NEURAL INFORMATION PROCESSING SYSTEMS 2025

FracFace: Breaking the Visual Clues—Fractal-Based Privacy-Preserving Face Recognition

Dai Wanying[1,4], Beibei Li[1*], Naipeng Dong[2*], Guangdong Bai[3], Jin Song Dong[4]
[1]The School of Cyber Science and Engineering, Sichuan University
[2]The School of Electrical Engineering and Computer Science, The University of Queensland
[3]City University of Hong Kong
[4]The School of Computing, National University of Singapore

SICHUAN UNIVERSITY 四川大學

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

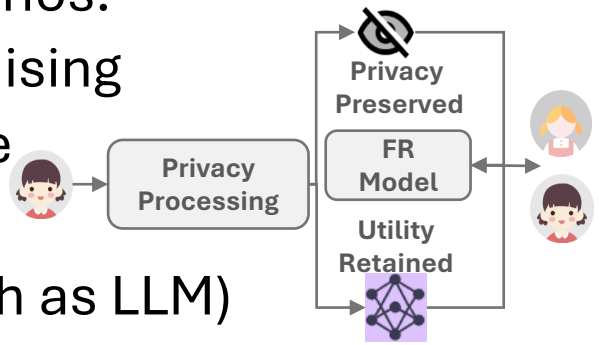
CityU 香港城市大學 City University of Hong Kong

NUS National University of Singapore

Background

NEURAL INFORMATION PROCESSING SYSTEMS 2025

- **Face Recognition (FR)**, a technology that utilize **the human face** for **biometric identification**, is widely used in security-related scenarios.
- However, privacy concern is raising
  - Unauthorized photo release
  - Peeper or curious people
  - Reconstruction attack (such as LLM)

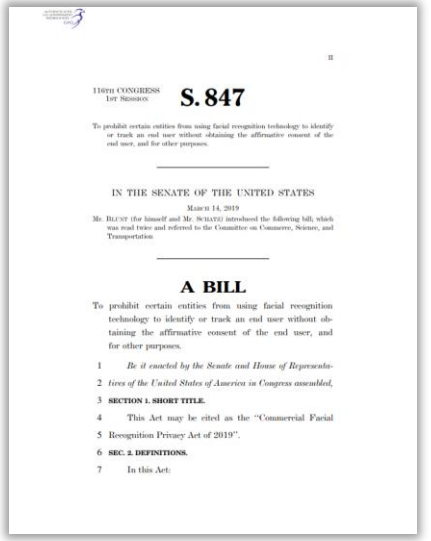


- Utility vs Privacy
  - Face recognition system has to work properly
  - People may not want to disclose their facial image
- So, can we process face image such that
  - Privacy information can not be revealed to visual clues→ Privacy
  - Machine can still recognize the identity → Utility

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

General Data Protection Regulation



S. 847

IN THE SENATE OF THE UNITED STATES

A BILL

Commercial Facial Recognition Privacy Act of 2019

Our Approach

NEURAL INFORMATION PROCESSING SYSTEMS 2025

Online Face Images I_i

Transform

F_l

F_h

Frequency Representation S

Frequency Projection

Frequency Fractal Mapping

$S^{(2)}$

Refined Frequency Component

Fractal Kernel M_0

6	7	8
5	0	1
4	3	2

Fractal Lattice L_0

6	7	8
5	0	1
4	3	2

Fractal Grid

60	61	62	69	70	71	78	89	80
89	54	55	68	63	64	77	72	73
78	67	56	67	66	65	76	75	74
51	52	53	6	7	8	15	16	17
50	45	46	5	0	1	14	9	10
49	48	47	4	3	2	13	12	11
42	43	44	33	34	35	24	25	26
41	36	37	32	27	28	23	18	19
40	39	38	31	30	29	22	21	20

Fractal Structural Privacy Map

Frequency Channels Refining

Pruning Space P

P_1 P_2 P_3

Frequency Band Attenuation

$S^{(1)}$ $S^{(2)}$

Refined Frequency Channel S'

Retain Discriminative Identity Features

Fractal Identity Tokens

Database

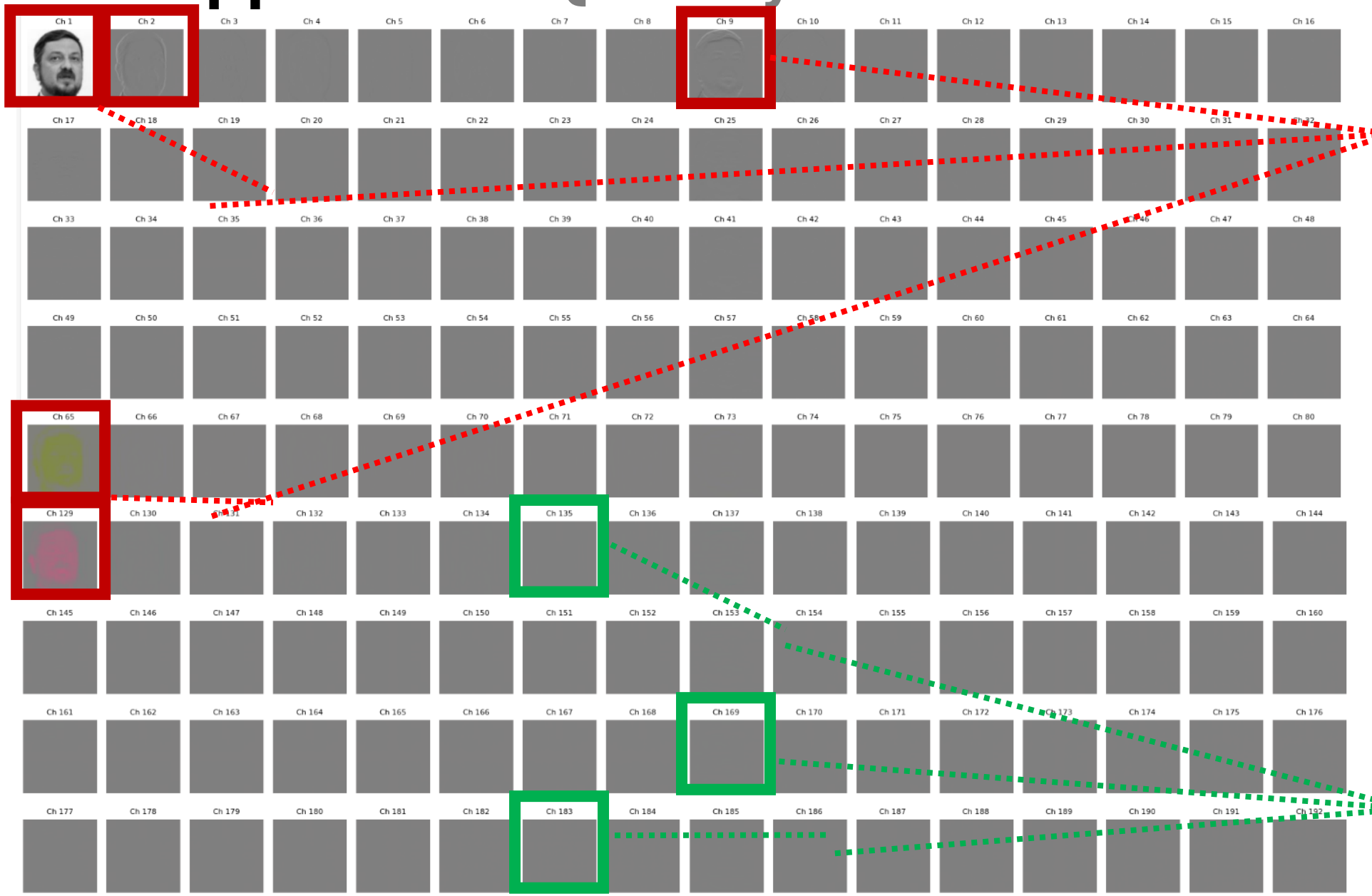
Model Training

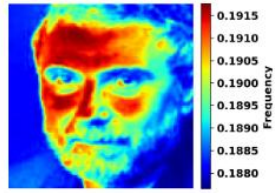
Identity Privacy Preservation

Our Approach

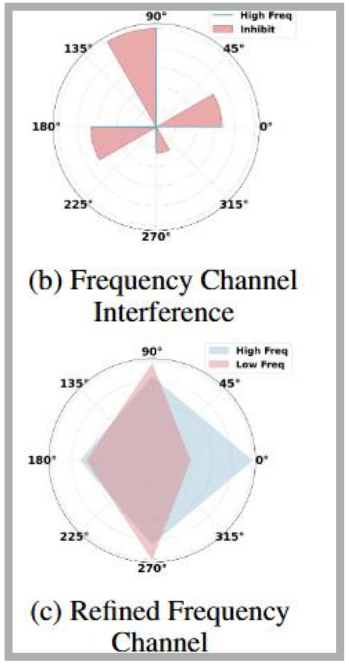
QR1:Why we need to refine?

NEURAL INFORMATION PROCESSING SYSTEMS 2025



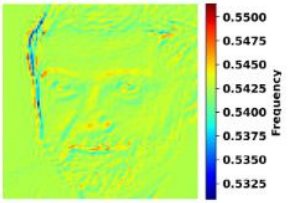


(a) Unrefined Frequency Spectrum



(b) Frequency Channel Interference

(c) Refined Frequency Channel



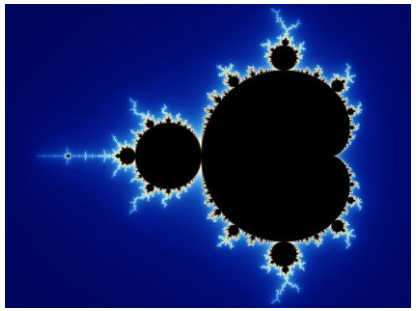
(d) Refined Frequency Spectrum

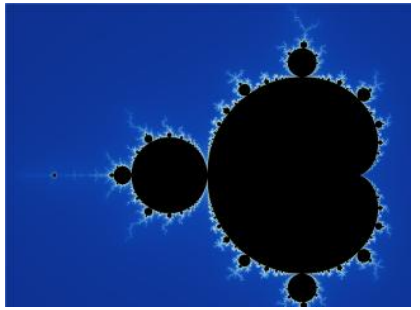
Our Approach

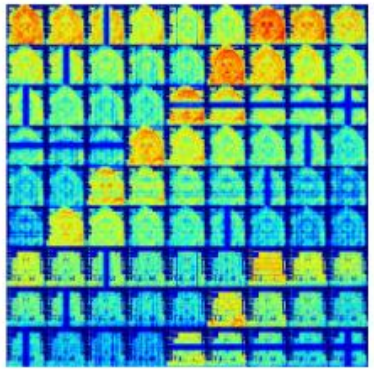
QR2:Why we introduce Fractal?

NEURAL INFORMATION PROCESSING SYSTEMS 2025

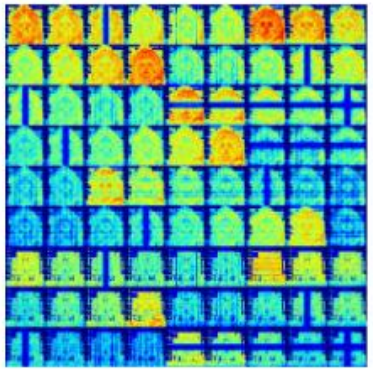
- ❖ Why **use fractal technology** instead of traditional random shuffling method?
- ✓ **Fractal Dimension** (FD) describes **the complexity** and **self-similarity** of an object, and **how it fills space at different scales**. Applying Fractal Dimension to PPFR:
- ❑ FD can measure the complexity of face images at different scales; (tra: Fuzz/Noise/Res/DP, etc → can not recognize by human; FracFace: conceal the VI irreversibly & maintaining identity)
- ❑ Avoid direct visualization; (Image Spatial → Frequency Domain → Fractal Domain)
- ❑ The recognition task can still be carried out normally (identity features can be retained);



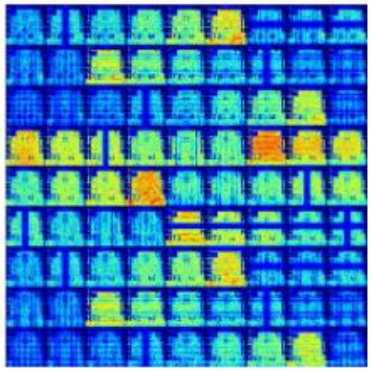




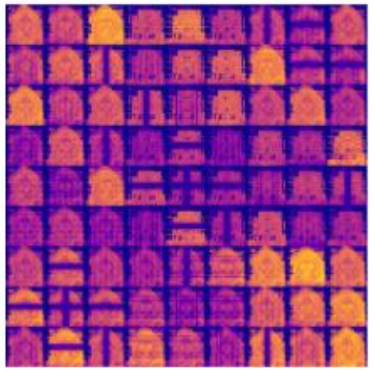
(a) Vanilla Frequency Domain Channel Visualization



(b) Refined Frequency Domain Channel Visualization (Part 1)



(c) Filtered Frequency Domain Channel Visualization (Part 2)



(d) Fractal Frequency Domain Channel Visualization

Evaluation accuracy

NEURAL INFORMATION PROCESSING SYSTEMS 2025

Table 1: The performance of privacy protection methods in terms of face recognition accuracy. The space-time domain is denoted by S, the frequency domain by F_1, and the fractal domain by F_2, respectively. Green denotes the proportion associated with the privacy protection level.

Method	LFW (%)	Celeba (%)	AgeDB (%)	CFP-FP (%)	CALFW (%)	CPLFW (%)	IJB-B 1e-4	IJB-B 1e-5	IJB-C 1e-4	IJB-C 1e-5	Domain	Protection	Venue
Arcface [5]	99.73	95.35	97.99	96.83	**95.89**	94.59	**94.81**	**91.98**	93.69	92.41	S	0%	CVPR-2019
Arcface-FD [41]	99.81	96.45	**98.27**	97.18	94.69	95.03	93.68	90.53	95.89	94.92	S	0%	CVPR-2020
PPFR-FD [37]	99.39	93.49	97.99	95.53	95.69	90.62	93.67	91.12	94.73	92.49	F_1	43%	AAAI-2022
Duetface [21]	99.81	92.13	96.17	93.24	95.18	92.19	92.63	90.32	95.28	94.16	F_1	45%	ACMMM-2022
PartialFace [22]	**99.82**	95.64	95.03	98.10	94.83	**95.61**	92.48	91.59	93.85	93.96	F_1	68%	ICCV-2023
Minusface [23]	99.79	95.89	96.03	96.94	95.93	92.89	93.89	93.51	**95.91**	**94.96**	F_1	85%	CVPR-2024
PRO-Face C [43]	99.29	91.69	93.79	95.63	89.44	90.65	88.38	83.27	90.89	89.94	F_1	40%	IEEE TIFS-2024
FaceObfuscator [14]	99.70	94.36	96.79	**98.82**	94.84	95.42	92.90	92.18	94.43	93.58	F_1	87%	USENIX-2024
FracFace (ours)	99.69	**95.91**	97.76	96.14	93.92	93.16	92.42	90.73	94.09	92.26	$S \rightarrow F_1 \rightarrow F_2$	100%	-

Evaluation privacy

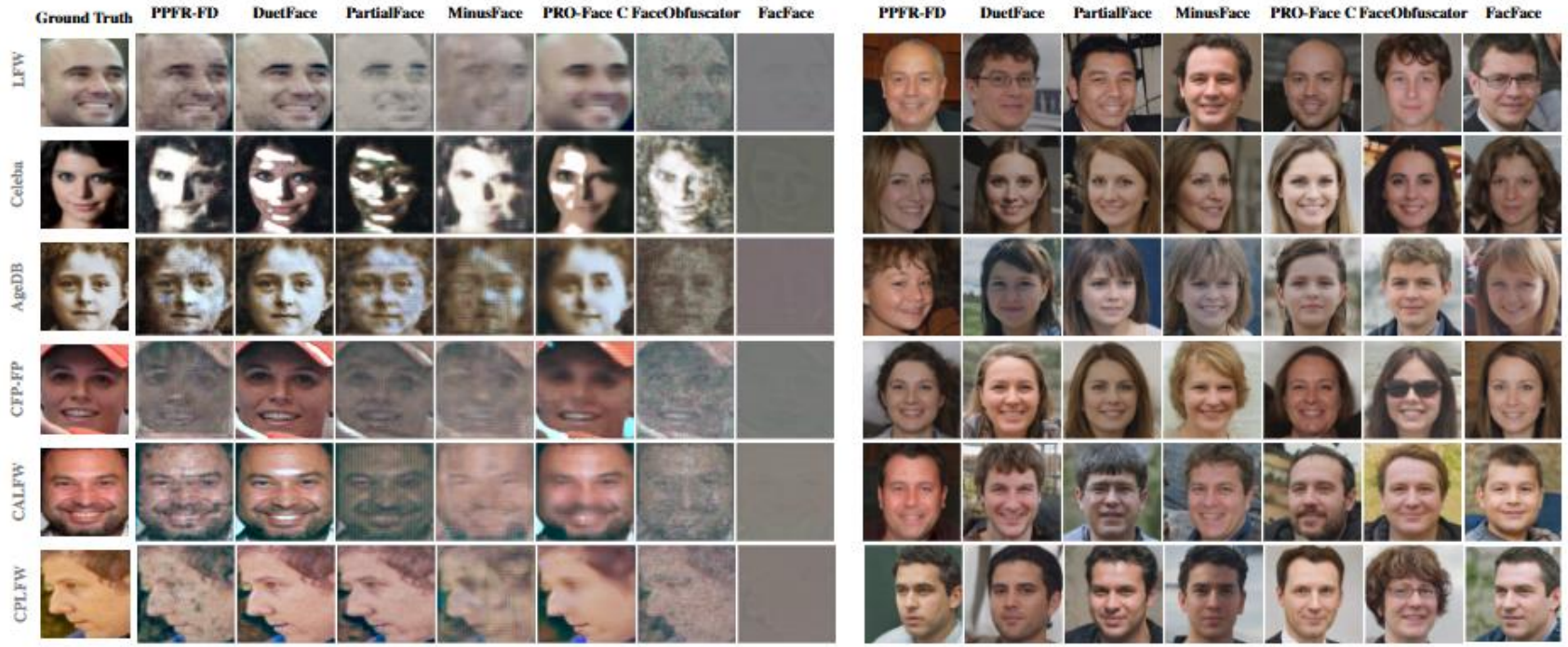


Figure 3: Evaluation of facial reconstruction vulnerabilities under U-Net and StyleGAN attacks.

(a) Target (b) $\mathcal{D}_1$ (c) $\mathcal{D}_2$ (d) $\mathcal{D}_3$ (e) $\mathcal{D}_4$ (f) $\mathcal{D}_5$ (g) $\mathcal{D}_6$ (h) $\mathcal{D}_7$ (i) $\mathcal{D}_8$

Figure 4: Comparative reconstruction results on CelebA targets with PGDiff. (a) shows the target image of the adversary attack; (b)-(i) shows the reconstruction outputs.

Evaluation privacy

NEURAL INFORMATION PROCESSING SYSTEMS 2025

(a) Target (b) $\mathcal{G}$ 1 (c) $\mathcal{G}$ 2 (d) $\mathcal{G}$ 3 (e) $\mathcal{G}$4 (f) $\mathcal{G}$ 7 (g) $\mathcal{G}$ 8 (h) $\mathcal{G}$ 5 (i) $\mathcal{G}$ 6

Figure 4: Comparative reconstruction results on CelebA targets. (a) shows the target image of the adversary attack; (b)-(i) shows the reconstruction outputs with StyleGAN.

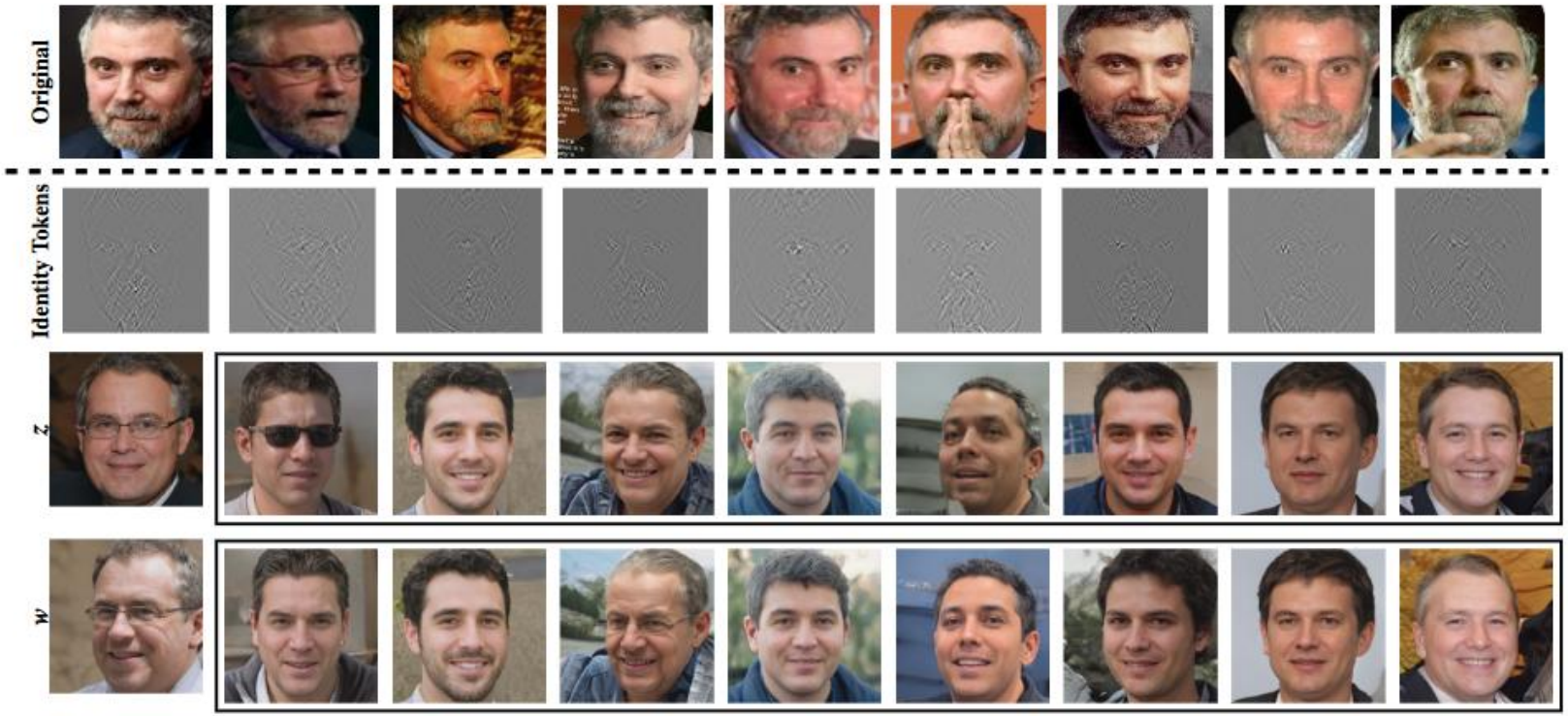
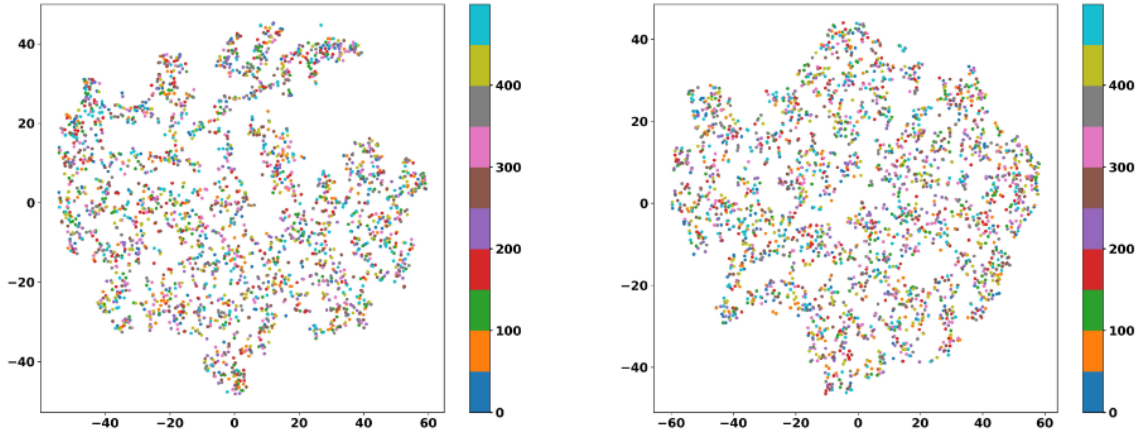


Figure 5: Visual analysis of StyleGAN vulnerabilities.

Evaluation privacy

NEURAL INFORMATION PROCESSING SYSTEMS 2025

A.1 Sparsity Analysis in Frequency Domain



(a) Frequency Channel Interference (b) Refined Frequency Channel

Figure 7: Analyzing the sparsity of frequency domain channels through t-SNE.

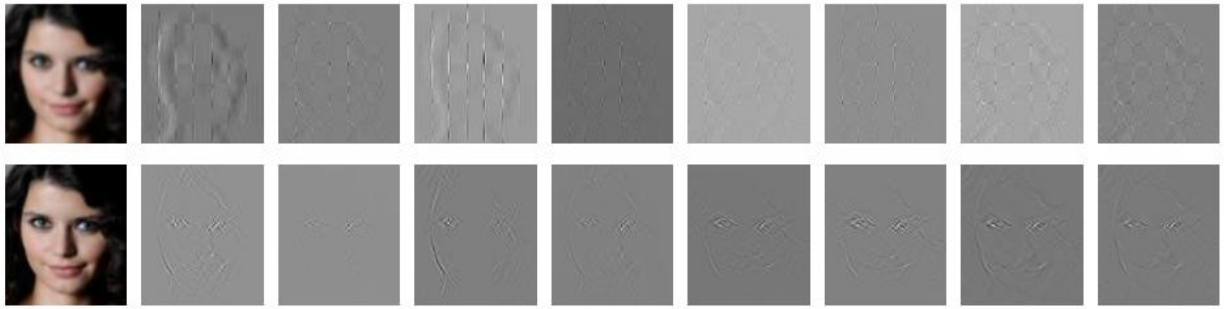


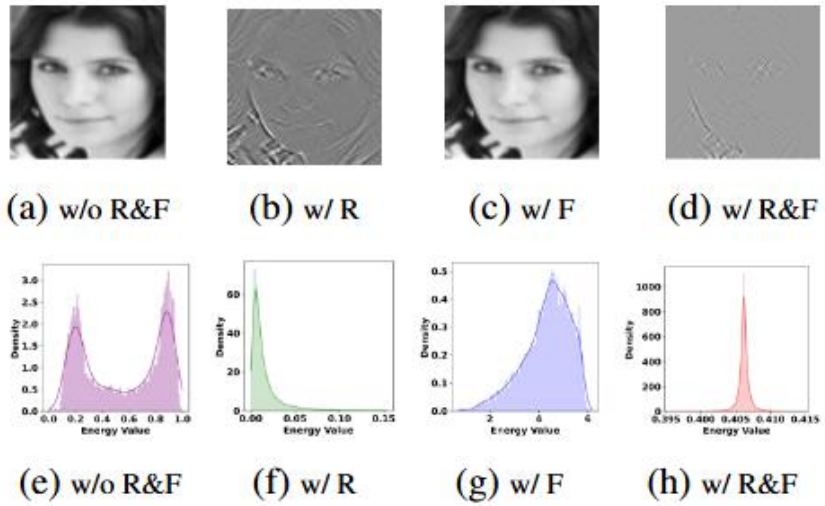
Figure 9: Resilient identity learning despite frequency degradation

Table 2: Benchmarking the privacy utility tradeoff under U-Net and StyleGAN based reconstruction attacks, evaluated by SSIM, LPIPS, MSE, PSNR, and IDS across two leakage scenarios.

Metric	Method	U-Net-based Face Reconstruction Attack						StyleGAN-based Face Reconstruction Attack					
		LFW	Celeba	AgeDB	CFP-FP	CALFW	CPLFW	LFW	Celeba	AgeDB	CFP-FP	CALFW	CPLFW
SSIM ↓	Arcface	0.9642	0.9883	0.9436	0.9351	0.9555	0.9188	0.9906	0.9827	0.9548	0.9820	0.9408	0.9307
	Arcface-FD	0.9623	0.9097	0.9242	0.9172	0.9544	0.9021	0.9761	0.9438	0.9342	0.9411	0.9618	0.9461
	PPFR-FD	0.4231	0.1488	0.3079	0.3720	0.3557	0.5204	0.3116	0.2681	0.2404	0.3523	0.3323	0.1696
	Duetface	0.4963	0.2570	0.4280	0.4965	0.5158	0.4249	0.3367	0.2303	0.2873	0.2397	0.3245	0.1663
	PartialFace	0.4953	0.2927	0.2404	0.3592	0.3715	0.4423	0.2845	0.2683	0.2544	0.3314	0.2487	0.1729
	Minusface	0.3864	**0.1461**	0.2319	0.3407	**0.2878**	0.3263	0.3421	0.2266	0.2409	0.2962	0.2587	0.1699
	PRO-Face C	0.5517	0.3684	0.5135	0.4737	0.4665	0.4685	0.3535	0.2676	0.2339	0.3217	0.2946	0.1656
	FaceObfuscator	**0.3771**	0.1984	0.3477	0.3428	0.3468	**0.3189**	0.3654	0.2585	0.2882	0.2960	0.2595	0.1395
	FracFace (ours)	0.3997	0.2195	**0.2045**	**0.2749**	0.3317	0.4357	**0.2836**	**0.2019**	**0.2278**	**0.2264**	**0.2305**	**0.1045**
LPIPS ↑	Arcface	0.0141	0.0708	0.0436	0.0330	0.0301	0.0824	0.0163	0.0192	0.0139	0.0117	0.0131	0.0167
	Arcface-FD	0.0175	0.0676	0.0418	0.0487	0.0312	0.0831	0.0180	0.0127	0.0133	0.0128	0.0133	0.0172
	PPFR-FD	0.5433	0.4522	0.5198	0.5430	0.6683	0.5059	0.7206	0.5443	0.6596	0.6022	0.5910	0.6916
	Duetface	0.5264	0.4350	0.3328	0.3442	0.3458	0.4249	0.7378	0.5461	0.6842	0.6007	0.6412	0.6208
	PartialFace	0.5197	0.5056	0.6536	0.5592	0.6952	0.6502	0.7558	0.5652	0.6733	0.5715	0.6604	0.6911
	Minusface	0.6809	0.6790	0.6607	0.6720	0.6305	0.6675	0.7313	0.5894	0.6732	0.6322	0.7253	0.6768
	PRO-Face C	0.5018	0.4341	0.4173	0.4812	0.4645	0.5403	0.7091	0.6004	0.6522	0.5749	0.6335	0.6719
	FaceObfuscator	0.6512	0.6289	0.5790	0.6332	0.6364	0.6012	0.7419	0.5320	0.6891	0.6218	0.6614	0.6535
	FracFace (ours)	**0.6907**	**0.6834**	**0.7389**	**0.7796**	**0.6958**	**0.6990**	**0.8307**	**0.6354**	**0.6935**	**0.6412**	**0.6655**	**0.6935**
MSE ↑	Arcface	0.0002	0.0058	0.0001	0.0015	0.0012	0.0021	0.0011	0.0018	0.0021	0.0029	0.0016	0.0014
	Arcface-FD	0.0002	0.0054	0.001	0.0030	0.0012	0.0024	0.0014	0.0024	0.0025	0.0023	0.0019	0.0021
	PPFR-FD	0.0170	0.0453	0.0390	0.0475	0.0372	0.0164	0.0514	0.0466	0.0340	0.0613	0.0686	0.0462
	Duetface	0.0249	0.0474	0.0253	0.0235	0.0224	0.0263	0.0621	0.0583	0.0452	0.0645	0.0631	0.0728
	PartialFace	0.0251	0.0415	0.0872	0.0389	0.0532	0.042	0.0156	0.0613	0.0695	0.0637	0.0793	0.0405
	Minusface	0.0619	0.0425	0.0754	0.0549	0.0537	0.0418	0.0729	0.0675	0.0711	0.0646	0.0593	0.0637
	PRO-Face C	0.0018	0.0256	0.0127	0.0209	0.0149	0.0171	0.0567	0.0480	0.0633	0.0583	0.0635	0.0495
	FaceObfuscator	0.0418	0.0466	0.0578	0.0512	0.0409	0.0545	0.0769	0.0795	0.0635	0.0698	0.0646	0.0794
	FracFace (ours)	**0.0921**	**0.0839**	**0.1694**	**0.0855**	**0.0591**	**0.0643**	**0.0869**	**0.0993**	**0.0909**	**0.0750**	**0.0753**	**0.0831**
PSNR ↓	Arcface	28.3762	26.3394	28.0351	28.1658	28.9046	26.6827	27.3627	23.9351	29.9237	26.5816	20.3843	25.7364
	Arcface-FD	26.1864	26.5831	28.5249	27.9832	25.1352	26.1258	28.2943	25.1971	29.5851	27.6278	23.4935	27.1539
	PPFR-FD	16.6922	15.2175	14.0937	13.2350	14.3056	17.8451	10.6539	13.3151	10.7322	11.4767	11.6374	10.3582
	Duetface	16.0382	14.2463	13.1962	16.2930	16.1359	15.7981	10.3639	11.0696	10.0926	10.7314	11.9891	11.6206
	PartialFace	13.0542	10.9401	10.5918	12.9035	12.7318	13.7378	9.9318	12.1278	10.1875	11.9616	11.3478	10.5448
	Minusface	11.2158	**9.3362**	11.2309	12.0672	11.9623	13.7816	11.3744	11.7088	11.4857	10.7283	12.2753	10.1364
	PRO-Face C	17.8753	15.9239	18.9573	16.7931	16.2451	16.7569	10.1446	11.6173	11.4588	10.9503	11.9773	11.3907
	FaceObfuscator	10.3351	10.9748	12.3641	10.6841	**10.7845**	12.6315	10.6150	10.7325	10.1433	10.6668	11.9029	10.9551
	FracFace (ours)	**8.6099**	9.9682	**9.5171**	**10.0953**	11.7843	**10.0827**	**9.7742**	**10.0369**	**10.0421**	**10.0562**	**10.9270**	**10.1239**
IDS ↓	Arcface	0.9932	0.9966	0.9989	0.9904	0.9928	0.9991	0.9968	0.9834	0.9910	0.8973	0.9627	0.9624
	Arcface-FD	0.9927	0.9939	0.9969	0.9918	0.9919	0.9982	0.9915	0.9620	0.9837	0.8993	0.9639	0.9728
	PPFR-FD	0.5699	0.6549	0.8402	0.8829	0.7968	0.6982	0.7587	0.8319	0.6915	0.6512	0.8250	0.6983
	Duetface	0.5830	0.6172	0.7921	0.8786	0.6217	0.6826	0.7388	0.8239	0.6074	0.6288	0.8116	0.6799
	PartialFace	0.4670	0.4572	0.7308	0.6353	0.5384	0.5204	0.7317	0.8043	0.6391	0.5962	0.7298	0.6194
	Minusface	0.3946	0.4007	0.4147	0.5428	0.4218	0.2600	0.7267	0.8062	0.5950	0.5649	0.7329	0.5481
	PRO-Face C	0.4124	0.5028	0.7978	0.7548	0.8325	0.7271	0.8299	0.8501	0.7064	0.6294	0.8562	0.7158
	FaceObfuscator	0.3830	0.4094	0.4972	0.4565	0.46247	0.3412	0.7187	0.7374	0.5785	0.6218	0.7253	0.6101
	FracFace (ours)	**0.0057**	**0.0081**	**0.0003**	**0.0011**	**0.0018**	**0.0024**	**0.6705**	**0.7334**	**0.5242**	**0.5239**	**0.6150**	**0.5458**

Evaluation efficiency (ablation)

NEURAL INFORMATION PROCESSING SYSTEMS 2025



(a) w/o R&F (b) w/ R (c) w/ F (d) w/ R&F

(e) w/o R&F (f) w/ R (g) w/ F (h) w/ R&F

Figure 6: Visual comparisons on the impact of modules FCR (R) and FFM (F).

Table 3: Ablation study on the joint effect of FCR and FFM on recognition accuracy

Method			LFW	AgeDB
FCR	FFM	Protection		
✗	✗	○	99.71	97.72
✗	✓	○	99.30	97.28
✓	✗	◐	84.53	76.84
✓	✓	●	99.59	96.35

Table 4: Fractal depth k

k	Accuracy ↑	SSIM ↓	LPIPS ↑
1	99.71	0.5227	0.5291
2	99.69	0.4015	0.6353
3	96.46	0.3729	0.7925
4	92.13	0.2580	0.8357

Table 5: FBA pruning strength

Ratio	Accuracy ↑	SSIM ↓	LPIPS ↑
20%	99.83	0.7857	0.3184
40%	99.71	0.6291	0.4833
50%	99.69	0.3012	0.6839
60%	89.26	0.3109	0.7294
80%	87.24	0.2793	0.8605

Summary contributions

NEURAL INFORMATION PROCESSING SYSTEMS 2025

- **Fractal-based frequency transformation** for disrupting spatial regularities and concealing reconstruction-relevant visual cues.
- **Collaborative refinement of frequency channels** through FCR and FFM to reduce sparsity and suppress identity-irrelevant features.
- **Substantial privacy gains** of 15%–60% under both white-box and black-box attacks with minimal recognition accuracy loss.

NEURAL INFORMATION PROCESSING SYSTEMS 2025

Thank You For Listening!

If you have any other questions, please contact me with

dai.wanyingg@gmail.com

Code is available at https://github.com/Fracbeautyface/FracFace.

SICHUAN UNIVERSITY 四川大學

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

CityU 香港城市大學 City University of Hong Kong

NUS National University of Singapore