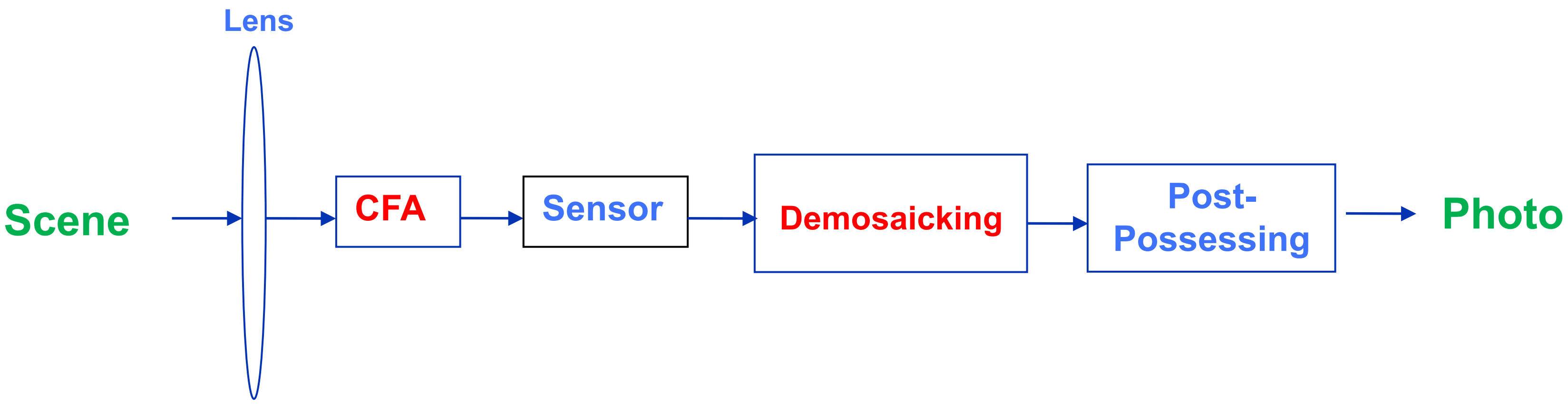
Image Forensics Based on Device Signatures Extracted from Images

Chang-Tsun Li

Department of Computer Science
University of Warwick
UK

Digital Image Acquisition Process

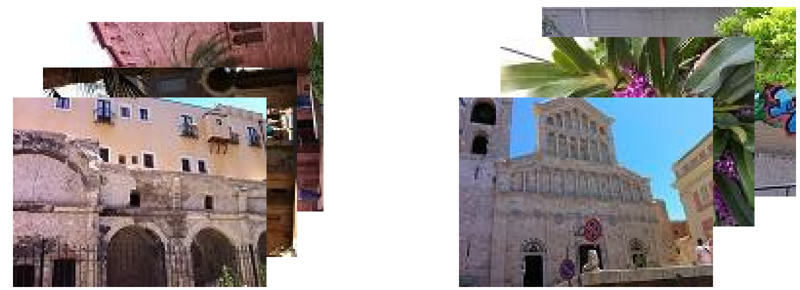


What is Image Forensics

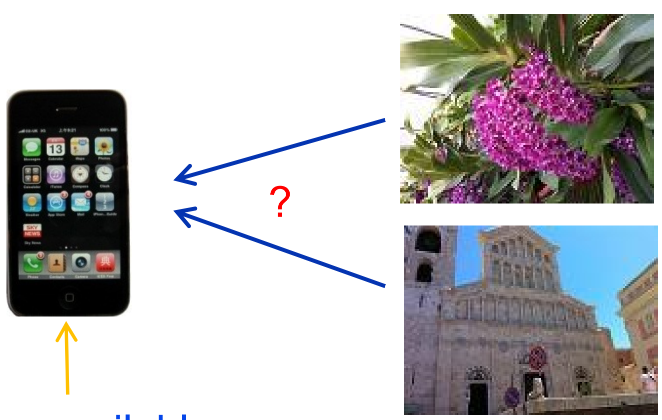
Images Forensics: The use of “signatures” left in the images by the imaging devices for

- source device identification

- image classification

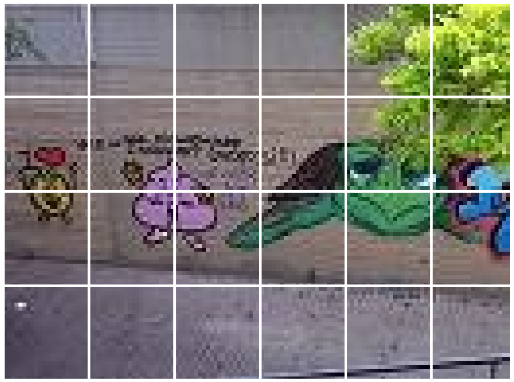


- source device linking



unavailable

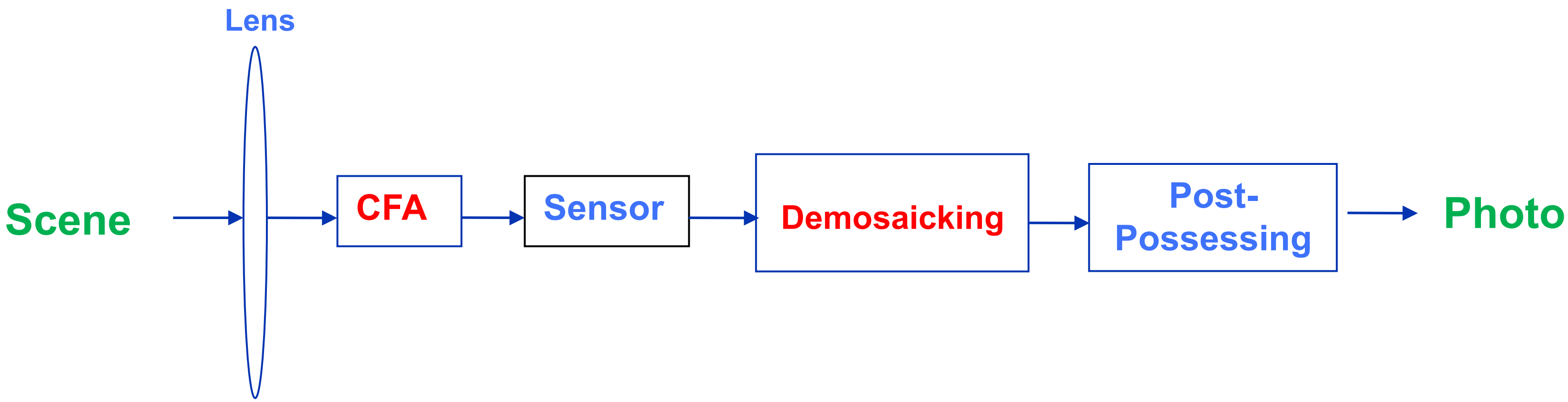
- content integrity verification



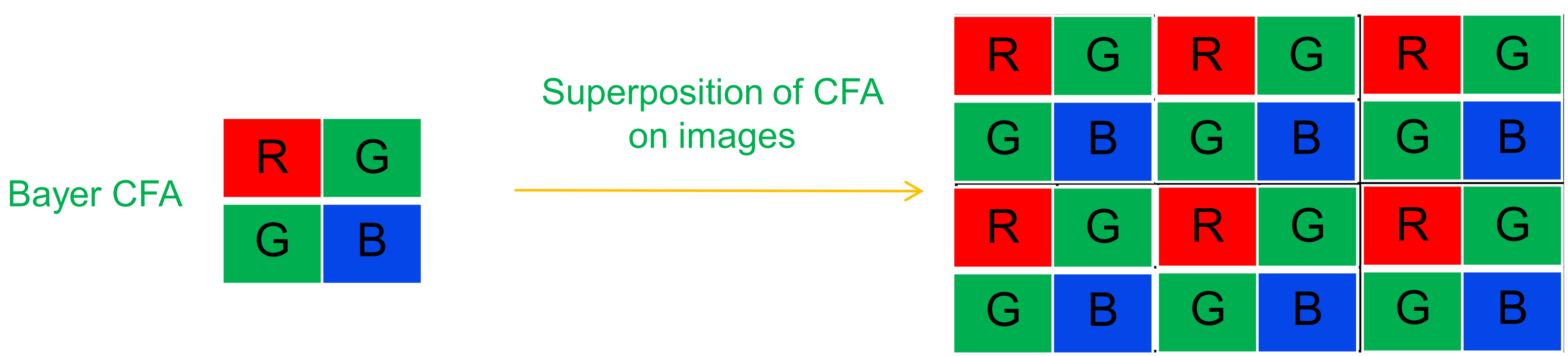
What Signatures

- Colour filter array (CFA) interpolation artefacts
- Camera response function
- Quantisation table of JPEG compression
- Sensor pattern noise
- More ….

Colour Filter Array & Demosaicking



CFA: Colour Filter Array



Capturing Physical Colours

R	G	R	G	R	G
G	B	G	B	G	B
R	G	R	G	R	G
G	B	G	B	G	B

CFA superposed on image I

123		126		120	
130		125		139	

I_R

	201		199		202
198		204		211	
	197		205		200
200		210		204	

I_G

	94		89		91
	96		91		92

I_B

CFA Interpolation

(-1,-1)	(-1,0)	(-1,1)
(0,-1)	(0,0)	(0,1)
(1,-1)	(1,0)	(1,1)

M(i,j): Interpolation Matrix

	201		199		202
198		204		211	
	197		205	?	200
200		210		204	

I_G

$$I_G(x,y) = \frac{1}{C} \sum_{i,j=-1}^{1} S(x+i, y+j) \cdot M(i,j) \cdot I_G(x+i, y+j)$$

$$C = \sum_{i,j=-1}^{1} S(x+i, y+j)$$

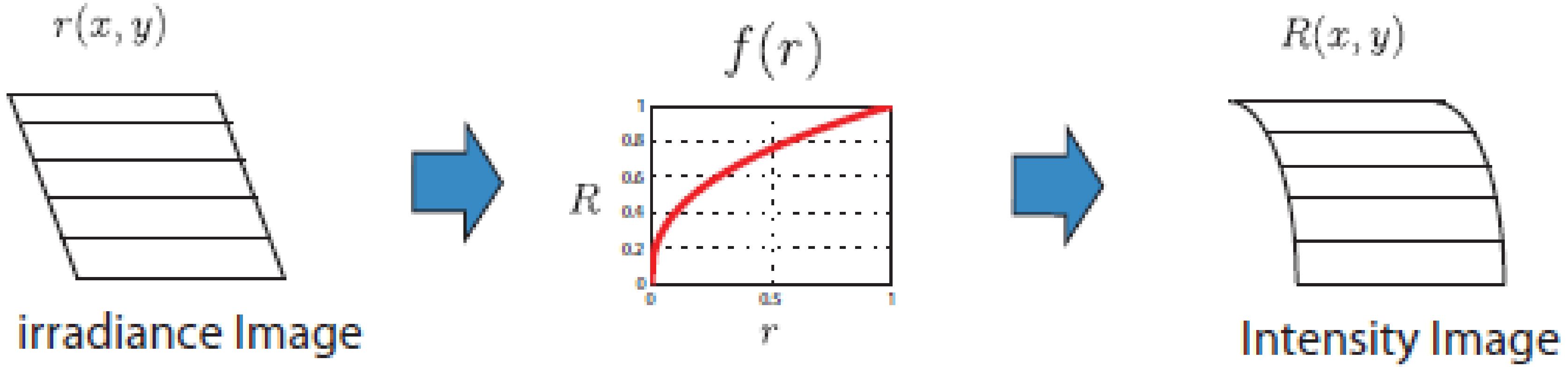
$$S(m,n) = \begin{cases} 0 & , I_G(m,n) = 0 \\ 1 & , I_G(m,n) \neq 0 \end{cases}$$

1	2	1
2	0	2
1	2	1

A specific *M(i,j)*

Camera Response Function (CRF)

- Camera response function (CRF) is a mapping of image irradiance (light energy incident on image sensors) to image intensity (output of a camera) for making the output image visually pleasing.
- CRF is the combination of the operations performed at the stages after the sensor
- CRF attributes are unique to each model and can be estimated to represent camera models



Quantisation Table of JPEG

- The choice of Quantisation Table in the JPEG compression algorithm is highly dependent on the particular camera manufacturer, and to a lesser extent on the model series
- The Quantisation Table stored as metadata may be removed or modified. So the ability of re-establishing the Quantisation Table from the content is therefore useful.
- Recompression may not remove the trace of the previous quantisation from the content, making it possible to establish compression history

Source Device Identification Based on Sensor Pattern Noise

Chang-Tsun Li

Department of Computer Science
University of Warwick
UK

What is Sensor Pattern Noise

- Sensor Pattern Noise (SPN) is the noise left in the images by the sensors of digital imaging devices such as cameras, camcorders and scanners.
- SPN is mainly caused by
  - manufacturing imperfection and
  - different sensitivity of pixels to light due to the inhomogeneity of silicon wafers.
- Sensors made from the same silicon wafer possess unique SPN.
- So identification based on SPN can be accurate to the level of individual devices, rather than just the level of models.

“Traditional” SPN Extraction Method

- Lukáš et al’s model for SPN extraction

  J. Lukáš et al., “Digital Camera Identification from Sensor Pattern Noise,” *IEEE TIFS,* 1(2),pp. 205 –214, 2006

$$n = I(i,j) - I'(i,j)$$

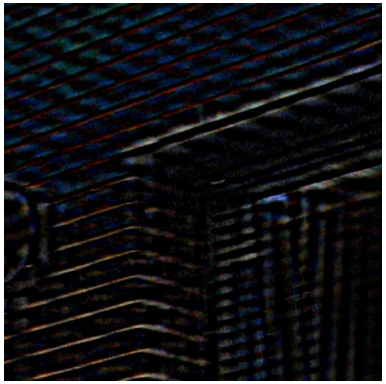
$$I' = Weiner\_filter(I)$$

  - I is the original image
  - I' is the low-pass filtered version of I by the Weiner filter applied in the wavelet transform domain
  - n is the extracted SPN
- SPN is the high-frequency component of the image.

Interference from Scene Details

- Details from scenes, e.g., brick walls, tree leaves, or other kinds of textures, contribute to the high-frequency components of images.

natural image



SPN

a clean SPN

a contaminated SPN

Our Proposal

- Proposal: Assigning weighting factors inversely proportional to the magnitude of the SPN components to get an enhanced SPN n_e .

  C.-T Li, "Source Camera Identification Using Enhanced Sensor Pattern Noise," *IEEE TIFS*, 5(2), pp. 280 - 287, 2010

- Rationale: The stronger a component in the SPN is, the greater the presence of details is, thus the less trustworthy the component should be.

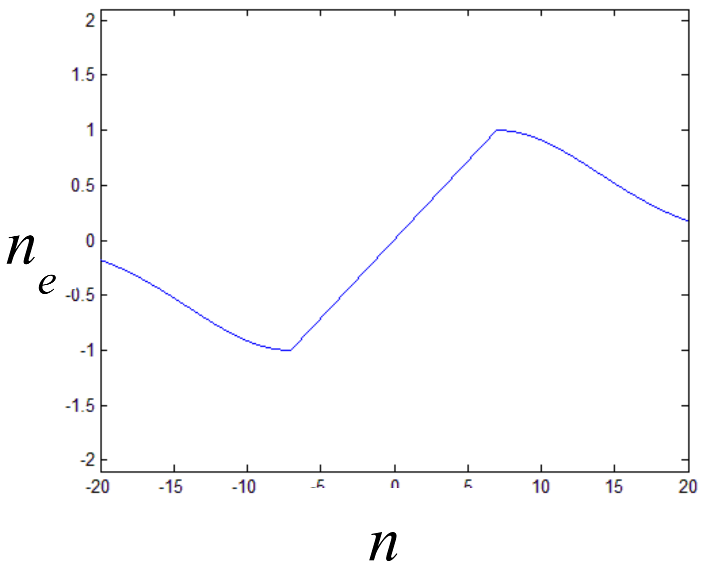
- Implementation:

  - Stronger SPN components ($|n| > \alpha$) should be attenuated monotonically and rapidly with respect to $|n|$ to suppress the influence from scene details.

  - For weaker SPN components (i.e., $|n| \le \alpha$), different considerations as discussed later are reflected in five models.

SPN Enhancer 1

- Monotonic attenuation for $|n| > \alpha$
- Linear transformation for $|n| \le \alpha$, i.e. every component is given the same weight



$$n_e(i,j) = \begin{cases} \frac{n(i,j)}{\alpha} & \text{, if } 0 \le n(i,j) \le \alpha \\ e^{-0.5\frac{(n(i,j)-\alpha)^2}{\alpha^2}} & \text{, if } n(i,j) > \alpha \\ \frac{n(i,j)}{\alpha} & \text{, if } -\alpha \le n(i,j) < 0 \\ -e^{-0.5\frac{(n(i,j)+\alpha)^2}{\alpha^2}} & \text{, if } n(i,j) < -\alpha \end{cases}$$

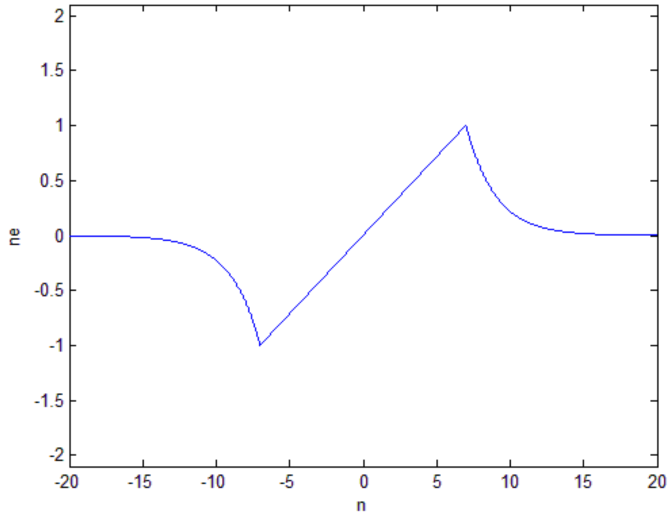
n : original SPN magnitude

n_e : enhanced magnitude

α : determines the rate *n* is attenuated

SPN Enhancer 2

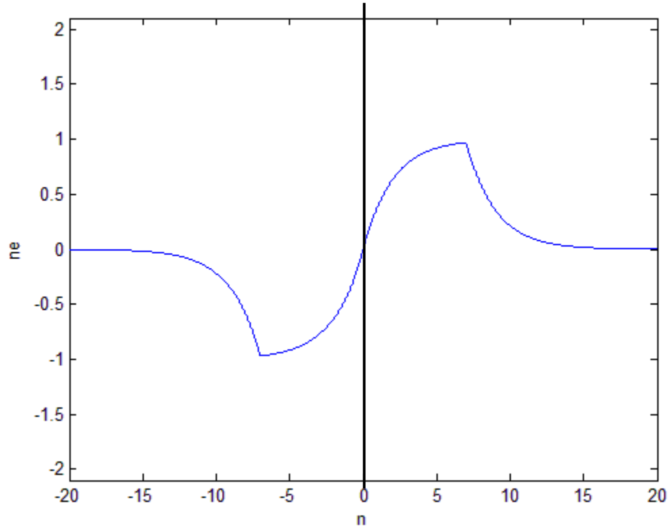
- Monotonic attenuation for $|n| > \alpha$ (more aggressive than Model 1)
- Linear transformation for $|n| \le \alpha$, i.e. every component is given the same weight



$$n_e(i,j) = \begin{cases} \frac{n(i,j)}{\alpha} & \text{, if } 0 \le n(i,j) \le \alpha \\ e^{\alpha - n(i,j)} & \text{, if } n(i,j) > \alpha \\ \frac{n(i,j)}{\alpha} & \text{, if } -\alpha \le n(i,j) < 0 \\ -e^{\alpha + n(i,j)} & \text{, if } n(i,j) < -\alpha \end{cases}$$

SPN Enhancer 3

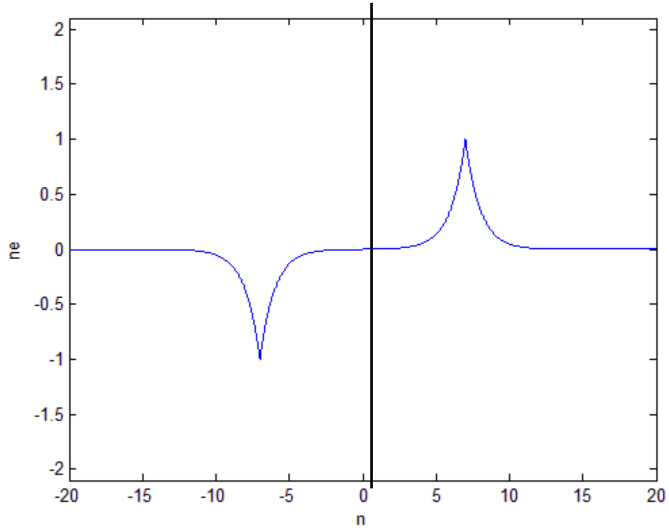
- Non-linear exponential transformation for $|n| \le \alpha$.
- By the gradients, we can see that (unlike model 1 & 2) this model gives greater significance to the SPN components on the lower ends and less significance to those closer to $\pm\,\alpha$



$$n_e(i,j) = \begin{cases} 1 - e^{-n(i,j)} & ,\text{if } 0 \le n(i,j) \le \alpha \\ (1 - e^{-\alpha}) \cdot e^{\alpha - n(i,j)} & ,\text{if } n(i,j) > \alpha \\ -1 + e^{n(i,j)} & ,\text{if } -\alpha \le n(i,j) < 0 \\ (-1 + e^{-\alpha}) \cdot e^{\alpha + n(i,j)} & ,\text{if } n(i,j) < -\alpha \end{cases}$$

Infeasible Model

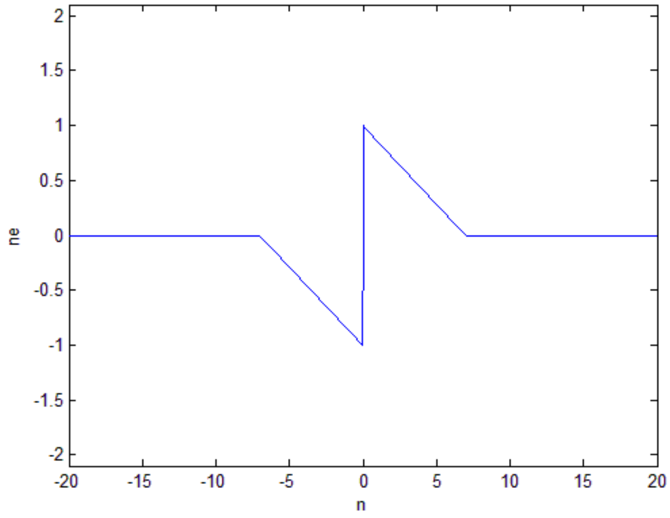
- Not any <u>non-linear exponential</u> transformation for $|n| \le \alpha$ is feasible.



$$n_e(i,j) = \begin{cases} 1 - e^{-n(i,j)} & \text{, if } 0 \le n(i,j) \le \alpha \\ (1 - e^{-\alpha}) \cdot e^{-\alpha + n(i,j)} & \text{, if } n(i,j) > \alpha \\ -1 + e^{n(i,j)} & \text{, if } -\alpha \le n(i,j) < 0 \\ (-1 + e^{-\alpha}) \cdot e^{-\alpha - n(i,j)} & \text{, if } n(i,j) < -\alpha \end{cases}$$

SPN Enhancer 4

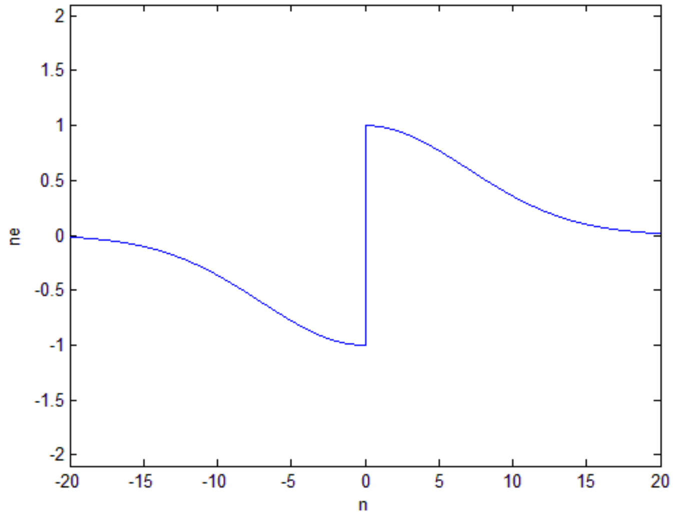
- Inversely proportional transformation: Allow the magnitude of n_e, (i.e., $|n_e|$) to *decrease* monotonically with respect to the magnitude of n.



$$n_e(i,j) = \begin{cases} 1 - \frac{n(i,j)}{\alpha} & ,\text{if } 0 \le n(i,j) \le \alpha \\ -1 - \frac{n(i,j)}{\alpha} & ,\text{if } -\alpha \le n(i,j) < 0 \\ 0 & ,\text{otherwise} \end{cases}$$

SPN Enhancer 5

- <u>Inversely proportional</u> transformation: Allow the magnitude of n_e, (i.e., $|n_e|$) to *decrease* monotonically with respect to the magnitude of n.



$$n_e(i,j) = \begin{cases} e^{-0.5n^2(i,j)/\alpha^2} & \text{, if } 0 \le n(i,j) \\ -e^{-0.5n^2(i,j)/\alpha^2} & \text{, otherwise} \end{cases}$$

Source Device Identification

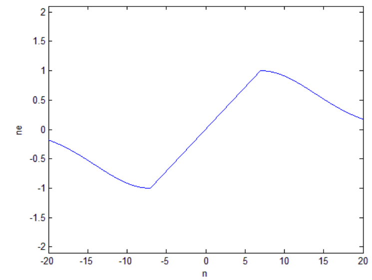
- Task: Given a set of cameras or reference SPNs of cameras and an image which has taken by one of the cameras, identify the camera that has taken the image.
- Similarity measure: normalised cross correlation between SPN n_i and n_j

$$\rho(i,j) = \frac{(n_i - \bar{n}_i)\cdot(n_j - \bar{n}_j)}{\left\| n_i - \bar{n}_i \right\| \cdot \left\| n_j - \bar{n}_j \right\|} \qquad , i,j \in \{1,2,3,\ldots,M\}$$

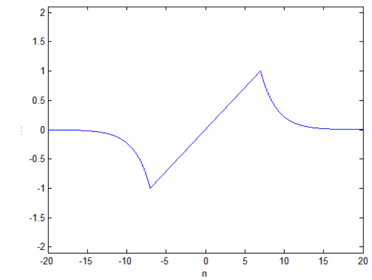
Identification Experiment

- Experiments: Tests have been carried out on image blocks of 128 × 128 pixels cropped from **1200 photos** of taken by **six** cameras, each responsible for **200.**
- Why small blocks: The performance of the models tested on small blocks is not close to 100%, which leaves room for revealing the real performance of each model.
- The six cameras are: Canon IXUS 850IS, Canon PowerShot A400, Canon IXY Digital 500, FujiFilm A602, FujiFilm FinePix A902, Olympus FE210

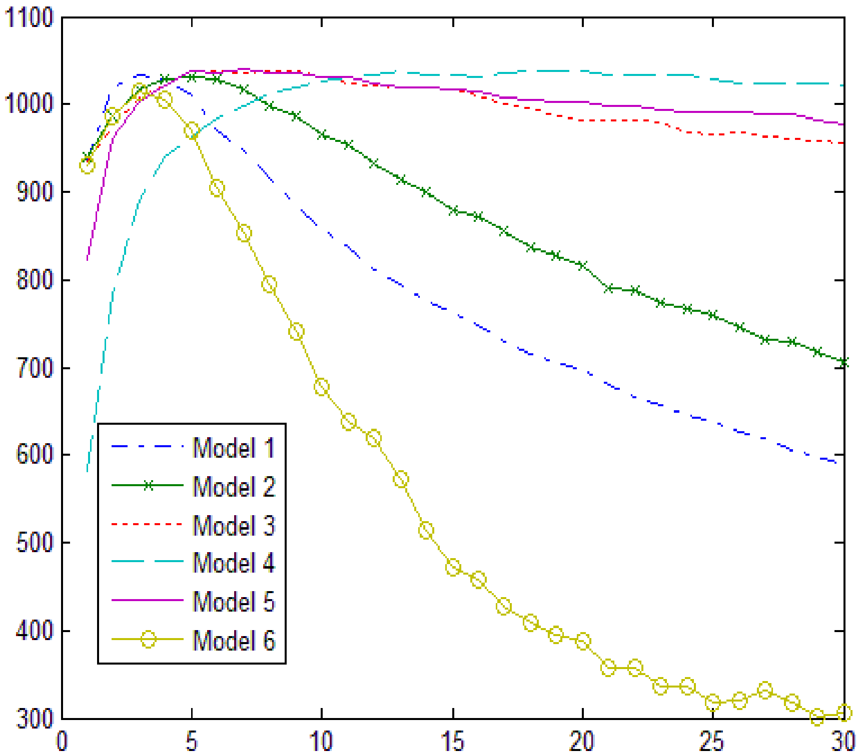
Performance Analysis – Model 1 & 2



Model 1



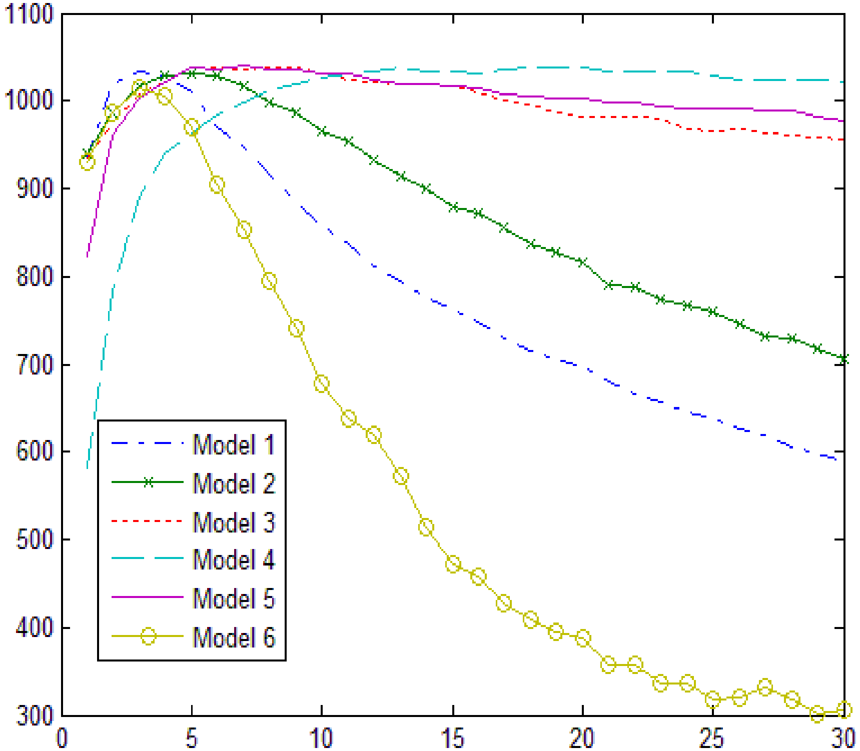
Model 2



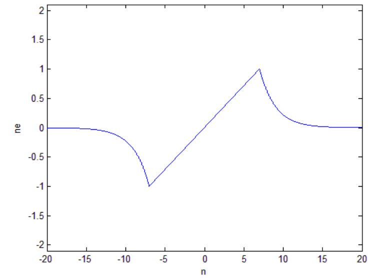
Performance, in terms of *number of correct source camera identifications out of 1200 images w.r.t α*

- Performance is good in a small range of *α* but drops rapidly when compared to Model 3, 4 and 5, indicating that the linear model for |n| ≤ α is too sensitive to the selection of the values for α.
- For |*n*| > *α*, Model 2 perform better than model 1, indicating that a greater attenuation rate is preferable for strong SPN components.

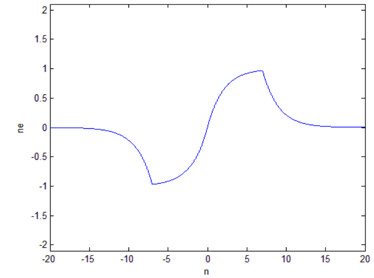
Performance Analysis – Model 2 & 3



Performance, in terms of *number of correct source camera identifications out of 1200 images w.r.t α*



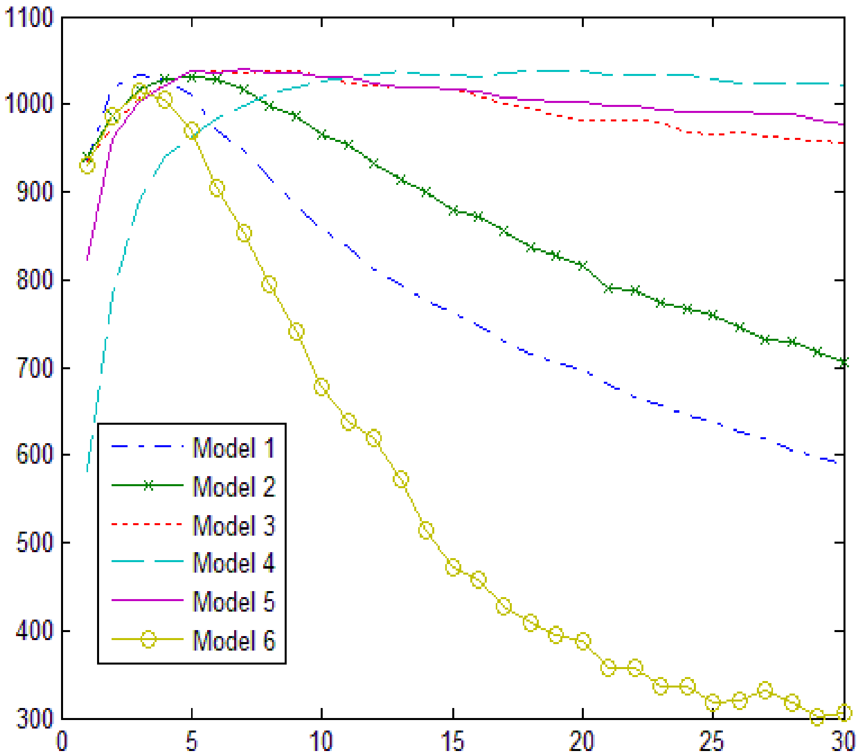
Model 2



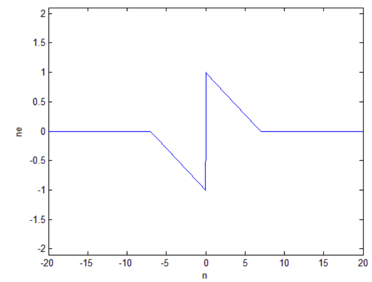
Model 3

- The difference between Models 2 and 3 is the transformations for |n| ≤ α
- Model 3 performs better than model 2, because Model 2 indiscriminatively assigns an equal weight to every component when $|n| < \alpha$ while Model 3 adaptively decreases the weight as $|n|$ grows (i.e., as the influence of scene details gets stronger).
- Model 6 is infeasible

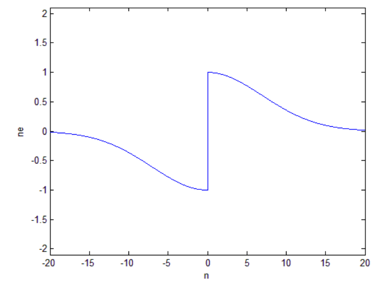
Performance Analysis – Model 4 & 5



Performance, in terms of *number of correct source camera identifications out of 1200 images w.r.t α*



Model 4



Model 5

- Both model perform well.
- We shall use model 5 with α = 7 in the experiment to be introduced later.

Identification With & Without Enhancement – True Positive

- True positive rates *with* and *without* applying Model 5 to the sensor pattern noises with $\alpha = 7$.
- The image is deemed as taken by the *source* camera if the similarity value is greater than a threshold 0.01.

	True positive rate (%) at different photo sizes								
	128 ×128	128 × 256	256 × 256	256 × 512	512 × 512	512 ×1024	1024 ×1024	1024 ×2048	1536 ×2048
without enhancement	61.68	67.5	71.42	77.92	82.33	87.12	93.25	96.75	97.42
with enhancement	79.75	85.58	91.00	93.17	94.75	96.33	97.95	98.25	98.25

Identification With & Without Enhancement – False Positive

- False positive rates *with* and *without* applying Model 5 to the sensor pattern noises with $\alpha = 7$.
- The image is deemed as taken by the *source* camera if the similarity value is greater than a threshold 0.01.
- True positive + False positive ≠ 100% because for some images, their SNP similarities with the 6 reference SNPs are lower than 0.01 and as a result no positive (neither true or false) is reported.

	False positive rate (%) at different photo sizes								
	128 ×128	128 × 256	256 × 256	256 × 512	512 × 512	512 ×1024	1024 ×1024	1024 ×2048	1536 ×2048
without enhancement	41.68	38.68	32.60	25.71	16.28	6.75	1.90	2.40	12.03
with enhancement	8.33	3.22	0.95	0.15	0.03	0	0	0.03	0.4

Trustworthiness of SPN

- Signature Removal: which could be maliciously carried out to confuse investigators

  How: Low-pass filtering or

  $$I_A'(i,j) = I_A(i,j) - \alpha \cdot n_A, \quad \alpha \text{ is a strength factor}$$

- Signature Substitution: could be applied to mislead forensic investigations

  How: $I_A'(i,j) = I_A(i,j) - \alpha \cdot n_A + \beta \cdot n_B \quad \alpha \text{ and } \beta \text{ are strength factors}$

Conclusions

- Image forensics using “fingerprint” left in the images by the imaging devices has emerged as a new area of research in the last few years.
- Sensor pattern noise (SPN) is one of the most promising types of fingerprint.
- The “traditional” SPN extraction method is unable to cope with the interference of the scene details.
- A simple, yet effective, SPN enhancer is proposed in this work.