Anti-I2V: Safeguarding your photos from malicious image-to-video generation

Duc Vu Anh Nguyen Chi Tran Anh Tran

Qualcomm AI Research is an initiative of Qualcomm Teachnologies, Inc.

Duc Vu & Anh Nguyen are looking for Summer 2027 Intern

CVPR JUNE 3-7, 2026 DENVER COLORADO

Problem

=> Source image protection is **critical to prevent misuse**

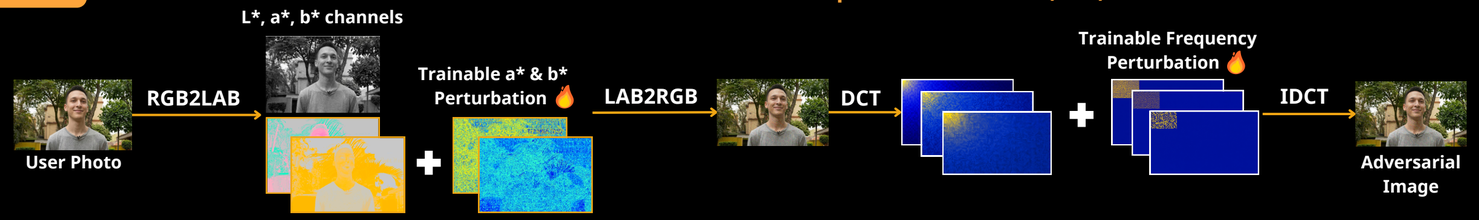
SOLUTION: Following adversarial attacks, add **imperceptible noise** to user image to **disrupt I2V models**

Contribution

1. **Dual-Space Perturbation (DSP):** Updates noise in both L∗a∗b∗ color and Frequency space
   => **Enhanced effectiveness & robustness**
2. **Inter Representation Collapse (IRC) and Inter Representation Anchor (IRA):** Layer-wise feature disruption in both denoising and VAE modules
   => **Degrade temporal coherence & generation fidelity**

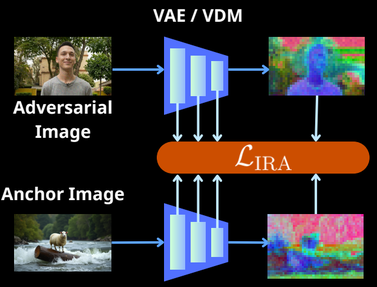
Method

Dual-Space Perturbation (DSP)



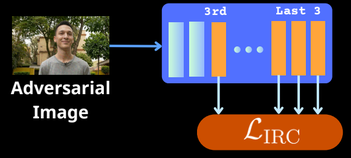
Goal: DSP creates **highly imperceptible** perturbations that are **difficult to purify or remove**

Inter Representation Anchor



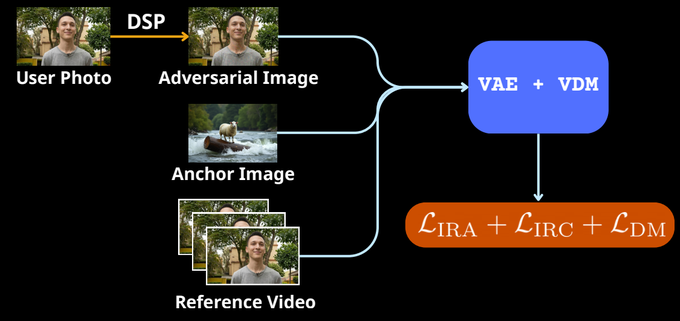
Goal: IRA aligns layer-wise feature of user input into **UNRELATED** image

Inter Representation Collapse



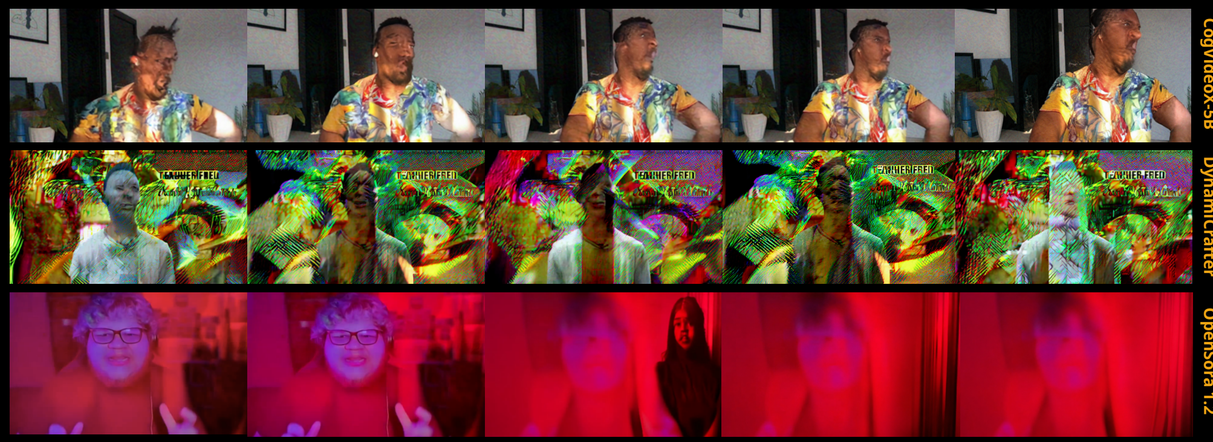
Goal: IRC **suppresses** rich semantic features (Late layers) into **low-information features** (Early layers)

Final Pipeline



Model	Method	CelebV-Text ISM ↓	CelebV-Text C-FIQA ↓	CelebV-Text Q-A(F) ↓	CelebV-Text Q-A(V) ↓	CelebV-Text DINO ↓	UCF101 ISM ↓	UCF101 C-FIQA ↓	UCF101 Q-A(F) ↓	UCF101 Q-A(V) ↓	UCF101 DINO ↓
CogVideoX-5B	Clean	0.721	0.522	0.746	0.802	0.828	0.466	0.373	0.361	0.436	0.801
	SDS+ [63]	0.591	0.482	0.473	0.563	0.754	0.381	0.291	0.286	0.344	0.754
	SDS- [63]	0.607	0.497	0.511	0.594	0.747	0.386	0.298	0.313	0.393	0.760
	AdvDM [31]	0.583	0.473	0.463	0.543	0.748	0.370	0.292	0.271	0.342	0.753
	MIST [30]	0.561	0.463	0.476	0.577	0.750	0.355	0.290	0.262	0.340	0.751
	VGMShield [44]	0.554	0.461	0.464	0.557	0.745	0.361	0.292	0.265	0.343	0.753
	Anti-I2V	**0.448**	**0.433**	**0.447**	**0.532**	**0.722**	**0.346**	**0.283**	**0.251**	**0.323**	**0.734**
DynamiCrafter	Clean	0.528	0.467	0.724	0.794	0.622	0.384	0.345	0.501	0.562	0.709
	SDS+ [63]	0.264	0.372	0.213	0.245	0.389	0.122	0.305	0.157	0.194	0.433
	SDS- [63]	0.278	0.418	0.223	0.250	0.392	0.128	0.338	0.164	0.226	0.439
	AdvDM [31]	0.269	0.370	0.167	0.207	0.397	0.110	0.335	0.162	0.201	0.451
	MIST [30]	0.262	0.379	0.232	0.269	0.386	0.100	0.335	0.322	0.381	0.493
	VGMShield [44]	0.286	0.431	0.243	0.289	0.401	0.108	0.336	0.318	0.374	0.486
	Anti-I2V	**0.151**	**0.303**	**0.032**	**0.047**	**0.167**	**0.068**	**0.268**	**0.057**	**0.084**	**0.164**
Open-Sora	Clean	0.598	0.508	0.712	0.782	0.811	0.400	0.382	0.409	0.437	0.750
	SDS+ [63]	0.502	0.481	0.494	**0.548**	0.730	0.355	0.293	0.360	0.389	0.692
	SDS- [63]	0.508	0.494	0.514	0.591	0.731	0.333	0.311	0.351	0.387	0.687
	AdvDM [31]	0.506	0.478	0.496	0.561	0.725	0.346	0.309	0.327	0.362	0.686
	MIST [30]	0.493	0.475	0.497	0.594	**0.710**	0.339	0.309	0.338	0.392	0.677
	VGMShield [44]	0.500	0.476	0.497	0.578	0.716	0.341	0.312	0.335	0.369	0.680
	Anti-I2V	**0.461**	**0.453**	**0.478**	0.554	0.713	**0.318**	**0.248**	**0.311**	**0.347**	**0.642**

State-of-the-Art on Diverse I2V Backbones



Results

- High Protection
- Robust
- Memory-Efficient (< 40GB VRAM)