CENTER FOR CYBER SECURITY

جامعة نيويورك أبوظبي

NYU | ABU DHABI

Towards Camera Identification From Cropped Query Images

Waheeb Yaqub
Manoranjan Mohanty
Nasir Memon

Source Camera Attribution

Social Media

Anonymous Image

- Verification: Was this picture taken with this camera?
- Identification: Was this picture taken from one a large collection of cameras?
- PRNU helps answer these questions.

PRNU[1]

- Uniform light → Different pixel values
- Physical property of sensor → resilient
- Similar noise pattern is in all images of a camera
- Signal = $I_0 + I_0 * PRNU + Other\ noise$

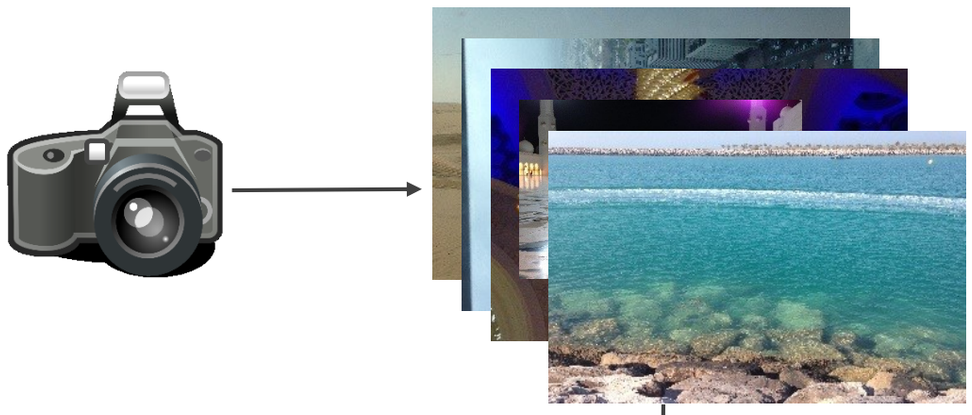
[1]:Jan Lukas, Jessica Fridrich, and Miroslav Goljan, “Digital camera identification from sensor pattern noise, ”IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, 2006.

NYU TANDON SCHOOL OF ENGINEERING

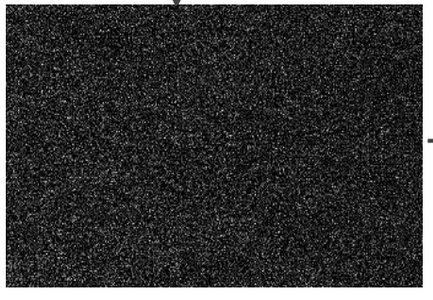
جامعة نيويورك أبوظبي
NYU ABU DHABI

Source Camera Verification

Images from Alice's Camera



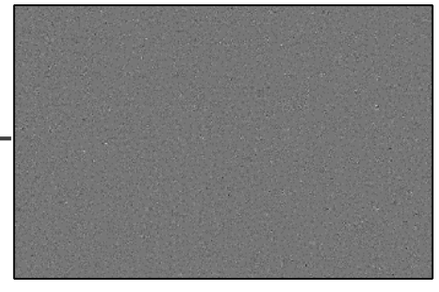
Anonymous Image



Fingerprint (FP)

Correlation

Decision?

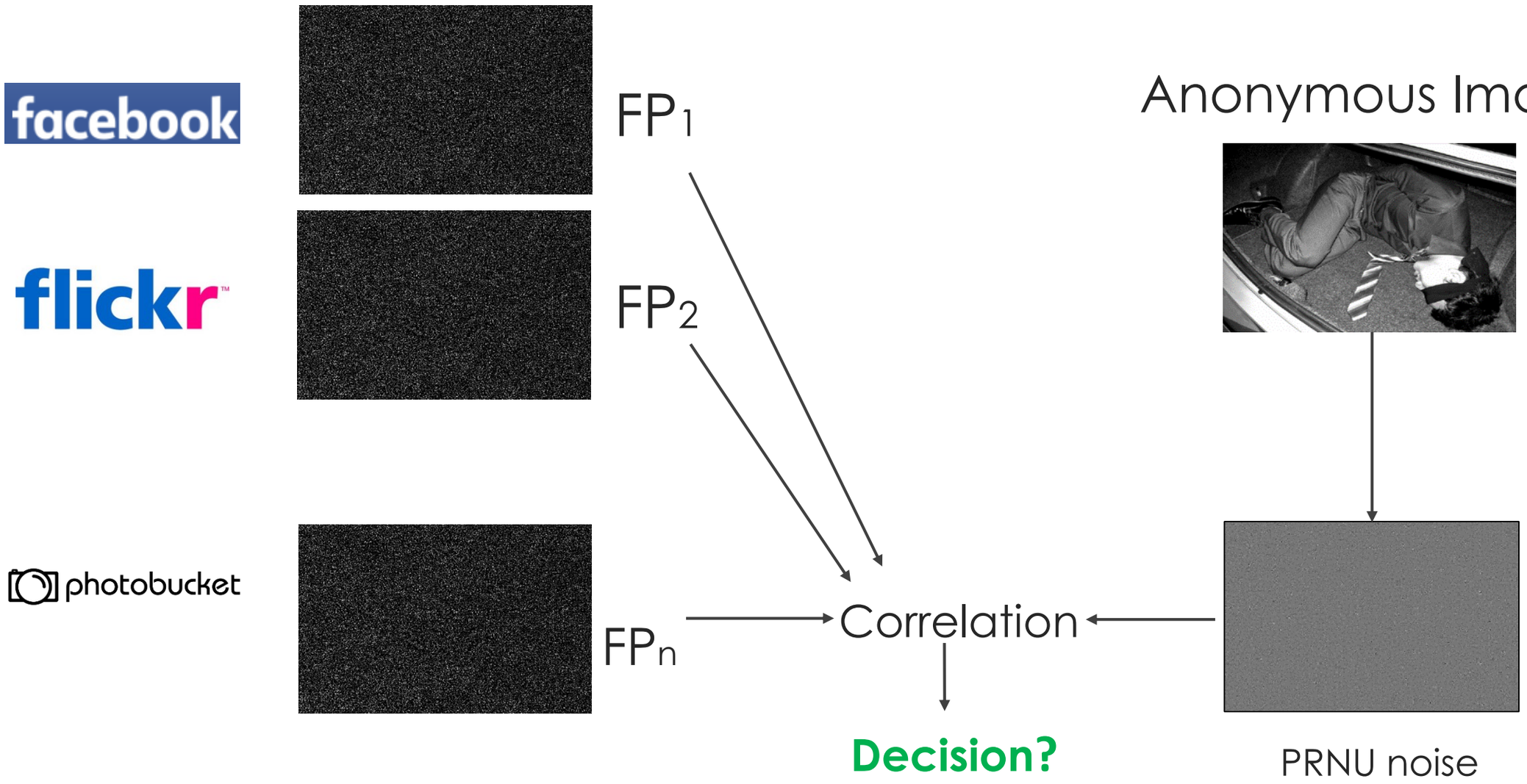


PRNU noise

NYU TANDON SCHOOL OF ENGINEERING

جامعة نيويورك أبوظبي
NYU ABU DHABI

Source Camera Identification



FP = Fingerprint

PRNU Based Source Camera Identification has Computational Overheads

- Correlation with billions of FP
- Existing speedups don't work with crop

FP = Fingerprint

Existing Methods of Speedup

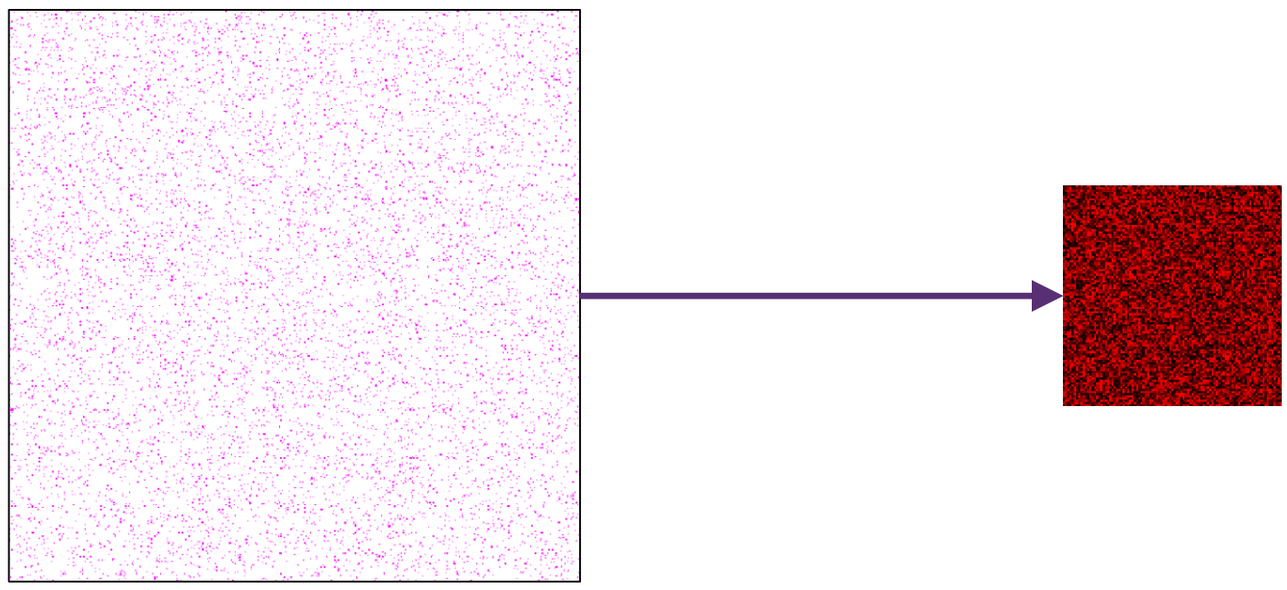
- Binarization: each fingerprint pixel by a single bit instead of 32bits
- ShortDigest: Only hottest & coldest pixel values
- Composite: fingerprint which is a mixture of many fingerprints

Existing Methods of Speedup (Binarization)

- 01010010111110101011110100010101010 → 1
- 10000001010101010010111010100111 → 0
- Hamming distance instead of correlation
- Computation & Storage (32 times better)
- Performance (3-5% drop)

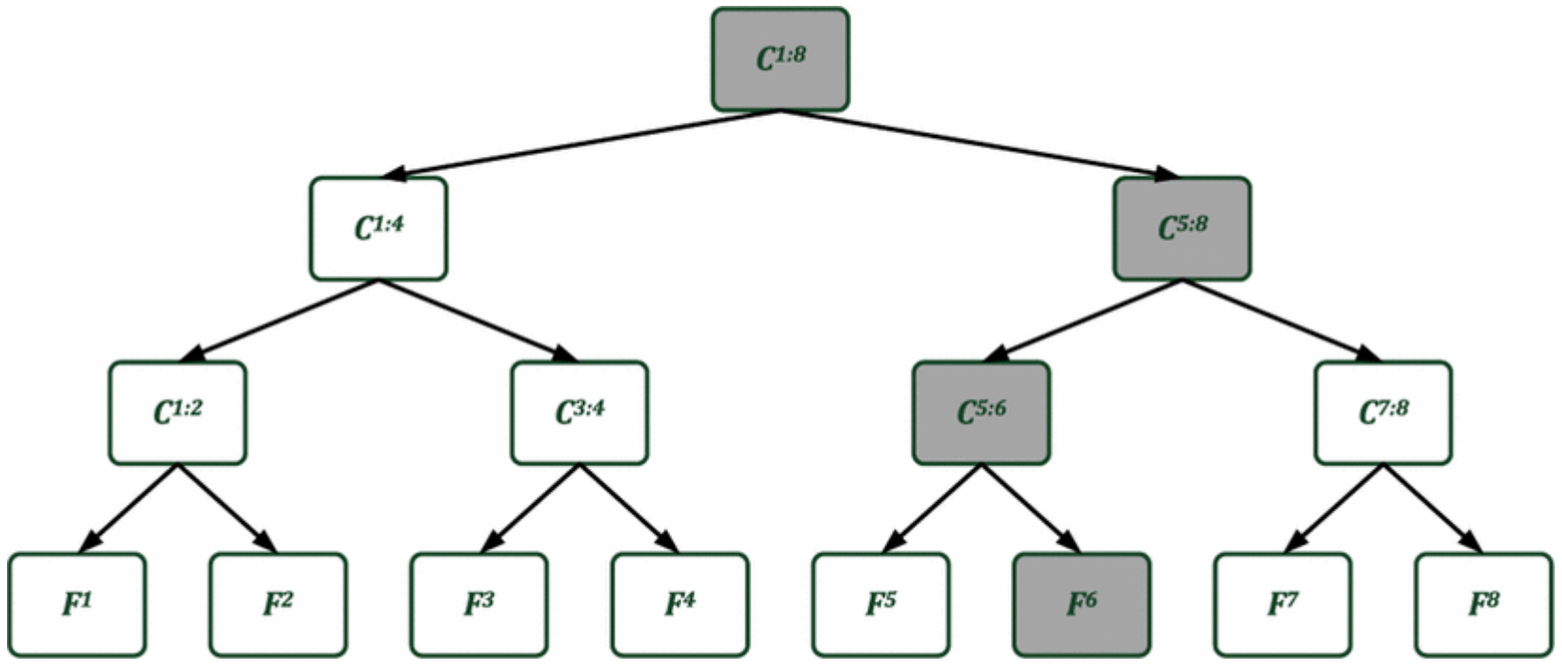
Existing Methods of Speedup (ShortDigest)

- Only hottest & coldest pixel values
- Storage, Speed (70-80 times)
- Performance (1-2% drop)



Existing Methods of Speedup (Composite)

- Speed (up to 90-100 times)
- Performance (1-2% drop)
- Storage (double storage)
- IO load(60-80 time improvement)



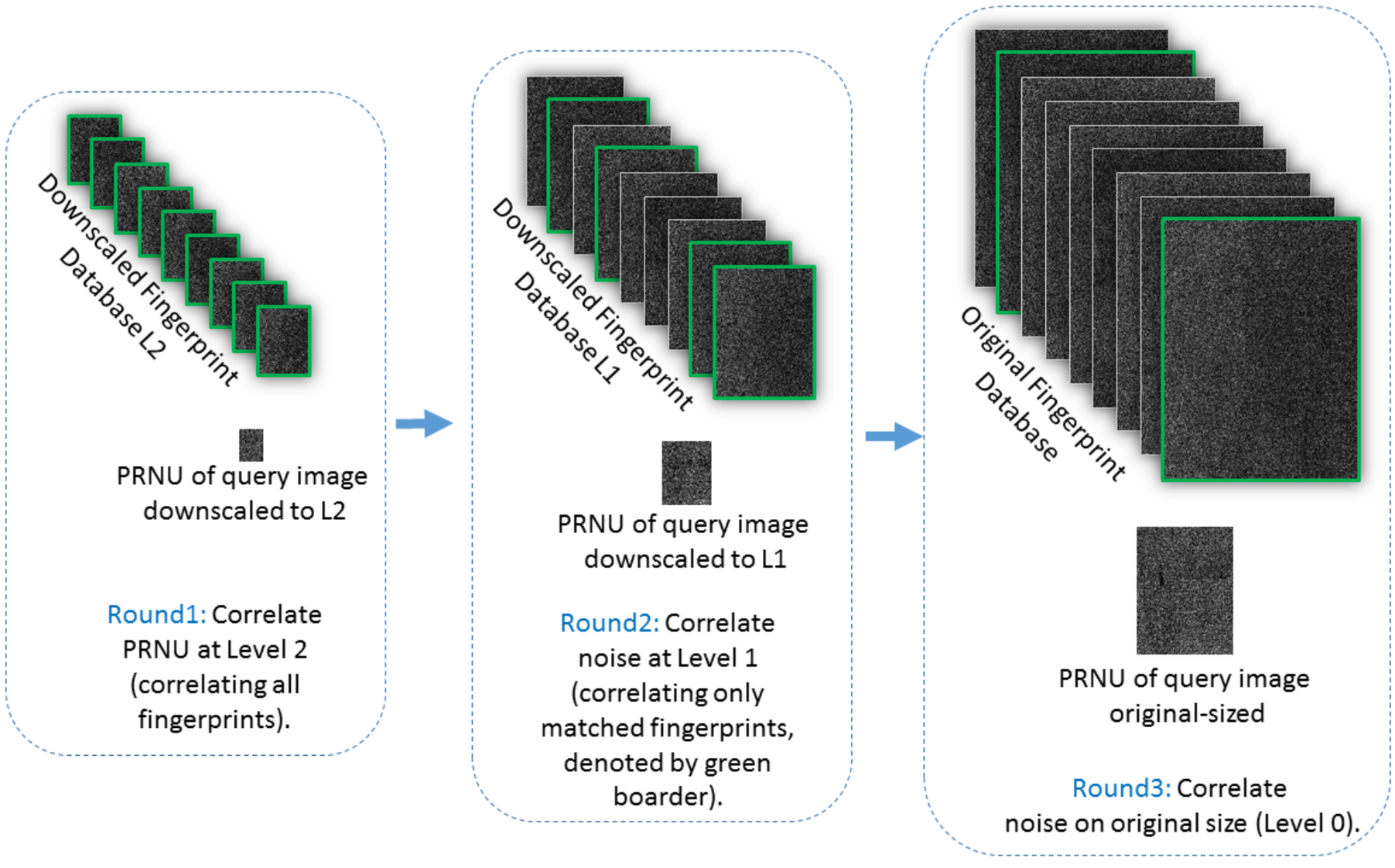
Our Contribution

- Speedup attribution can still be done when cropped images (speedup factor 13)
- Non-cropped images speeds up by factor of 55.
- Test with variety of scaling techniques
- Storage requirements increased by 33%

NYU TANDON SCHOOL OF ENGINEERING

جامعة نيويورك أبوظبي
NYU ABU DHABI

Our Proposed Scheme



Proposed Scheme (cropped)

Fingerprint downscaled to L2

PRNU of query image downscaled to L2

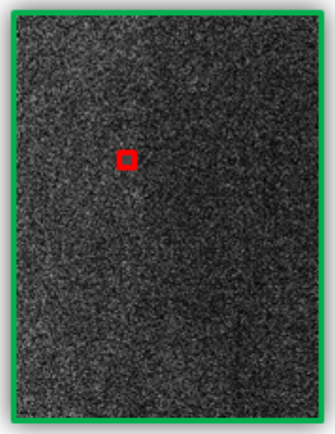
Round1: Correlation with NCC

Fingerprint downscaled to L1

PRNU of query image downscaled to L1

Round2: PCE correlation for potential cropped locations

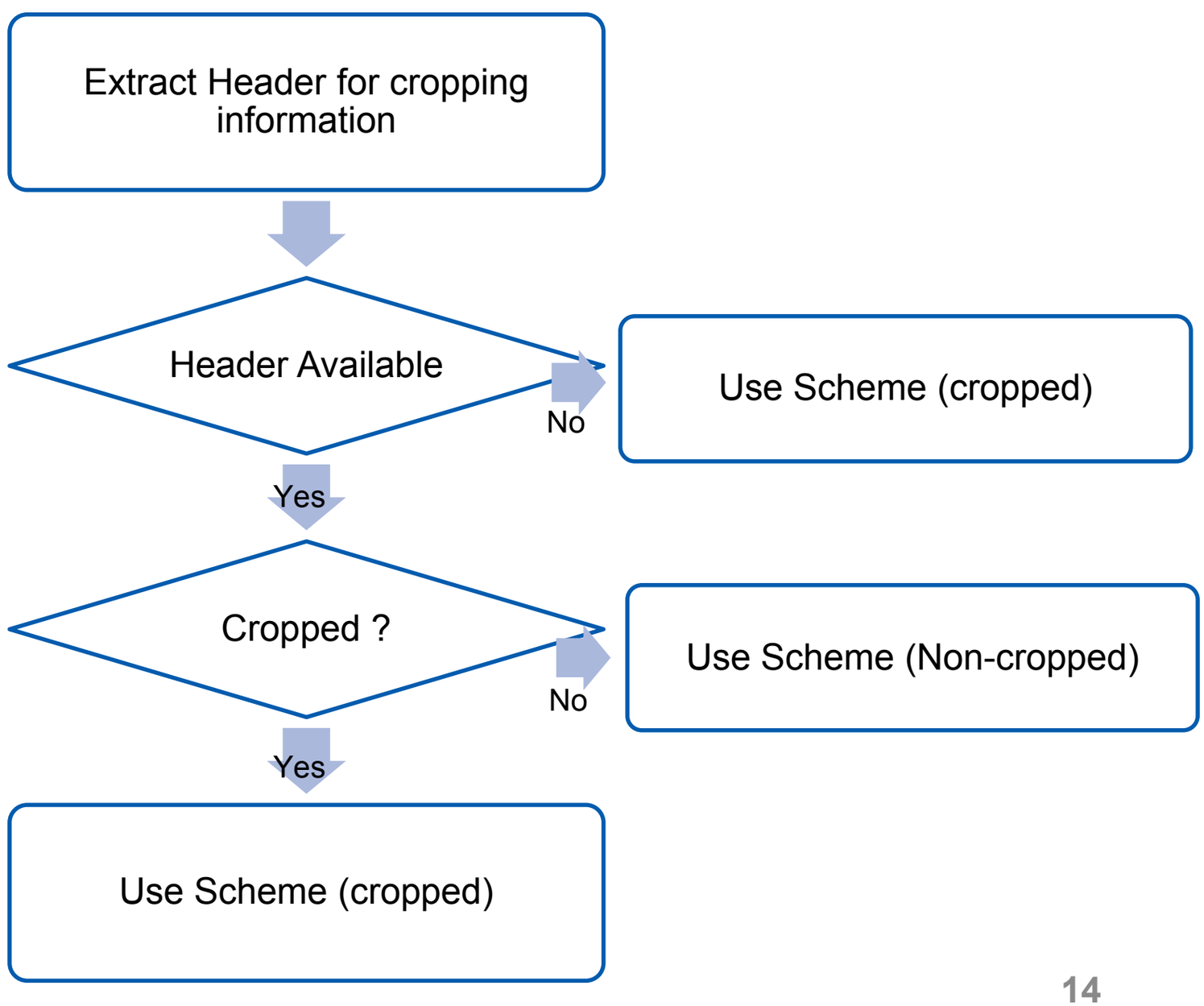
Original Fingerprint



PRNU of originally-sized query image

Round3:. PCE correlation for potential cropped locations

Our Proposed Scheme (flowchart)



Simple Example of Scaling PRNU

- F1 ≈ mean(f1+f2+f5+f6) ; Each pixel contribution is considered when scaling
- Bilinear interpolation Instance for one level

Fingerprint

f_1	f_2	f_3	f_4
f_5	f_6	f_7	f_8
f_9	f_{10}	f_{11}	f_{12}
f_{13}	f_{14}	f_{15}	f_{16}

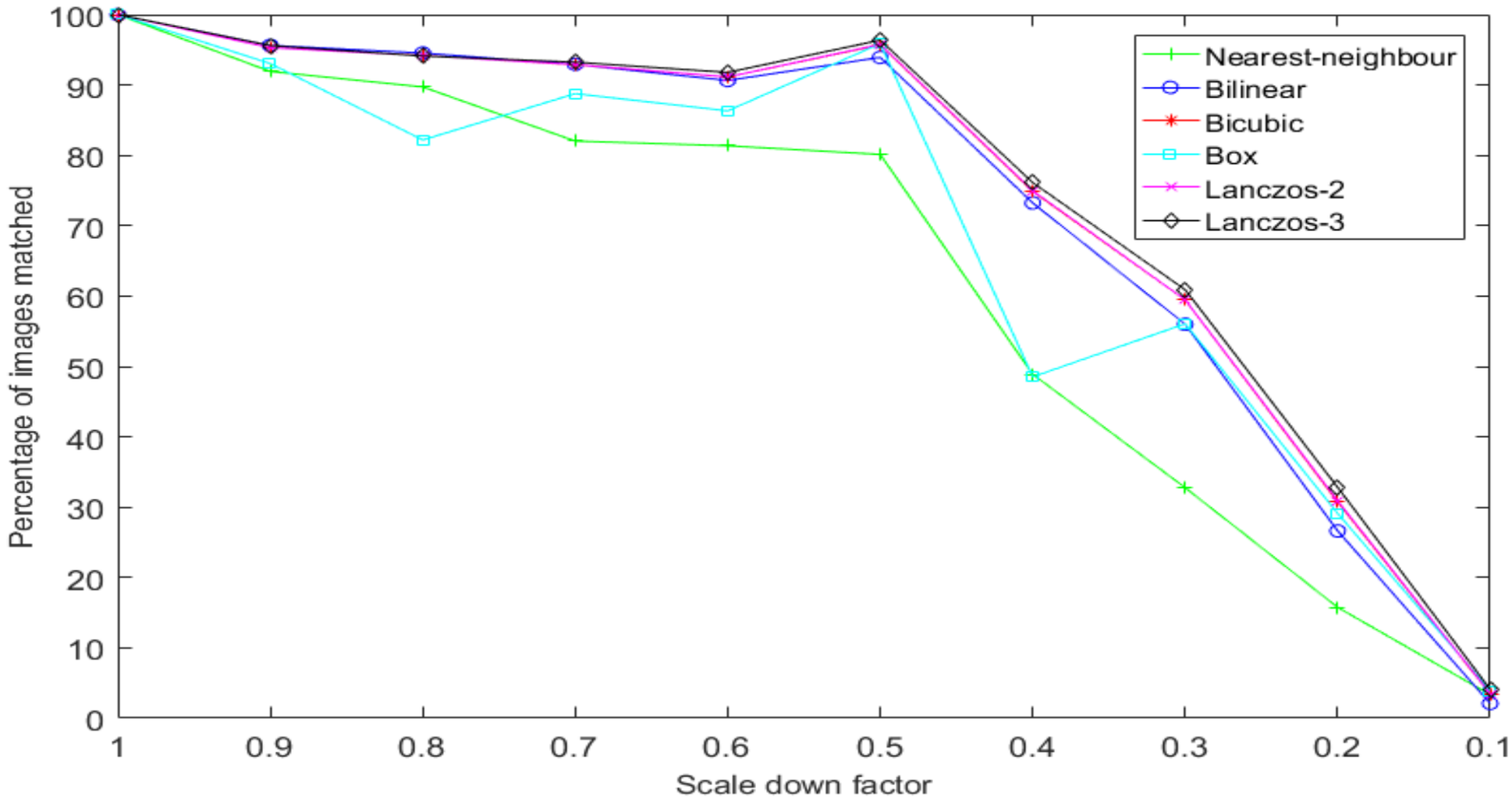
Group for Scaling

f_1	f_2	f_3	f_4
f_5	f_6	f_7	f_8
f_9	f_{10}	f_{11}	f_{12}
f_{13}	f_{14}	f_{15}	f_{16}

Scaled

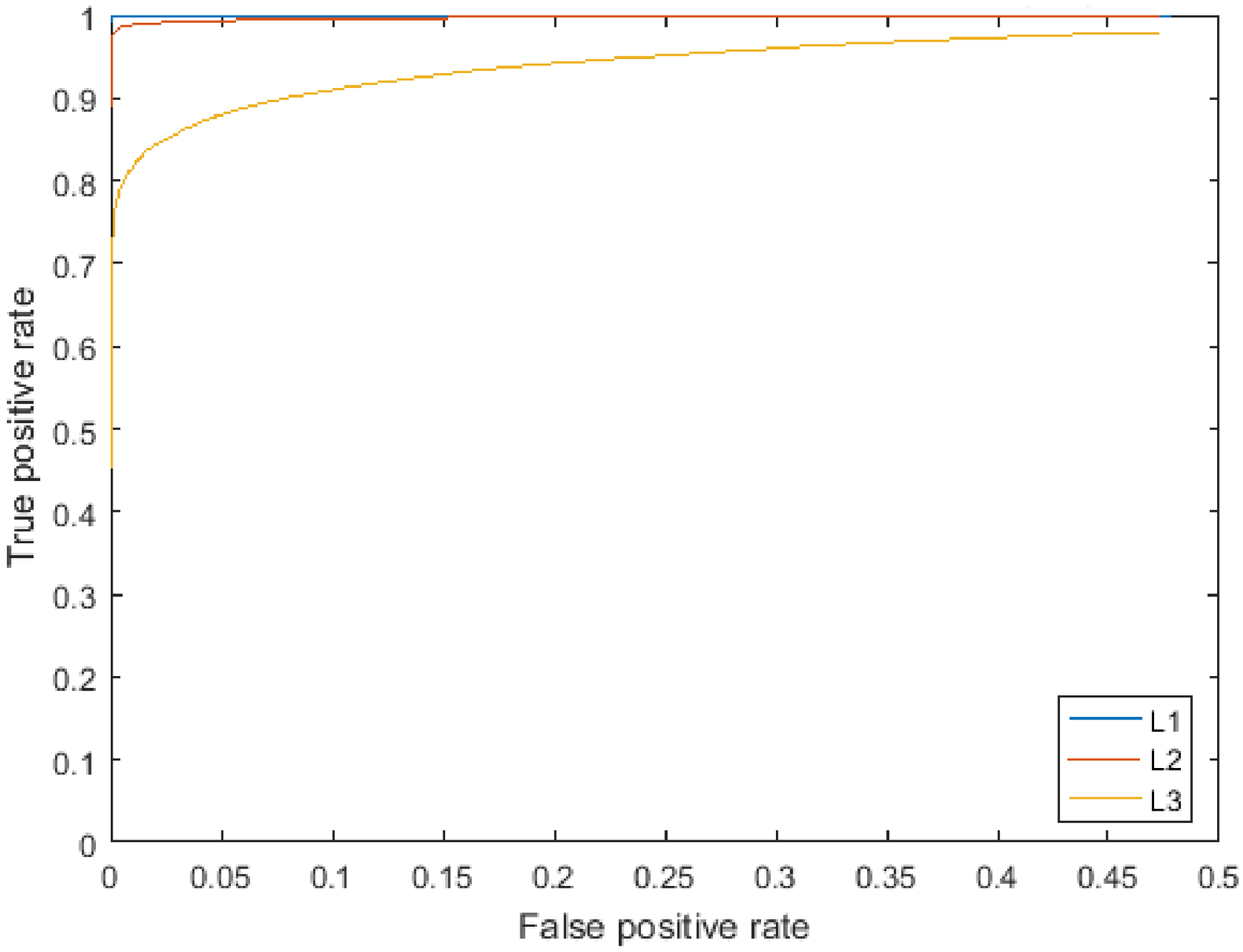
F_1	F_2
F_3	F_4

Various Scaling Methods

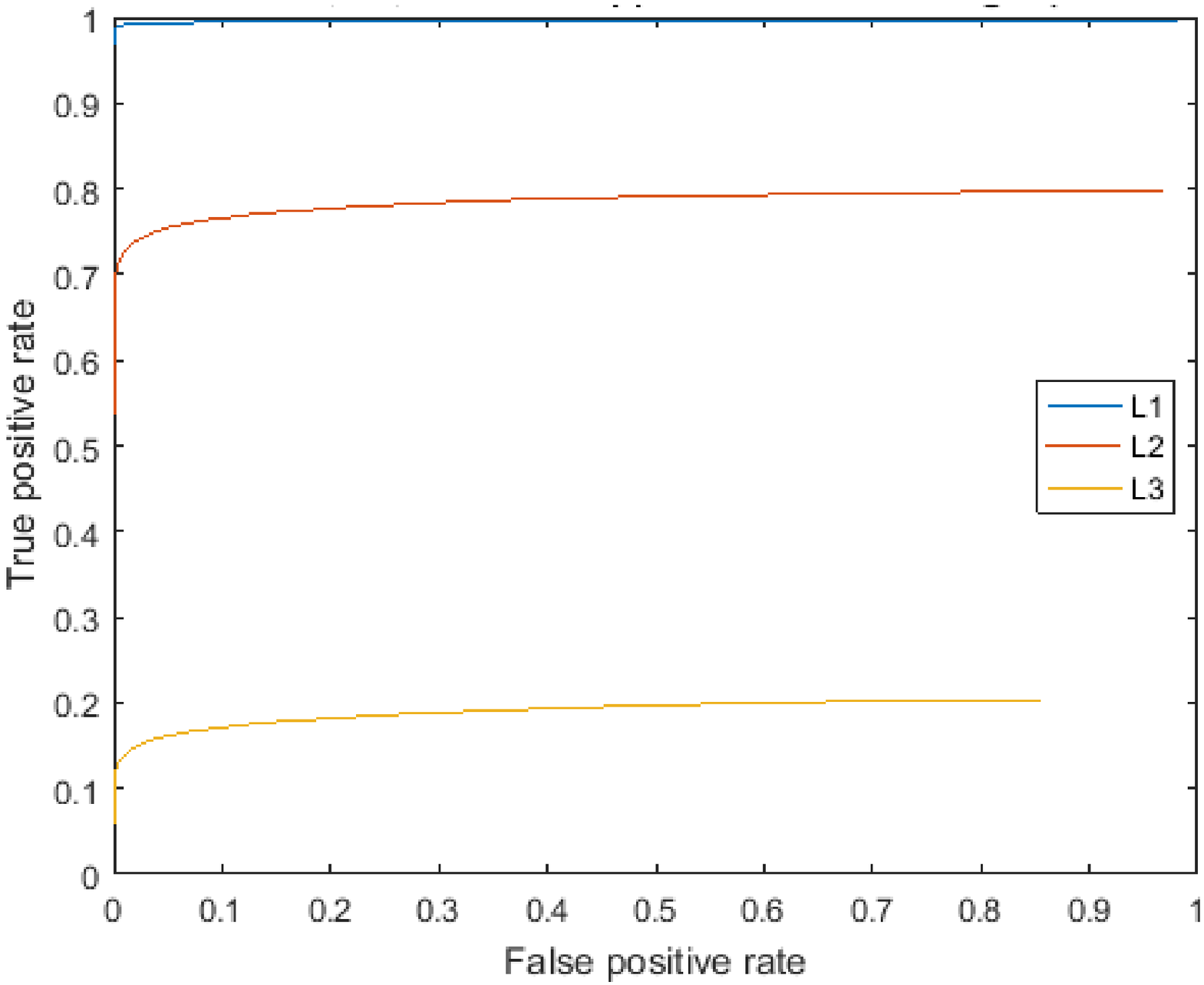


Lanczos scaling methods has the highest true positive rate compared to other scaling methods

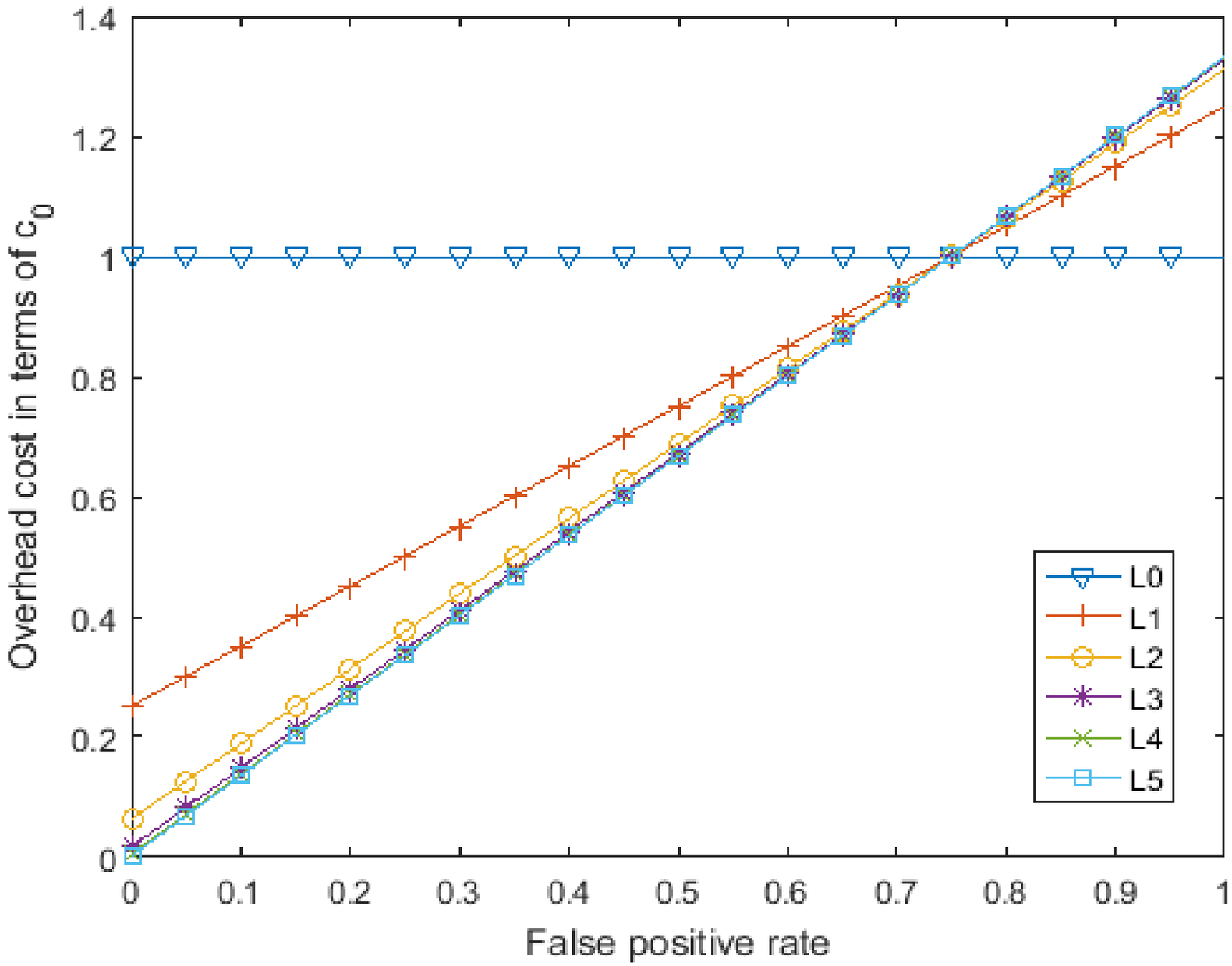
ROC for Different Scaling Levels



ROC for Different Scaling Levels- Cropped



Overhead Cost for Scaling



Conclusion

- In practice, images in social media are cropped and scaled and camera identification is difficult; conventional speed optimization techniques are either ineffective or do not apply
- Iteratively scaling the FP noise can be used to correlate cropped images

Questions
email :
memon@nyu.edu

W. Yaqub, M. Mohanty and N. Memon, "Towards Camera Identification from Cropped Query Images," *2018 25th IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, 2018, pp. 3798-3802.