

# Attack examples

Attack: PGD

Optimisation target: Reconstruction loss

Codec: bmslj2018-hyperprior

Original image



PGD

Attacked image



compression

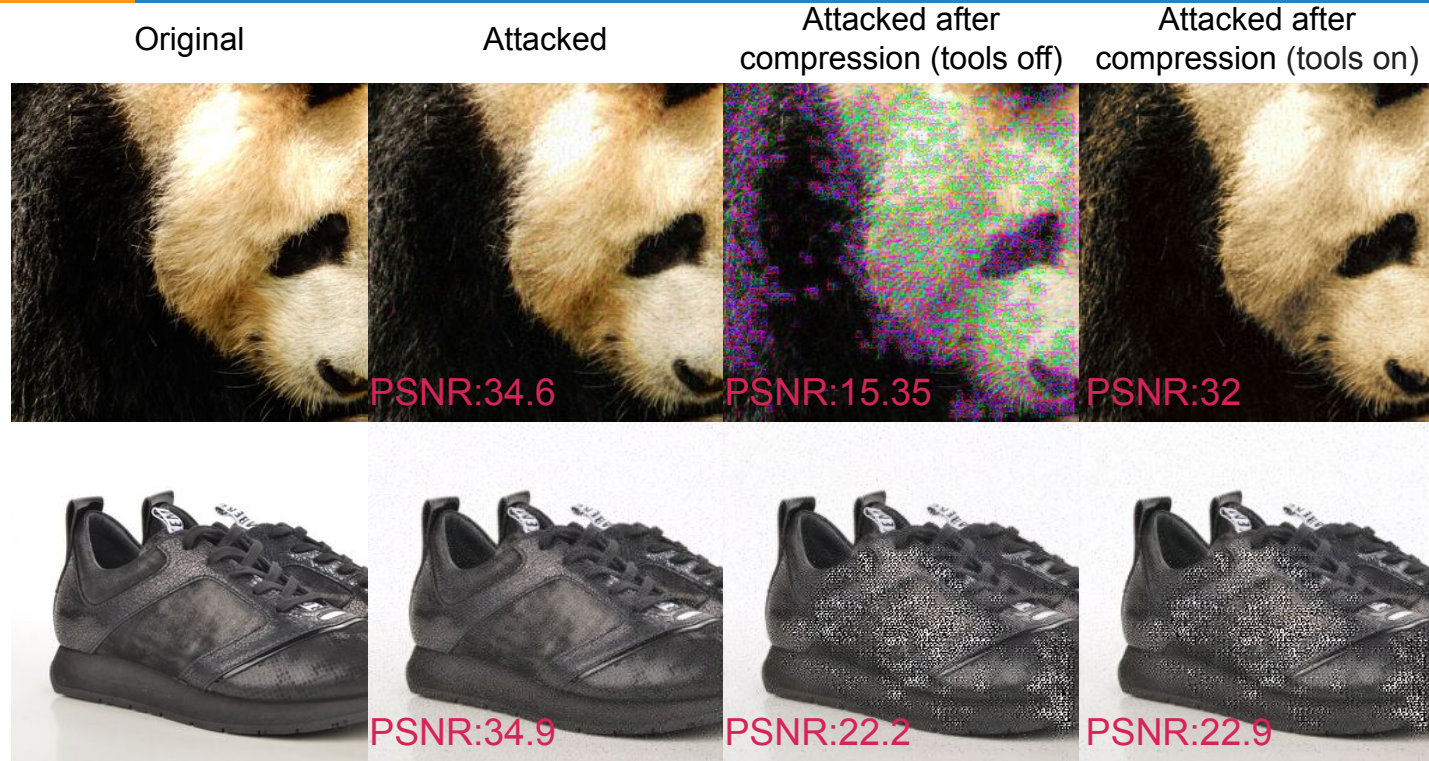
Attacked image after compression



# JPEG AI v5.1 (hop) examples

Attack:  
MADC

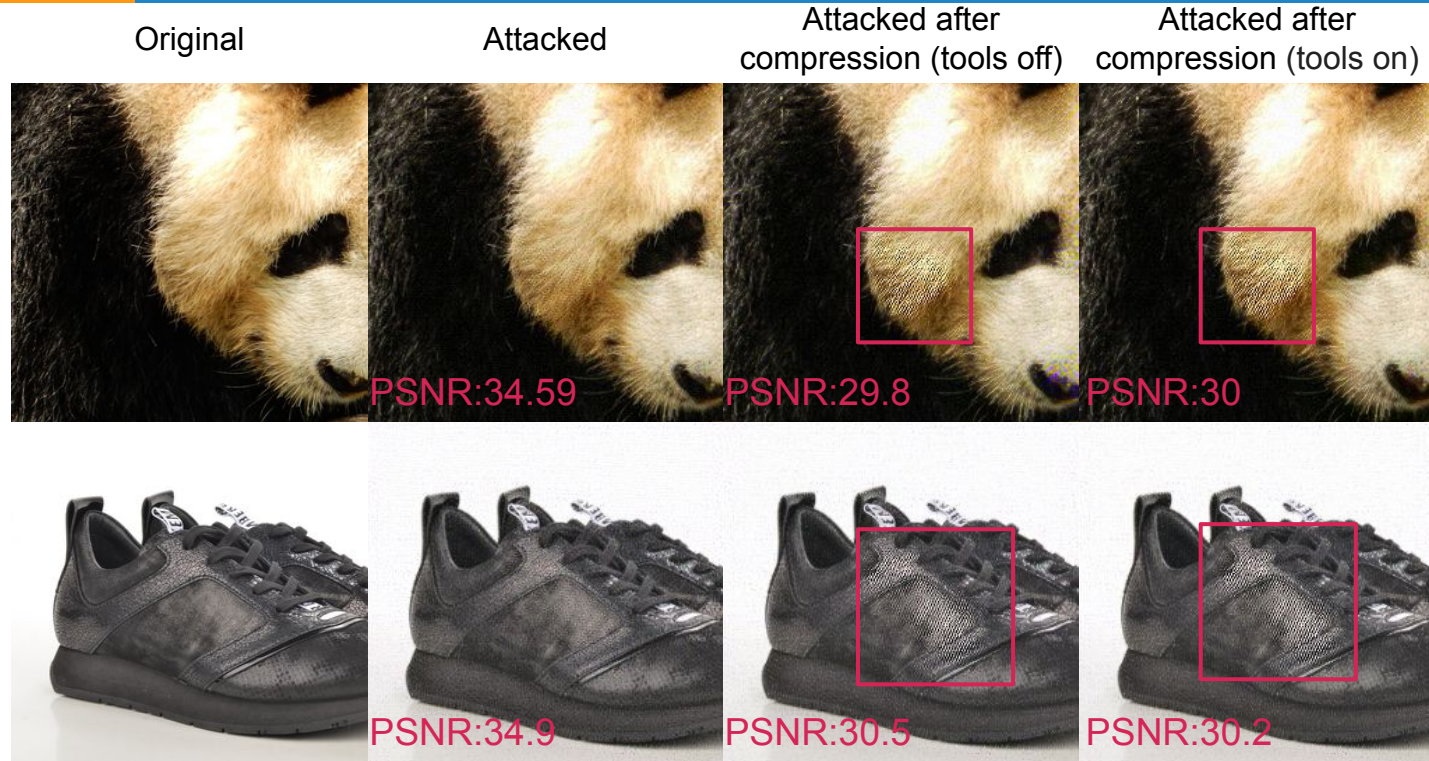
Optimisation target:  
Added-noises





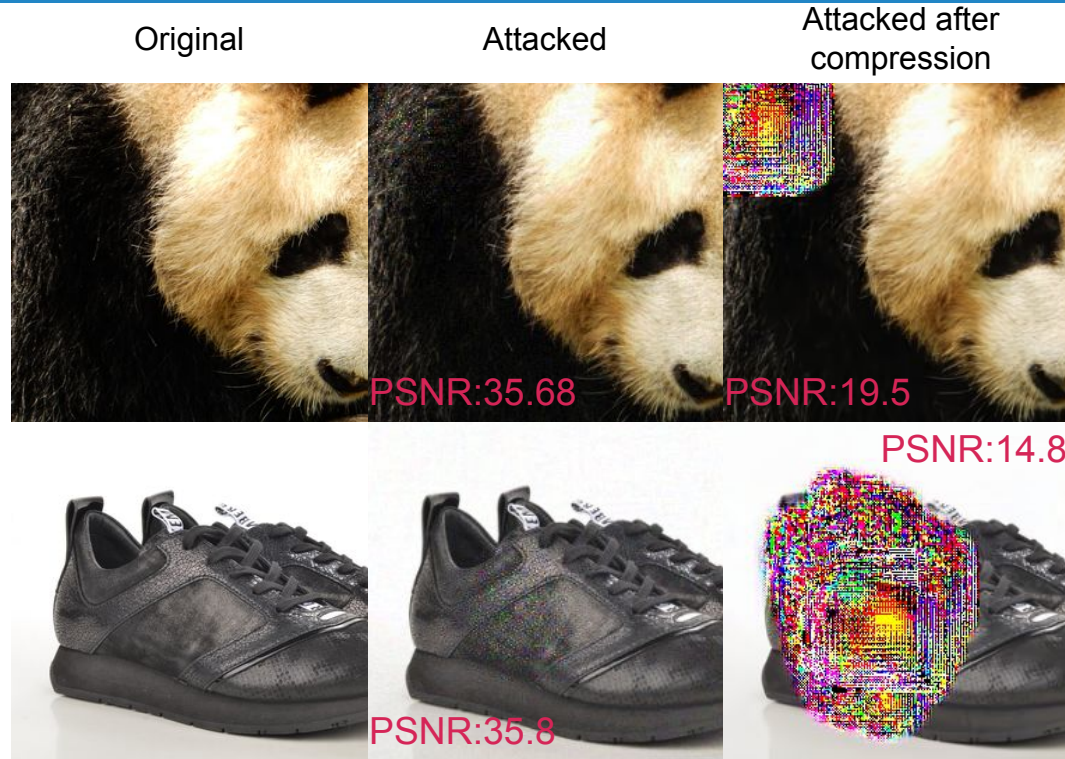
# JPEG AI v6.1 (hop) examples

Attack:  
MADC  
Optimisation target:  
Added-noises



# Cheng 2020 anchor examples

Attack:  
MADC  
Optimisation target:  
Added-noises





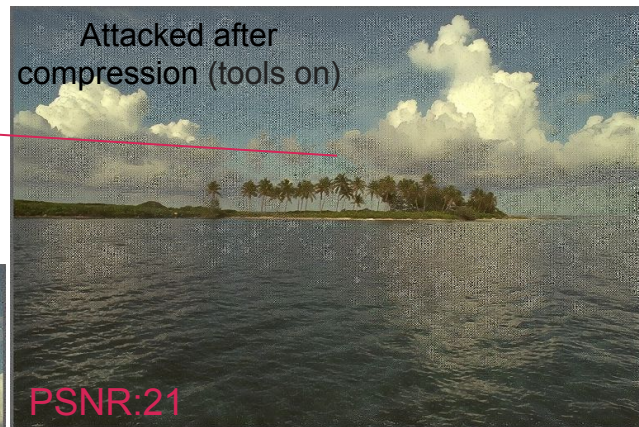
# JPEG AI v5.1 (bop) examples

Attack:  
MADC  
Optimisation target:  
Added-noises-Y



Original

Attacked





# JPEG AI v6.1 (bop) examples

Attack:  
MADC  
Optimisation target:  
Added-noises-Y

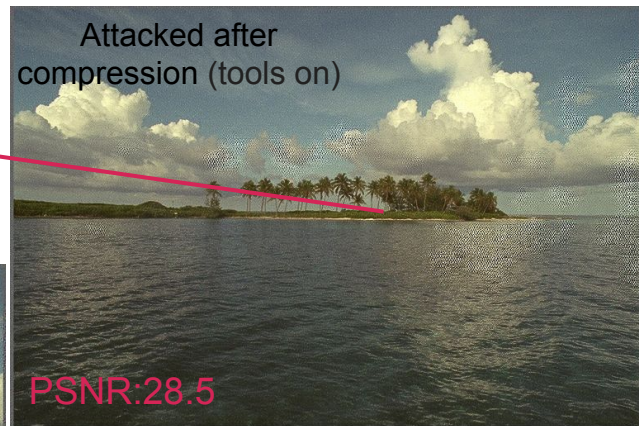


Original

Attacked



PSNR:35.2



PSNR:28.5

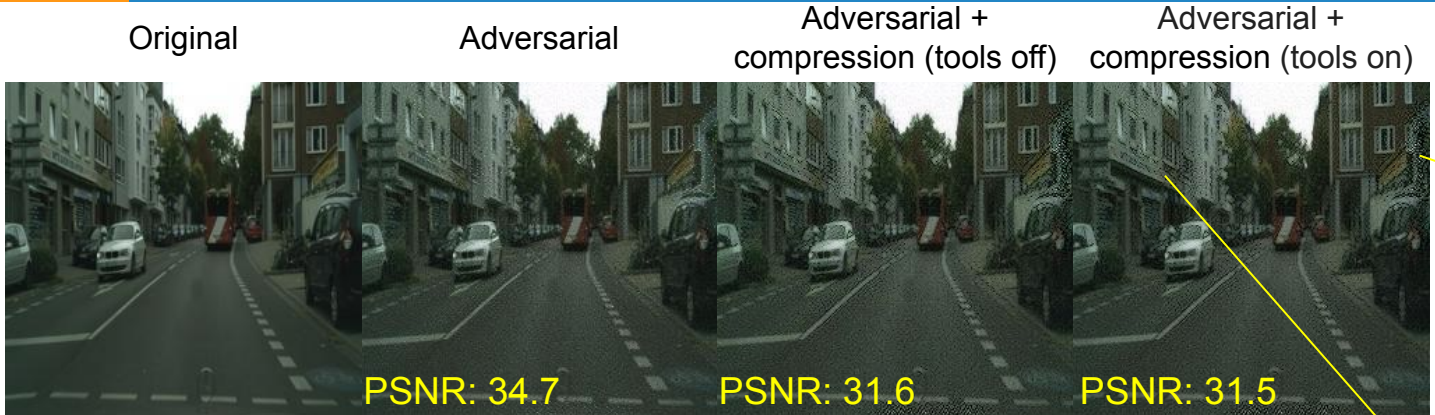


PSNR:28.7

# JPEG AI (hop) v5.1 vs v6.1 examples

Attack:  
MADC  
Optimisation target:  
Added-noises-Y

V6.1



V5.1



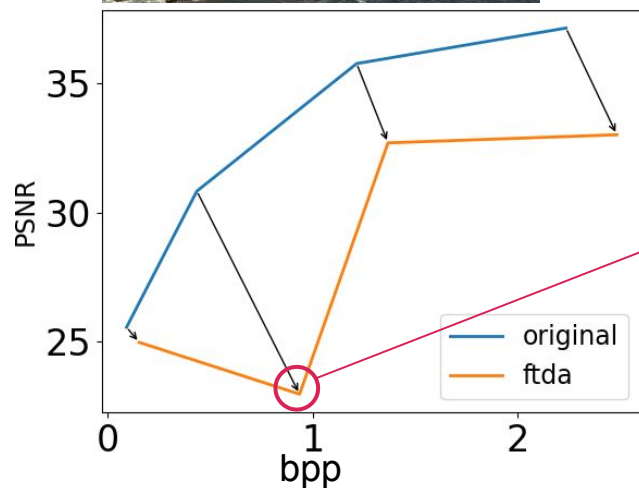


# JPEG AI attacks

## v6.1 BOP examples



rd-curves for original  
and attacked images



compression





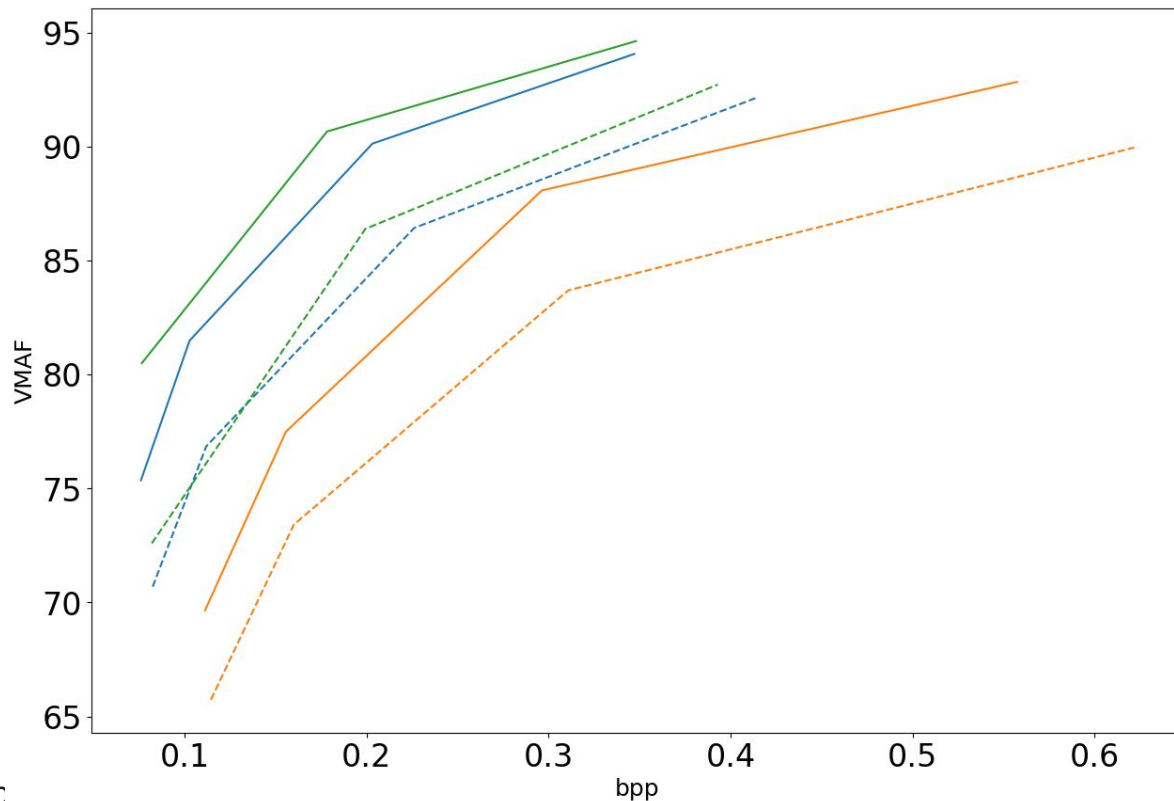
# NICs attacks

## RD-curves examples

I-FGSM attack with  $\epsilon = 5/255$



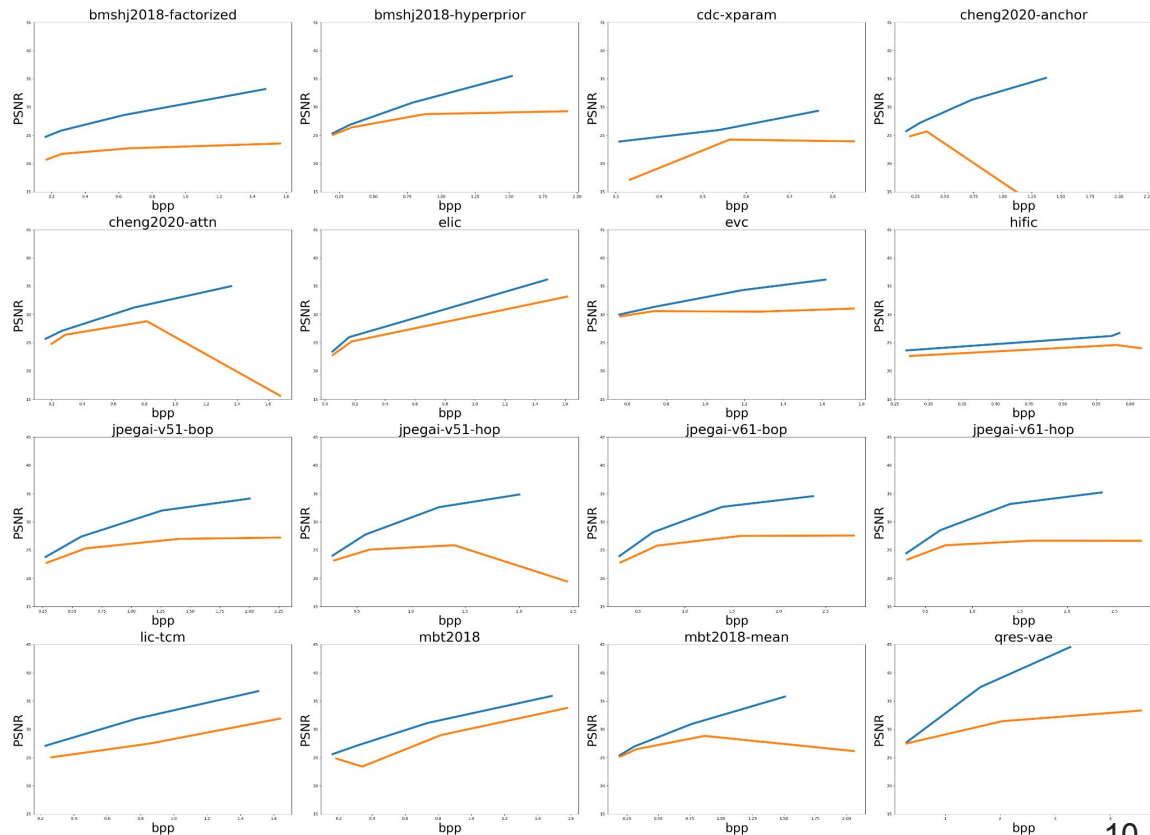
- cheng2020-attn original
- - cheng2020-attn attacked
- bmsbj2018-factorized original
- - bmsbj2018-factorized attacked
- lic-tcm original
- - lic-tcm attacked



# Results: codecs' robustness

## RD-curves, attack: FTDA

— Original  
— Adversarial



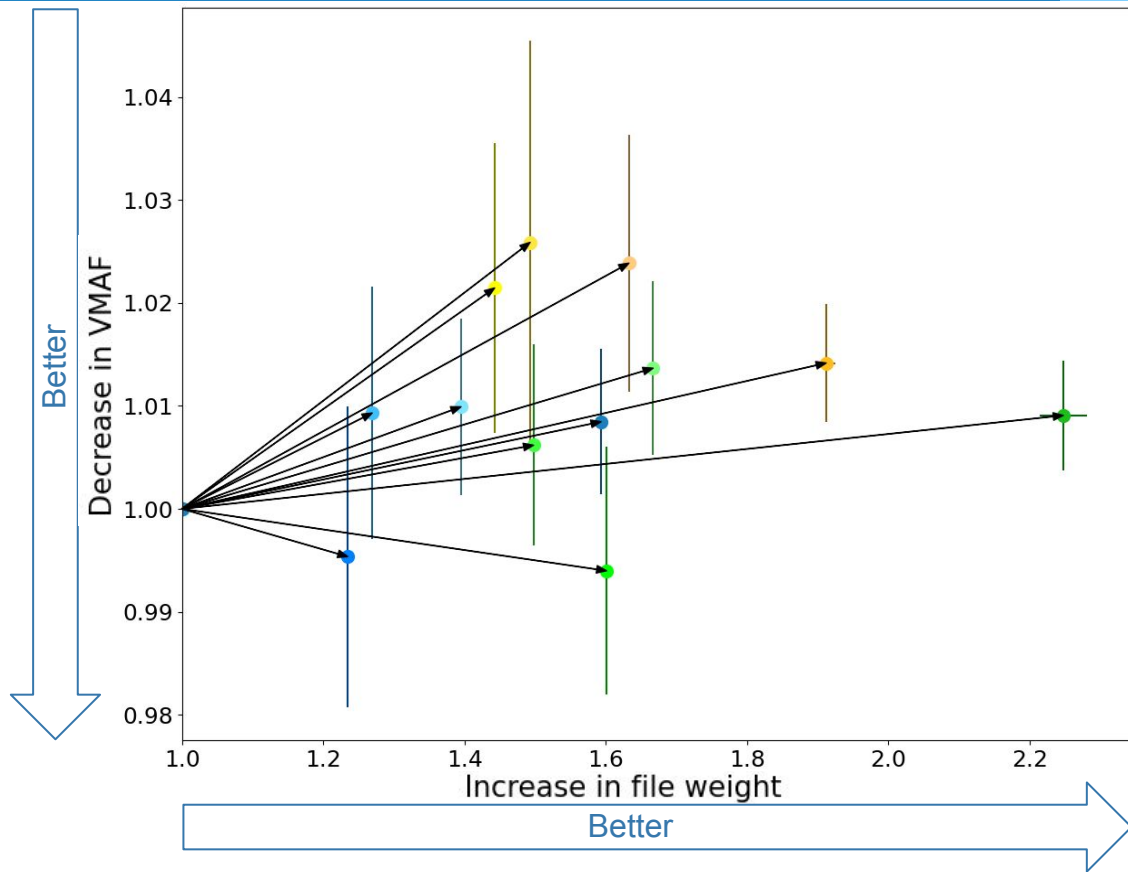
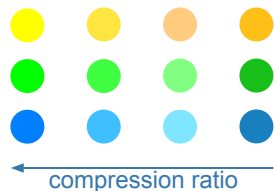


# NICs bitrate attacks

## Results

I-FGSM attack with  $\epsilon = 5/255$

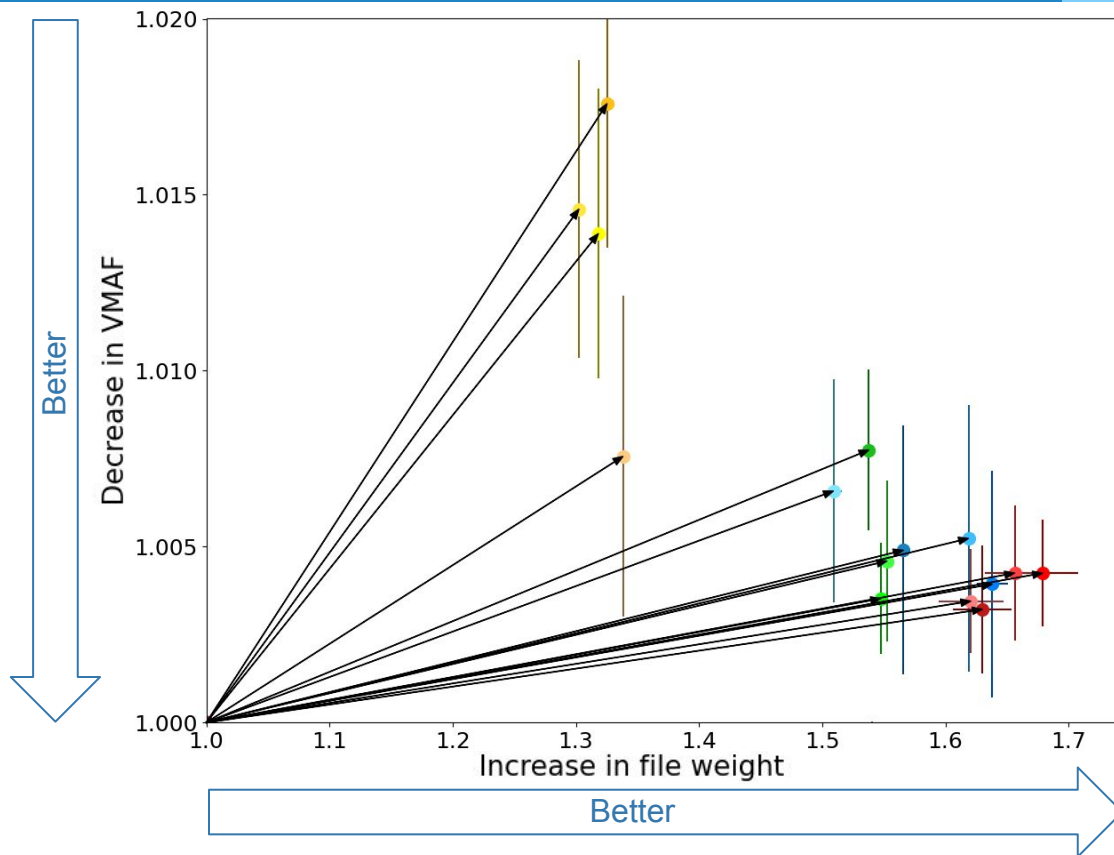
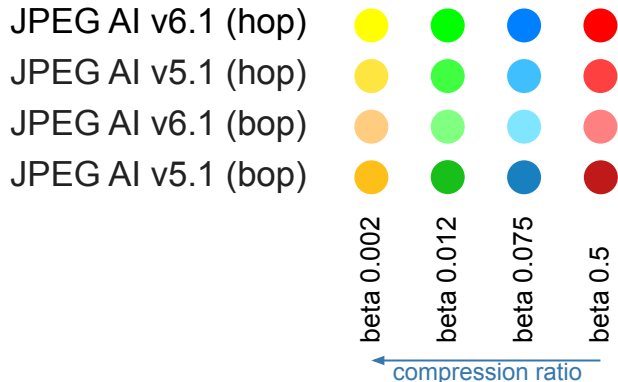
Cheng 2020 attn  
bmshj 2018 (hyper)  
bmshj 2018 (factor)



# JPEG AI bitrate attacks

## Results

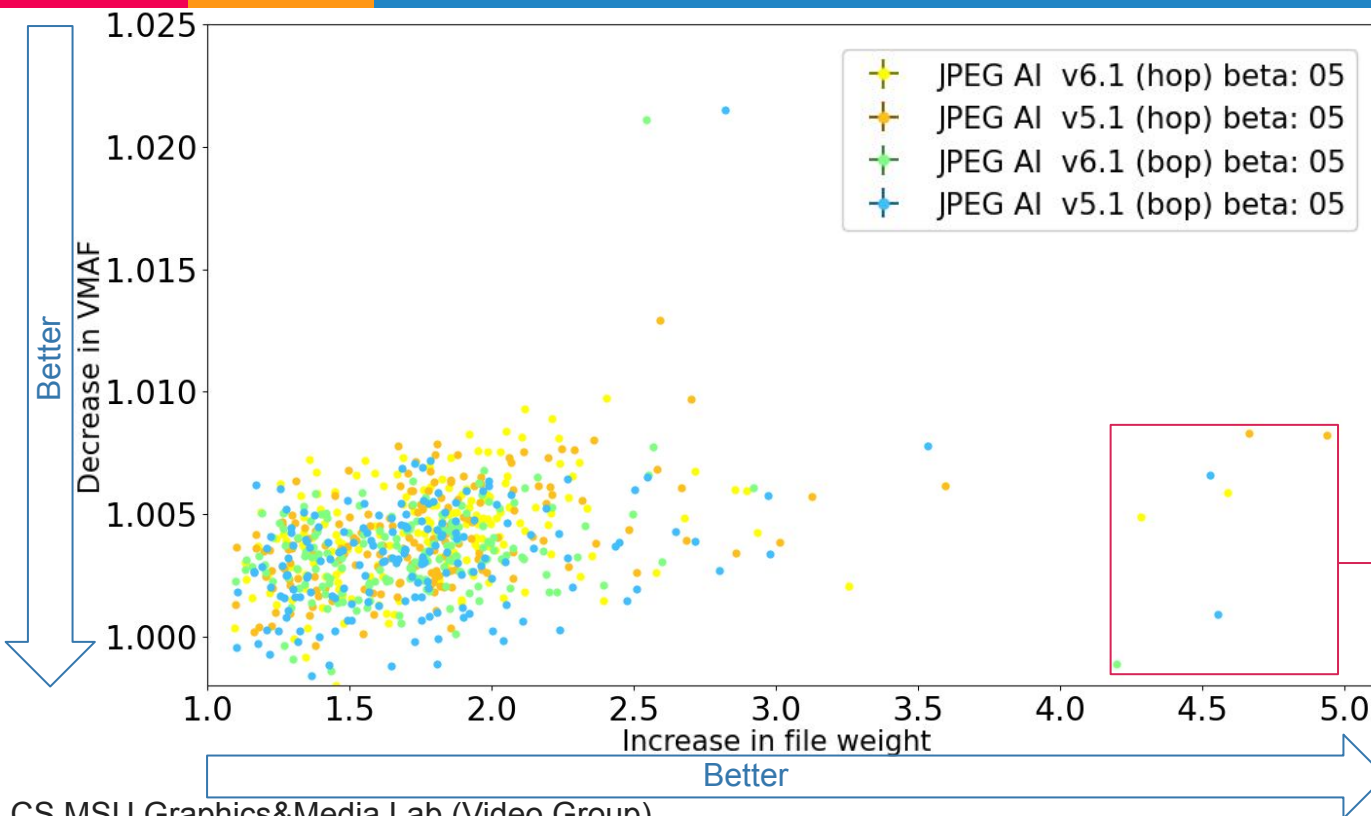
I-FGSM attack with  $\epsilon = 5/255$





# JPEG AI bitrate attacks

## High-bitrate examples



I-FGSM attack with  $\text{eps} = 5/255$

All versions of the codec are vulnerable to attack.

# JPEG AI bitrate attacks examples

Input

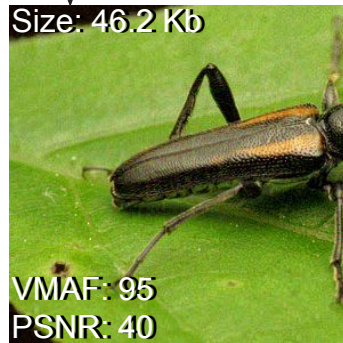
JPEG AI v6.1 (HOP)

JPEG 2000

Original



Attacked



+220% of size

+146% of size

In this example, the coding noise resistance of JPEG AI is 1.5 times lower than that of JPEG 2000



# JPEG AI v5.1 bitrate attacks examples

