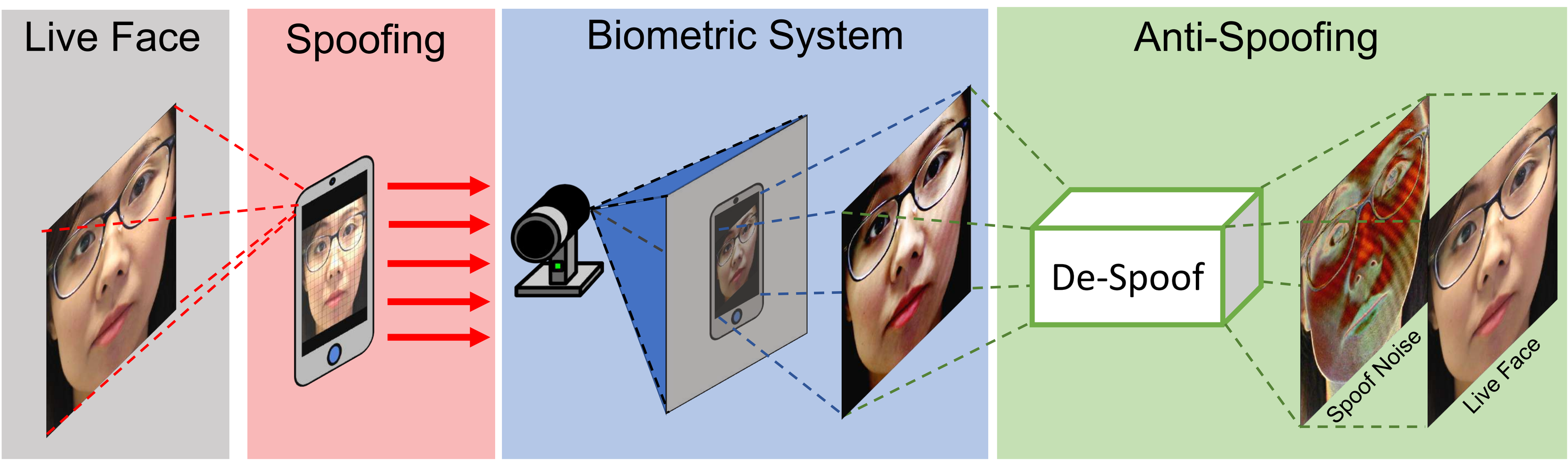
Face De-Spoofing: Anti-spoofing via Noise Modeling

Amin Jourabloo*, Yaojie Liu*, Xiaoming Liu
Department of Computer Science and Engineering, Michigan State University, MI

MICHIGAN STATE UNIVERSITY · Computer Vision Lab · ECCV 2018 European Conference on Computer Vision

Introduction



- Decompose a spoof face into spoof noise and live face
- Analyze the properties of the spoof noise
- Focus on print and replay attack

A Case Study of Spoof Noise Pattern

➤ What are the causes of spoof noise pattern?

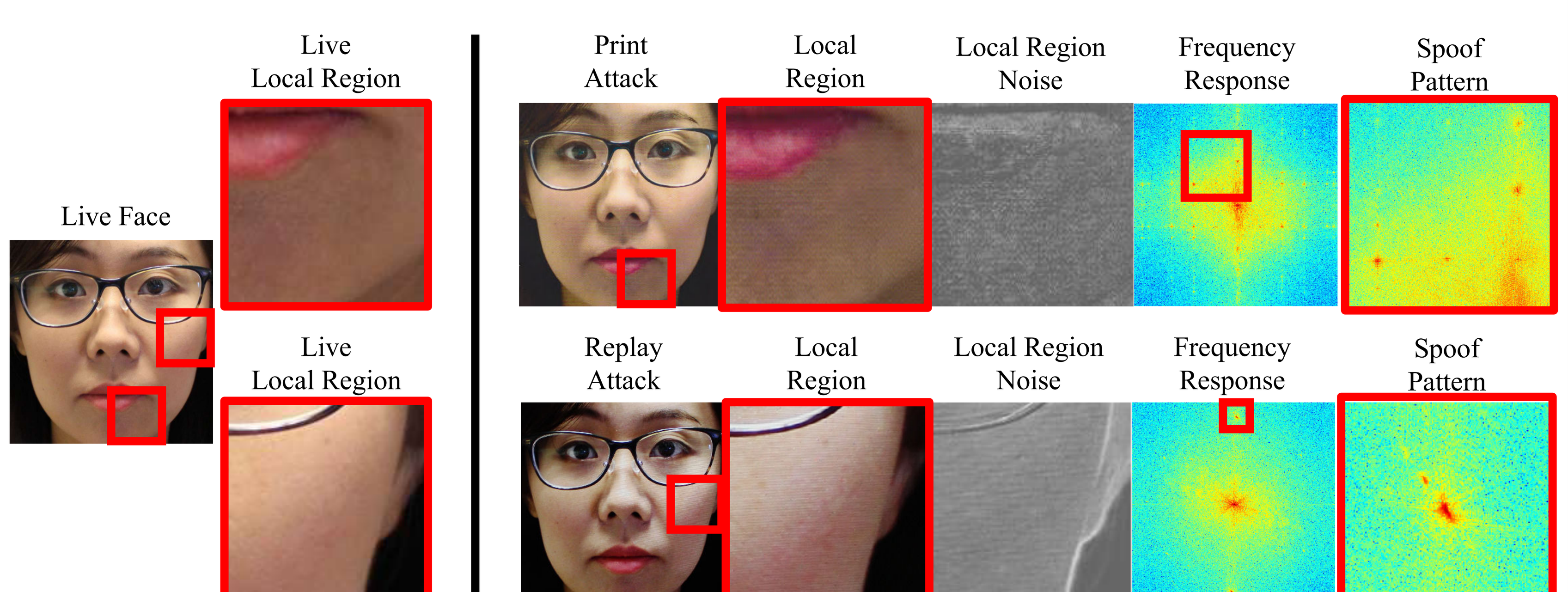
- Color Distortions
- Display artefacts
- Presenting artefacts
- Imaging artefacts

➤ What are the characteristics of spoof noise pattern?

- Repetitive
- Ubiquitous

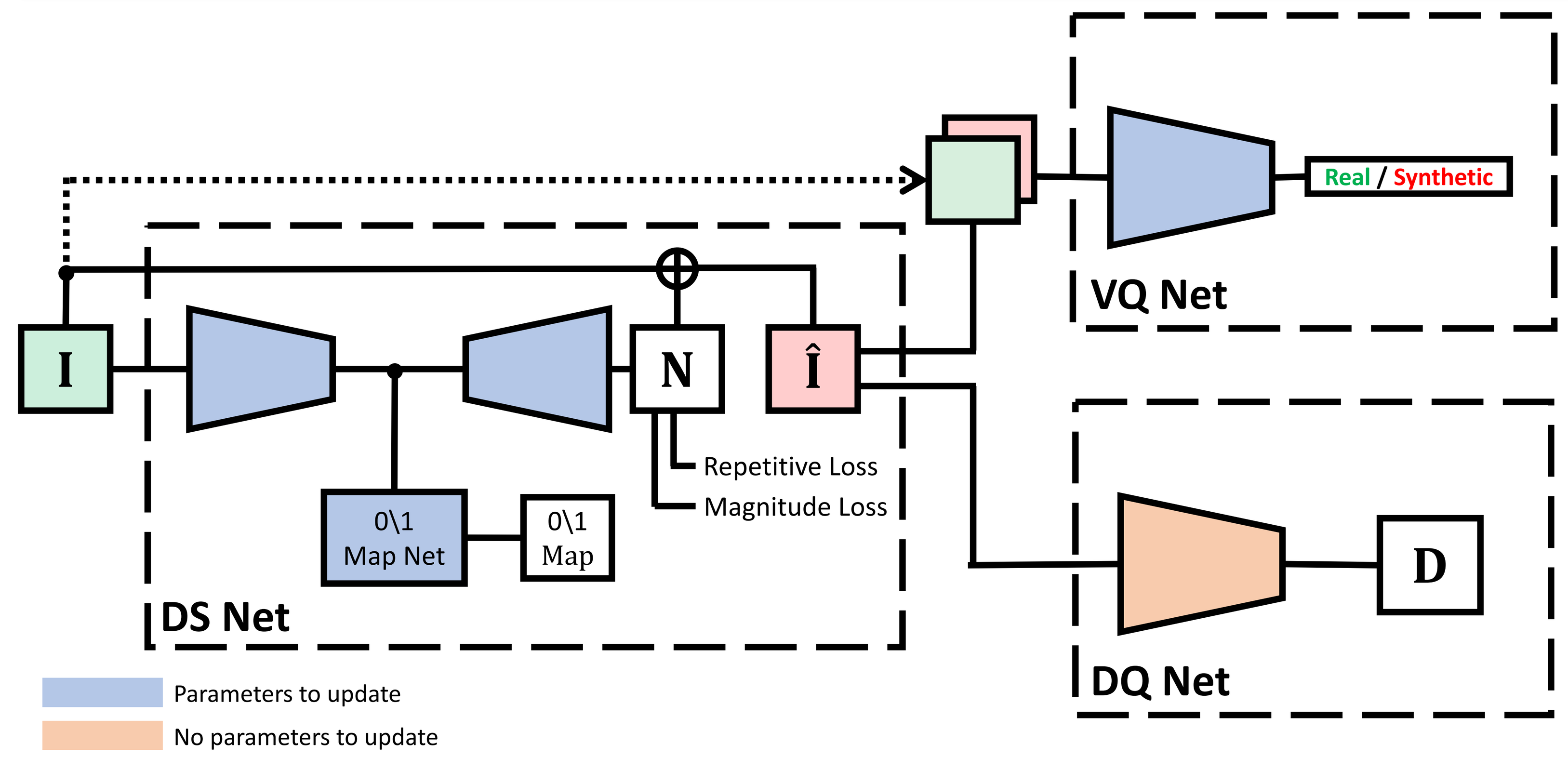
➤ How to model the spoofing process?

$$\mathbf{x} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{n} = \hat{\mathbf{x}} + (\mathbf{A} - \mathbb{I})\hat{\mathbf{x}} + \mathbf{n} = \hat{\mathbf{x}} + N(\hat{\mathbf{x}})$$



* denotes equal contribution by the authors.

Proposed Method



➤ De-Spoof Net (DS Net)

- To estimate spoof noise pattern N and reconstruct the live image Î
- Use 3D face shape to do non-rigid registration.

➤ Discriminative Quality Net (DQ Net)

- To guarantee reconstructed Î is photorealistic

➤ Visual Quality Net (VQ Net)

- To guarantee reconstructed Î is recognized as live by a pretrained model

Loss Functions

➤ De-Spoof Net (DS Net)

- Repetitive Loss

$$J_r = \begin{cases} -\max(H(\mathcal{F}(\mathbf{N}), k)), & \mathbf{I} \in Spoof \\ \|\max(H(\mathcal{F}(\mathbf{N}), k))\|_1, & \mathbf{I} \in Live \end{cases}$$

- Zero\One Map Loss

$$J_z = \|\mathrm{CNN}_{01map}(\mathbf{F}; \Theta) - \mathbf{M}\|_1$$

- Magnitude Loss

$$J_m = \|\mathbf{N}\|_1 \quad \text{for live}$$

➤ Discriminative Quality Net (DQ Net)

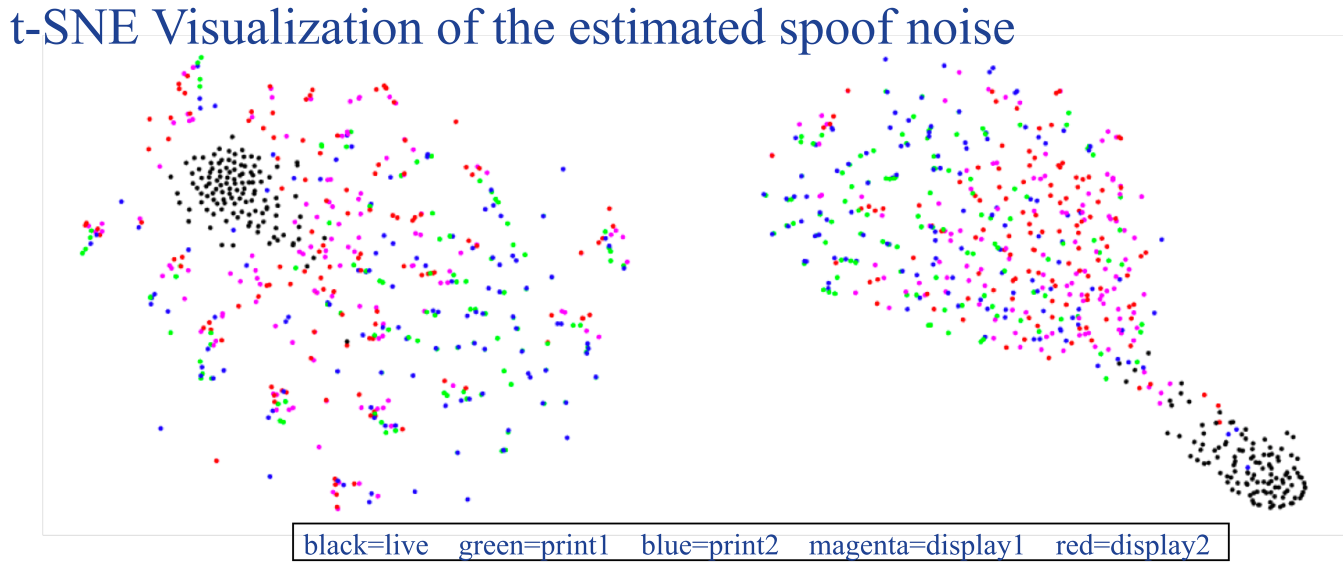
$$J_{DQ} = \left\|\mathrm{CNN}_{DQ}(\hat{\mathbf{I}}) - \mathbf{D}\right\|_1$$

➤ Visual Quality Net (VQ Net)

$$J_{VQ_{train}} = -\mathbb{E}_{\mathbf{I}\in\mathcal{R}} \log(\mathrm{CNN}_{VQ}(\mathbf{I})) - \mathbb{E}_{\mathbf{I}\in\mathcal{S}} \log(1 - \mathrm{CNN}_{VQ}(\mathrm{CNN}_{DS}(\mathbf{I})))$$

Experimental Results

➤ t-SNE Visualization of the estimated spoof noise

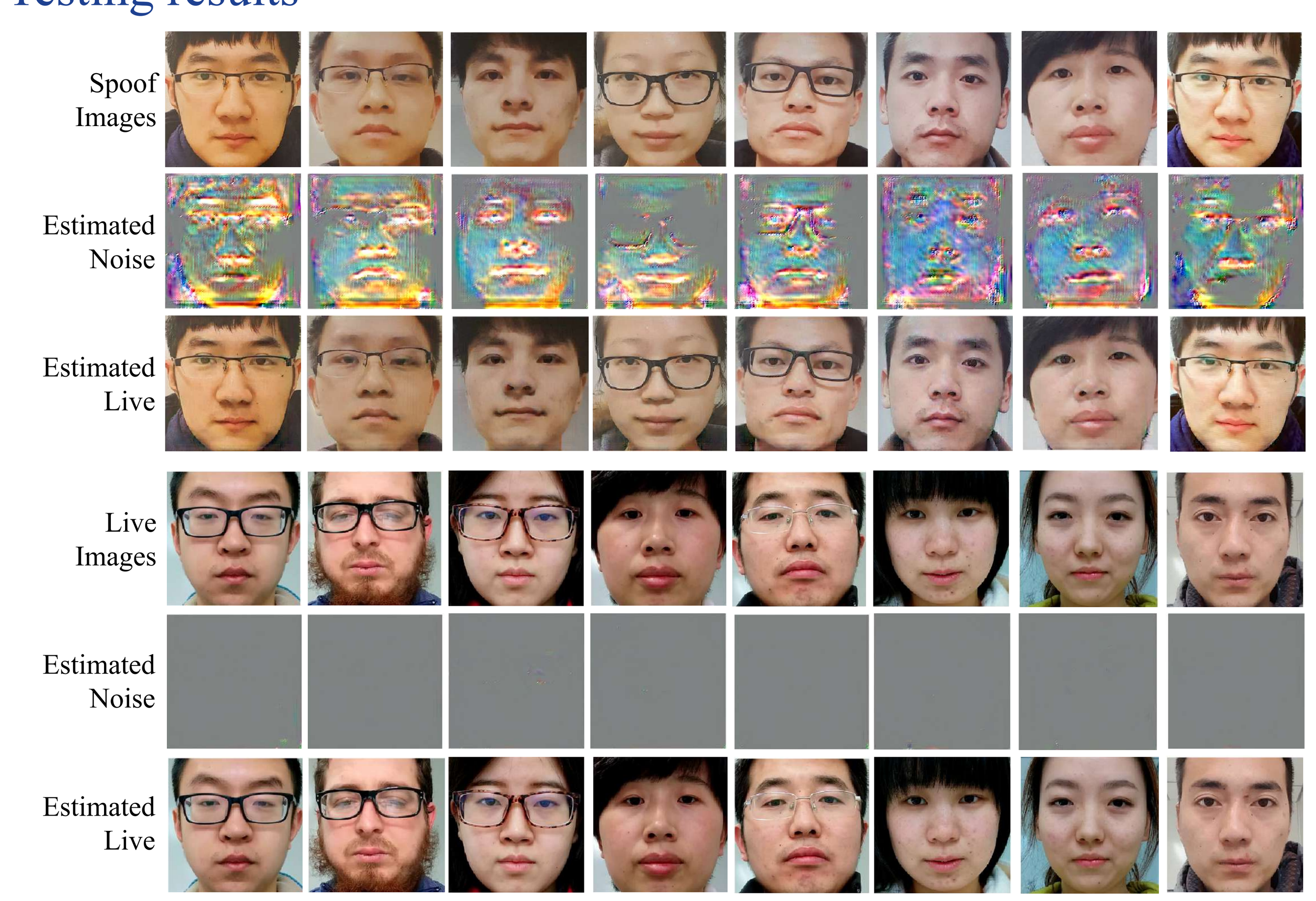


black=live green=print1 blue=print2 magenta=display1 red=display2

➤ Intra-test on Oulu

Protocol	Method	APCER	BPCER	ACER
Various illumination conditions	CPqD	2.9%	10.8%	6.9%
	GRADIANT	1.3%	12.5%	6.9%
	CVPR 18	1.6%	1.6%	1.6%
	Proposed method	**1.2%**	**1.7%**	**1.5%**
Different spoof medium	MixedFASNet	9.7%	2.5%	6.1%
	Proposed method	**4.2%**	**4.4%**	**4.3%**
	CVPR 18	2.7%	2.7%	2.7%
	GRADIANT	3.1%	1.9%	2.5%
Different camera devices	MixedFASNet	5.3±6.7%	7.8±5.5%	6.5±4.6%
	GRADIANT	2.6±3.9%	5.0±5.3%	3.8±2.4%
	Proposed method	4.0±1.8%	3.8±1.2%	3.6±1.6%
	CVPR'18	**2.7±1.3%**	**3.1±1.7%**	**2.9±1.5%**
All above challenges	Massy_HNU	35.8±35.3	8.3±4.1%	22.1±17.6%
	GRADIANT	5.0±4.5%	15.0±7.1%	10.0±5.0%
	CVPR'18	9.3±5.6%	10.4±6.0%	9.5±6.0%
	Proposed method	**5.1±6.3%**	**6.1±5.0%**	**5.6±5.7%**

➤ Testing results



➤ Acknowledgement

- This research is based upon work supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via IARPA R&D Contract No. 2017-17020200004. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.