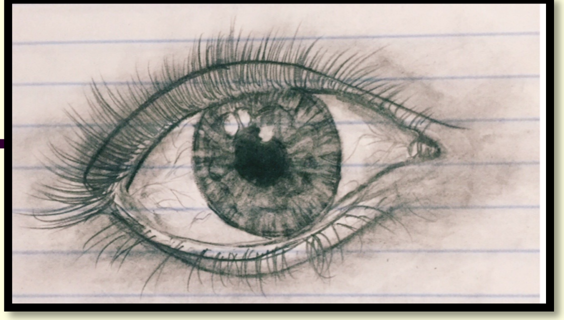


# On the Integrity and Privacy of Biometric Data


Arun Ross

Michigan State University

http://iprobe.cse.msu.edu/

# The iPRoBe Lab

**http://iprobe.cse.msu.edu**

**https://twitter.com/iPRoBeLab**

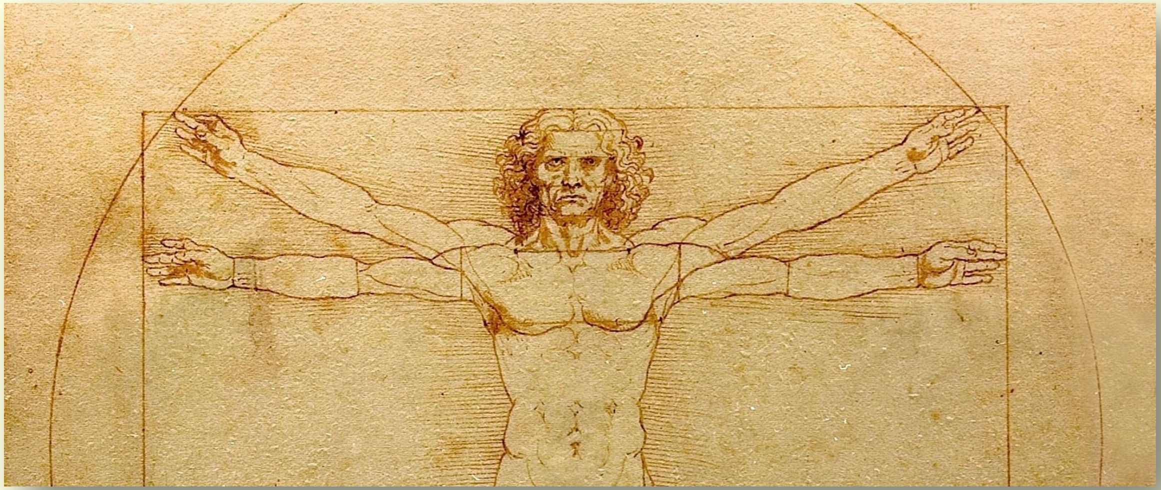

- Integrated Pattern Recognition and Biometrics Lab
- Currently: 8 PhD + 4 MS Students
- Graduated: 26 MS Thesis Students + 11 PhD Students

# Research Theme

- **Adversarial Biometrics**
  - Spoofing Biometric Traits
  - Digitally Altered Biometric Data
  - Degraded Biometric Data
- **Privacy**
  - What Else Does Your Biometric Data Reveal?
  - Privacy Preserving Biometrics
- **Biometric Fusion**
  - Multiple Biometrics | Multispectral Biometrics
  - Biometrics + Demographics

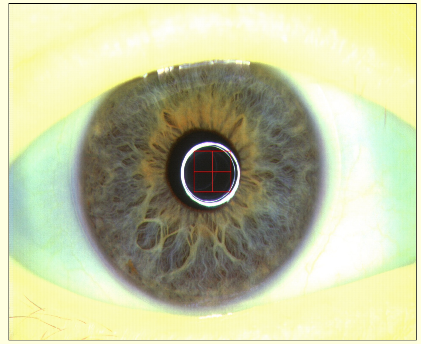
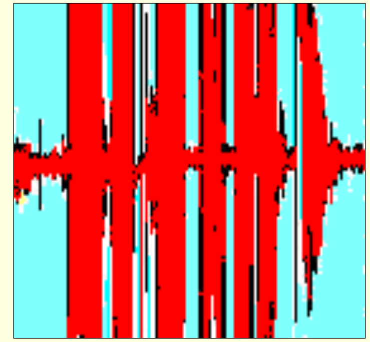
# Biometrics

- Automated recognition of individuals based on their **biological** and **behavioral** characteristics
- Traits from which **distinguishing, repeatable** features can be extracted

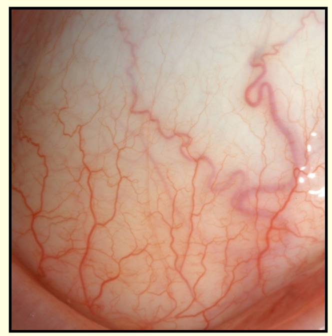


# Biometric Traits












# Biometric Applications

Iris: Health Care

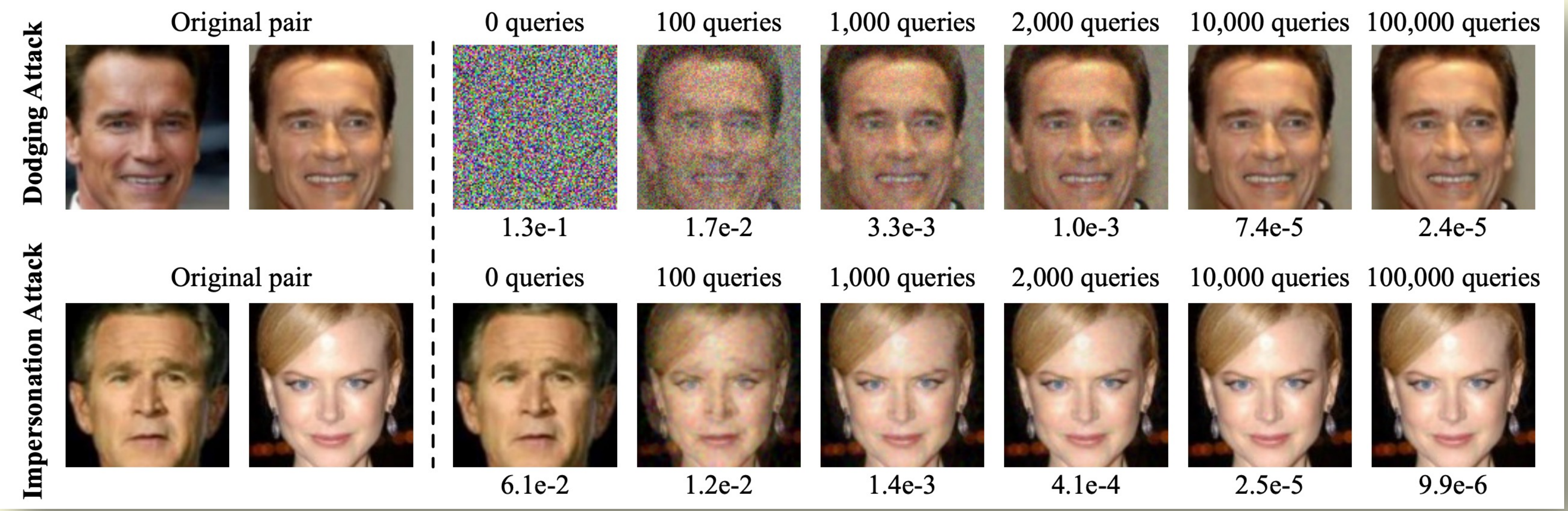
Fingerprint: Refugee Services

Fingerprint: US OBIM

Face: Apple Face ID


Finger Vein: ATMs

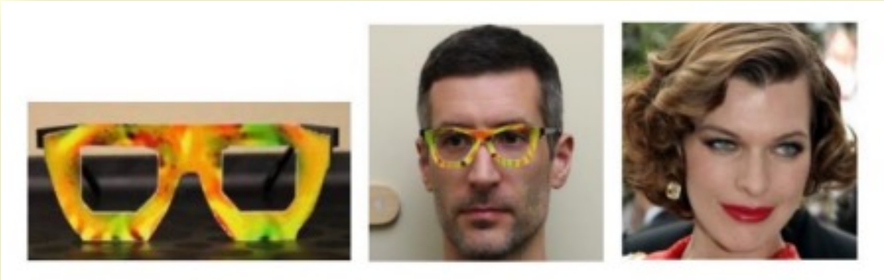
# Altered Data: Blackbox Attacks




Dong et al, "Efficient decision-based black-box adversarial attacks on face recognition", CVPR 2019

# Altered Data: Physical Attacks

- Presentation attacks: face masks
- 3D printed glasses: for dodging and impersonating others
  - Sharif et al., "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition, 2016
- Adversarial patches printed on T-Shirts to evade detectors
  - Thys et al., "Fooling automated surveillance cameras: Adversarial patches to attack person detection," CVPRW 2019



User Target



https://syncedreview.com/2019/04/24/now-you-see-me-now-you-dont-fooling-a-person-detector/

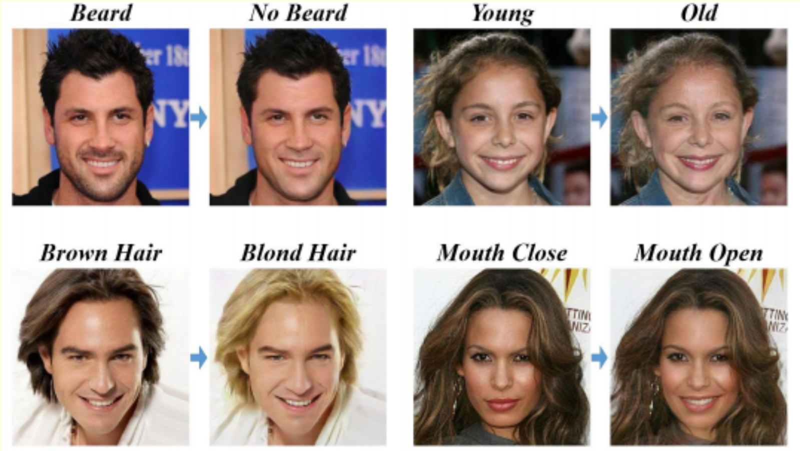
# Real-world Challenges

## Motivation – Why is the focus on biometric images?

- Widespread use of Photoshop and Snapchat filter on face images
- Deep learning-based manipulations are increasingly prevalent (attribute modifications, makeup transfer)

**Media forensics**

https://www.hindawi.com/journals/tswj/2013/795408/

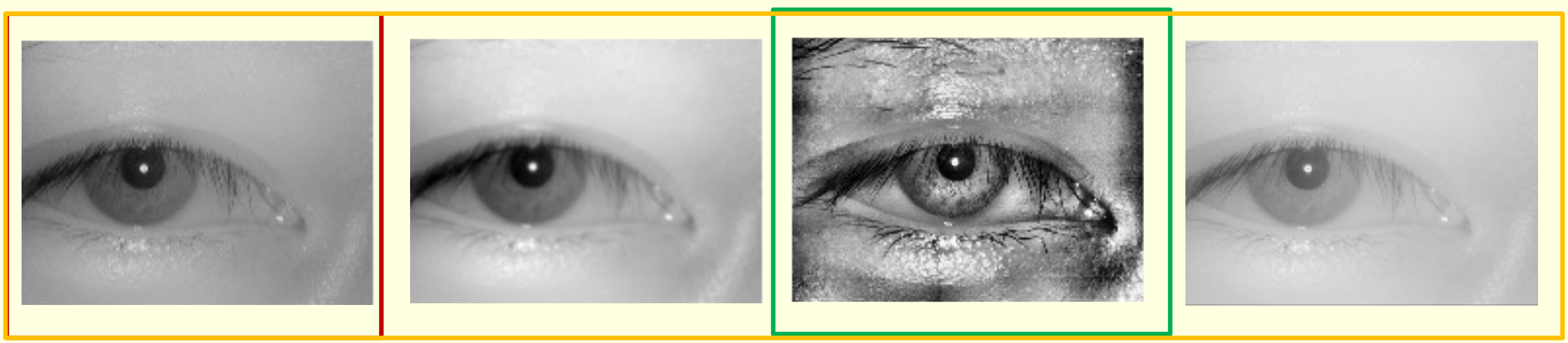



https://arxiv.org/pdf/1711.10678.pdf

https://neurohive.io/en/news/adobe-trained-a-neural-network-that-detects-photoshopped-faces/

# Image Forensics

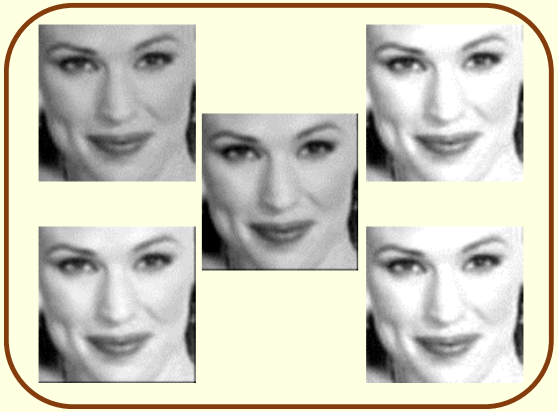
- **Origin:** Which sensor produced this image?
- **Altered:** Is this an altered image?
- **Relationship:** How are these images related?



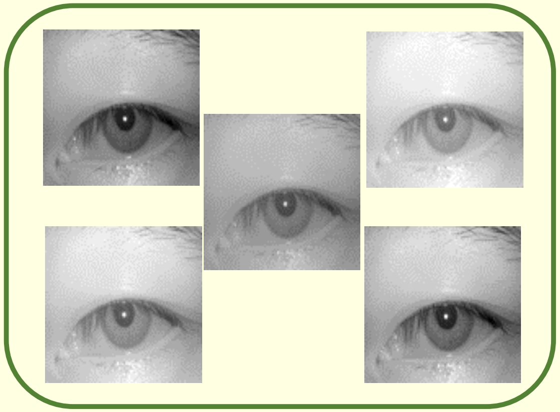
# Digital Data: Near Duplicates

- Near Duplicates: Subtly Modified Images

Brightness adjustment



Gamma transformation

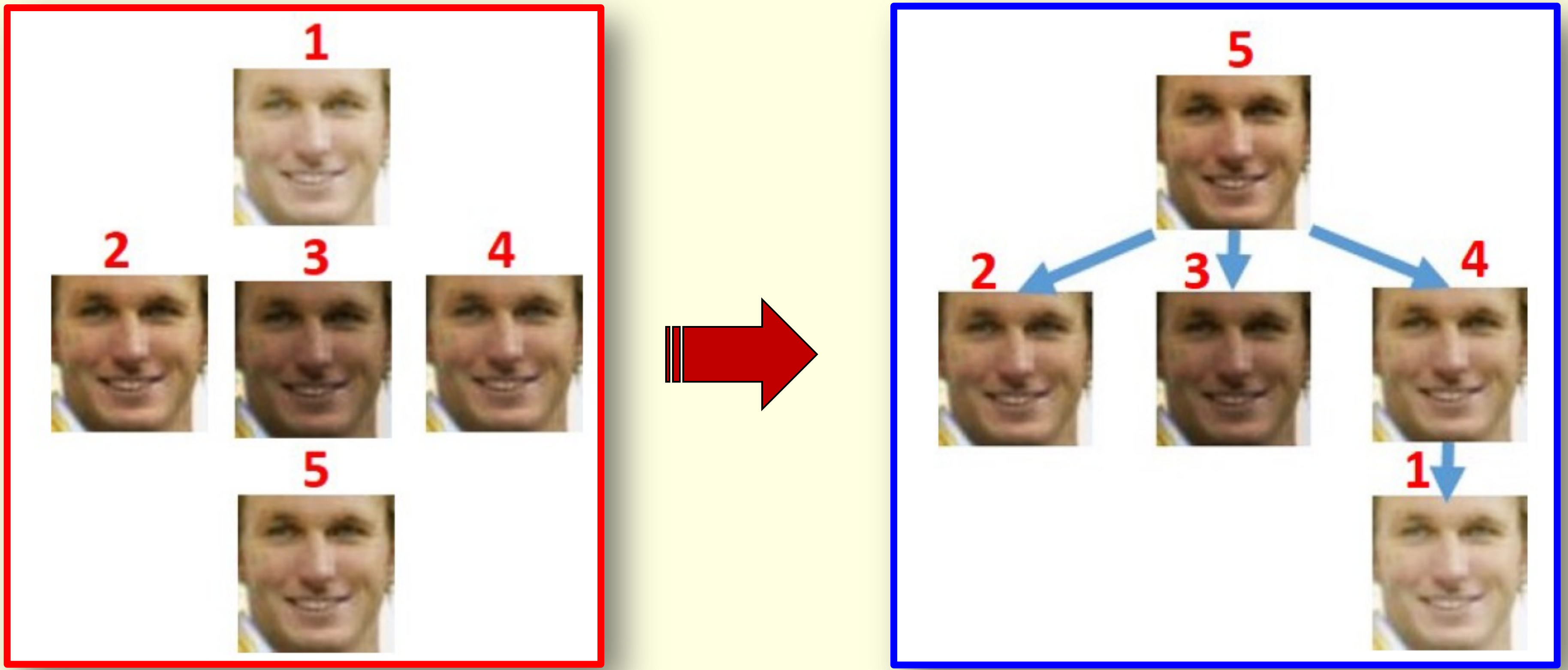


Rotation

S. Banerjee and A. Ross, “Face Phylogeny Tree Using Basis Functions,” IEEE TBIOM, 2020

# Relationship Between Images

- Phylogeny Tree: Relationship between near duplicate images






S. Banerjee and A. Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM, 2020

# Importance of Problem

- Deduce whether a set of photometrically transformed images originated from a single source image or multiple sources
- Detection of image tampering hinted by significant photometric variation between two images
- Determination of transformation parameters relating two images

**Forensics + Data Analysis**

# Image Phylogeny Tree (IPT)

- IPT construction is a 2-step process:
  - STEP I : Computing pairwise asymmetric measure
  - STEP II: Using a tree-spanning algorithm

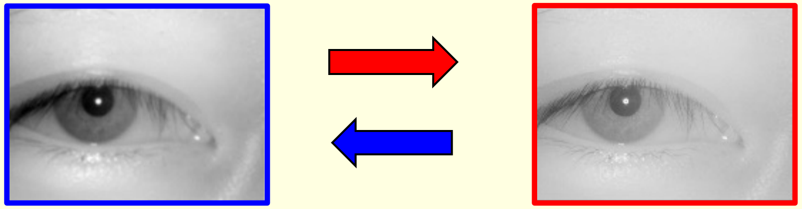

Set of 5 near-duplicate photometrically related images

Compute an asymmetric similarity/dissimilarity matrix depicting pair-wise relationships

Use a tree-spanning algorithm to construct IPT

# What are the Challenges?

- Photometric Transformations ▸ Large number
  - E.g., Brightness, Contrast, CLAHE, Gamma, Median, Gaussian
- Each Transformation ▸ multiple parameters
  - E.g., Gaussian: window size and variance
- Each Parameter ▸ multiple values
  - E.g., Window size: 3x3, 5x5, 9x9, 13x13, ….
- Need to distinguish between A→B and B→A



# Our Approach

- Use a generic parametric transformation function to model the relationship between any two images
- Given two images, **A** and **B**, estimate the parameters of the function in both directions
- Use the likelihood of the parameters to determine which of the two cases is more likely, i.e., **A → B** or **B → A**


- **Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019**
- **Banerjee and Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM 2020**

# Transformation Function

Source image

Parameters

Target image

$$B(u,v) = \mathrm{T}[A(u,v)|\alpha]$$

Transformation Function

# Transformation Function

- Model transformation from $\boldsymbol{A} \rightarrow \boldsymbol{B}$ such that the pair-wise photometric error (PE) is **minimized** for all pixels $p$

$$\min_{\boldsymbol{\alpha}} PE\ (\boldsymbol{A}, \boldsymbol{B}) = \min_{\boldsymbol{\alpha}} \sum_{p=1}^{N} \|\boldsymbol{B}(p) - \tau(\boldsymbol{A}(p); \boldsymbol{\alpha})\|_2^2$$

- We approximate transformations using a set of **basis** functions

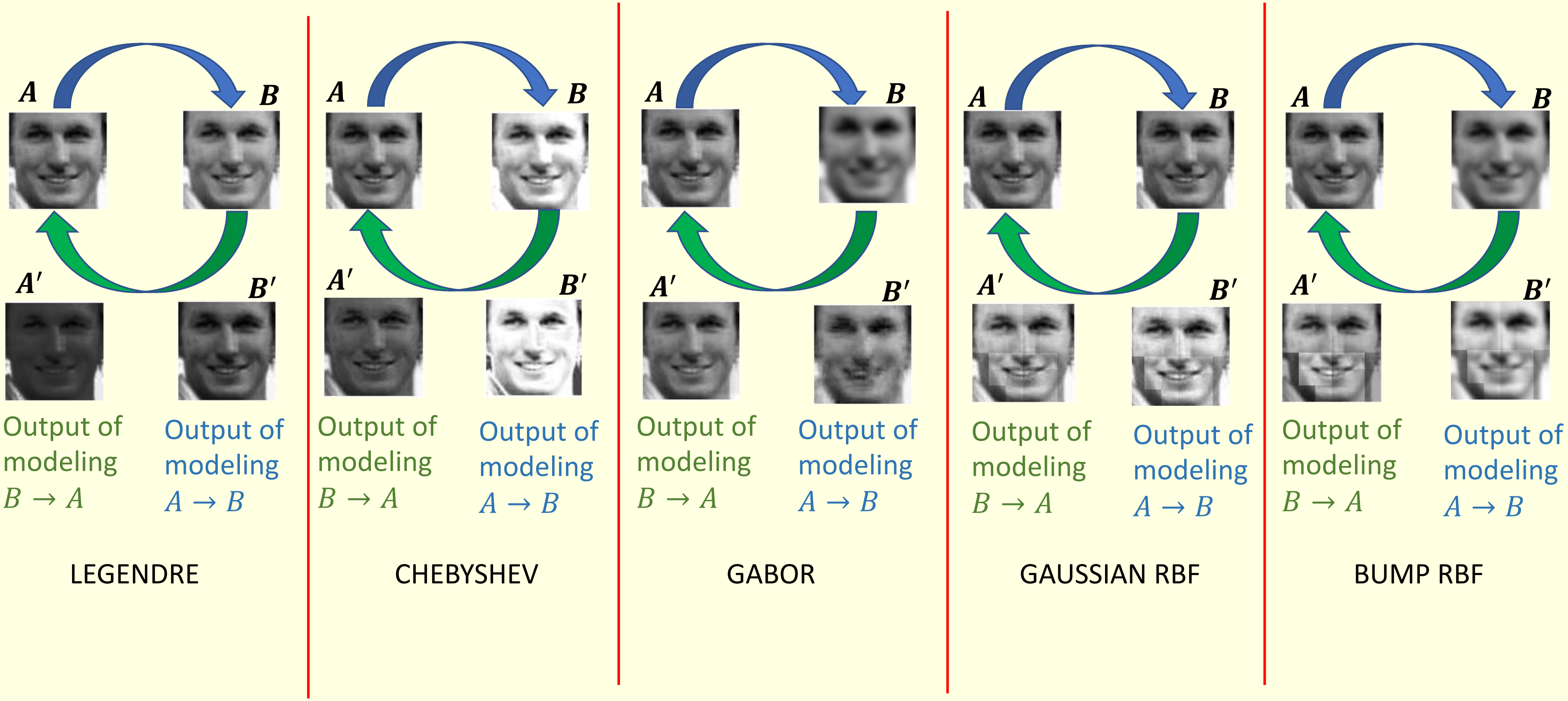
# Basis Functions

| Basis Functions | | Utility | Formulation |
|---|---|---|---|
| Polynomials | Legendre | Used for image template matching and image reconstruction | $L_n(p) = 2^n \sum_{k=0}^{n} p^k \binom{n}{k} \binom{\frac{n+k-1}{2}}{n}$ |
| | Chebyshev | Used for approximating complex functions (spectral convolutions) | $C_n(p) = p^n \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (1 - x^{-2})^k$ |
| Wavelets | Gabor | Used as texture descriptors, acts as bandpass filters | $\varphi(p, \theta, \lambda) = g(p, \lambda) \cdot w(p, \theta)$ <br> $\lambda = \{2, 3, 4, 5\};\ \theta = \{0^\circ, 45^\circ, 90^\circ, 135^\circ\}$ |
| Radial Basis Functions | Gaussian | Used for interpolation | $K(p) = exp\|p - \mu\|^2$ |
| | Bump | Used as smooth cutoff functions | $K(p) = exp\left(-\frac{1}{1 - p^2}\right)$ |

$p$: *Pixel intensity value* ; $n$: *Polynomial order* ; $\mu$: *Mean pixel intensity value* ; $\lambda$: *Scale* ; $\theta$: *Orientation*

**Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019**

# Basis Functions




- Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019
- Banerjee and Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM 2020

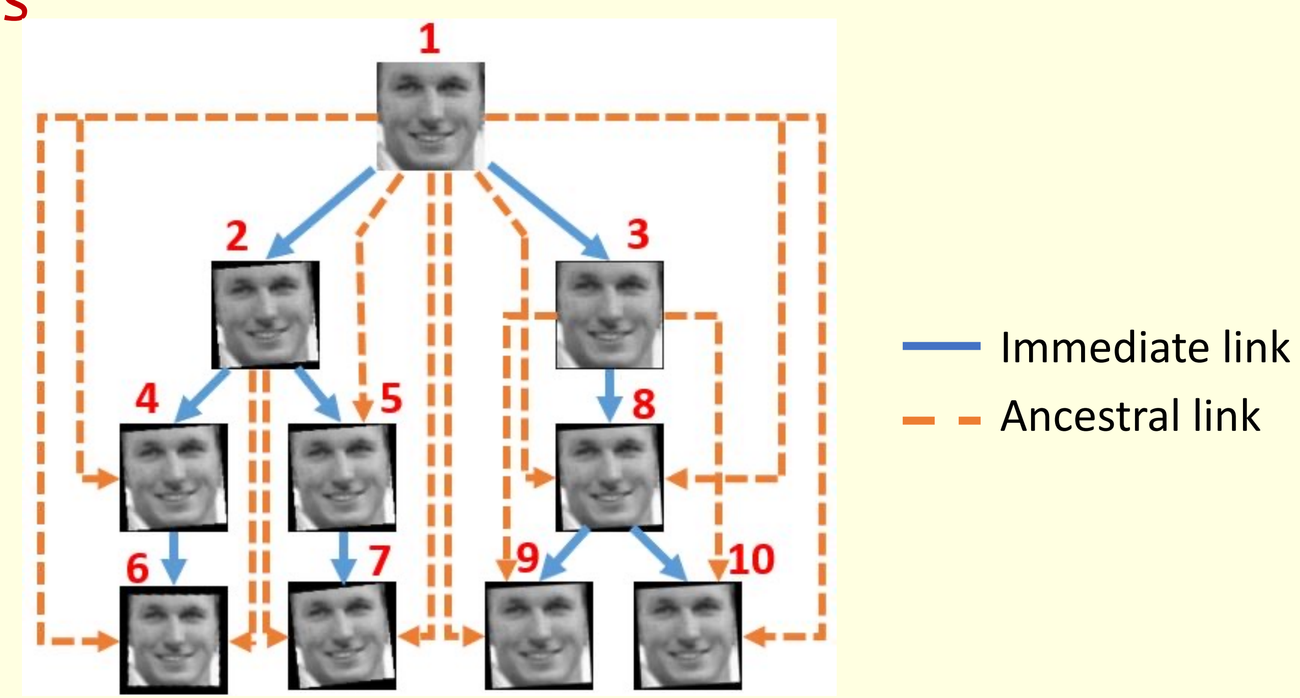
# Asymmetric Measure

- Modeling the transformation in both directions results in two estimated parameter vectors $(\boldsymbol{\alpha}, \boldsymbol{\beta})$
- Compute the likelihood ratio $\left(\boldsymbol{\Lambda}_{\alpha} = \frac{p_f(\boldsymbol{\alpha})}{p_r(\boldsymbol{\alpha})}, \boldsymbol{\Lambda}_{\beta} = \frac{p_f(\boldsymbol{\beta})}{p_r(\boldsymbol{\beta})}\right)$ of the estimated parameters to obtain asymmetric measure
- Use depth first search to construct IPT


- **Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019**
- **Banerjee and Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM 2020**

# Experiments

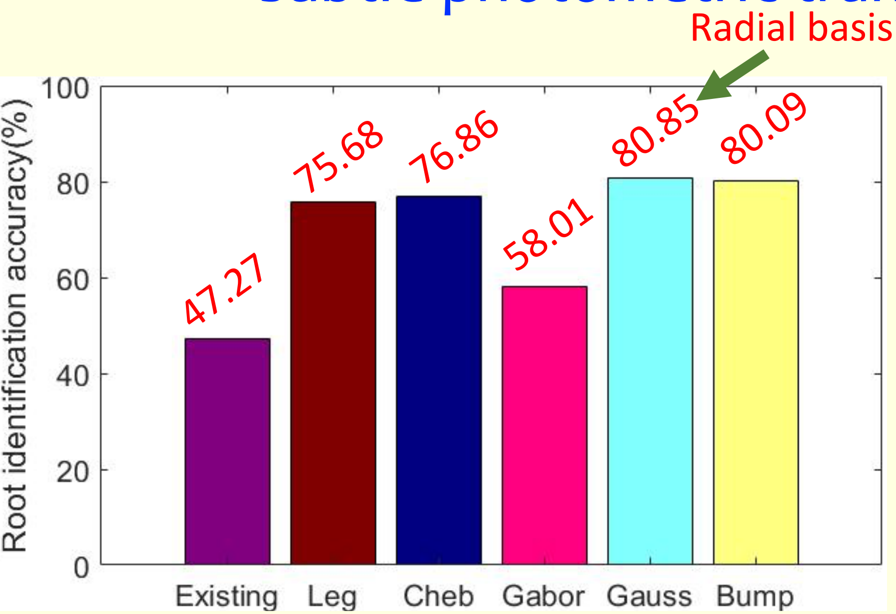
- We generated 2,727 IPTs by subjecting face images to random sequence of 4 transformations resulting in 27,270 images

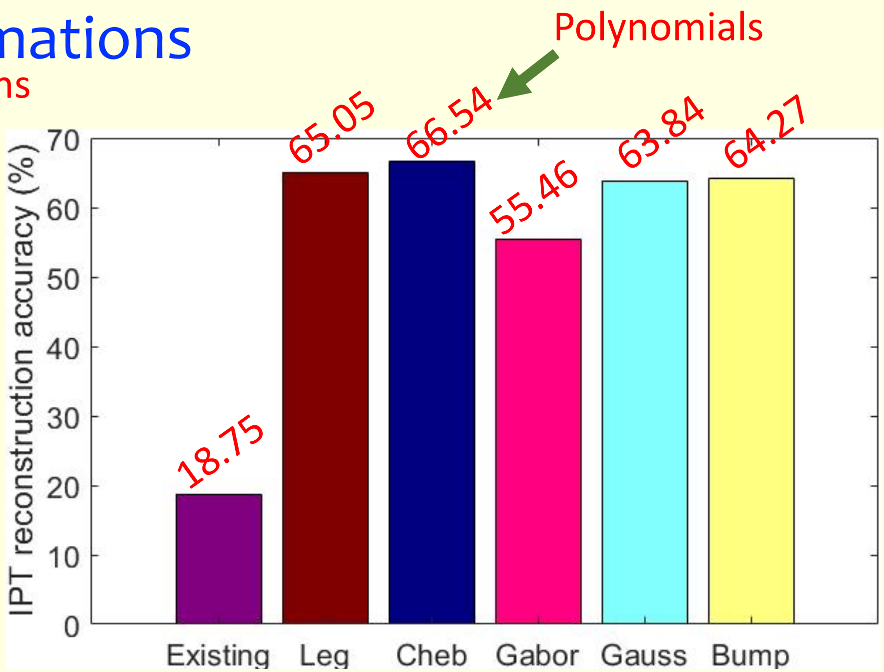



- **Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019**
- **Banerjee and Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM 2020**

# Performance

- We compared the performance with an existing method
- The problem is a very challenging one:
  - face images vs natural scenes
  - subtle photometric transformations




**ROOT IDENTIFICATION** **IPT RECONSTRUCTION**



Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019

# Generalizability

- **Unseen modalities:** 7,260 near-duplicate iris images from CASIA Iris V2 Device 2 dataset
- **Unseen transformations:** 175 near-duplicates using Photoshop and 1,080 near-duplicates using deep learning-based transformations

| Experimental Settings | | Root identification accuracy (%) | IPT reconstruction accuracy (%) |
|---|---|---|---|
| **Unseen modality** | Iris | 95 | 68 |
| **Unseen transformations** | Photoshop | 90 | 100 |
| | Deep learning-based | 83 | 65 |


- Banerjee and Ross, "Face Phylogeny Tree: Deducing Relationships Between Near-Duplicate Face Images Using Legendre Polynomials and Radial Basis Functions," BTAS 2019
- Banerjee and Ross, "Face Phylogeny Tree Using Basis Functions," IEEE TBIOM 2020

# Digital Data: DeepFakes

- DeepFakes: Synthetically Generated Images

https://thispersondoesnotexist.com/

# DeepTalk: Speech Synthesis

## Why do we need DeepTalk?

DeepTalk lets you choose...

You want to listen to...


Morning News


Weather Update


Audiobook

From your smart speaker...

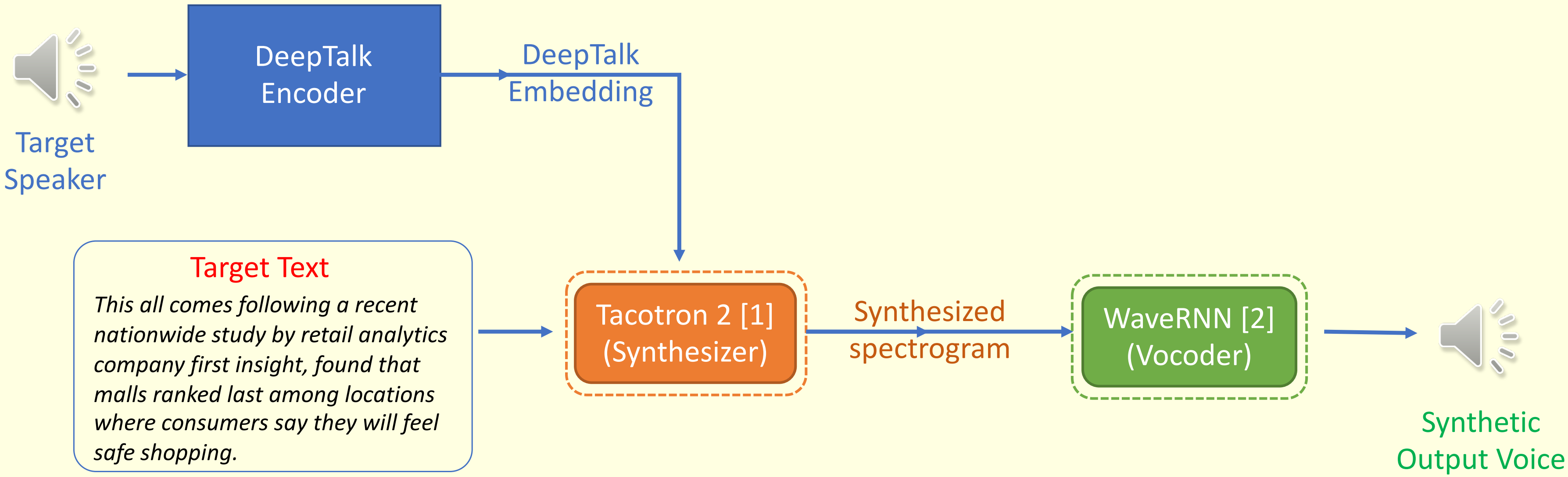
The voice of your favorite Newscaster

**To deliver all your media content**

All images taken from https://pixabay.com/

Chowdhury et al., "DeepTalk: Vocal Style Encoding for Speaker Recognition and Speech Synthesis,", ICASSP 2021

# DeepTalk: Speech Synthesis




[1] Skerry-Ryan et al. "Towards end-to-end prosody transfer for expressive speech synthesis with tacotron." *arXiv preprint arXiv:1803.09047* (2018).
[2] Shen et al. "Natural TTS synthesis by conditioning wavenet on mel spectrogram predictions." In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 4779-4783. IEEE, 2018.

**Chowdhury et al., "DeepTalk: Vocal Style Encoding for Speaker Recognition and Speech Synthesis,", ICASSP 2021**

# DeepTalk: Speech Synthesis

**News Article**

***This all comes following a recent nationwide study by retail analytics company first insight, found that malls ranked last among locations where consumers say they will feel safe shopping.***

Original Voice of Hannah

DeepTalk generated voice of Hannah after Phase 1

**DeepTalk generated voice of Hannah after Phase 2**

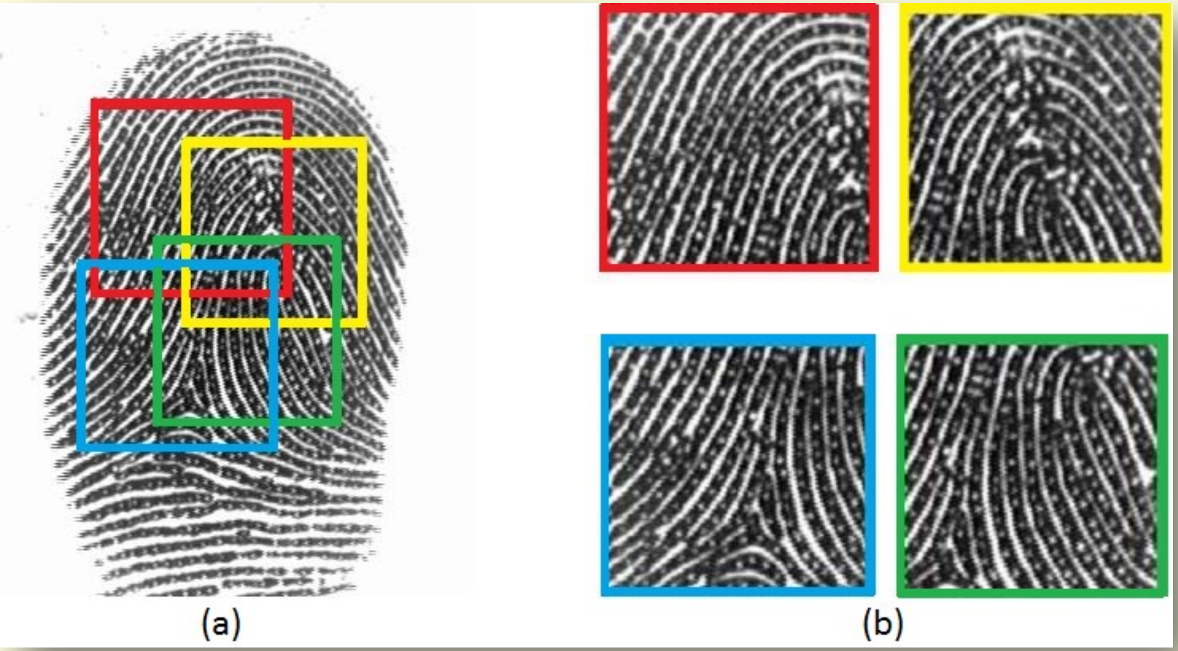
Original Voice of Ted

DeepTalk generated voice of Ted after Phase 1

**DeepTalk generated voice of Ted after Phase 2**

**Chowdhury et al., "DeepTalk: Vocal Style Encoding for Speaker Recognition and Speech Synthesis,", ICASSP 2021**

# Partial Fingerprints




- Small sensors | Capture a limited portion of full finger
- Multiple partial fingerprints are captured | Enroll multiple fingers
- Access granted if the sensed partial fingerprint matches any one of the partial fingerprint of any enrolled finger

# MasterPrints!

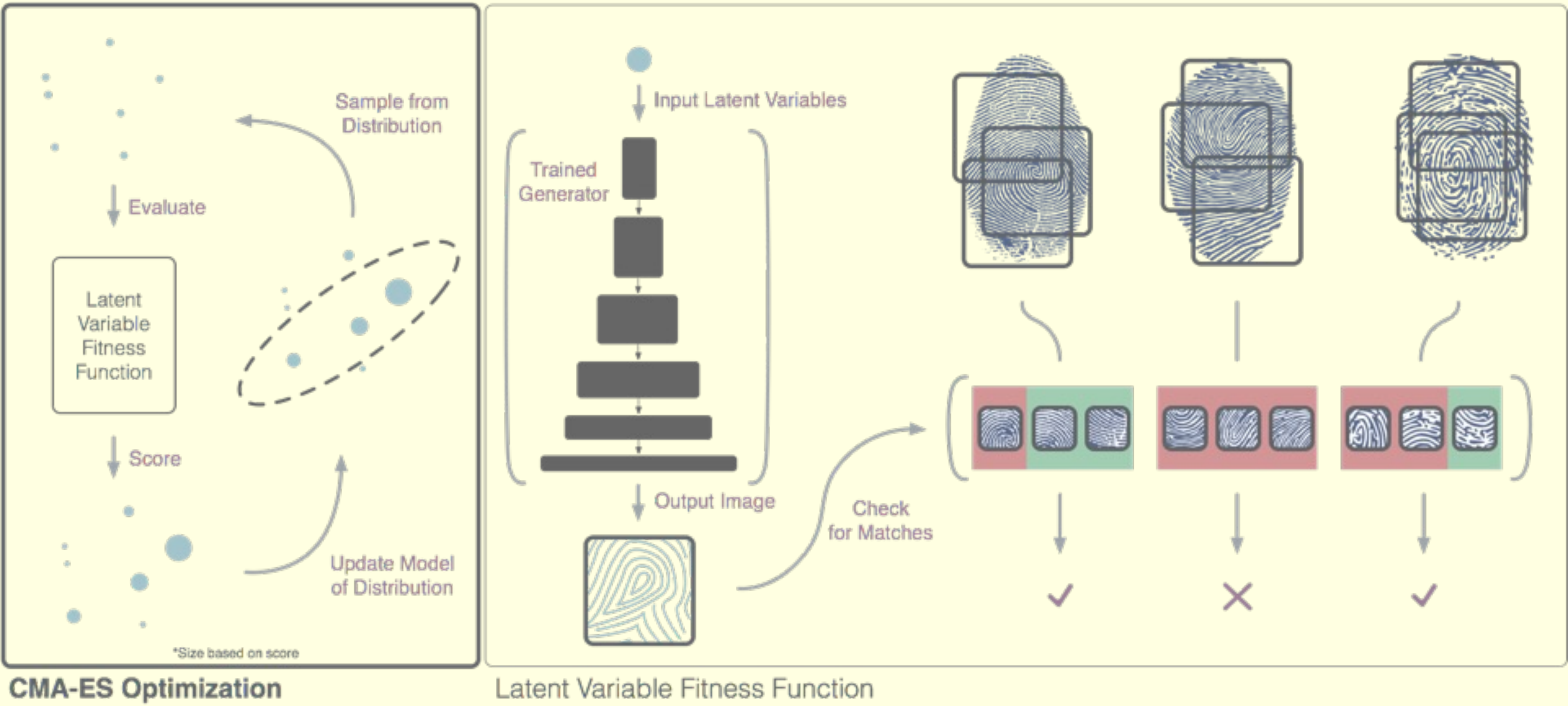
- Fingerprints that match with a large proportion of the fingerprint population
- Could be either full prints or partial prints

**Roy, Memon, Ross, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems," TIFS 2017**

# “MasterPrints”

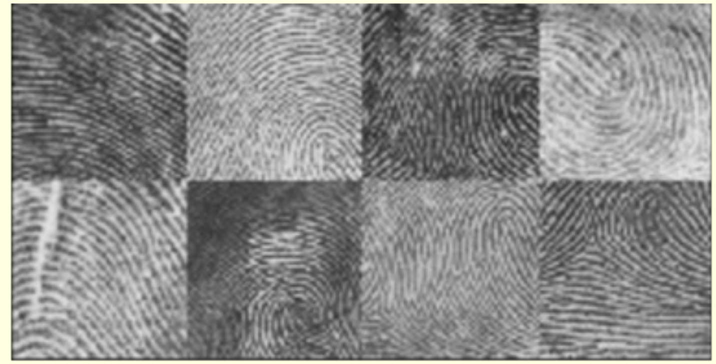
Roy, Memon, Ross, “MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems,” TIFS 2017

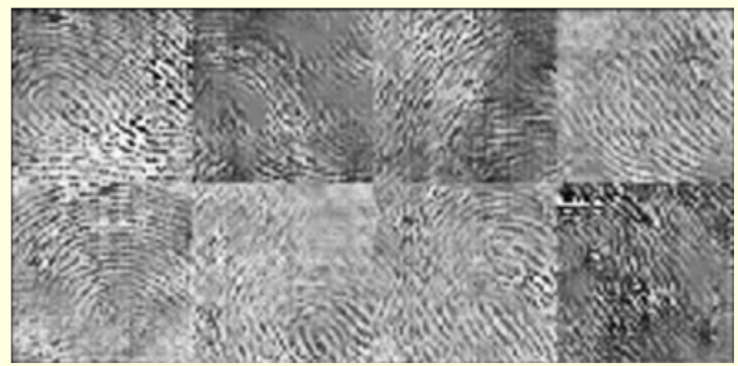
# Latent Variable Evolution




Bontrager et al., "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution," BTAS 2018

# GAN-based DeepMasterPrints





Increases vulnerability of small sensors to dictionary and spoof attacks

**Bontrager et al., "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution," BTAS 2018**

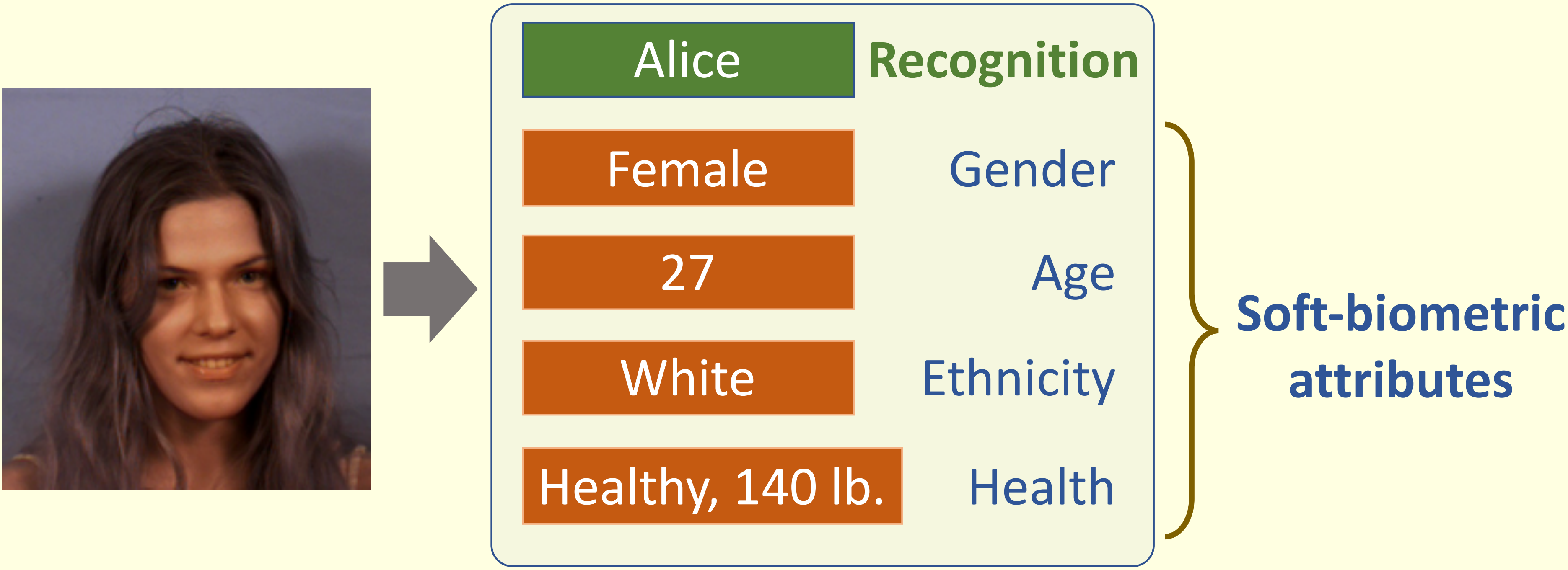
# Attack Success Rate

| | 0.01% FMR | 0.1% FMR | 1% FMR |
|---|---|---|---|
| Single MasterPrint | 1.88% | 6.60% | 33.40% |
| Multiple MasterPrints | 6.88% | 30.69% | 77.92% |
| Single DeepMasterPrint | **1.11%** | **22.50%** | **76.67%** |

**Experiments on FingerPass DB7 Dataset using VeriFinger Matcher**

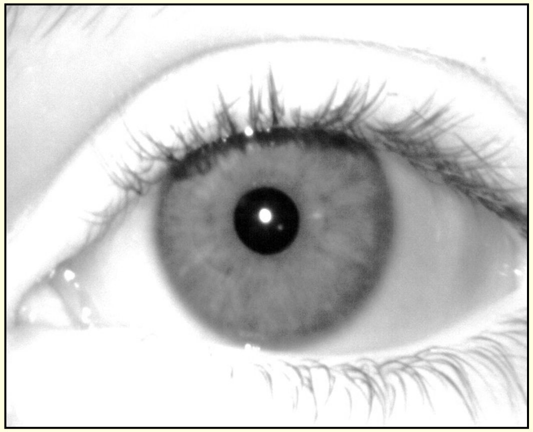
**Bontrager et al., "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution," BTAS 2018**

# Soft Biometrics




- Age, Gender, Ethnicity, can be **automatically derived** from the face image
- That is, a **trained classifier or a regressor** may be used to automatically deduce certain soft biometric attributes

# Biometrics + Forensics



- Subject is a Male (90% Confidence), White (85% Confidence)
- Image taken using an Aoptix camera
- Iris stroma is plain textured
- Highly constricted pupil suggests strong ambient illumination

**Bridges the gap between human and machine description of data**

**OR**

**Compromises privacy?**

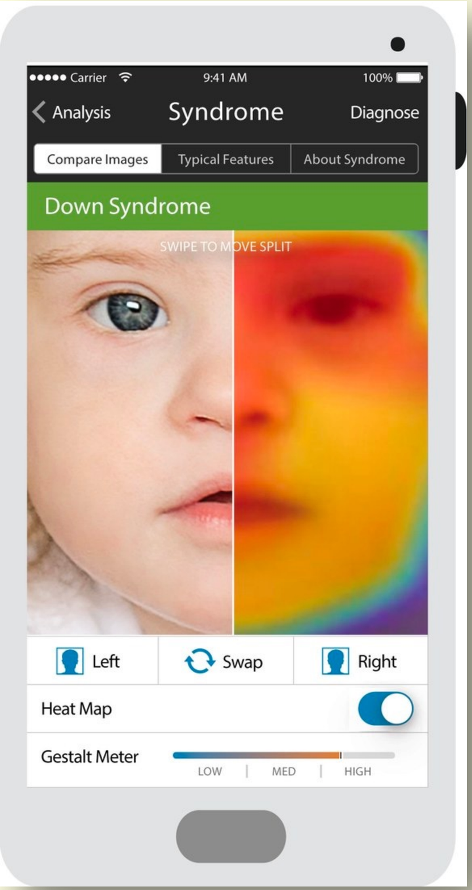
# Face2Gene

MEGAN MOLTENI SCIENCE 01.09.17 01:00 PM

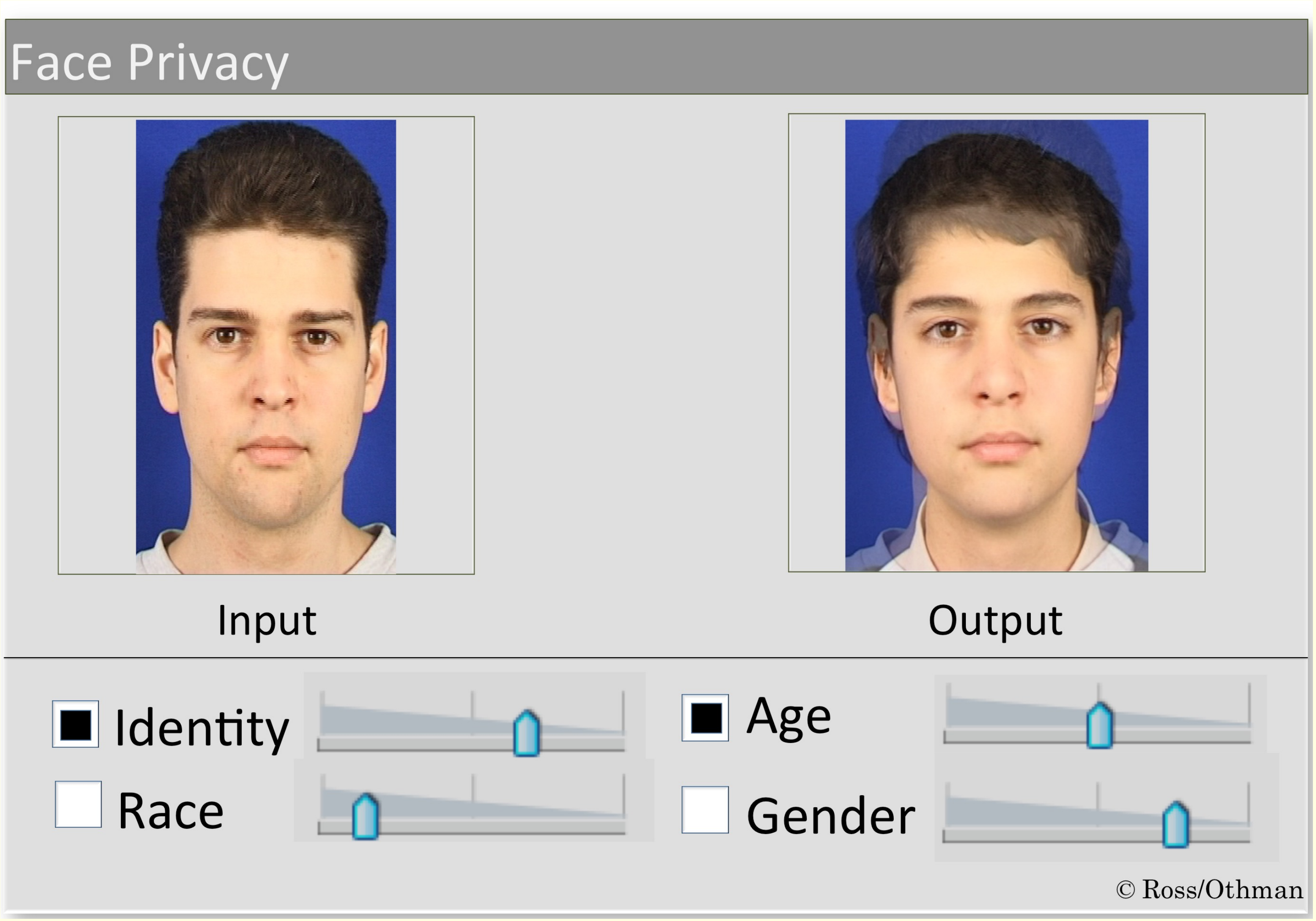
## THANKS TO AI, COMPUTERS CAN NOW SEE YOUR HEALTH PROBLEMS

"In hindsight it was all clear to me," says Gripp, who is chief of the Division of Medical Genetics at A.I. duPont Hospital for Children in Delaware, and had been seeing the patient for years. "But it hadn't been clear to anyone before." What had taken Patient Number Two's doctors 16 years to find took Face2Gene just a few minutes.

Face2Gene is a suite of phenotyping applications that facilitate comprehensive and precise genetic evaluations.



# Controllable Privacy

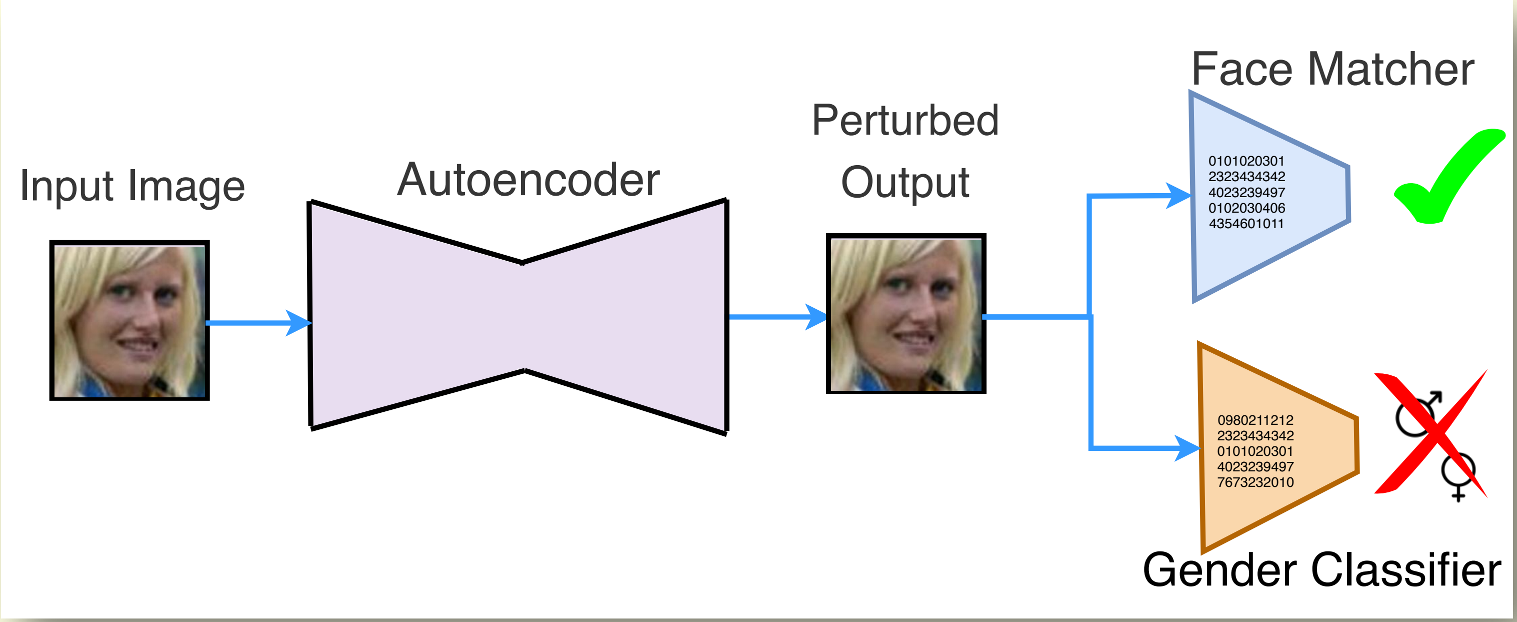





Othman and Ross, "Privacy of Facial Soft Biometrics," ECCVW 2014

# Semi-Adversarial Networks (SAN)

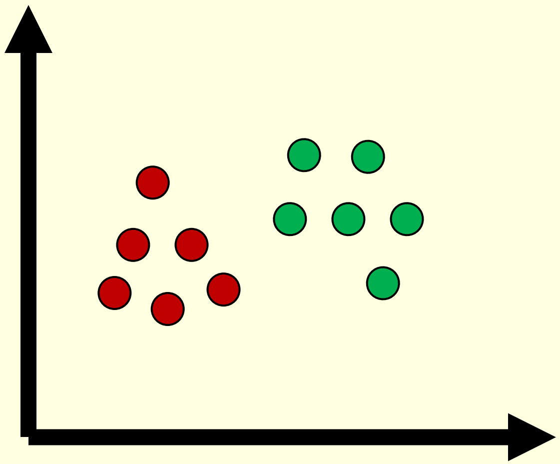
- Design a transformation model to:
  - Confound gender attribute ➔ gender classifiers will not work
  - Retain recognition capability ➔ face matchers will still work



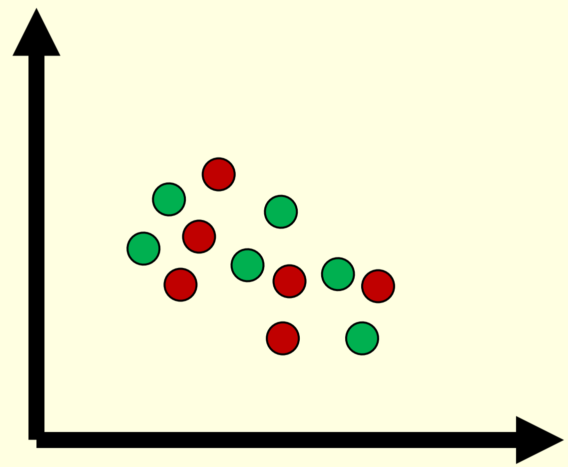

Mirjalili et al., Semi-Adversarial Networks: Convolutional Autoencoders for Imparting Privacy to Face Images, ICB 2018

# Semi-Adversarial Networks (SAN)

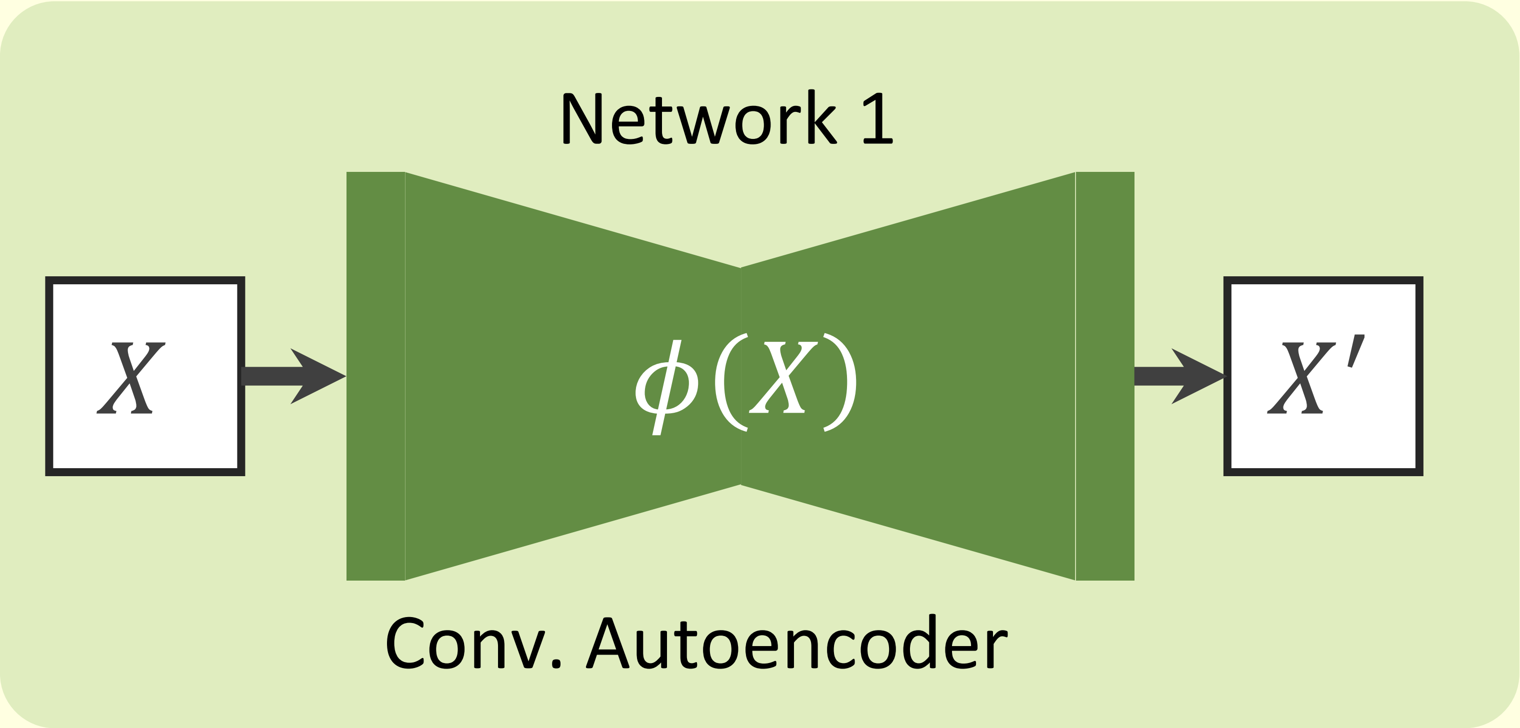
**Original Image Space**



**Transformed Image Space**

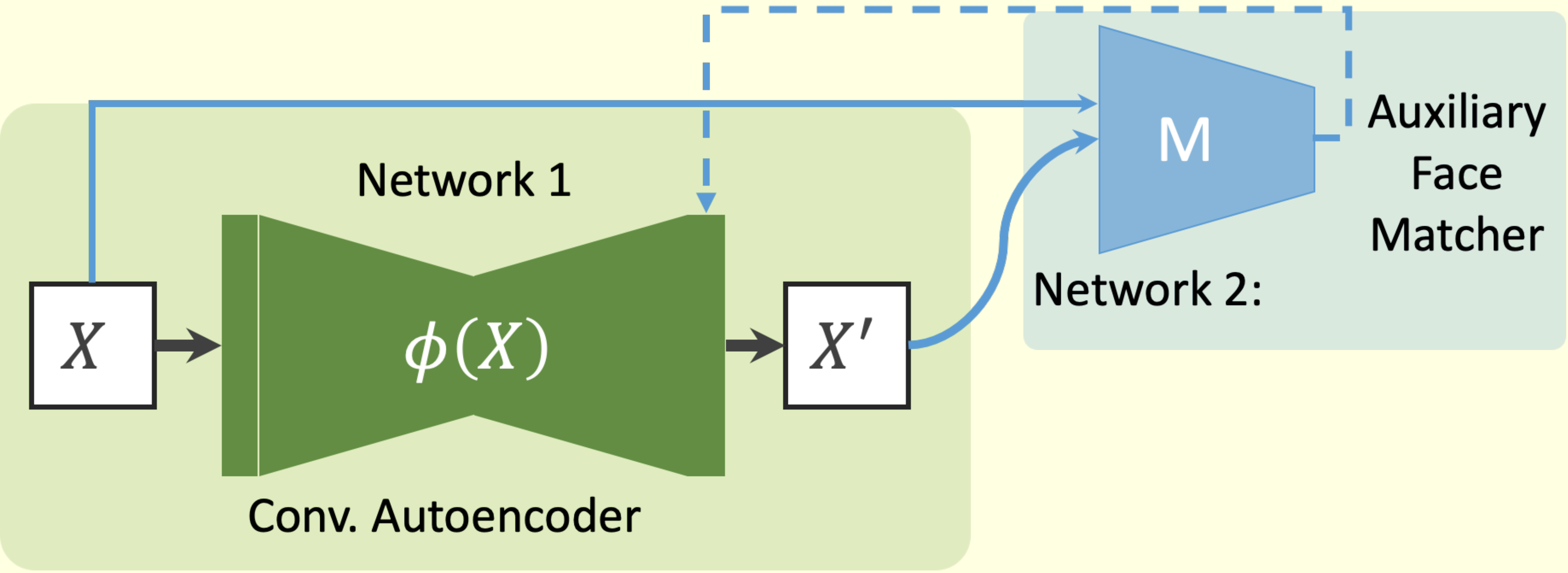


# General Architecture of SAN Model



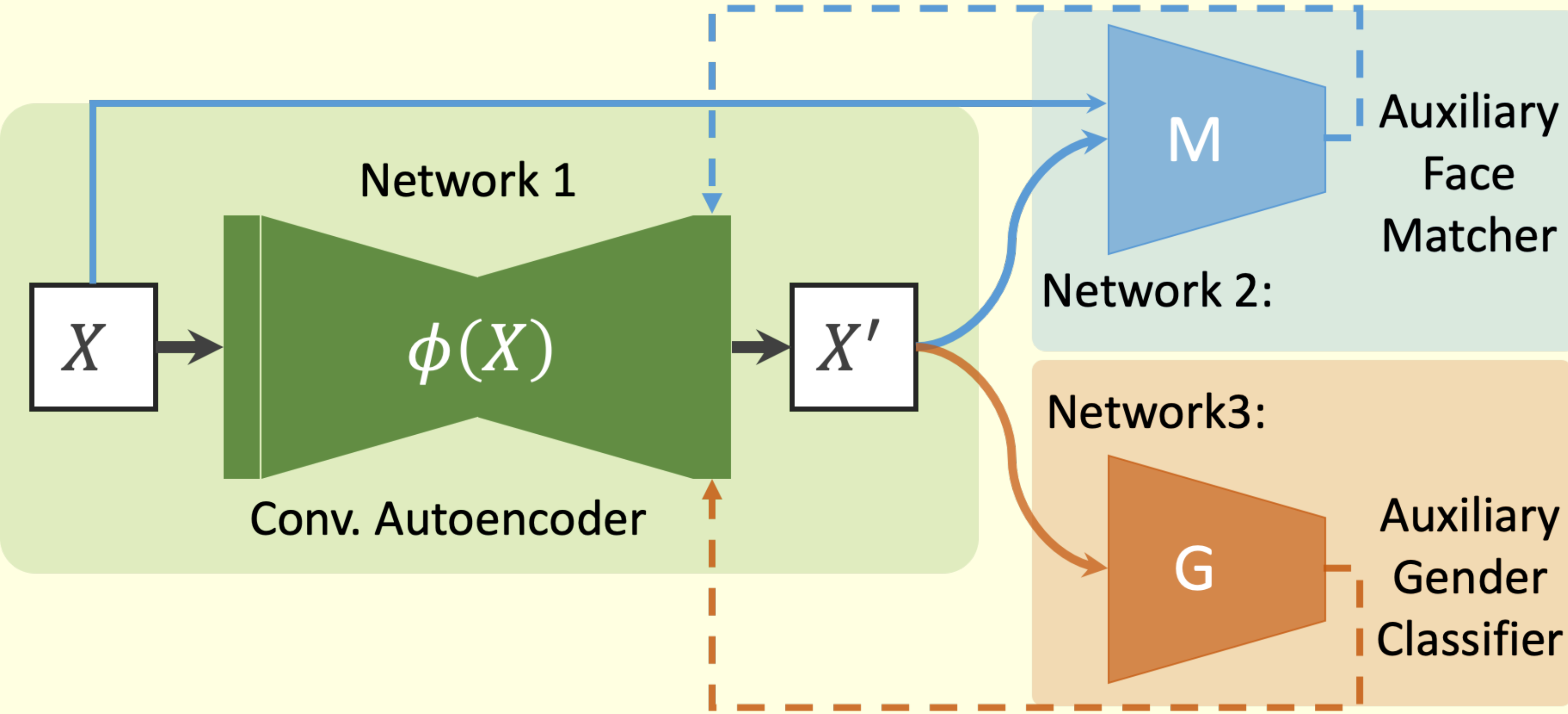

Mirjalili et al., Semi-Adversarial Networks: Convolutional Autoencoders for Imparting Privacy to Face Images, ICB 2018

# General Architecture of SAN Model



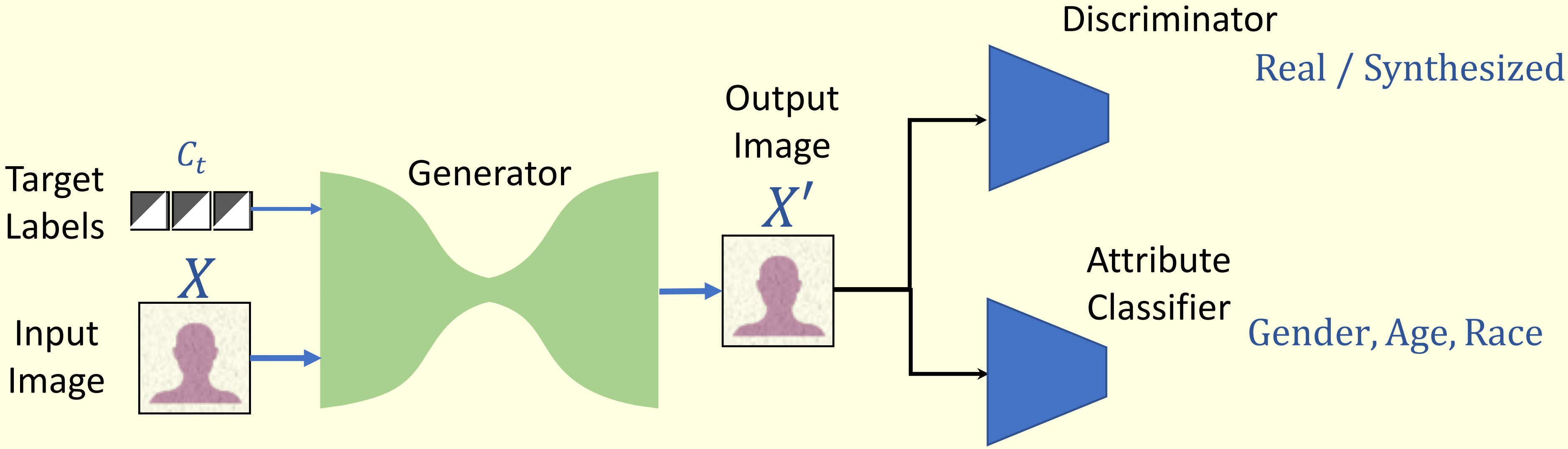

Mirjalili et al., Semi-Adversarial Networks: Convolutional Autoencoders for Imparting Privacy to Face Images, ICB 2018

# General Architecture of SAN Model



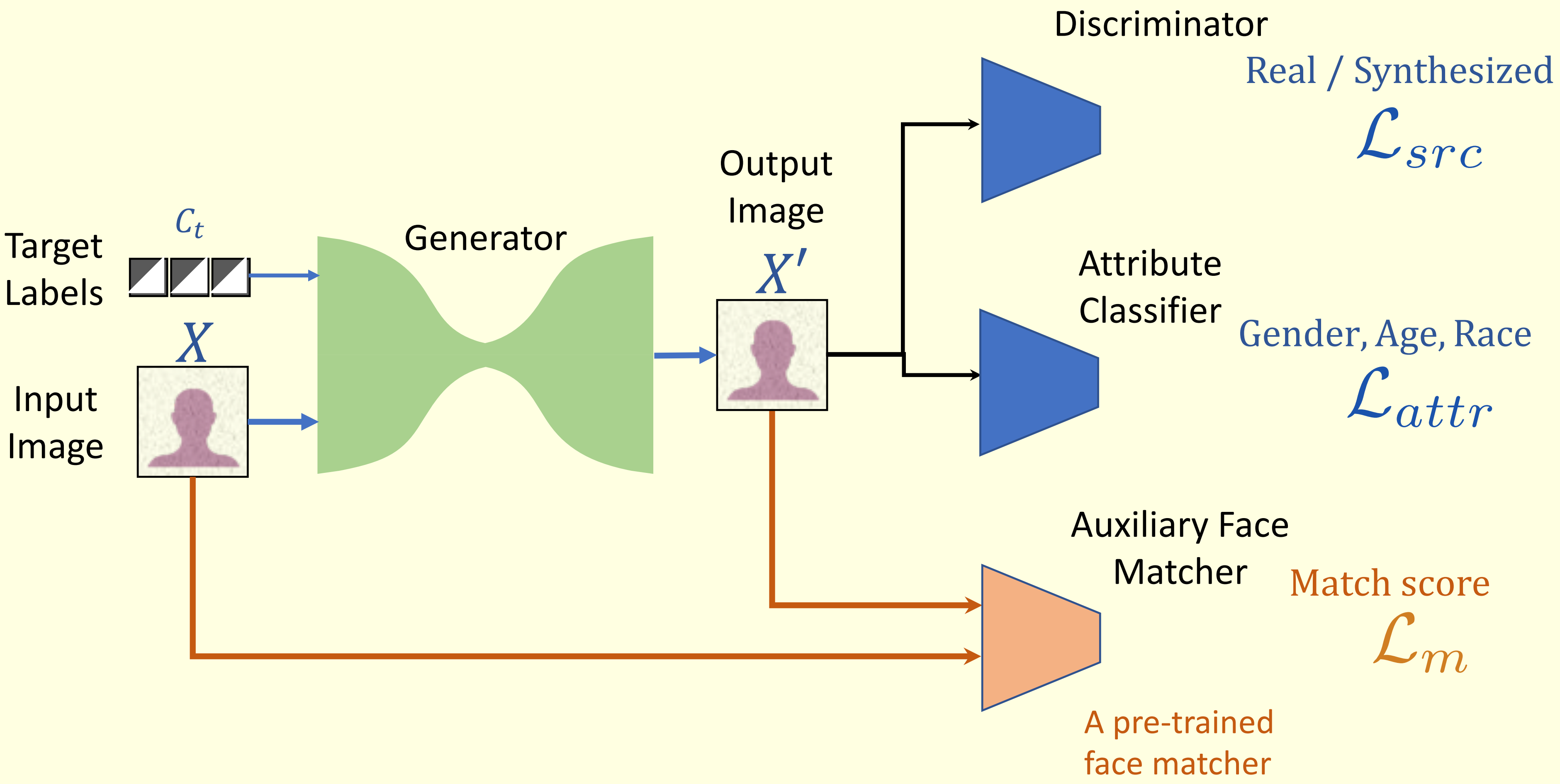

Mirjalili et al., Semi-Adversarial Networks: Convolutional Autoencoders for Imparting Privacy to Face Images, ICB 2018

# Multi-attribute Privacy




- ❑ Input image $X$ from original label $c_0$
- ❑ A regular cycle-GAN that generates output image $X'$ for a given input image $X$ and target label vector $c_t$.

# Multi-attribute Privacy




- ❑ Auxiliary Face Matcher derives the matching-loss term to ensure that the output image X' matches with input X.

# PrivacyNet: Loss Functions

- Losses for training the discriminator $D_{src}$ and $D_{attr}$:

  1. Source term (real vs. synthesized)

$$\mathcal{L}_{D,src} = \mathbb{E}_X \left[-\log(D_{src}(X))\right] + \mathbb{E}_{X,c_t} \left[-\log(1 - D_{src}(G(X, c_t)))\right]$$

  2. Attribute term

$$\mathcal{L}_{D,attr} = \mathbb{E}_{X,c_0} \left[-\log(D_{attr}(c_0|X))\right]$$

- Losses for training the generator $G(X, c_t)$:

  1. Source term

$$\mathcal{L}_{G,src} = \mathbb{E}_{X,c_t} \left[\log(D_{src}(G(X, c_t)))\right]$$

  2. Attribute term

$$\mathcal{L}_{G,attr} = \mathbb{E}_{X,c_t} \left[-\log(D_{attr}(c_t|G(X, c_t)))\right]$$

  3. Matching term

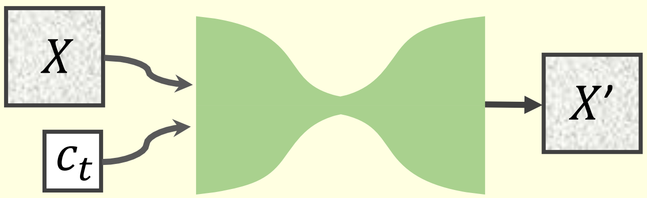
$$\mathcal{L}_{G,m} = \mathbb{E}_{X,c_t} \left[\|R(X) - R(G(X, c_t))\|_2^2\right]$$

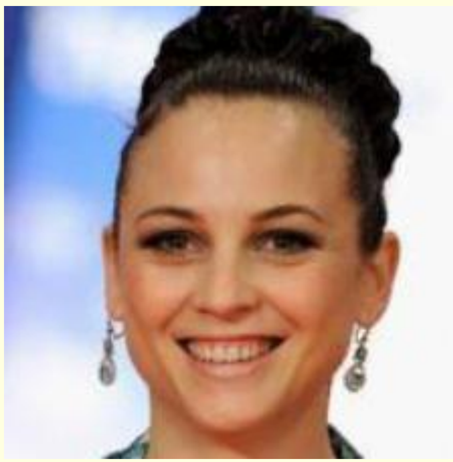
  4. Reconstruction loss (cycle-consistency)

$$\mathcal{L}_{rec} = \mathbb{E}_{X,c_0,c_t} \left[\|X - G(G(X, c_t), c_0)\|_1\right]$$

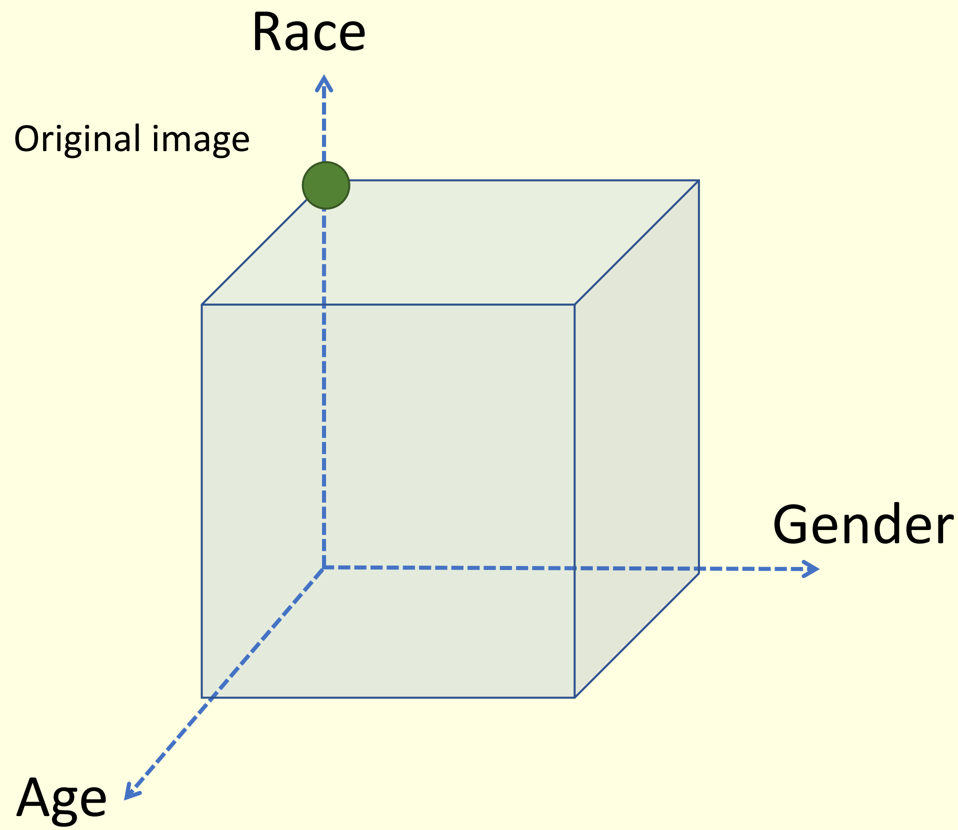
Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet



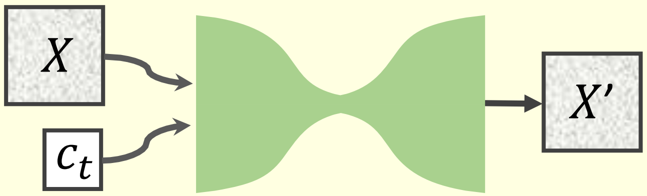
Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]





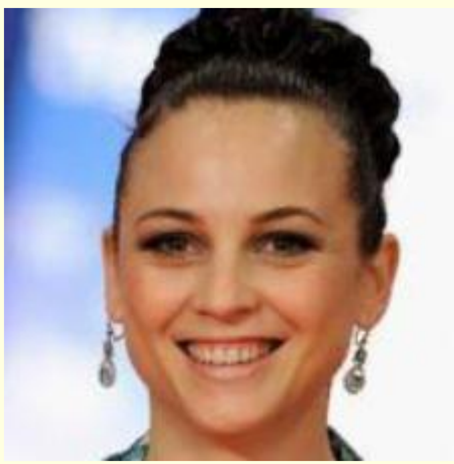

Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet

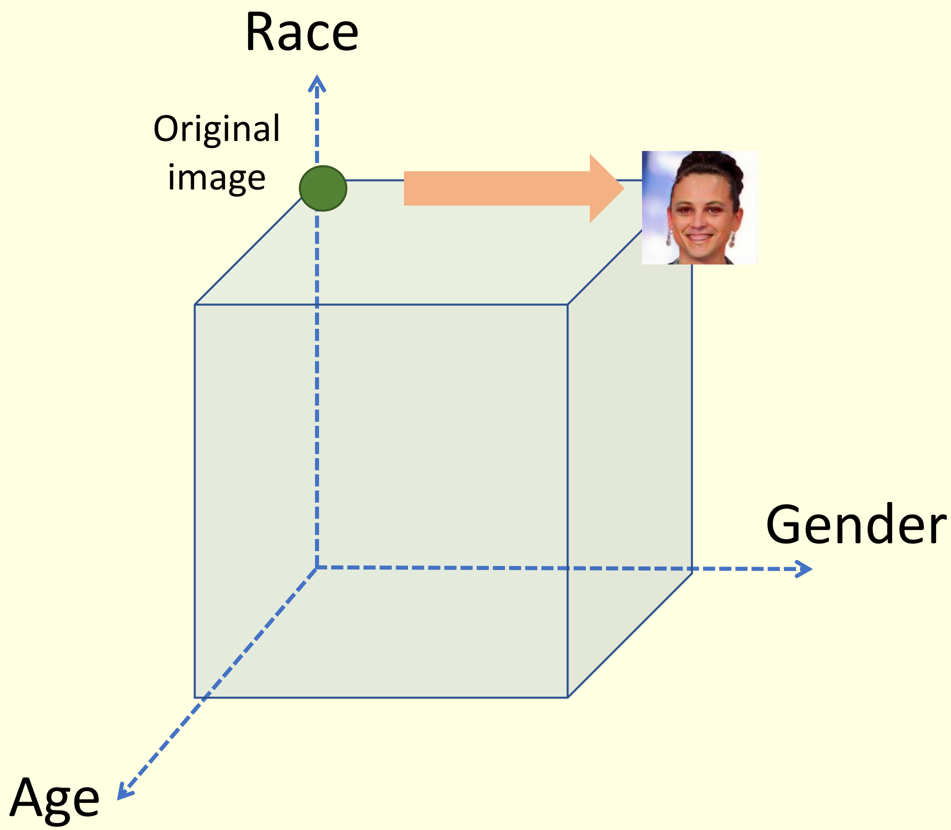



$c_t$

[Male, Mid-age, Cauc.]



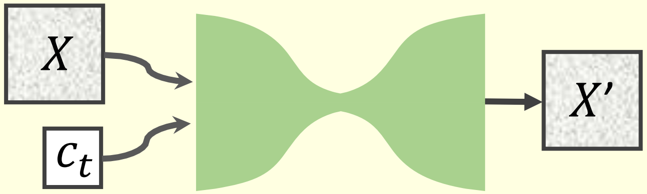
Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet

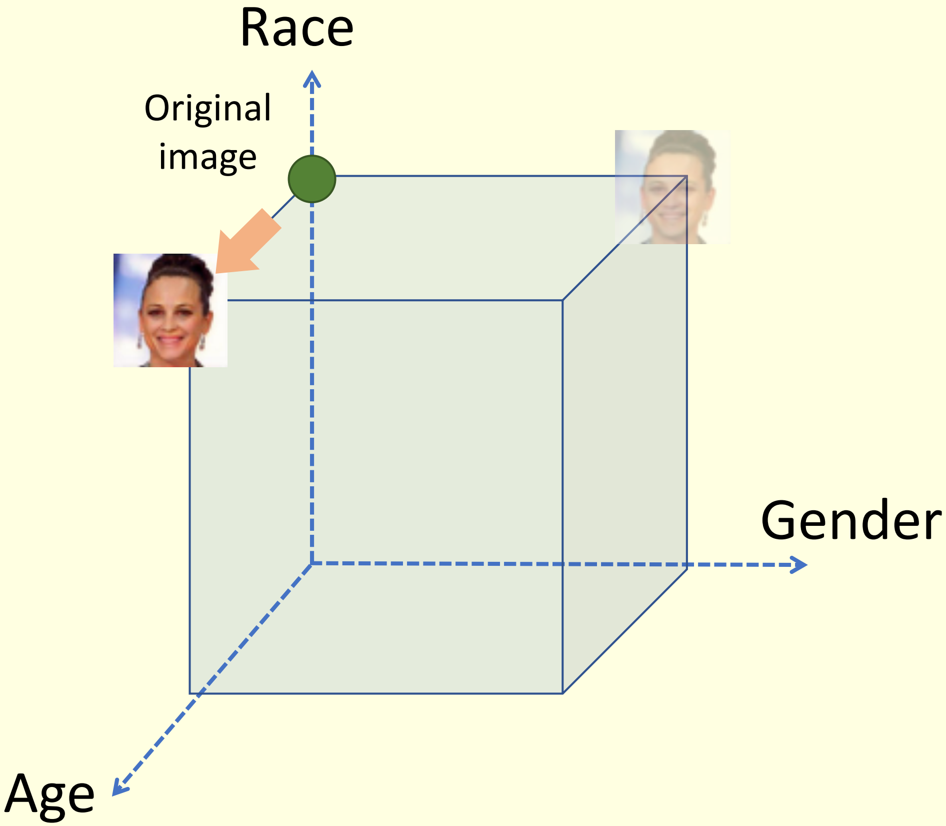



$\boldsymbol{c_t}$

[Male, Mid-age, Cauc.]

**[Female, Old, Cauc.]**

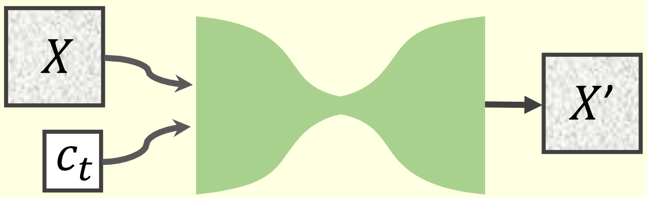
Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet




$c_t$

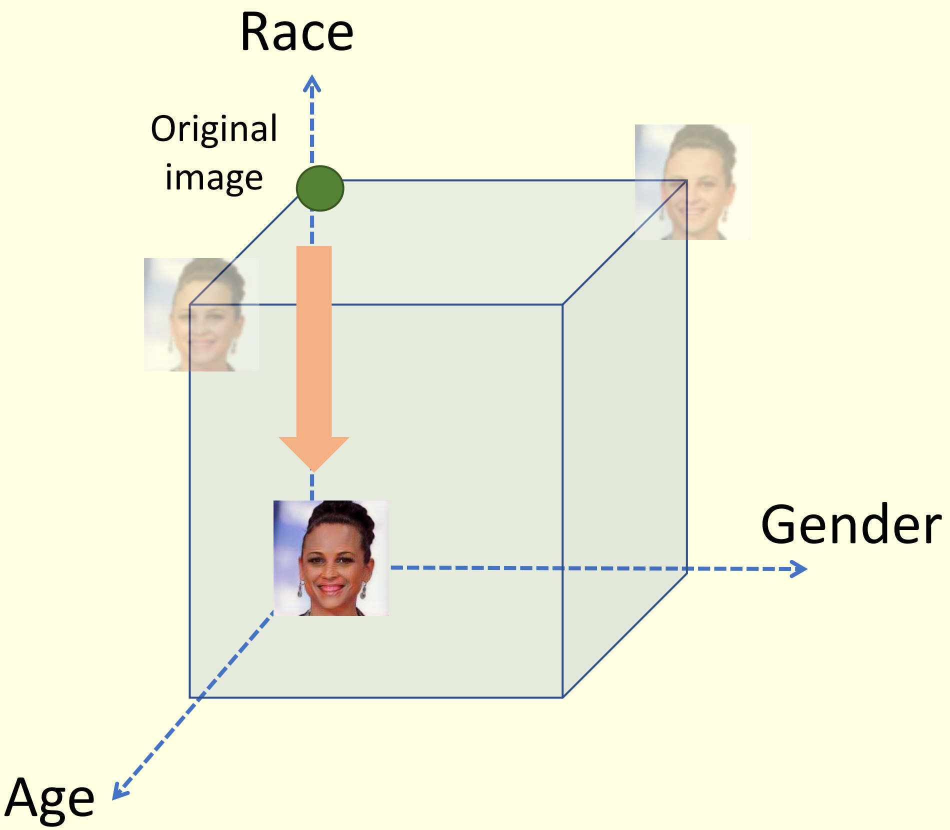
[Male, Mid-age, Cauc.]

[Female, Old, Cauc.]

**[Female, Mid-age, Afric.]**

Original Label $c_0$: [0, 1, 1]

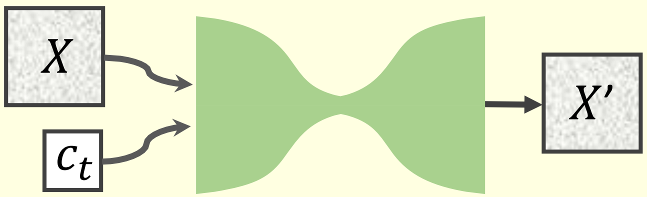
[Female, Middle-aged, Caucasian]

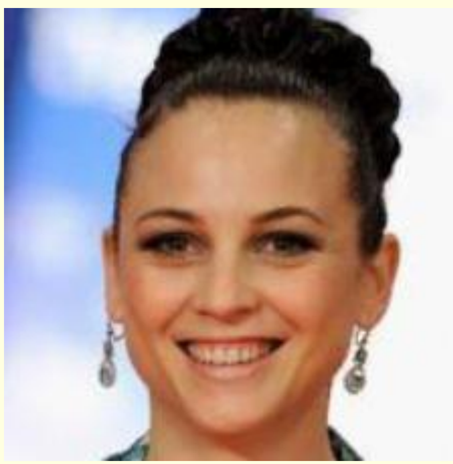





Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet

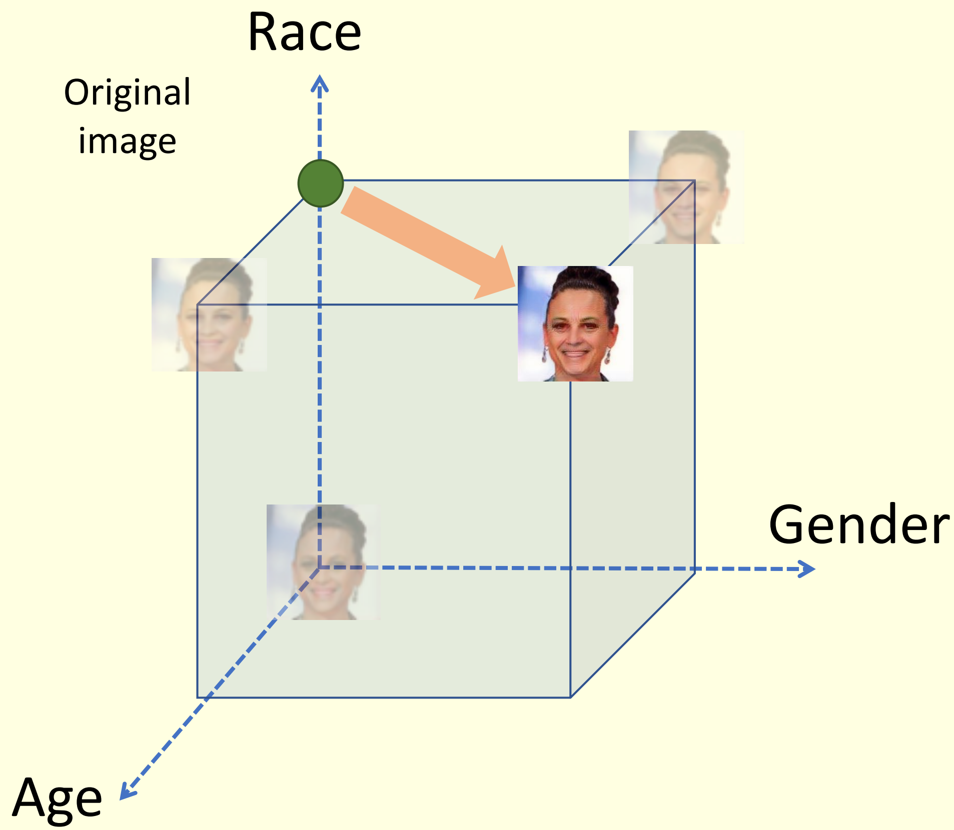


Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]

$c_t$

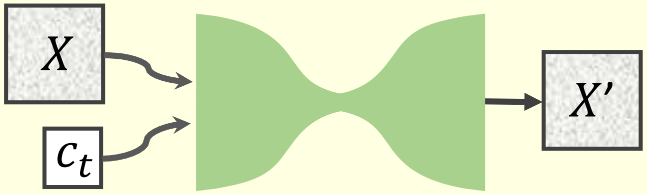
[Male, Mid-age, Cauc.]
[Female, Old, Cauc.]
[Female, Mid-age, Afric.]
**[Male, Old, Cauc.]**






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

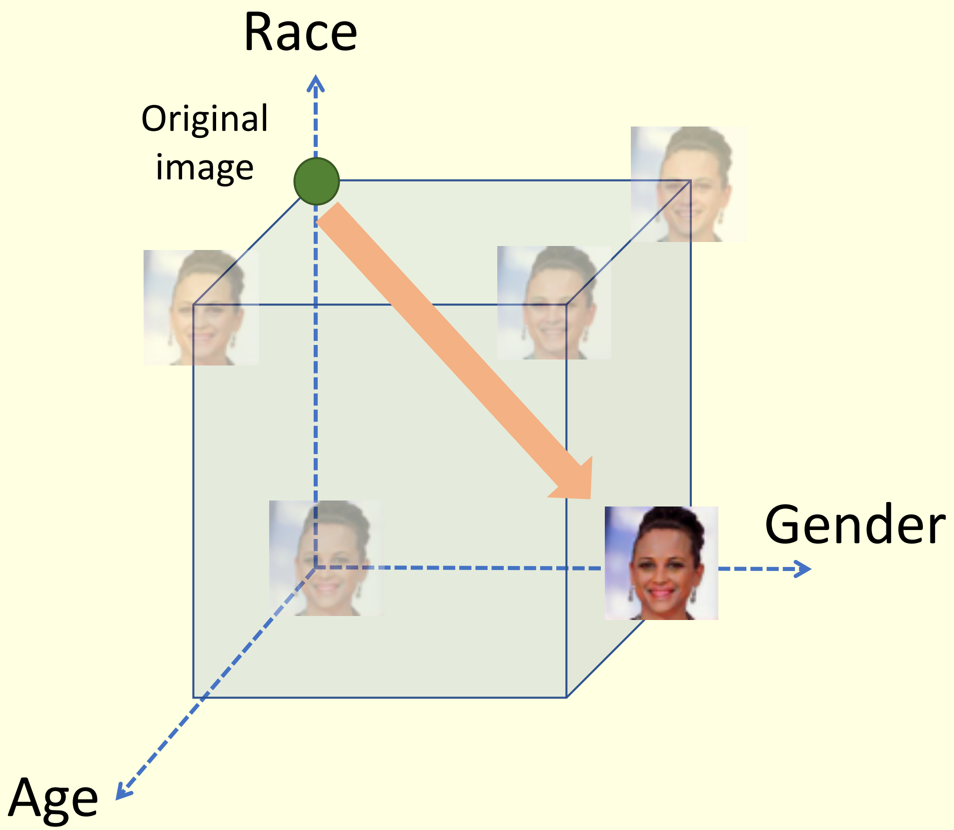
# Face Transformation Using PrivacyNet




Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]

$c_t$

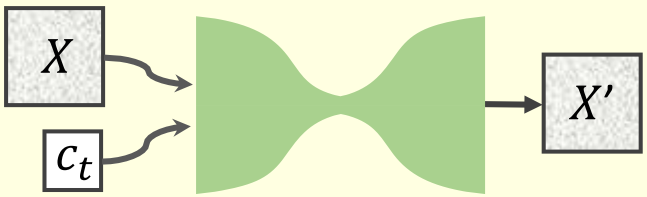
[Male, Mid-age, Cauc.]
[Female, Old, Cauc.]
[Female, Mid-age, Afric.]
[Male, Old, Cauc.]
**[Male, Mid-age, Afric.]**

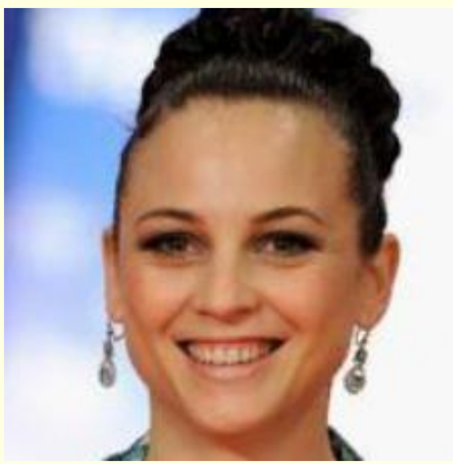





Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet

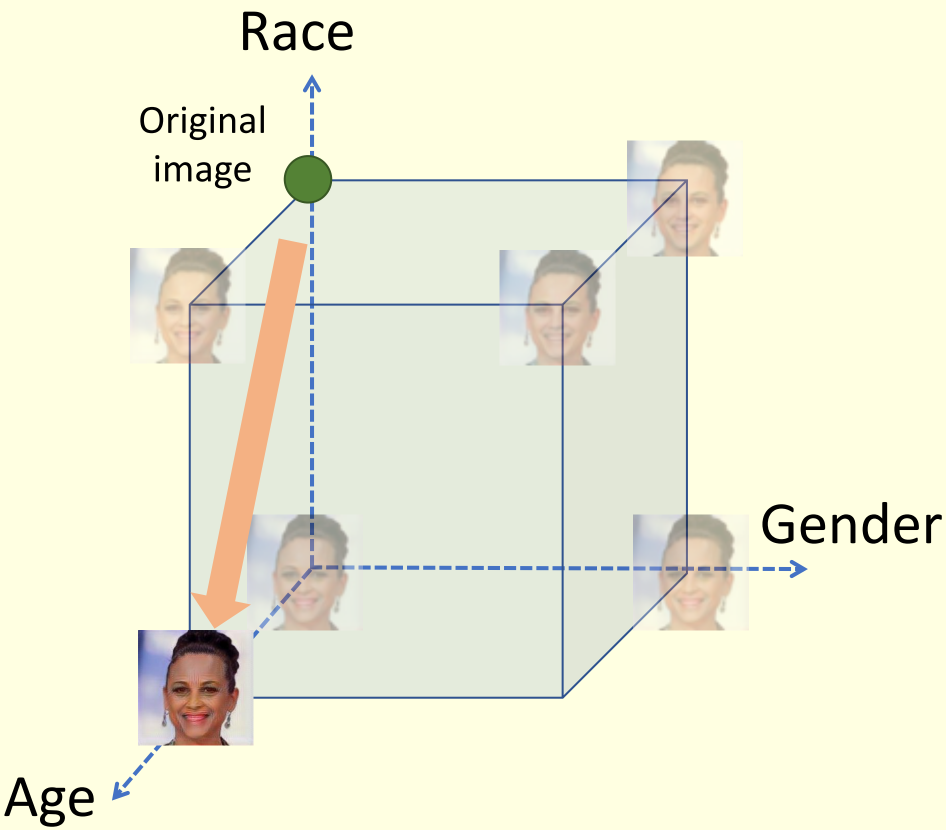


Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]

$\boldsymbol{c_t}$

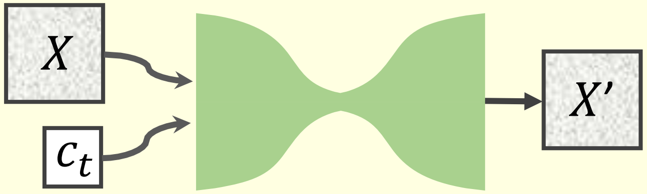
[Male, Mid-age, Cauc.]
[Female, Old, Cauc.]
[Female, Mid-age, Afric.]
[Male, Old, Cauc.]
[Male, Mid-age, Afric.]
**[Female, Old, Afric.]**






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

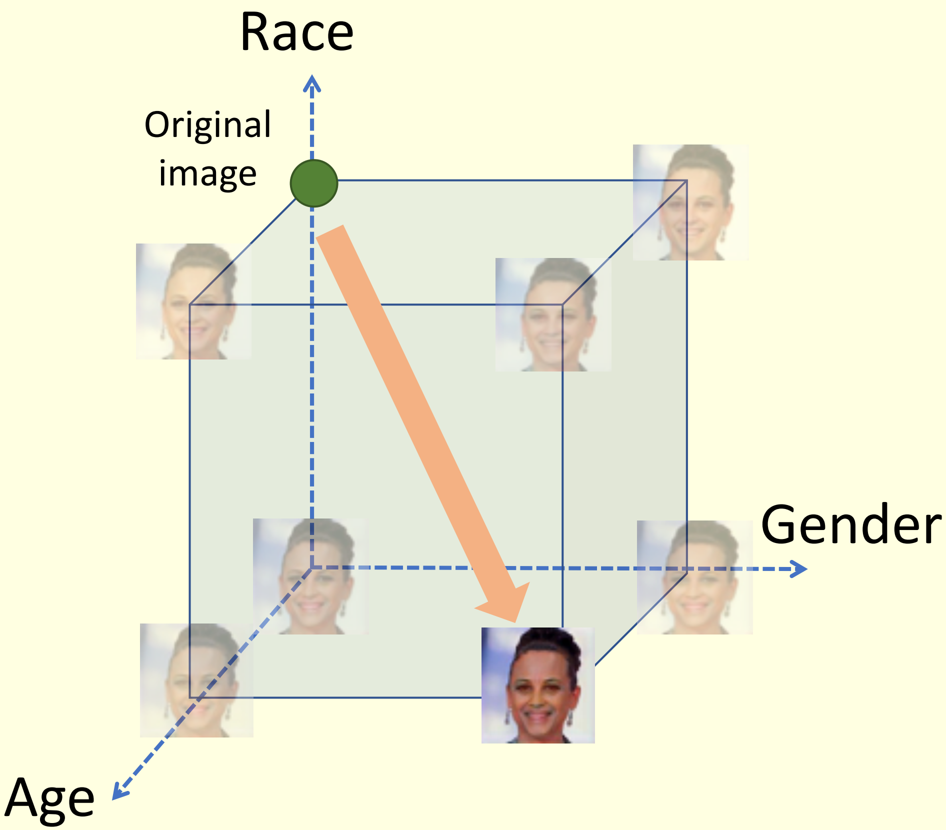
# Face Transformation Using PrivacyNet




Original Label $c_0$: [0, 1, 1]
[Female, Middle-aged, Caucasian]

$c_t$

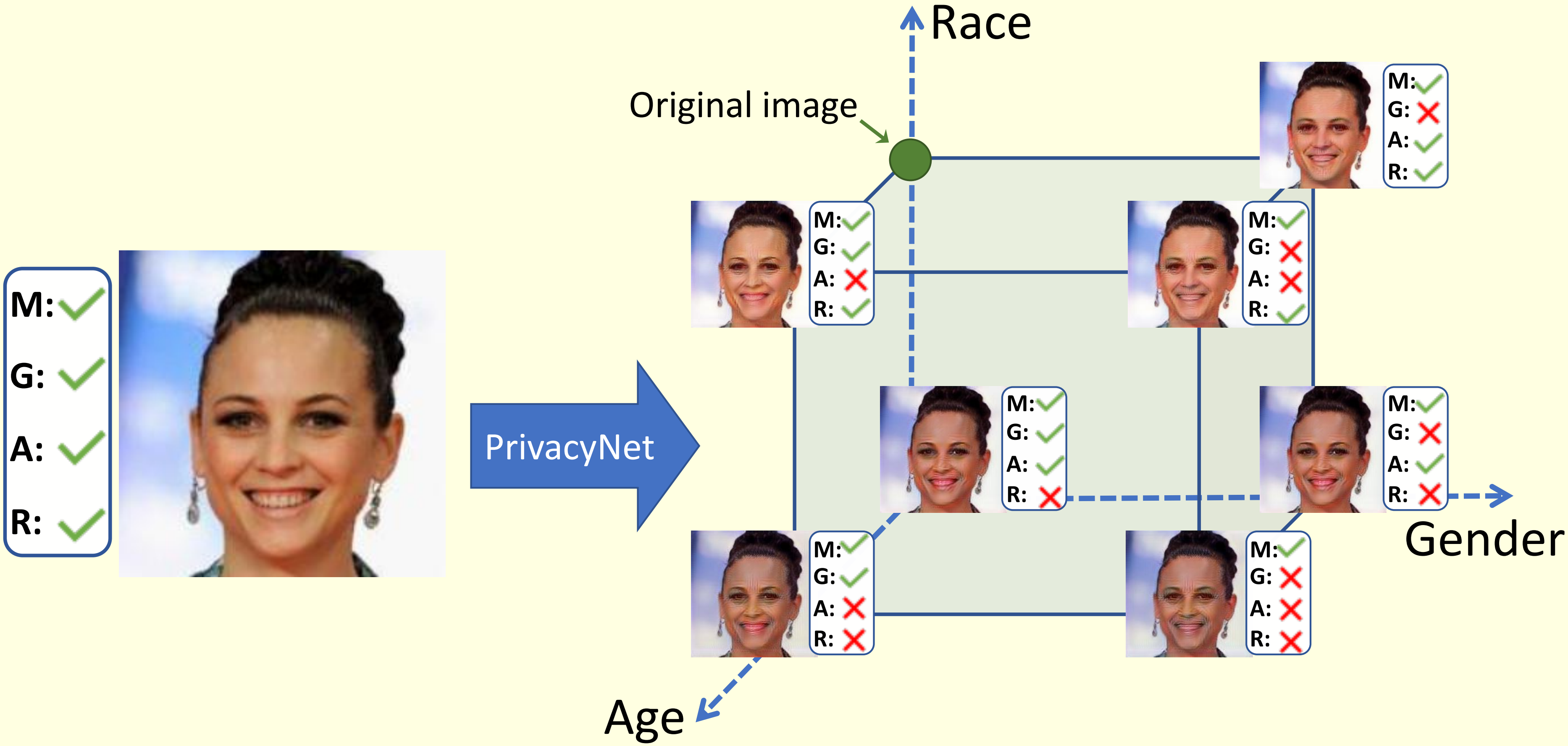
[Male, Mid-age, Cauc.]
[Female, Old, Cauc.]
[Female, Mid-age, Afric.]
[Male, Old, Cauc.]
[Male, Mid-age, Afric.]
[Female, Old, Afric.]
**[Male, Old, Afric.]**






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

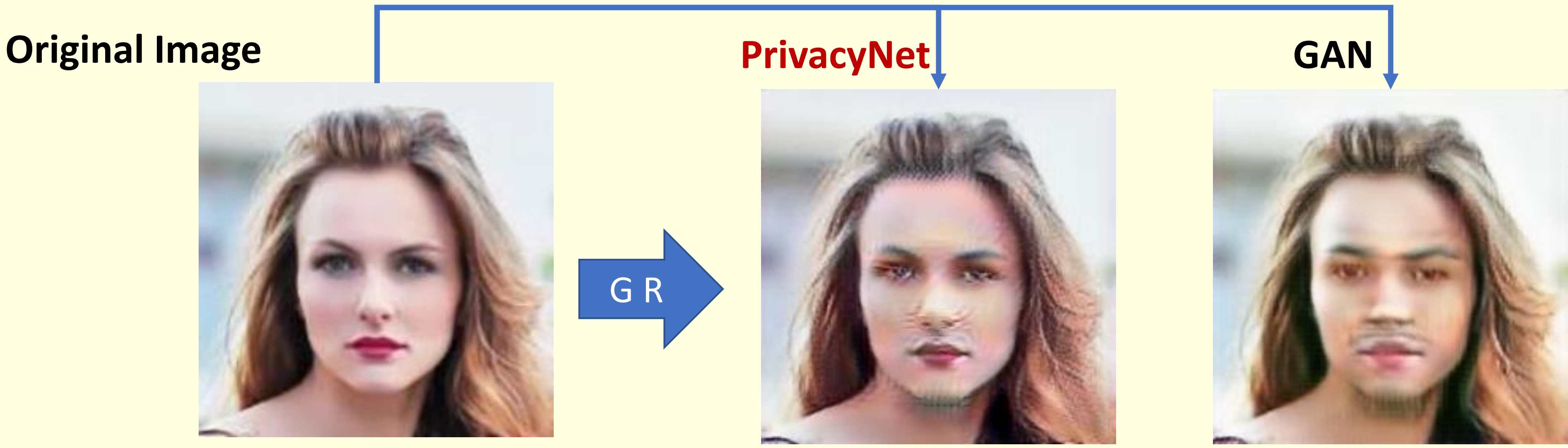
# Face Transformation Using PrivacyNet






Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Face Transformation Using PrivacyNet



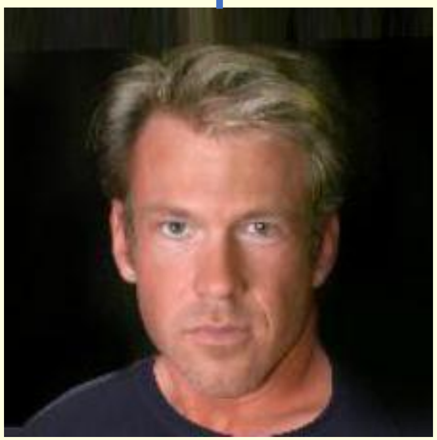

Match Scores with original image:

| | PrivacyNet | GAN |
|---|---|---|
| M-COTS: | 0.99 | 0.41 ↓ |
| DR-GAN: | 0.93 | 0.69 ↓ |
| SE-ResNet-50: | 0.72 | 0.14 ↓ |

Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

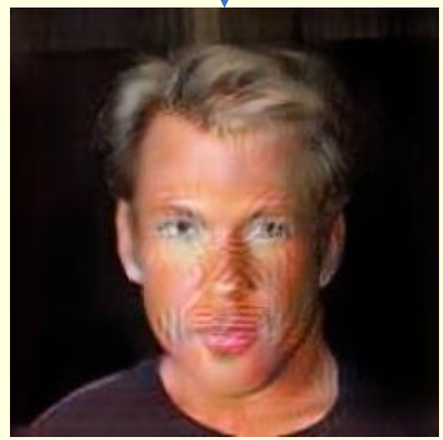
# Face Transformation Using PrivacyNet

**Original Image**



G R

**PrivacyNet**



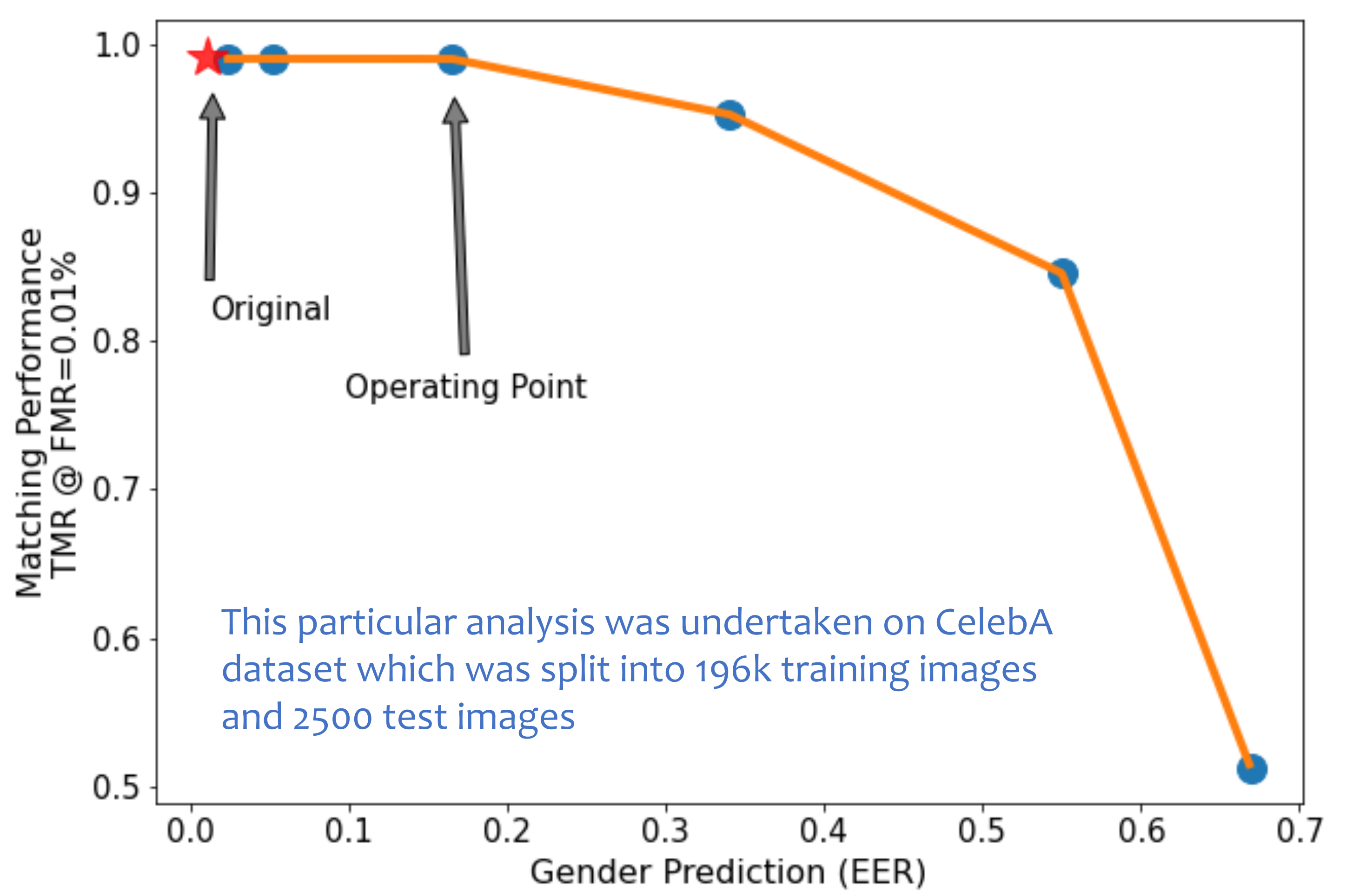
**GAN**

**Match Scores with original image:**

| | PrivacyNet | GAN |
|---|---|---|
| M-COTS: | 0.99 | 0.39 ↓ |
| DR-GAN: | 0.93 | 0.74 ↓ |
| SE-ResNet-50: | 0.81 | 0.31 ↓ |

Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020

# Experimental Results



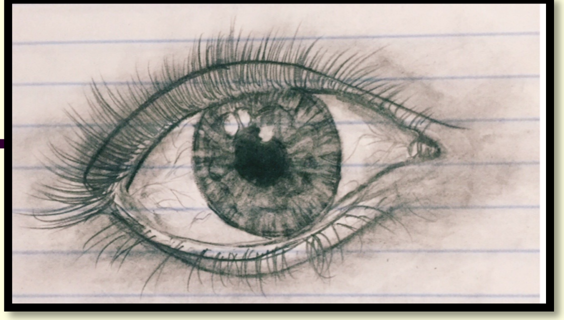

This particular analysis was undertaken on CelebA dataset which was split into 196k training images and 2500 test images



**Mirjalili et al., PrivacyNet: Semi-Adversarial Networks for Multi-attribute Face Privacy, IEEE TIP 2020**

# Summary

- Altered and Synthetic Data
  - Sensor Privacy
  - Morph Attacks
  - Deep MasterPrints
- Digital Image Forensics
  - Which sensor did this image come from?
  - Has this image been digitally tampered?
  - What is the relationship between a set of images?
- Privacy
  - Semi-adversarial Networks (SAN): Controllable Privacy



# On the Integrity and Privacy of Biometric Data


## Arun Ross

## Michigan State University

http://iprobe.cse.msu.edu/