Izboljšava cevovoda za deidentifikacijo obrazov

Tadej Ciglarič, Žiga Emeršič, Peter Peer, Blaž Meden
FRI UL

Konferenca ROSUS, Maribor, 2018

Kaj je proces deidentifikacije?

- Deidentifikacija je proces zakrivanja osebnih informacij z namenom zaščite zasebnosti posameznikov, katerih osebne lastnosti so prisotne v podatkih.

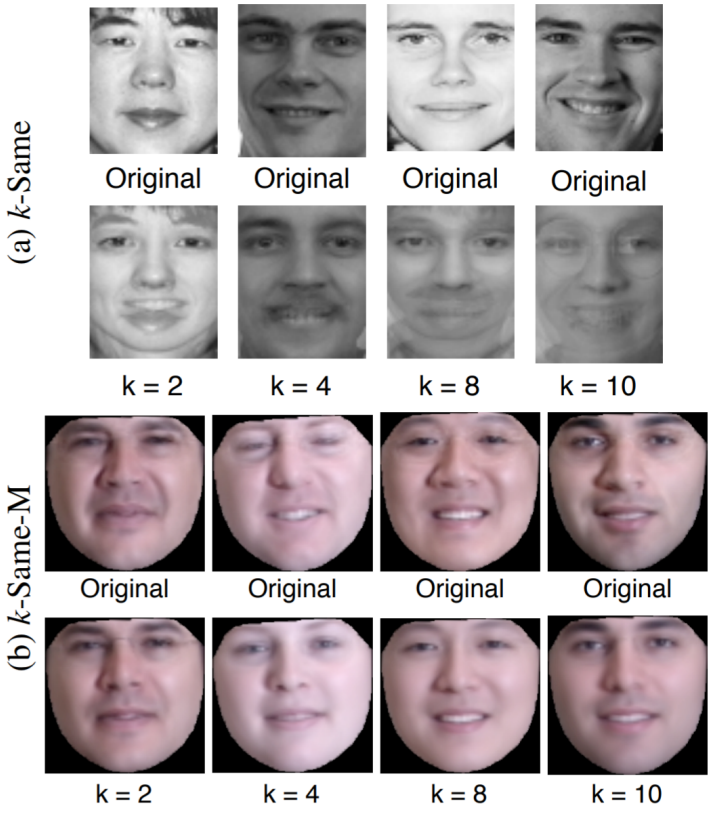
- Motivacija za deidentifikacijo obrazov na slikah in videu:
  - Ogromne količine video podatkov se dnevno ustvarijo iz nadzornih videosistemov.
  - Drugi viri so socialna omrežja ter storitve, npr. Google Street View ali FourSquare.
  - Deljenje teh podatkov brez predhodne deidentifikacije lahko krši pravice o zasebnosti posameznikov (videi npr. lahko vsebujejo obraze – identiteto – posameznikov).
  - Podatki se zato ponavadi deidentificirajo, preden se delijo oz. nadaljnje analizirajo.
  - Pri tem želimo zakriti osebne identifikatorje, neosebne atribute pa želimo ohraniti za nadaljnjo analizo (npr. spol, izraz na obrazu, itd.).

  - Zadnje delo iz tega področja predlaga cevovod za deidentifikacijo obrazov z uporabo generativnih nevronskih mrež (Meden idr., 2017).

Obstoječe metode

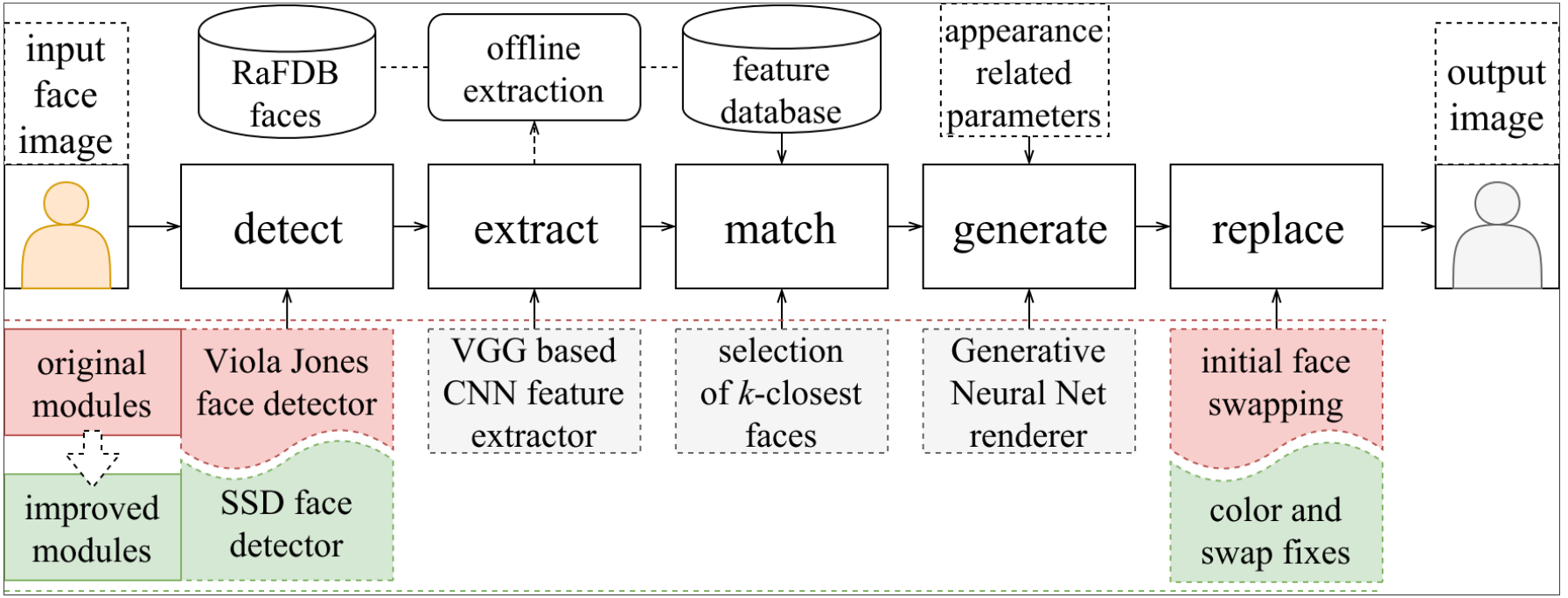
- Naivni pristopi (z uporabo enostavnega filtriranja): *blacking out*, *blurring*, *pixelization*.

- Formalne metode – sledijo načelu *k*-anonimnosti (algoritmi *k*-enakih):
  - *k*-Same-Pixel (Newton idr., 2005)
  - *k*-Same-M, k-Same-Select (Gross idr., 2009)
  - *k*-Diff-Furthest (Sun idr., 2015)
  - *k*-Same-Net (Meden idr., 2018) >>>>>



Predlagan cevovod za deidentifikacijo

Omogoča deidentifikacijo obrazov na slikah ali v videu.



Primeri generiranih slik z generativno mrežo

Generiramo lahko različne obraze, pri tem pa mreža upošteva vhodne parametre, npr. ciljni izraz na obrazu (**ohranjanje uporabnosti podatkov** oz. angl. *Data Utility*):

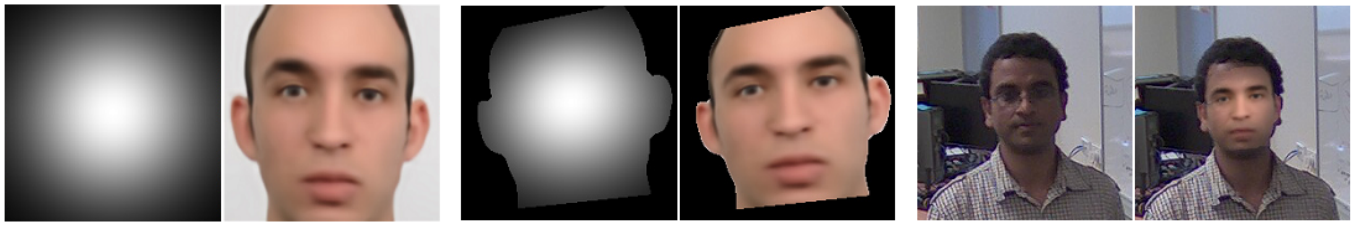
Problemi obstoječe rešitve

- Osnovni detektor obrazov (Viola − Jones) deluje dobro le v optimalnih pogojih za detekcijo (frontalni obrazi, ustrezna osvetlitev, ustrezna velikost).
  - V kolikor ti pogoji niso izpolnjeni (majhni, nefrontalni obrazi, variabilna osvetlitev), detekcija deluje nezadovoljivo.
- Zamenjava obrazov na podlagi segmentacije barve kože, ki je utežena z masko normalne porazdelitve, lahko za seboj pusti vizualne artefakte, ki so vidni na robovih opravljene zamenjave ciljnega obraza z generiranim obrazom.
  - Barva generiranih obrazov je prevzeta iz optimalnih pogojev, pod katerimi so bile zajete slike obrazov iz baze RaFD – zato se barva ne ujema z barvo kože, ki jo imajo obrazi v videu.

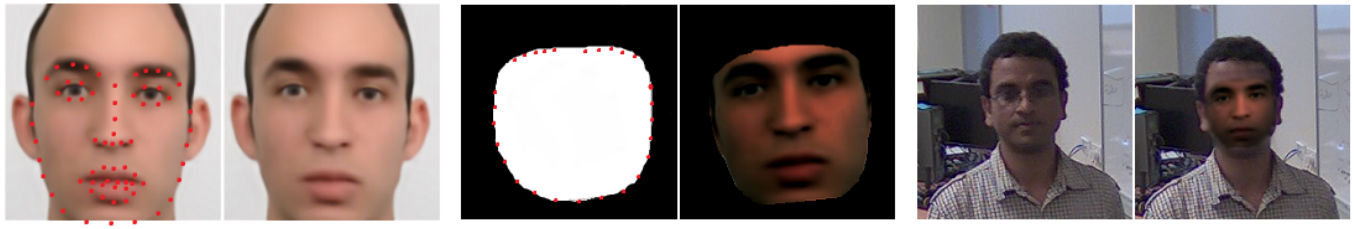
Problemi obstoječe rešitve

Implementirane izboljšave

- Detektor Viola − Jones nadomeščen z detektorjem SSD.
- Izenačitev barv (*color equalization*) na podlagi analize histogramov.
- Konveksna ovojnica značilnih točk obraza zamenja Gaussovo masko.
- Izvorna impl.:

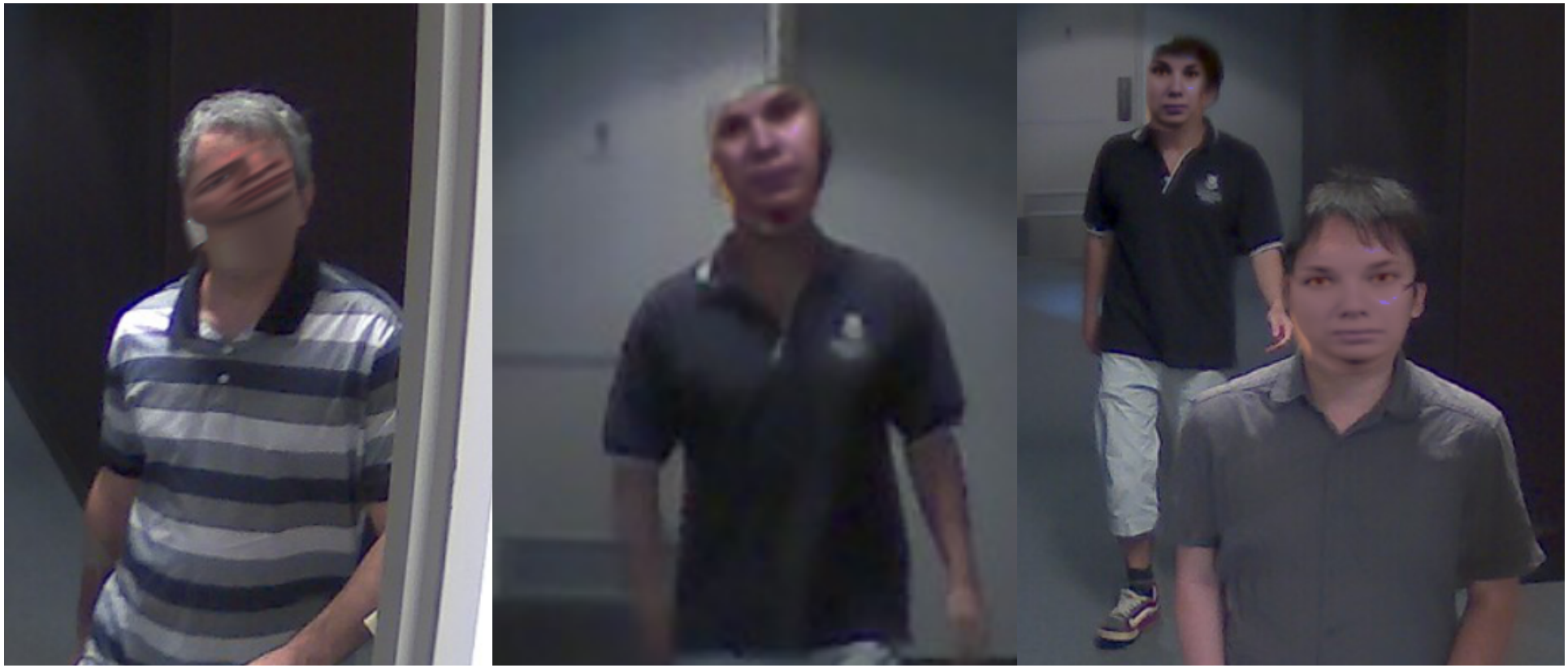


- Izboljšave:



Rezultati – primeri izboljšane deidentifikacije

Rezultati – primeri slabe lokalizacije SSD



Zaključki

- Realizirali smo dve pomembni izboljšavi obstoječega cevovoda za deidentifikacijo obrazov.
- Z uporabo novega detektorja SSD je detekcija bolj zanesljiva.
- Proces lepljenja nadomestnih obrazov na ciljne subjekte sedaj vsebuje manj vizualnih napak.

- Obstoječe težave pri detekciji značilnih obraznih točk bi lahko naslovili z dodatnim učenjem le-tega iz detekcij uporabljenega SSD detektorja. (Lahko pa gremo na drugi detektor točk ali globoki detektor.)
- Cilji dela v prihodnosti bodo naslavljali segmentacijo las oz. pričeske ter deidentifikacijo čelne regije (regije izven domene značilnih obraznih točk).