Adversarial Examples with Specular Highlights

Supplementary Material

Vanshika Vats[1, 2] and Koteswar Rao Jerripothula[2]

[1]University of California, Santa Cruz
[2]Indraprastha Institute of Information Technology, Delhi
vvats@ucsc.edu, koteswar@iiitd.ac.in

1. Performance on ImageNet-AH

Since ImageNet-AH is a cumulative dataset of the artificial specular highlight failures of the models, we also present the individual performance of each model on the whole dataset in Fig. 1. Here, as it can be observed, Xception network is least affected by specular adversaries, followed by Inception-v3, conforming with the results in the main text. VGG-16, VGG-19 and MobileNet-v2 show a drastic fall in class prediction performance.

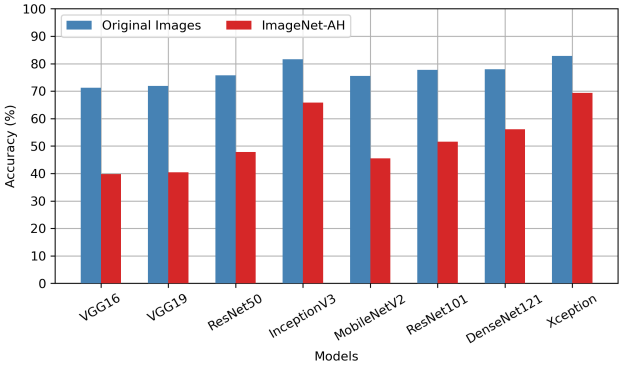

Figure 1: Performance of various models on ImageNet-AH as compared to their original non-specularly highlighted images.

2. ImageNet-AH Classes

Following [1], we use 200-class subset of ImageNet-1K to form ImageNet-AH. The class names and codes of these classes are given below:
n01443537: goldfish, n01484850: great white shark, n01494475: hammerhead, n01498041: stingray, n01514859: hen, n01518878: ostrich, n01531178: goldfinch, n01534433: junco, n01614925: bald eagle, n01616318: vulture, n01630670: common newt, n01632777: axolotl, n01644373: tree frog, n01677366: common iguana, n01694178: African chameleon, n01748264: Indian cobra, n01770393: scorpion, n01774750: tarantula, n01784675: centipede, n01806143: peacock, n01820546: lorikeet, n01833805: hummingbird, n01843383: toucan, n01847000: drake, n01855672: goose, n01860187: black swan, n01882714: koala, n01910747: jellyfish, n01944390: snail, n01983481: American lobster, n01986214: hermit crab, n02007558: flamingo, n02009912: American egret, n02051845: pelican, n02056570: king penguin, n02066245: grey whale, n02071294: killer whale, n02077923: sea lion, n02085620: Chihuahua, n02086240: Shih-Tzu, n02088094: Afghan hound, n02088238: basset, n02088364: beagle, n02088466: bloodhound, n02091032: Italian greyhound, n02091134: whippet, n02092339: Weimaraner, n02094433: Yorkshire terrier, n02096585: Boston bull, n02097298: Scotch terrier, n02098286: West Highland white terrier, n02099601: golden retriever, n02099712: Labrador retriever, n02102318: cocker spaniel, n02106030: collie, n02106166: Border collie, n02106550: Rottweiler, n02106662: German shepherd, n02108089: boxer, n02108915: French bulldog, n02109525: Saint Bernard, n02110185: Siberian husky, n02110341: dalmatian, n02110958: pug, n02112018: Pomeranian, n02112137: chow, n02113023: Pembroke, n02113624: toy poodle, n02113799: standard poodle, n02114367: timber wolf, n02117135: hyena, n02119022: red fox, n02123045: tabby, n02128385: leopard, n02128757: snow leopard, n02129165: lion, n02129604: tiger, n02130308: cheetah, n02134084: ice bear, n02138441: meerkat, n02165456: ladybug, n02190166: fly, n02206856: bee, n02219486: ant, n02226429: grasshopper, n02233338:

cockroach, n02236044: mantis, n02268443: dragonfly, n02279972: monarch, n02317335: starfish, n02325366: wood rabbit, n02346627: porcupine, n02356798: fox squirrel, n02363005: beaver, n02364673: guinea pig, n02391049: zebra, n02395406: hog, n02398521: hippopotamus, n02410509: bison, n02423022: gazelle, n02437616: llama, n02445715: skunk, n02447366: badger, n02480495: orangutan, n02480855: gorilla, n02481823: chimpanzee, n02483362: gibbon, n02486410: baboon, n02510455: giant panda, n02526121: eel, n02607072: anemone fish, n02655020: puffer, n02672831: accordion, n02701002: ambulance, n02749479: assault rifle, n02769748: backpack, n02793495: barn, n02797295: barrow, n02802426: basketball, n02808440: bathtub, n02814860: beacon, n02823750: beer glass, n02841315: binoculars, n02843684: birdhouse, n02883205: bow tie, n02906734: broom, n02909870: bucket, n02939185: caldron, n02948072: candle, n02950826: cannon, n02951358: canoe, n02966193: carousel, n02980441: castle, n02992529: cellular telephone, n03124170: cowboy hat, n03272010: electric guitar, n03345487: fire engine, n03372029: flute, n03424325: gasmask, n03452741: grand piano, n03467068: guillotine, n03481172: hammer, n03494278: harmonica, n03495258: harp, n03498962: hatchet, n03594945: jeep, n03602883: joystick, n03630383: lab coat, n03649909: lawn mower, n03676483: lipstick, n03710193: mailbox, n03773504: missile, n03775071: mitten, n03888257: parachute, n03930630: pickup, n03947888: pirate, n04086273: revolver, n04118538: rugby ball, n04133789: sandal, n04141076: sax, n04146614: school bus, n04147183: schooner, n04192698: shield, n04254680: soccer ball, n04266014: space shuttle, n04275548: spider web, n04310018: steam locomotive, n04325704: stole, n04347754: submarine, n04389033: tank, n04409515: tennis ball, n04465501: tractor, n04487394: trombone, n04522168: vase, n04536866: violin, n04552348: warplane, n04591713: wine bottle, n07614500: ice cream, n07693725: bagel, n07695742: pretzel, n07697313: cheeseburger, n07697537: hotdog, n07714571: head cabbage, n07714990: broccoli, n07718472: cucumber, n07720875: bell pepper, n07734744: mushroom, n07742313: Granny Smith, n07745940: strawberry, n07749582: lemon, n07753275: pineapple, n07753592: banana, n07768694: pomegranate, n07873807: pizza, n07880968: burrito, n07920052: espresso, n09472597: volcano, n09835506: ballplayer, n10565667: scuba diver, n12267677: acorn

3. ImageNet-PT Classes

As mentioned in the main manuscript, a 10-class subset of ImageNet-AH is chosen to form ImageNet-PT, considering the feasibility of physically printing the images and throwing specular highlight on them. The class names and codes of these classes are as follows:
n01498041: stingray, n01944390: snail, n02066245: greywhale, n02110958: pug, n02226429: grasshopper, n02950826: cannon, n03594945: jeep, n03947888: pirate, n04591713: winebottle, n07768694: pomegranate

References

[1] Dan Hendrycks, Kevin Zhao, Steven Basart, Jacob Steinhardt, and Dawn Song. Natural adversarial examples. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 15262–15271, June 2021. 1