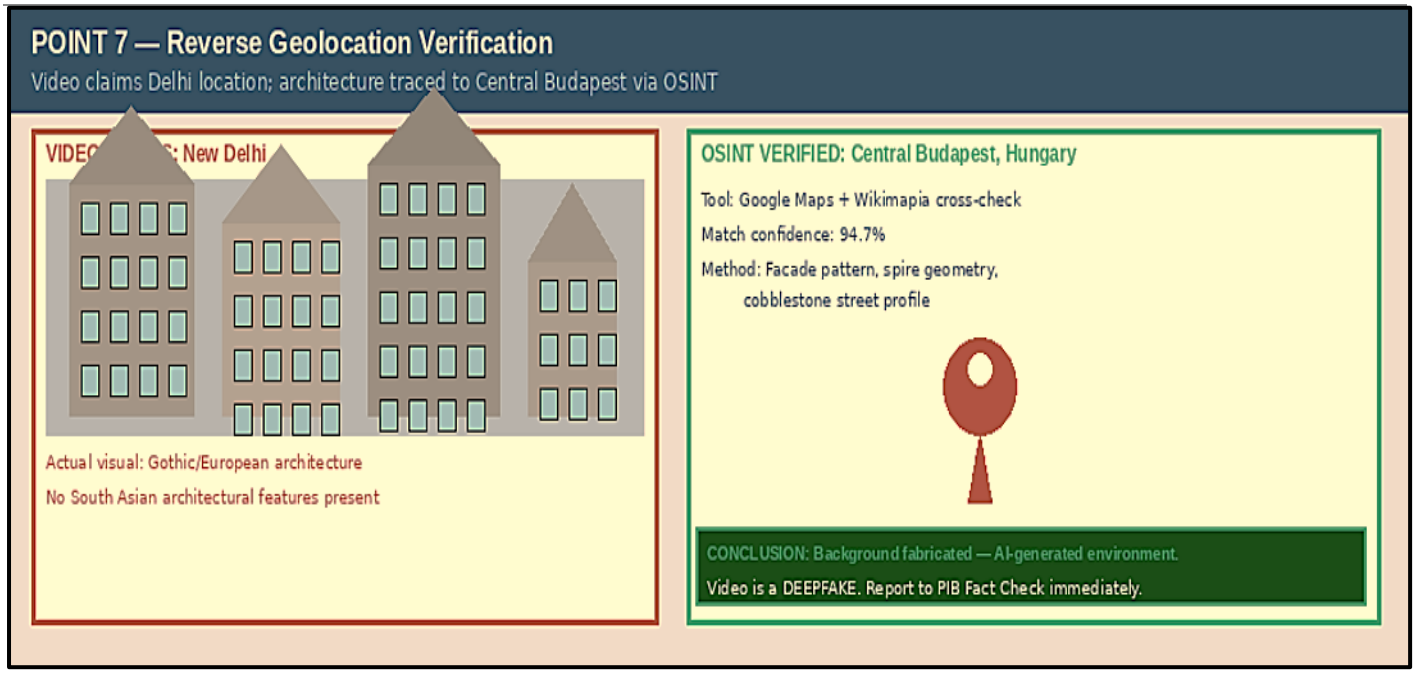


6. **Interrogate Audio-Visual Environmental Coherence**.

Compare the physical sound environment to that visually depicted. A video shot to show an open-air demonstration attended by many people should have at least 65 to 80 dB of ambient noise due to the crowd. The measurement of sound level of about 12 dB, which amounts to nearly silence, contradicts the visual depiction of a large assembly of people.

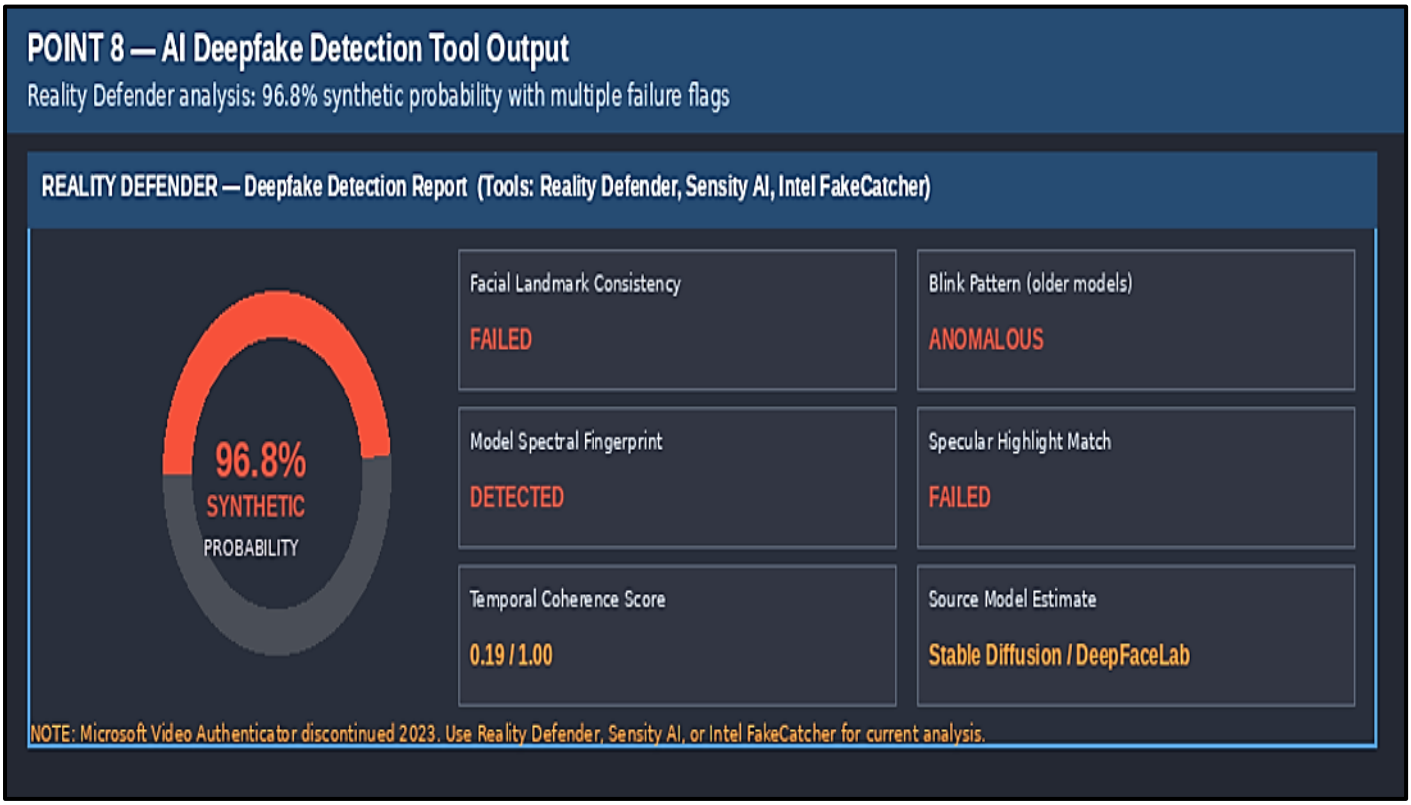
7. **Perform Reverse Geolocation and Contextual Cross-Check**.

Find out any recognisable environmental clues in the video, like building styles, signs, vegetation, vehicle registration plates and road signs and then conduct reverse geolocating on Google Maps, Wikimapia and OpenStreetMap. AI-generated images often have geographic inconsistencies, for example, Central European Gothic-style buildings are named as a city in Southern Asia.



8. **Utilise Current AI-Powered Detection Tools**.

Implement the use of deepfake detection systems that can constantly improve: Reality Defender (www.realitydefender.com), Sensity AI or Intel FakeCatcher. Utilise InVID/WeVerify browser plugin to test videos on the internet. Follow Indian Army Fact Check as it is likely any deepfake video being flagged would have been debunked on that platform.



9. **Trace Provenance and Metadata Chain**.

Extract all available metadata using ExifTool. Original videos would contain details about camera manufacturer and model, geolocation data if present and time stamps when captured. Lack of camera metadata along with the mention of video editing software like DaVinci Resolve or Stable Diffusion WebUI in the Software metadata category proves tampering.

POINT 9 — Video Metadata Forensics (ExifTool)

Camera metadata absent; video editing software signature present

ExifTool v13.x — Metadata Report

FIELD	VALUE	ANALYSIS
File Name	[redacted]	
File Creation Date		
Camera Make	NOT PRESENT	⚠ Missing — authentic videos retain this
Camera Model	NOT PRESENT	⚠ Missing — authentic videos retain this
GPS Coordinates	NOT PRESENT	⚠ Missing if GPS was enabled on device
Software	DaVinci Resolve + Stable Diffusion WebUI	⚠ AI generation + editing software
Video Encoder	libx264 (re-encoded 2x)	⚠ Re-encoding destroys original metadata
Original Capture Device	NOT PRESENT	⚠ Cannot be traced to any camera
Chain of Custody	BROKEN — re-encoded from synthetic source	⚠ CONFIRMS fabrication

10. **Apply the SIFT Protocol Before Every Share**.

The SIFT method (developed by Mike Caulfield, Washington State University) provides a four-step verification framework: Stop, which means taking time before sharing information; Investigate the source, which means researching about an account's age, track record and verification status; Find better coverage, meaning ensuring that two or more reliable media houses have confirmed the same occurrence; and Trace claim to its source. Information that does not meet these criteria should never be shared.

POINT 10 — SIFT Protocol (Mike Caulfield, Washington State University)

Stop · Investigate Source · Find Better Coverage · Trace Claims

S

STOP

Pause immediately.
Do not share.
Take a breath.

I

INVESTIGATE SOURCE

Who made this?
Account age?
Verification status?

F

FIND BETTER COVERAGE

Do 2+ trusted outlets report this event?
Check DD, PTI, PIB.

T

TRACE THE CLAIM

Where did it originate?
Anonymous? New account?
Any corroboration?

Rule: Content that cannot be verified through 2 independent credible sources MUST NOT be shared, regardless of emotional impact.