DeepFake Analysis Report

Analysis Date: 5/22/2025, 1:47:16 AM

Executive Summary

This report presents a comprehensive analysis of the submitted media for potential deepfake manipulation. It includes technical metadata, detection results, and a risk assessment to help understand the authenticity of the content.

Key Results

Prediction: Fake

Confidence: Very Low%

Frames Analyzed: 200

Detection Results

What does this mean?

The analysis shows the percentage of frames that exhibit characteristics of manipulation versus those that appear authentic. Higher fake percentages indicate a greater likelihood of deepfake manipulation in the content.

Technical Metadata

Technical metadata provides important information about the file's properties, format, and encoding. This information can help identify inconsistencies that may indicate manipulation.

Basic Details

Property	Value
Filename	01_02__talking_angry_couch__YVGY8LOK.mp4
File Size	10.98 MB
Format	Unknown

Technical Details

Property	Value
Codecs	Unknown
Bit Rate	Unknown
Start Time	Unknown
Streams	Unknown

Understanding the Technical Metadata

Codecs: Compression technologies used in the file. Unusual codec combinations may indicate manipulation.
Bit Rate: The amount of data processed per second. Inconsistent bit rates across frames can indicate editing.
Streams: The number of media streams in the file. Unexpected stream counts might indicate manipulation.

Software & Risk Analysis

Software information reveals tools used to create or modify the file. Certain software combinations are common in deepfake creation.

Software Information

Property	Value
Encoded By	
Error	
Writing Application	Lavf58.26.101
Writing Library	

Risk Assessment

Risk Level: Elevated risk - ffmpeg tools often used in video manipulation

This assessment evaluates the likelihood that the media has been manipulated based on the technical characteristics and software signatures detected. It considers patterns common in deepfake creation tools and techniques.

Understanding Software Indicators

Writing Application: The software used to create the file. Certain applications are commonly used in deepfake creation.

Writing Library: The underlying software libraries used. Some specialized libraries are associated with media manipulation.

Error Information: Errors in the file structure may indicate rushed editing or manipulation attempts.

Encoded By: Identifies the encoding software used, which can reveal inconsistencies in the media's creation process.

Detailed Analysis & Recommendations

Analysis Methods

This analysis employed multiple detection algorithms to identify deepfake indicators including:

- Facial inconsistency detection
- Audio-visual synchronization analysis
- Metadata examination
- Digital fingerprint analysis
- Temporal consistency evaluation

Each method contributes to the overall confidence score, with multiple confirmations strengthening the assessment reliability.

Common Deepfake Indicators

Indicator	Description
Unnatural blinking	Deepfakes often struggle to accurately reproduce natural eye blinking patterns
Facial boundary issues	Poor blending at edges where manipulated faces meet original video
Audio-visual mismatches	Lip movements that don't sync precisely with spoken words
Metadata inconsistencies	Unusual software signatures or editing patterns
Unnatural lighting	Inconsistent shadows or lighting that doesn't match across the face

Recommendations

Based on the analysis results, we recommend the following:

1. Treat this content with appropriate skepticism based on the detection confidence level

2. Request additional verification from the content source if being used for important purposes

3. Consider conducting additional analysis if the content is critical for decision-making

4. Be aware that deepfake technology continues to evolve, and detection methods must evolve alongside it