magix

The Surge of Deepfake Cyber Threats

The Magix R&D Lab

Authors

Primary Author: Floyd Tshoma

Co-Author: Tim Butler

Co-Author: Hlayisani Shondlani

Executive Summary

Deepfakes are fake videos or audio recordings made using AI. They can look or sound exactly like a real person, such as a CEO, politician, or police officer, even when that person never said or did those things.

Criminals are using deepfakes to scam people and businesses. These fakes are so realistic that even trained professionals are being fooled. They are being used in scams, fake investment ads, political misinformation, and identity theft.

Reports show that biometric deepfakes, such as faces, fingerprints or voices, are being used more and more across Africa. Incidents involving people, such as Patrice Motsepe, and companies alike, such as Luno, are growing at an alarming rate.

The need to understand and train for recognizing deepfakes is becoming increasingly necessary as attacks become more prevalent. Detecting flaws in deepfakes, performing additional verification steps, and investing in software for protection are recommended as mitigation factors.

Deepfakes are no longer just a technical curiosity, they’re a growing threat. Businesses, governments, and individuals must stay alert. Cybercriminals are already using this technology to steal millions, spread false information, and damage trust. The time to act is now.

Case Study: Successful Deepfake Attack Using Zoom

In 2024, a Hong Kong finance manager at a global company received what looked like a routine video call from the company's CFO and team. He spoke clearly, looked confident, and asked for an urgent $25 million transfer. The manager didn't think twice, until it turned out the CFO was never on the call. It was a deepfake, an AI-generated impersonation, alongside the other members of the team. The incident resulted in significant financial losses and was only discovered once the manager later checked with the corporation's head office. This was further exacerbated by the Hong Kong police discovering that numerous stolen identity cards were used to make loan applications and open bank accounts, all using deepfakes to trick facial recognition programs.

> "Can I please have an urgent **$25 million** transfer?"

Welcome to the new frontier of cybercrime, as authorities across the world are growing increasingly concerned at the sophistication of deepfake technology. In this article, we breakdown the facts and details involving deepfakes.

What are Deepfakes?

Deepfakes use artificial intelligence to create hyper-realistic fake videos or voice recordings of real people, usually referred to as synthetic media. At the core of the deepfake pipelines sits the Generative Adversarial Networks (GANs), which train two different networks together: a generator, which creates candidate media, and a discriminator, that tries to distinguish the generated media from real data. With these iterative and "adversarial" training, the generator learns to produce media closer and closer to the real data, until the discriminator cannot tell the difference.

Many deepfakes use an auto encoder for face swapping, which will be the primary focus of this white paper. In the instance of face-swapping, two encoder-decoder models are trained simultaneously, where one focuses on Person A and the other on Person B. The encoder for each person will discern and learn the general structure of the face (shape, expression, movement), while its decoder learns the specific appearance for each person. Swapping the decoders between the two produces nearly seamless face replacements.

Think of a scammer mimicking your boss's voice or even face perfectly. They're no longer science fiction. They're here, and they're fooling everyone from business executives to election officials.

Cybersecurity experts are raising red flags as a new wave of deepfake attacks is sweeping across industries globally, with alarming implications for businesses, politics, and public safety.

Recent incidents have shown a surge in the use of AI generated deepfake videos and voice clones to impersonate high-profile executives, political leaders, and even law enforcement officials. These sophisticated manipulations are now being used not just for misinformation and fraud, but also as tools in highly targeted spear-phishing and social engineering attacks.

What is real

Are you real or are you a deep fake?

What's happening in South Africa right now?

Corporate Deepfake fraud is rising

Scammers are impersonating CEOs and CFOs in video calls or voice messages, tricking employees into transferring millions. These deepfakes are so realistic, even tech-savvy staff are falling for them.

Political Deepfakes stir election misinformation in South Africa

In the weeks leading up to South Africa's 2024 general elections, deepfake videos featuring international political figures started circulating online, spreading misinformation and confusion among voters. One video was viewed over 159,000 times globally, falsely portrayed U.S. President Donald Trump endorsing the South African political party uMkhonto weSizwe (MK). The deepfake was created using AI voice cloning tools and was distributed primarily through social media platforms.

These artificial videos generated using open access platforms were created with minimal technical expertise, yet appeared convincing enough to mislead segments of the population.

As deepfake technology becomes more accessible, it's use in the political arena is expected to increase, raising urgent questions about the regulation of synthetic media, the responsibilities of tech platforms, and the readiness of electoral bodies to respond to AI-driven threats.

Even police voices are being cloned

People are getting phone calls from "law enforcement" threatening arrest or fines. Except it's not the police it's AI.

Case Studies of Deepfake Technology used in Africa

Deepfake technology is increasingly being exploited in Africa, leading to significant challenges for businesses and individuals. Here are some notable instances:

CASE STUDY: Investment deepfake featuring Patrice Motsepe

Direct YouTube Link: https://www.youtube.com/watch?v=pA4Kjvgb9LI

In early 2025, South Africa's Financial Sector Conduct Authority (FSCA) issued a warning about fraudulent investment schemes using deepfake videos of businessman Patrice Motsepe. These scams, operated by entities like Gold Earnings and Africa Gold, falsely depicted Motsepe endorsing investment opportunities promising returns of up to 46%. Neither Motsepe nor his company, African Rainbow Minerals, had any association with these entities.

CASE STUDY: Luno crypto platform targeted with deepfake audio

In mid-2024, an employee at Luno, a prominent South African cryptocurrency exchange, received a WhatsApp voice message that appeared to be from a senior executive. The message, created using deepfake audio technology, instructed the employee to authorize a significant transaction. Fortunately, the employee identified the deception before any funds were transferred.

The Rise in biometric fraud across Africa

In 2024, a new kind of digital threat quietly swept across Africa, one that didn’t rely on brute force hacks or phishing emails, but instead wore a convincing human face.

It started with a spike in failed identity verifications. Smile ID, a leading digital identity verification company operating across the continent, began detecting an unusual pattern. Their systems, which processed more than 110 million ID checks from January to December 2024, flagged an alarming rise in deepfake videos. At first, it was just a few impersonations attempts here and there. But within months, it turned into a bloodbath. By year end, deepfake based fraud had spread.

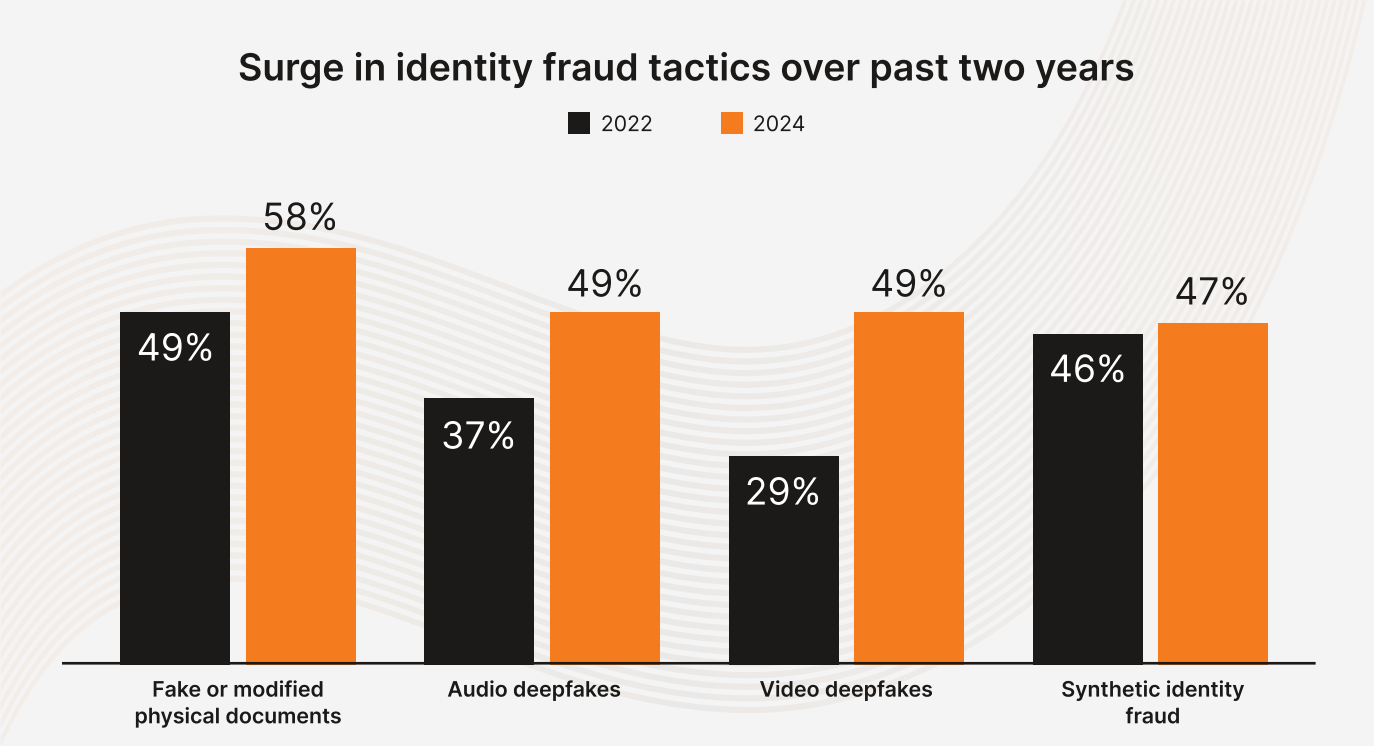
What Smile ID uncovered is part of a wider and more disturbing trend which is the weaponization of generative AI for biometric fraud. Criminals are now using AI tools to fabricate lifelike faces, voices, and documents, blurring the line between real and fake. These synthetic identities are then used to bypass biometric systems, impersonate individuals, and commit financial crimes with ease.

The issue isn't confined to Africa, but with its rapidly digitising economies and evolving security infrastructure, Africa is particularly vulnerable.

Generative AI was linked to over one third of all new biometric fraud cases detected in 2024, Smile ID reported. The scale and sophistication of these attacks are placing immense pressure on businesses and institutions that rely on digital ID verification.

One of the most shocking examples came when a deepfake video was used to impersonate the African Union's Chairperson. The video, which circulated briefly online, was convincing enough to spark confusion and concern. While it was quickly debunked, the incident highlighted the potential damage these attacks can inflict, not just financially, but on public trust.

Cybersecurity experts warn that these AI-powered impersonations are being used to infiltrate vulnerable platforms, exploit weak security systems, and disrupt civic and financial institutions. As Africa accelerates its digital transformation, the need for advanced fraud detection and stronger biometric safeguards has never been more urgent.



Deepfake romance scams by 'Yahoo Boys'

Cybercriminals known as "Yahoo Boys," primarily based in Nigeria, have been using real-time deepfake technology to conduct romance scams. By employing face-swapping tools, they convincingly impersonate individuals during video calls, deceiving victims into sending money. These tactics have contributed to substantial financial losses globally.

Deepfake romance scams by 'Yahoo Boys'

In South Africa, scammers have circulated deepfake videos featuring Elon Musk and Johann Rupert promoting fraudulent investment opportunities. These videos, shared widely on social media, have misled individuals into investing in non-existent schemes, underscoring the dangers of manipulated media.

How Deepfakes Are Created

Deepfakes used to be funny TikTok clips. Now, they’re being used to rob companies, manipulate voters, and impersonate law enforcement. Deepfakes affect everyone, and to understand them helps us to be aware and alert to them.

Let’s do a quick recap from the earlier introduction, tied to the references below: The deepfake AI is powered by two machine learning models working against each other. The “generator” algorithm is trained using sample imagery, audio, and/or video to create a new piece of media (Merged Frame) or manipulate an existing one that collectively resembles the samples as closely as possible.

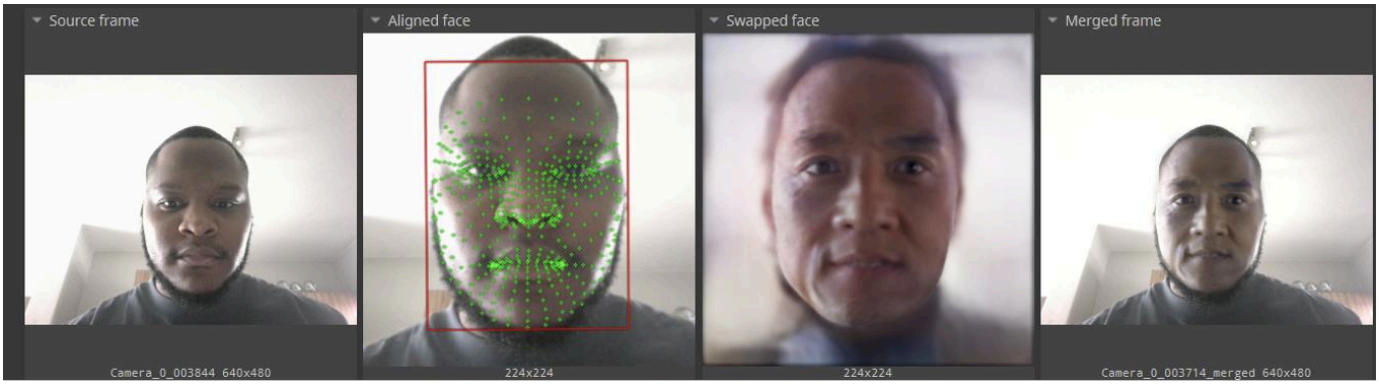
In initial steps, the camera watches the face of the person driving the conversation (the source). Then, using sophisticated algorithms to map the key points in the face to accurately depict facial structure and movements (aligned face) to seamlessly blend the mimicked face (swapped face) upon their own.

This produces the final image (merged frame), where the algorithms morph, blend and colour correct the face to be a near-perfect replica.

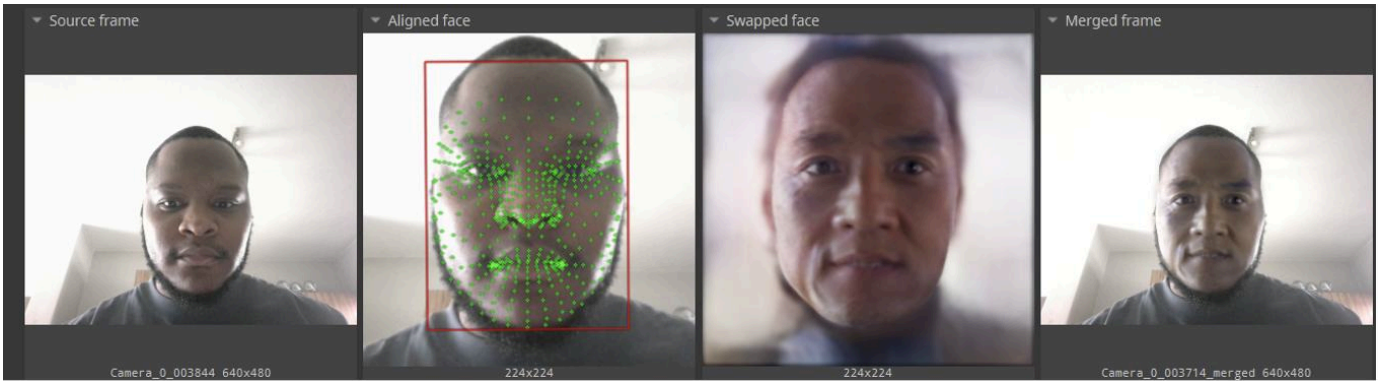
Magix R&D Lab Simulations

As seen below, an individual person can use the Deepfake technology to look like different people. These examples focused on real-time (streaming) deepfakes, which combine the method described earlier into low-latency pipelines, which continuously captures frames from the webcam, runs each frame through a pre-trained face-swap model (optimized with lightweight encoders and decoders), and renders the swapped face into the outgoing video in real-time

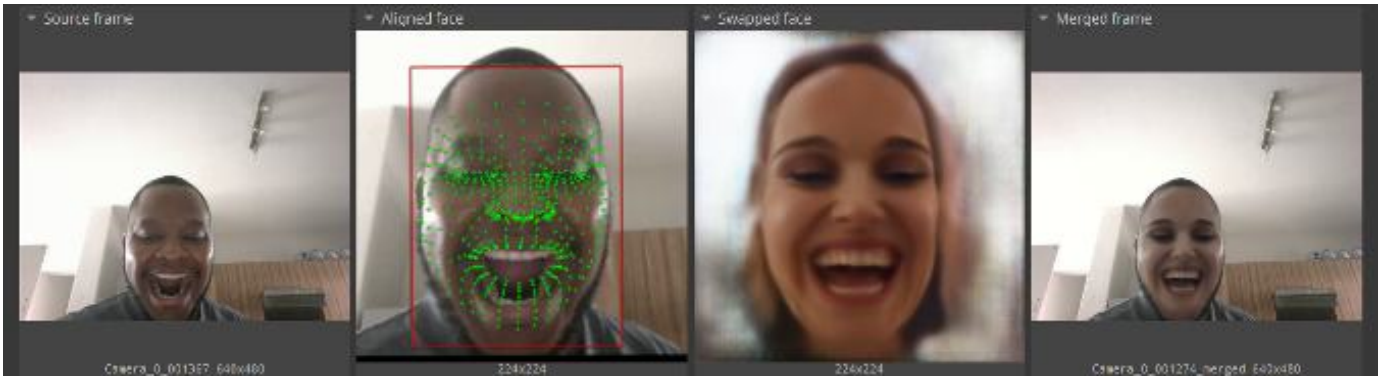
Sample 1: B-Jackie B-Chan



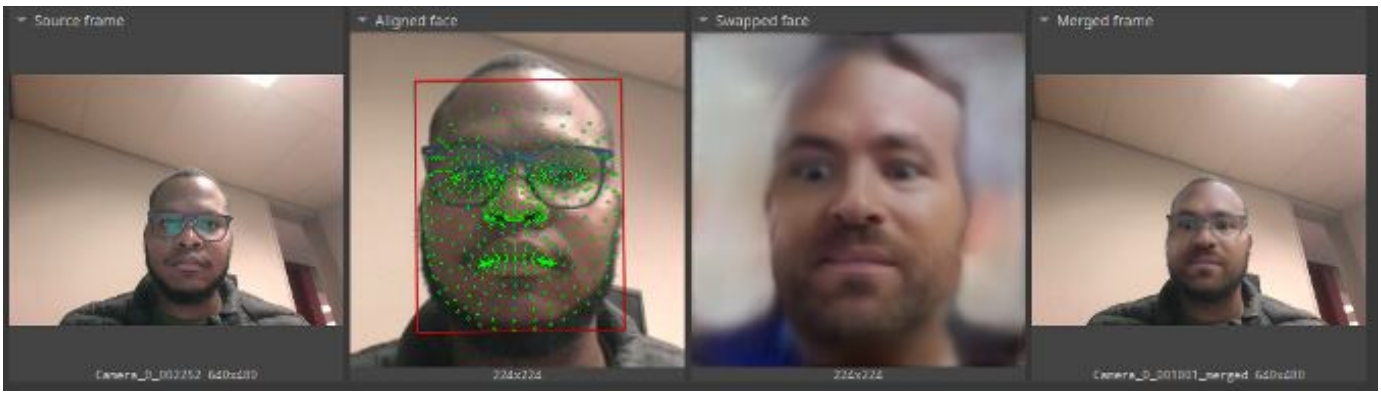
Sample 2: Mr B-Bean



Sample 3: B-Portman



Sample 4: B-Ryan B-Reynolds



With the right equipment, i.e. a strong CPU, GPU and abundance of RAM, coupled with numerous reference photos of the subject that is to be imitated, the resulting image could be close to one-hundred percent accurate.

During our testing phase, we initiated an online live call within the team. The deepfake was streaming live on the call and was unerringly accurate. Although there was stuttering on the stream, especially when switching the face on the fly, the accuracy was still believable. The stuttering was due to the limitation of the hardware and not the deepfake itself.

Recommendations to Reduce Exposure to Deepfake Attacks

Pause before you act

If something feels off, even if it looks or sounds real, trust your instincts and verify it through another channel. Many deepfakes are designed to exploit urgency, and rushing into action is what the malicious actors count on. Take a moment to assess; if you receive an unexpected request involving sensitive data or money, step back and verify it independently.

Use callbacks and security phrases

Establish a trusted way to confirm identity, especially for sensitive decisions like money transfers. One example can include that if you receive an instruction over video or audio, hang-up and call the person back using a known internal number. Another example is to use unique, pre-agreed passphrases for any sensitive communications, and provide an additional layer of security for a malicious actor to compromise for them to be successful.

Train your people

Regular training on deepfakes and social engineering is no longer optional, it’s essential. These should include articles, videos and events that teach users to recognise deepfakes and manipulated media, understanding common social engineering tactics (urgency, authority, fear), and even running simulations to test staff responses. This ensures that your staff become a strong first line of defence.

Invest in detection tools

There are now AI tools that can spot signs of deepfake manipulation in real-time. These function by scanning for any facial inconsistencies (blinking rates, unnatural expressions), analysing audio for any synthetic speech patters and monitoring metadata or compression anomalies in media files.

Look for flaws

For visual clues, pay extra attention to the mouth, forehead and neck when on a video call, these are areas of the body that can often betray the use of AI. For deeper examination, look to unnatural skin textures, flickering shadows and inconsistent lighting. For audio flaws, a robotic or overly smooth voice tone, odd pauses, mismatched lip-syncing and missing background noises are also key indicators.

Limit Publicly Available Media

Having an abundance of photos, videos or audio of staff members online creates a pool of resources for a malicious actor to train their deepfake engines. Encouraging staff, especially senior executives, to manage their digital footprint will help reduce these malicious efforts. Limiting what they share on social media, make personal profiles private and being cautious about public interviews and webinars can all help with this.

Establish a Culture of Verification

Building a workplace culture where staff feel empowered to question requests, even from leadership. Make it the norm and encourage double-checking odd instructions, especially when under pressure.

Conclusion

AI-generated identity fraud is multiplying across the globe. Recent surveys and cybersecurity report consistently show double, nearly triple digit increases in deepfake incidents in 2024 and 2025

Businesses are seeing larger average losses, and organized crime rings are leveraging inexpensive “deepfake-as-a-service” tools to launch sophisticated attacks. The financial toll (millions per scam, projected billions overall) and pervasiveness, with nearly half of firms affected, understand why deepfakes are now a major cybercrime concern.

magix

This white paper was compiled by the Magix Lab team

Sources

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

https://www.geeksforgeeks.org/generative-adversarial-network-gan/#:~:text=1,receives%20is%20real%20or%20fake

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=A%20generative%20adversarial%20network%2C%20or,boost%20their%20levels%20of%20accuracy

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=A%20generative%20adversarial%20network%2C%20or,boost%20their%20levels%20of%20accuracy

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=A%20generative%20adversarial%20network%2C%20or,boost%20their%20levels%20of%20accuracy

https://developers.google.com/machine-learning/gan/gan_structure#:~:text=Here%27s%20a%20picture%20of%20the,whole%20system

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=A%20generative%20adversarial%20network%2C%20or,boost%20their%20levels%20of%20accuracy

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=A%20generative%20adversarial%20network%2C%20or,boost%20their%20levels%20of%20accuracy

https://developers.google.com/machine-learning/gan/gan_structure#:~:text=Here%27s%20a%20picture%20of%20the,whole%20system

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=Deepfakes%20leverage%20autoencoders%20by%20training,images%20in%20the%20reconstruction%20process

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=Deepfakes%20leverage%20autoencoders%20by%20training,images%20in%20the%20reconstruction%20process

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=Deepfakes%20leverage%20autoencoders%20by%20training,images%20in%20the%20reconstruction%20process

https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/#:~:text=videos%20so%20uncannily%20authentic,%E2%80%94%20a%20stunningly%20accurate%20representation

https://arxiv.org/html/2411.19537v1#:~:text=introduce%20a%20face%20reenactment%20GAN%2C,3DMM%20and%20obtain%20predefined%2

Sources

0keypoints

https://arxiv.org/html/2411.19537v1#:~:text=introduce%20a%20face%20reenactment%20GAN%2C,3DMM%20and%20obtain%20predefined%20keypoints

https://www.youtube.com/watch?v=pA4Kjvgb9LI

https://www.moonstone.co.za/fsca-warns-of-deepfake-fraud-featuring-patrice-motsepe/

https://weetracker.com/2024/08/12/luno-fights-ai-deepfake-scams/

https://www.yahoo.com/news/surge-deepfakes-heightens-fraud-risk-083132665.html

https://www.youtube.com/watch?v=gK5iaAUsG-s

https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/

https://www.occrp.org/en/news/identity-fraud-in-africa-rises-sharply-deepfakes-lead/

https://www.youtube.com/watch?v=-kILAg5EBrs

https://www.dailymaverick.co.za/article/2024-06-04-rise-in-investment-scams-and-deepfakes-perpetrated-by-fraudsters-on-social-media/

https://www.deepfakevfx.com/downloads/deepfacelive/#:~:text=Real,video%20using%20trained%20face%20models

https://www.deepfakevfx.com/downloads/deepfacelive/#:~:text=Real,video%20using%20trained%20face%20models

https://regulaforensics.com/news/deepfake-fraud-doubles-down/#:~:text=Regula%E2%80%99s%20survey%20data%20shows%20a,compared%20to%202022%20survey%20data

https://regulaforensics.com/news/deepfake-fraud-doubles-down/#:~:text=In%202024%2C%20every%20second%20business,devices%20and%20identity%20verification%20solutions

https://securitybrief.co.uk/story/identity-fraud-in-europe-surges-by-150-deepfakes-on-the-rise#:~:text=The%20report%20reveals%20a%20concerning,end%20users%20have%20become%20victims

https://securitybrief.co.uk/story/identity-fraud-in-europe-surges-by-150-deepfakes-on-the-rise#:~:text=One%20of%20the%20standout%20findings,Business%20Development%2C%20Europe%20at%20Sumsub

Sources

https://regulaforensics.com/news/deepfake-fraud-doubles-down/#:~:text=Regula%E2%80%99s%20survey%20data%20shows%20a,compared%20to%202022%20survey%20data

https://www.gendigital.com/blog/insights/reports/threat-report-q4-2024#:~:text=Crypto%20scams%20evolved%20further%2C%20with,7%20million%20in%20Q4%2F2024%20alone

https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html