universität innsbruck

UNCOVER

Landscape More Secure Than Portrait ?

Zooming Into the Directionality of Digital Images With Security Implications

Benedikt Lorch, Rainer Böhme

33rd USENIX Security Symposium · Philadelphia · 16 August 2024

Landscape vs Portrait

Security Effect of Orientation Mismatch

Steganography detection
Does an image contain a secret message?

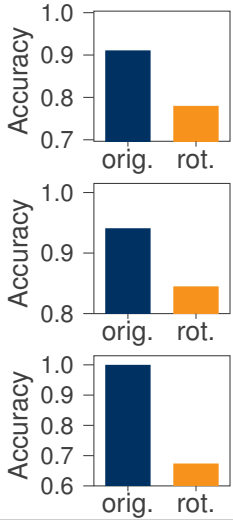
2-class classification, EfficientNet-B0

Forensic source identification
Identify camera from a set of known camera models

27-class classification, EfficientNet-B5

Synthetic image detection
Distinguish real images from generative AI

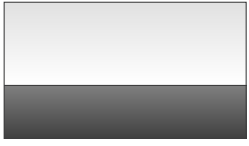
2-class classification, EfficientNet-B0



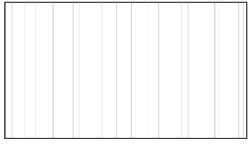
Causes of Directionality

Directionality: Horizontal pixel sequences differ in their statistical properties from vertical pixel sequences.

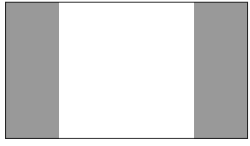
Directionality is introduced in several stages during image acquisition.



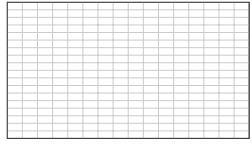
Scene content



Sensor



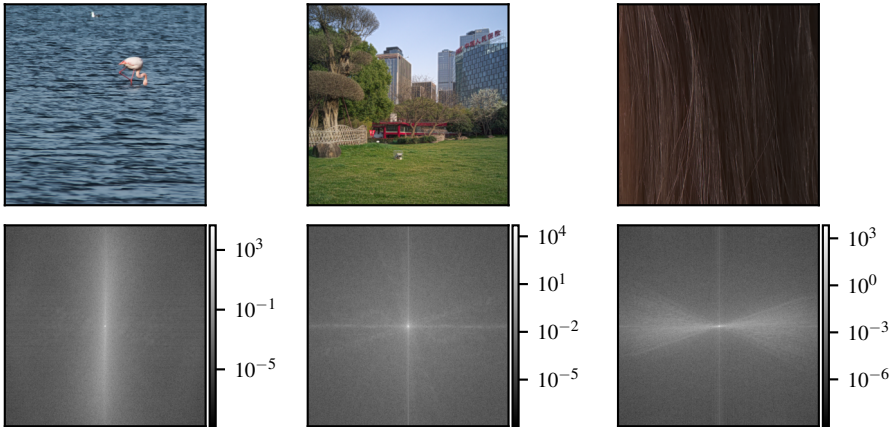
Raw-to-image conversion



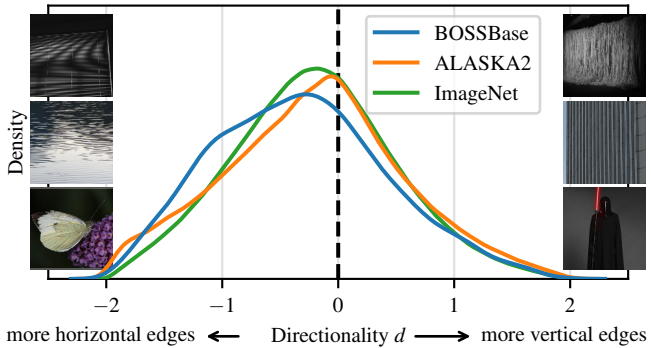
Compression

Scene Content

Examples from the popular steganalysis dataset ALASKA2



Distribution of Directionality in Popular Datasets

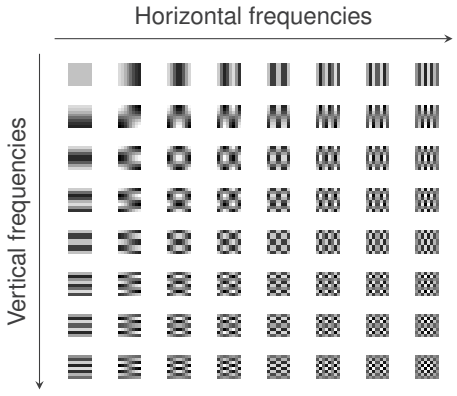


In many image datasets, horizontal edges are more prevalent than vertical edges.

Bas, Filler, Pevný, "Break our steganographic system": The ins and outs of organizing BOSS", *Information Hiding*, 2011.
Cogranne, Giboulot, Bas, "ALASKA#2: Challenging academic research on steganalysis with realistic images", *IEEE Int. Workshop on Information Forensics and Security*, 2020.
Deng, Dong, Socher, Li, Kai, Li, "ImageNet: A large-scale hierarchical image database". *IEEE Conference on Computer Vision and Pattern Recognition*, 2009.

Asymmetric JPEG Quantization Tables (QT)

Represent each 8×8 block as linear combination of cosine functions (DCT).



Divide DCT coefficients by QT.
Example QT in the JPEG standard:

Horizontal frequencies

Vertical frequencies

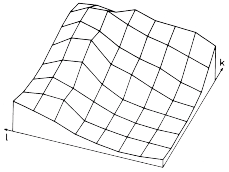
16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

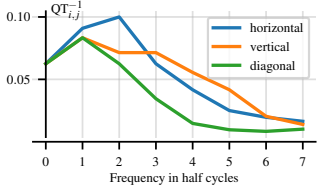
Origin of the Standard JPEG Quantization Table

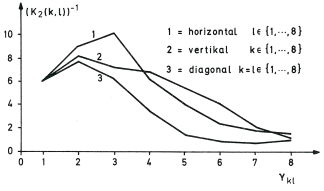
JPEG standard

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Measurements of human sensitivity to DCT base images, ~1982







H. Lohscheller, “Einzelbildübertragung mit wachsender Auflösung”, Dissertation, Technische Hochschule Aachen, 1982

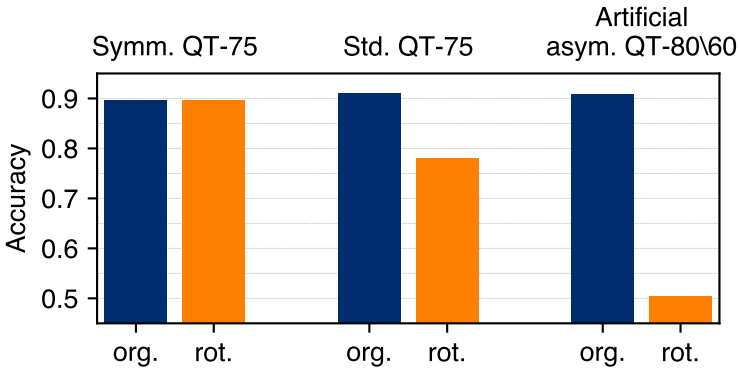
Prevalence of Asymmetric Quantization Tables

Dataset	Standard QTs	Asymmetric luma QT
Dresden	31 %	96 %
VISION	50 %	68 %
Forchheim	52 %	99 %

Many quantization tables are asymmetric, including the ones *libjpeg* uses by default.

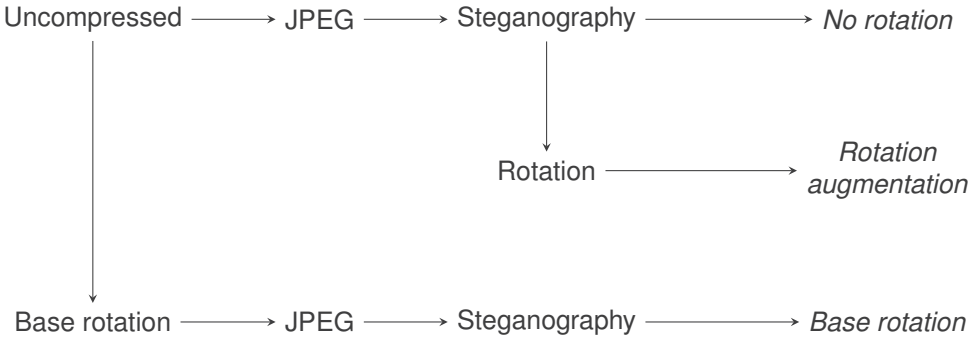
Gloe, Böhme, “The 'Dresden image database' for benchmarking digital image forensics”, *ACM Symposium on Applied Computing*, 2010.
Shullani, Fontani, Iuliani, Al Shaya, Piva, “VISION: A video and image dataset for source identification”, *EURASIP Journal on Information Security*, 2017.
Hadwiger, Riess, “The Forchheim image database for camera identification in the wild”, *International Conference on Pattern Recognition Workshops*, 2020.

Steganalysis: Effect of Asymmetric QTs

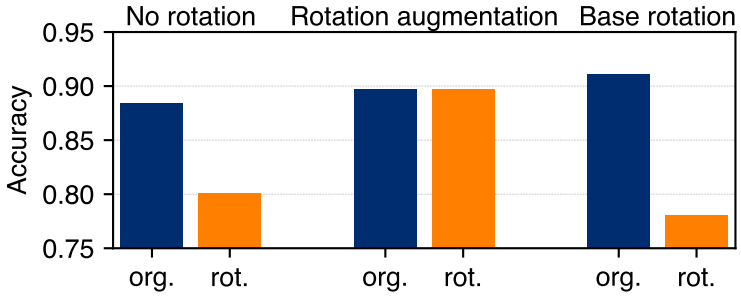


ALASKA dataset, experimental setup *base-rot*, J-UNIWARD 0.4 bpnzAC, EfficientNet-B0

Rotation Augmentation vs Base Rotation



Steganalysis: Effect of Rotation Augmentation

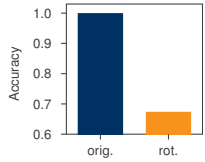


- Rotation augmentation makes detector **generalize** to rotated images.
- Base rotation leads to **maximum accuracy** on the original orientation.

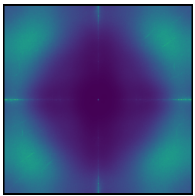
Steganalysts have to choose between generalization and maximum accuracy.

ALASKA dataset, J-UNIWARD 0.4 bpnzAC, EfficientNet-B0

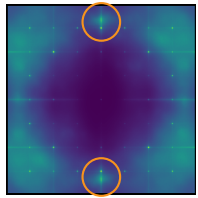
Directionality in Stable Diffusion XL Images



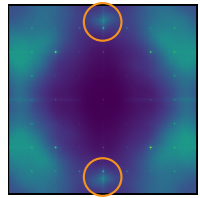
Real

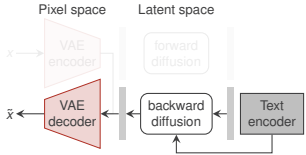


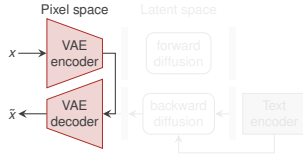
SDXL prompt-to-image



SDXL VAE 1.0







Directional artifacts originate from the variational autoencoder.

Takeaways

- Directionality of images matters across security applications: steganalysis, forensic source identification, authentication
- Multiple causes: scene content, human perception, and technological choices
- Unaddressed directionality causes ML methods to overfit to a single orientation.
- Augmentation improves generalization, but underperforms single-orientation detector.

{benedikt.lorch,rainer.boehme}@uibk.ac.at

GitHub