Supplementary Material : Feature Distillation: DNN-Oriented JPEG Compression Against Adversarial Examples

Zihao Liu[1], Qi Liu[1], Tao Liu[1], Nuo Xu[1], Xue Lin[2], Yanzhi Wang[2], Wujie Wen[1]
[1] Flordia International University, [2] Northeastern University
{zliu021,qliu020,tliu023,nxu003,wwen}@fiu.edu, {xue.lin, yanz.wang}@northeastern.edu

In this supplementary material, we compare the visual artifacts (PSNR/SSIM) of three random selected images compressed by our "feature distillation" (FD) method and the standard JPEG at different quality factors (QFs).

1 Comparison of Visual Quality–Qualitative

Fig. 1 and Fig. 2 illustrate the corresponding visual results produced by default JPEG compression and our "feature distillation" method, respectively. As Fig. 2 shows, it is hardly to perceive the differences between the original (QF=100, JPEG) and our FD(1x) compressed images for human eyes. To better mitigate the most recent BPDA attack, we further increase the quantization step of our method–FD(2x) and FD(3x). As Fig. 2 shows, the visual distortions are still very limited compared with JPEG images with lower QFs.

2 Comparison of Visual Quality–Quantitative

As Table. 1 shows, all these three images compressed by our method (FD(1x)) can achieve reasonable PSNR and SSIM, e.g. close to that of $QF = 75$ for JPEG, which is still acceptable for most visual systems. Similarly, the PSNR and SSIM of our FD(2x) and FD(3X) are comparable with JPEG method at $QF = 50$ and $QF = 20$, respectively.

Table 1: The comparision of PSNR/SSIM between "feature distillation" (FD) and JPEG.

	Img. 1		**Img. 2**		**Img. 3**	
	PSNR	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**
JEPG(QF=75)	33.63	0.94	28.64	0.94	35.64	0.97
JEPG(QF=50)	31.41	0.92	26.05	0.89	33.75	0.96
JEPG(QF=20)	28.81	0.87	23.56	0.82	31.03	0.94
FD(1x)	33.05	0.93	29.12	0.94	34.86	0.97
FD(2x)	30.03	0.89	26.29	0.89	32.53	0.95
FD(3x)	28.44	0.86	24.15	0.84	31.11	0.94

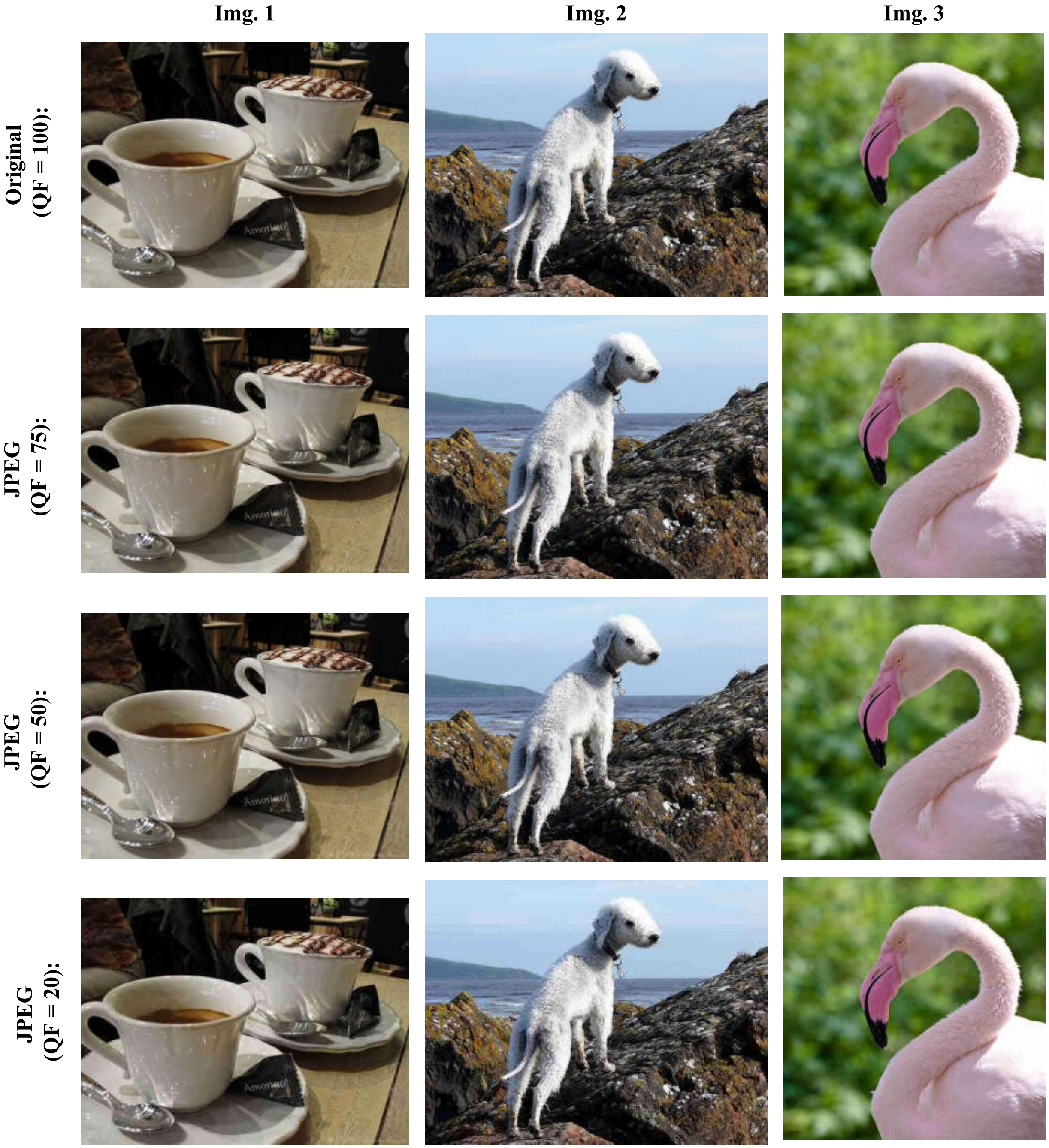

Figure 1: Example visual results produced by default JPEG compression.

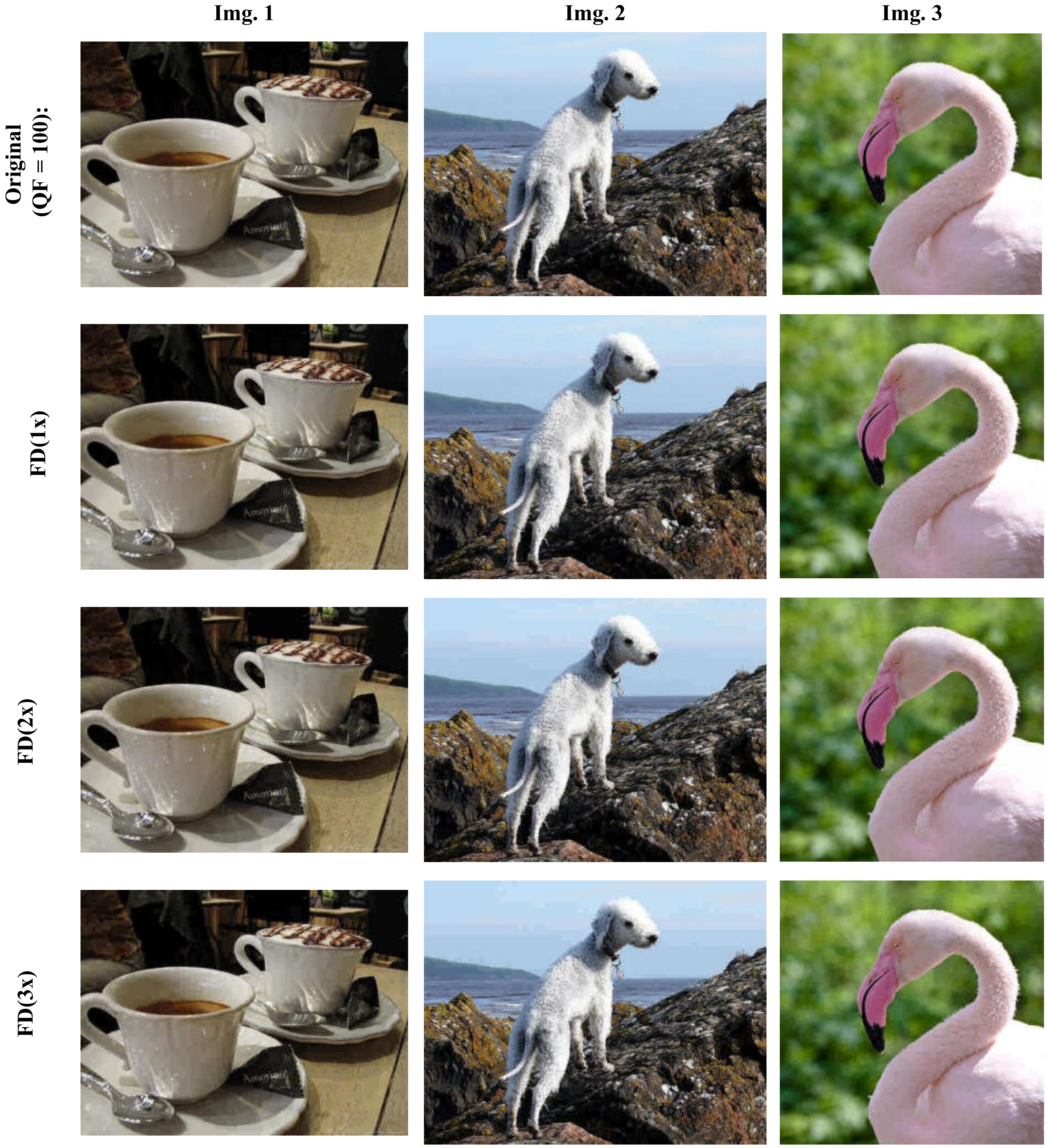

Figure 2: Examples visual results produced by “feature distillation” method.