UNIVERZA V LJUBLJANI

FRI

Fakulteta za računalništvo in informatiko

Slikovna forenzika

dr. Borut Batagelj
sodni izvedenec

FORENZIČNO-KRIMINALISTIČNO TEHNIČNE PREISKAVE preiskave fotografij ter posnetkov video kamer (video nadzor)

Laboratorij za računalniški vid, UL-FRI
raz. področje: slikovna biometrija

26. marec 2024

Zakon o sodnih izvedencih, sodnih cenilcih in sodnih **tolmačih (ZSICT)**

2. člen (status)

(1) Sodni izvedenci so osebe, imenovane za neomejen čas s pravico in dolžnostjo, da sodišču na njegovo zahtevo podajo izvid in mnenje glede strokovnih vprašanj, za katera tako določa zakon ali glede katerih sodišče oceni, da mu je pri njihovi presoji potrebna pomoč strokovnjaka.

vir: http://www.pisrs.si

Strokovna **vprašanj**a

- Ali se na posnetkih pojavljajo iste osebe?
- Ali se na posnetku nahaja obdolženi?
  - obrazne karakteristike
  - poškodbe
  - višina
  - dolžina obuvala

- Analiza gibanja sumljive osebe.
- Izboljšava zaseženega videoposnetka.
- Ali so posnetki/fotografije pristne?
  - določiti, potrditi snamalno napravo
  - določiti čas nastanka

Pristnost posnetkov

- Obdani z vizualnimi podobami
- Zaupanje: nekoč in danes
  - Rumeni tisk, modna industrija, mediji
  - Znanstvene revije
  - Politična propaganda
  - Ponarejanje dokazov na sodišču
  - Različne slikovne potegavščine (email)

- Ponarejanje je dandanes enostavno
  - Razširjenost digitalnih kamer
  - Dostopnost do programske opreme za manipulacijo
- Naloga digitalne forenzike: Povrniti zaupanje

Globoki ponaredki

You Won’t Believe What Obama Says In This Video!

Metode za odkrivanje ponaredkov

- Aktivne metode
  - Vodni žig
  - Digitalni podpis
  - CAI in C2PA

- Pasivne metode
  - Ni vidnih sprememb
  - Spremeni se notranja statistika podatkov
    - Klasične metode
    - Metode na osnovi globokega učenje

Pasivne metode

1. Na nivoju slikovnega elementa
2. Na nivoju formata (izgubno stiskanje)
3. Lastnosti kamere: leče, senzor, obdelava na čipu
4. Fizikalne lastnosti (objekt-osvetlitev-kamera)
5. Geometrijske lastnosti (fotogrametrija)

Hany Farid, Image Forgery Detection, A survey

Na nivoju slikovnega elementa

- Druge analize
  - identifikacija : DNK, prstni odtis, obraz
  - odontologija : zobovje
  - entomologija = nauk o žuželkah : insekti
  - geologija : prst, zemlja

- Digitalna računalniška forenzika: bit

- Forenzična analiza slik: slikovni element

Na nivoju slikovnega elementa

Kloniranje

- Ponovitev dela slike
  - Pretiravanje, zavajanje
  - Prekrivanje osebe ali objekta
- Računska kompleksnost
  - rešitev: DCT ali PCA s podobnimi koeficienti

Objavljena slika

Originalna slika

Na nivoju slikovnega elementa

Ponovno vzorčenje

- Nova kompozicija
  - Del slike povečamo/zmanjšamo, zasukamo
    - Ponovno vzorčenje => korelacija sosednih elementov

Na nivoju slikovnega elementa

Ponovno vzorčenje

- Nova kompozicija
  - Del slike povečamo/zmanjšamo, zasukamo
    - Ponovno vzorčenje => korelacija sosednih elementov

Na nivoju slikovnega elementa

Spajanje

- Dve ali več slik v eno
- Spremembe na robu vizualno niso opazne
- Spremenijo pa se Fourierove statistike višjega reda

Oprah

v telesu Ann Margret

Na nivoju slikovnega elementa

Statistika

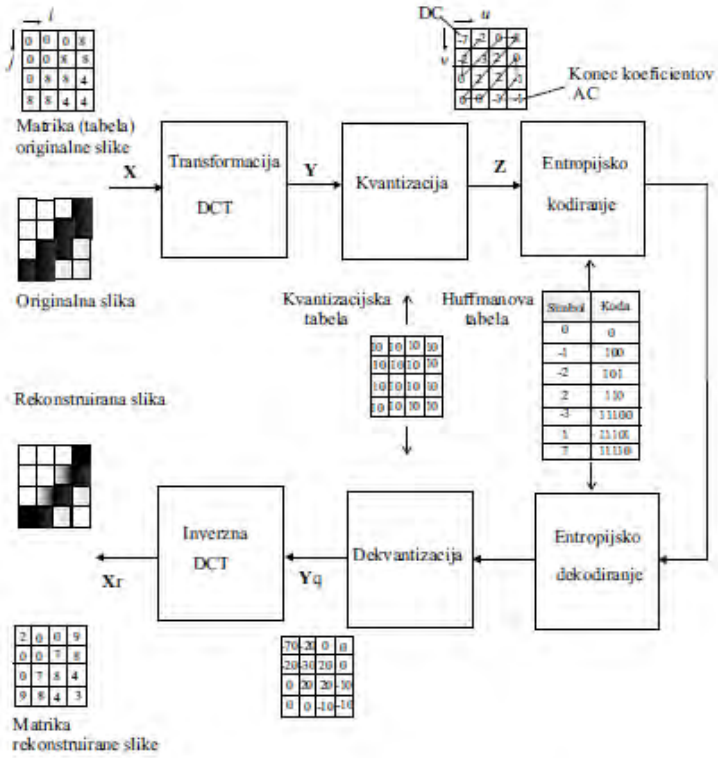
- Veliko kombinacij slik: $256^{n*n,}$ $n=10 \approx 10^{240}$
- Zelo malo takšnih, ki imajo nek pomen
- Fotografije sledijo določenim statistikam
  - Izračunane statistike => ali je bila slika spremenjena
    - Lahko se ugotovi
      - povečavo, filtriranje
      - pravo fotografijo ali rač. generirano
      - skrita sporočila (steganografija)

Na osnovi formata

- Prvo pravilo forenzične analize
  - Ohraniti dokaze
- Ali je izgubni format JPEG težava?

- Lastnosti JPEG se lahko uporabi za forenzično analizo:
  - Kvantizacija
  - Dvojna kompresija
  - Nivojska analiza napake
  - JPEG bloki

Na osnovi formata
JPEG Kvantizacija



- Shema stiskanja na nivoju fotoaparata
- Določimo izvorno napravo
- Razlike znotraj ene kamere (nastavitve)
- Prekrivanje med različnimi kamerami

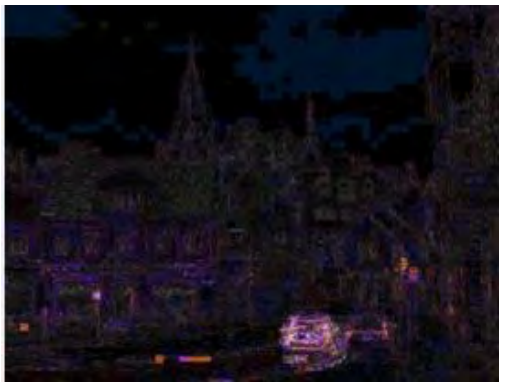
= digitalna slikovna balistika

➡ izvor slike lahko potrdimo ali ovržemo

Na osnovi formata
Dvojni JPEG

- Manipulacija -> ponovno shranjevanje
  - original v JPG
  - sprememba v JPG
- Dvojna kompresija dodanih delov
  - Nepravilnosti pri izgubnem stiskanju
  - Služi za dokaz manipulacije

- Na celotni sliki ne more dokazati zlonamerne spremembe
  - sliko smo lahko samo ponovno shranili

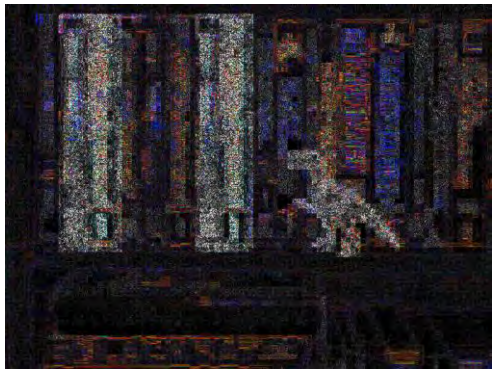


Dvojna kompresija na delu slike!

Na osnovi formata

Nivojska analiza napake

- Zaznamo dele na sliki, ki imajo različno kompresijo
  - Podobne površine imajo isto stopnjo kvalitete
  - Nov del ima drugačno stopnjo kvalitete
  - Različne dele vidimo predstavljene z nivoji svetlosti
  - Predmeti ki so bili dodani zadnji so svetlejši



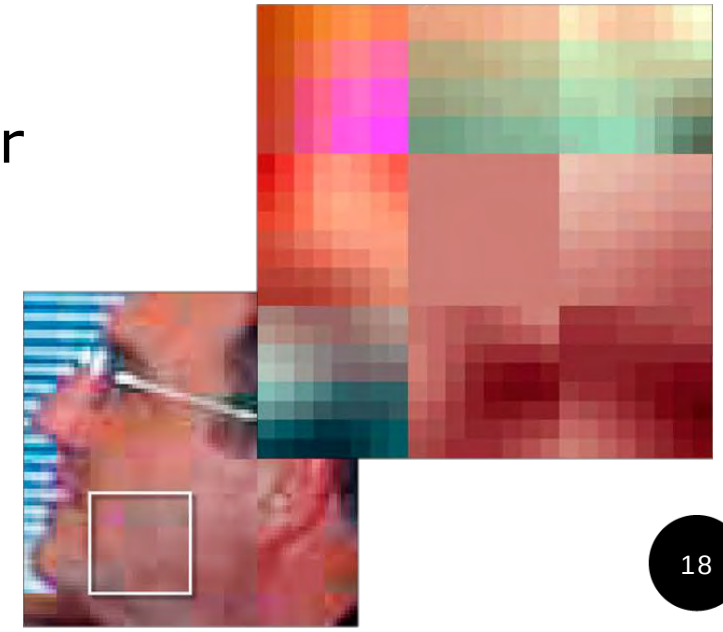
Error level analysis - ELA

Na osnovi formata

JPEG bloki

- Osnova JPEG kompresije so DCT bloki
- Obdelava (transformacija+kvantizacija) se vrši na blokih velikosti 8×8
- Na robovih blokov nastane popačenje
- Če sliko spremenimo se to pozna na robnih točkah

- Izračuna se lastnosti iz delov kjer ni popačenja
  => določitev spremenjenih regij



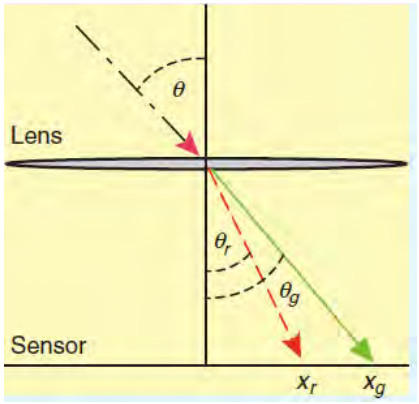
Na osnovi kamere

- Utori na izstrelku
  - povezava z orožjem

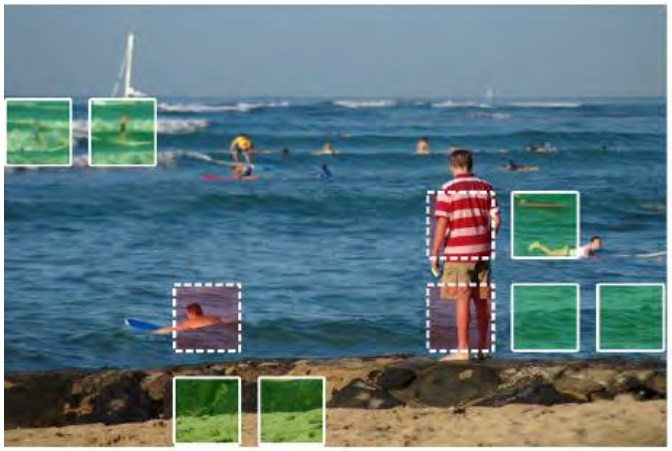
- Lastnosti kamere se odražajo na slikah
  - Kromatična aberacija
  - Barvna matrika
  - Odziv kamere
  - Šum senzorja

Na osnovi kamere

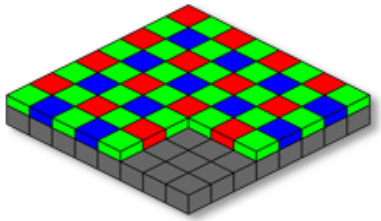
Kromatična aberacija



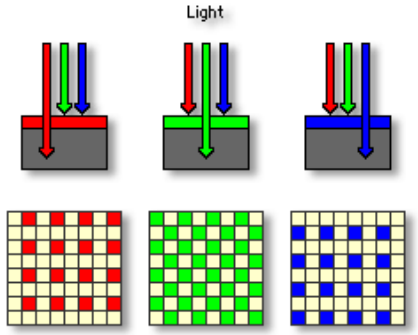
- Lom svetlobe različnih valovnih dolžin
- Primerjava barvnih kanalov
  - Vektor odmikov R in G kanala



Na osnovi kamere
Barvna matrika

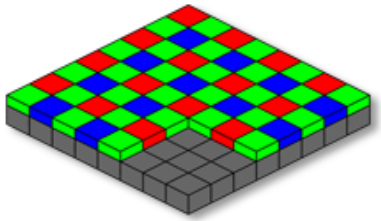


Color Filter Array Sensor

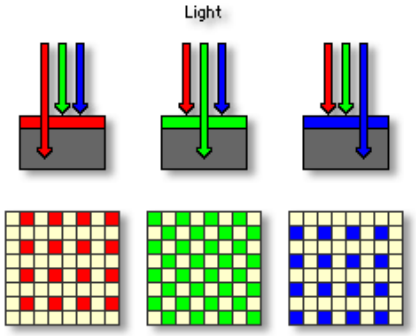


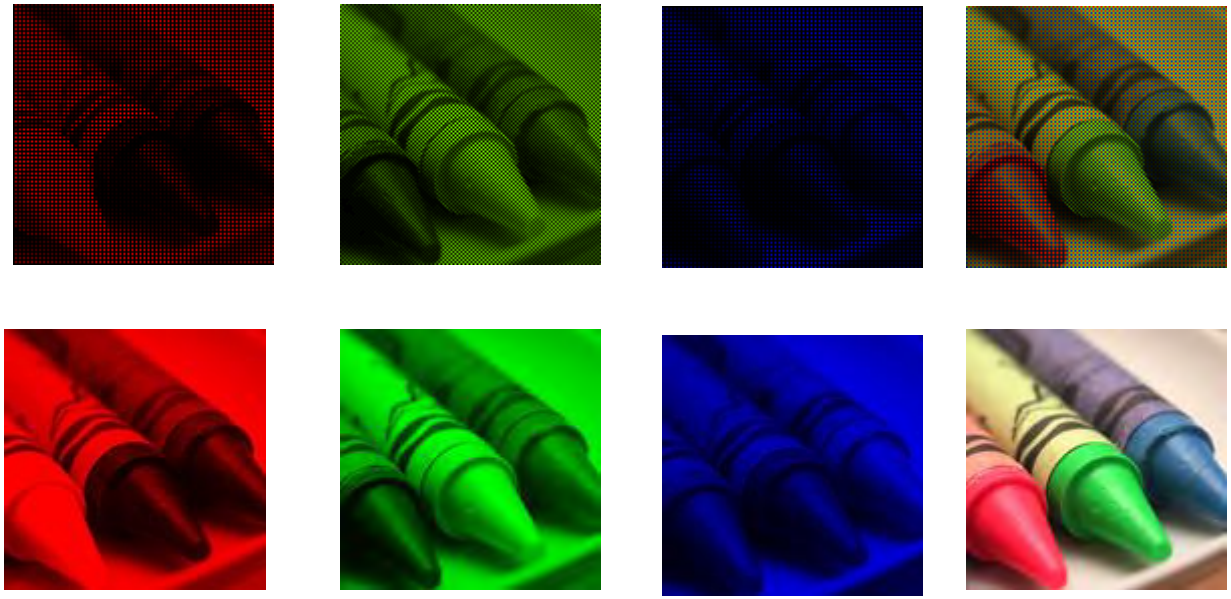
- Barvna slika: 3 barvni kanali RGB
- En svetlobni senzor: različne barve s pomočjo barvnega filtra (CFA)
- Vsak slikovni element senzorja svoj filter
  - Za vsak slik. element ena barva
  - Ostali dve se izračunata s pomočjo interpolacije (demozaičenje)
- Interpolacija pusti na sliki sled
  - Statistična odvisnost v vsakem barvnem kanalu
  - Filter se ponavlja -> vzorec je ponavljajoč
  - Odstopanje od vzorca ➡ sprememba

Na osnovi kamere
Barvna matrika



Color Filter Array Sensor



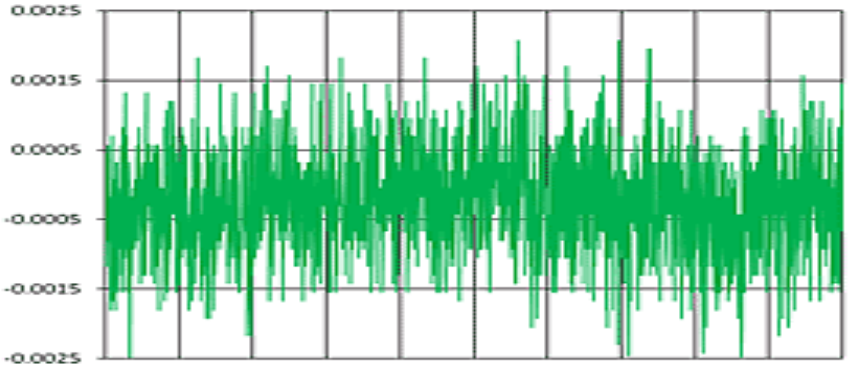


Na osnovi kamere

Odziv kamere

- Senzorji so večinoma linearni
  - Odvisnost med količino svetlobe in vrednost pripadajočega slik. elementa = linearna
- Nelinearni filter za izboljšanje slike
  - Vseeno se ohrani odvisnost
- Izračun odzivne funkcije
  - Preiskovanje po sliki
  - Odziv odstopa ➡ spremembe

Na osnovi kamere
Šum senzorja



- Slika na sezorju
- Obdelave:
  - Kvantizacija
  - Belina
  - Interpolacija
  - Barvna korekcija
  - Gama korekcija
  - Filtriranje
  - JPEG stiskanje

Vse to pusti določeno sled
- je bila slika obdelana
- iz katere naprave

Fizika

- Dve slavni osebi se sprehajata po plaži
- Lahko, da se osebi sploh ne poznata
  - Izrezane in dodane v okolje
- Težko je zagotoviti svetlobnim pogojem
  - Enake za obe osebi
  - Skladne z okoljem

April, 2005

- Tehnike
  - Usmerjenost svetlobe (2D, 3D)
  - Osvetlitev prostora

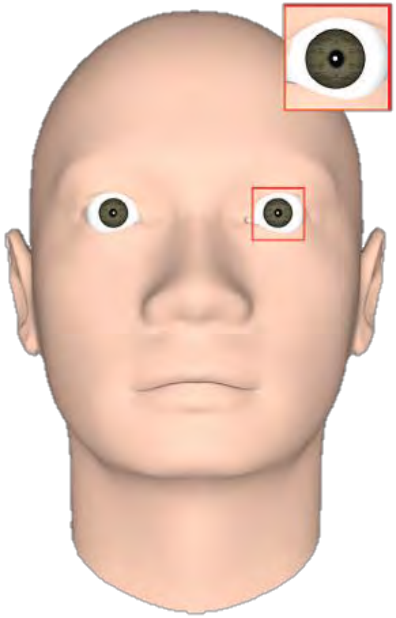
Fizika

Usmerjenost svetlobe (2D)

- Osvetlitev obraza iz desne
- Količina svetlobe
  - Normala na površino
  - Smer svetlobe
- določitev izvora svetlobe v 3D
  - potrebujemo 3 normale
  - iz ene slike zelo težko
- Omejimo se samo na 2D
  - Še vedno uporabno za forenzične raziskave
    - Za različne objekte in ljudi preverimo, če je osvetlitev konstantna

Fizika

Usmerjenost svetlobe (3D)



– Pomagamo si z odbojem v očeh
  • Primerjamo za različne ljudi

Fizika

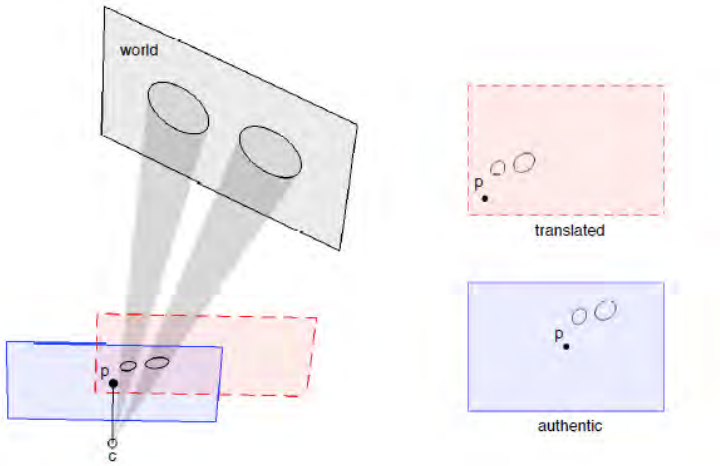
Osvetlitev prostora

- V prejšnih primerih
  - Predpostavka da imamo en izvor
- V praksi
  - Različne osvetlitve
  - Različne pozicije

- Potrebujemo najmanj 9 normal iz površine

Fotogrametrija

- Verodostojne slike
  - Izhodiščna točka = center kamere se projecira blizu centra slike
- Premaknemo objekt/osebo
  - Premakne se tudi izhodiščna točka => slika je bila spremenjena



Fotogrametrija

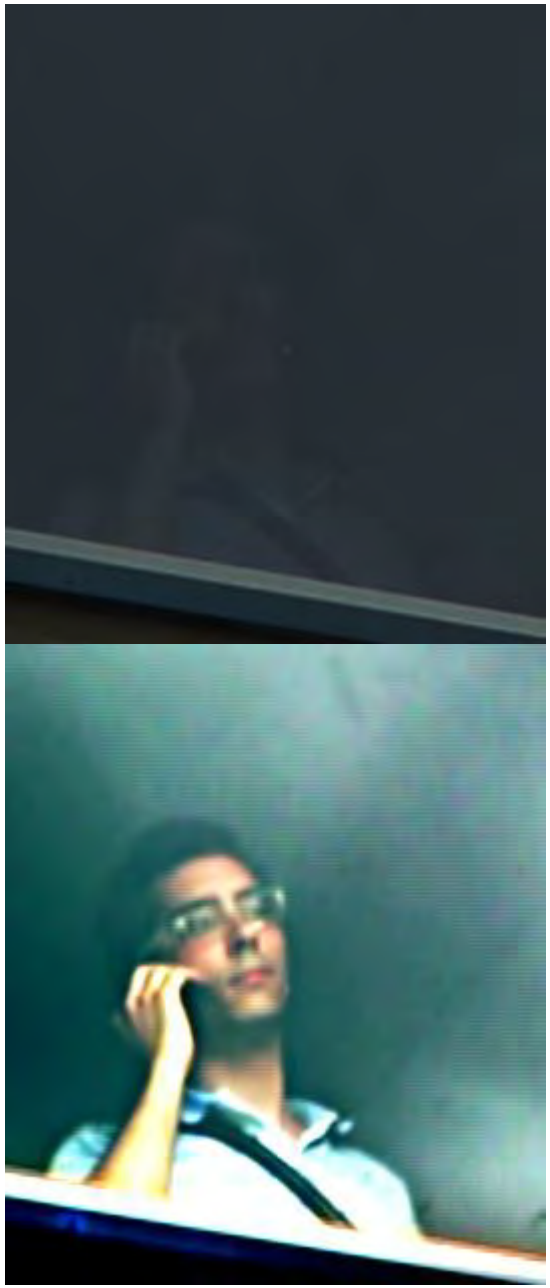
- Transformacija slike
  - Meritve


  - Razberemo oznako/besedilo


Ocena višine (SVM)

Druge tehnike

1. Posvetlitev (nočni posnetki)
2. Povečava kontrasta
3. Odstranitev šuma
4. Stabilizacija videa
5. Popravek premika
6. Razvijanje 360 posnetka
7. Korekcija napak leč



AMPED SOFTWARE http://ampedsoftware.com/

Globoki ponaredki

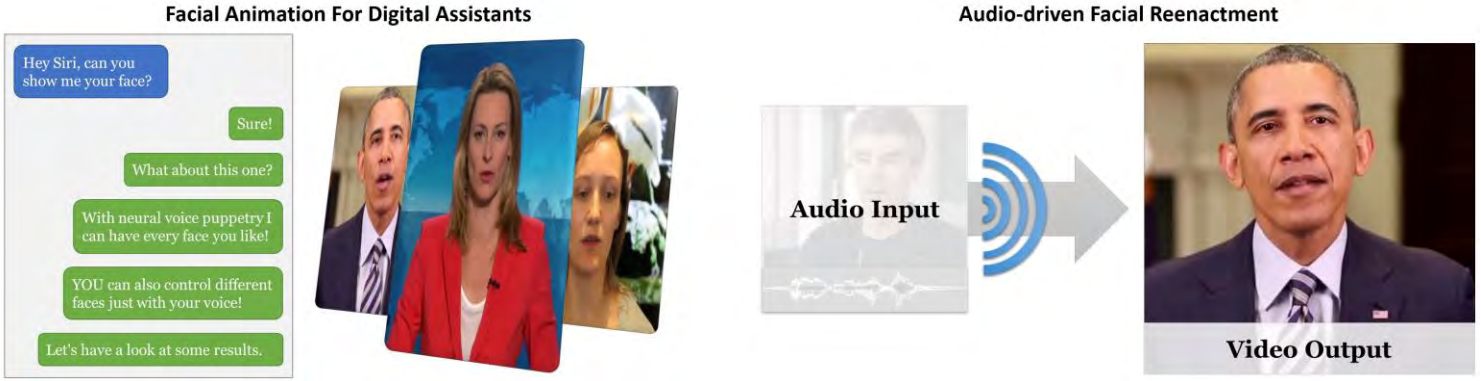
Face2Face: Real-time Face Capture and Reenactment of RGB Videos

Manipulacija - govor

[#VoCo. Adobe MAX 2016 (Sneak Peeks) | Adobe Creative Cloud]

Neural Voice Puppetry

- audio-driven facial video synthesis
- Cilj: prilagoditev videa za dani zvočni vhod
  - NVIDIA: Omniverse Audio2Face



https://www.youtube.com/watch?v=9L6gbDRMMxw

Manipulacija - video

Porast globokih ponaredkov (DeepFakes)

Ideja ni nova.

1997 2014 2015 2016 2017 2018 2019 2020 2021

Video rewrite: Driving visual speech with audio" SIGGRAPH (1997)

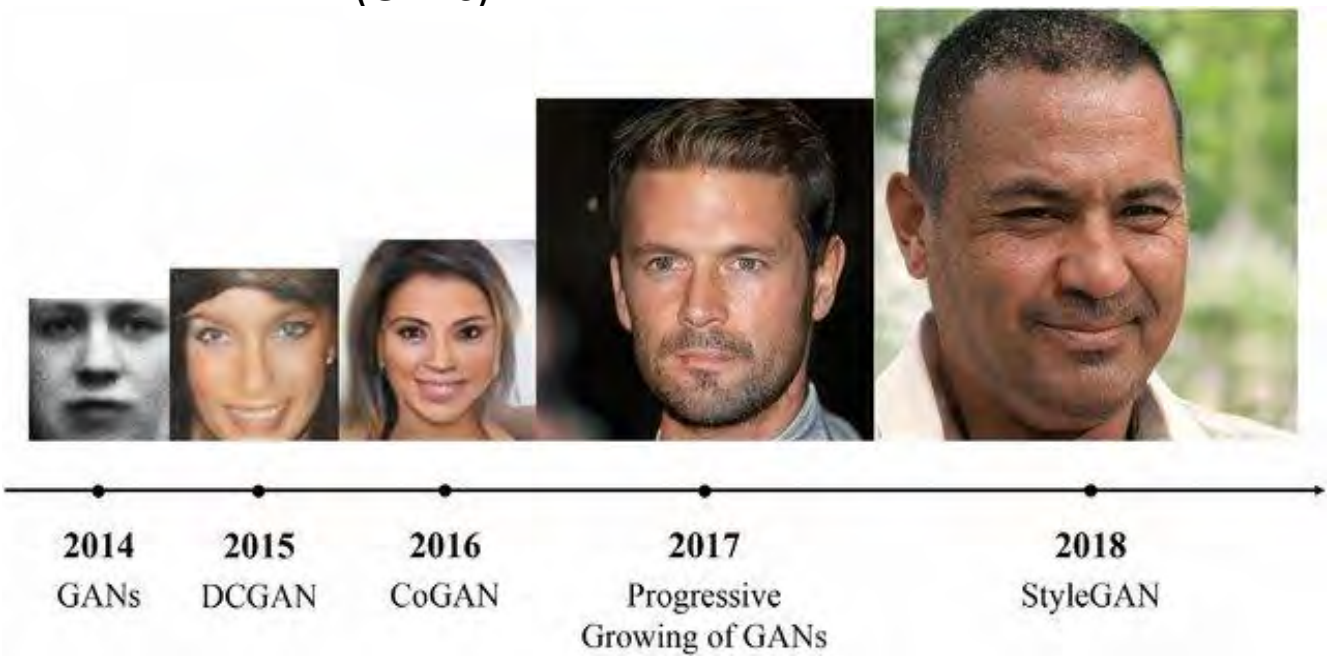
Nvidia, "Unsupervised image-to-image translation", NIPS (2017)

November 2017: Reddit user named **deepfakes** started sharing face-swapping pornographic videos

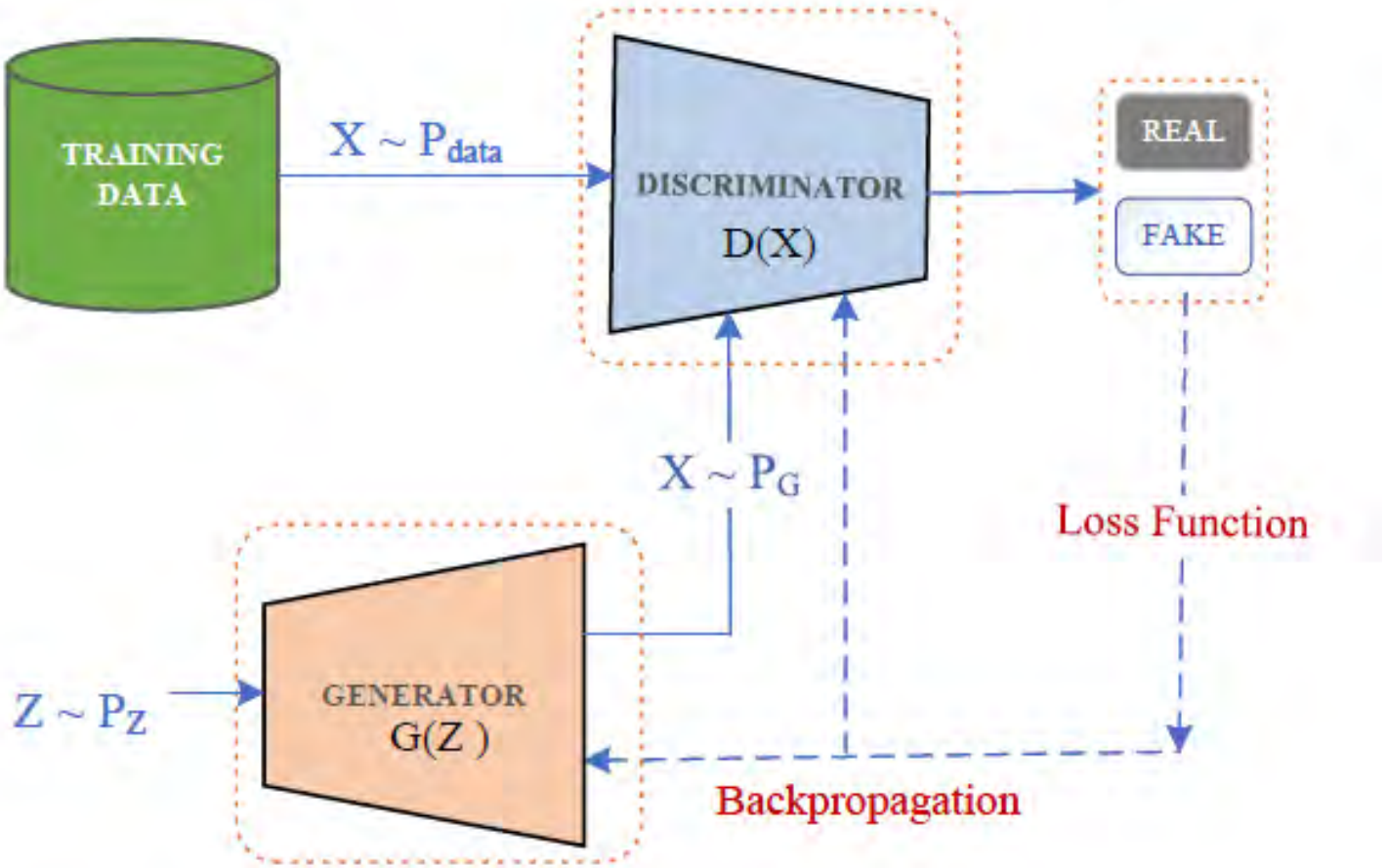
Porast globokih ponaredkov (DeepFakes)

1997 2014 2015 2016 2017 2018 2019 2020 2021

Goodfellow et. al.,
"Generative ***Adversarial*** Networks
" (GANs)



GAN


TRAINING DATA
X ~ P_data
DISCRIMINATOR
D(X)
REAL
FAKE
X ~ P_G
Loss Function
Z ~ P_Z
GENERATOR
G(Z)
Backpropagation

Hitro širjenje

4 pomembi faktorji:

1. Socialna omrežja/platforme

   Facebook, instagram, twitter, youtube, snapchat, LinkedIn, pinterest, tiktok, WeChat

2. Procesorska moč : GPU

   Omogoča poganjanje zapletenih algoritmov na katerih slonijo AI metode

3. Tehnologija globokega učenja

   Učenje s pomočjo globokih konvolucijskih mrež

4. Prosto dostopna programska oprema na odprtih platformah: GitHub

   FaceSwap, FAKEAPP, ZAO

Metode za manipulacijo obraza

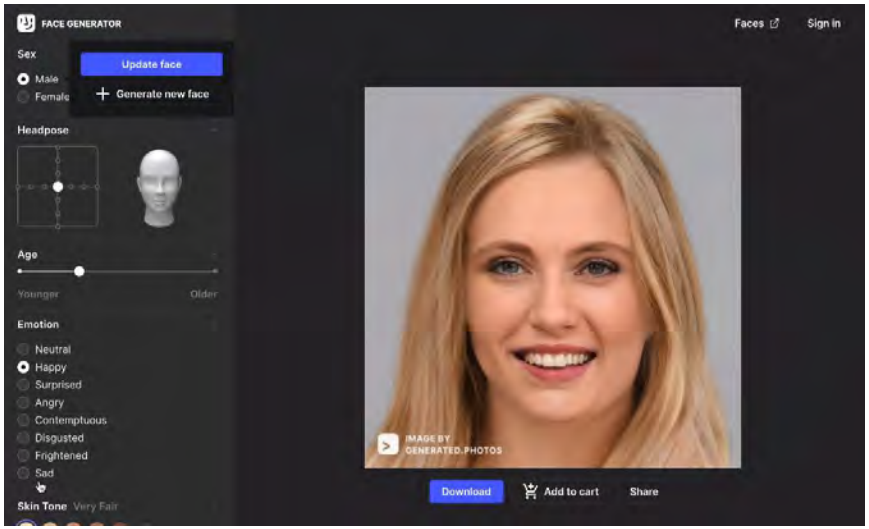
- Generiranje novega obraza
- Zamenjava identitete
- Manipulacija določenih atributov
- Zamenjava izraza (ustnice)
- Druge manipulacije

Generiranje novega obraza

- https://thispersondoesnotexist.com/
- https://generated.photos/face-generator

Uporabnost:
- 3D modeliranje (igre)
- Filmska industrija

Nevarnosti:
- lažni profil na soc. omrežjih
  - Letno odkrijejo več tisoč lažnih računov.



Zamanjava identitete

- S pomočjo rač. grafike
- S pomočjo globokih nevronskih modelov

Izvorna slika: identiteta ponorna slika: atributi Generirana slika

Uporabnost:
- Zabavna industrija
- Filmska industrija

Nevarnosti:
- Lažni pornografski posnetki
- goljufije

Y. Zhu, Q. Li, J.Wang, C.-Z. Xu, and Z. Sun, “One shot face swapping on megapixels,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2021, pp. 4834–4844.

For fun

Nicolas Cage DeepFake

Tom Cruise Deepfake

AGT 2022 by [Metaphysic](https://www.youtube.com/watch?v=mPU0WNUzsBo)
(https://www.youtube.com/watch?v=mPU0WNUzsBo)

America's Got Talent Semi-Finals
https://www.youtube.com/watch?v=mJeE9BNEa-o

My attempt

Let's bite the science

Replacing the face of Nataša Ivanuš Čuček [left] with that of the presenter Renata Dacinger.

Manipulacija določenih atributov

- Sprememba frizure, barva kože, spola, starosti

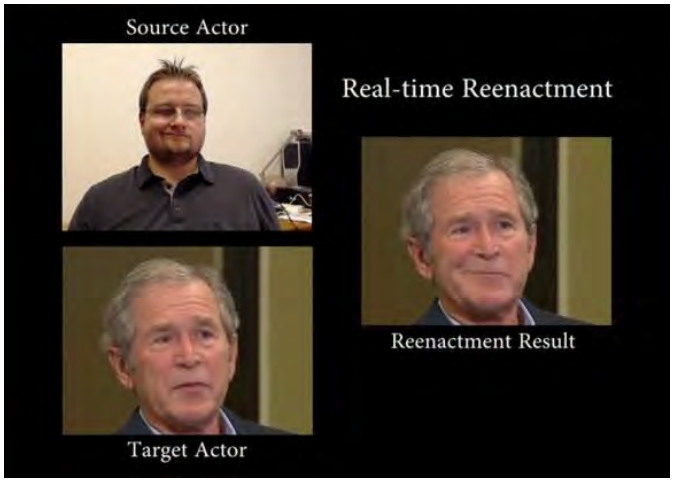
Mobilna aplikacija:
FaceApp

Uporabnost:
- Virtualno okolje
  - Preizkus modnih dodatkov
  - Ličila
  - Kozmetika
  - Pričeska

Zamenjava izraza (ustnice)

- Rekonstrukcija obraza

- Tehnike:
  - Face2Face
  - Neural Textures

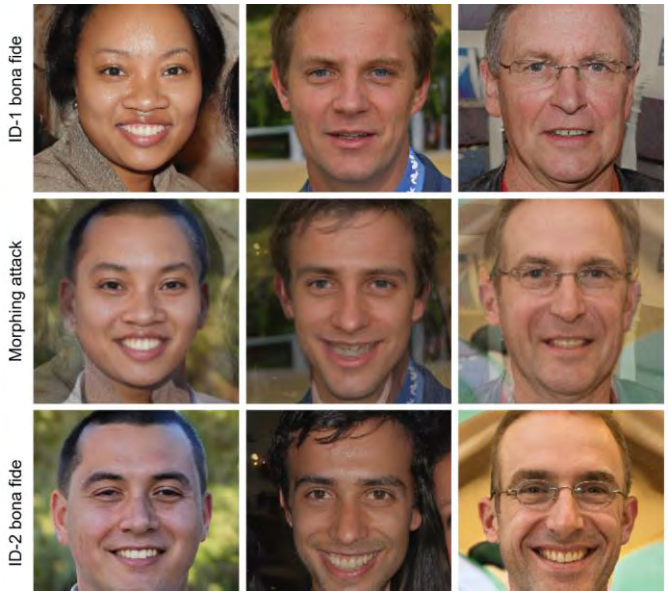


https://www.youtube.com/watch?v=ohmajJTcpNk

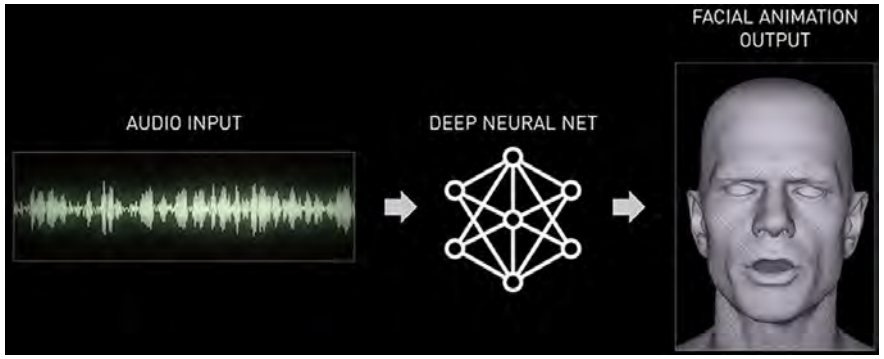
Goljufija
- Nekdo reče kar ni rekel

Druge manipulacije

- Preoblikovanje obraza (morphing)
  - Ustvarjanje umetnih biometričnih vzorcev obraza
- Anonimizacija (deidentifikacija) obraza
  - Odstranitev identitete (ali določne značilnosti) iz obraza



- Zamenjava izraza
  - Iz zvoka v video
  - Iz besedila v video
  - Sinhronizacija ustnic na podlagi novega besedila ali govora



Pornoindustrija

Fig. 5: Examples of accurately detected breast regions on the left and poorly detected breast regions on the right. Some images are cropped to better fit the figure and censored with black boxes here in the paper, whereas the dataset contains original images.

Avtomatska detekcija in prepoznava oseb (žensk) na podlagi prsi.

Preliminary Study on Detection of Breasts,
Pristavnik Vrešnjak Matic, Perušić Ani, Emeršič Žiga, Peer Peter, Batagelj, Borut

Politika

Dictators - Vladimir Putin.mp4

Dictators - Kim Jong-Un.mp4

- Politična kampanija

FAKE: Haryanvi, a dialect of Hindi.

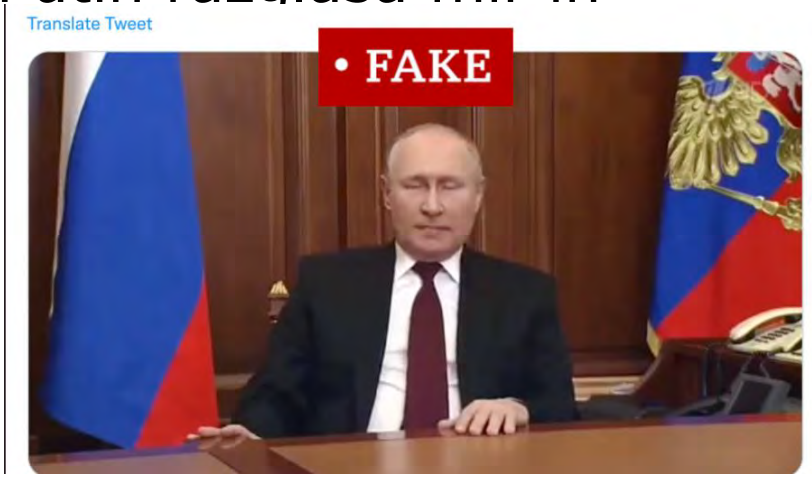
ORIGINAL: English

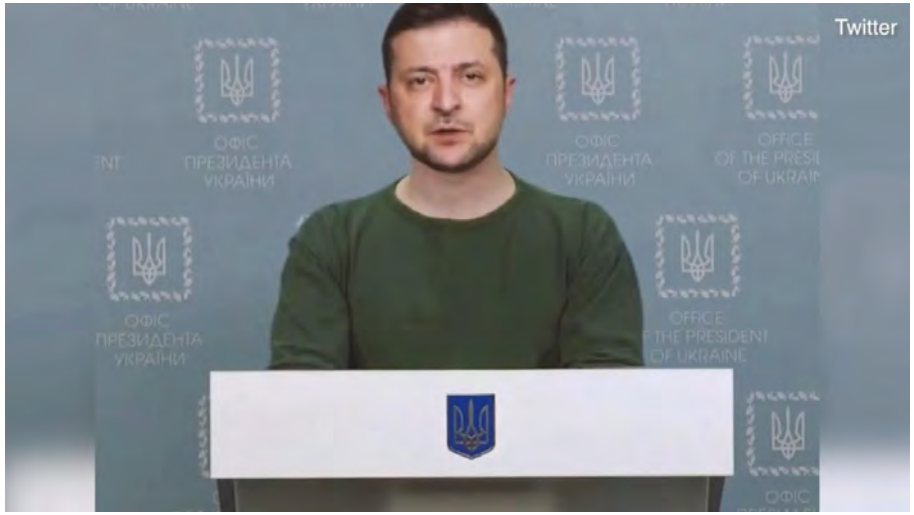
https://www.karlsnotes.com/deepfakes-in-an-indian-election-campaign/

Politika

- Vojna v Ukrajini

Putin razglaša mir in

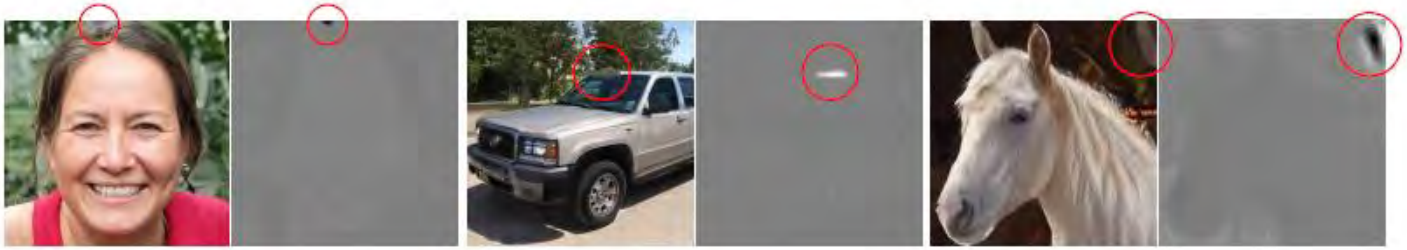




Zelenski govori o predaji

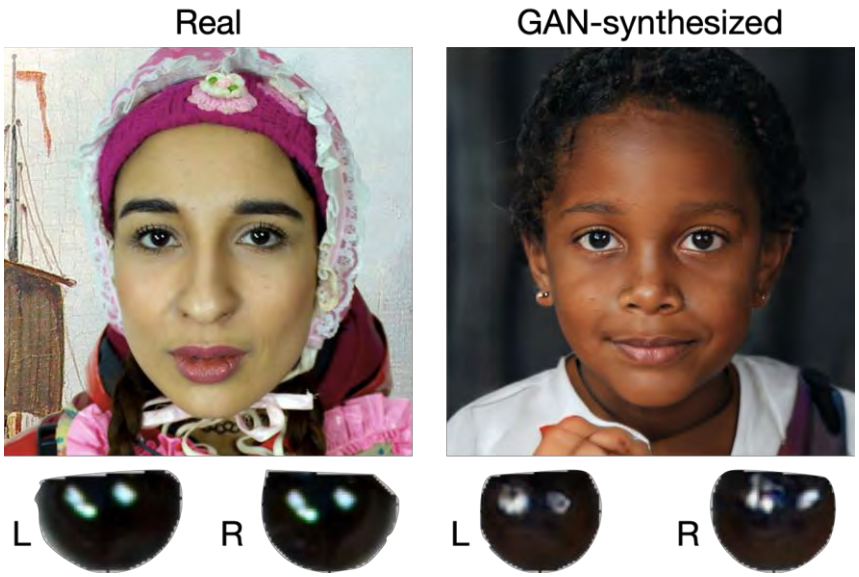
Detekcija globokih ponaredkov (slike)

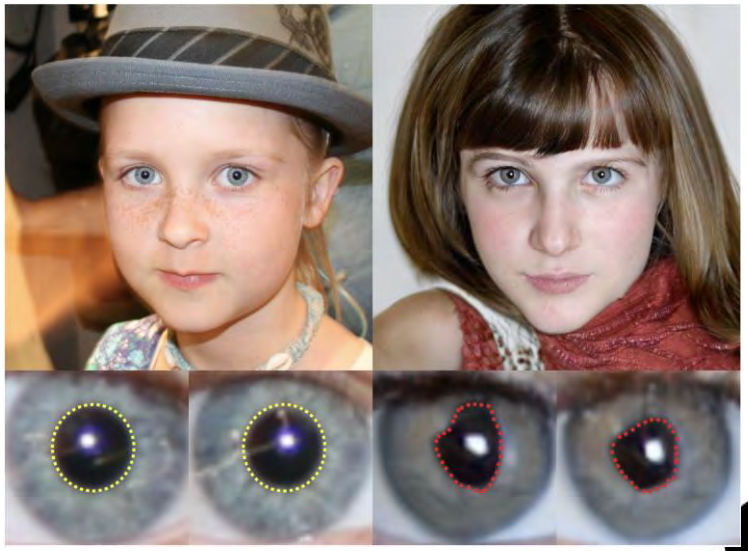
- Vidne napake na generiranih oz. spremenjenih slikah
  - Artefakti na sliki (ozadje)
  - Zobje pri nefrontalnih obrazih



Detekcija globokih ponaredkov (slike)

- Vidne napake na generiranih oz. spremenjenih slikah
  - Artefakti na sliki (ozadje)
  - Zobje pri nefrontalnih obrazih
  - Simetrija (uhlji, oči, uhani)
  - Nepravilne zenice in odsev





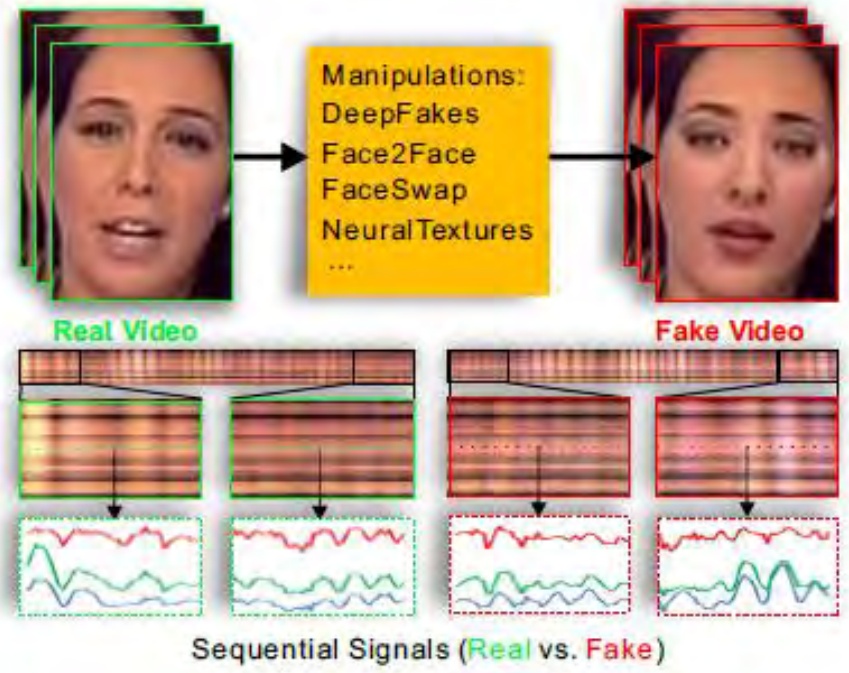
Detekcija globokih ponaredkov (slike)

- Vidne napake na generiranih oz. spremenjenih slikah
  - Artefakti na sliki (ozadje)
  - Zobje pri nefrontalnih obrazih
  - Simetrija (uhlji, oči, uhani)
  - Nepravilne zenice in odsev
  - Iskanje zameglitev na robovih

Li et al. 2020, Face X-ray for More General Face Forgery Detection

Detekcija globokih ponaredkov (video)

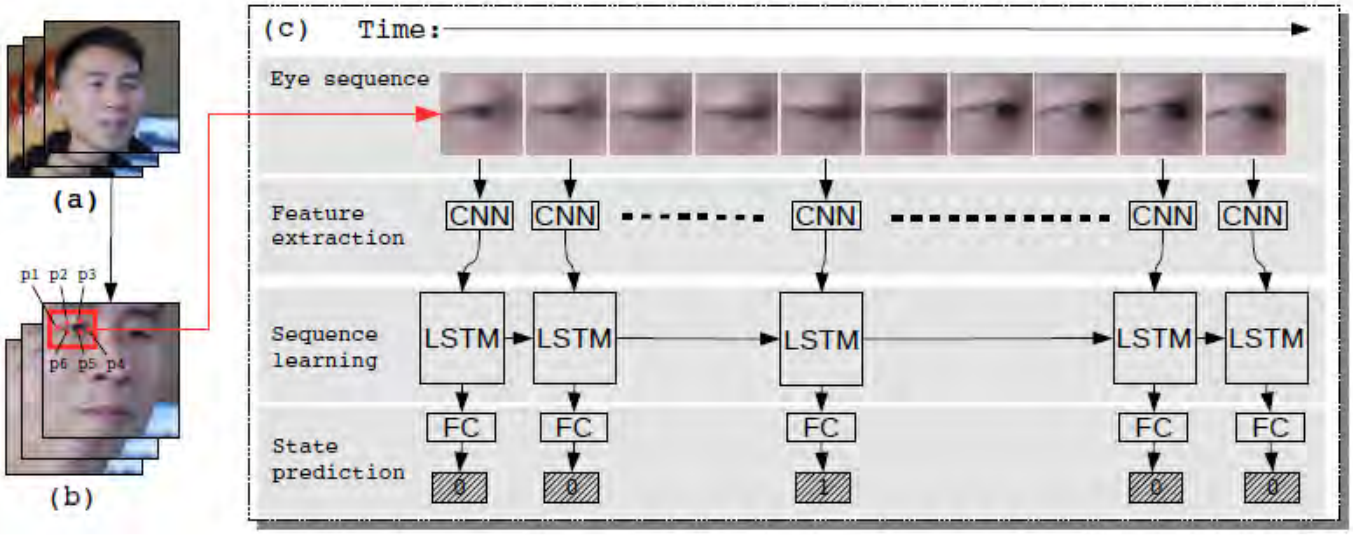
- Nepravilnosti med okvirji
  - Ritem utripanje srca (fotopletizmografija)



Qi et al. 2020, DeepRhythm: Exposing DeepFakes with Attentional Visual Heartbeat Rhythms

Detekcija globokih ponaredkov (video)

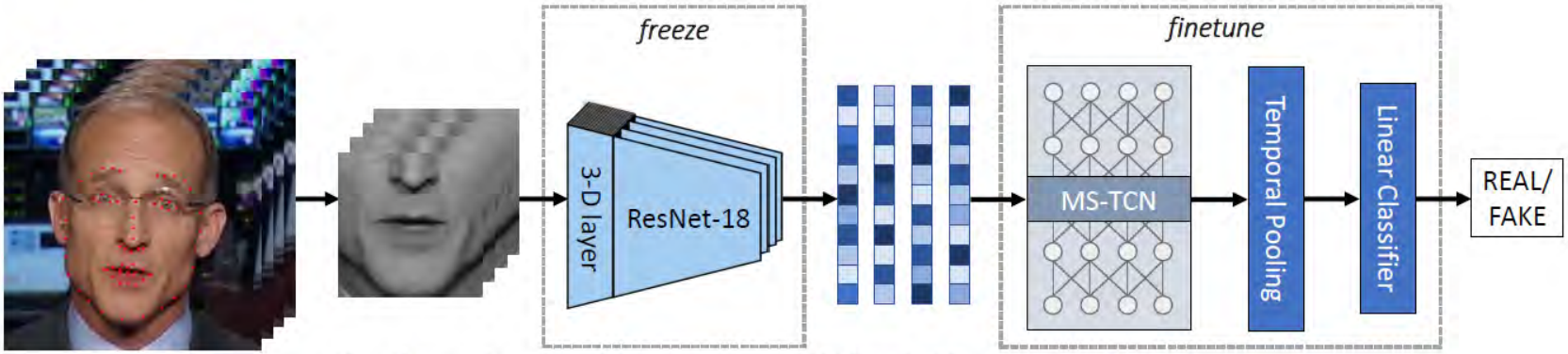
- Nepravilnosti med okvirji
  - Ritem utripanje srca (fotopletizmografija)
  - Neenakomerno mežikanje



Li et al. 2018, In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking

Detekcija globokih ponaredkov (video)

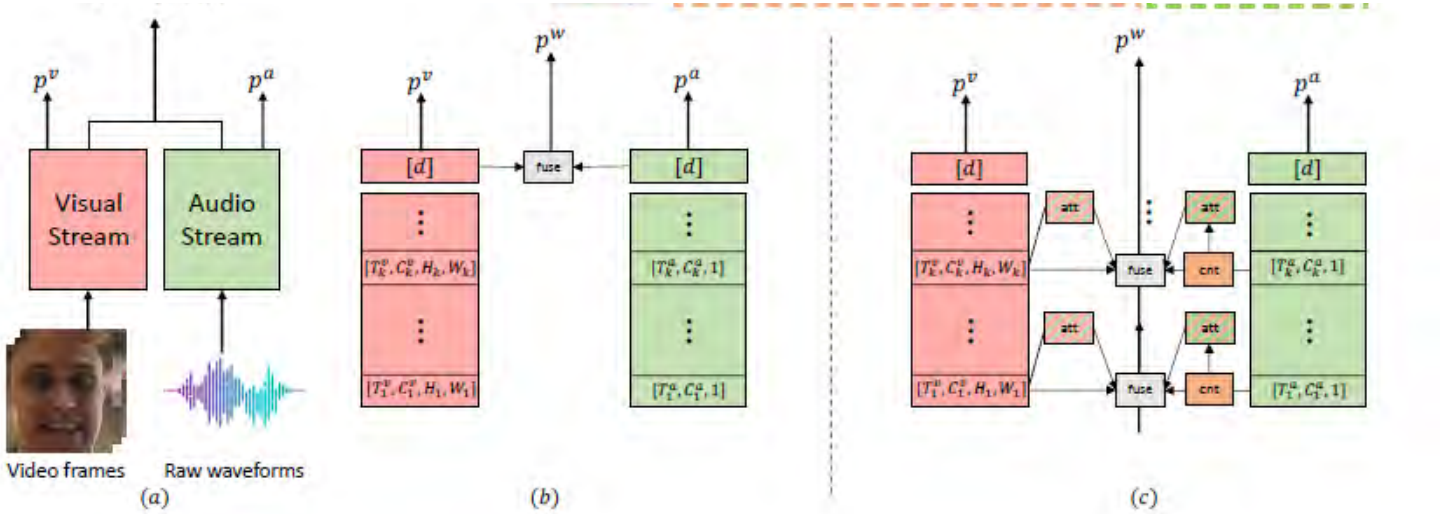
- Nepravilnosti med okvirji
  - Ritem utripanje srca (fotopletizmografija)
  - Neenakomerno mežikanje
  - Neskladnost v premikanje ustnic



Haliassos et al. 2021, Lips Don't Lie: A Generalisable and Robust Approach to Face Forgery Detection

Detekcija globokih ponaredkov (video)

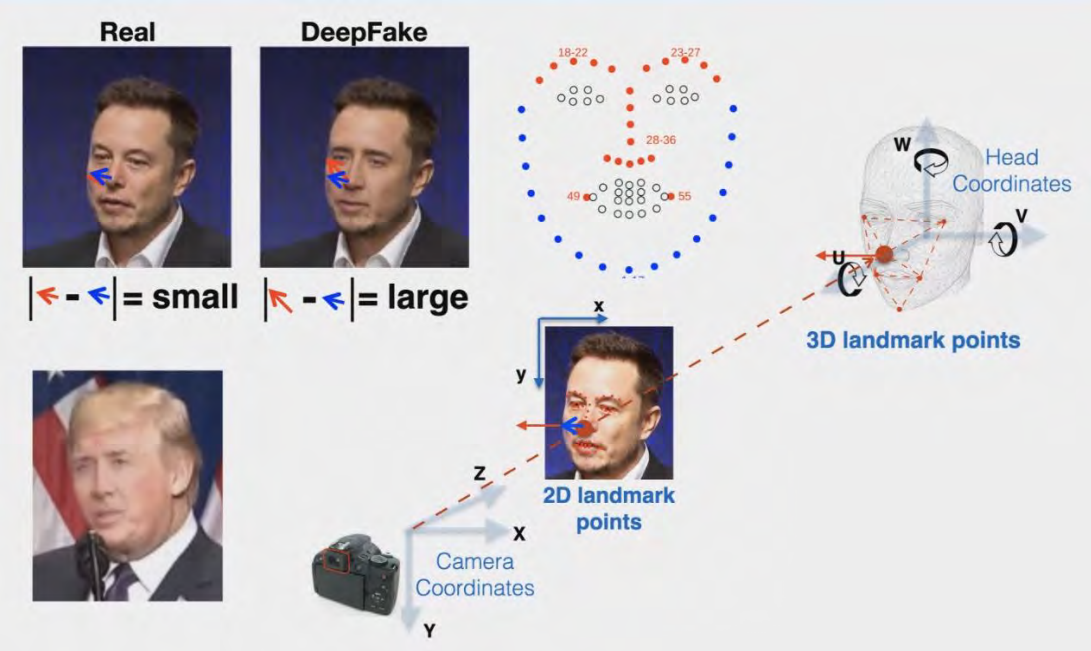
- Nepravilnosti med okvirji
  - Neskladnost med avdio in video



Zhou et al. 2021, Joint Audio-Visual Deepfake Detection

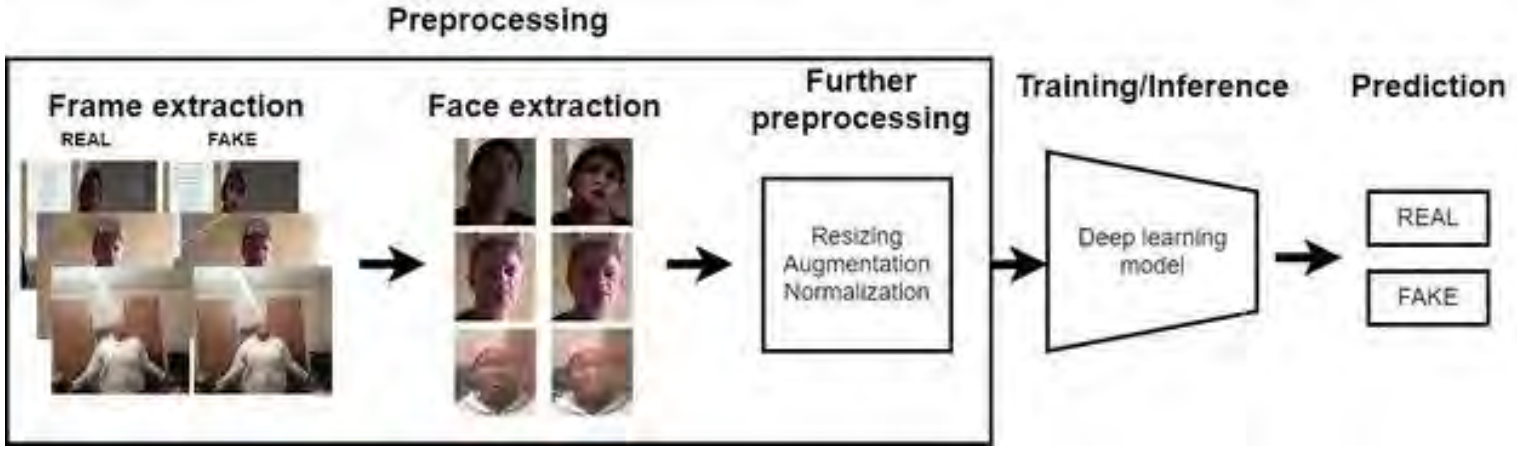
Detekcija globokih ponaredkov (video)

- Nepravilnosti med okvirji
  - Neskladni premiki
    - Nekonsistentnosti pri različnih položajih glave



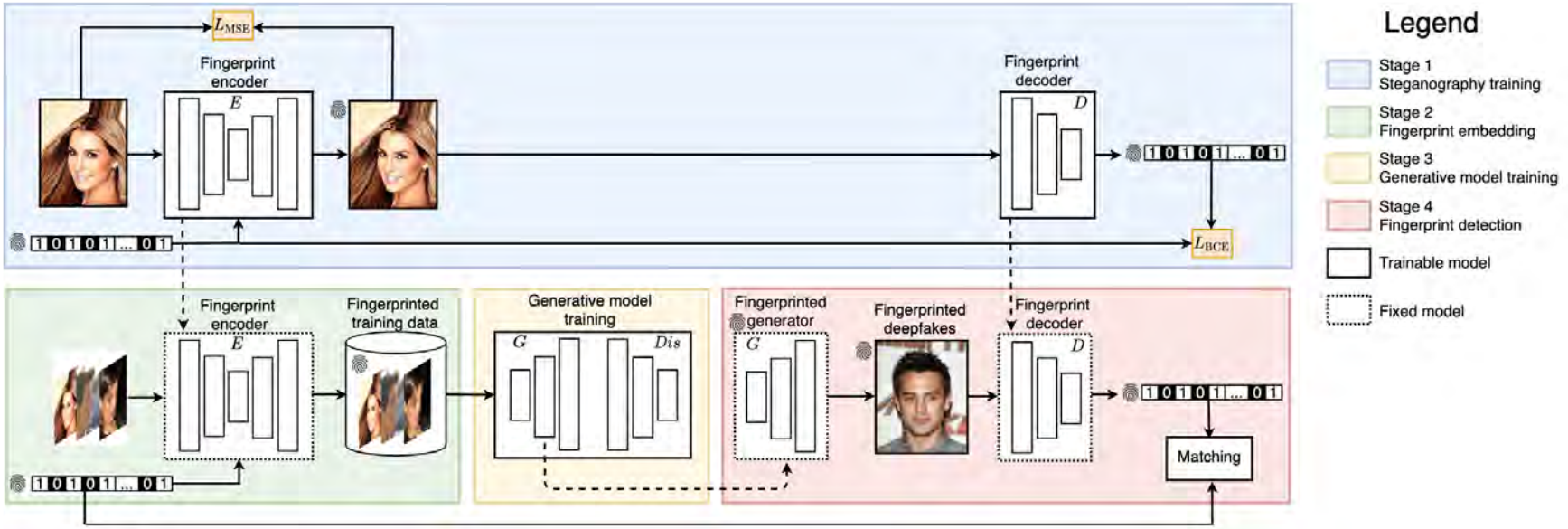
Yang et al. 2018, Exposing Deep Fakes Using Inconsistent Head Poses

CNN: Na podlagi podatkov



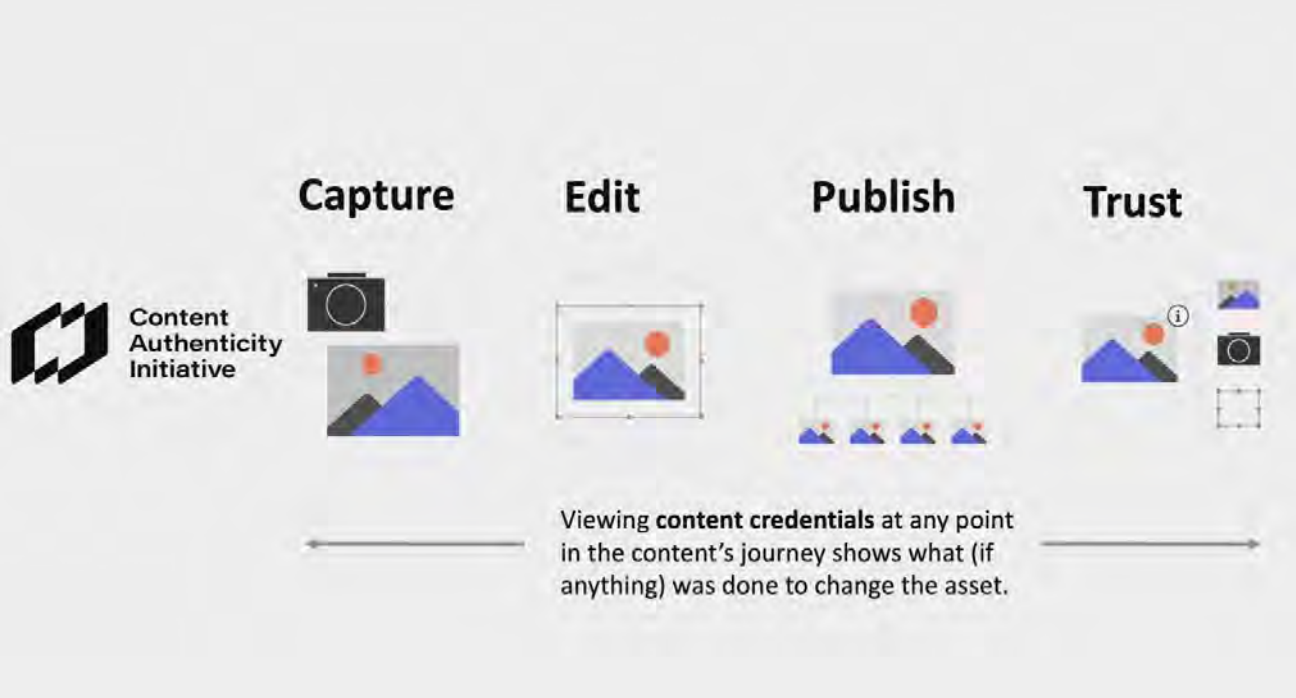
- Iskanje teksture
- Učenje na podlagi podslik (patch)
- Iskanje vzorca (Fingerprint) ki ga generira GAN

Digitalni žig



Yu et al. 2021, Artificial Fingerprinting for Generative Models: Rooting Deepfake Attribution in Training Data

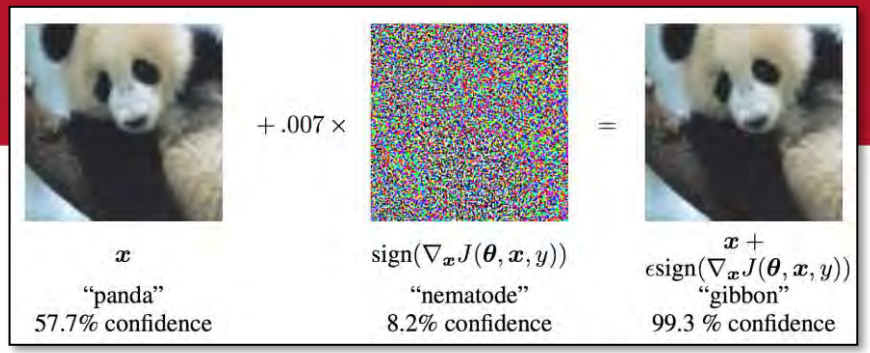
Pobuda: pristnost vsebine



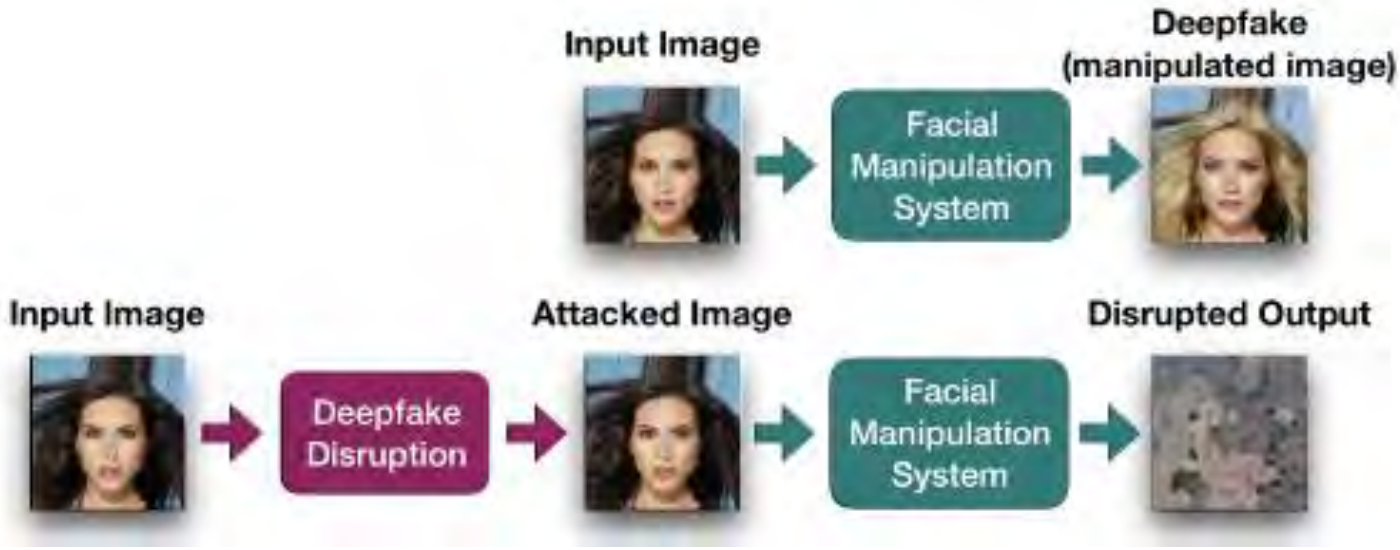
The Coalition for Content Provenance and Authenticity (C2PA)

https://c2pa.org/

Nasprotniški napad



Goodfellow et al. 2015

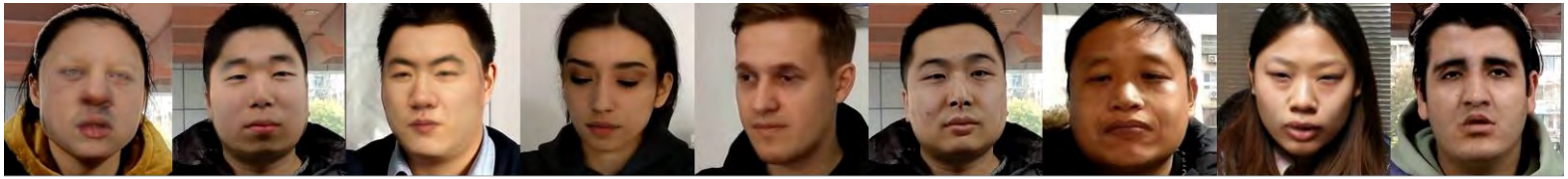


Ruiz et al. 2020, Disrupting Deepfakes: Adversarial Attacks Against Conditional Image Translation Networks and Facial Manipulation Systems

DeepFake - tekmovanje

- 2020: Deepfake Detection Challenge (DFDC)
  - AWS, Facebook, Microsoft
- DeepFake Game Competition (DFGC) @ IJCB 2022
  - Metode za ustvarjanje
  - Metode za detekcijo
- Face Morphing Attack Detection Based on Privacy-aware Synthetic Training Data (SYN-MAD) @ IJCB 2022
  - A face morphing attack aims at creating images that automatically or by human experts are matched to faces of more than one individual.
- 2023 DeepFake Game Competition on Visual Realism Assessment (DFGC-VRA)

DFGC-VRA 2023



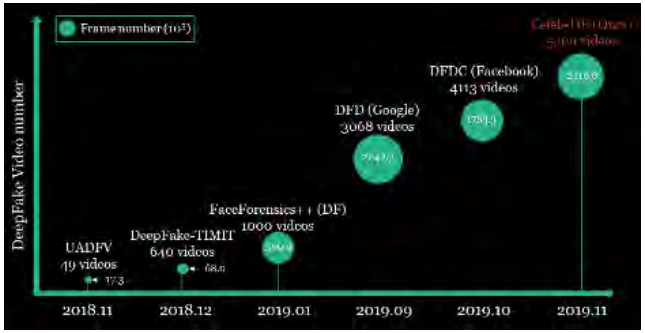
gt: 1.2, pred: 1.81 | gt: 1.6, pred: 1.52 | gt: 1.8, pred: 1.96 | gt: 2.0, pred: 2.08 | gt: 2.2, pred: 2.19 | gt: 2.4, pred: 2.63 | gt: 2.6, pred: 2.67 | gt: 2.8, pred: 2.65 | gt: 3.0, pred: 2.99

gt: 3.2, pred: 2.77 | gt: 3.4, pred: 2.98 | gt: 3.6, pred: 3.9 | gt: 3.8, pred: 3.52 | gt: 4.0 pred: 3.88 | gt: 4.2, pred: 4.14 | gt:4.4, pred: 3.88 | gt: 4.4, pred: 4.15 | gt: 4.4, pred: 4.22

To assess how ‘realistic’ deepfake videos seem to human viewers

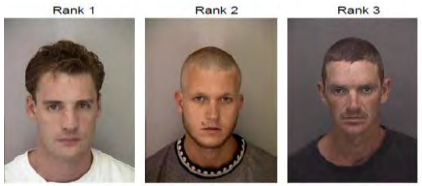
Model	Test Set	PLCC↑	SRCC↑	Score↑
OPDAI	1	**0.8578**	**0.8372**	**0.8851**
	2	**0.9423**	**0.9214**	
	3	**0.8928**	**0.8592**	
HUST	1	0.8117	0.7864	0.8564
	2	0.9281	0.9215	
	3	0.8842	0.8348	
Our Ensemble	1	0.8091	0.7633	0.8545
	2	0.9287	0.9197	
	3	0.8746	0.8318	
Organizer baseline[23]	1	0.3778	0.4731	0.5470
	2	0.5949	0.7322	
	3	0.4898	0.6139	

Baze

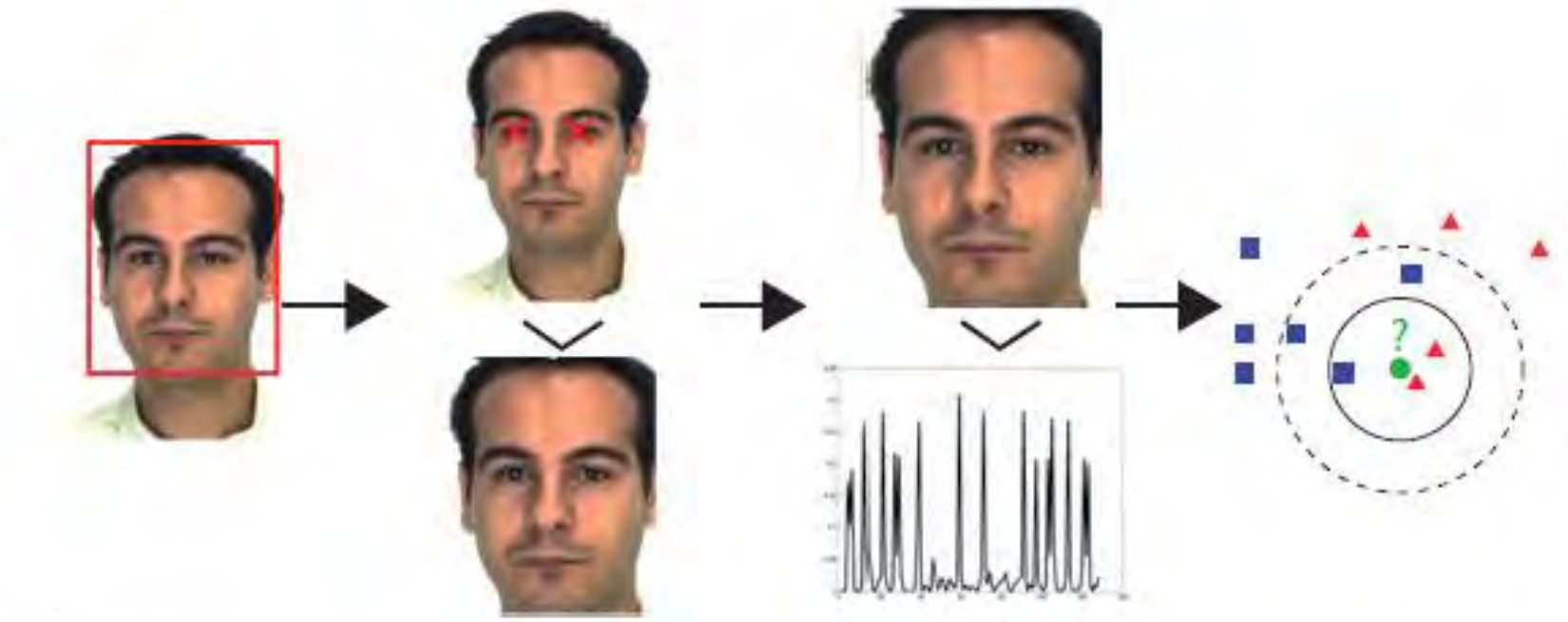

Frame number (10^3)
DeepFake Video number
DFDC (Facebook)
4113 videos
DFD (Google)
3068 videos
FaceForensics++ (DF)
1000 videos
DeepFake-TIMIT
640 videos
UADFV
49 videos
2018.11
2018.12
2019.01
2019.09
2019.10
2019.11

Prepoznava obrazov v forenzičnih aplikacijah

- Identifikacija
  - Prstni odtisi, kri (DNK), odtis stopala
  - Veliko kamer -> prepoznava iz obraza
- Trenutni sistemi za prepoznavanje obrazov
  - V pomoč
  - Še veliko izzivov
    - Slike **slabše** kvalitete
    - Robustnost na staranje
    - Uporaba znamenj na obrazu
    - Primerjava (sestavljenih) obraznih skic s sliko
      - » Zorni kot kamere



Klasični sistem za prepoznavo obrazov



iskanje obraza

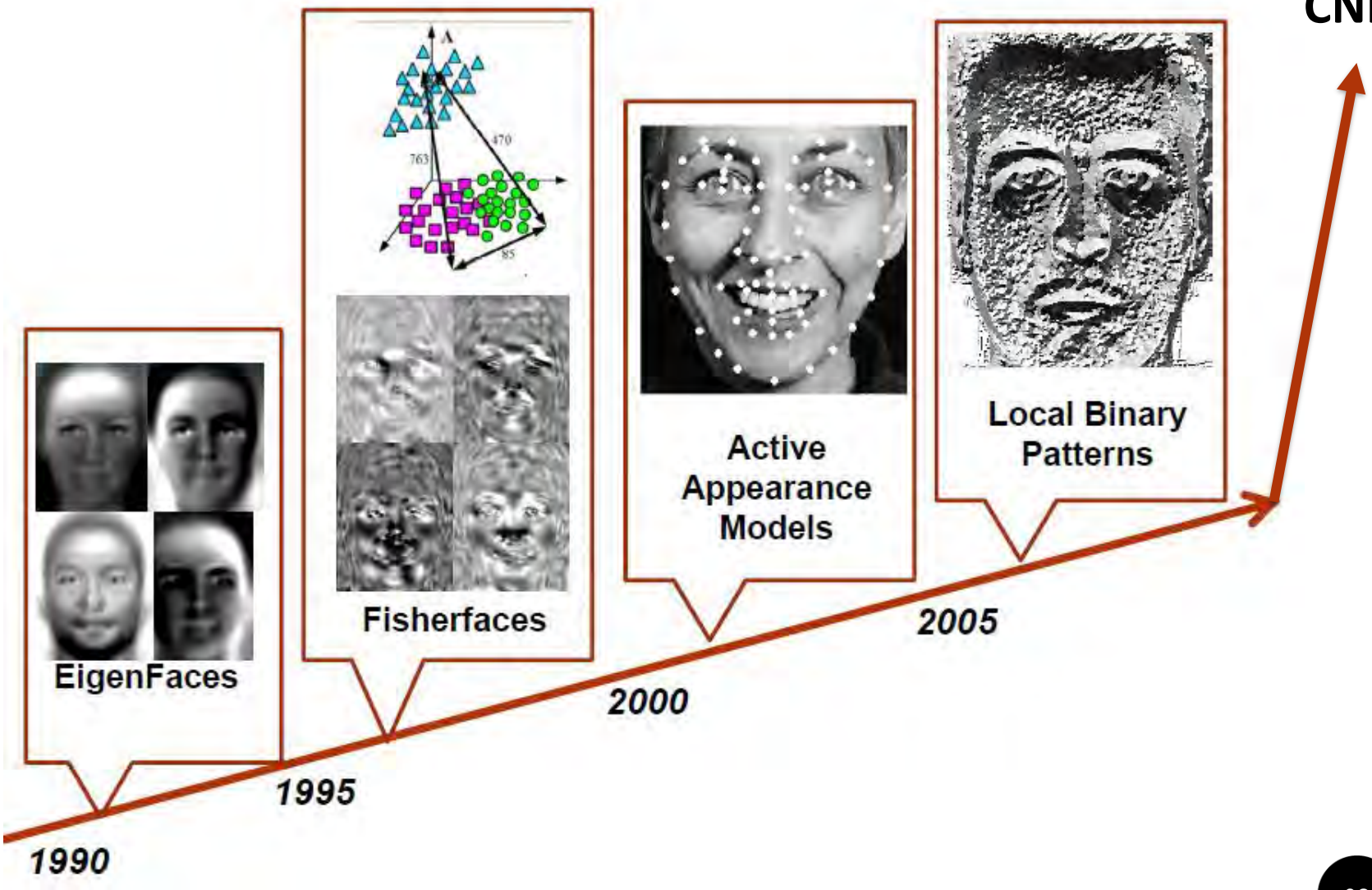
normalizacija slike

izločitev značilk

ujemanje

Napredek metod

Konvolucijske Nevronske mreže CNN

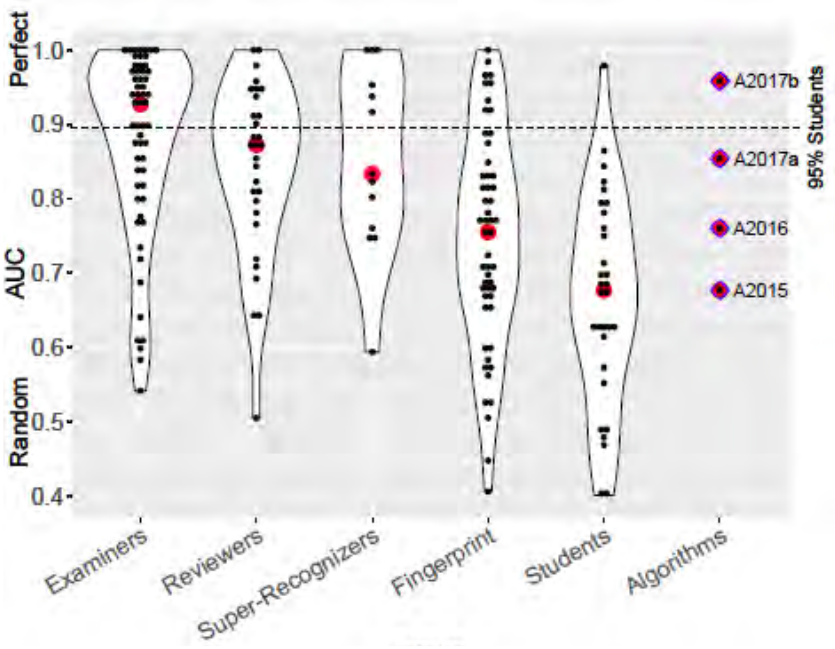


Zadnje raziskave[1]

- Različne skupine
  - Forenzični preiskovalci za obrazno prepoznavo
  - Prepoznavalci obrazov
  - Superpoznavalci
  - Preiskovalci za prstne odtise
  - Študentje

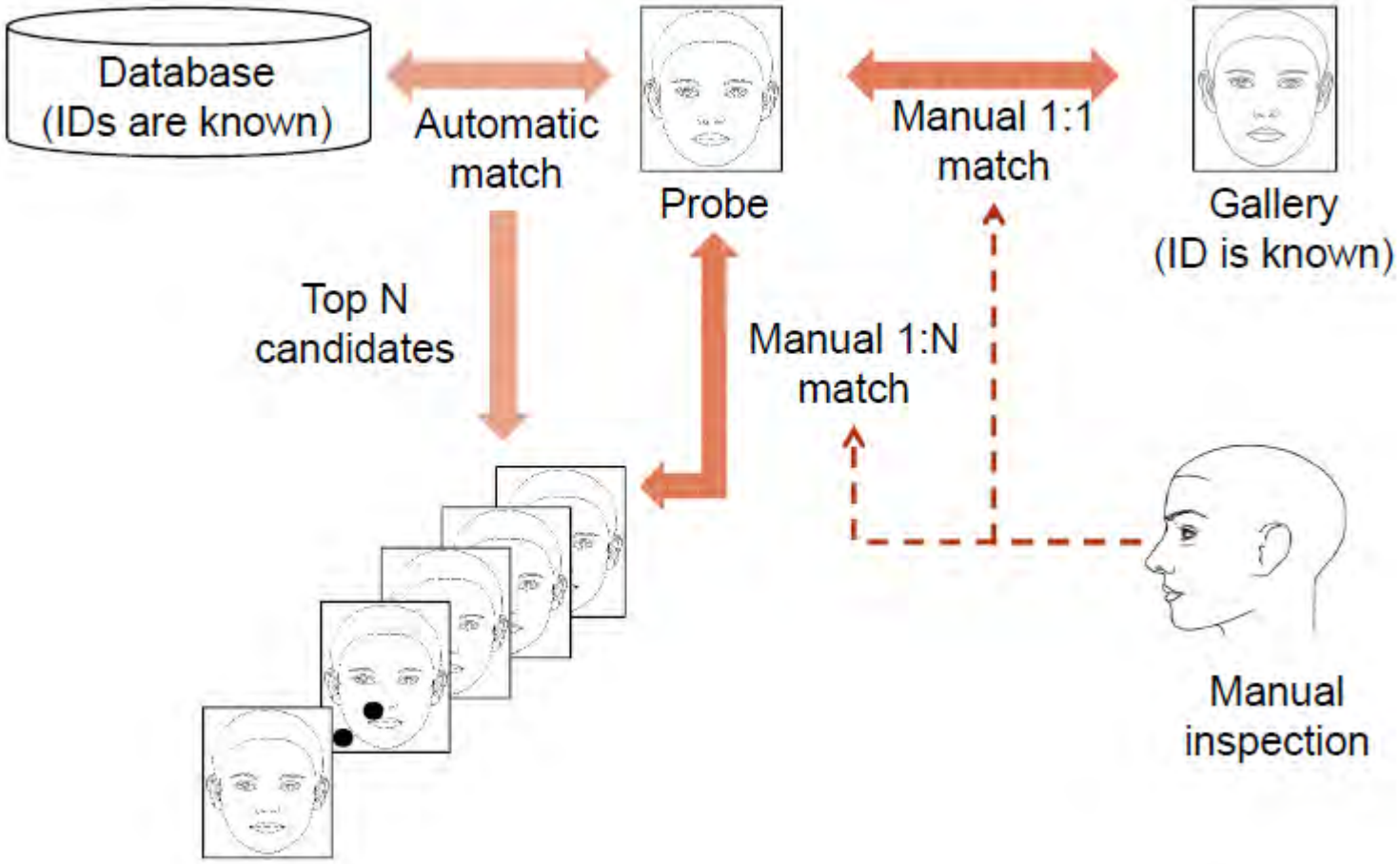
Proti

- Računalniški sistemi (CNN)
  - A2015 – A2017[2]



Vir: 1. P. Jonathon Phillips s sod., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms
2. Ranjan, Rajeev, Carlos D. Castillo, and Rama Chellappa. "L2-constrained softmax loss for discriminative face verification."

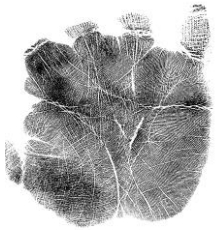
Delovanje forenzičnih aplikacij



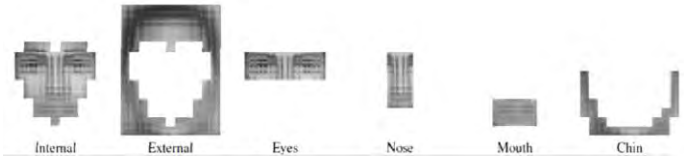
Nadaljnje delo


- Video posnetki (različni pogledi, kvaliteta)
- Prepoznava blizu infrardeče osvetlitve
- Tetovaže
- Identifikacija:
  - Odtisi dlani, uhlji, beločnica, prstne sledi





- Prihodnost
  - Večja veljava obrazne prepoznave na sodišču
  - Prepoznava obraznih delov in verjetnost ujemanja
    - oči, nos, usta, obrvi, ličnice



University *of Ljubljana*
Faculty *of Computer and Information Science*

Hvala za pozornost

26. marec 2024

Ali sta osebi isti?

Ali sta osebi isti?

Ali sta osebi isti?