sensity

Deepfake Detection Report

#37514

TABLE OF CONTENTS

1. Report Summary

Overall Summary

Based on the outcomes of each independent assessment, the content is classified as **suspicious** and may warrant further expert review depending on the context of use.

Pixel And Voice Analysis

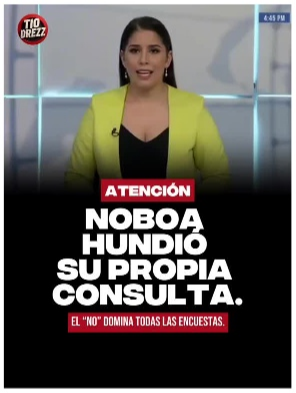
The file exhibits flags for **AI-generated elements**, with detection of **potential lipsync in visual features and voice synthesis in audio features**.

Forensic Analysis

Forensic file analysis shows no indicators pointing to generation platforms or manipulation.

2. Submission Details

Report Status	Suspicious
User Name	valeria@lupa.com.ec
Submission Date	14 November 2025 10:36:27



Analysis Overview

Face Manipulation	Suspicious
AI Generated Content	Valid
Voice Analysis	Suspicious
Forensic Analysis	Valid

File Details

File Name/URL	ssstik.io_@tiodrezzec_1763134364018.mp4
File Type	video
File Hash (SHA256)	d13637655580e86f615e7179602fff72271e8d101e401f0c43e95cddd0093828
File Size (KB)	5224589
Duration	01:49
File Resolution	576 × 768

3. Full Analysis

3.1. Pixel Analysis

3.1.1. Face Manipulation

Our proprietary algorithm checks for facial manipulations by learning to recognize visual artifacts and inconsistencies commonly introduced by AI generators. The method follows the approach of [1]. Heatmaps are generated post-hoc by [2].

Result	⊗ **Suspicious**
Confidence	89.8%
Manipulation Type	lipsync

Visual Explanations
A higher confidence score indicates a greater probability that the file contains characteristics consistent with AI-generated or manipulated content, with at least 50% certainty. View heatmap/s below for suspect face regions.

Pixel based assessment
The heatmap depicts the areas where the model detected a higher likelihood of synthesis at the pixel level.

[1] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Niessner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in *IEEE Xplore*, IEEE, Oct. 2019, pp. 1–11. doi: https://doi.org/10.1109/ICCV.2019.00009.

[2] R. Draelos and L. Carin, "Use HiResCAM Instead of Grad-CAM for Faithful Explanations of Convolutional Neural Networks," arXiv.org, Nov. 2021. Available: https://arxiv.org/abs/2011.08891

3.1.2. AI Generated Content

Our proprietary algorithm checks for AI-generated content by identifying low-level artifacts left by image and video generators. The method follows the approach of [1]. Heatmaps are generated post-hoc by [2]. Segment-level explanations are generated post-hoc by [3].

Result	✓ **Valid**

[1] S.-Y. Wang, O. Wang, R. Zhang, A. Owens, and A. Efros, "CNN-generated Images Are Surprisingly Easy to spot... for Now," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Los Alamitos, CA, USA: IEEE, Apr. 2020, pp. 8692–8701. Available: https://doi.org/10.1109/CVPR42600.2020.00872

[2] R. Draelos and L. Carin, "Use HiResCAM Instead of Grad-CAM for Faithful Explanations of Convolutional Neural Networks," arXiv.org, Nov. 2021. Available: https://arxiv.org/abs/2011.08891

[3] X. Zhao *et al.*, "Fast Segment Anything," arXiv.org, Jun. 2023. Available: https://arxiv.org/abs/2306.12156

3.2. Voice Analysis

Our proprietary algorithm detects AI generated voices by analyzing subtle acoustic artifacts that are commonly introduced during speech generation by AI. The method follows the approach of [1].

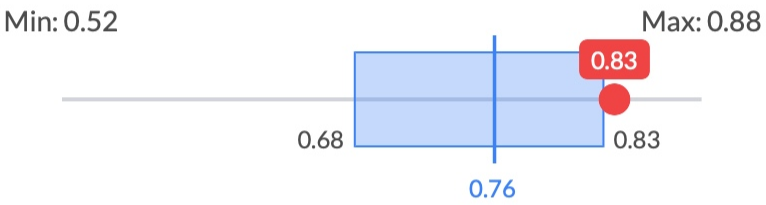
Speaker	Result	Language	Gender
Speaker 1	Suspicious - 93.7%	Spanish(ES) - 99.0%	Female - 99.0%
Speaker 2	Valid	Spanish(ES) - 97.2%	Male - 98.8%

Speaker 1 - Outlier Audio Features

This analysis highlights potential indications of AI-generated or manipulated audio. The following features extracted from the input audio are compared to the distribution of natural human speech based on a collection of 1645 samples of Female speech in Spanish language. Each box plot represents the 10 and 90 quantiles of the natural distribution.

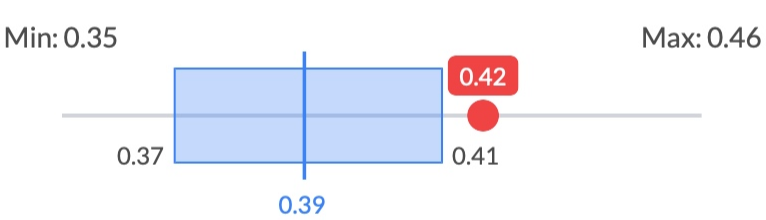
Naturalness

An overall measure of how human-like and fluent the audio sounds.



Spectral Artifacts

Unusual distortions or patterns in the frequency content of audio, often introduced by compression, synthesis, or editing.



[1] P. Kawa, M. Plata, and P. Syga, "SpecRNet: Towards Faster and More Accessible Audio DeepFake Detection," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Los Alamitos, CA, USA: IEEE, Oct. 2022, pp. 792–799. Available: https://doi.org/10.1109/TrustCom56396.2022.00111

3.3. Forensic File Analysis

Our forensic analysis suggests potential source platforms based on structural similarities to previously analyzed files using the approach of [1], metadata pattern matching, and verification of C2PA provenance certificates [2]. The matches presented are not definitive as they reflect patterns observed in our existing database, which is continually growing but not exhaustive. These findings should be interpreted as supporting signals rather than standalone conclusions, and are best used in combination with results from other detection methods.

Result	Valid

[1] M. Iuliani, D. Shullani, M. Fontani, S. Meucci, and A. Piva, "A Video Forensic Framework for the Unsupervised Analysis of MP4-Like File Container," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 635–645, Mar. 2019. https://doi.org/10.1109/TIFS.2018.2859760

[2] Coalition for Content Provenance and Authenticity, "Resources - C2PA," c2pa.org, 2025. https://c2pa.org/about/resources/

3.3.1 File Metadata Structure: Matched File History

For each file stored in our forensic library, the known and validated history of its provenance is tracked. When a submitted file matches a known metadata structure in our library, this section will include the matching file's most recent processing step, including its originating device.

Model

iPhone 8, iPhone X, iPhone XR

Most Recent Processing Step

TikTok

3.3.2 File Metadata Structure: Structural Validity Check

These tests assess whether the file has been altered at the binary level, such as through manual editing using a hex editor, as opposed to conventional video or audio editing software. If any modification or validation checks fail, the corresponding test and its results are documented in this section.

A failed test does not, on its own, confirm that manipulation has occurred. Instead, these findings should be interpreted within the broader context of the forensic analysis.

Modification Tests

No structural modifications have been detected.

3.3.3 File Metadata Structure: Decoded Metadata

File

File Name	9cf80061-8849-41e4-a7cf-871cc6ae0c2e.mp4
Directory	/tmp/tmpdjfrmypy
File Size	5224589
File Modify Date	2025:11:14 15:36:30+00:00
File Access Date	2025:11:14 15:36:30+00:00
File Inode Change Date	2025:11:14 15:36:30+00:00
File Permissions	100644
File Type	MP4
File Type Extension	MP4
MIME Type	video/mp4

Quick Time

Major Brand	isom
Minor Version	0.2.0
Compatible Brands	isom, iso2, avc1, mp41
Movie Header Version	0

Create Date	0000:00:00 00:00:00
Modify Date	0000:00:00 00:00:00
Time Scale	1000
Duration	109.411
Preferred Rate	1
Preferred Volume	1
Preview Time	0
Preview Duration	0
Poster Time	0
Selection Time	0
Selection Duration	0
Current Time	0
Next Track ID	3
Track Header Version	0
Track Create Date	0000:00:00 00:00:00
Track Modify Date	0000:00:00 00:00:00
Track ID	1
Track Duration	109.411
Track Layer	0
Track Volume	1
Balance	0
Audio Format	mp4a
Audio Channels	2
Audio Bits Per Sample	16
Audio Sample Rate	44100
Buffer Size	0
Max Bitrate	32013
Average Bitrate	32013
Matrix Structure	1 0 0 0 1 0 0 0 1
Image Width	576
Image Height	768
Media Header Version	0
Media Create Date	0000:00:00 00:00:00

Media Modify Date	0000:00:00 00:00:00
Media Time Scale	15360
Media Duration	109.4
Media Language Code	und
Handler Description	VideoHandler
Graphics Mode	0
Op Color	0 0 0
Compressor ID	avc1
Source Image Width	576
Source Image Height	768
X Resolution	72
Y Resolution	72
Bit Depth	24
Color Profiles	nclx
Color Primaries	1
Transfer Characteristics	1
Matrix Coefficients	1
Video Full Range Flag	0
Pixel Aspect Ratio	1:1
Video Frame Rate	30
Handler Type	mdta
Aigc Info	{"aigc_label_type":0}
Comment	vid:v14044g50000d4bboqvog65u14rc9vng
Vid Md5	37e7c1ea42bb4ccca43fc24cf2920f56
Encoder	Lavf58.76.100
Media Data Size	5134286
Media Data Offset	90303

Composite

Image Size	576 768
Megapixels	0.442368
Avg Bitrate	375413
Rotation	0

4. Scope and Conditions of Analysis

This document has been automatically generated to provide a technical assessment of submitted media. The report aims to identify signs of synthetic media manipulation or other digital alterations in support of threat intelligence, evidentiary documentation, or expert review.

The accuracy and reliability of this report are dependent on the integrity of the submitted media. We assume that the file was provided in its original state and has not been altered, cropped, edited, recorded via screen capture, or otherwise manipulated prior to submission.

Any modification of the original content by the submitting party, including changes to resolution, format, or playback method, may compromise the validity of the analysis. We cannot guarantee the forensic reliability of results derived from media that has not been preserved in its original form.

5. Legal and Compliance Declarations

GDPR Compliance Statement

We are committed to ensuring that all processing of personal data within its systems complies with the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR) [1].

Any personal data contained in this report has been processed lawfully, fairly, and transparently, and solely for the purpose of media analysis and threat detection. The data is subject to strict access controls, secure storage protocols, and data minimisation practices.

Where applicable, personal data is anonymized or pseudonymized, and retained only for as long as necessary to fulfill the legitimate interest of security analysis or contractual obligations to the client.

We act as a data processor or data controller depending on the context of engagement, and upholds data subject rights as defined under the GDPR, including the rights to access, rectification, erasure, and restriction of processing.

Clients are responsible for ensuring that any media submitted for analysis has been obtained and shared in accordance with applicable data protection laws and with appropriate legal basis for processing.

Statement of Impartiality

This report has been generated using automated tools and standardized procedures without bias or influence. No conflicts of interest are present.

Statement of Integrity

No modifications have been made to the original media during analysis. Where relevant, cryptographic hash values (e.g. SHA-256) have been computed to support data integrity verification.

As an auto-generated report, original file integrity verification must be conducted separately by the submitting party.

Statement of Limitations

This report is generated by automated analysis and is intended to support, not replace, expert forensic evaluation. The results should be interpreted in conjunction with contextual information and expert judgment.

Expert Use Declaration

This report is suitable for expert review and presentation in legal proceedings, when submitted by or under the supervision of a qualified expert.

Statement of Compliance

This report has been generated by our platform using automated systems and procedures, developed in accordance with recognized international standards for the handling and analysis of digital media evidence.

To the best of the company's ability, and within the constraints of an automated reporting process, the methodology and systems used align with the principles and requirements of the following international standards

- ISO/IEC 17025:2017 – General requirements for the competence of testing and calibration laboratories [2]
- ISO/IEC 17020:2012 – Requirements for the operation of various types of bodies performing inspection [3]
- ISO/IEC 27037:2012 – Guidelines for the identification, collection, acquisition, and preservation of digital evidence [4]

While this report is not produced within an ISO-accredited forensic laboratory, all reasonable steps have been taken to ensure the reliability, reproducibility, and transparency of the analysis.

This report is intended to support expert review and may be used as part of a wider evidentiary process when accompanied by appropriate oversight.

[1] General Data Protection Regulation (EU) 2016/679 (GDPR): The European Parliament and the Council of the European Union, "General Data Protection Regulation (EU) 2016/679 (GDPR)," General Data Protection Regulation (GDPR), May 04, 2018. https://gdpr-info.eu/

[2] ISO/IEC 17025:2017: International Organization for Standardization, ISO/IEC 17025:2017. Geneva, Switzerland: International Organization for Standardization, 2017. Available: https://www.iso.org/standard/66912.html

[3] ISO/IEC 17020:2012: International Organization for Standardization, ISO/IEC 17020:2012. Geneva, Switzerland: International Organization for Standardization, 2019. Available: https://www.iso.org/standard/52994.html

[4] ISO/IEC 27037:2012: International Organization for Standardization, ISO/IEC 27037:2012. Geneva, Switzerland: International Organization for Standardization, 2012. Available: https://www.iso.org/standard/44381.html

6. Appendix

Glossary of Terms

Term	Definition
AI-Generated Content	Media that has been partially or entirely produced using artificial intelligence models, such as deepfake generators.
Auto-generated Report	A report created automatically by software without manual intervention, relying on machine learning outputs and preset formats.
Benign	Returned when the file structure or metadata suggests creation via software typically embedded in cameras or other hardware-based capture devices.
Camera Original	A term indicating that a file is likely to have originated directly from a recording device without post-processing.
Confidence Score	A numerical value indicating the system's certainty in its detection outcome. Higher scores reflect greater likelihood of manipulation or authenticity.
Confidence Threshold	The predefined score level (e.g. 90%) above which a system considers its analysis result to be sufficiently reliable.
Critical	Returned when the file was created or modified using software, platforms, or tools commonly associated with synthetic media generation or manipulation.
Face Manipulation	The alteration or synthetic generation of facial features or expressions using AI techniques.
Metadata	Data about the data contained within a file.
Forensic Metadata Analysis	The examination of file attributes and metadata to determine origin, modification history, and consistency with known sources.
Hash Value (SHA-256)	A cryptographic fingerprint of a file used to verify integrity and detect any changes.
Heatmap	A visual representation that highlights areas of an image based on the model's confidence levels. Brighter or more intense colors typically indicate higher likelihood of AI-generated content at the pixel level.
Pixel-Level Analysis	A fine-grained assessment that evaluates individual pixels for features indicative of synthetic manipulation or generation.
Segment-Level Analysis	A higher-level evaluation where objects or regions in the image are grouped and assessed as units, based on visual features and AI pattern recognition.
Source Model / Generating Model	The AI system or architecture believed to have produced synthetic content (e.g., HeyGen, StyleGAN).
Suspect	Returned when the file has been created or processed by software, platforms, or tools that do not involve AI and are unlikely to have meaningfully altered the file's content.
Synthetic Media	Content that has been algorithmically generated or manipulated, often by machine learning models, including deepfakes.
Voice Manipulation	The artificial generation or modification of vocal audio using speech synthesis or voice cloning tools.