

# The Many-faced God: Attacking Face Verification System with Embedding and Image Recovery

Mingtian Tan, Zhe Zhou, Zhou Li

Fudan University, China

University of California, Irvine, USA





## Background

### Face Verification System

-border control

-company entrance

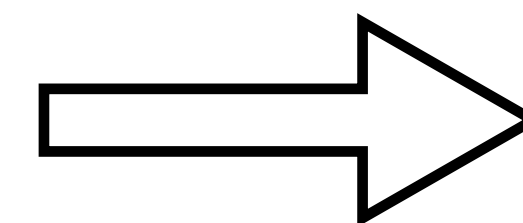
-mobile device



## Background

### Face Verification System

- border control
- company entrance
- mobile device



**Embeddings**



## Background

### Data Privacy Leakage Task

- Membership Inference Attack
- Attribute Inference Attack

**Distinguish Training Data and Test Data**

**Complete Data from part of information**

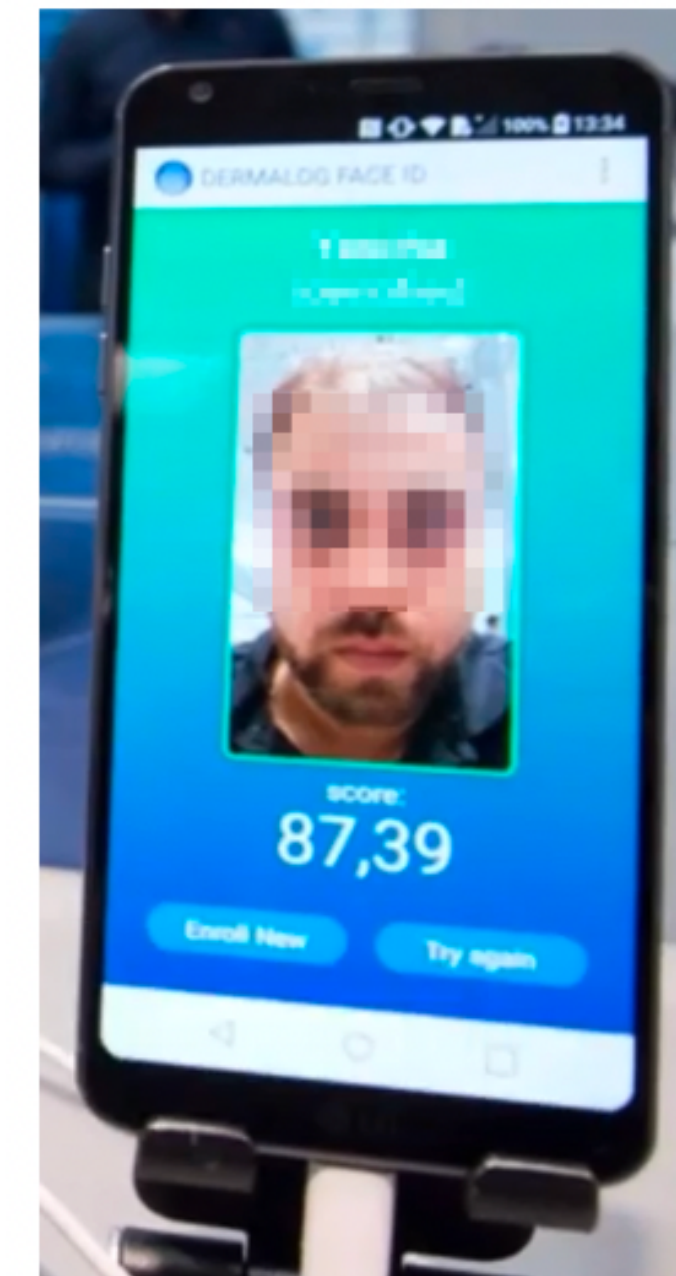




## □ Background

### Our Data Privacy Leakage

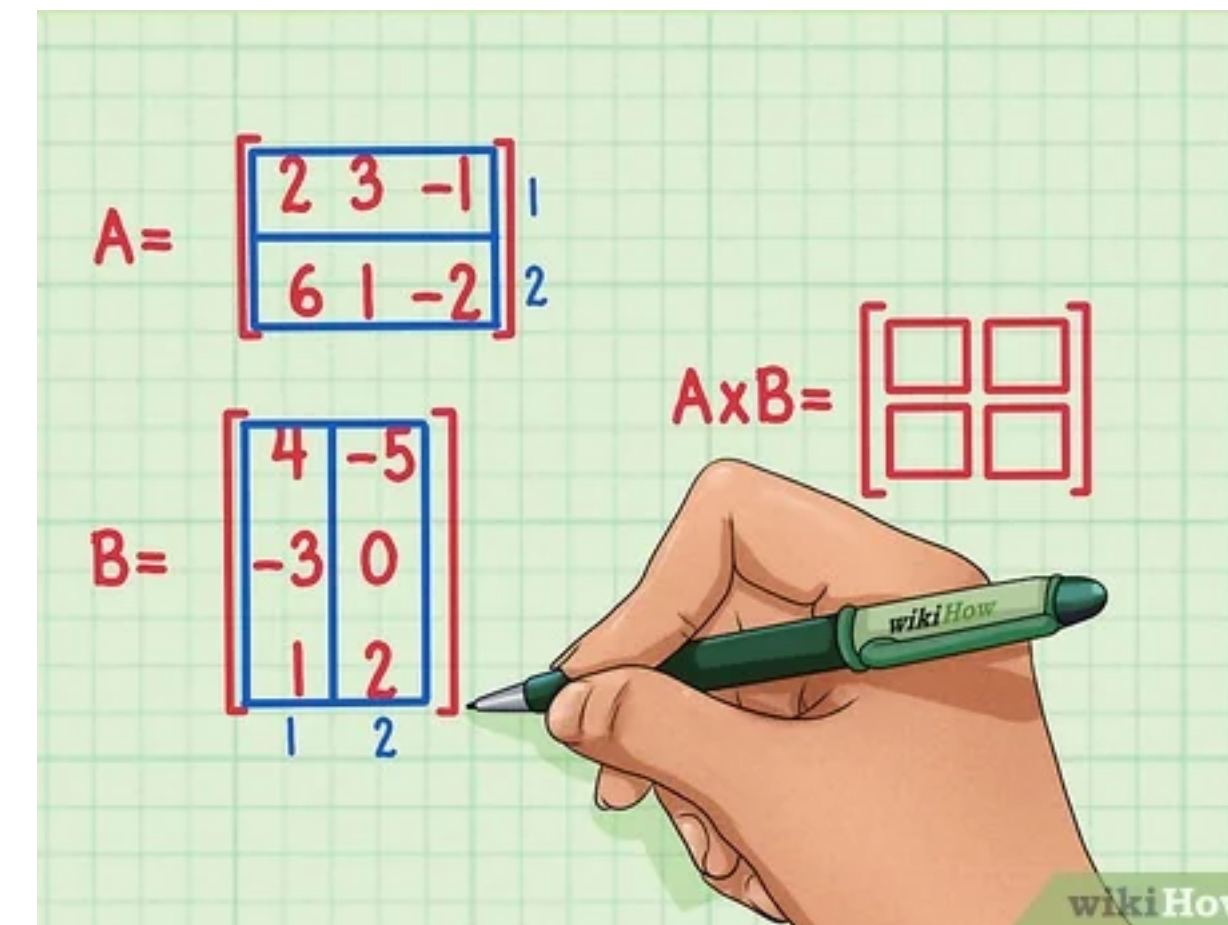
- Information leakage from FVS
- Embedding recovery from leakage
- Image recovery with embedding



## □ Background

### Our Data Privacy Leakage

- Information leakage from FVS
- Embedding recovery from leakage
- Image recovery with embedding



Embedding



Original Img



## □ Methodology

Get Information leakage from FVS



Attacker - ID number

Embedding A



Victim

Embedding V

Distance

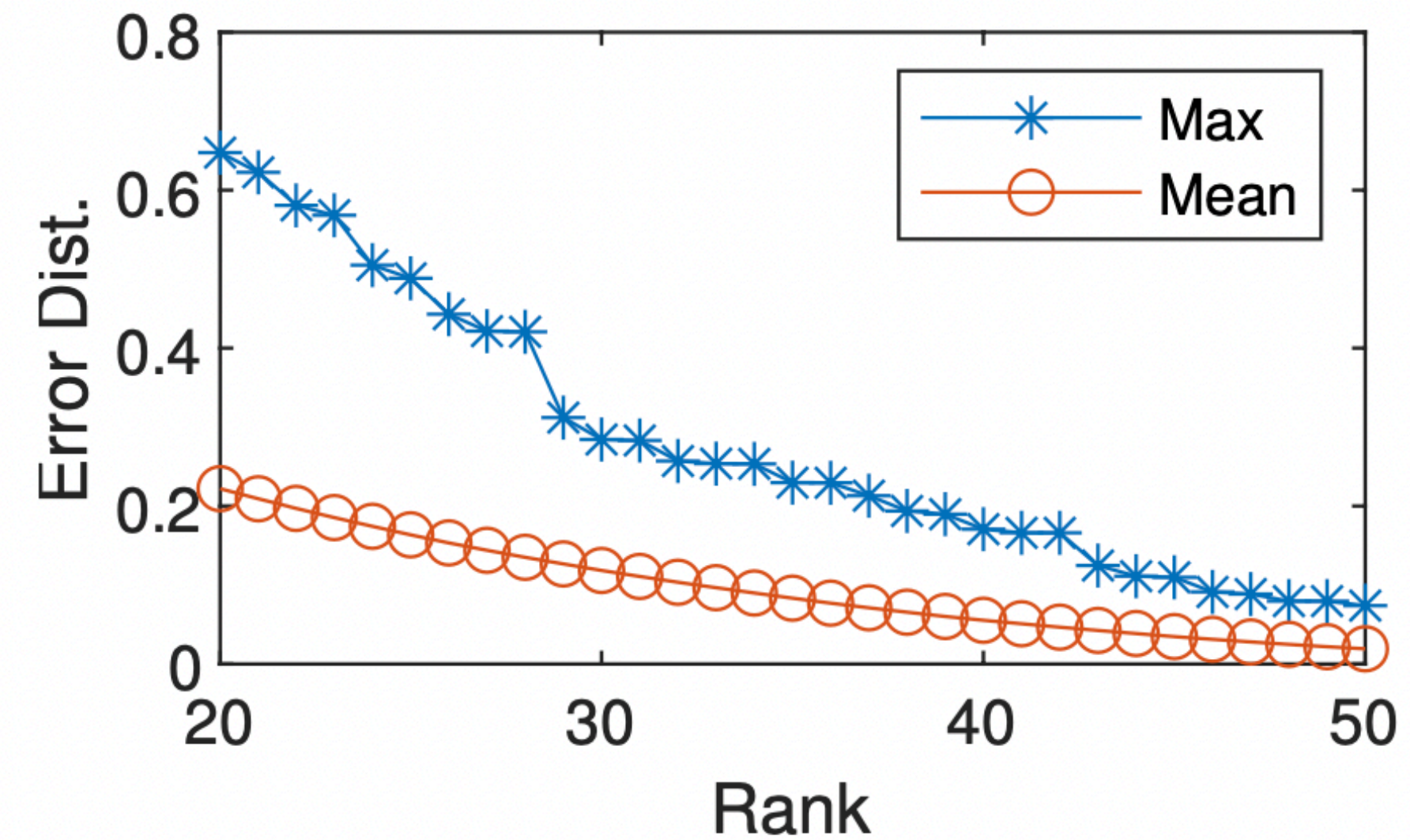
*self-service FVS in Chinese Entry & Exit Bureau*

## □ Methodology

Recover Embedding from leakage

$$\begin{aligned} \|\vec{e}_s - \vec{e}_1\| &= d_1 \\ \|\vec{e}_s - \vec{e}_2\| &= d_2 \\ &\dots \\ \|\vec{e}_s - \vec{e}_n\| &= d_n \end{aligned}$$

Equation Solving

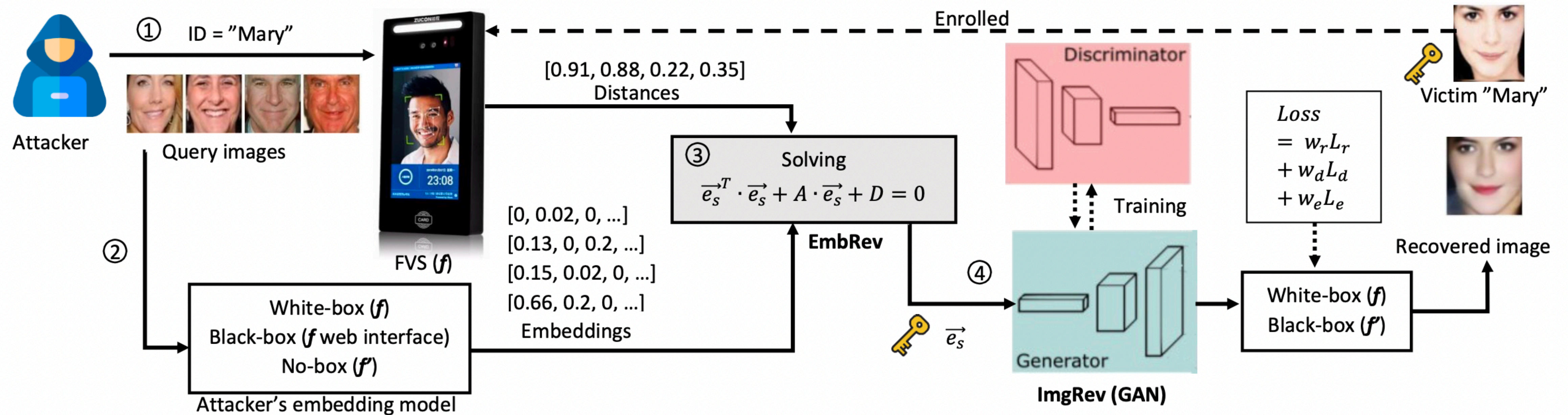


SVD Rank Retained



# Methodology

## Attack Model Overview

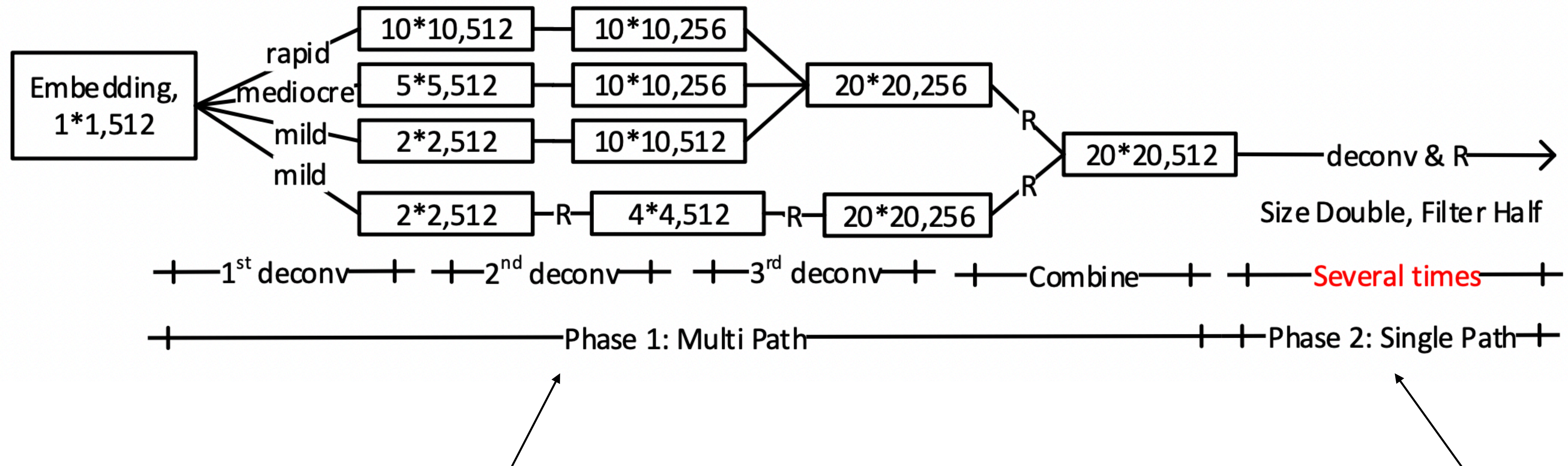


embedding-reverse GAN (erGAN)



# Methodology

## Generator of erGAN



Extract information from Embedding

Recover the Image from Information



## Evaluation

Model	Emb. Dim.	Distance Type
Residual Inception Network	1792	Cosine
Clarifai Online Face Embedding [10]	1024	Cosine
Facenet 20180402-114759 [51]	512	Cosine
Facenet 20170512-110547 [51]	128	L2

Embedding Model (EM)

Embedding Recovery Evaluation

LFW Dataset

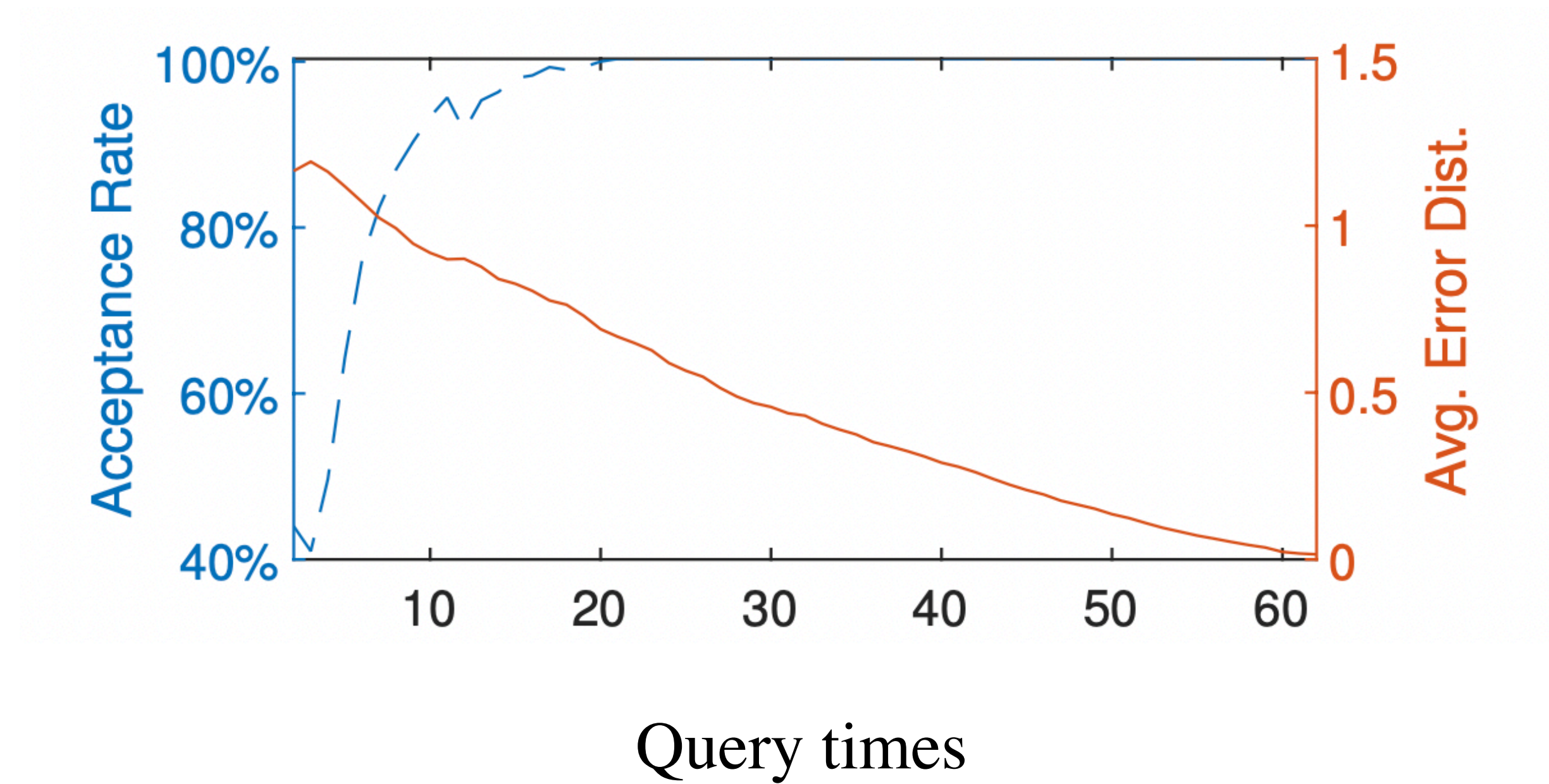
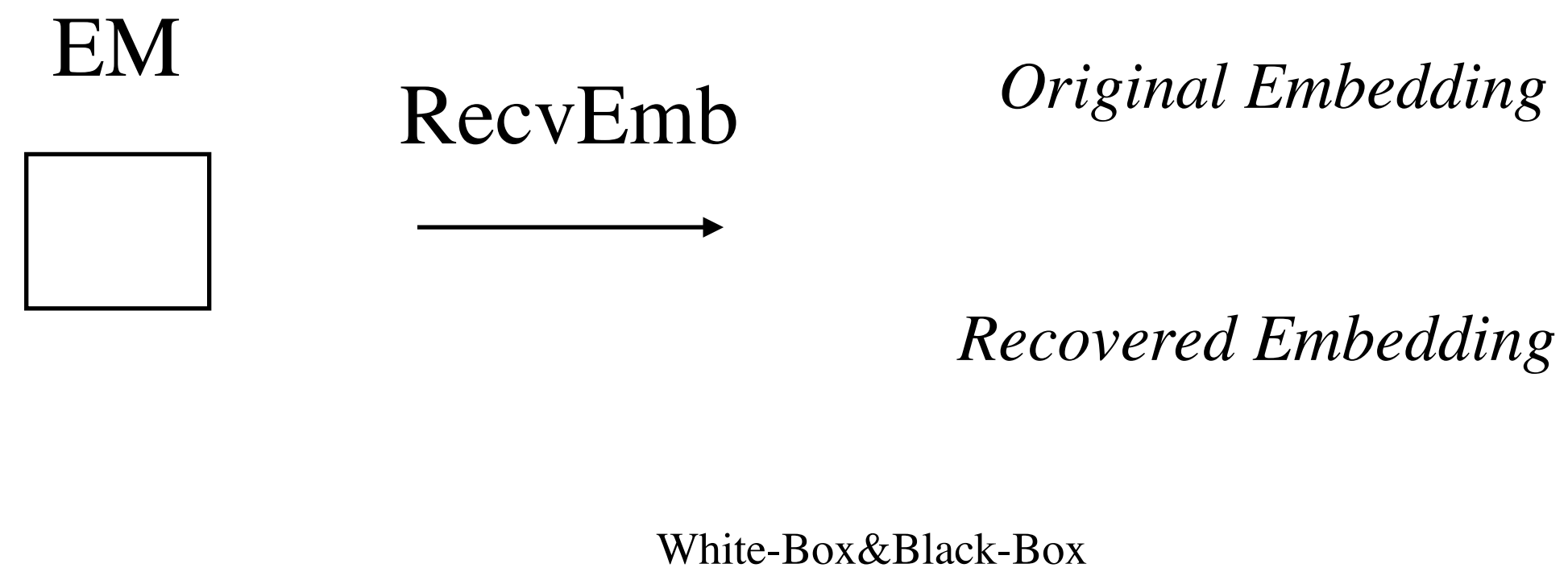
Face Recovery Evaluation

celebA dataset



# □ Evaluation

## Embedding Recovery Evaluation



*EM : Facenet 128 model*



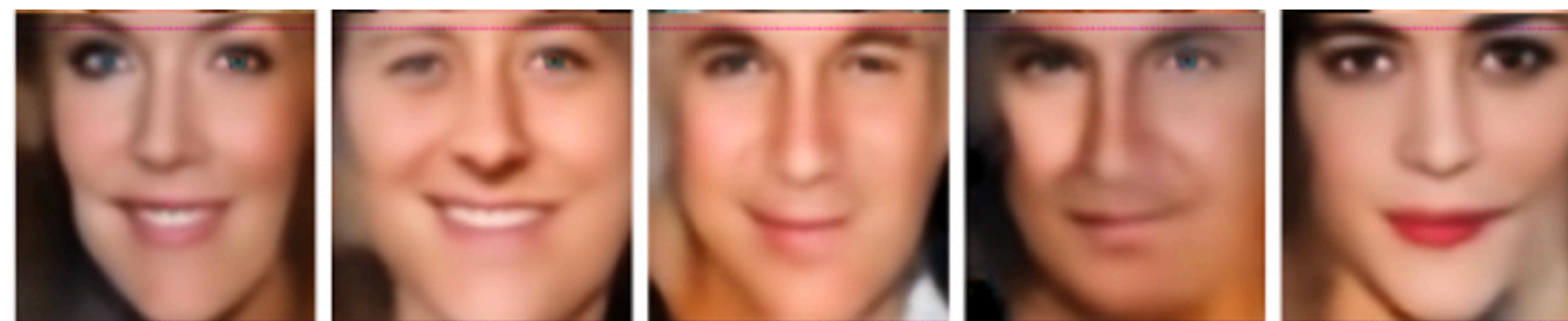
# □ Evaluation

## Face Recovery Evaluation

*Original*



*Facenet-128*



*Facenet-512*



*Clarifai-1024*



*WebRes-1024*



*White-box*



*Le*







## Evaluation

### Face Recovery Evaluation

Model	Blackbox Baseline				White- box	Blackbox $L_e$
	128	512	1024	1792		
Acc.	93.07%	97.23%	98.63%	93.87%	94.20%	96.23%
FID	114.11	157.47	33.94	49.39	86.00	61.25

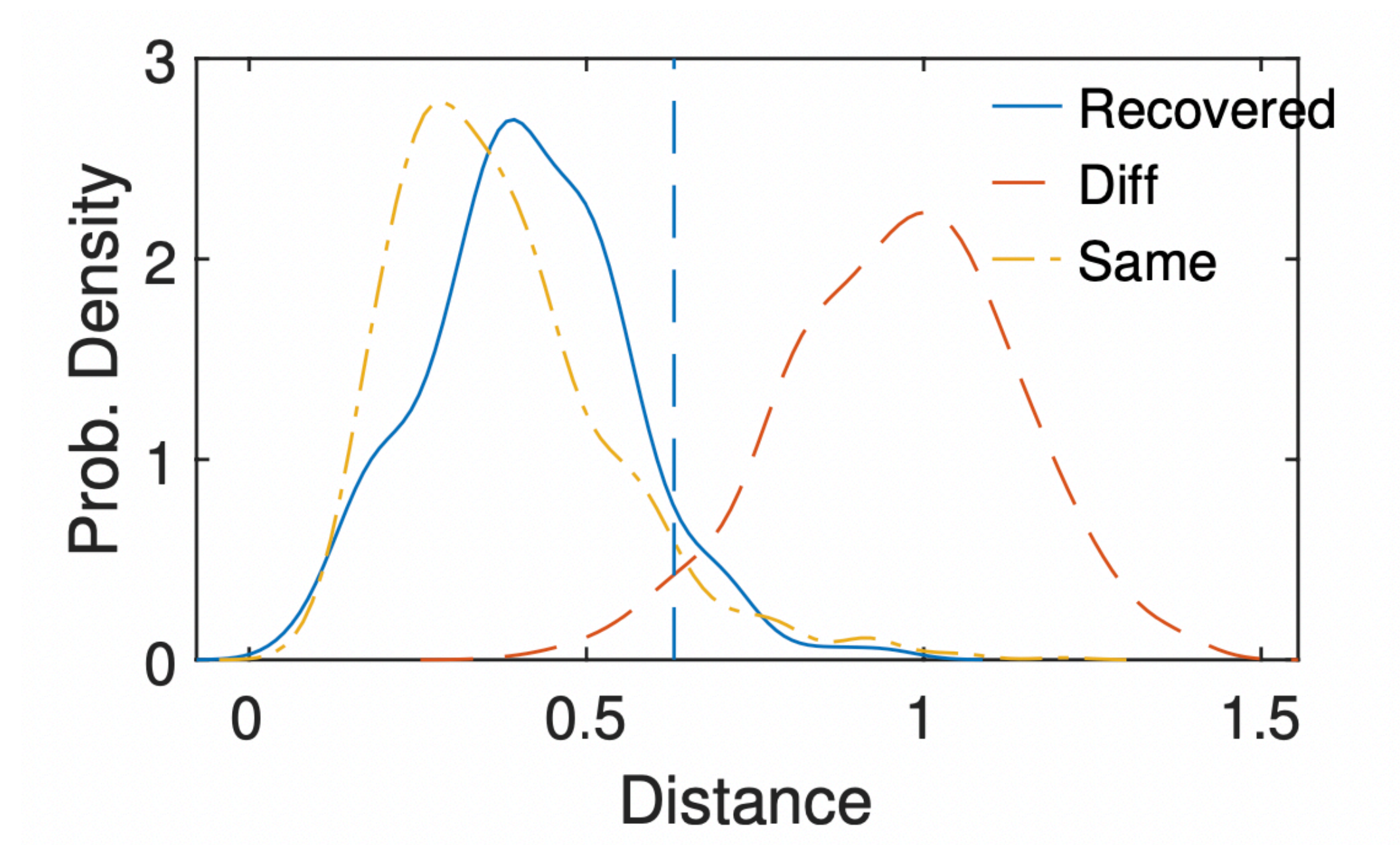
**The second row show the acceptance rate of the images recovered**

**The third shows the FID of the generated images (smaller is better).**

# □ Evaluation

## Face Recovery Evaluation

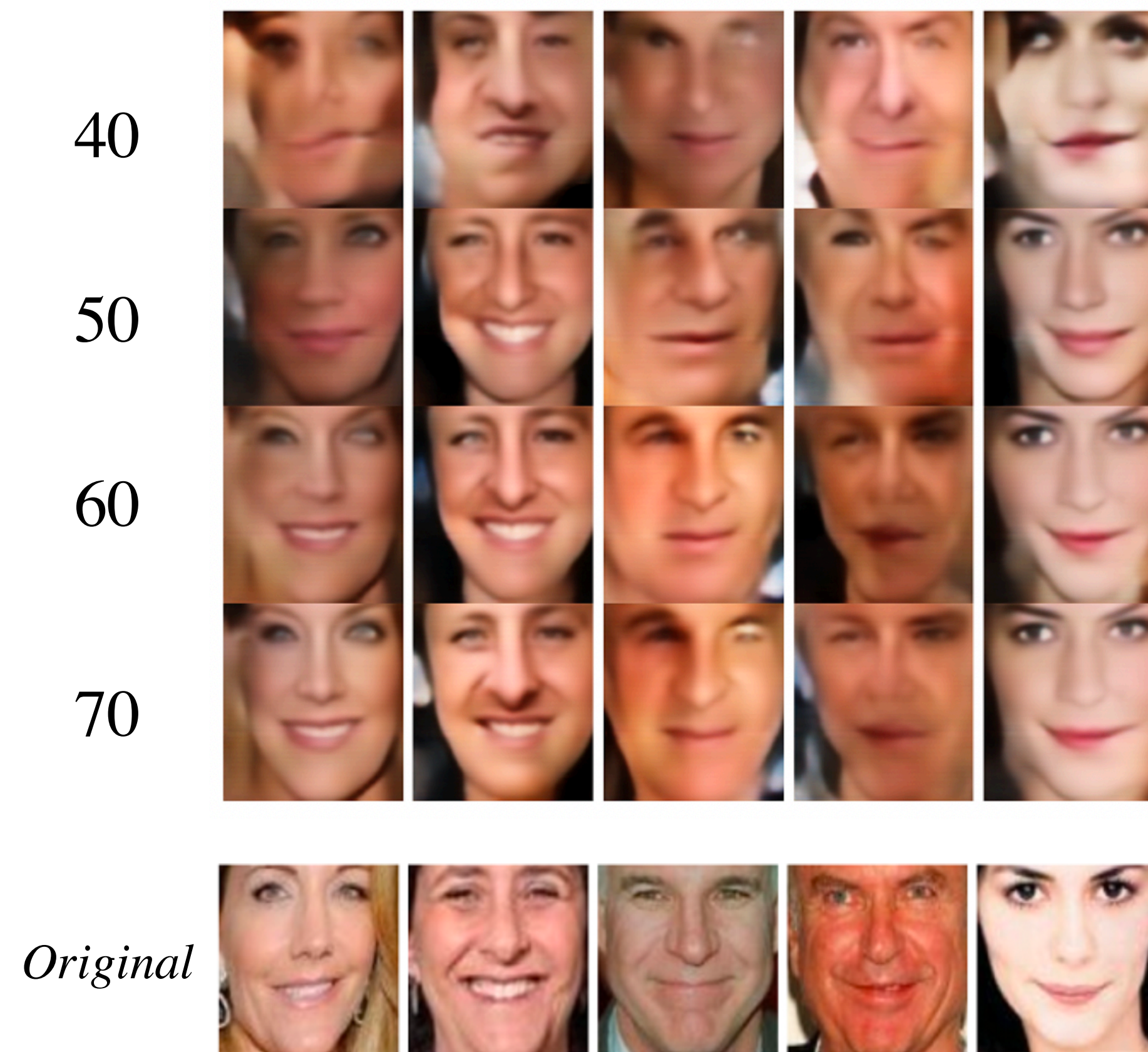
### Stability





## □ Evaluation

### Face Recovery Evaluation



Images Recovered with different number of queries.

**Thank you !**