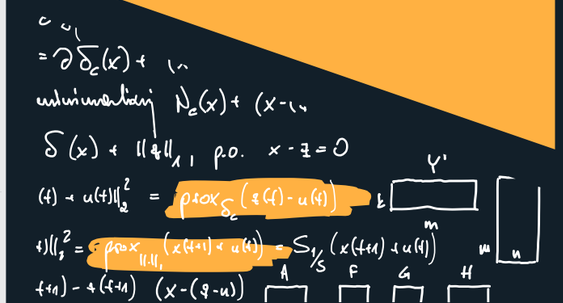


dr inż. Ewelina Bartuzi-Trokielewicz
mgr inż. Michał Ołowski
mgr inż. Joanna Gajewska
mgr inż. Alicja Martinek
inż. Adrian Kordas
mgr inż. Michał Koźbiał

SCIENCE
NASK

Co sprawia, że loteria cieszy się popularnością?

Co sprawia, że loteria cieszy się popularnością?

Wysoka wygrana

Co sprawia, że loteria cieszy się popularnością?

Wysoka wygrana

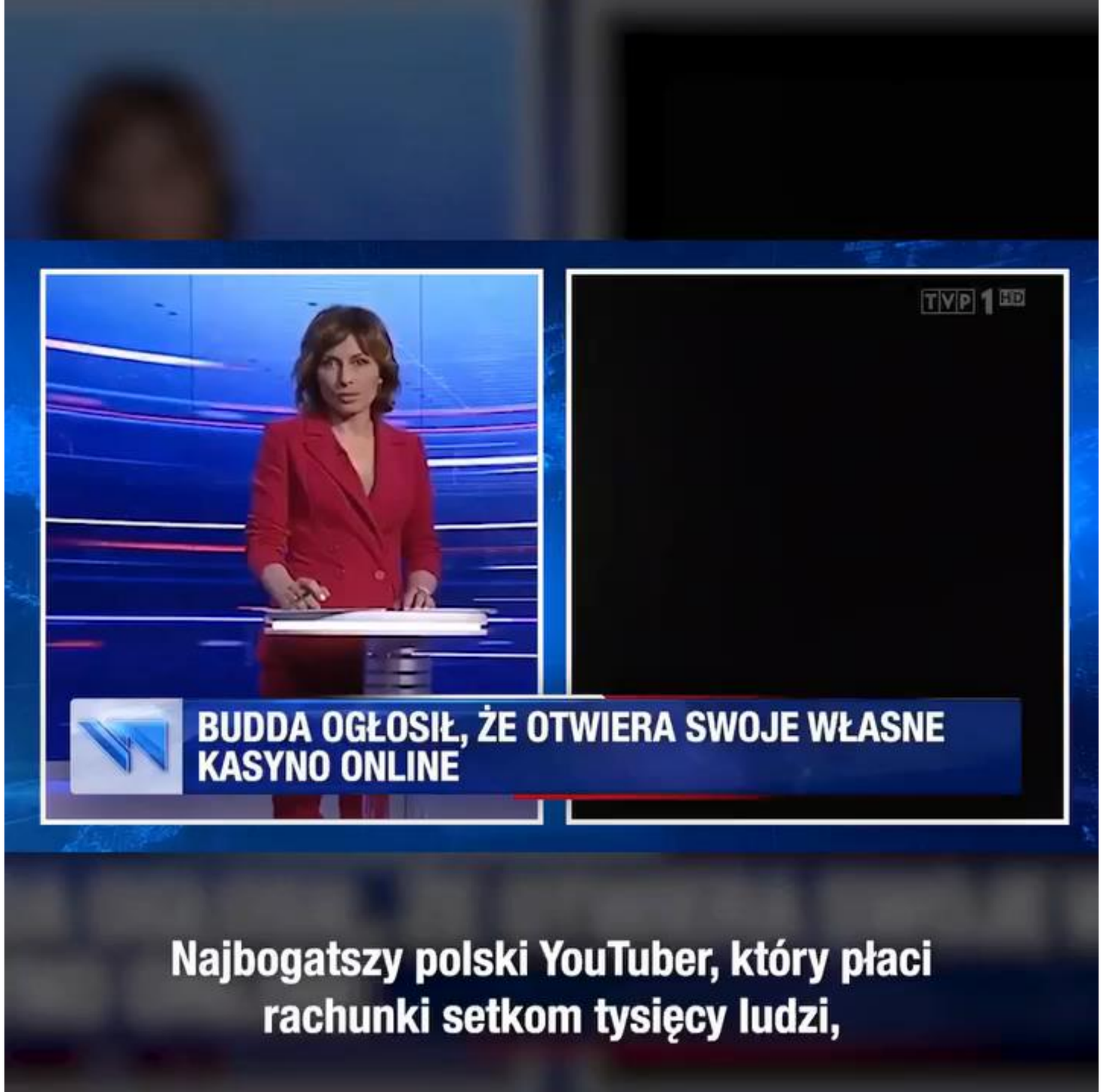
Niski próg wejścia

Co sprawia, że loteria cieszy się popularnością?

Wysoka wygrana

Niski próg wejścia

Zaufane źródło


TVP 1 HD
BUDDA OGŁOSIŁ, ŻE OTWIERA SWOJE WŁASNE KASYNO ONLINE
Najbogatszy polski YouTuber, który płaci rachunki setkom tysięcy ludzi,

Brzmi wiarygodnie?

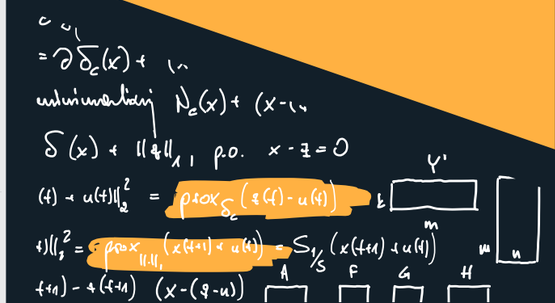
Wygląda wiarygodnie?

Nic bardziej mylnego!

Bądź ostrożny by potem nie było AIAIAI

Jak dobrym kłamcą jest AI?

dr inż. Ewelina Bartuzi-Trokielewicz
mgr inż. Michał Ołowski
mgr inż. Joanna Gajewska
mgr inż. Alicja Martinek
inż. Adrian Kordas
mgr inż. Michał Koźbiał



SCIENCE NASK

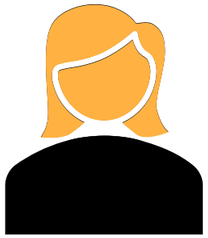
DEEPFAKE

Nowy wymiar kłamstwa

Czym jest DEEPFAKE

Technika manipulacji zdjęcia lub nagrania

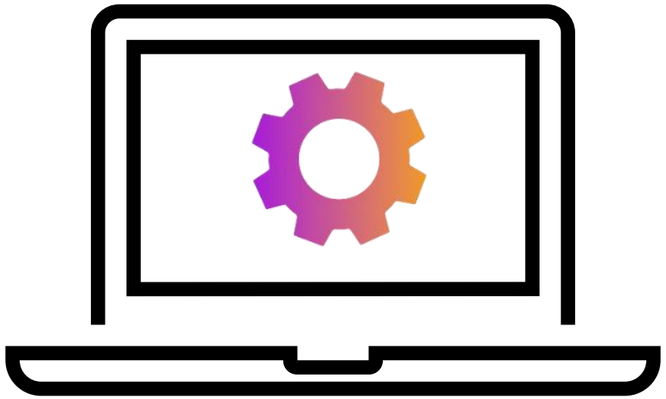
przy użyciu sztucznej inteligencji,



w których twarz lub głos osoby są zastąpione inną tożsamością.

baza zdjęć twarzy

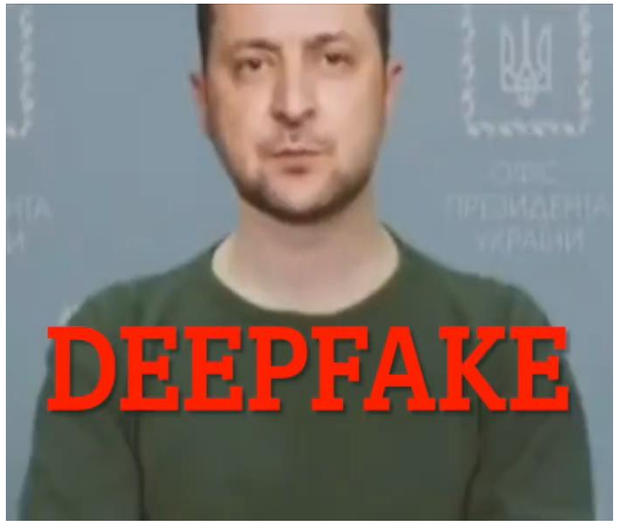
baza próbek głosu



Zastosowania

Rozrywka i Media

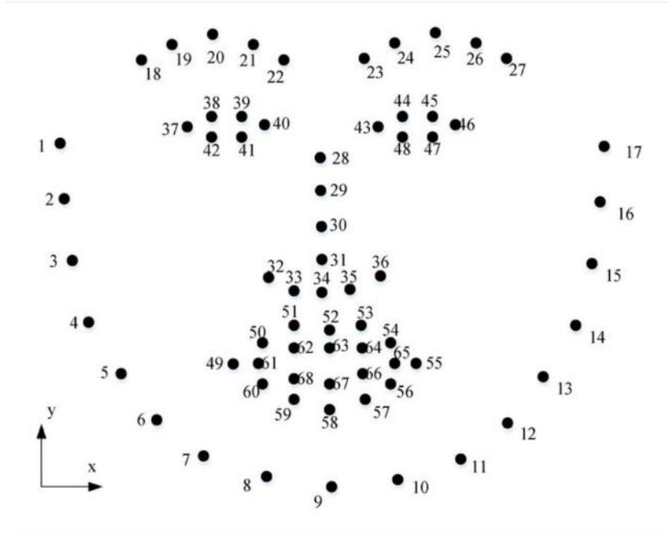
Edukacja i Szkolenia

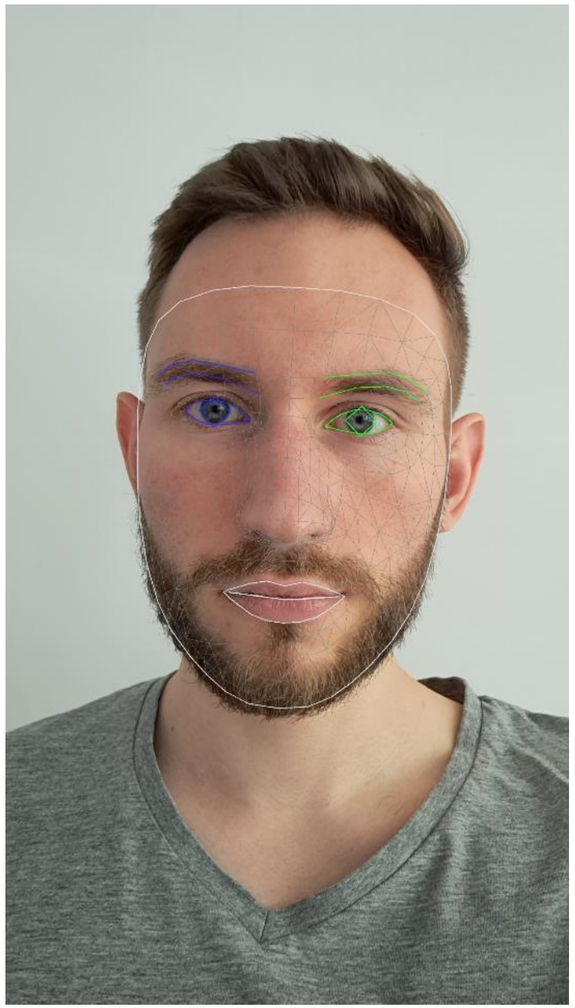


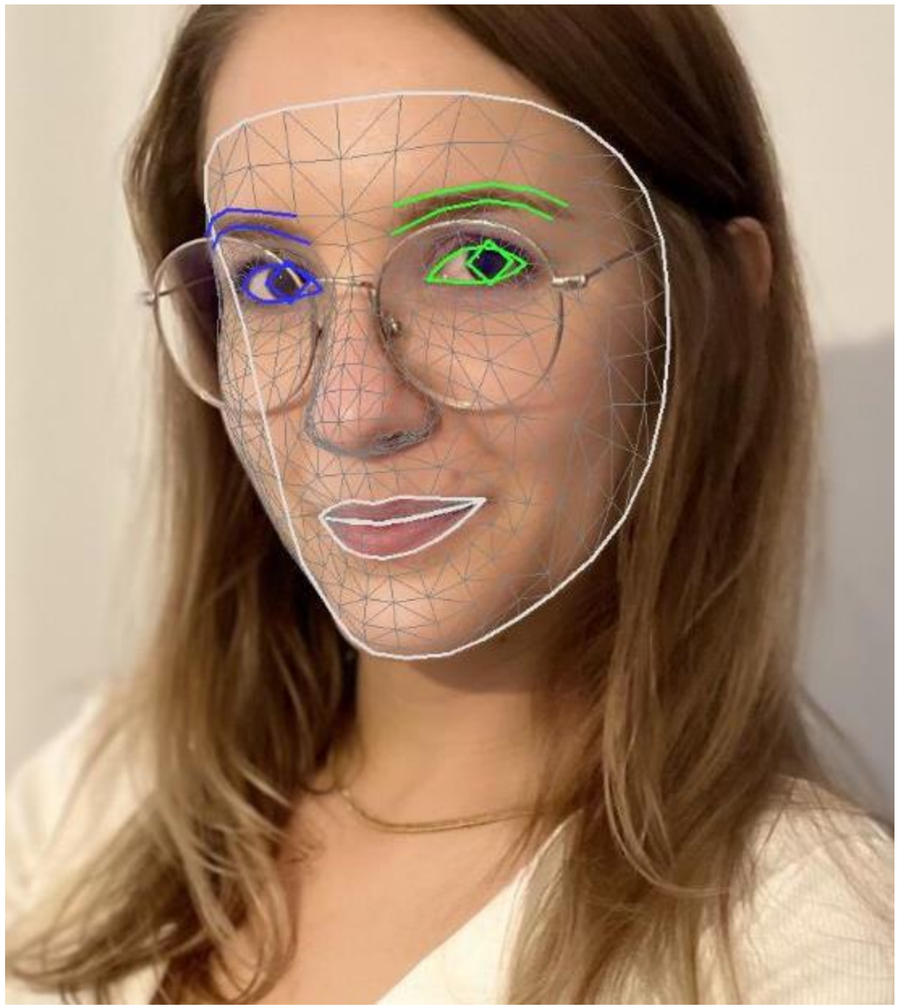
Dezinformacja i dyskredytacja

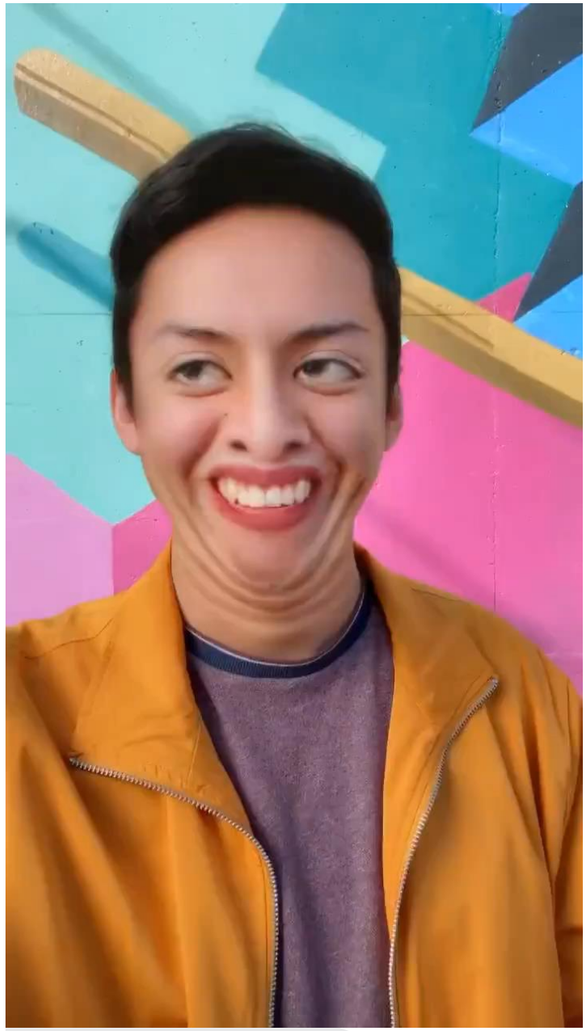
Jak maszyny widzą twarz?

Jak maszyny widzą twarz?

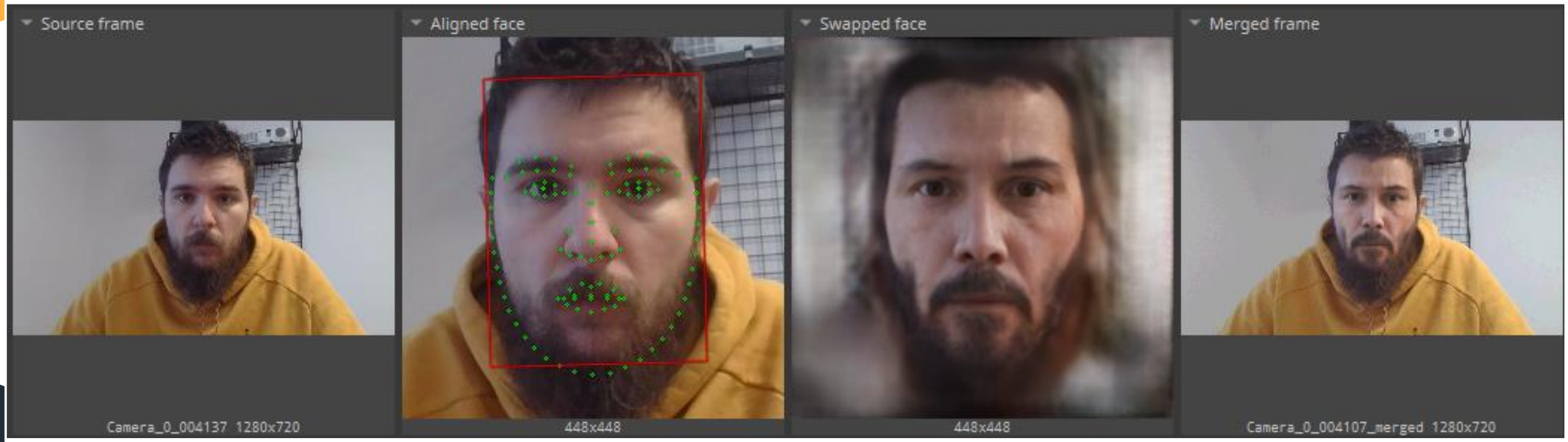








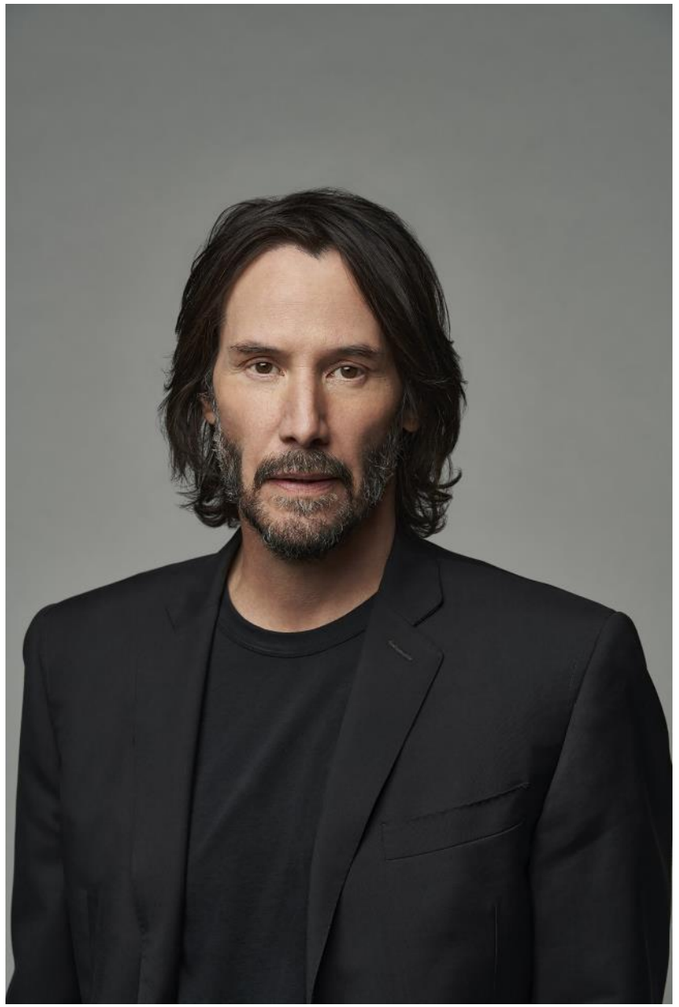
snapchat.com


Source frame
Aligned face
Swapped face
Merged frame
Camera_0_004137 1280x720
448x448
448x448
Camera_0_004107_merged 1280x720

Czym jest deepfake?

- zamiana tożsamości *(identity swap)*

https://codingislove.com/wp-content/uploads/2023/07/Face-swap-iron-man-elon-musk.jpg



SCIENCE
NASK

tiktok @iamjesserichards

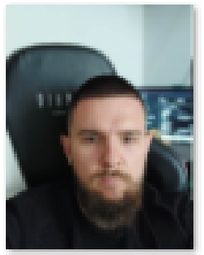
SCIENCE
NASK

tiktok @iamjesserichards

SCIENCE
NASK

SCIENCE
NASK

Iron Man.mp4



ja.png

Czym jest deepfake?

- Odtwarzanie / animacja twarzy
  (Face Reenactment)

arXiv:2104.11280

Rekonstrukacja twarzy

Czym jest deepfake?

- modyfikacja atrybutów twarzy
  (face attributes modification)

Źródło: arXiv:1711.10678v3

Modyfikacja atrybutów twarzy (face attributes modification)
Możliwe jest zmienienie wielu atrybutów twarzy, takich jak kolor oczu, kształt nosa, usta, brwi, kości policzkowe i wiele innych.

E. Bartuzi-Trokielewicz, M. Ołowski, A. Kordas, (2023), "Deepfake: jak sztuczna inteligencja może nas oszukiwać?", Cyberprofilaktyka NASK

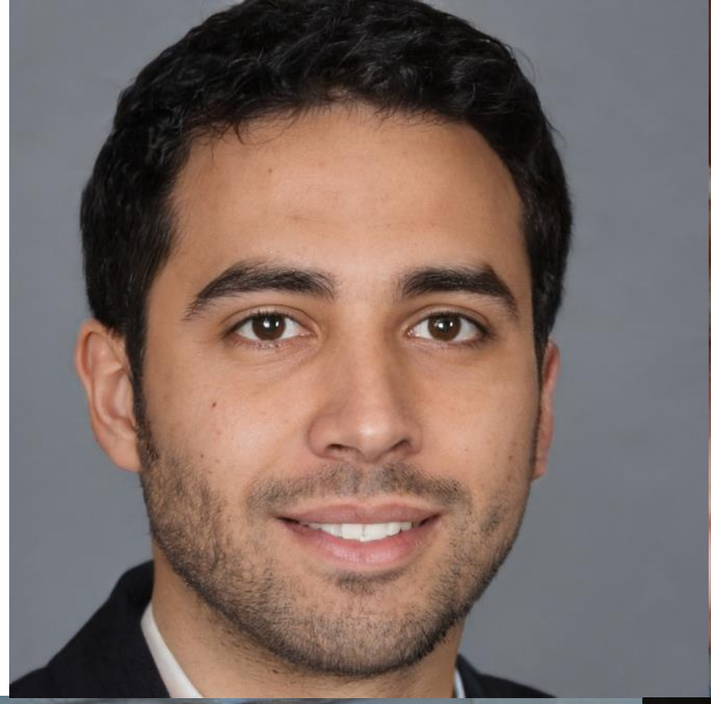
Czym jest deepfake?

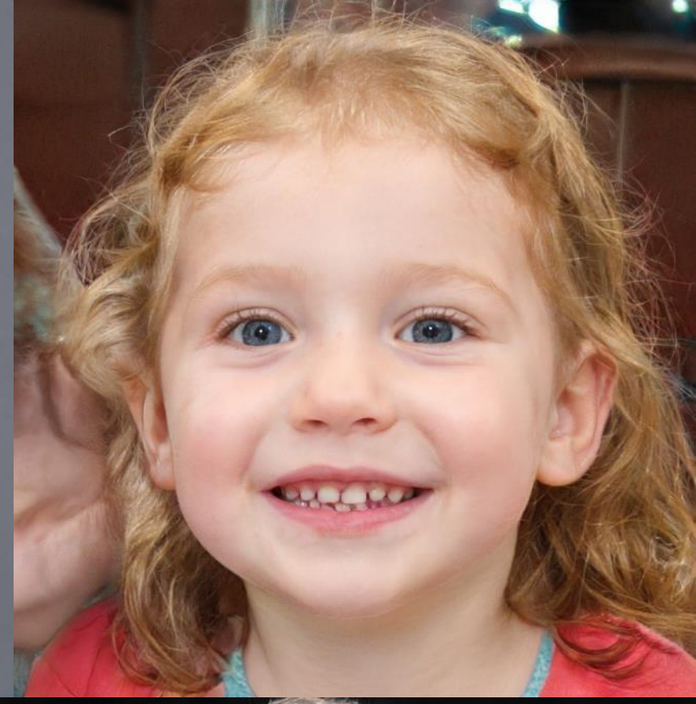
- Łączenie twarzy
  (face blending)

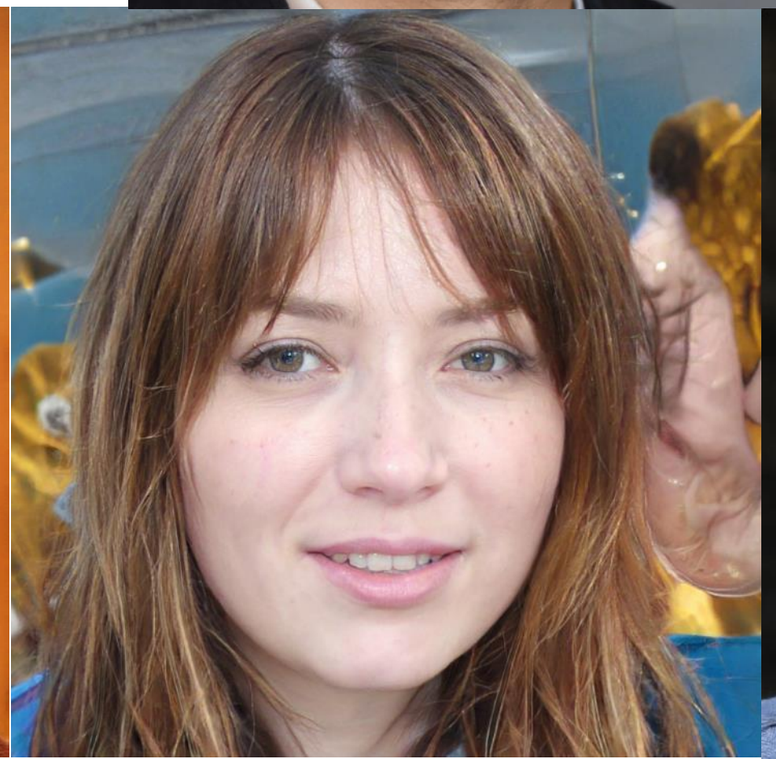
Gragnaniello, et.al.: Detection of AI-Generated Synthetic Faces.

Czym jest deepfake?

- w pełni syntetyczna twarz
  (fully synthetic face)







https://thispersondoesnotexist.com

W POSZUKIWANIU WSPÓLNEJ PRZESTRZENI

SCIENCE
NASK

Synchronizacja ust ze ścieżką audio

Daj głos...

...a komputer zacznie nim mówić

Klonowanie głosu

text-to-speech

speech-to-speech

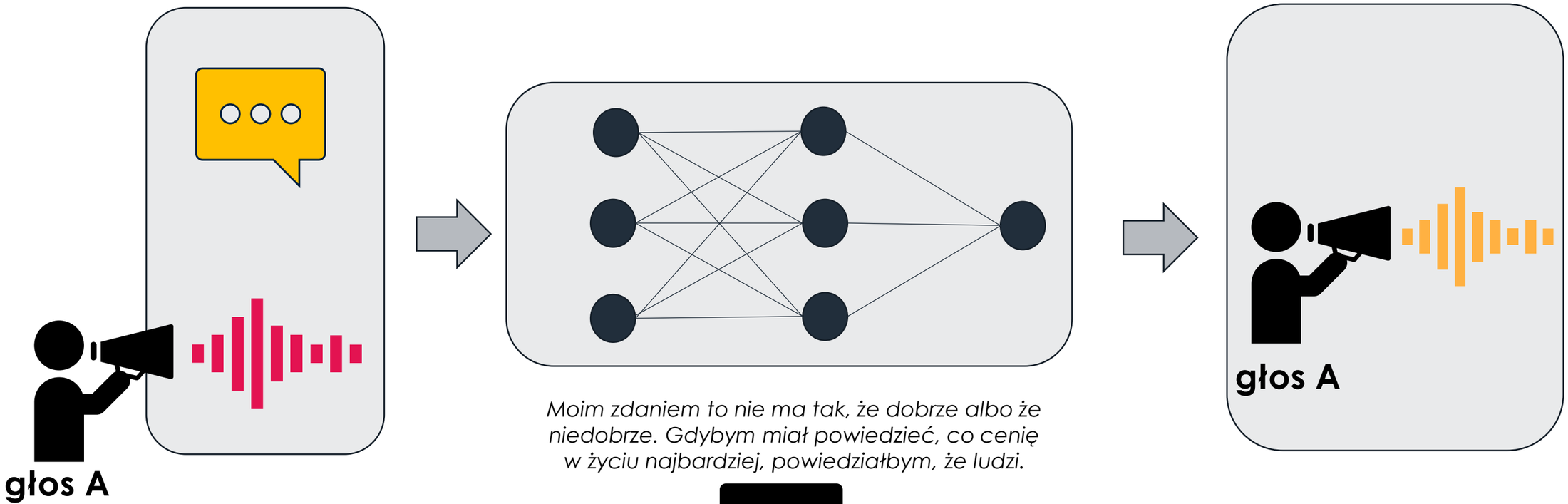
Postęp w generowaniu ludzkiej mowy

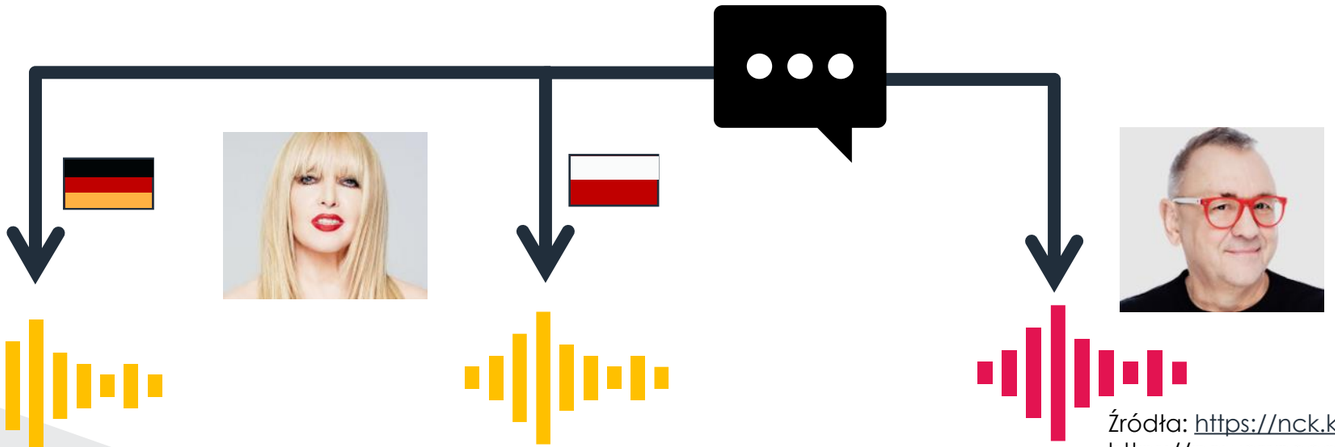
The Blue Lagoon is a 1980 American romance and adventure film directed by Randall Cleiser.

Źródła:
deepmind.com/blog/wavenet-a-generative-model-for-raw-audio
https://elevenlabs.io/
https://github.com/suno-ai/bark

Czym jest deepfake?

text-to-speech



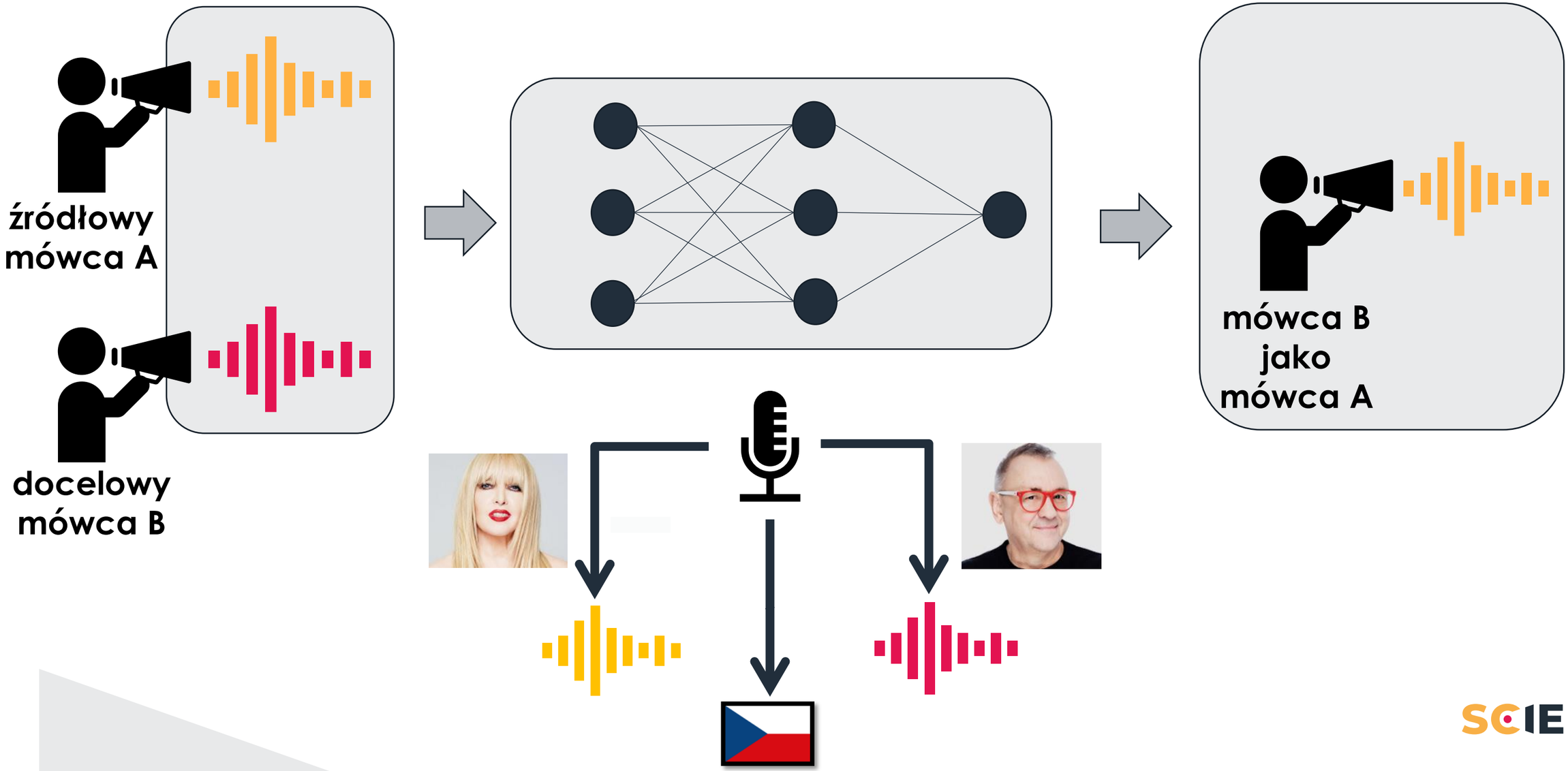


Źródła: https://nck.krakow.pl/maryla-rodowicz-akustycznie/
https://powerspeech.pl/wp-content/uploads/2020/03/J_OWSIAK-4.png.webp

SCIENCE NASK

Czym jest deepfake?

speech-to-speech



Ile minut głosu wystarczy aby stworzyć DeepFake?

text-to-speech **1 minuta**

speech-to-speech **7 minut**

Źródło: https://archive.factordaily.com/ai-based-voice-cloning-deepsync/

Czy DEEPFAKE'i są idealne?

Syntetyczny chaos

Na co warto zwrócić uwagę w głosie?

- nienaturalne pauzy
- nietypowe intonacje, zmiana głosu lub akcentu w trakcie wypowiedzi, nagłe zmiany tonu, wysokości dźwięku
- dziwna wymowa słów
- nietypowy styl mówienia dla danej osoby: ton czy tempo mowy, sposób wymowy
- brak naturalnych odgłosów tła lub niespójne hałas w tle
- „cyfrowe chrząszcze”

Źródło: https://archive.factordaily.com/ai-based-voice-cloning-deepsync/

tiktok.com/@deeptomcruise

tiktok.com/@deeptomcruise

tiktok.com/@deeptomcruise

tiktok.com/@deeptomcruise

Na co jeszcze warto zwrócić uwagę?

- **Artefakty przy obrocie głowy**

SCIENCE
NASK

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- **Niezgodność ruchu warg z mową**

Na co jeszcze warto zwrócić uwagę?

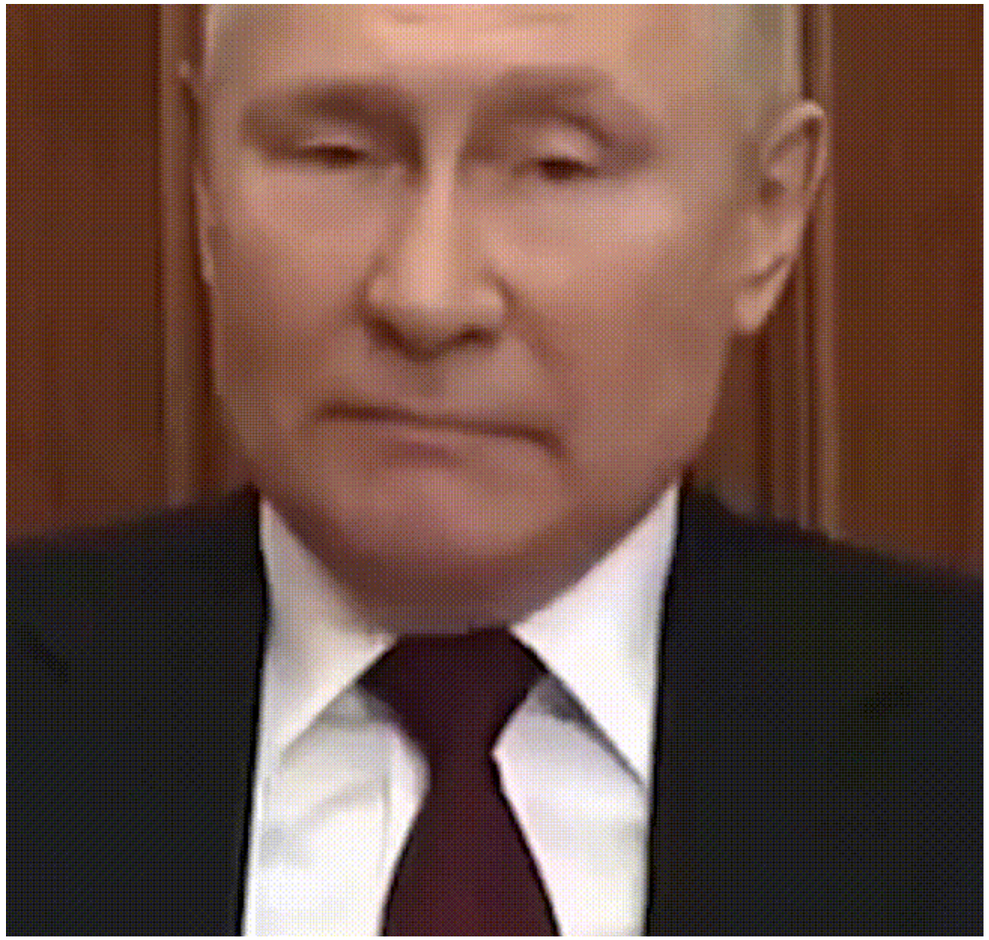
- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- **Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby**

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- **Mruganie**

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- Mruganie
- **Zmiany w geometrii twarzy**



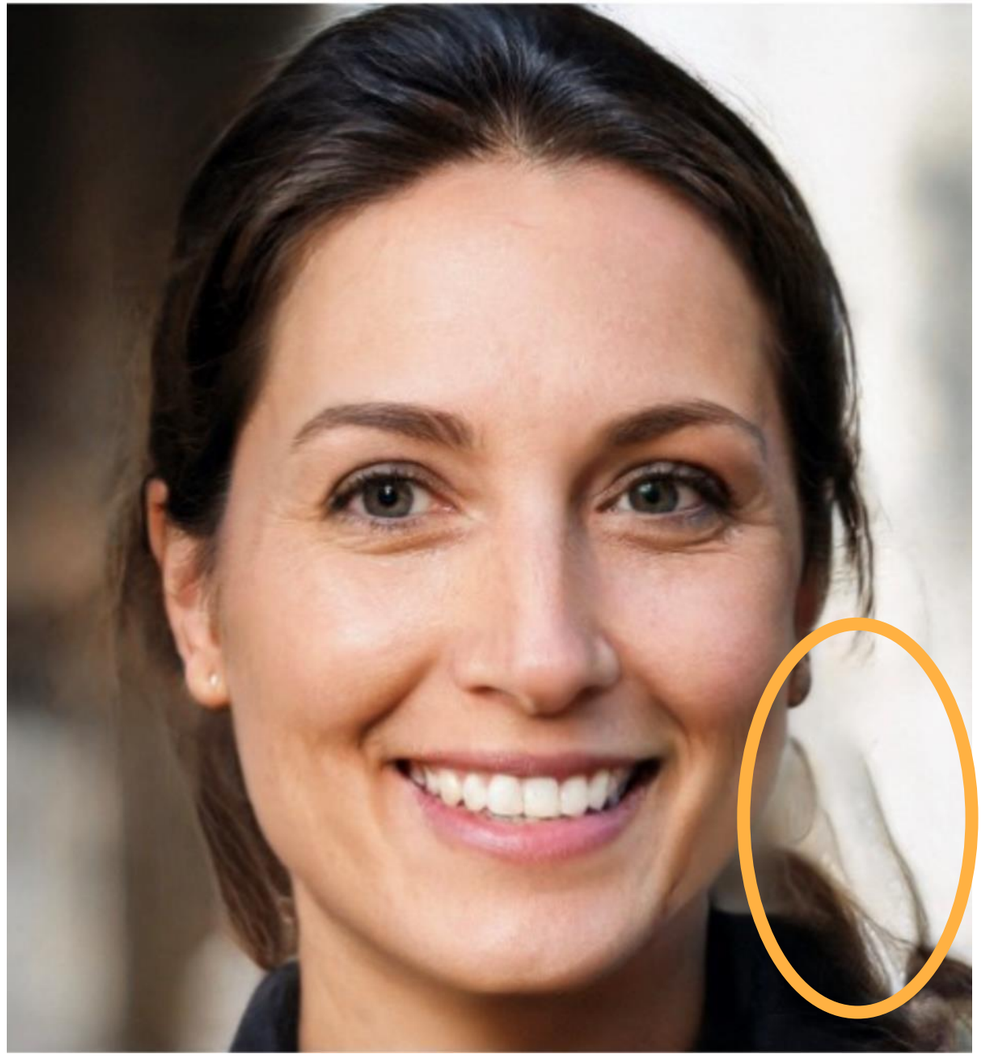
SCIENCE
NASK

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- Mruganie
- Zmiany w geometrii twarzy
- **Zgodność emocji w głosie, na twarzy i w zachowaniu**

Na co jeszcze warto zwrócić uwagę?

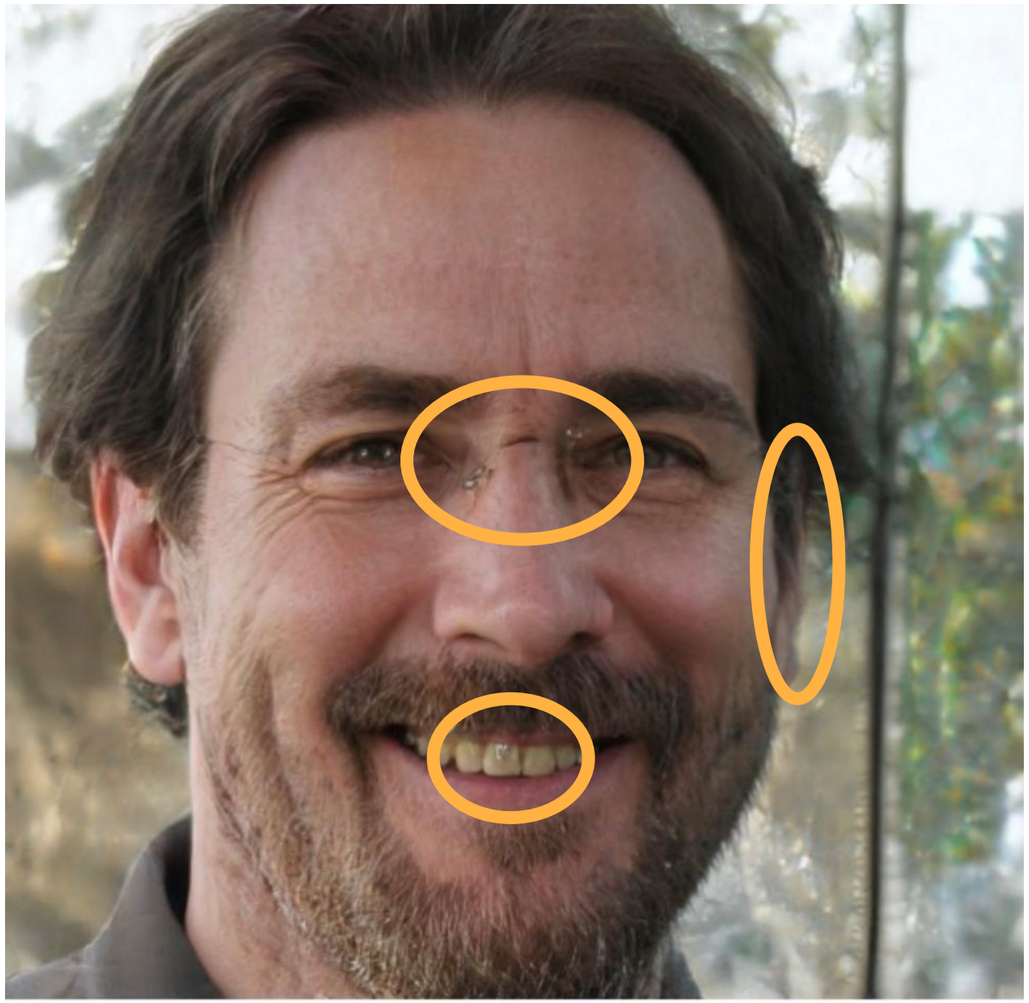
- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- Mruganie
- Zmiany w geometrii twarzy
- Zgodność emocji w głosie, na twarzy i w zachowaniu
- **Odpadające włosy**



SCIENCE
NASK

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- Mruganie
- Zmiany w geometrii twarzy
- Zgodność emocji w głosie, na twarzy i w zachowaniu
- Odpadające włosy
- **Błędy generacji**



SCIENCE
NASK

Na co jeszcze warto zwrócić uwagę?

- Artefakty przy obrocie głowy
- Niezgodność ruchu warg z mową
- Rozmazania wyostrzenia wokół ust, brak lub rozmazane zęby
- Mruganie
- Zmiany w geometrii twarzy
- Zgodność emocji w głosie, na twarzy i w zachowaniu
- Odpadające włosy
- Błędy generacji
- **Niezgodność elementów i/lub tła**

SCIENCE
NASK

FINGERPRINTS

- ukryte cechy

This is likely AI

Free Research Preview. AI or Not may produce inaccurate results

CORRECT

Paste image URL here

AI OR NOT?

Drop your image anywhere or **upload** from your device

źródło: aiornot.com

This is likely

Human

Free Research Preview. AI or Not may produce inaccurate results

CORRECT

Paste image URL here

AI OR NOT?

Drop your image anywhere or **upload** from your device

źródło: aiornot.com

This is likely

Human

Free Research Preview. AI or Not may produce inaccurate results

CORRECT

Paste image URL here

AI OR NOT?

Drop your image anywhere or **upload** from your device

źródło: aiornot.com

Quiz

Sprawdźcie swoją wiedzę!

SCIENCE
NASK

Audio-zagadka

1

2

3

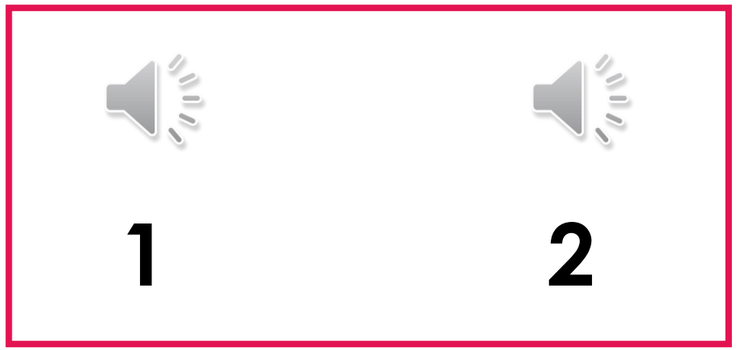
4

5

prawda

SCIENCE
NASK

Więcej zagadek



prawda

Instrukcja

Go to

www.menti.com

Enter the code

3632 3363

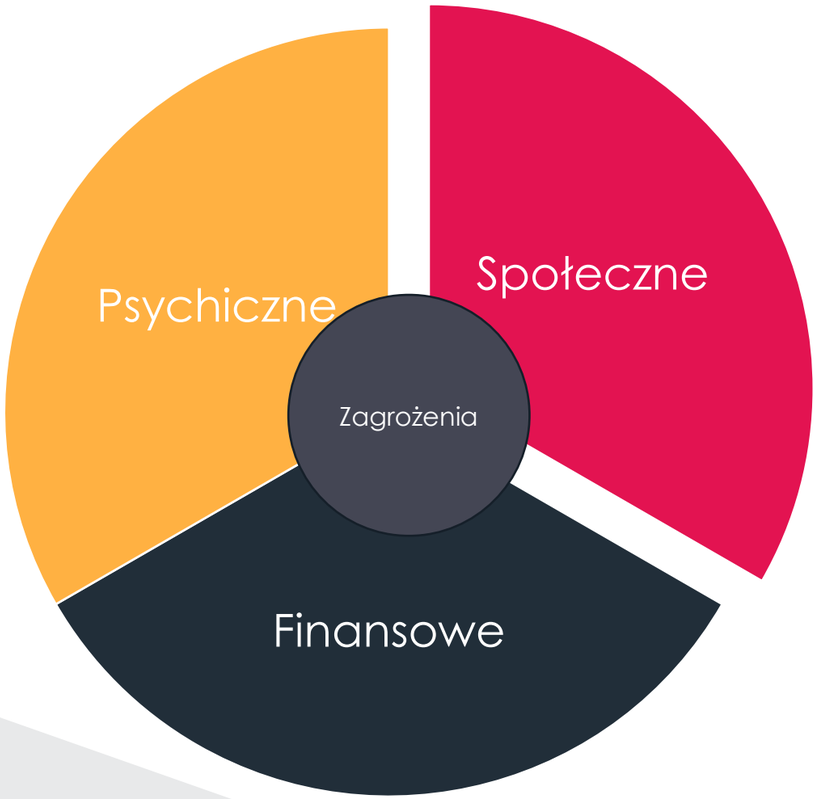
Or use QR code

SCIENCE
NASK

SCIENCE
NASK

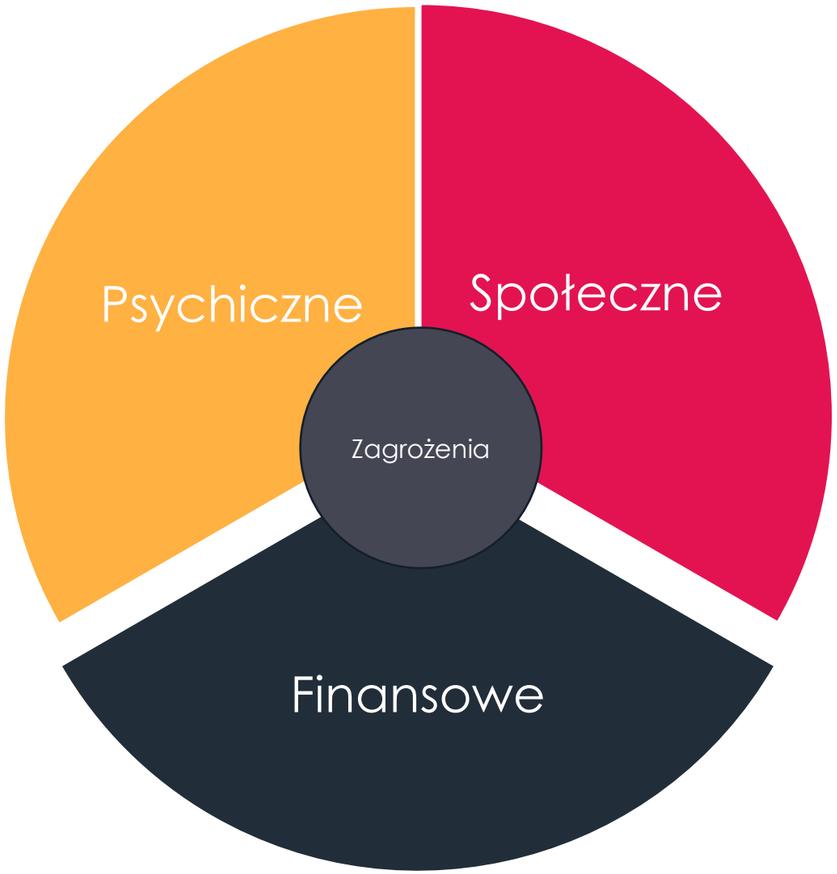
Skuteczne narzędzie

Niebezpieczne narzędzie



1. Szerzenie dezinformacji
2. Szkody dla instytucji publicznych
3. Zagrożenie dla demokracji
4. Osłabianie lub niszczenie stosunków międzynarodowych
5. Zachwianie bezpieczeństwa narodowego

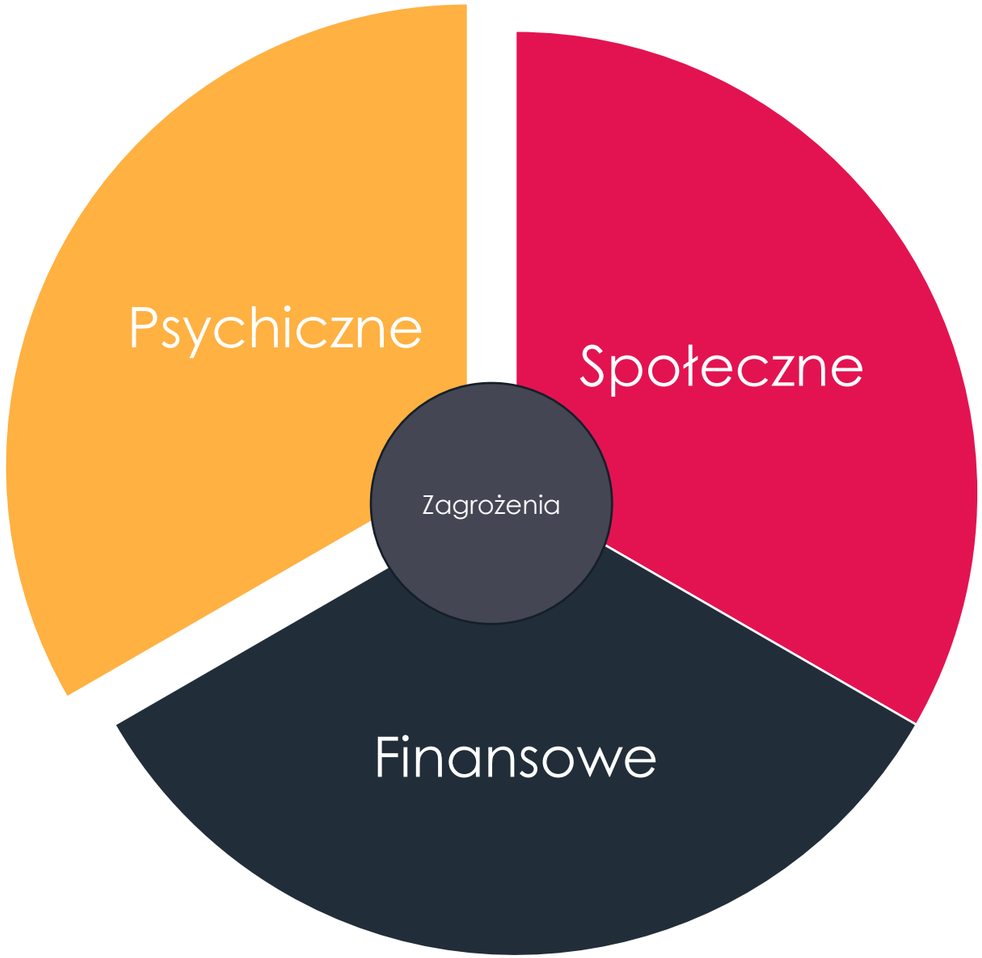
SCIENCE
NASK



1. Kradzież tożsamości
2. Oszustwa i wyłudzenia
3. Manipulacja cenami akcji
4. Uszkodzenie reputacji

SCIENCE
NASK

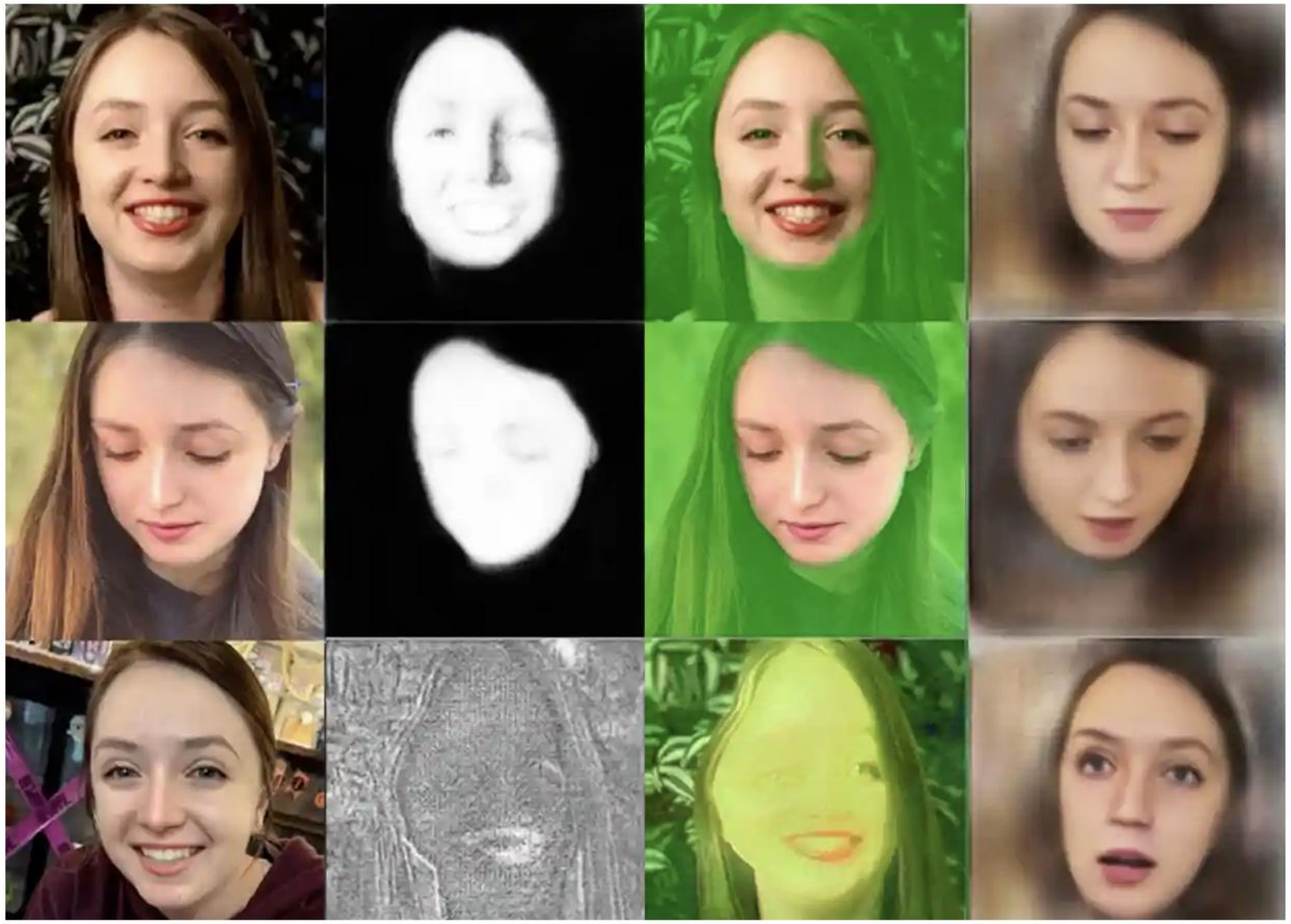
1. Zniesławienie
2. Podważanie zaufania
3. Zastraszanie



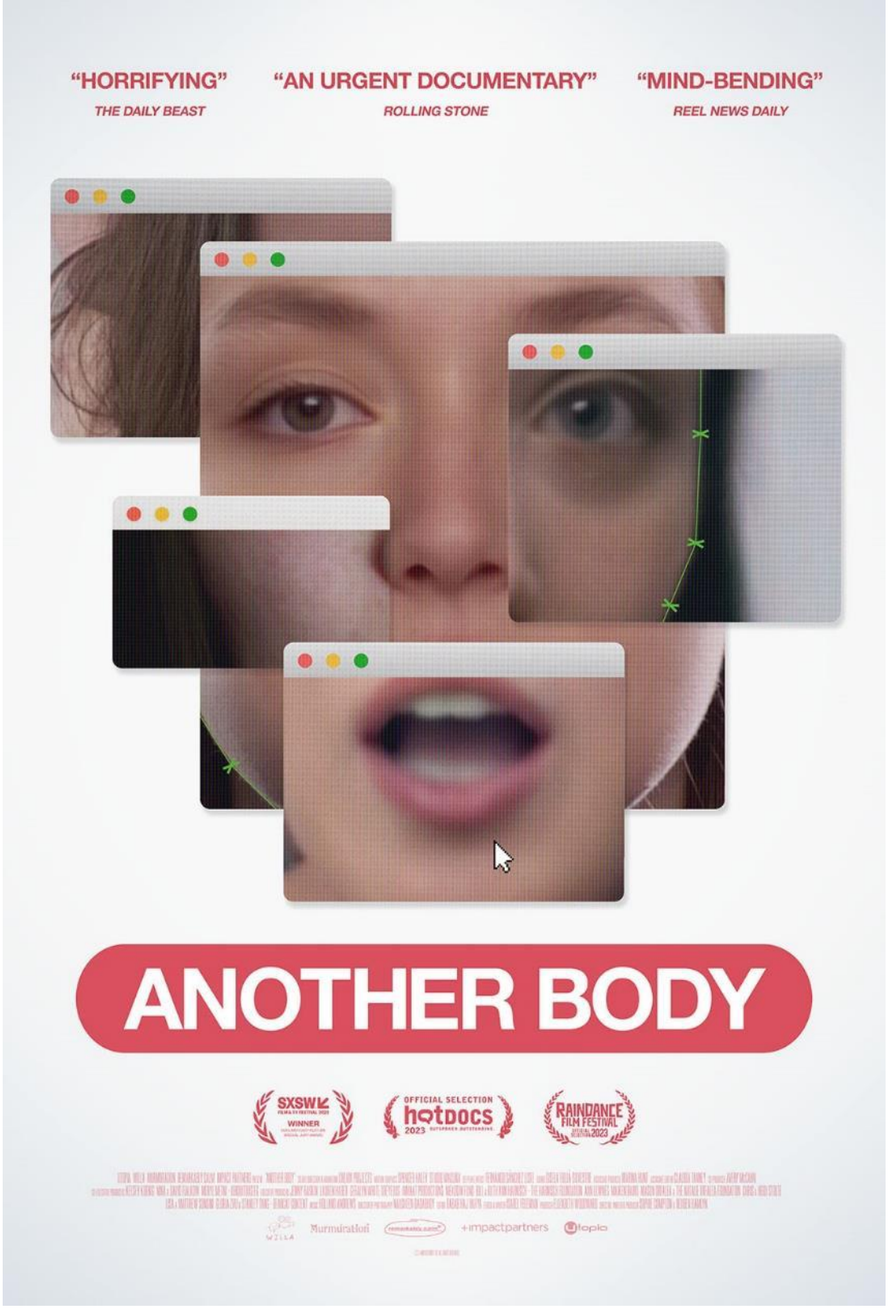
Another Body review – alarming deepfake pornography documentary

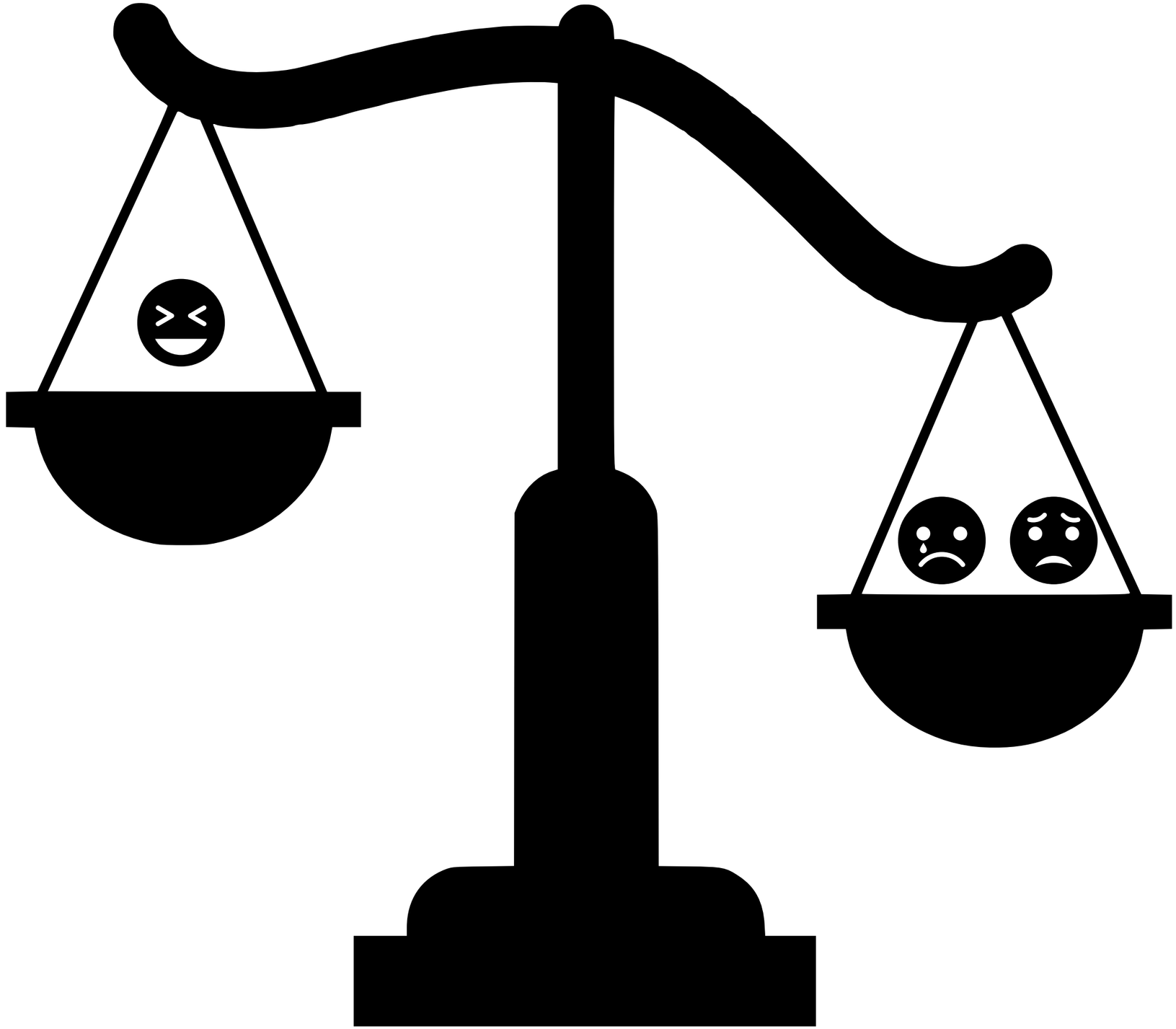
★★★☆☆

One woman strives to uncover the person misusing her image online in insufficiently probing look at a growing problem



'A story that is just beginning to unfold': Another Body.





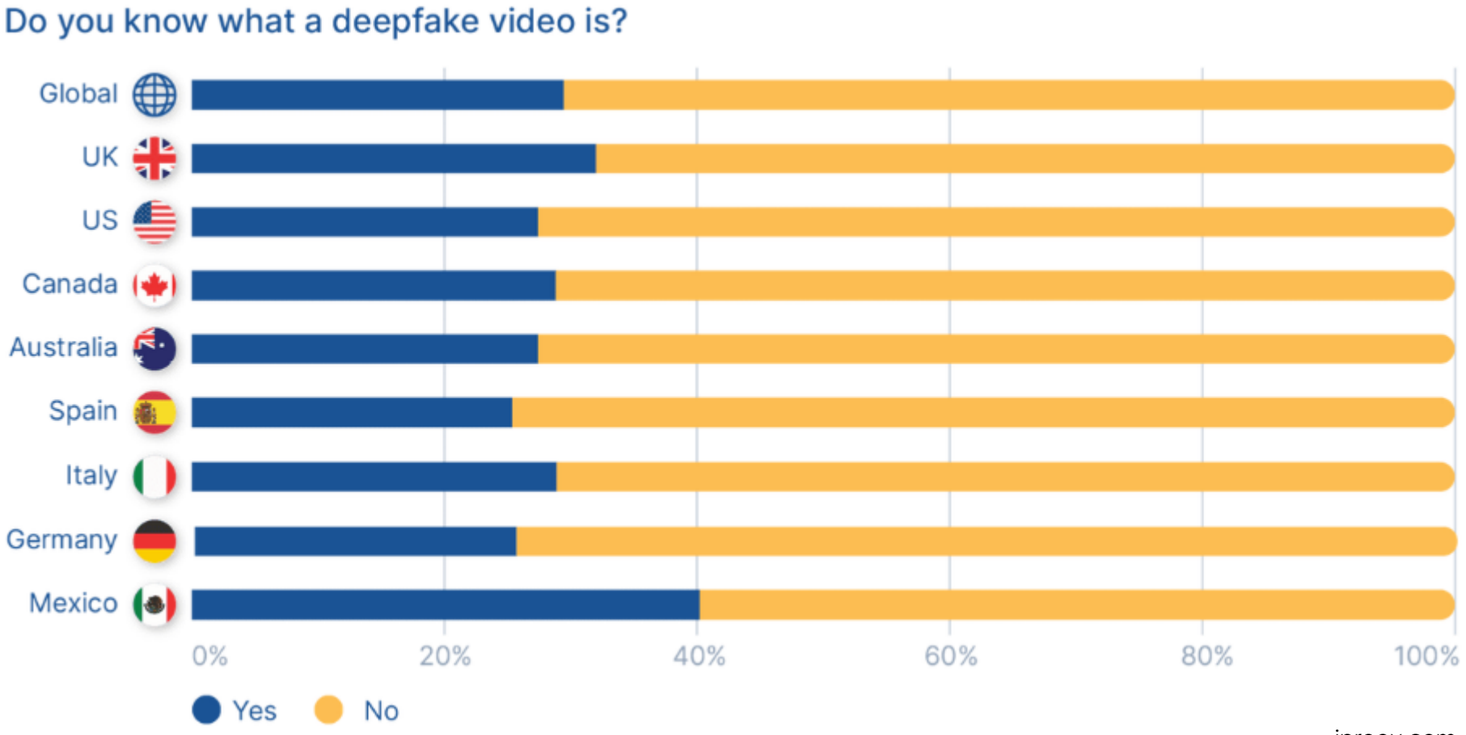
SCIENCE
NASK

Realne zagrożenie

Jak chronić się przed deepfake'ami?

Deepfake to złożony problem, który można zwalczać za pomocą kombinacji środków na różnych poziomach.

– Edukacja



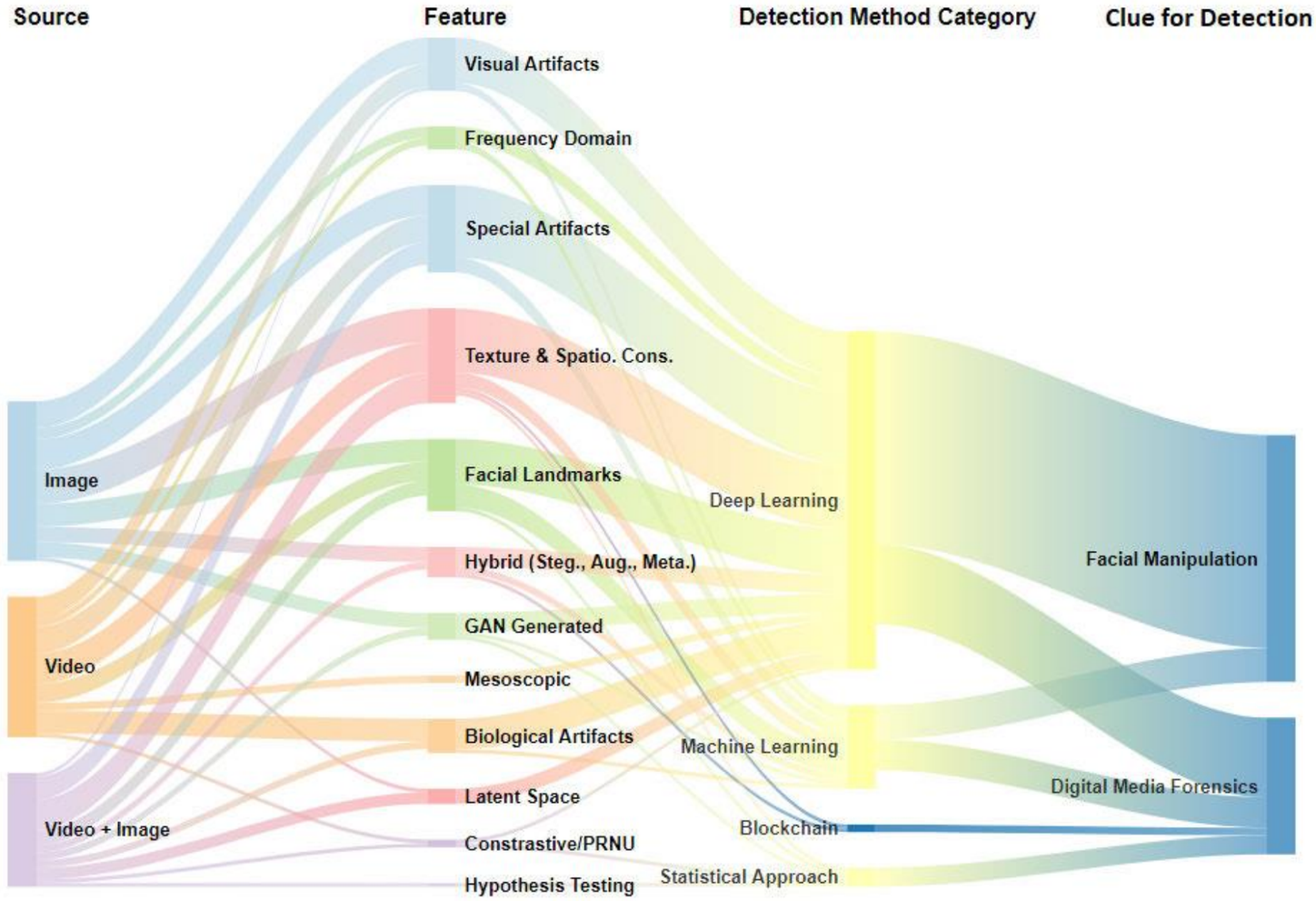
iproov.com

SCIENCE
NASK

Deepfake to złożony problem, który można zwalczać za pomocą kombinacji środków na różnych poziomach.

– Edukacja

– Metody wykrywania



Deepfake to złożony problem, który można zwalczać za pomocą kombinacji środków na różnych poziomach.

– Edukacja

– Metody wykrywania

– Regulacje prawne

Rada
Unii Europejskiej

Międzyinstytucjonalny numer referencyjny:
2021/0106(COD)

Bruksela, 25 listopada 2022 r.
(OR. en)

14954/22

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

SCIENCE
NASK

Gdy staniesz się celem ataku

Nie daj się oszukać!

- Myśl krytycznie
- Rozpoznaj manipulację
- Weryfikuj źródła informacji
- Edukuj dzieci i uświadom rodzinę i znajomych
- Poszerzaj swoją własną wiedzę

Gdy staniesz się celem ataku

Bądź sceptyczny gdy rozmówca prosi o pieniądze

Nie opieraj się na zapewnieniach o jego tożsamości

Rozłącz się i zadzwoń do faktycznej osoby

SCIENCE
NASK

WATCHDOG PRAVDA DEMAGOG CyberDefence 24

SPIDER'SWEB Nauka to lubię CRAZY NAUKA Instytut Zamenhofa

NASK #FakeHunter pap POLSKA AGENCJA PRASOWA

Kodeks dobrych praktyk

Wspólnie przeciw dezinformacji

SCIENCE NASK

Zapraszamy do kontaktu!

deepfake@nask.pl

SCIENCE
NASK

Dziękujemy za uwagę!

Obserwuj NAS(K)

/NASKpl

/NASK_pl

/nask

/nask.pl

/NASKPIB

nask.pl

SCIENCE
NASK