PARAVISION

A Guide to Deepfake Detection in Interviews and Hiring

Hiring is rapidly moving online. Video interviews, both live and pre-recorded, have become the norm for many organizations seeking to evaluate candidates efficiently and in support of remote or hybrid work. But as recruitment moves online, so do new forms of deception. The emergence of deepfakes has created serious risks for HR and recruiting teams.

Today, anyone can access tools that convincingly swap faces or create synthetic personas. In hiring, these technologies can be exploited to misrepresent identity, qualifications, or eligibility to work. Reports of “deepfake interview” incidents, where applicants use manipulated video feeds to impersonate others, are increasing across industries.

Organizations need tools that can detect these synthetic threats with speed, accuracy, and fairness – without disrupting legitimate applicants. This is where Paravision Deepfake Detection comes in.

November 2025

The Deepfake Threat in Hiring

As deepfake technology becomes more accessible, attackers are finding new ways to exploit hiring and verification processes. These digital deceptions go beyond simple identity theft, creating entirely fake applicants, hiding the real people behind interviews, or mimicking trusted professionals to gain access to sensitive systems.

IMPERSONATION & IDENTITY THEFT

Attackers can use deepfakes to impersonate real individuals – such as cleared contractors or skilled professionals – by overlaying another person's likeness during live interviews. Once hired, these impostors can gain unauthorized access to sensitive systems or data.

SYNTHETIC IDENTITIES

Fraudsters are also creating entirely fictitious personas, supported by fabricated documents and AI-generated profile images. Without deepfake detection, these candidates can slip through standard screening processes undetected.

CREDENTIAL LAUNDERING & OUTSOURCIND

Some applicants use deepfakes to disguise who is actually speaking, allowing someone else to complete the interview on their behalf or to evade geographic or compliance restrictions. These incidents are especially common in remote and contract-based work environments.

Scenario	What the Recruiter Sees	Who's Actually Speaking	Core Risk
Impersonation & Identity Theft	Recruiter sees candidate Alice, a qualified professional with needed credentials.	Actually Beatrice, an impostor using Alice's face without Alice knowing.	Beatrice could gain access to company data using Alice's identity.
Synthetic Identities	Recruiter sees candidate Charlie, whose profile looks real.	No real person exists, and the full profile is AI-generated.	A completely fake candidate passes screening.
Credential Laundering & Outsourcing	Recruiter sees candidate Dana on the video call who seems competent.	Eve, a different person, is answering questions behind the scenes using Dana's likeness.	Dana hires Eve to pass the interview or to outsource the work to a person in a different geographic location.

Why Conventional Measures Fall Short

Conventional background checks and video interviews can confirm a person's resume or connection, but not the authenticity of their video. Even skilled recruiters struggle to detect subtle AI manipulations, as modern deepfakes are photorealistic, consistent, and difficult to spot in real time. This is further compounded by the challenges of video communications: poor bandwidth, high compression, and low frame rate can all further obscure AI-manipulated imagery.

Human judgment alone is no longer enough. Automated deepfake detection adds the critical layer of assurance needed to validate digital interactions at scale.

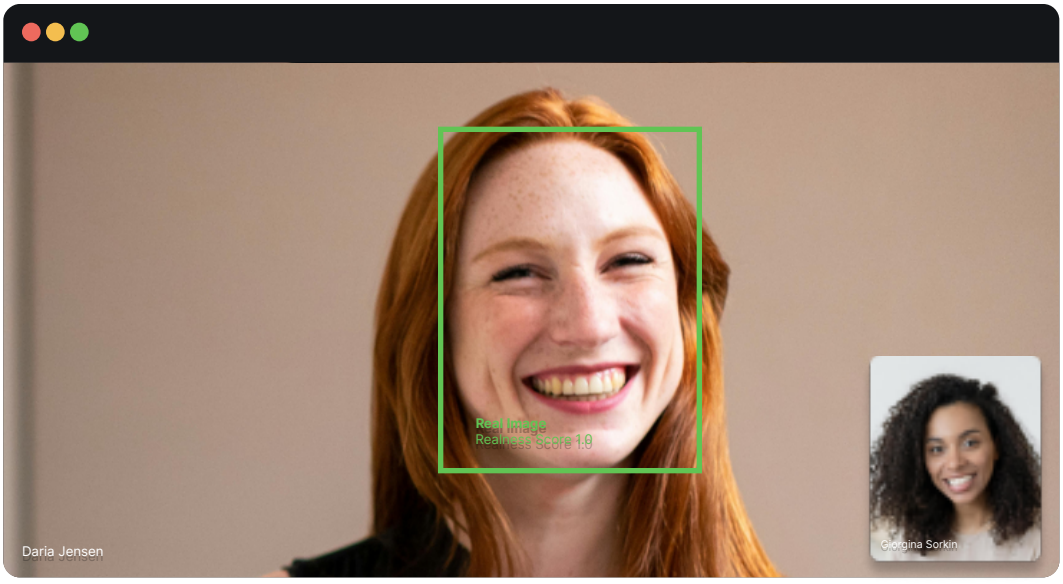
Paravision Deepfake Detection

Paravision Deepfake Detection enables organizations to verify that the faces presented in digital interviews and onboarding sessions are genuine. Using advanced AI, it identifies the subtle textures and other pixel-level information that reveal synthetic manipulation – far beyond what the human eye can perceive.

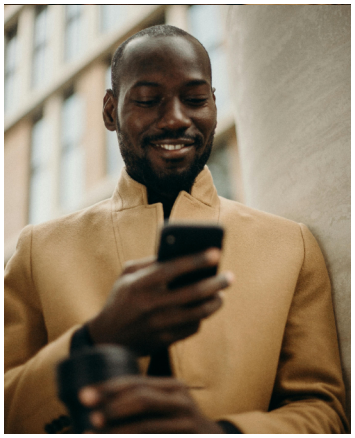
Human judgment alone is no longer enough. Automated deepfake detection adds the critical layer of assurance needed to validate digital interactions at scale. Paravision Deepfake Detection detects multiple forms of manipulation, including:

- Face Swaps: One person's face digitally replaced with another's
- Expression Swaps: Altered facial movements or emotional cues
- AI-Generated Faces: Fully synthetic personas created using generative AI

Each image or video is analyzed and assigned a realness score, flagging content that may have been altered or generated. These insights can be used to automatically trigger enhanced verification or manual review.



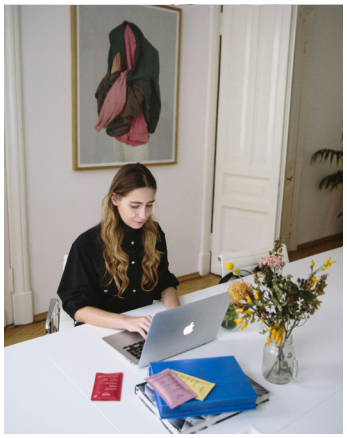
Integrating Deepfake Detection Into the Hiring Workflow



01

Candidate Screening

Paravision Deepfake Detection can be used during early screening in parallel with an IDV (Identity Verification) workflow to confirm candidate identities, and to ensure candidate videos or images are authentic and unaltered.



02

Live Interview Protection

Integrated into HR or video platforms, Paravision Deepfake Detection can analyze live feeds in near real-time, detecting signs of manipulation and alerting recruiters to suspicious activity without disrupting the interview.

03

Post-Interview Review

Recordings can be analyzed after completion to confirm authenticity, providing a valuable audit trail for compliance in sectors such as finance, defense, or government contracting.

Benefits for Employers and HR Platforms

PREVENT FRAUD AND ESPIONAGE	Prevent unauthorized individuals from gaining access to internal systems or sensitive information.
PRESERVE FAIRNESS AND TRUST	Ensure legitimate candidates are evaluated on their merits, not displaced by AI-enabled impostors.
STAY AHEAD OF EVOLVING THREATS	Continuous model updates protect against new generations of synthetic media attacks.

PARAVISION

Trusted Identity AI

For more information or to schedule a demo, please contact us at:

info@paravision.ai