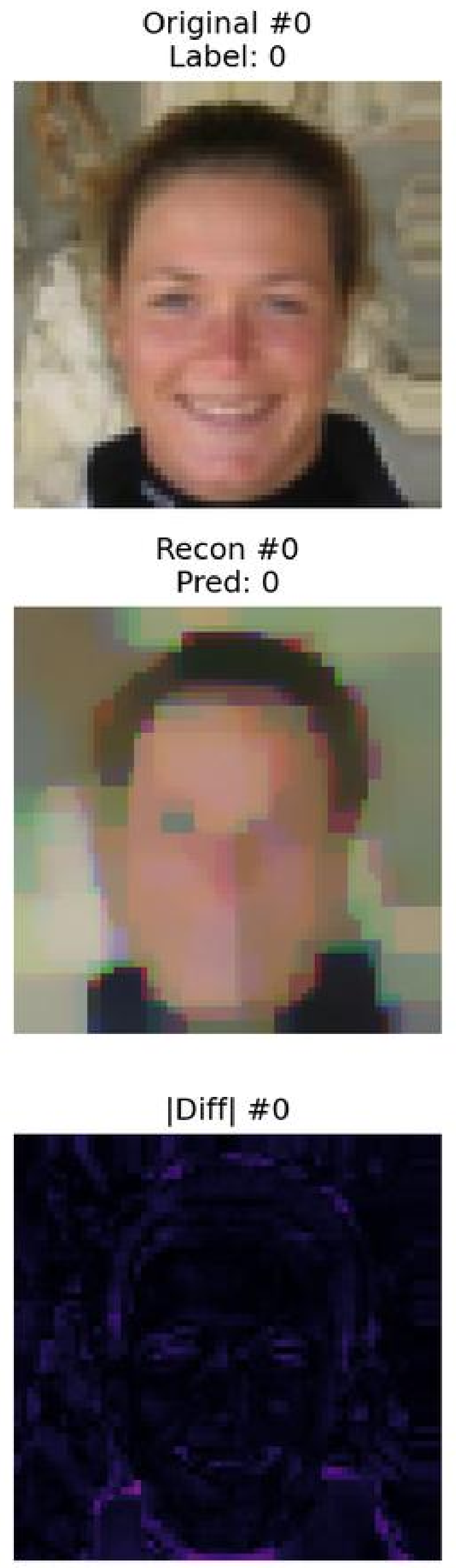
Federated Learning Privacy Attack Analysis

Defense Comparison • Anchor Client: Single Run

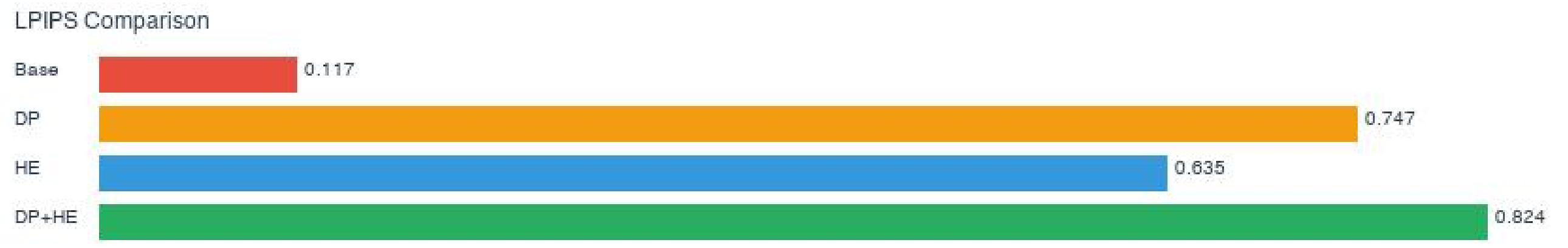
2025-12-16

BASELINE

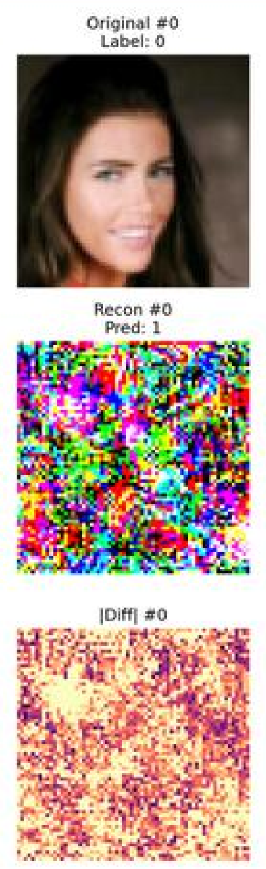


Attack Metrics

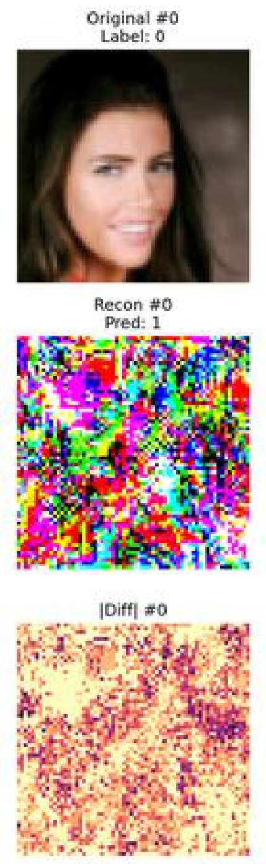
PSNR: **29.3750**
SSIM: **0.9203**
LPIPS: **0.1172**
LabelMatch**1.00**



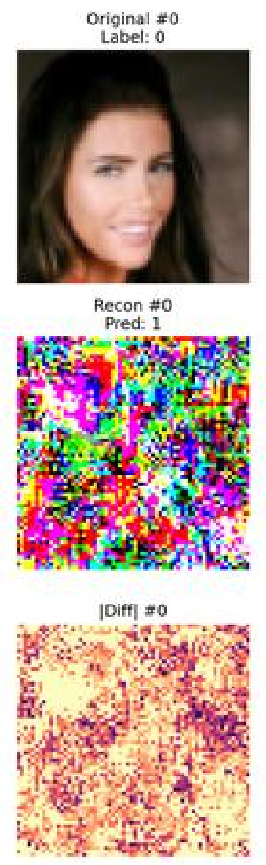
DIFFERENTIAL PRIVACY



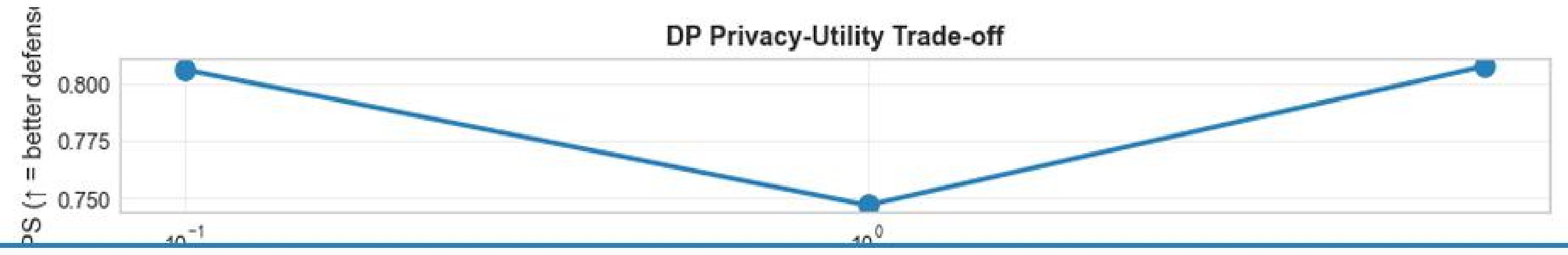
ε=8 (weak)
LPIPS: 0.807
SSIM: -0.001
PSNR: 6.7



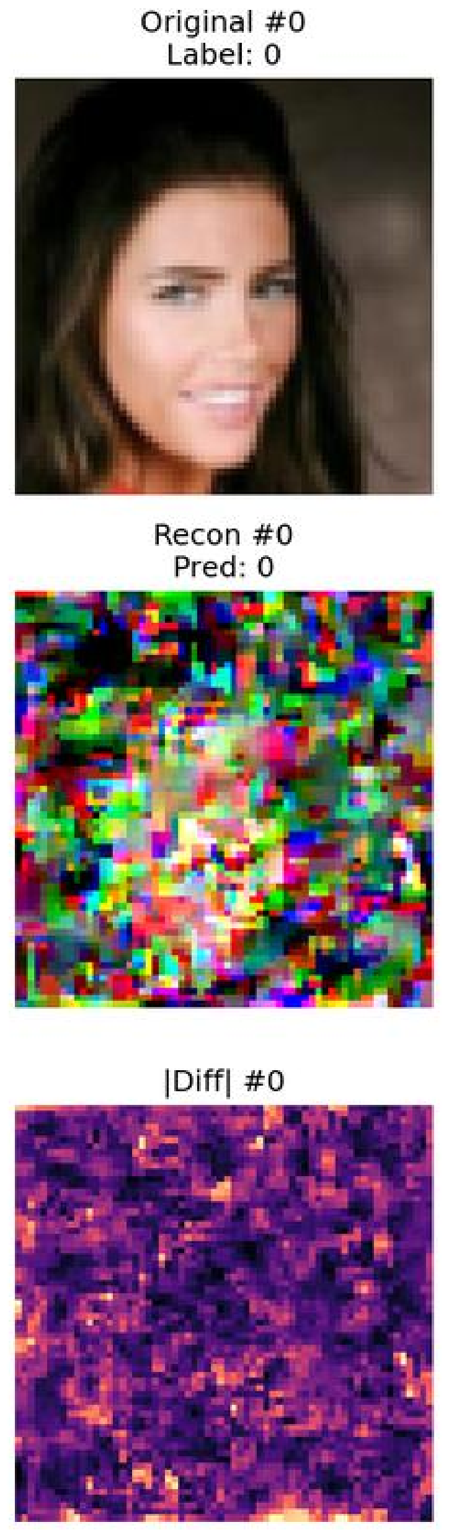
ε=1 (moderate)
LPIPS: 0.747
SSIM: -0.001
PSNR: 6.3



ε=0.1 (strong)
LPIPS: 0.806
SSIM: -0.001
PSNR: 6.4



HOMOMORPHIC ENCRYPTION



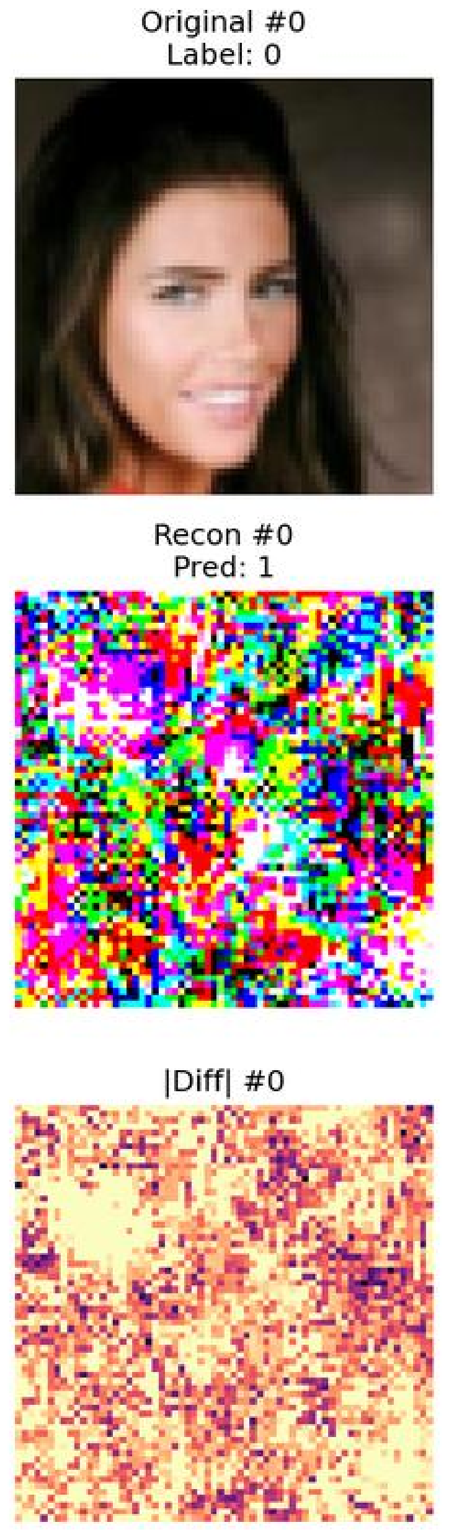
HE Defense Metrics

PSNR: **14.0320**
SSIM: **0.3434**
LPIPS: **0.6345**
LabelMatch**1.00**

Key Insight:

HE increases LPIPS by 0.517,
degrading attack quality.

DP + HE COMBINED



Combined Defense Metrics

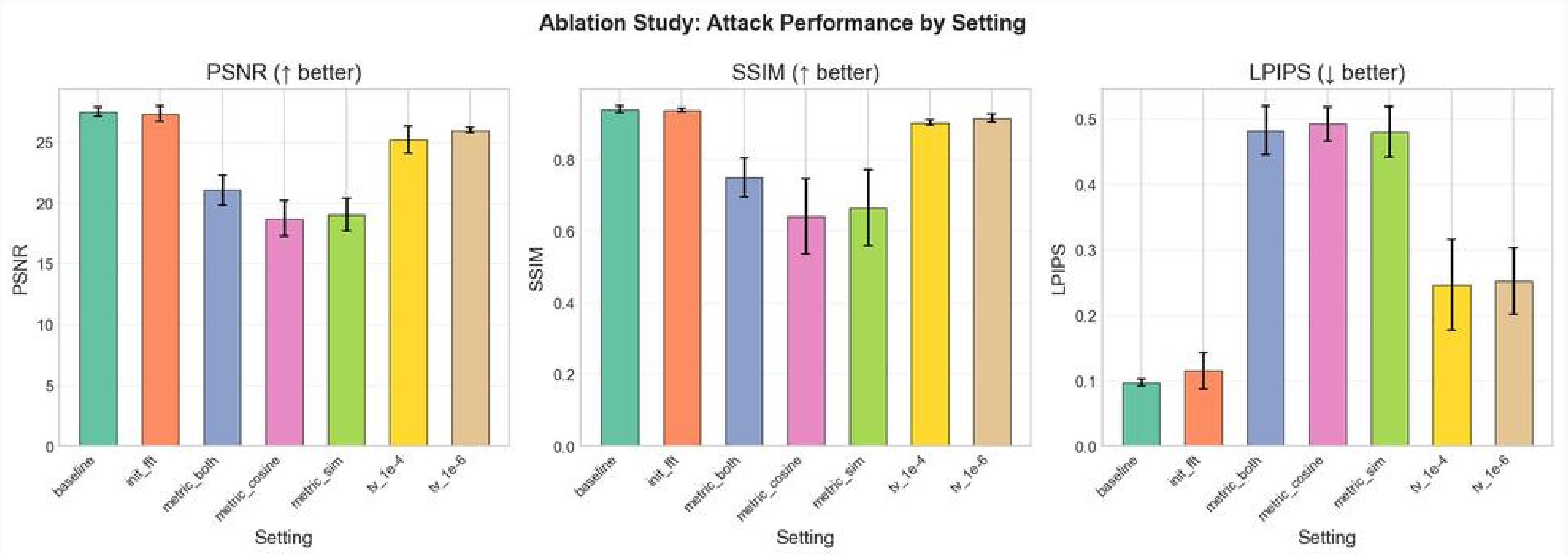
□ BEST

PSNR: **6.3660**
SSIM: **-0.0027**
LPIPS: **0.8243**
LabelMatch**0.00**

Defense Summary:

Combined DP+HE achieves
best protection (highest LPIPS).

ABLATION STUDY



Setting	PSNR	SSIM	LPIPS
baseline	27.53±0.36	0.94±0.01	0.10±0.01
init_fft	27.36±0.64	0.94±0.01	0.12±0.03
metric_both	21.08±1.25	0.75±0.05	0.48±0.04
metric_cosine	18.75±1.47	0.64±0.11	0.49±0.03
metric_sim	19.05±1.39	0.67±0.11	0.48±0.04
tv_1e-4	25.23±1.13	0.90±0.01	0.25±0.07
tv_1e-6	26.01±0.24	0.92±0.01	0.25±0.05

Key Takeaways

- Best setting: 'baseline' (LPIPS: 0.098)
- 'metric_cosine' shows 0.395 higher LPIPS (worse attack)
- SSIM varies by 0.299 across ablation settings