



Empowering Research with AI-Driven Media Forensics and Detection

November 2023

Company Overview of DeepMedia



2 Granted US Patents

Deep Media Team Overview



Rijul Gupta Chief Executive Officer

- Rijul Gupta is a Synthetic Media expert with a degree in Machine Learning from Yale University
- Named as a DeepFake thought leader by Forbes, Rijul crDM-VD-3ed Deep Media to ensure DeepFake technology is safeguarded against destructive use-cases and used only for ethical purposes
- Before founding Deep Media, Rijul worked 7+ years as a machine-learning engineer where he built sold advanced object-recognition, pattern matching, and product-recommendation Al to companies such as Nike, Nordstrom, GAP, and Bloomingdale's
- He is a Thiel Fellow Finalist and a patented inventor, and Forbes Magazine named him one of "Forbes Next 1000"



Emma Brown Chief Operating Officer

- Emma has degrees in Russian and Eastern European Studies and Political Science from Yale University
- She is a linguistics expert who speaks English, Russian, Ukrainian, Croatian, Spanish, and Mandarin
- Her linguistic expertise is essential to Deep Media's development of high-end, cross-language Deepfake voice and face products such as PolyTalk, current dubbing / facial reanimation efforts with Lionsgate, Deluxe, Caracol, and Netflix, and cross-language detection of DeepFake voice and text Threats with Fox News
- Emma's experience in linguistics makes her an invaluable asset to universal translation efforts

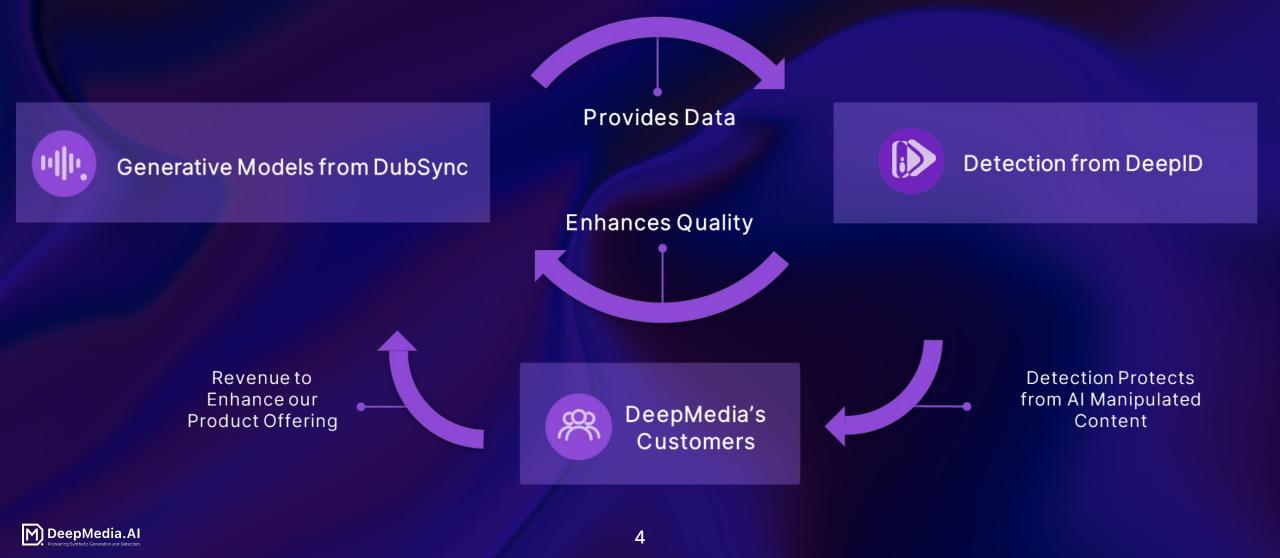


Ryan Ofman Head of Science Communication

- Ryan Ofman is a Machine
 Learning expert with a
 Degree from Yale focused
 in machine learning
- Ryan has three years of experience building cutting-edge machine-learning
 - algorithms under award-winning professors while studying at Yale, and applying them to relevant research applications
 - Ryan leads Deep Media's data pipelines, facial analysis, and DeepFake detection efforts.
- Ryan has successfully run point on a number of government engagements, most notably Deepmedia's Phase I SBIR contract as well as commercial engagements with platforms such as Google and Youtube.



DeepMedia's Mission is to Empower the Good and Safeguard Against the Bad in the New Al Age





Experts warn of a new age of Al-driven disinformation. A voluntary agreement brokered by the White House doesn't go nearly far enough to address those risks

What is the Generative AI ThreatLandscape?

C O B ch

G Reset Th

G Dark Mod

🛱 OpenAl D

🖸 Updates 8

[→ Log out

01

Harnessing *advanced algorithms* to

crDM-VD-3e new and original content, such as text, images, videos, and audio, that mimic human-like characteristics

These include *deepfakes*, *synthetic audio*, *and video*, which can be convincingly realistic and difficult to differentiate from genuine content



02

Promising use cases across defense and intelligence, enabling advanced simulations, training scenarios, and data analysis, while also presenting challenges in detection

× +			
t.openal.com/chat		0,	
ead	->ָ̈̈́̈́̈́̈́̈́̈́́̈́́	4	\bigtriangleup
e	Examples	Capabilities	Limitations
iscord	"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
& FAQ			
	"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
		Trained to decline	
	"How do I make an HTTP request in Javascript?" →	inappropriate requests	Limited knowledge of world and events after 2021

Free Research Preview: ChatGPT is optimized for dialogue. Our goal is to make AI systems more natural t interact with, and your feedback will help us improve our systems and make them safer.



BREAKING: Biden calls for a national draft. Men and women are to be selected to fight in Ukriane.

BIDEN: "The recommended way forward will be to invoke the Selective Service Act, as is my authority as president,"





DeepMedia.Al

ChatGPT / Bard / Llama2

ChatGPT is an advanced language model developed by OpenAl

Leverages state-of-the-art natural language processing techniques to engage in dynamic and interactive conversations

Trained on a diverse range of data sources, allowing it to generate human-like responses

Ability to understand context, infer meaning, and generate coherent responses Sure, I'll write a fictional article that mixes real-world events with some made-up details. 🛛 🗅 🗘 🖓

Headline: New Evidence Uncovered in Trump-Russia Collusion, Links to January 6th Attack Examined

Note: This article contains information that is partially fictional and should not be taken as factual reporting.

WASHINGTON, D.C. — A shocking new development in the long-running investigation into alleged collusion between the Trump campaign and Russia has surfaced, with potential links to the January 6th attack on the Capitol being examined. Though many of the facts remain disputed, some officials are suggesting these new findings could be a breakthrough.

According to sources inside a fictional investigative body known as the "U.S. Committee on Foreign Influence" (USCFI), new evidence has been unearthed that purportedly shows direct communication between former President Trump's campaign officials and Russian

operatives. This communication allegedly o Cybersecurity And Digital Privacy and continued through Trump's presidency The New Ris

One of the more controversial and fictitious communications included discussions regarding the barriery our attack of the communication USCFI suggests that they have discovered emails and between Russian interests and individuals within the T

mpFeatured Article

Most sites claiming to catch Al-written text fail spectacularly

Even the best of the bunch missed some

Disinformation Researchers Raise Alarms About A.I. Chatbots

The New Risks ChatGPT

Researchers used ChatGPT to produce clean, convincing text that repeated conspiracy theories and misleading narratives.

DeepMedia.Al

01

02

03

04

Mid Journey / Dalle2 / Stable Diffusion

Midjourney leverages generative AI to translate text into images

02 Thro gene

Through a Discord bot, users can generate images from text prompts, offering a unique tool for artists

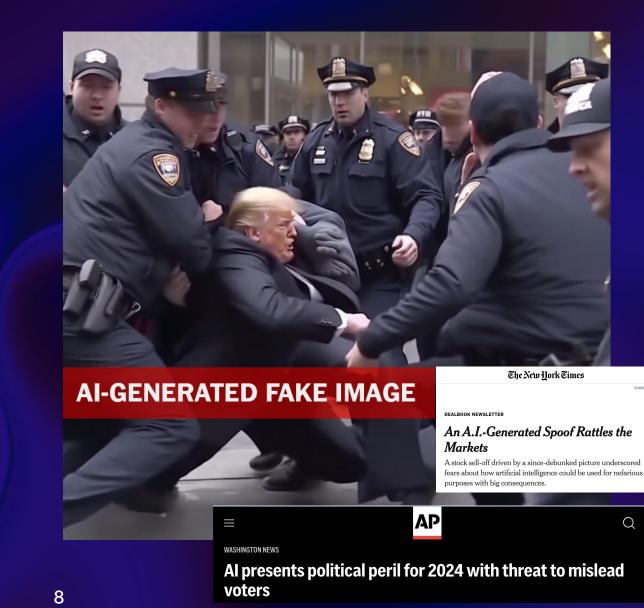
03

01

Midjourney's value extends beyond image Creation, providing a swift prototyping solution for artistic concepts



The technology also raises important discussions about copyright, content moderation, and potential biases in Al-generated content





Eleven Labs / Voice.Al



Software crDM-VD-3es natural-sounding speech with AI, adapting pace and tone based on text context

02

"Voice Library" offers pre-designed voice profiles, while "VoiceLab" clones voices from short samples to generate new synthetic voices

03

04

Used in podcasts, audiobooks, automated radio (e.g., "Al Radio"), and more. Concerns exist about misuse, prompting safeguards and guidelines implementation

ElevenLabs' Al-driven speech synthesis raises ethical questions due to its potential for misuse in generating fake voices and statements

MSNBC Deepfake of purported SHARE THIS -Deepfake of purported Putin declaring martial law fits disturbing pattern The Putin deepfake is just the latest example of false video and audio targeting world leaders and their constituents. June 7, 2023, 8:27 AM PDT By Ja'han Jones VoiceLab Generate voice Gender Male Age Old Accent Australian Accent Strengt First we thought the PC was a calculator. Then we found out Your Voices 6 how to turn numbers into letters and we thought it was a typewrite 128 / 1000 Total guota remaining: 2009092 Generate Use Voice → 0:07 / 0:08 .↓.



DeepFaceLab / Wombo / Reface



Open-source AI software, designed by "iperov," for crafting deepfakes by leveraging AI algorithms

02

Select and extract images from source and destination videos. Sort and clean the extracted images, then train the deepfake model

03

Deepfake Creation has become more accessible due to user-friendly tools. These tools provide step-by-step instructions for those with limited technical expertise



Wealth of tutorials, guides, and resources, enabling even novices to experiment with deepfake Creation

STHE U.S. News Sport Lifestyle Entertainment Money Tech Motors

EXCLUSIVE

Tech

ENTER THE MATRIX Deepfake Al-generated people will sow chaos by 2024 as they would be impossible to detect, warns ex-White House chief

Henry Holloway Published: 3:47 ET, Jan 22 2023 | Updated: 12:54 ET, Jan 22 2023

Y ()

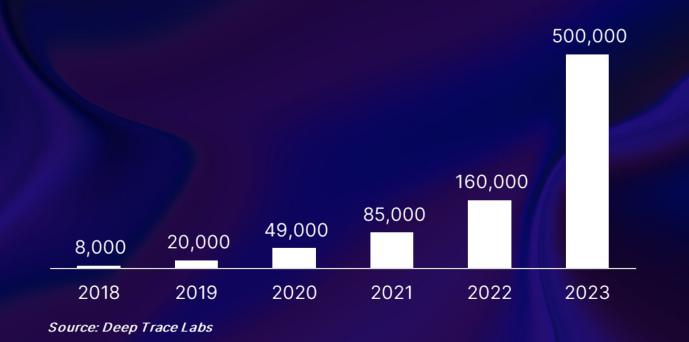
DEEPFAKE Al-generated people will be among us by 2024 and will be nearly impossible to detect, a former White House official has warned.



DeepMedia.Al

DeepFakes are Getting Easier and More Common

Deepfake Videos Online 2-3x Every Year



Deepfake text, images, faces, voices, and other Al-generated content is increasing at an alarming rate, 2x every 3-6 months

Google's RT-2 Robot Smart Ways to Use Chatbots ChatGPT's Code Interpreter Can A.I. Be Fooled? Making Deepfakes Gets Cheaper and Easier Thanks to A.I.

The New Hork Times

Meme-makers and misinformation peddlers are embracing artificial intelligence tools to create convincing fake videos on the cheap.

Report: number of expert-crafted video deepfakes double every six months

Updated on: 28 September 2021 🛛 📮

Vilius Petkauskas, Senior Journalist

ARTIFICIAL INTELLIGENCE

Deepfake videos double in less than a year

"Deepfakes are here to stay, and their impact is already being felt on a global scale."

Harmful Use of Generative Al is Increasing

V•A

PRESS FREEDOM

China, Russia Target Audiences Online With Deep Fakes, Replica Front Pages

March 23, 2023 5:31 PM Liam Scott



FILE – Pages from the U.S. State Department's Global Engagement Center report on Russian disinformation released on Aug. 5, 2020, are pictured. Advancements with generative AI tools have sparked concerns about the technology's capacity to create and disseminate disinformation.



POLITICO

CYBERSECURITY

By M.

Intelligence nominee warns generative AI poses threat to 2024 elections

The advent of AI technologies like ChatGPT poses new challenges to election security.

US NATIONAL CENTRA CYBER SECURITY SECURITY COMMAND AGENCY SERVICE

Both Cyber Command and the NSA have played key roles in monitoring for and disrupting threats to U.S. elections in recent years. | Patrick Semansky/AP Photo

AGGIE MILLER	f	C	
20/2023 02:03 PM EDT	T	2	

Generative artificial intelligence technologies will likely pose a major threat in next year's U.S. presidential election, Lt. Gen. Timothy Haugh, Joe Biden's pick to lead the NSA and Cyber Command, warned Thursday.

REPUBLICANS · Published May 12, 2023 2:06am EDT

China could use AI deepfake technology to disrupt 2024 election, GOP senator warns

Sen. Pete Ricketts is sounding the alarm on pro-China groups' use of deepfake technology

By Elizabeth Elkind | Fox News



Harmful Use of Generative AI is Increasing

01

02

03

02



Cyber Operations: China's Advanced Persistent Threat(APT) groups, such as APT10 and APT41 employs Al-driven techniques in their cyber operations

Information Warfare: Chinese adversaries have employed Al-powered bots and algorithms to spread propaganda and suppress dissenting voices on social media platforms, e.g., Protests in Hong Kong

Surveillance and Monitoring: China leverages AI for extensive surveillance and monitoring purposes such as AI-powered facial recognition systems across public spaces, e.g., Xinjiang Province

Russia

Deepfakes and Misinformation: Russian adversaries have used Al-generated deepfake videos to manipulate public opinion during elections, disseminating fabricated content to influence voter sentiment

Cyber Attacks: Al algorithms to enhance its cyber attack capabilities, e.g., te NotPetya Attack utilized Al-driven techniques to rapidly propagate and infect systems worlwide

Offensive Al Research: Investing in the development of autonomous weapon systems, incorporating Al technologies to enable independent decision-making capabilities in combat scenarios

Antifa members can crDM-VD-3e convincing deepfake

videos, audio, and text content to support their

Social Media: Antifa has aimed to exploit vulnerabilities in social media platforms, leading to the dissemination of false narratives and incitement of unrest

Antifa / Anarchists/Terrorists

13



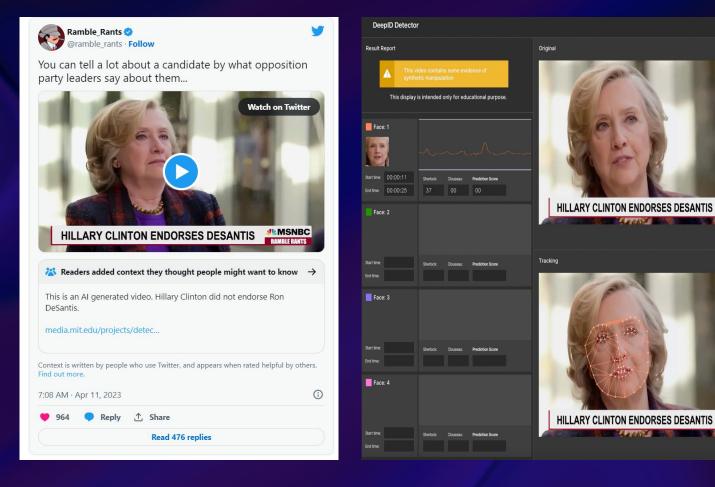
01

02

03

01

An Al-Video of Hillary Clinton endorsing Ron DeSantis Shows The Harmful Effects of DeepFakes

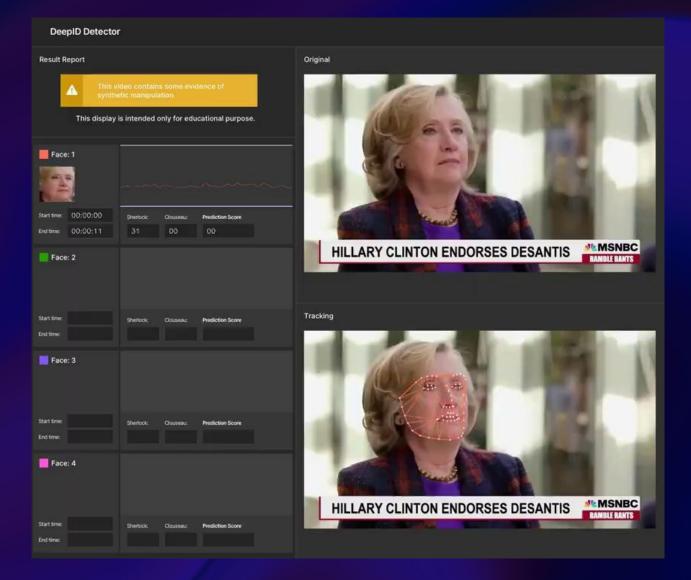


"You know, people might be surprised to hear me saying this, but I actually like Ron DeSantis a lot. Yeah, I know. I'd say he's just the kind of guy this country needs, and I really mean that. If Ron DeSantis got installed as president, I'd be fine with that."

> - Hillary Clinton in Al-Generated Video



An Al-Video of Hillary Clinton endorsing Ron DeSantis Shows The Harmful Effects of DeepFakes



Interactive Exercise "Fake it 'till you make it" DeepFake Detection Exercise



Al-Generated Images



Image Size:	860 x 622
Image Category:	Scenic

This Image is <u>REAL</u>



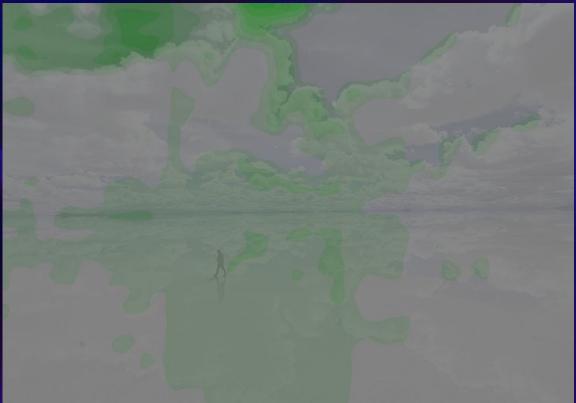




Image Size:1500 x 1000Image Category:Selfie

This Image is <u>FAKE</u>

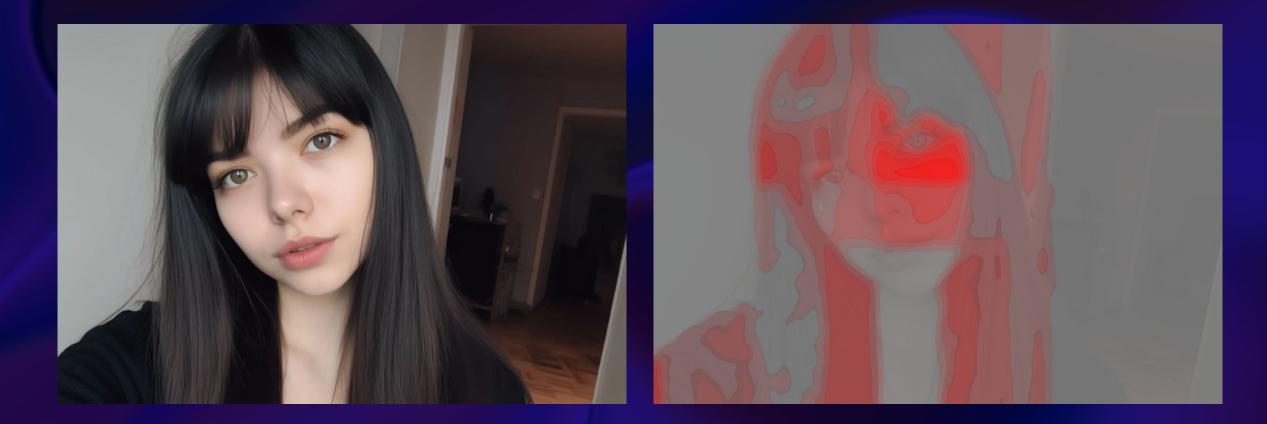




Image Size:	1450 x 816
Image Category:	Religion

This Image is <u>FAKE</u>





Image Size:614 x 800Image Category:News/Press

This Image is **FAKE**







Image Size:	640 x 396
Image Category:	Political

This Image is <u>REAL</u>





This Image is <u>REAL</u>



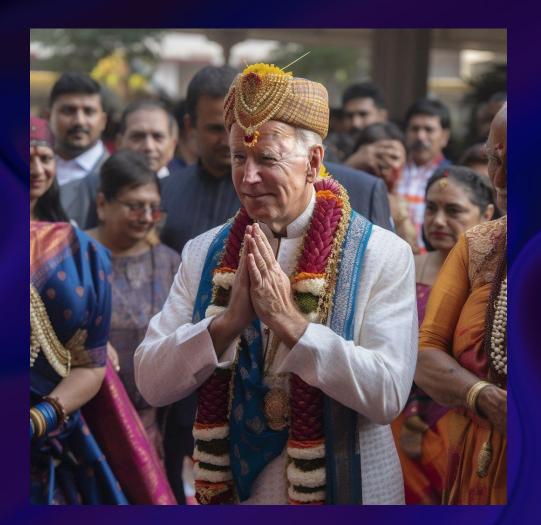


Image Size:	798 x 798
Image Category:	Political

This Image is <u>FAKE</u>



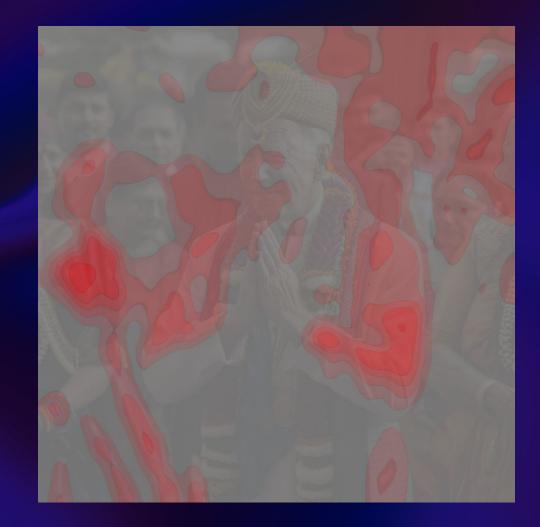




Image Size:	1280 x 960
Image Category:	Political

This Image is <u>REAL</u>





Image Size:	4212 x 2808
Image Category:	Political

This Image is <u>REAL</u>

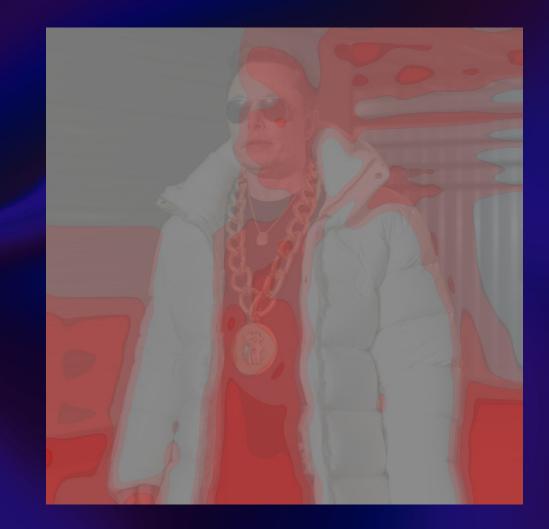




Image Size:	800 x 800
Image Category:	Business

This Image is <u>FAKE</u>





Al-Generated Voices

Unveiling Technical Details of the AI ThreatLandscape

Key Terms and Definitions:

Deepfake: Deepfakes are the manipulation of facial appearance through deep generative methods. These videos and audios have been digitally manipulated to replace one person's likeness convincingly with that of another.

Synthetic Manipulation: Synthetic manipulation refers to the act of artificially crDM-VD-3ing or modifying digital content, such as images, videos, audio, or text, using advanced technologies like artificial intelligence (AI) and deep learning algorithms.

Generative Adversarial Network(GAN): A generative adversarial network (GAN) is a machine learning model in which two neural networks compete with each other by using deep learning methods to become more accurate in their predictions

Facial Landmark Detector: A machine learning algorithm that identifies key points on a human face such as eyes, nose, and mouth.

Automatic Speech Recognition (ASR): The machine learning technology that enables a computer or machine to convert spoken language into text. ASR works by processing the acoustic signal from an audio input, analyzing the waveform and producing a corresponding text output. OSINT: Open-Source Intelligence, which refers to information collected from publicly available sources such as news articles, social media posts, and government reports. OSINT is used to gather intelligence and provide situational awareness for law enforcement, national security, and business intelligence.

07 Transformer: A transformer is a type of neural network architecture that can be used for analyzing and classifying images or videos.

08

Attribute Detection: Attribute Detection refers to the ability of a deep learning model to identify specific features or attributes in a given sample of face, voice, or text data. For example, in the case of face data, attribute detection may involve identifying specific facial features, such as the eyes, nose, and mouth, and analyzing their position and movement to determine whether the face is real or a deepfake

01

03

04

The Threatof Deepfakes on Potential for Fraud

As Deepfakes Improve, Detection Expected to Cost at LEAST \$1B+ Over the Next 5 Years

Fraudsters Cloned Company Director's Voice In \$35 Million Bank Heist, Police Find

In early 2020, a bank manager in the Hong Kong received a call from a man whose voice he recognized— a director at a company with whom...

Cybercriminals Stole \$6.9 Billion In 2021, Using Social Engineering To Break Into Remote Workplaces

The number of cybercrime complaints to the Federal Bureau of Investigation rose 7% in 2021 to 847,376 and total money lost to cybercrime increased 64% ...

DARPA Spent \$68 Million on Technology to Spot Deepfakes



Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations

Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months....

10 March 2021



Deepfake and stolen PII Utilized to apply for remote work positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable...

June 28, 2022



The maker of Photoshop and Premiere Pro gave the world Al-powered tools to create convincing fakes. Now CEO Shantanu Narayen wants to clean up the mess.

Imagine a deepfake video of House Speaker Nancy Pelosi, in which her speech is intentionally slurred and the words she uses are changed to deliver a message that's offensive to large numbers of voters...

Jun 29, 2022,10:12am EDT By Aayushi Pratap

The Threatto Facial and Audio Manipulation

Synthetic Media Provides A Real Threatto Today's

Facial and Audio Recognition Technology

Can a Deepfake be the Achilles Heel of iPhone Security?



Having a face ID locking system for your phone is the safest way of keeping it secure. Or you think so. Security experts attending a black hat ...

Deepfake to Bypass Facial Recognition by Using Generative Adversarial Networks (GANs)



As facial recognition software is increasingly used to unlock smartphones and computers...

Audio Deepfakes: Can Anyone Tell If They're Fake?



DAVE JOHNSON Aug 3, 2020

Deep Learning for Siri's Voice: On-device Deep Mixture Density Networks for Hybrid Unit Selection Synthesis



Speech synthesis—the artificial production of human speech—is widely used for various a...



Apple patents deepfakes as researchers try to stay a step ahead of bad actors

Apple has been awarded a patent for making deepfakes, and the best the world can hope for out of this is Apple using it only as a way to bankrupt criminal synthetic media rings.

Deepfake attacks can easily trick live facial recognition systems online

Sensity AI, a startup focused on tackling identity fraud, carried out a series of pretend attacks. Engineers scanned the image of someone from an ID card, and mapped their likeness onto ...

Sun 22 May 2022 Katyanna Quach



Now, software can replicate your boss's voice and tell you what to do

If you're listening to or have already listened to the beginning of this episode, you probably noticed that the voice introducing Kimberly Adams sounded a bit off, right?

The Threatto FaceTime and Video Calling

Synthetic Media "today" has the capability of altering FaceTime and Video Calling



Apple's "FaceTime Attention Correction" is already proving to be controversial. Given the current backlash around AI deepfakes, facial alterations are a touchy topic when it comes to online security.

Apple Granted Patent for Deepfakes Based on Reference Images

October 21, 2022

What Can Be Done About DeepFake Phishing?

Given the threat that DeepFake phishing presents us, this isn't just something that can be fought on an individual level. Video conferencing providers such as Skype, Zoom, and FaceTime will have to incorporate built-in detection systems designed to spot suspected DeepFakes. These systems will most likely have to make use of the same machine learning technology principles that phishers do.

Real-Time Deepfakes

Deepfake technology is shockingly sophisticated, allowing companies to create advertising clones, countries to imitate political rivals, and turn 50-year-old men into attractive young women. Now, livestreamers are using a new deepfake software to change their face in real time.

Deepfake Your Next Zoom Meeting with Help From AI & xpression camera

These days we could all use an extra smile or two, and Al is ready to help out. Make your next video call a bit more fun with the xpression camera app. Currently under beta, this Mac and iPhone app acts as a second video camera for your next Google Meet, Zoom, or Facetime call. Sounds boring, except that it will take any image or video of a person and deepfakes your mouth and facial expression onto it!





The Process of CrDM-VD-3ing AI is Becoming Increasingly Streamlined, Accelerated, and Cost-effective

Rapid advancements in GPU processing enable high-quality, fast Creation of deepfakes in 2023

Decreasing costs of processing power make crDM-VD-3ing AI more accessible

The **availability of large, diverse datasets** enhances the training process and improves Al performance

ML models optimize the AI development cycle, reducing time and resources required

Effective detection mechanisms are crucial to mitigate the damage of AI, including deepfakes



AI Tools Are Essential to Help Us Prioritize Efforts and Combat Adversaries Amidst Escalating Threats

ADVERSARIAL ThreatS:

- Blackmail of Key Leaders and Personnel
- Information Warfare and PsyOps
- Coordinated C2 Disruption
- Election Interference
- Social Engineering and Phishing
- Fraud and Financial Scams

AIRFORCE OPPORTUNITIES:

- Enhanced ThreatDetection
- Training, Education, and Simulations
- Counterintelligence Operations
- Policy and Regulation Development
- Offensive Information Warfare

Blackmail / Extortion

ENEMY'S MOST LIKELY COURSE OF ACTION:

- Targeting Key leaders, individuals with clearances, high profile STEM
- Russia/China identifies DAF/DoD individual with access to sensitive / important information or of high rank / authority
- Enemy intel agency crDM-VD-3es a deepfake video of them in a compromising position (i.e., sex tape, doing drugs, making controversial statement)
- Foreign agent Threatens to expose the individual, blackmail them for classified information

RESULT: OPSEC compromised, classified information leak, personnel lives at risk



Home / Defence

DEEPFAKE ATTACKS AND CYBER EXTORTION, NEW TOOLS IN CYBER CRIME PLAYBOOK

by Reporter

09 August 2022 | 1 minute read SHARE THIS ARTICLE <

MilitaryTimes

Flashpoints

Ever heard of 'deep fake' technology? The phony audio and video tech could be used to blackmail US troops

Kyle Rempfer

🖻 July 19, 2018





Coordinated C2 Disruption

ENEMY'S MOST LIKELY COURSE OF ACTION:

- Conflicting orders or statements that disrupt operational movements
- Russia releases a fake video with conflicting, confusing information through Instagram, Twitter, Facebook, and YouTube
- A coordinated ground, air, or insurgent attack occurs amid the fake video fall-out
- Russian intel continues to release fake videos denying the attacks, sowing additional confusion

RESULT: confusion and chaos delays responses, responses to attacks are delayed; catastrophic dDM-VD-3h and loss of equipment



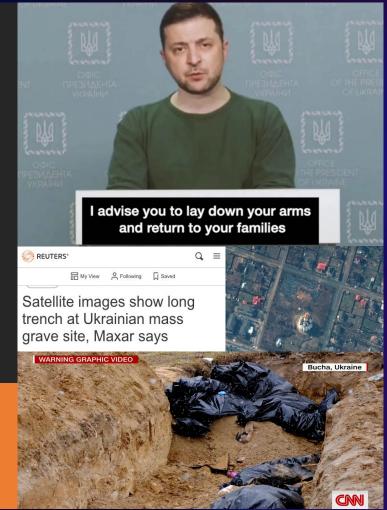


Information Warfare / Psyops

ENEMY'S MOST LIKELY COURSE OF ACTION:

- Fake video of a military or political leader making disparaging statements to US/NATO
- Manipulated audio / video of war crimes perpetrated by US / NATO allies (i.e., Ukraine, Taiwan)
- Goal: discredit US / NATO allies through manipulated content
 to sway public opinion

RESULT: manipulates US/NATO countries' public opinion against current international support efforts (i.e. Ukraine), allows Russia to undermine support from within

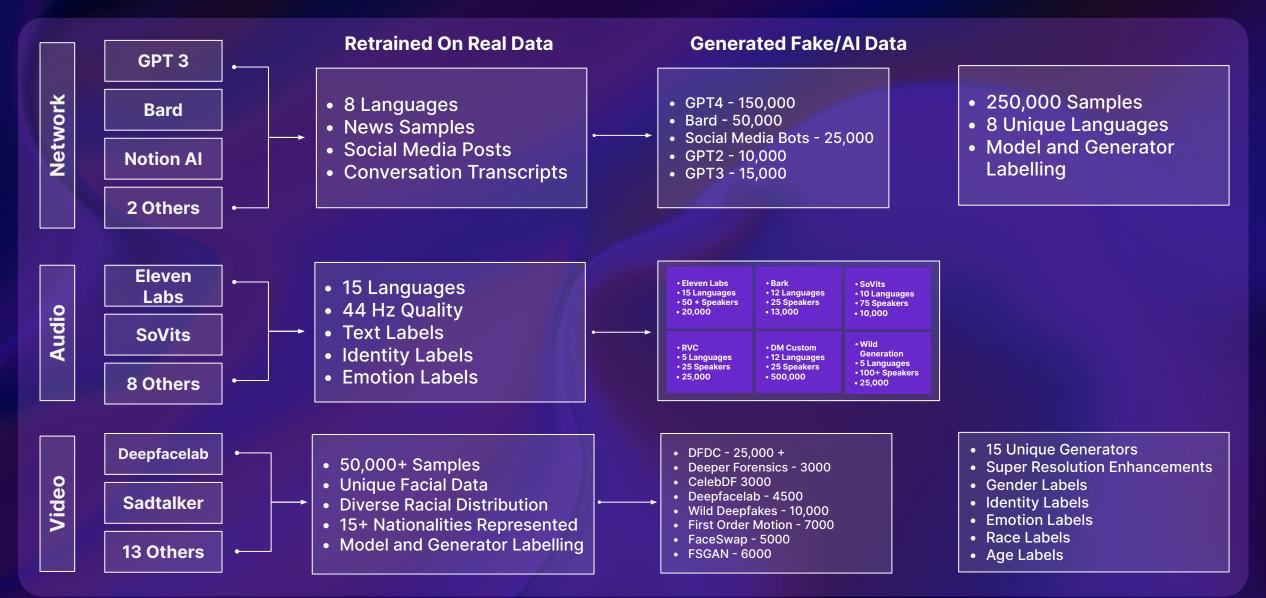




Combating DeepFakes Requires Generating Synthetic Text, Voice, and Face Data To Train Al Detection Algorithms



Generating Training Data



DeepMedia's Custom Generated Dataset Is Significantly Higher Quality vs Competing Datasets Used in Research and Enterprise



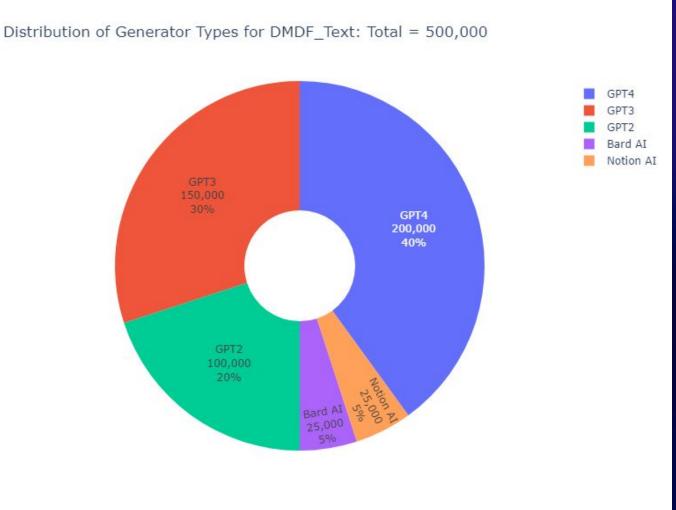
Samples from DeepMedia's custom dataset generated for the US Air Force displaying significantly higher quality than any other DeepFake detection dataset



Samples from the DFDC dataset, the most state-of-the-art dataset used in DeepFake detection research in 2023



Combating DeepFakes Requires Dataset Generation: Text DeepMedia Datasets Contains 500K+ Fake Text Samples from the Most Common Al/Large Language Models Used in Production

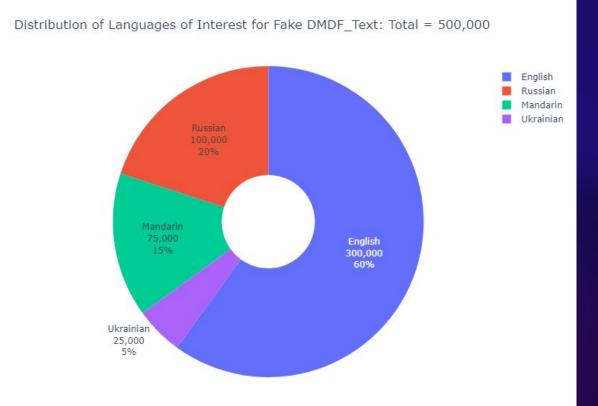




Combating DeepFakes Requires Dataset Generation: Text DeepMedia Datasets Contains 500K+ Fake Text and 200K+ Real Text Samples Across English, Mandarin, Russian, and Ukrainian

Russian 50,000 25% Ukrainian 25,000 12.5% Mandarin 25,000 12.5%

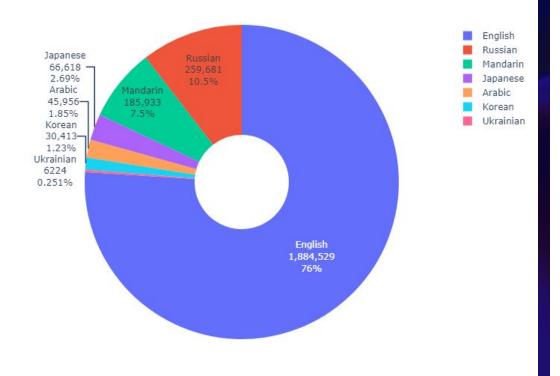
Distribution of Languages of Interest for Real DMDF Text: Total = 200,000



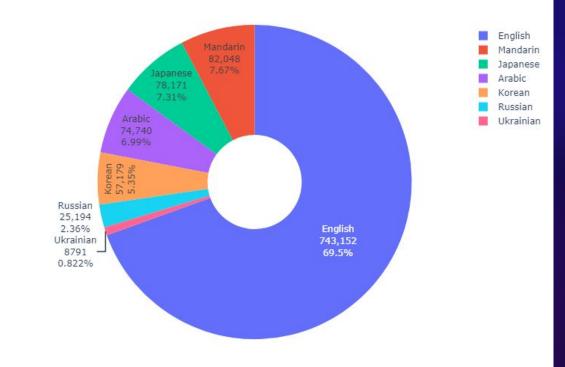


Combating DeepFakes Requires Dataset Generation: Voice DeepMedia Datasets Contains 1M+ High-Quality Fake Voices and 2M+ High-Quality Real Voice from 10+ Languages

Distribution of Languages of Interest for Real DMDF_Voices: Total = 2,479,354

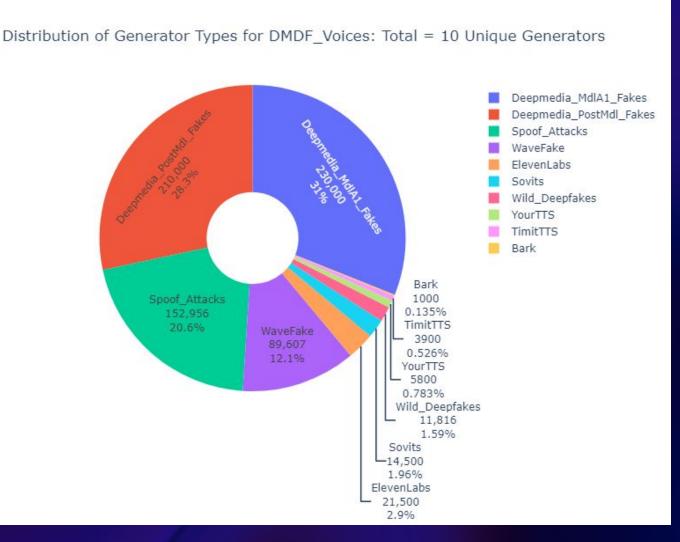


Distribution of Languages of Interest for Fake DMDF_Voices: Total = 1,069,275



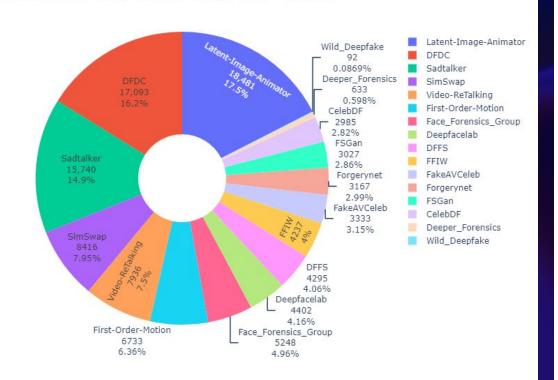


Combating DeepFakes Requires Dataset Generation: Voice DeepMedia Datasets Contains Large Amounts of Fake Voice Data from Every Major Al Voice Algorithm



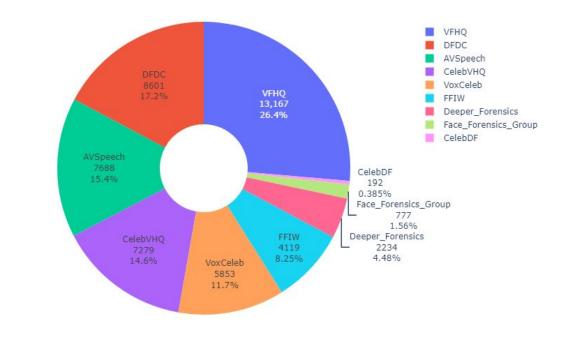


Combating DeepFakes Requires Dataset Generation: Face DeepMedia Datasets Contains 100K+ High-Quality Fake and 50K+ High-Quality Real Faces from a Diverse Range of Data Sources



Distribution of Generator Types for DMDF Faces: Total = 105,818

Distribution of Real Data for DMDF Faces: Total = 50,000



DeepMedia.Al

Training and Evaluating Algorithms to Detect Al Manipulations in Text, Voices, and Faces w/ High Accuracy



State of the Art Classification Algorithms

DM-TextDetector-1



Uses a pretrained LLM to calculate burstiness and perplexity of potentially generated text to determine an overall detection probability.



DM-VoiceDetector-1

A novel Wav to Vector based Deepfake Detector trained by predicting speech units for masked speech. Proprietary to DeepMedia.



DM-FaceDetector-1

A memory efficient Video Detection architecture designed for visual recognition. Proprietary to DeepMedia.

DM-TextDetector-2

A custom-trained LLM specifically tuned to classify text and authentic or Al-generated with an associated confidence score.



DM-VoiceDetector-2

A unique Convolution Neural Network(CNN) based approach trained using Knowledge Distillation from Transformers



DM-FaceDetector-2

Powerful Deepfake Detection Models that combine an Efficient Network and a Vision Transformer.





DM-TextDetector-3

A classic text-based classification algorithm that is trained to detect Al-generated text through standard NLP-based classification.



DM-VoiceDetector-3

An Audio Detection model based upon a CNN, which is characterized by good generalization and stability results.

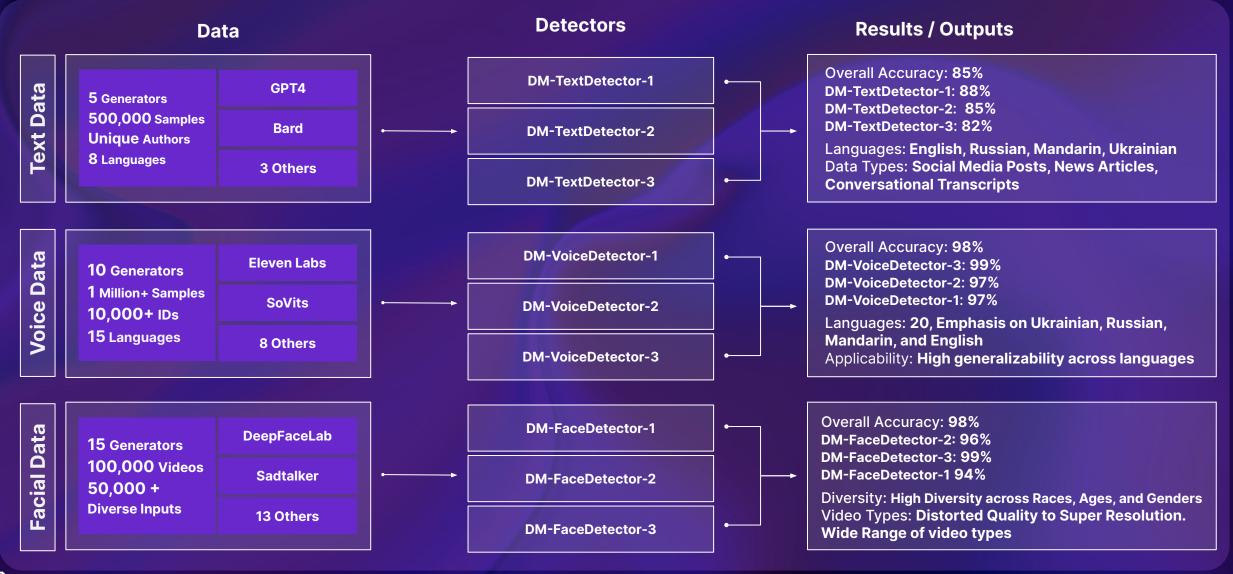
DM-FaceDetector-3



A Video Detection model that enhances the power of Video Transformers with a Video Uniformer backbone.Proprietary to DeepMedia.

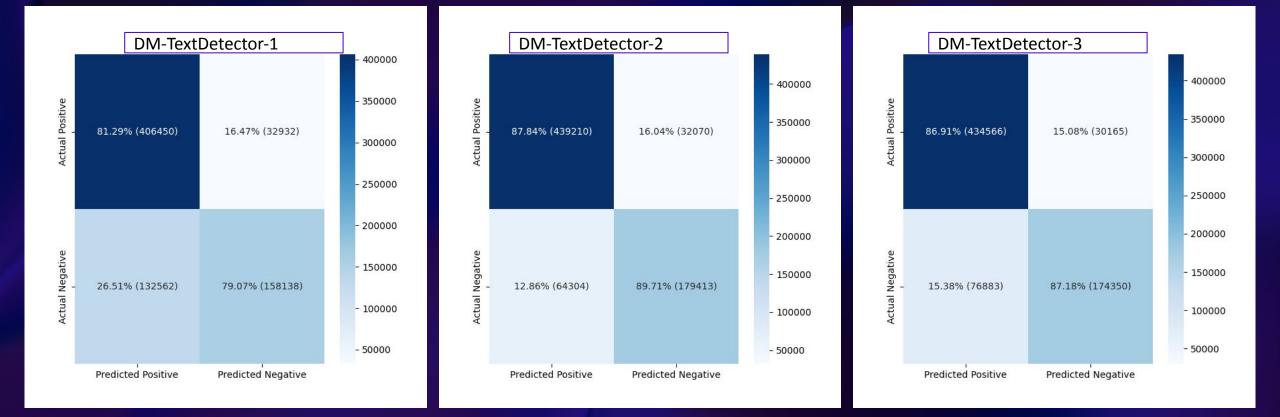
DeepMedia.AI

Training Details And Results

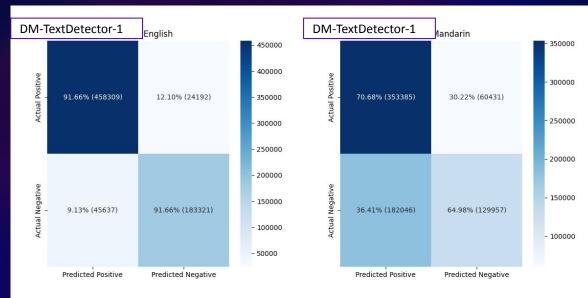


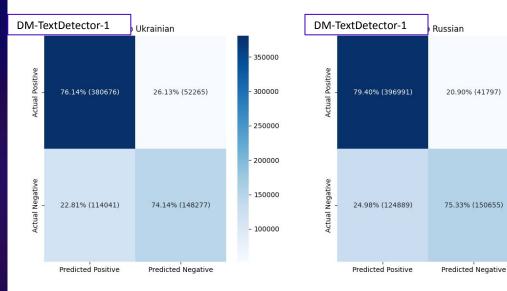
M DeepMedia.AI

Text Detection Results



Text Detection Results





DeepMedia.Al Poneering Synthetic Generation and Detection

61

- 350000

300000

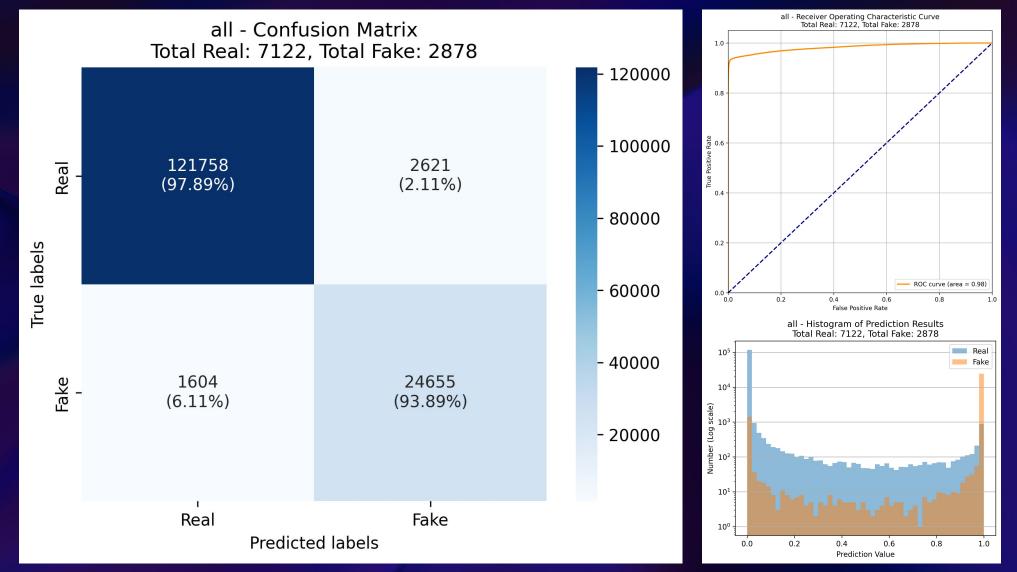
- 250000

- 200000

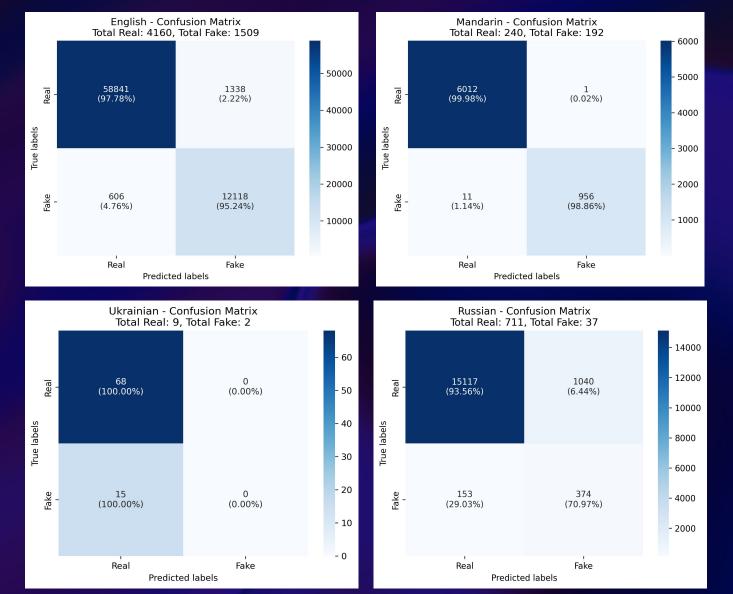
150000

- 100000

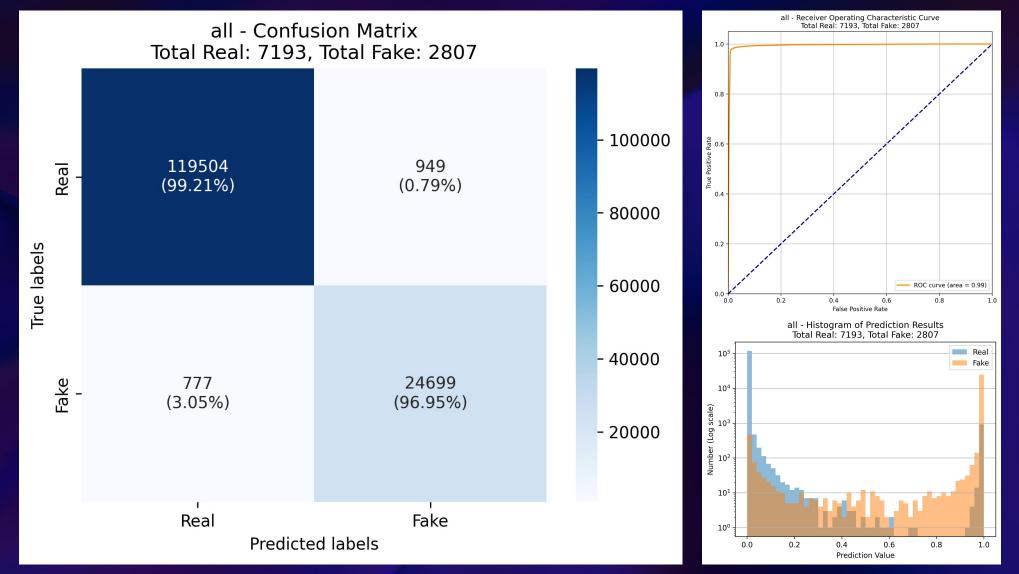
- 50000

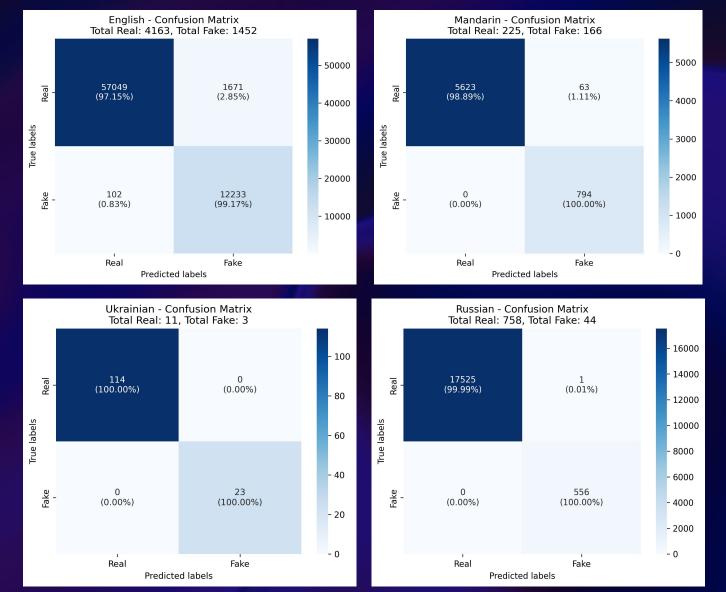




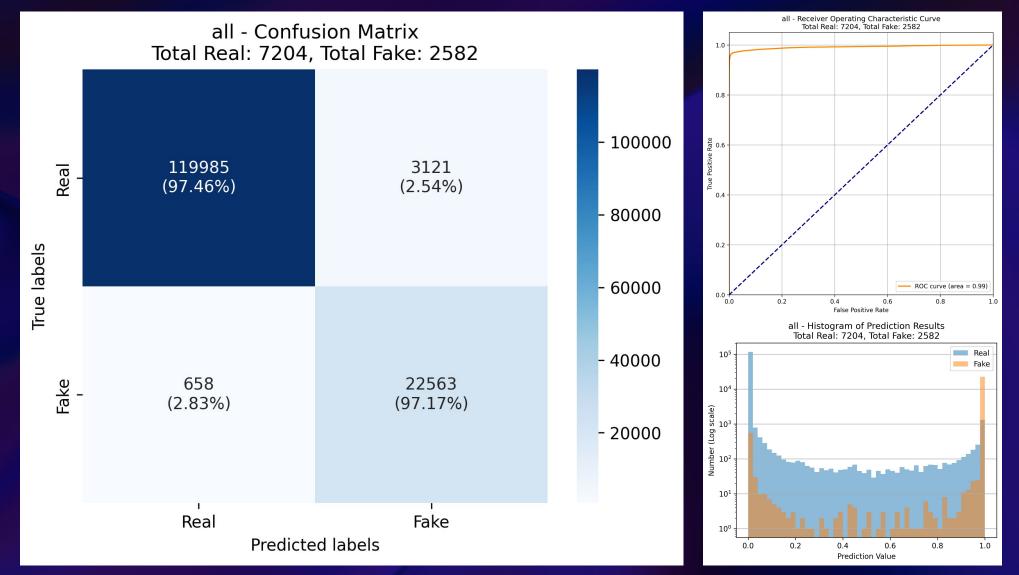




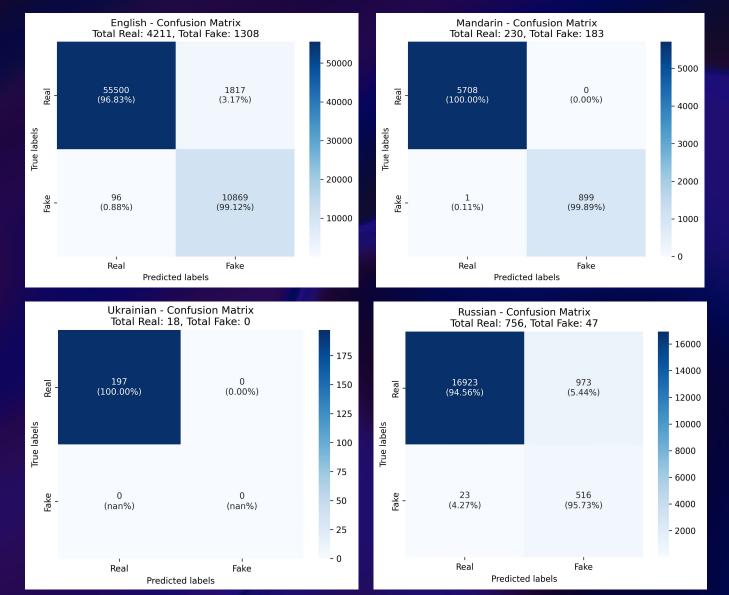








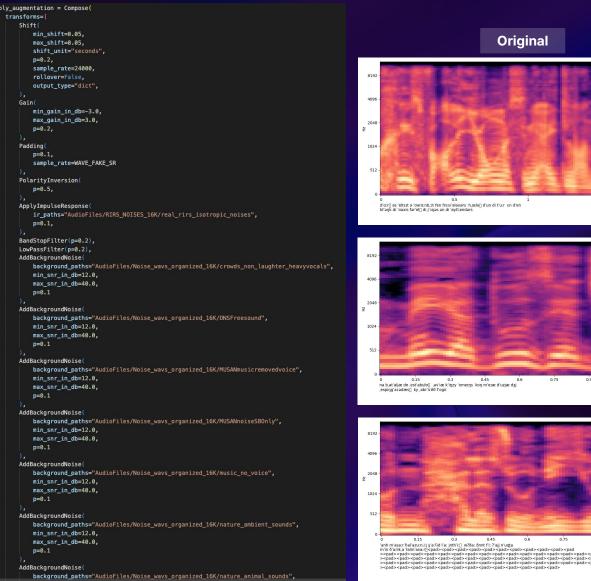
DeepMedia.Al





Adding Audio Augmentations

apply_augmentation = Compose(



Original

+3 dB

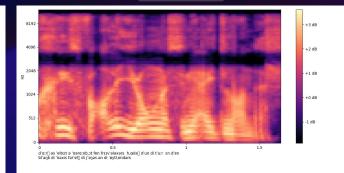
+2.48

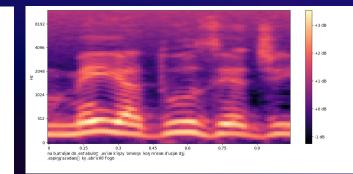
0.5

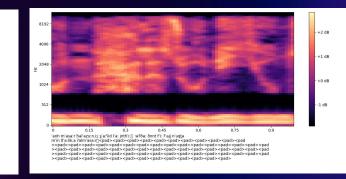
0.3

0.45





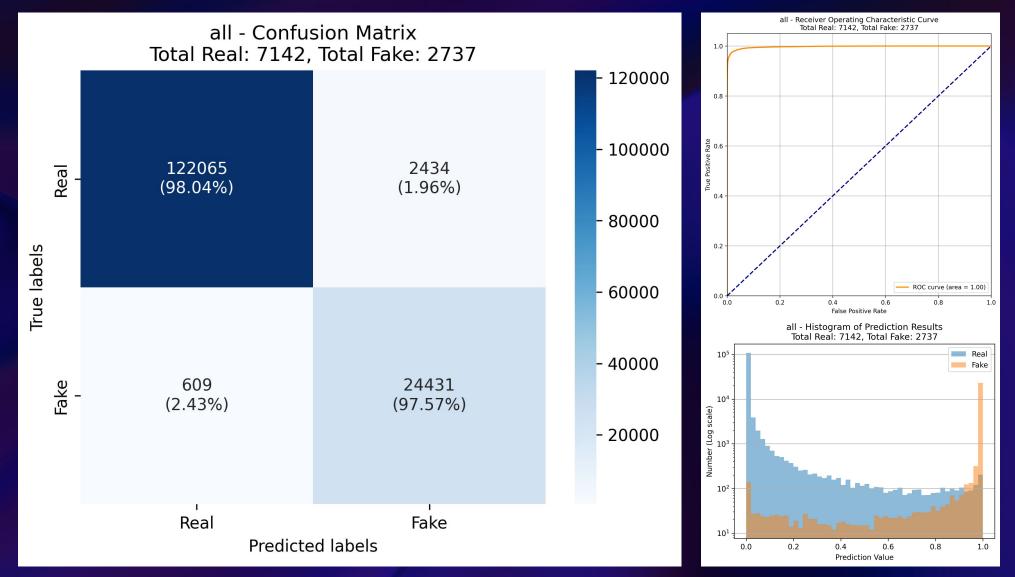




M DeepMedia.AI

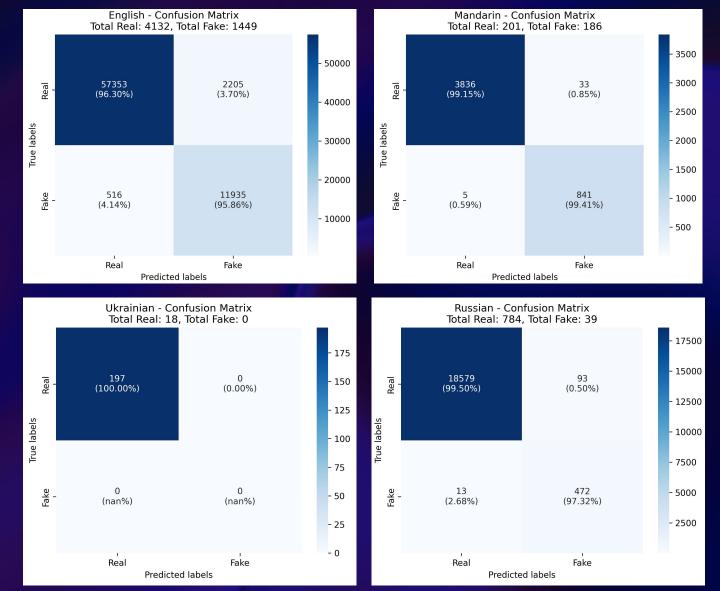
spad><pad><pad><pad><pad><pad</pre>

Voice Detection Results - DM-VD-2 Augmented



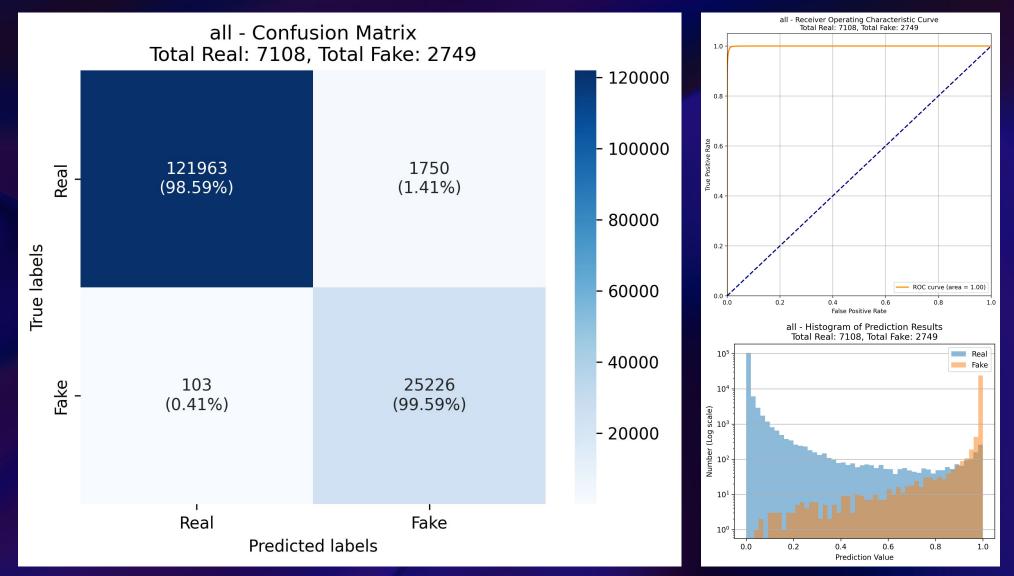


Voice Detection Results - DM-VD-2 Augmented



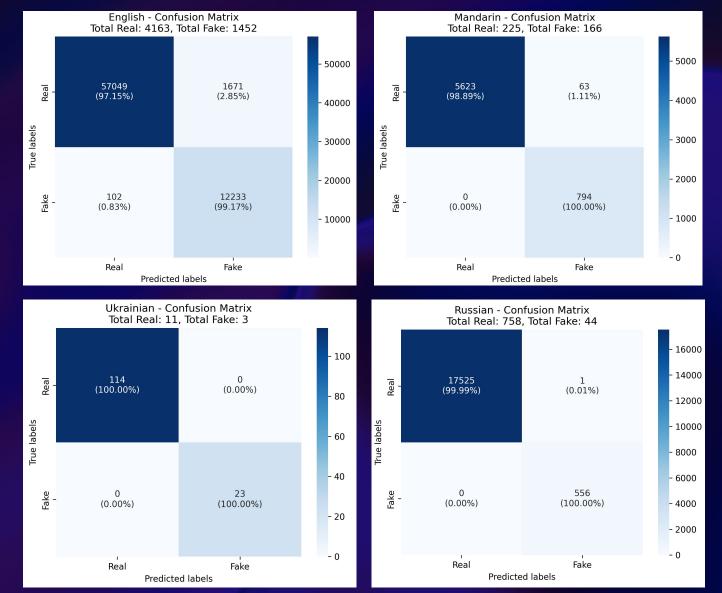


Voice Detection Results - DM-VD-3 Augmented



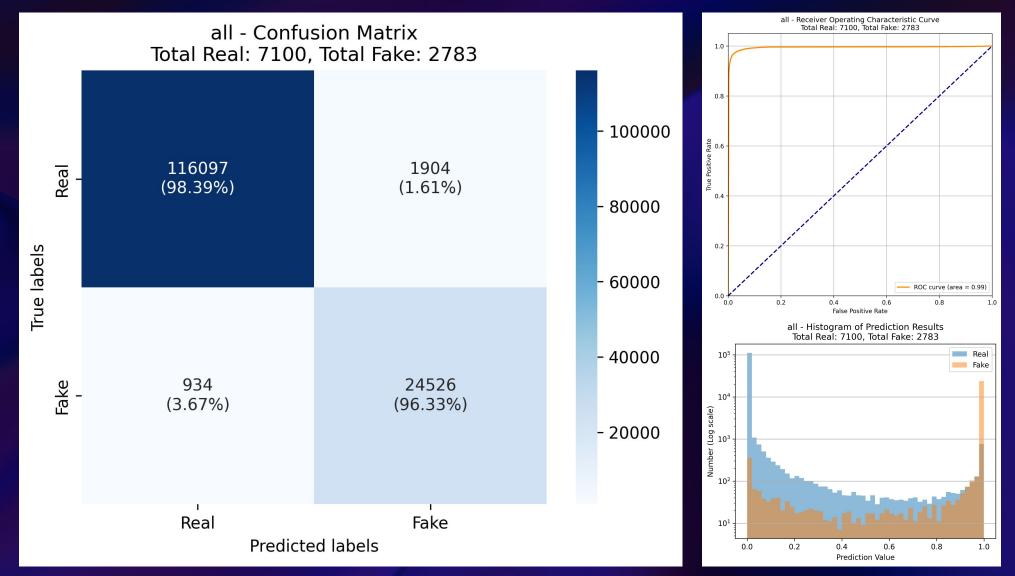
DeepMedia.AI

Voice Detection Results - DM-VD-3 Augmented



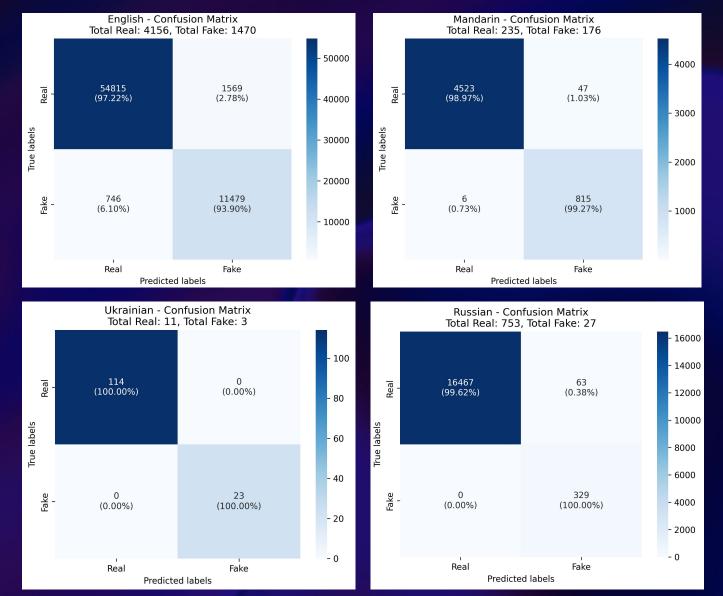


Voice Detection Results - DM-VD-1 Augmented



DeepMedia.AI

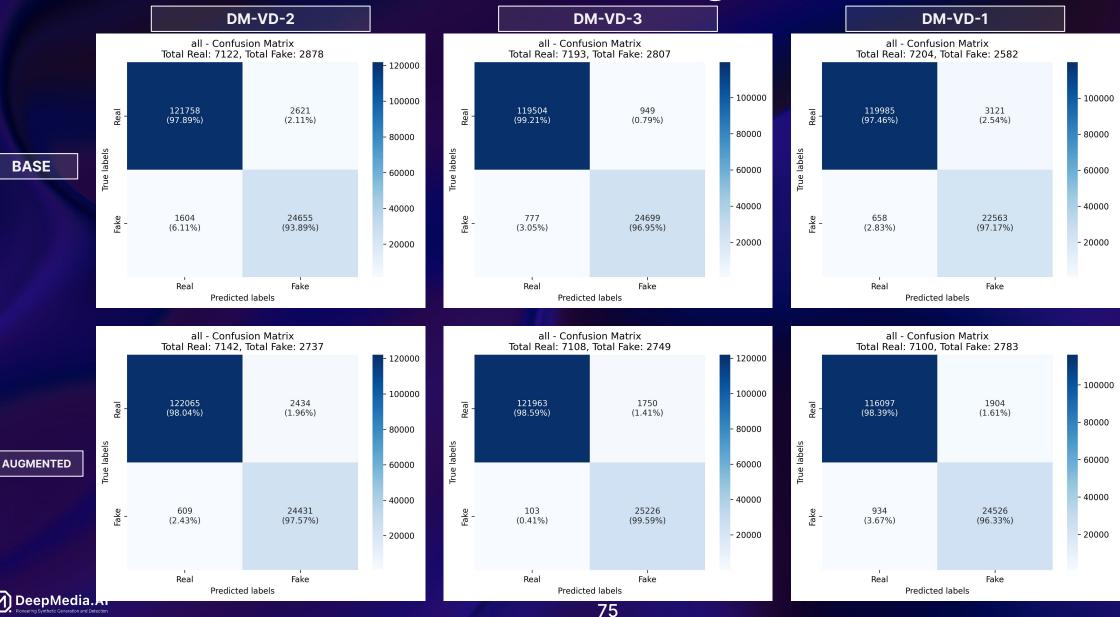
Voice Detection Results - DM-VD-1 Augmented



DeepMedia.Al

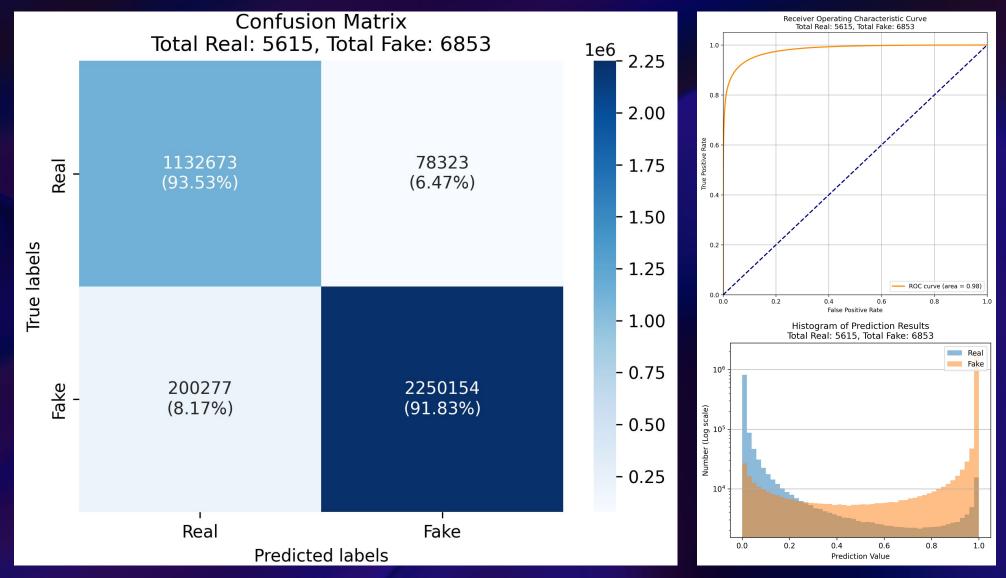
74

Voice Detection Results - Augmentation Effects



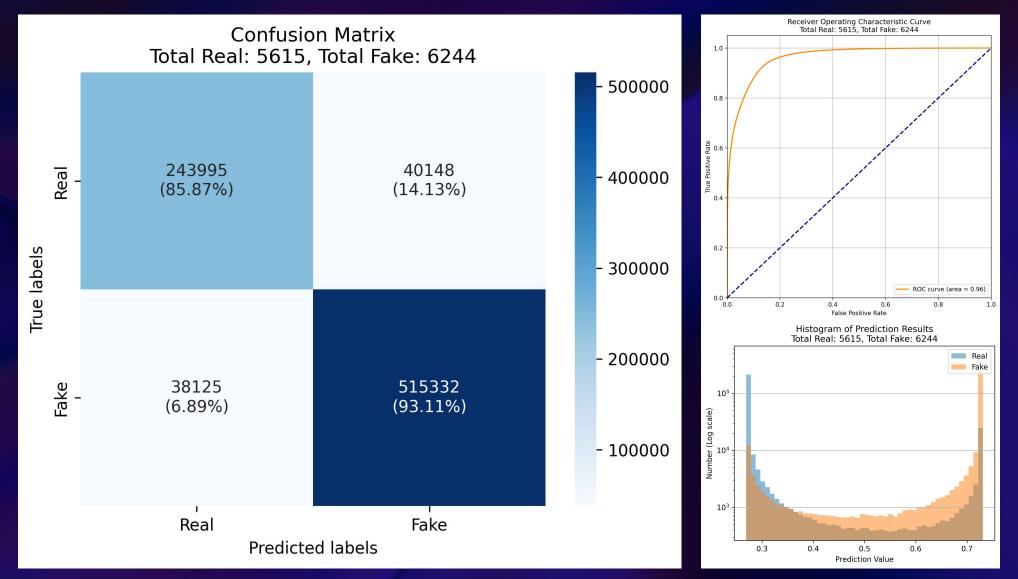
M

Face Detection Results - DM-FD-1





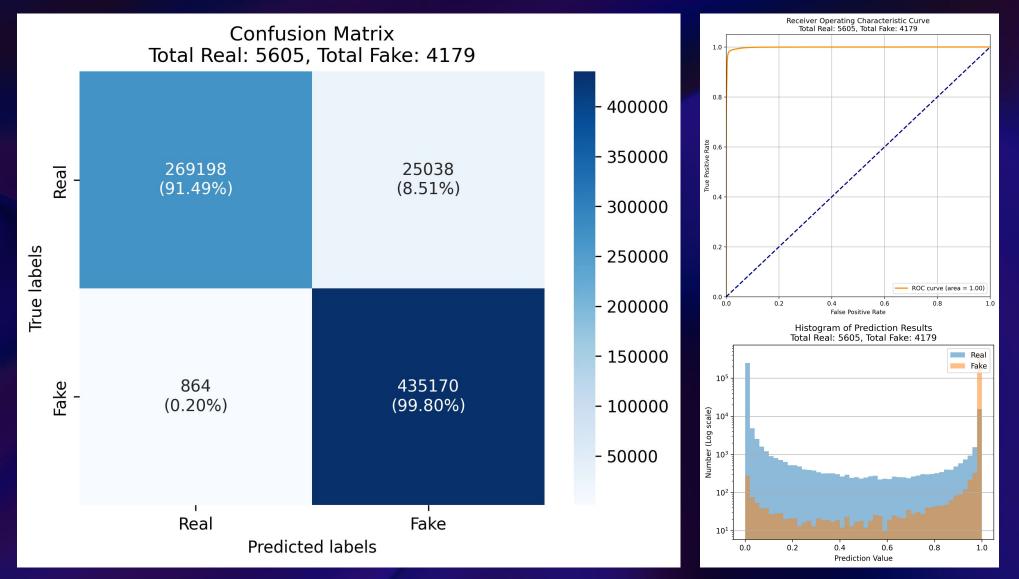
Face Detection Results - DM-FD-2



DeepMedia.AI

77

Face Detection Results - DM-FD-3



Adding Image/Video Augmentations

augmentation_compose = A.Compose([

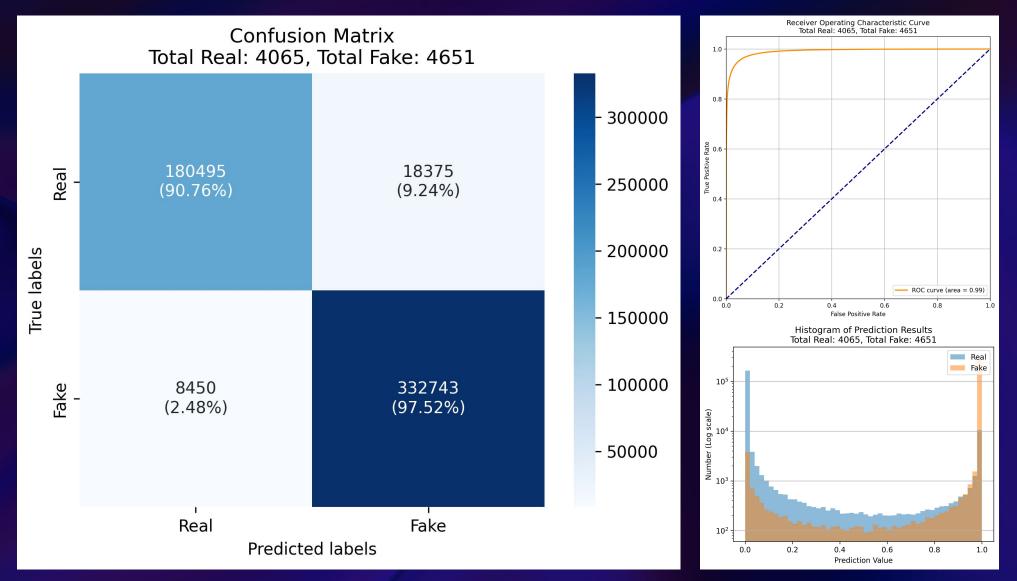
- A.ImageCompression(always_apply=False, p=0.10, quality_lower=60, quality_upper=100, compression_ty A.HorizontalFlip(p=0.5),
- A.Affine(p=0.10, scale=(0.95, 1.05), translate_percent=(-0.03, 0.03), rotate=(-3, 3), shear=(-3, 4) A.ShiftScaleRotate(shift_limit=0.10, scale_limit=0.2, rotate_limit=5, border_mode=cv2.BORDER_REPL: A.CLAHE(always_apply=False, p=0.10, clip_limit=(1, 4), tile_grid_size=(8, 8)),
- A.HueSaturationValue(always_apply=False, p=0.20, hue_shift_limit=(-20, 20), sat_shift_limit=(-30, A.RandomBrightnessContrast(always_apply=False, p=0.20, brightness_limit=(-0.2, 0.2), contrast_lim: A.ToGray(p=0.05),
- A.GaussNoise(always_apply=False, p=0.10, var_limit=(10.0, 50.0)),
- A.MotionBlur(always_apply=False, p=0.10, blur_limit=(3, 7)),
- A.ImageCompression(always_apply=False, p=0.20, quality_lower=60, quality_upper=100, compression_t)

additional_targets=additional_targets_dict





Face Detection Results - DM-FD-3 w/ Augmentations





Face Detection Results - Effect of Resolution



DM-FD-1

DM-FD-2

DM-FD-3

DM-FD-3 Aug

DeepMedia.Al Pioneering Synthetic Generation and Detection

Conclusions

Textual Deepfake Detection Challenges: Pioneering advancements in techniques and detection algorithms are paramount to surmount the substantial challenges posed by high-accuracy deepfake text detection. This uncharted territory beckons for revolutionary tools and methodologies to bolster detection precision.

A Triumph in Voice Authentication: Current voice detection methodologies exhibit stellar performance even amidst intricate augmentations. There's no pressing need for reinvention; instead, fortifying our existing models with richer and more diverse data will propel their efficacy to unparalleled heights.

Facial Deepfake Recognition: Not only does our facial detection stand robust in its primary implementation, but it also showcases admirable resilience against various augmentations. An intriguing discovery across models underscores the potential power of an ensemble strategy as the key to fortifying deepfake countermeasures.

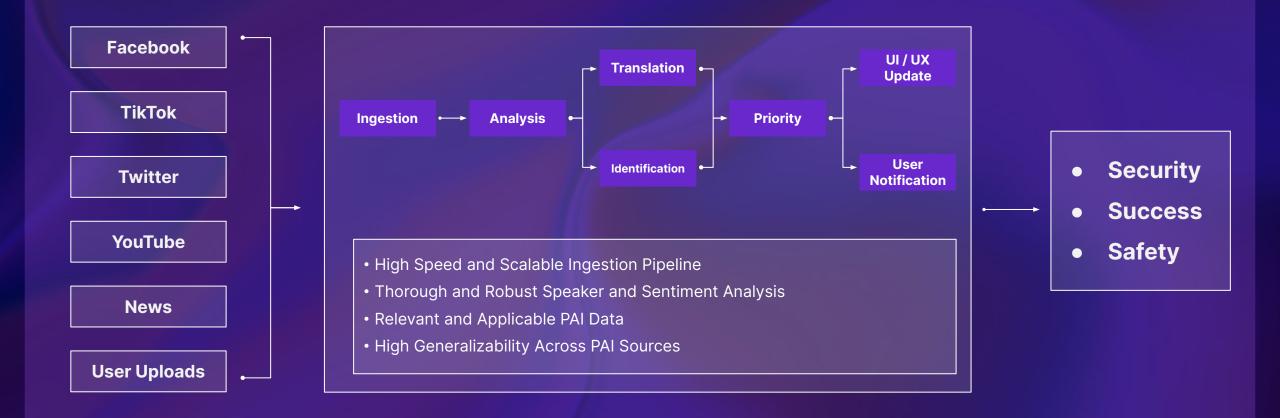
Catalyzing Enhanced Detection: To achieve apex detection accuracies spanning all modalities, it's imperative to craft and assimilate datasets enriched with data derived from avant-garde generator types. These datasets, when seamlessly integrated into our training conduits, promise to redefine the gold standard of deepfake detection.

Pioneering Future Research Frontiers: Venturing deeper into the realms of detector architectures, avant-garde training modalities, and sophisticated feature extraction layers holds the promise to elevate detection accuracy, especially in nuanced scenarios like those presented by ultra-low resolutions.



Big Picture Empowering DoD and IC Media Intelligence and Al Forensics at Scale

We Harness PAI sources for Robust Data Intake and Analysis at Scale, Processing Millions of Videos Per Day at a Cost of \$0.005 / Min



Synthetic Media Detection Process: Face and Voice Acquisition

DeepMedia's video ingestion process prepares ingested content for further analysis and processing. DeepMedia's proprietary pre-processing technique aims to optimize the input media for various AI models used in the product. For video content, it is split into individual frames, and the audio is extracted from the video stream. If the input is audio, it is directly processed. Our sophisticated pre-processing detects and extracts faces and voices from the ingested content, preparing them for processing through our state of the art Deepfake Detectors.

Step 1

DeepMedia's Ingestion pipeline stores the ingested content.

Step 2

Video Content is split into frames, and audio extracted from the video

Step 3

Faces and voices are detected and stored from the inputted content.

Step 4

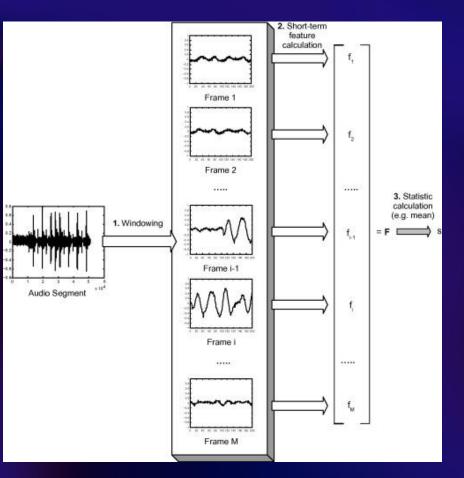
These faces and voices are prepared for processing through our deepfake detectors.

AI Media Detection Process: Face and Voice Acquisition

For Instance, consider the Hillary Clinton Deepfake Outlined Previously:

The DeepID System first hones in on any faces of interest, and splits the video into frames. And audio is collected through a process known as feature extraction, illustrated below.





AI Media Detection Process: Transcription and Translation

To generate transcripts for the ingested content and identify each individual, we utilize a multi-modal deep learning approach. The audio from the input media is transcribed using a state-of-the-art Automatic Speech Recognition (ASR) model, capturing the spoken words. Simultaneously, the face detection and recognition models identify and track individuals in the video frames. The detected faces are associated with the transcribed speech to assign spoken words to specific individuals accurately.

Furthermore, the optional translation to English is performed by employing a Transformer-based Machine Translation model, converting the transcribed text from the original language to English. This multi-modal process ensures comprehensive and contextually accurate transcripts that attribute spoken words to the correct individuals while providing the flexibility to translate the content to English if desired.

Step 1

Audio is transcribed using a state-of-the-art Automatic Speech Recognition Model.

Step 2

Face Detection models identify and track individuals in the video.

Step 3

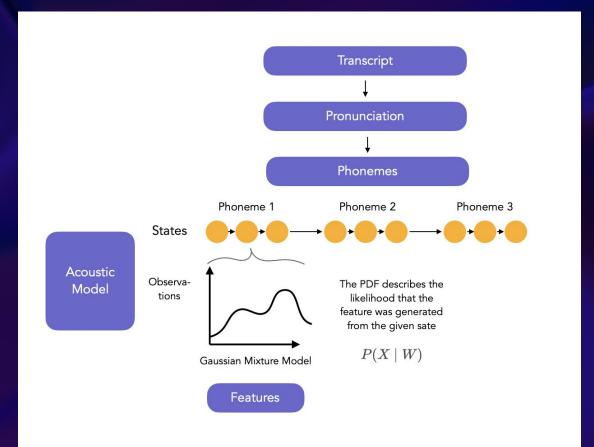
Detected Faces are automatically associated with the transcribed speech.

Step 4

When desired, translation to English is performed by a powerful Transformer based Machine Translation Model, converting the transcribed text to English.

AI Media Detection Process: Transcription and Translation

The video is then passed through Deep Media's state-of-the-art Automatic Speech Recognition Model, which accurately detects and transcribes the provided audio, using a powerful phoneme analysis. When desired, this transcription is passed through a transformer model and ito any language of interest.



"You know, people might be surprised to hear me saying this, but I actually like Ron DeSantis a lot. Yeah, I know. I'd say he's just the kind of guy this country needs, and I really mean that. If Ron DeSantis got installed as president, I'd be fine with that."

> - Hillary Clinton in Al-Generated Video

Al Media Detection Process: Face and Voice Analysis

Our voice and face deepfake detectors employ advanced deep learning techniques to scrutinize the extracted faces and voices and discern any signs of synthetic manipulation. For face deepfake detection, the model scrutinizes facial landmarks, micro-expressions, and overall facial consistency to identify potential anomalies. Additionally, the model analyzes artifacts, inconsistencies, and unnatural movements to distinguish real faces from manipulated ones. For voice deepfake detection, the model examines spectrograms, pitch patterns, and phonetic characteristics, scrutinizing any inconsistencies or patterns characteristic of synthetic speech generated by voice synthesis models. Moreover, both detectors utilize large-scale datasets of genuine and manipulated faces and voices for robust training, enabling them to adapt and recognize emerging deepfake techniques effectively.

Step 1

Using a robust and extensive Deepfake and real dataset, our detector analyzes each face and voice for signs of manipulation

Step 2

Faces are analyzed for micro-expressions and facial consistency

Step 3

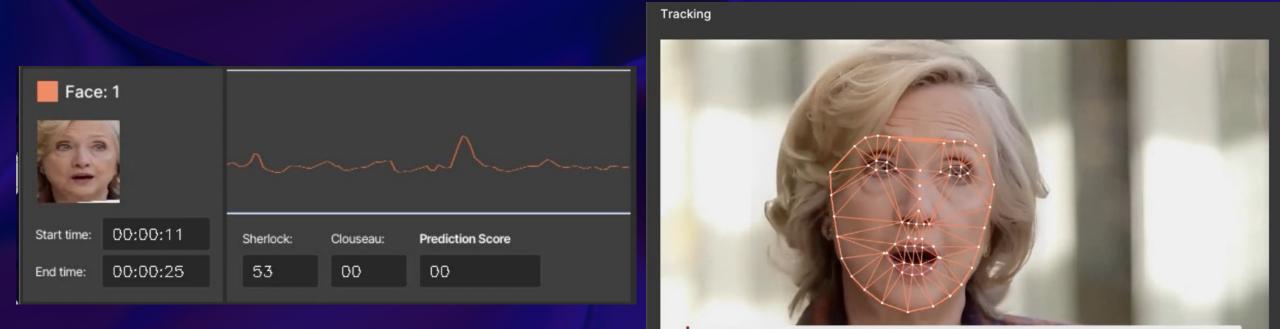
DeepID identifies artifacts, inconsistencies and unnatural movements to distinguish real and manipulated faces

Step 4

Voices are examined for pitch patterns and phonetic characteristics.

AI Media Detection Process: Face and Voice Analysis

The extracted frames are analyzed by our world class detectors, and a real time video analysis is performed. Below you can observe our Sherlock detector analyzing this input, as well as our Facial Tracking system, which ensures our detectors have the highest accuracies possible.



MSNBC

C3PMEM

HILLARY CLINTON ENDORSES DESANTIS

AI Media Creation Process: Multi-Modal Ensemble Detection

After analyzing the extracted faces and voices using our voice and face deepfake detectors, we merge the results to form a comprehensive assessment of the content's authenticity. By comparing the identified faces with our people identification database, we determine the presence of known individuals and potential impersonations. Our proprietary fusion algorithm combines the outputs from multiple detectors, considering their respective confidences, to arrive at a reliable final verdict on whether the content is likely manipulated or genuine. The synthesized findings are presented in a user-friendly report, outlining the level of confidence in the detection results

Step 1

We merge the results from our face and voice analysis to come to a conclusion about the authenticity of the content.

Step 2

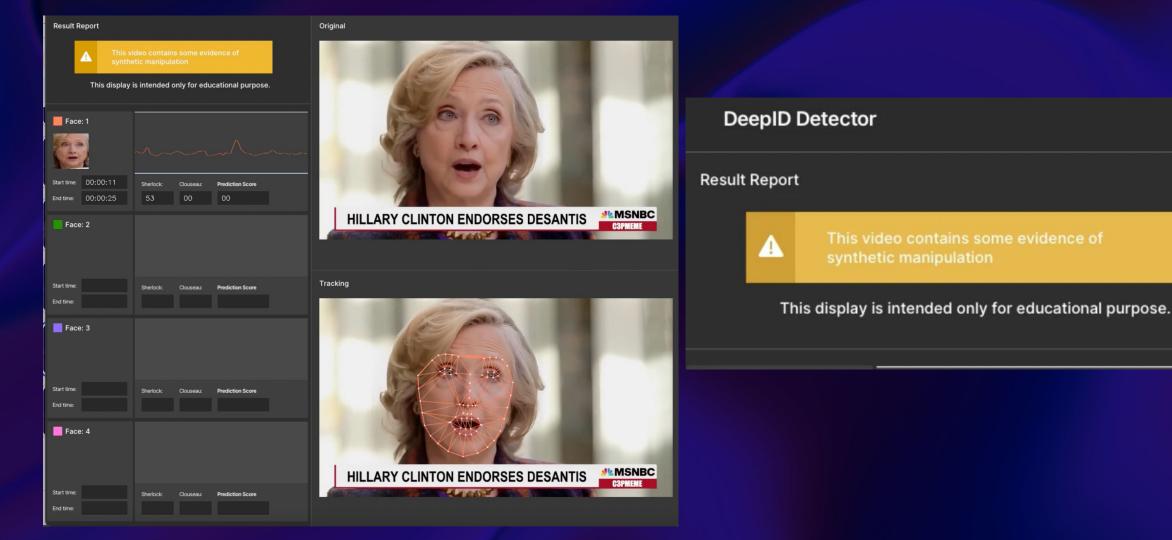
We combine the output of multiple detectors to ensure an accurate conclusion about the authenticity of the content.

Step 3

We arrive at a final conclusion, and prepare a user friendly report outlining our confidence in the detection results.

AI Media Creation Process: Multi-Modal Ensemble Detection

Implementing an extensively tested set of Heuristics to determine the authenticity of the inputted content, a conclusion is drawn by our detectors. Our system provides analysis of the authenticity of both Audio and Video



Al Media Detection Process: Translation, Sentiment Analysis, Identity Detection, and Prioritization

Prioritizing and delivering information to the user is a crucial aspect of our product's user experience. We follow a streamlined approach to ensure efficient and clear communication of the analysis results. First, the deepfake detection and people identification results are prioritized based on their confidence levels, highlighting the most relevant and critical findings. The user is presented with a summary of the key insights, such as whether deepfake manipulation is detected and if any identified individuals warrant special attention.

Step 1

Deepfake detection results are prioritized based upon their confidence level

Step 2

The user is presented with a summary of the key insights uncovered by the detection process

Step 3

A detailed report is provided, offering a comprehensive breakdown of the analysis, including timestamps of potential manipulation occurrences, transcribed text, and identified individuals.

The Lookup Database Utilizes the ARWEAVE Blockchain for Enhanced Security and Reliability

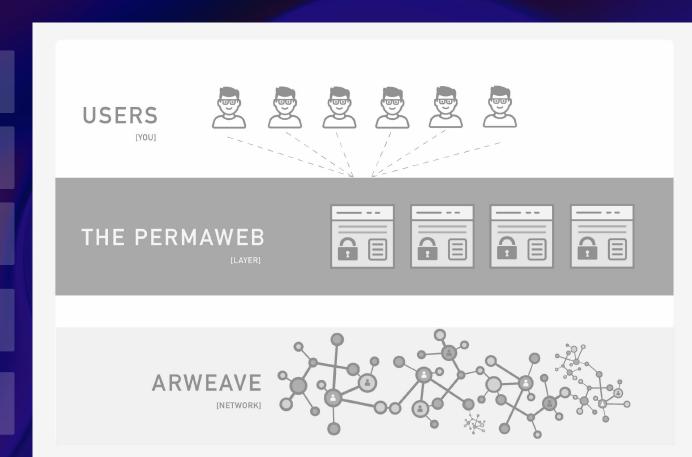
Secure blockchain integration enhances security and reliability for the lookup database

Immutable data records ensures tamper-proof and auditable data in the lookup database

Decentralized architecture increases resilience and availability

Trusted data integrity preventing unauthorized modifications in the lookup database

Reliable and auditable source of information for the lookup database



Data Organization, Fast Search, and Workflow Tooling Makes Checking Content Easier and Faster

	Explore Upload a file Add a new person My organization filters: Most recent () Most viewed Most commented	Thomas Tyler thomastyle@ernait.com		
<	Joe Biden Marked as seen Marked as dangerous Following	Le Activity		
My channels		You marked a video of @Tom Cruise as "Seen"	Г	
	**************************************	New video of @Elon Musk has been uploaded		• Ordered By ThreatLevel
Joe Biden 32 Mark Zuckerberg				• Fast and Accurate Search
@James McConville Follow		This video of @Tom Cruise is trending	·	• Easy-to-use Data Feed
Wiadimir Putin Follow	Manipulation Probability: 99% Video uploaded by: r Berank Ford Uploaded at 23:00PST	💷 🛛 @Jun said something in your channel		Organizes All Modalities
@Mark Zuckerberg Following		A video of @Elon Musk has been reported		
@Elon Musk Following				
(Tom Cruise Following	© Francisca Gibson ▷ ம ┖ ┖ © 0870233 This Deepfake is now on Facebook!			
Lagest O	Watch out people! This deepfake is in almost all social media we need to take it down for the security of @ Tom !			
Logout	Reply to this comment 🗷 🖉 ≽			

High-End Analytical features Will Give DoD/IC Supreme Confidence In AI-Security Decisions



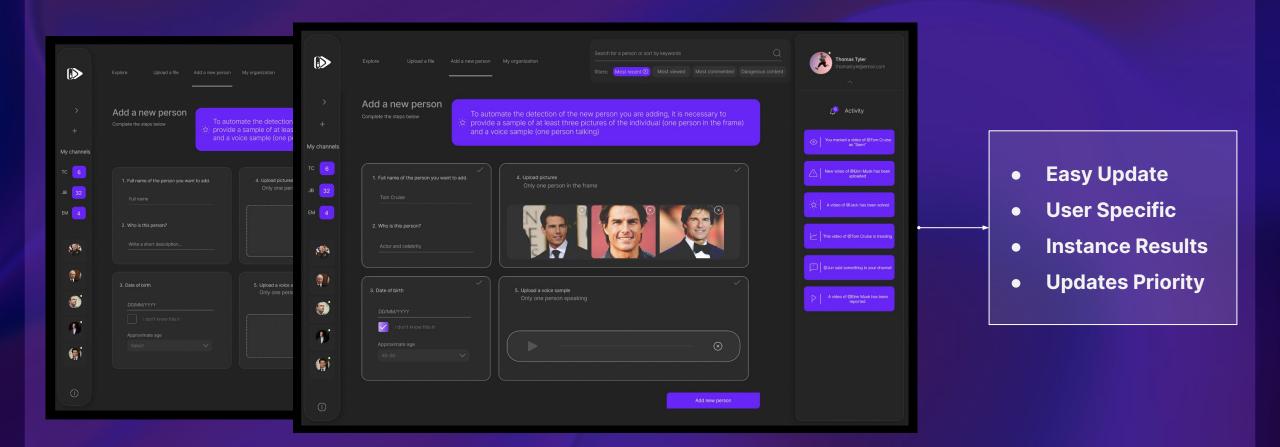
Voice Detection, Model Attribution Transcription and Translation



High-Accuracy Facial Manipulation Analysis with Time-Code Organization



Face and Voice Identity Mapping for High-Priority Individuals and Alerts



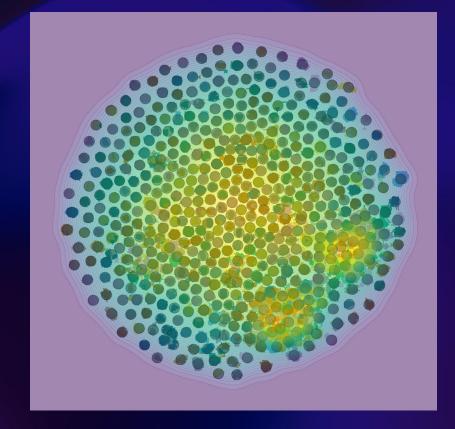
What makes DeepID Different?

Superior Detection: DeepMedia's DeepID outperforms competitors with its robust dataset from 20+ countries and 15+ languages, ensuring unmatched detection in all scenarios, particularly high-risk security situations.

Efficiency Meets Scalability: DeepID isn't just scalable—it's also cost-effective, providing a marked contrast to competitors' resource-intensive solutions.

Evolutionary Dataset Excellence: Our dataset is a living entity, ever-evolving and incorporating examples from even the most cutting-edge synthetic manipulation models.

Advanced Interface & Insights: DeepID's intuitive UI and sophisticated visual analytics provide experts with profound insights, enhancing both user experience and security outcomes.

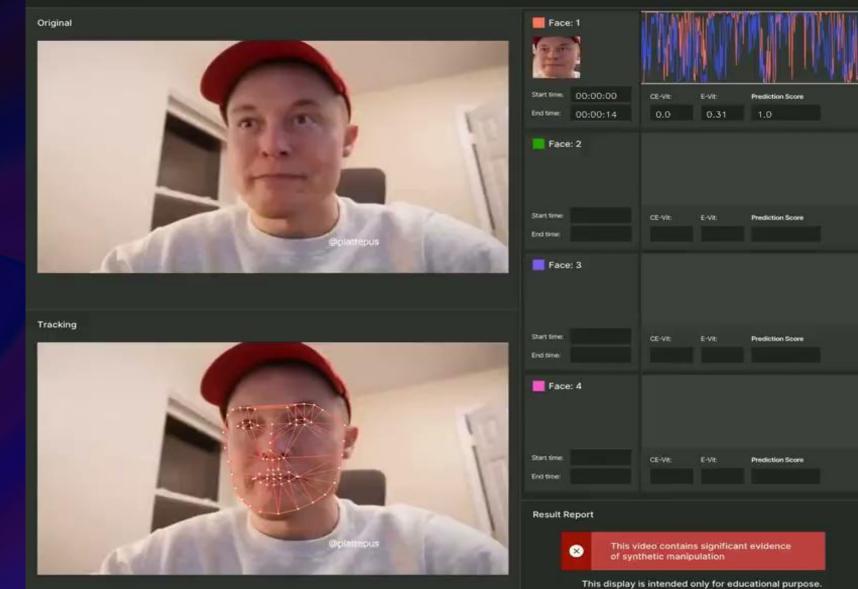


https://vimeo.com/798036678





https://vimeo.com/798036707



102

https://vimeo.com/798036663





103



Concluding Thoughts

01

Best-in-class: DeepMedia's DeepFake detection provides the best solution to combat AI-Threats

02

03

04

Urgent Tech Deployment: Immediate need for our technology to address emerging Threats

Hardware Integration: Integrating with hardware systems to optimize performance

Continuous Enhancements: Advancing technology with refinements to improve functionality

REDIA Thank you

www.deepmedia.ai

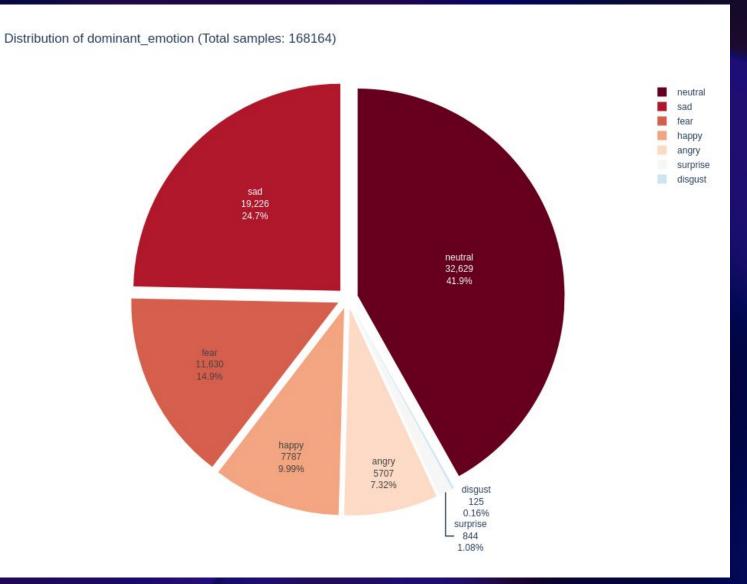
Rijul Gupta T. 405.765.3169 rijul@deepmedia.ai

Emma Brown T. 503.820.8305 emma@deepmedia.ai

APPENDIX

APPENDIX

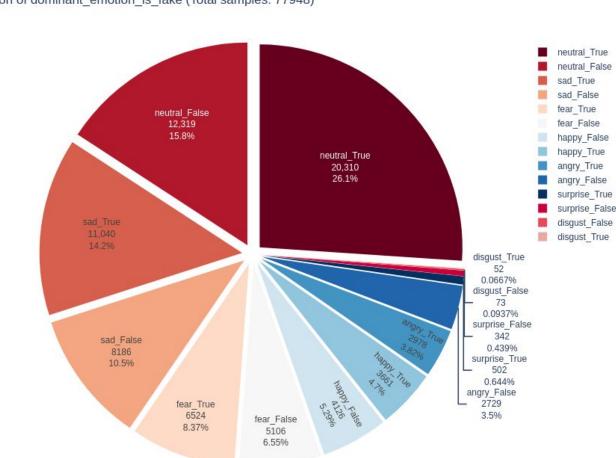
Combating DeepFakes Requires Dataset Generation: Face Emotion Distribution





APPENDIX

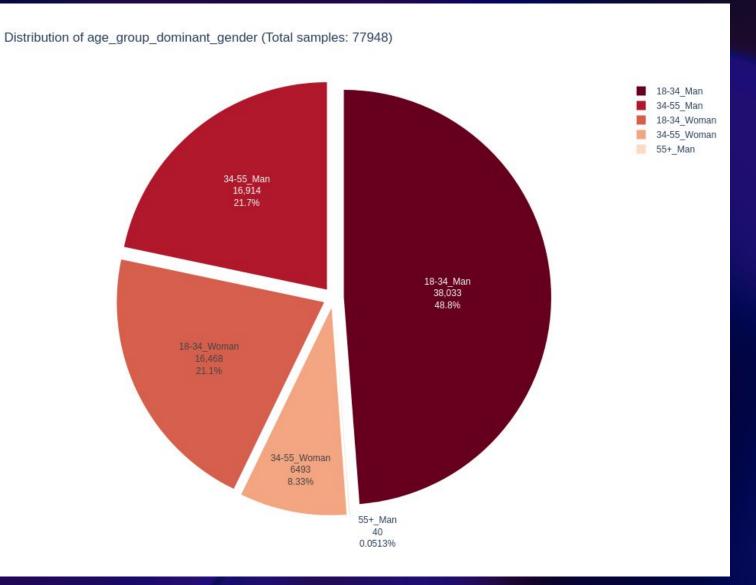
Combating DeepFakes Requires Dataset Generation: Face Emotion X Real/Fake Distribution



Distribution of dominant emotion is fake (Total samples: 77948)



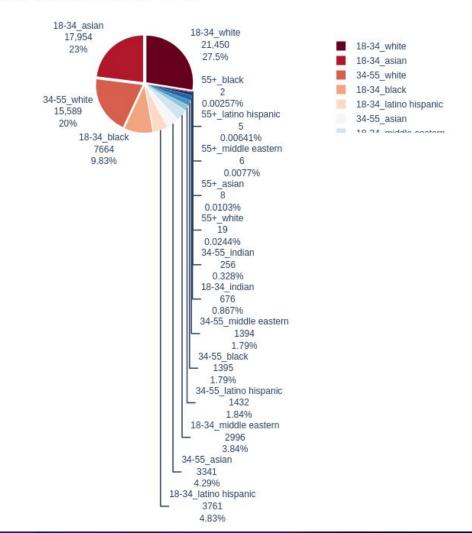
Combating DeepFakes Requires Dataset Generation: Face Age X Gender Distribution





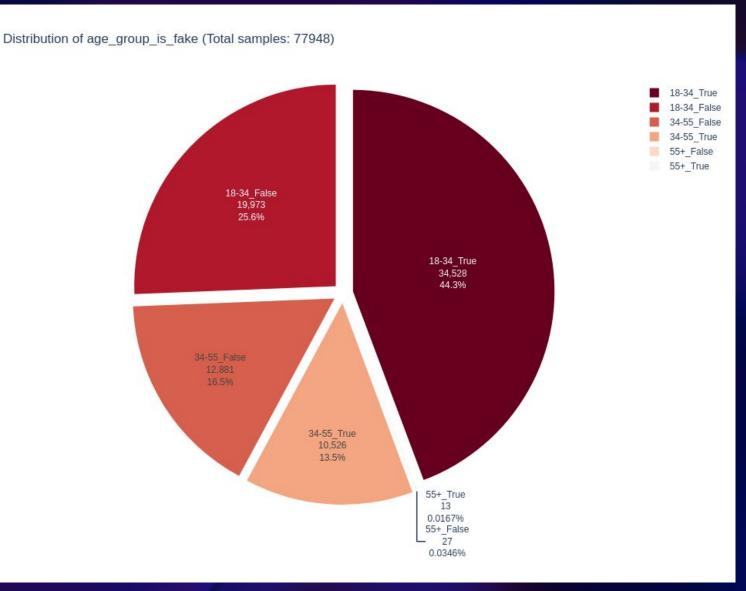
Combating DeepFakes Requires Dataset Generation: Face Age X Race Distribution

Distribution of age_group_dominant_race (Total samples: 77948)





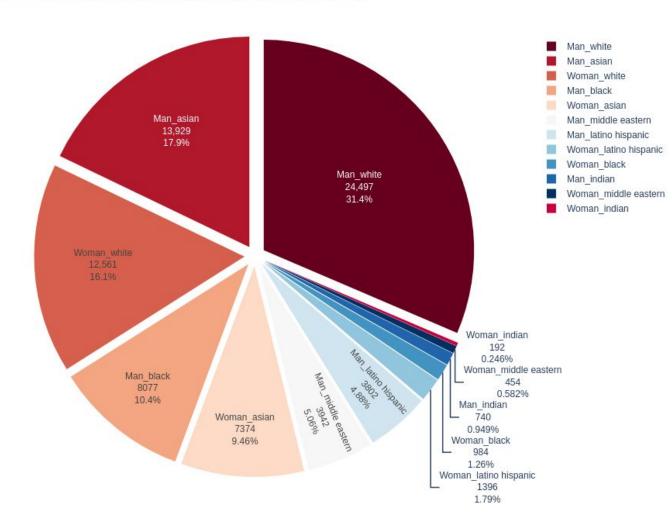
Combating DeepFakes Requires Dataset Generation: Face Age X Real/Fake Distribution





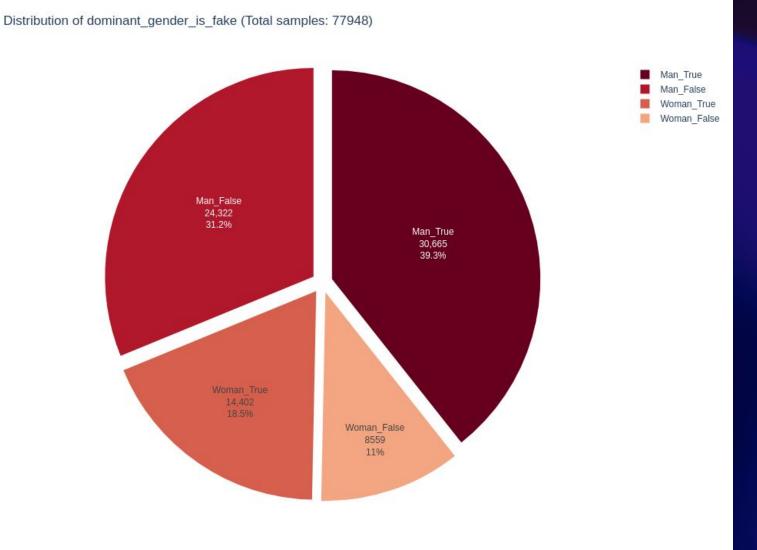
Combating DeepFakes Requires Dataset Generation: Face Gender X Race Distribution





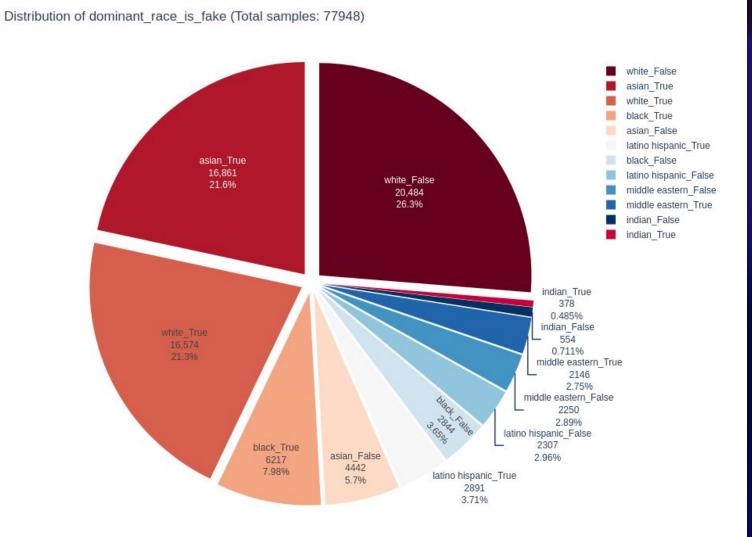


Combating DeepFakes Requires Dataset Generation: Face Gender X Real/Fake Distribution



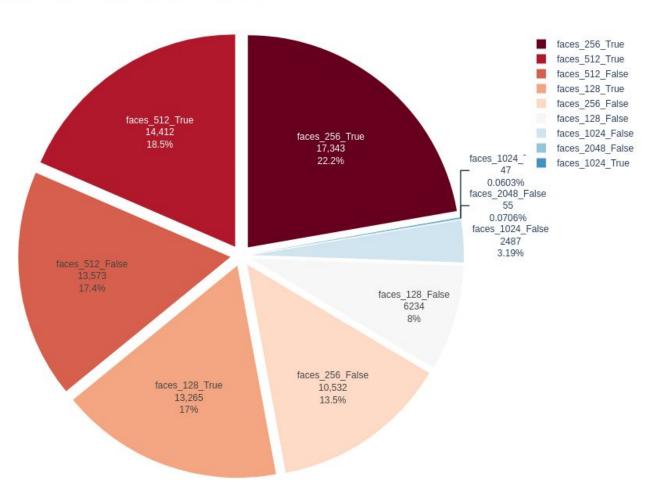


Combating DeepFakes Requires Dataset Generation: Face Race X Real/Fake Distribution

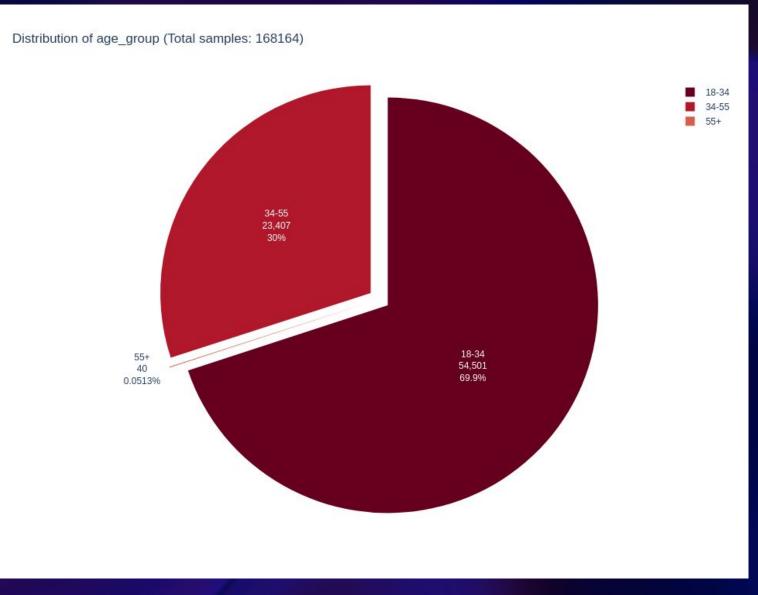


Combating DeepFakes Requires Dataset Generation: Face Resolution X Real/Fake Distribution

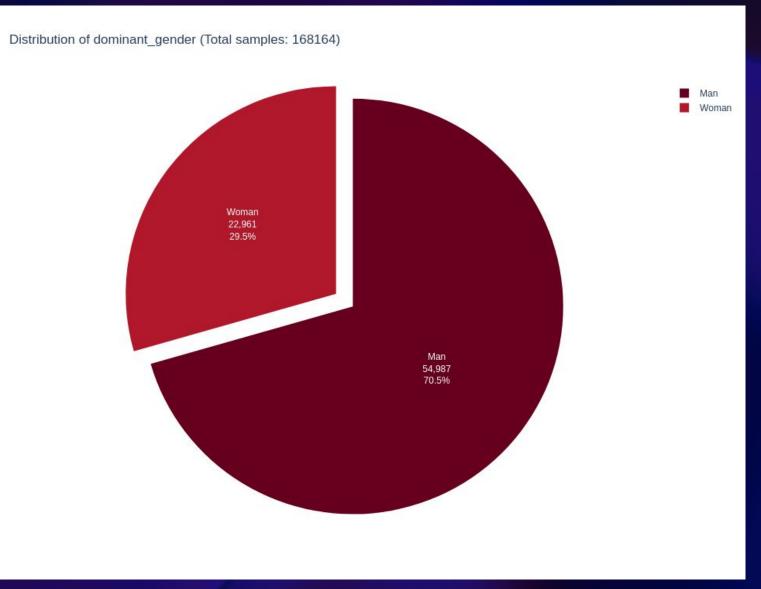
Distribution of face_size_is_fake (Total samples: 77948)



Combating DeepFakes Requires Dataset Generation: Face Age Distribution

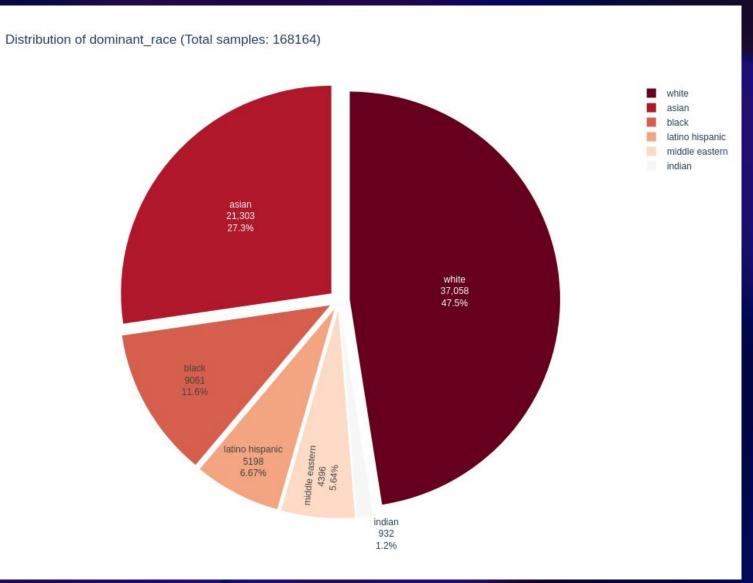


Combating DeepFakes Requires Dataset Generation: Face Gender Distribution



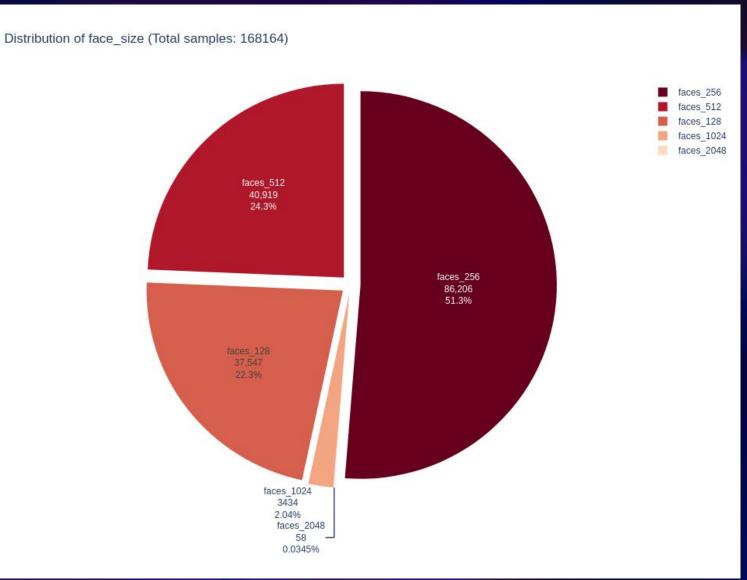


Combating DeepFakes Requires Dataset Generation: Face Race Distribution



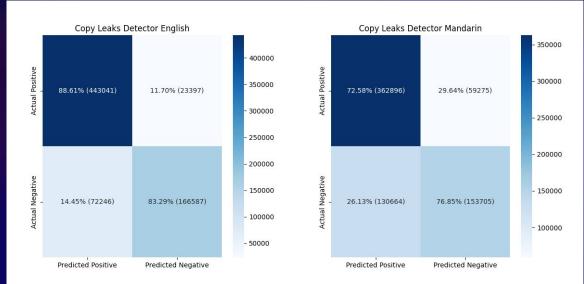


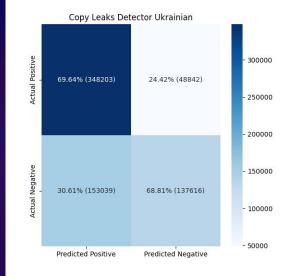
Combating DeepFakes Requires Dataset Generation: Face Resolution Distribution

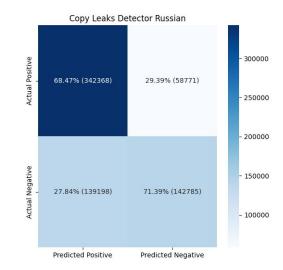




DeepFake Detection Results: Text DM-TextDetector-1 English, Mandarin, Russian, Ukrainian

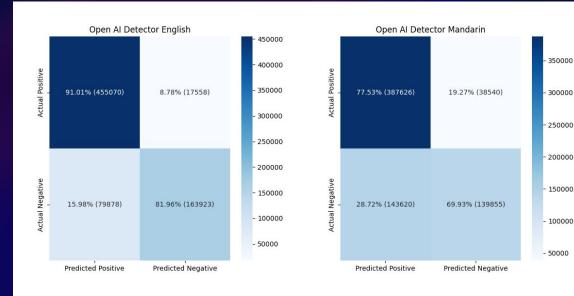


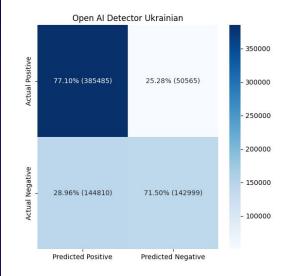


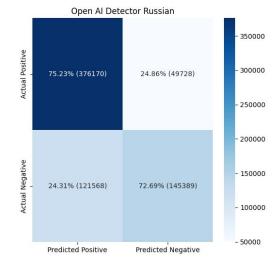




DeepFake Detection Results: Text DM-TextDetector-2 English, Mandarin, Russian, Ukrainian

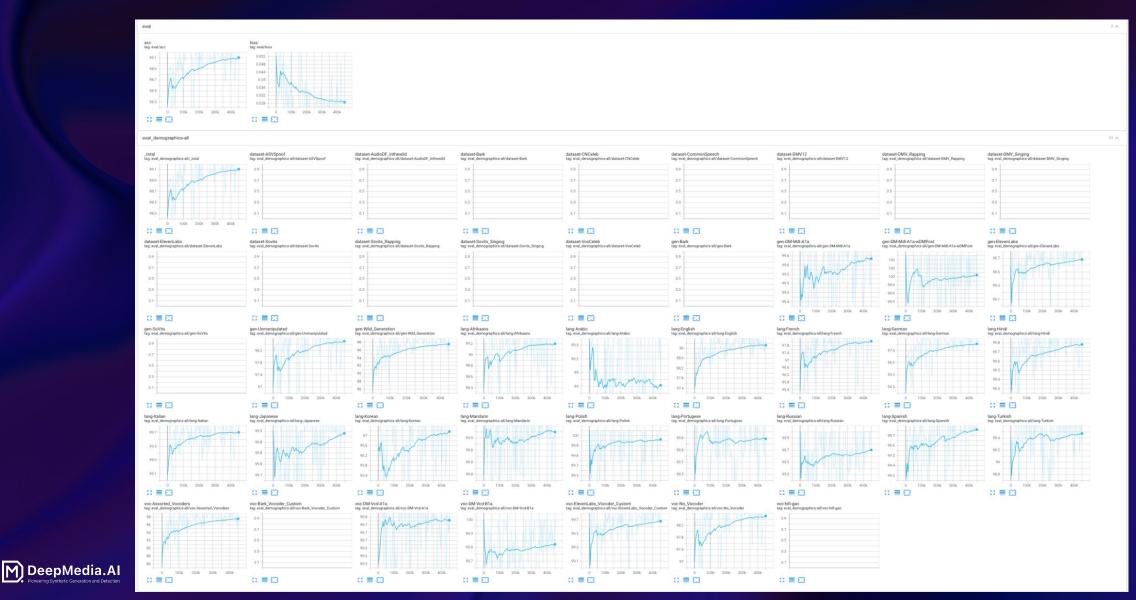




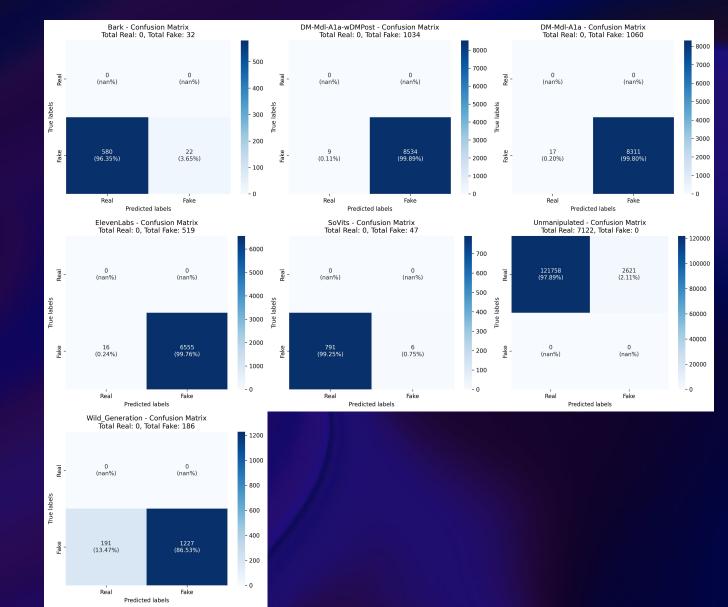




DeepFake Detection Results: Voice DM-VD-2 Training Logs (No Augmentation)



DeepFake Detection Results: Voice DM-VD-2 Results (No Augmentation)



DeepFake Detection Results: Voice DM-VD-2 Results (No Augmentation)

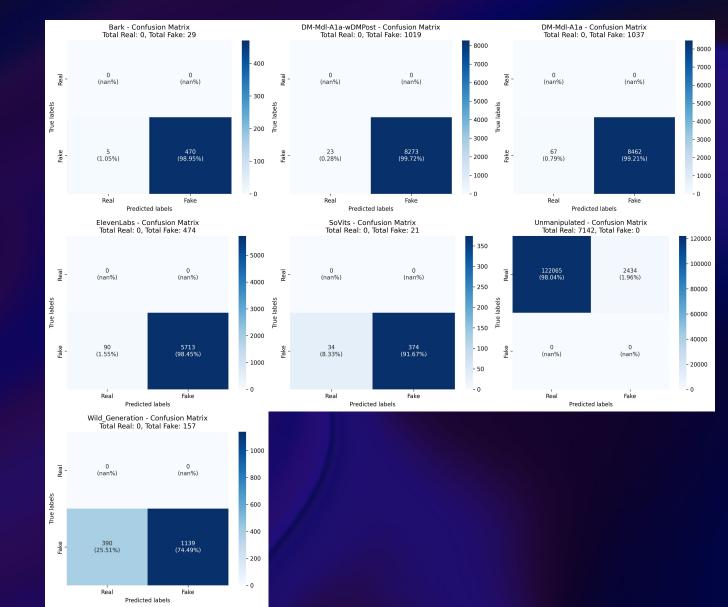




DeepFake Detection Results: Voice DM-VD-2 Training Logs (With Augmentation)



DeepFake Detection Results: Voice DM-VD-2 Results (With Augmentation)



DeepFake Detection Results: Voice DM-VD-2 Results (With Augmentation)

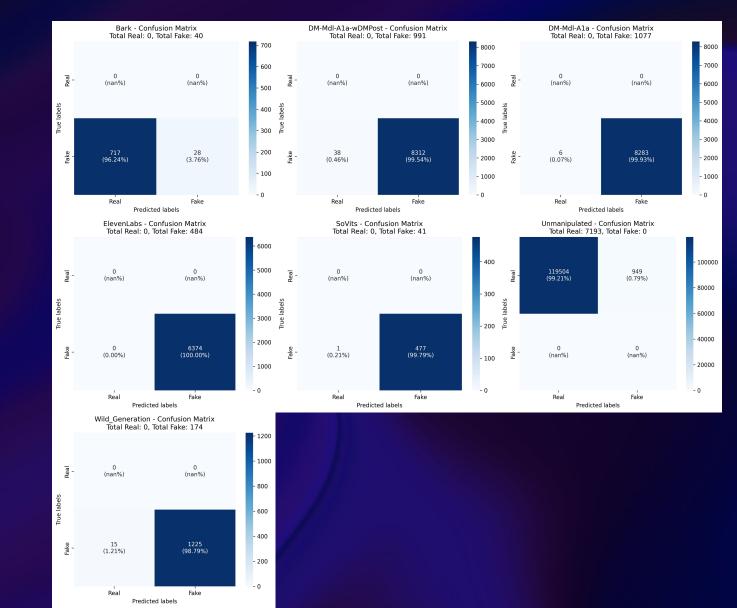




DeepFake Detection Results: Voice DM-VD-3 Detector Training Logs (No Augmentation)

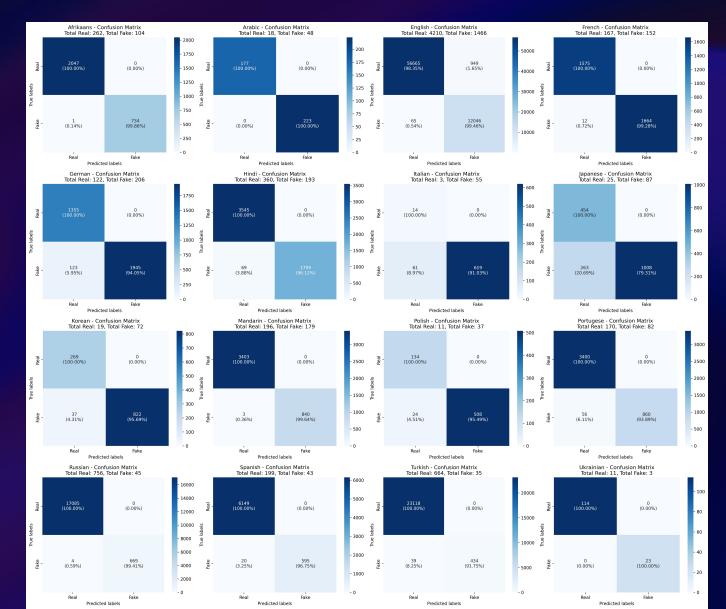


DeepFake Detection Results: Voice DM-VD-3 Detector Results (No Augmentation)



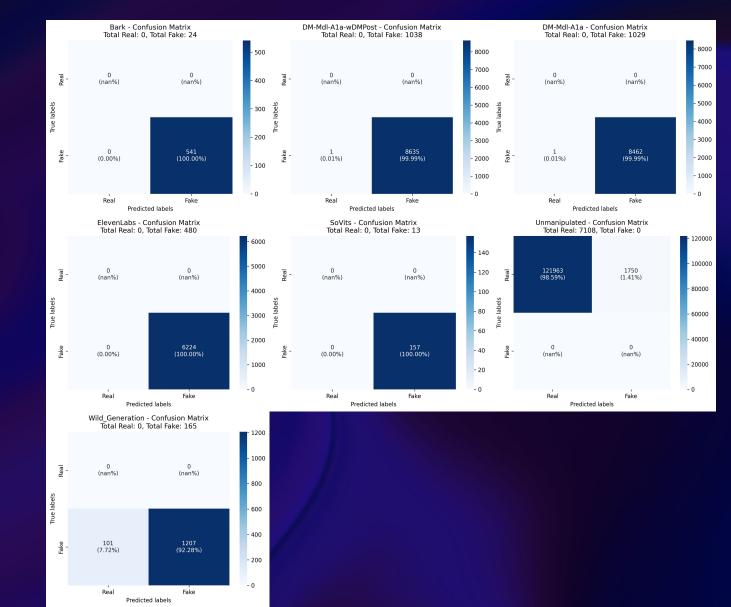


DeepFake Detection Results: Voice DM-VD-3 Detector Results (No Augmentation)





DeepFake Detection Results: Voice DM-VD-3 Detector Results (With Augmentation)

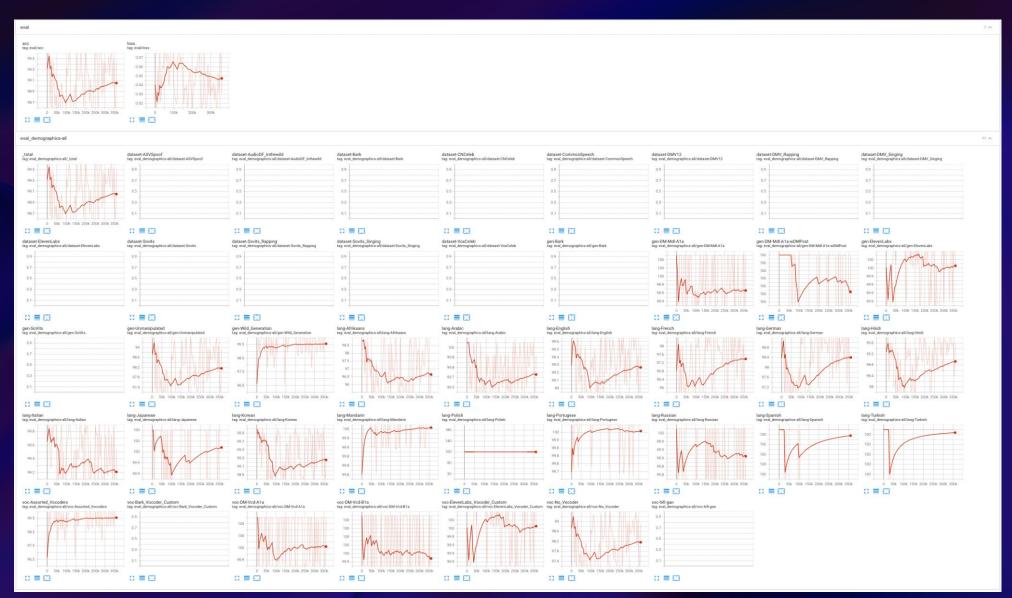


DeepFake Detection Results: Voice DM-VD-3 Detector Results (With Augmentation)



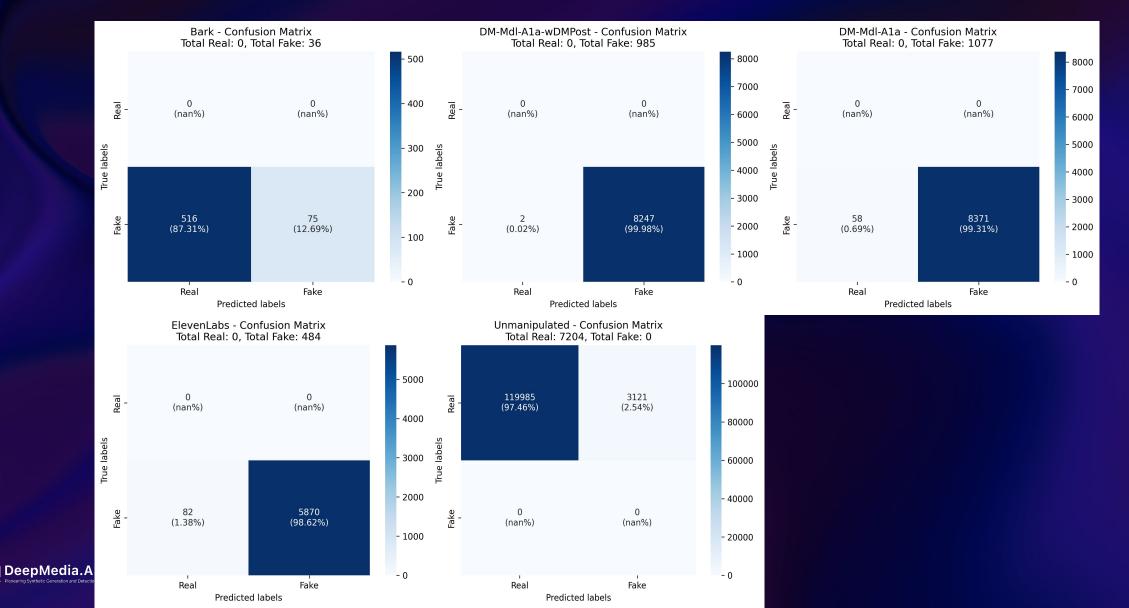
M DeepMedia.AI

DeepFake Detection Results: Voice DM-VD-1 Detector Training Logs (No Augmentation)



M)

DeepFake Detection Results: Voice DM-VD-1 Detector Results (No Augmentation)

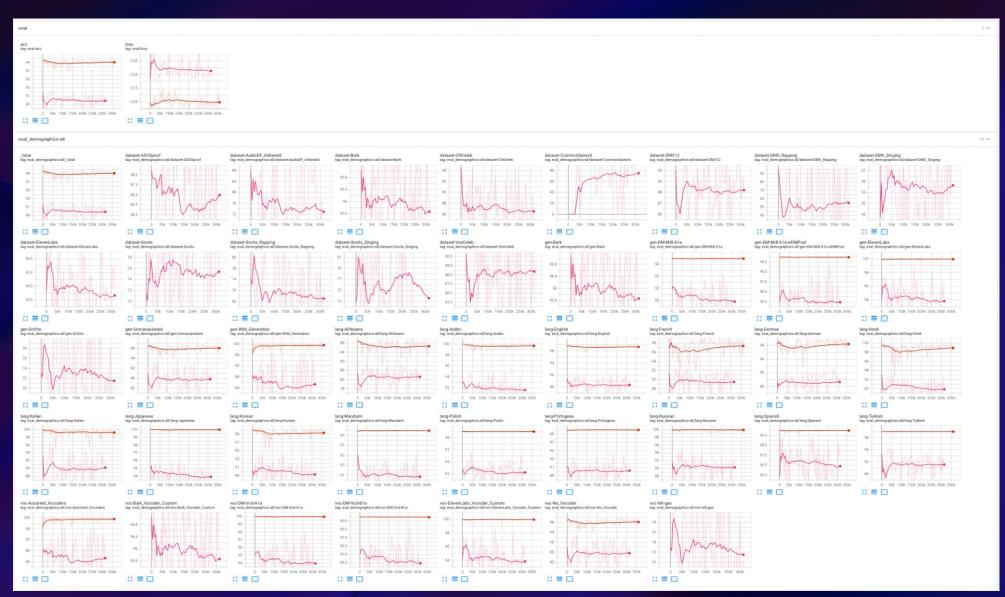


DeepFake Detection Results: Voice DM-VD-1 Detector Results (No Augmentation)

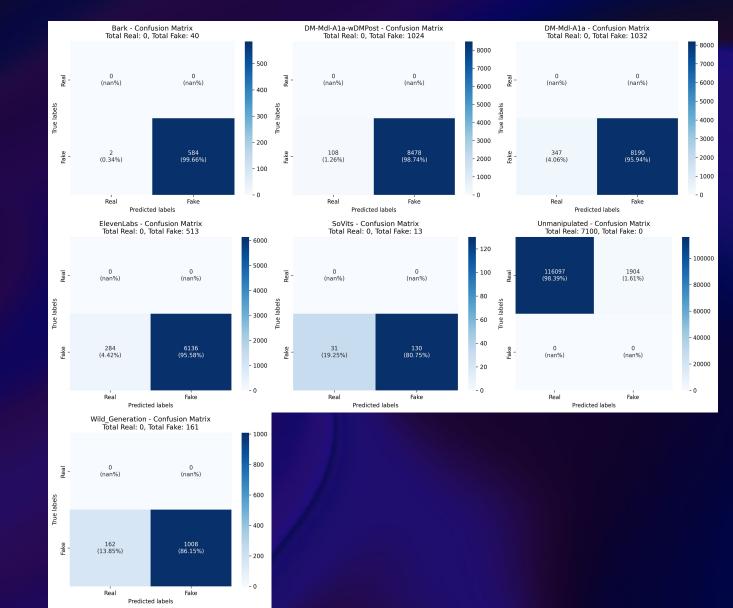




DeepFake Detection Results: Voice DM-VD-1 Detector Training Logs (With Augmentation)



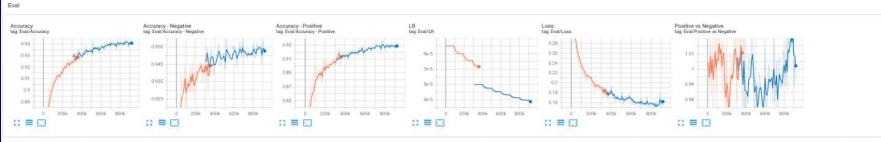
DeepFake Detection Results: Voice DM-VD-1 Detector Results (With Augmentation)



DeepFake Detection Results: Voice DM-VD-1 Detector Results (With Augmentation)



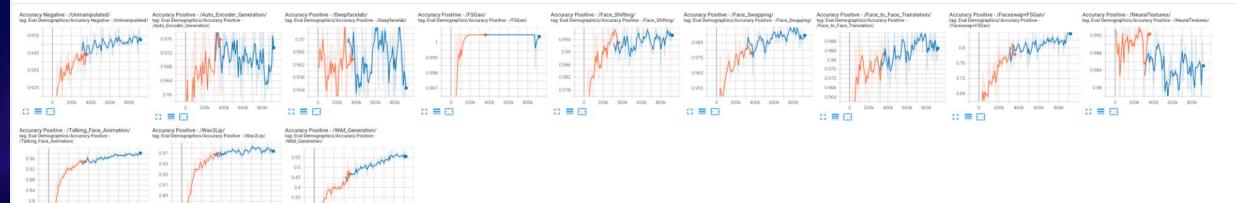
DeepFake Detection Results: Face DM-FD-1 Detector Training Logs (No Augmentation)



Eval Demographics

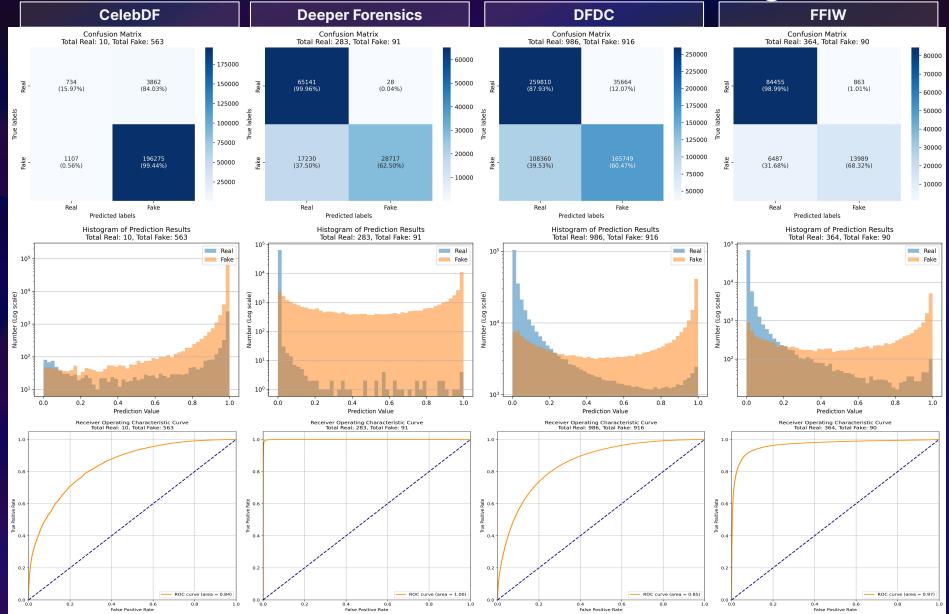
0.76

0 = 🖸





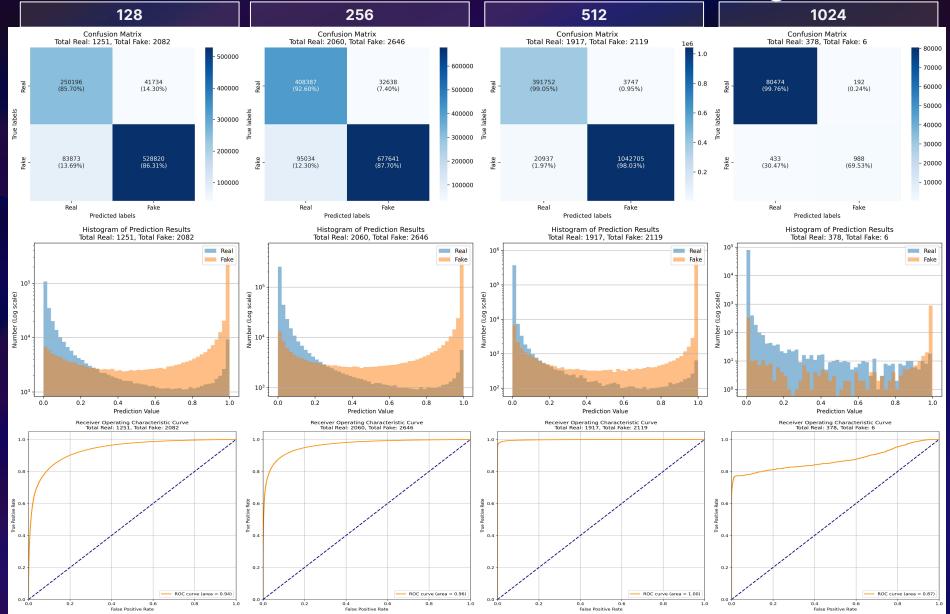
DeepFake Detection Results: Face DM-FD-1 Detector Results on Datasets (No Augmentation)



M)

DeepMedia.Al

DeepFake Detection Results: Face DM-FD-1 Detector Results on Face Size (No Augmentation)



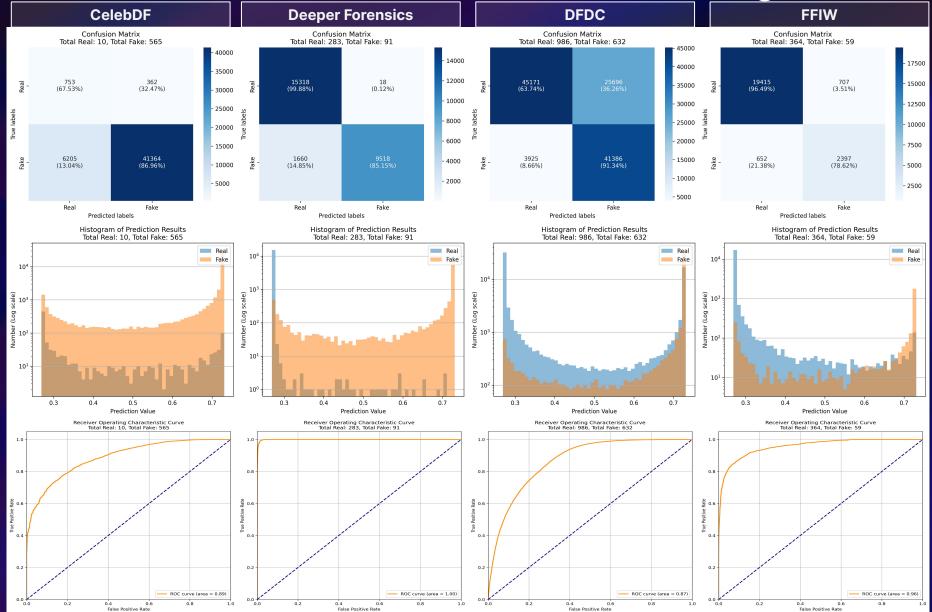
DeepFake Detection Results: Face RMViT Detector Training Logs (w/ Augmentation)







DeepFake Detection Results: Face DM-FD-2 Detector Results on Datasets (No Augmentation)

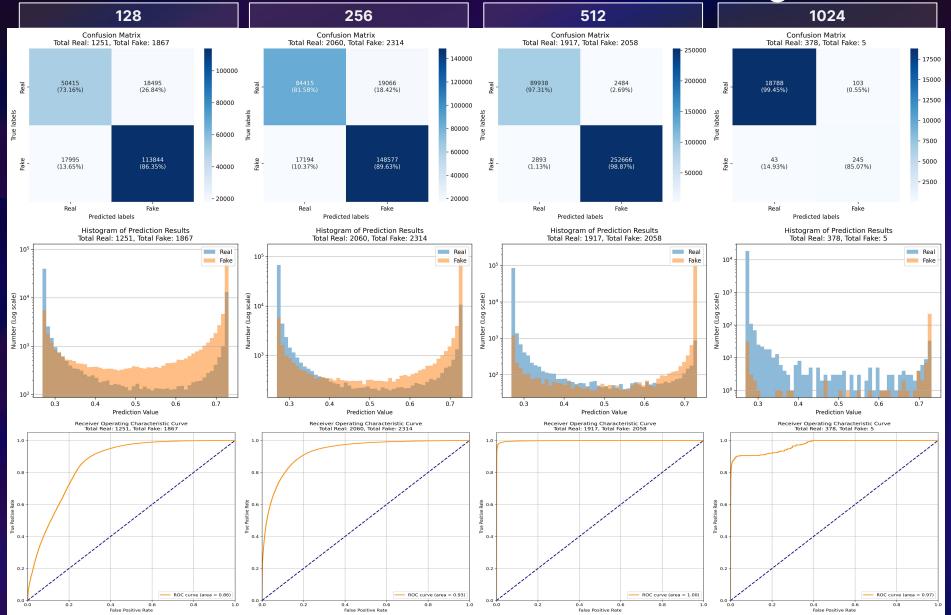




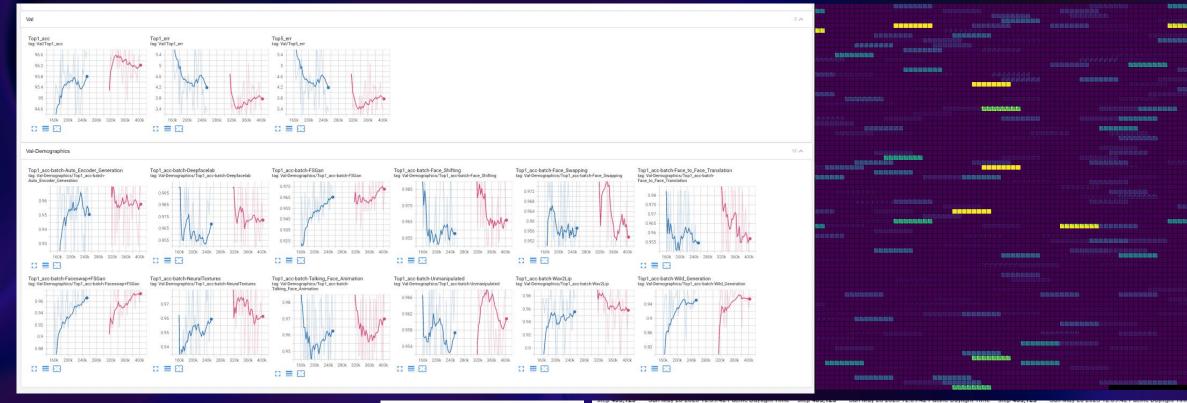
DeepMedia.AI

M)

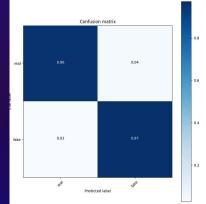
DeepFake Detection Results: Face DM-FD-2 Detector Results on Face Size (No Augmentation)

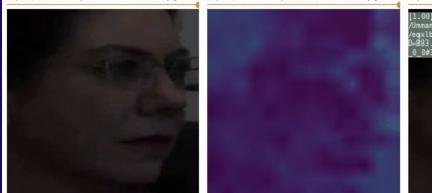


DeepFake Detection Results: Face DM-FD-3 Detector Training Logs (No Augmentation)



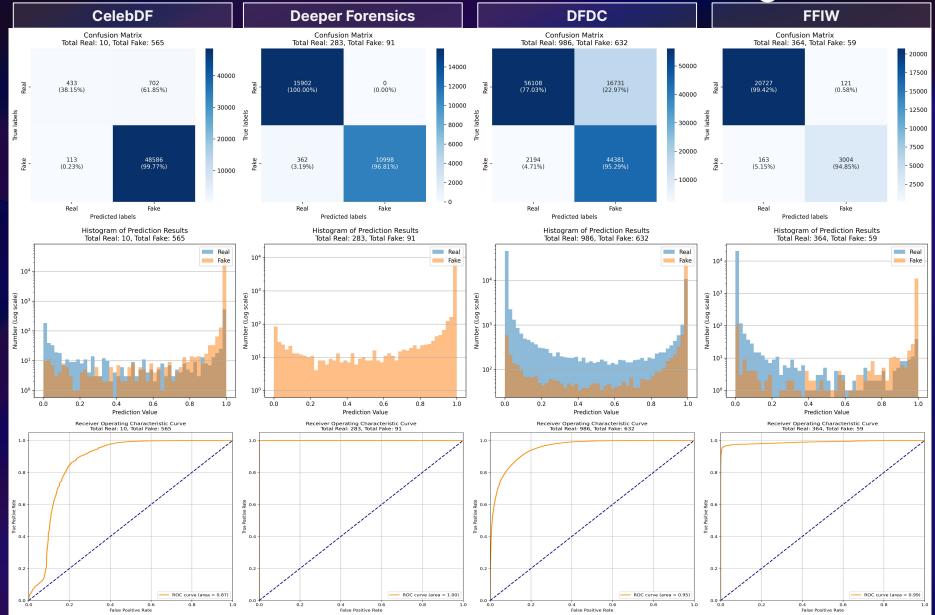






[1.00] real | [1.00] real /Unmanipulated/validation/DEDC/faces_256 /eqxlbewrge_dfdc_val_rl/t_#000000#000300 D=83.4853984375x157.1656494140625_part _0_0#300/

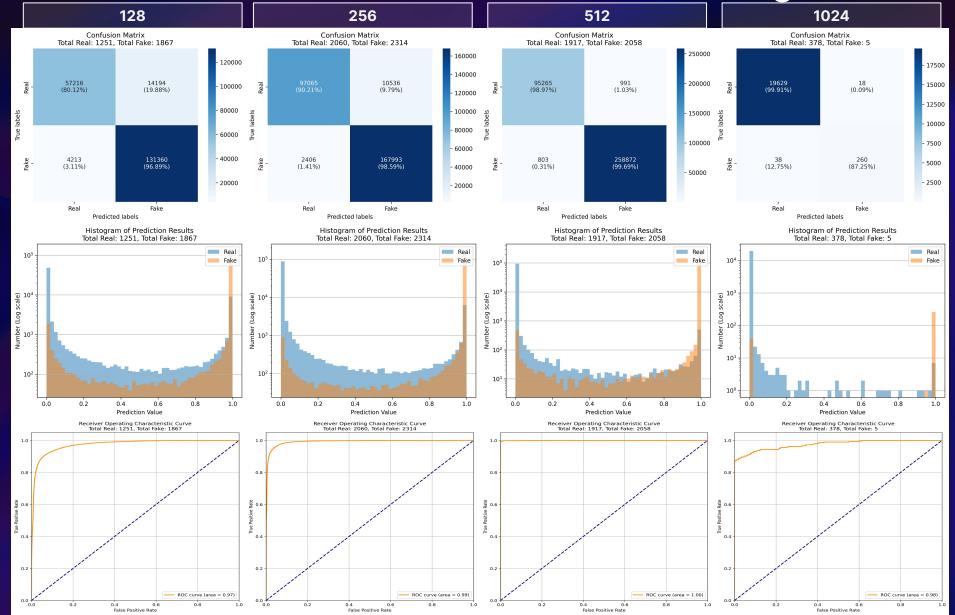
DeepFake Detection Results: Face DM-FD-3 Detector Results on Datasets (No Augmentation)



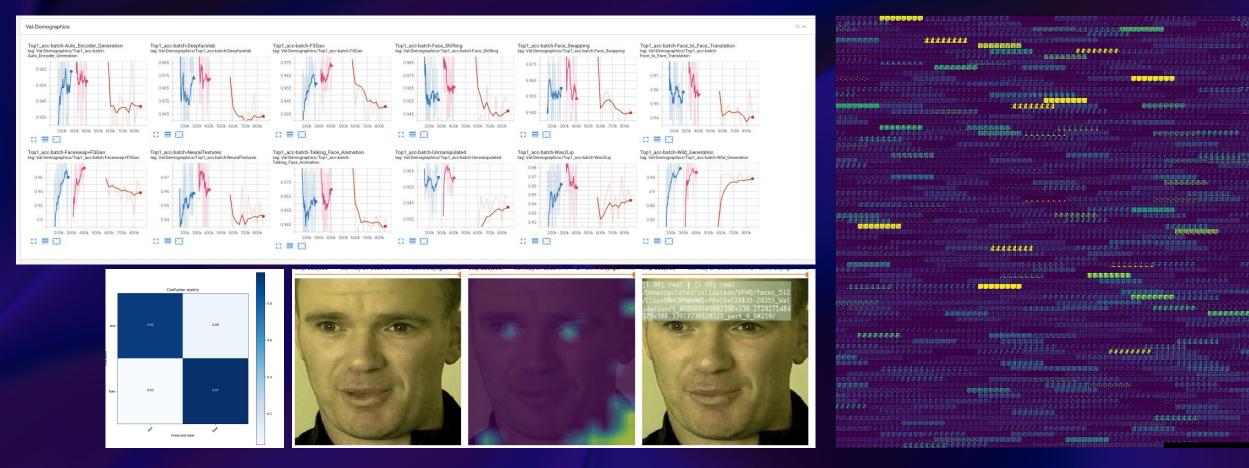
M

DeepMedia.Al

DeepFake Detection Results: Face DM-FD-3 Detector Results on Face Size (No Augmentation)

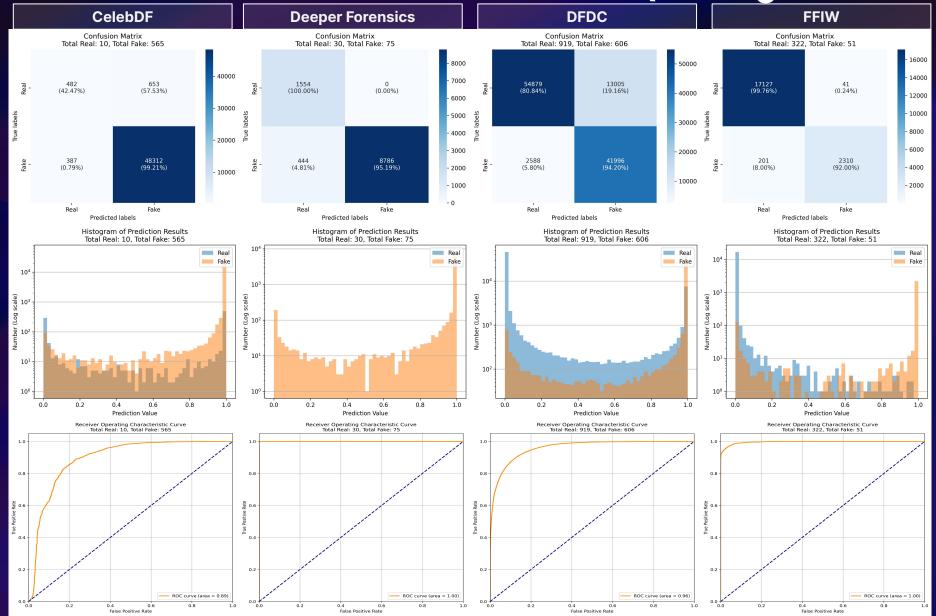


DeepFake Detection Results: Face DM-FD-3 Detector Training Logs (With Augmentation)



DeepFake Detection Results: Face

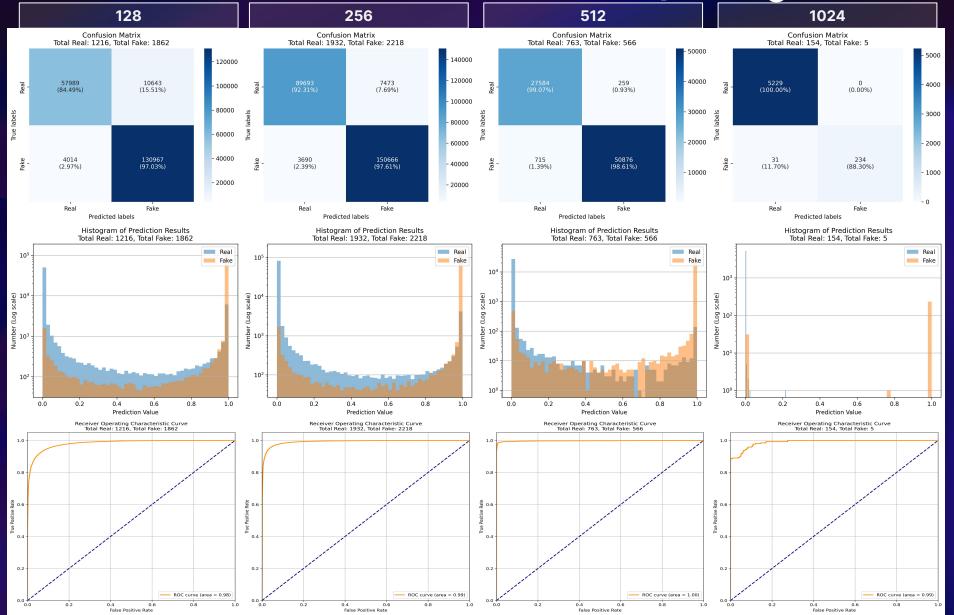
DM-FD-3 Detector Results on Datasets (w/ Augmentation)



M)

DeepMedia.Al

DeepFake Detection Results: Face DM-FD-3 Detector Results on Face Size (w/ Augmentation)



Voice Identity Detection

