Visage Technologies

LINKÖPING UNIVERSITY

Ansiktsigenkänning

Vad? Hur? Varför?

Jörgen Ahlberg

Vetenskapsdagen vid Linköpings universitet 2021-10-07

1

AGENDA

Ansiktsigenkänning

- Vad är ansiktsigenkänning?
- Hur fungerade det (inte?) förr?
- Hur fungerar det nu?
- Hur bra är det?
- Hur lurar man ansiktsigenkänning?
- Varför?

2

Visage Technologies

LINKÖPING UNIVERSITY

Vad är ansiktsigenkänning?

Jörgen Ahlberg

Vetenskapsdagen vid Linköpings universitet 2021-10-07

3

VAD ÄR ANSIKTSIGENKÄNNING?

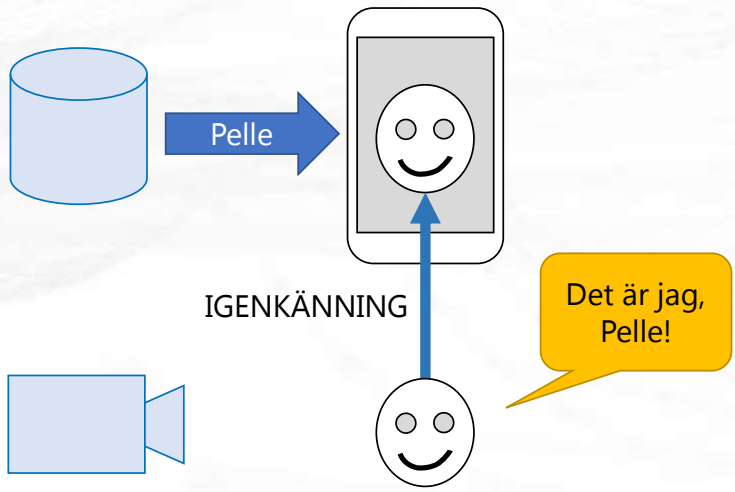
Ansiktsigenkänning? Nej, detektion!

4

5

VAD ÄR ANSIKTSIGENKÄNNING?

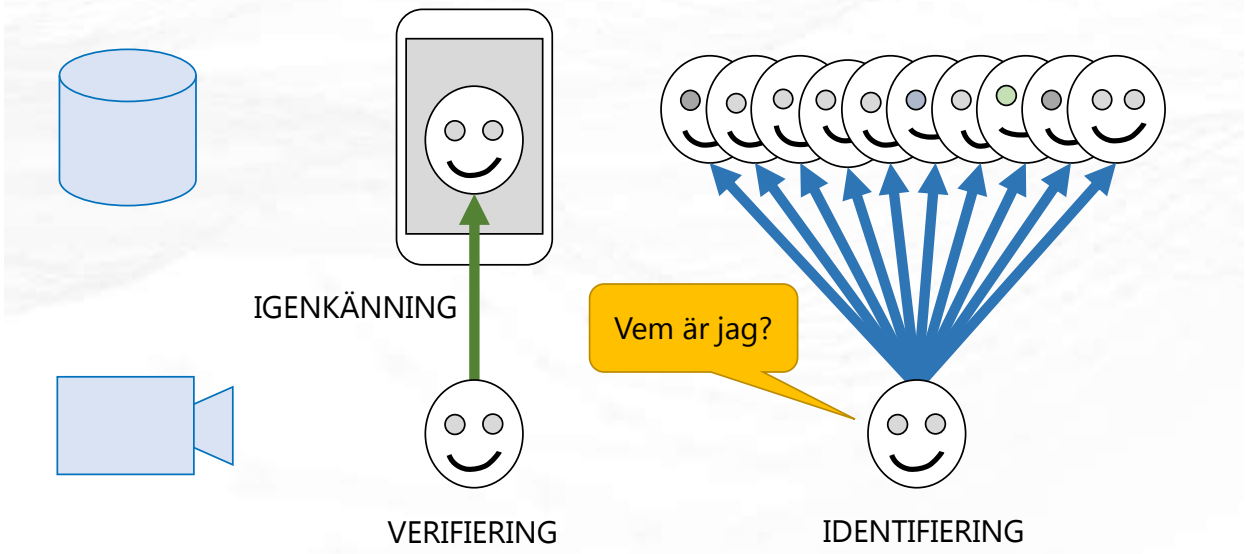
Igenkänning, verifiering och identifiering



6

VAD ÄR ANSIKTSIGENKÄNNING?

Igenkänning, verifiering och identifiering



7

Visage Technologies

LINKÖPING UNIVERSITY

Hur fungerade ansiktsigenkänning?

Jörgen Ahlberg

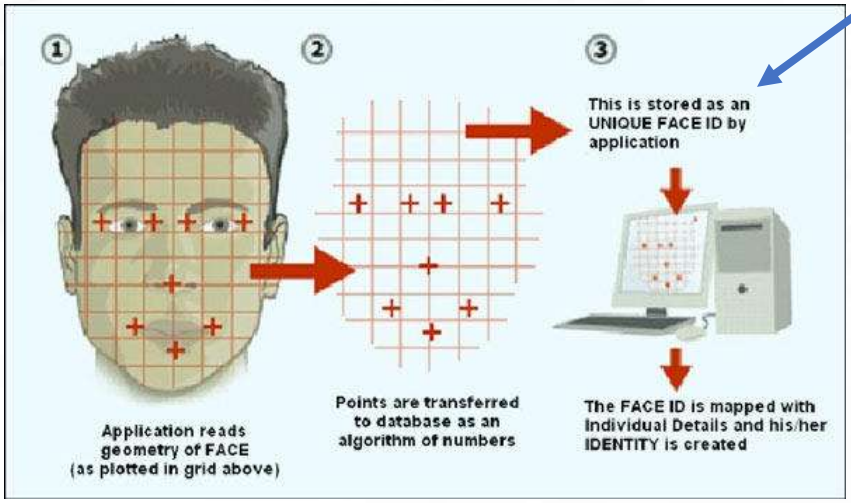
Vetenskapsdagen vid Linköpings universitet 2021-10-07

8

HUR FUNGERADE ANSIKTSIGENKÄNNING?

Förhistorisk ansiktsigenkänning

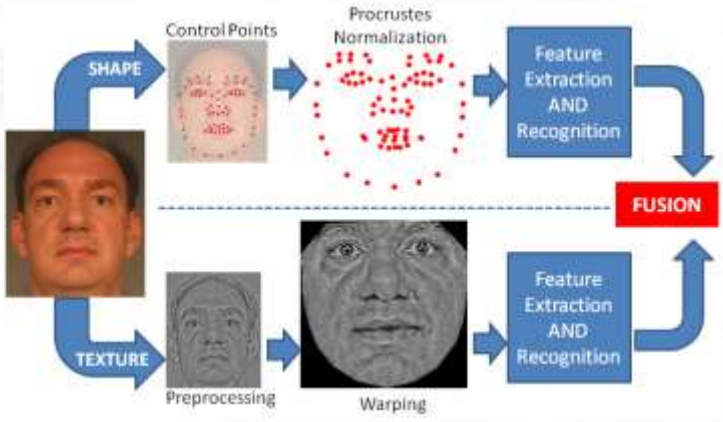
Egenskapsvektor
16 dimensioner



9

HUR FUNGERADE ANSIKTSIGENKÄNNING?

Historisk ansiktsigenkänning

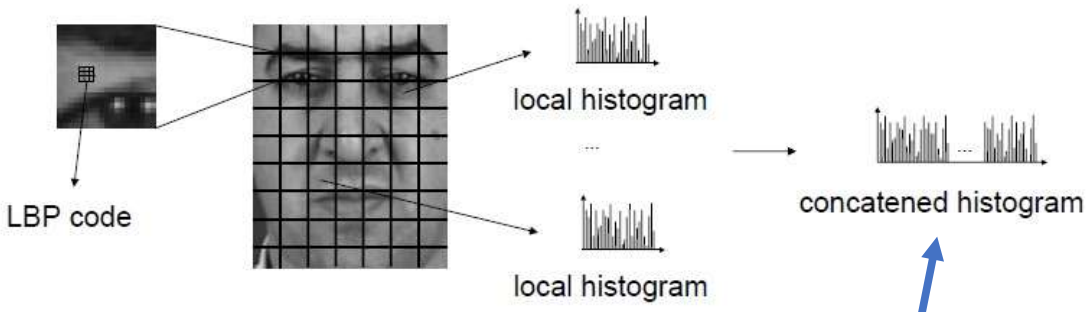


Använd bilden, inte bara formen.

10

HUR FUNGERADE ANSIKTSIGENKÄNNING?

Ansiktsigenkänning igår



Diverse påhittade egenskaper extraheras från bilden.

Egenskapsvektor
100-tals dim

11

HUR FUNGERADE ANSIKTSIGENKÄNNING?

Modern ansiktsigenkänning (just nu, iaf)

Egenskaper som tränats fram extraheras från bilden.

Egenskapsvektor
1000-tals dim

12

Visage Technologies

LINKÖPING UNIVERSITY

Hur fungerar ansiktsigenkänning?

Jörgen Ahlberg

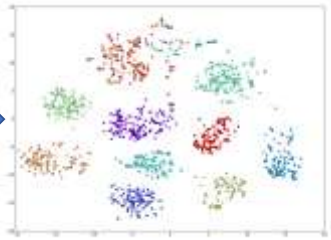
Vetenskapsdagen vid Linköpings universitet 2021-10-07

13

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Så funkar det

1. Detektera ansiktet
2. Geometrisk normalisering
3. Egenskapsvektor
4. Matchning



14

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Registrering

Jörgen:  → 72 42 63 74 12 8

Namn	Egenskapsvektorer
Jörgen	72 42 63 74 12 8
Jörgen	75 40 63 71 12 8
Jörgen	74 44 61 75 14 9
Pelle	63 85 42 63 74 86
Pelle	62 85 45 60 71 83

15

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Matchning

 → 70 41 60 70 10 7 ?

Namn	Egenskapsvektorer	Skillnad
Jörgen	72 42 63 74 12 9	14
Jörgen	**75 40 63 71 12 8**	**13**
Jörgen	74 44 61 75 14 9	19
Pelle	63 85 42 63 74 86	219
Pelle	62 85 45 60 71 83	214

16

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Så funkar det

1. Detektera ansiktet
2. Geometrisk normalisering
3. Egenskapsvektor
4. Matchning

17

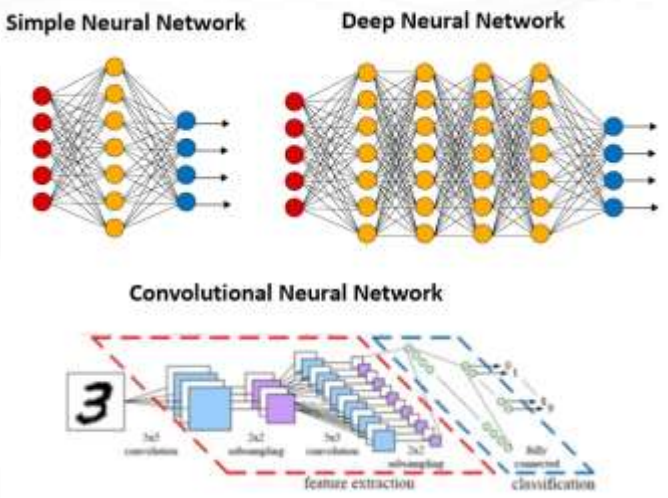
HUR FUNGERAR ANSIKTSIGENKÄNNING?

Modern ansiktsigenkänning (just nu, iaf)

18

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Neurala nätverk



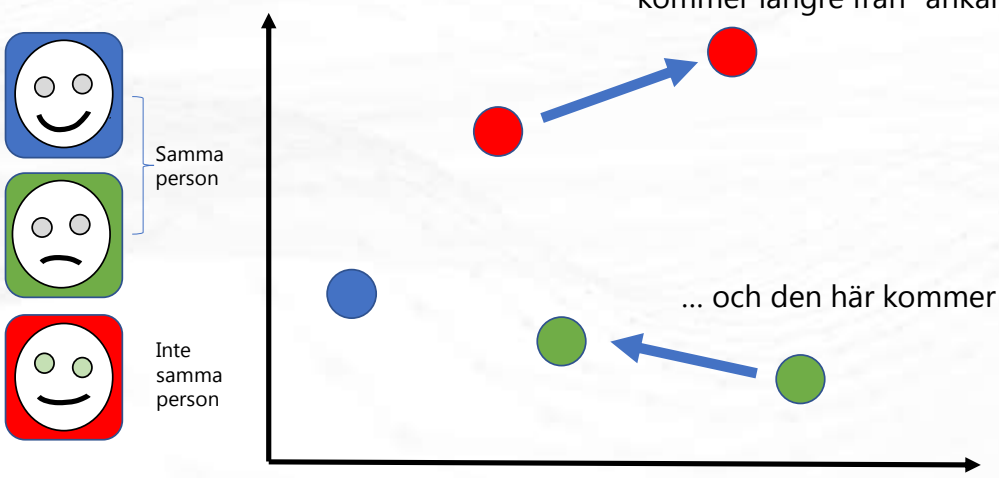
www.tritytech.com

19

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Trippelträning

Ändra parameterna så att den här kommer längre från ”ankaret”…



Repetera… för jättemånga ansikten. Men var får man tag i dem?

20

HUR FUNGERAR ANSIKTSIGENKÄNNING?

Träningsdata

- **Labeled Faces in the Wild (LFW)**
  - A database of face photographs designed for studying the problem of *unconstrained face recognition*.
  - >13,000 images of faces collected from the web labeled with the name of the person pictured.
  - 1680 of the people pictured have two or more distinct photos in the data set.
- **MS Celebs**
  - Microsoft Celeb (MS-Celeb-1M) is a dataset of 10 million face images harvested from the Internet for the purpose of developing face recognition technologies.
- **MegaFace**
- …

21

HUR FUNGERAR ANSIKTSIGENKÄNNING?

De-facto-standardtest: MegaFace

- **Challenge 1:** Train on any dataset, test your method with **1 million** distractors
- **Challenge 2:** Training on **672K** identities (4.7 million photos), test at million scale

- Distractors
  - 1 million photos
  - 690,572 unique users
- Training set
  - 4.7 million photos
  - 672,057 unique identities
  - 3-2469 photos / person (average 7)

22

NIST

PROJECTS/PROGRAMS

Face Recognition Vendor Test (FRVT)

DESCRIPTION

Ongoing FRVT Activities

FRVT: FACE MASK EFFECTS

NIST has published NISTIR 8311 - Ongoing FRVT Part 6A: Face recognition accuracy with face masks using pre-COVID-19 algorithms, the first out of a series of reports aimed at quantifying face recognition accuracy for people wearing masks. The initial approach was to apply masks to faces digitally (i.e., using software to apply a synthetic

23

Visage Technologies

LINKÖPING UNIVERSITY

Är det bra, då?

Jörgen Ahlberg

Vetenskapsdagen vid Linköpings universitet 2021-10-07

24

HUR BRA ÄR ANSIKTSIGENKÄNNING?

Idag

False match ratio. Släpper in någon som inte är Pelle.

False negative match ratio. Släpper inte in Pelle trots att det är Pelle.

- ”Superhuman performance”. NIST: FMR: 0.000001. FNMR: 0.0025.
- Kräver att ansiktet syns, i en användbar bild!

Användbara?

25

Visage Technologies

LINKÖPING UNIVERSITY

Hur lurar man ansiktsigenkänning?

Jörgen Ahlberg

Vetenskapsdagen vid Linköpings universitet 2021-10-07

26

HUR LURAR MAN ANSIKTSIGENKÄNNING?

Syfte?

- Undvika: Att inte bli igenkänd
- Lura (”spoofing”): Att bli igenkänd som någon annan

27

HUR LURAR MAN ANSIKTSIGENKÄNNING?

Undvika

CV Dazzle

D-ID

Facebook

28

HUR LURAR MAN ANSIKTSIGENKÄNNING?

Lura

- Visa ett foto på en annan person
- Visa ett foto med hål för ögon och mun
- Visa en video med en annan person
- Visa en animering av en annan person

- Interaktiv ”liveness detection”
- Face flash liveness detection
- 3D
- Heartbeat estimation

29

Visage Technologies

LINKÖPING UNIVERSITY

Visage SDK

http://visagetechnologies.com/demo

Jörgen Ahlberg

Vetenskapsdagen vid Linköpings universitet 2021-10-07

30