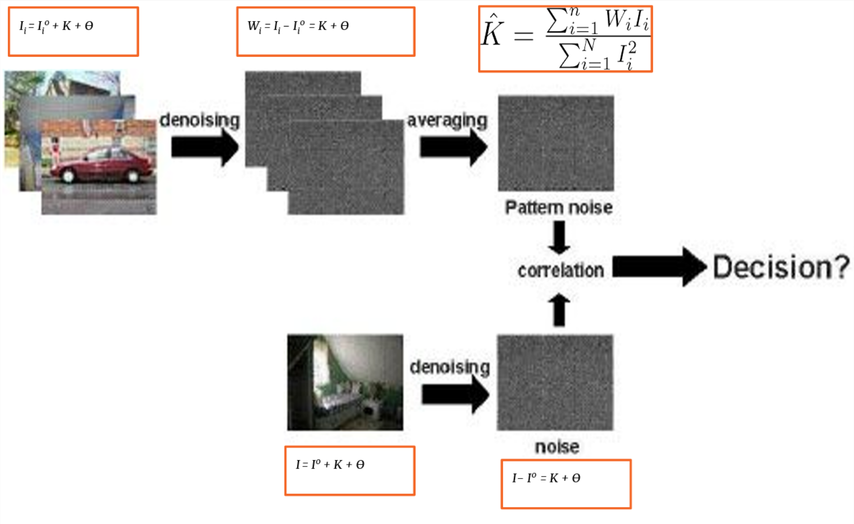
Extracting Signal Pattern Noise

Bill N, Guannan C, Patrick F, Sadegh S, Timothy P, Silvia G, Matt B

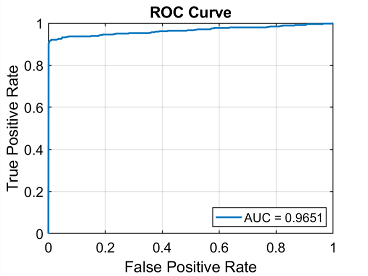
February 16, 2024

SAMBa ITT19

Problem outline



Visualising the given data



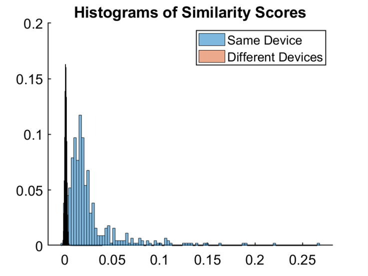
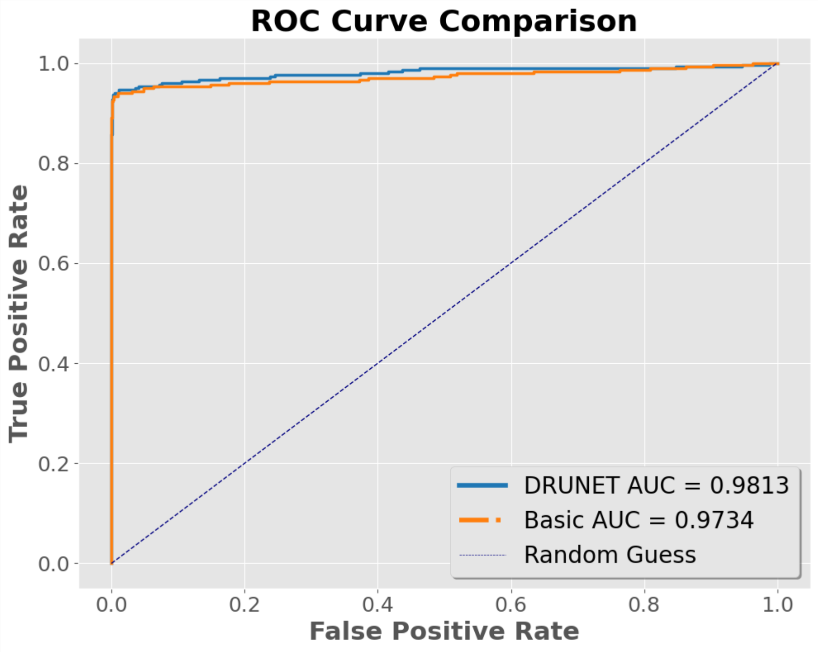


Figure 1: Examining the SPNs of 443 queries with each of the 443 indices, examining the true and false positive rates.
(i.e. Plotting the data CameraForensics gave us, with the code CameraForensics gave us!)

A Pretrained CNN Denoiser (DRUNet) vs Wavelet

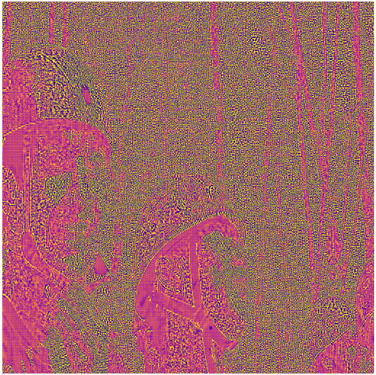
- The current approach uses wavelet denoising, which is analytical and uses handcrafted filters which can lead to a loss of important features in natural images. $\times$
- Fully data-adaptive approach - DRUNET — A CNN trained to denoise natural images, over different noise levels.
  - 32 million parameters (trained over very large dataset) $\checkmark$
  - Black box, not interpretable $\times$
  - One hyperparameter — **noise level** σ $\times$
  - Fast to apply after training $\checkmark$


ROC Curve Comparison
True Positive Rate
False Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
DRUNET AUC = 0.9813
Basic AUC = 0.9734
Random Guess

Wavelet residual vs DRUnet residual

Original Image

$|Residual_{wavelet} - Residual_{DRUnet}|$



A "Plug-and-play" method

- A second data-adaptive approach is variational regularisation.
- Variational regularisation:

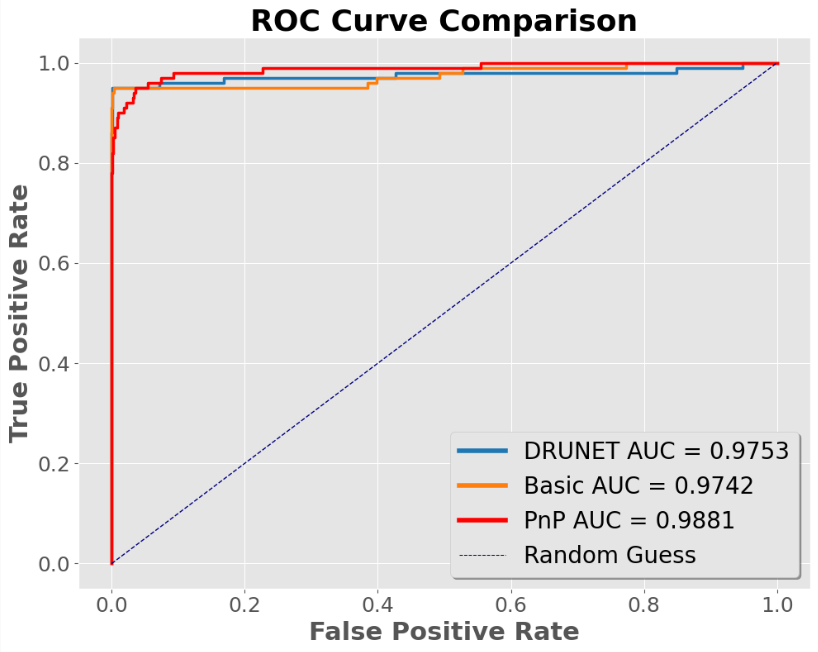
$$\min_x \frac{1}{2}||x - y||_2^2 + \mathcal{R}_{\boldsymbol{\theta}}(x)$$

Regularisation term $\mathcal{R}_{\boldsymbol{\theta}}$ e.g. data-adaptive

- More interpretable ✓
- Adaptive to data ✓

Replace optimisation steps involving the regularisation term with the DRUNET denoiser D_σ - "Plug-and-play prior".

$$u_k = x_k - \lambda \nabla_x \left(\frac{1}{2}||x_k - y||_2^2 \right)$$
$$x_{k+1} = D_\sigma(u_k)$$


ROC Curve Comparison
True Positive Rate
False Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
DRUNET AUC = 0.9753
Basic AUC = 0.9742
PnP AUC = 0.9881
Random Guess

A Bilevel Learning Framework

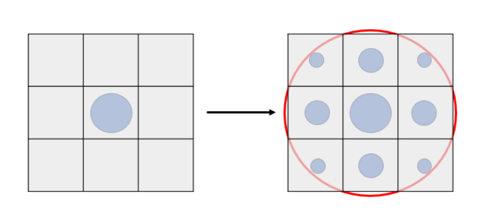
- Thus far, pre-trained models haven't been tailored to our problem.
- We can fine-tune pre-trained data-driven approaches using **bilevel learning**.

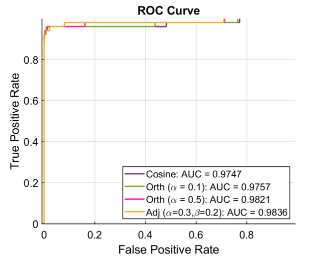
Given a similarity metric $\ell(s_i, s_j)$, which we want to maximise if s_i, s_j are taken from the same device, and minimise otherwise.

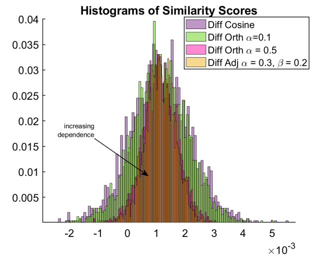
$$\min_{\boldsymbol{\theta}} \sum_{i,j} (-1)^{\delta_{ij}} \ell(\hat{s}_i(\boldsymbol{\theta}), s_j)$$

$$\hat{s}_i(\boldsymbol{\theta}) = y_i - \left(\arg\min_x \frac{1}{2} ||x - y_i||_2^2 + \mathcal{R}_{\boldsymbol{\theta}}(x) \right)$$

Measure of comparison – Pixel vs locality



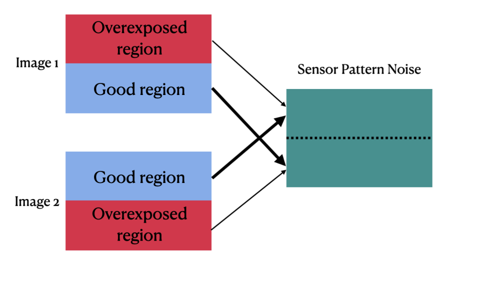




Here α is the total weighting placed on orthogonal neighbours and β is the total weighting of diagonal neighbours. Smaller sample.

Averaging Noise Residuals

- When we have multiple images from the same camera we average the noise residuals to better estimate the SPN.
- Taking a median of the noise residuals instead of a mean might prove more robust when parts of the image set are overexposed.
- Furthermore, there may be scope for down-weighting overexposed regions in the average.



Mean vs Median - Results

- We found the DRUNET noise residuals for 20 images from the same camera. Unfortunately we couldn't find a set of images from the same camera with overexposed regions.
- We took the cosine similarity of each noise residual and the mean of the remaining 19. This was compared to the cosine similarity of each noise residual and the median of the remaining 19.
- A larger cosine similarity for SPN derived as a mean was observed in all 20 cases, with no clear change in the variance for the medians.

Conclusions and Future Work

Conclusions

- Pre-trained DRUNET outperforms wavelet denoising.
- Considering neighbouring pixels in the similarity measure separates the clusters (for smaller sample size).
- A preliminary test suggests means outperform medians when combining DRUNET noise residuals from the same camera.

Future Work

- Implement bilevel learning.
- Examine alternative measures to cosine similarity (should neighbouring pixels be considered?).
- Retest means vs medians when overexposed regions are present in the image set.