Camera Forensics

Jean-Baptiste Boin, Tiffany Jou
Psych 221, Winter
03/20/2013

Goal

- Classify real vs. fake images
- Localize tampered region in fake images

Background

- Camera Forensics
  - Exploit periodicity of Color Filter Array
- Unknown sampling lattice + Unknown interpolation
  - Expectation-Maximization (EM)

Algorithm

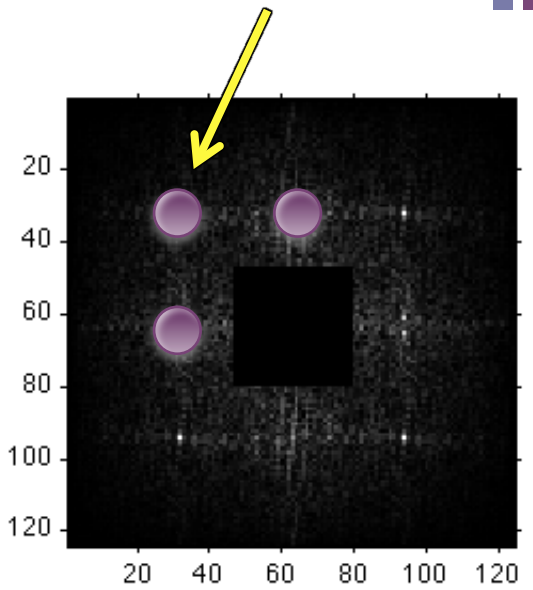
- Sliding blocks: 64x64
  - 32 pixels increments
- EM
- Localization: Clustering
- Classification

Algorithm: EM

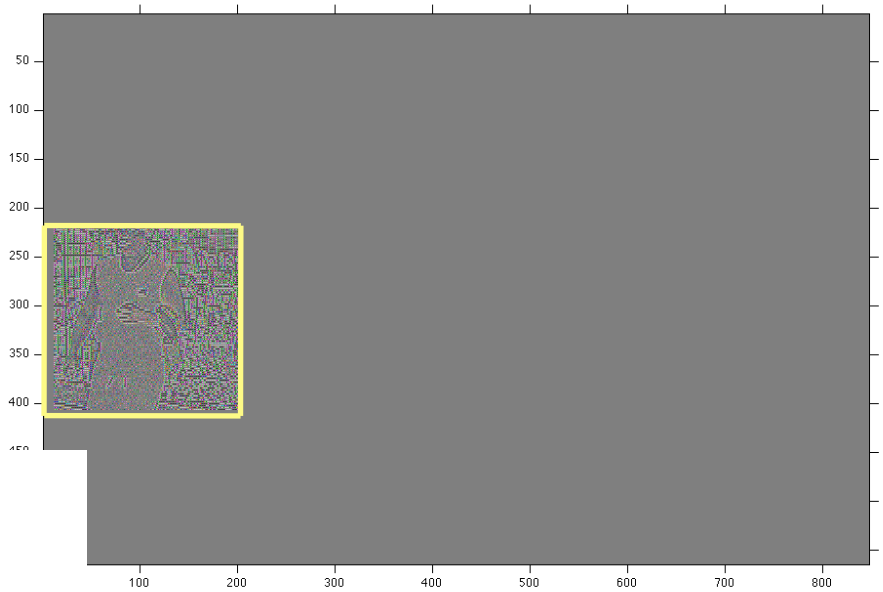
- Probability map: Fourier Transform
- Alphas
  - Describe interpolation

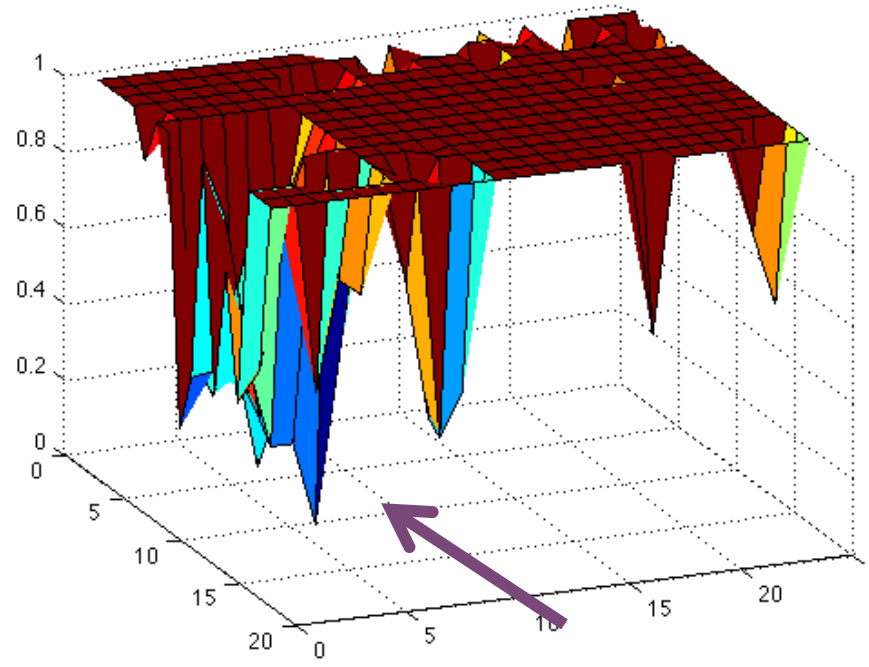
FFT

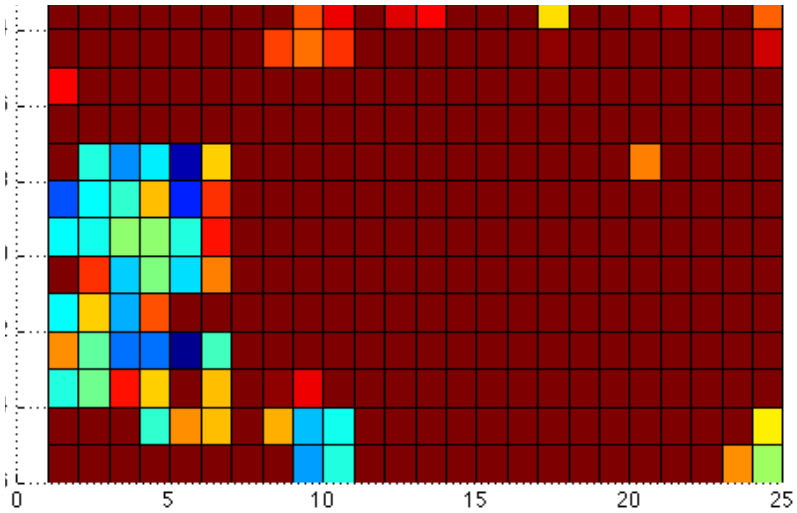
- Assume Bayer pattern
- Normal FFT block: high intensity in at least one of 3 points
- Pick the one with highest intensity
- Normalize this value with max value
- “FFT peak” : represents block
- 3 color channels



FFT


50
100
150
200
250
300
350
400
100
200
300
400
500
600
700
800

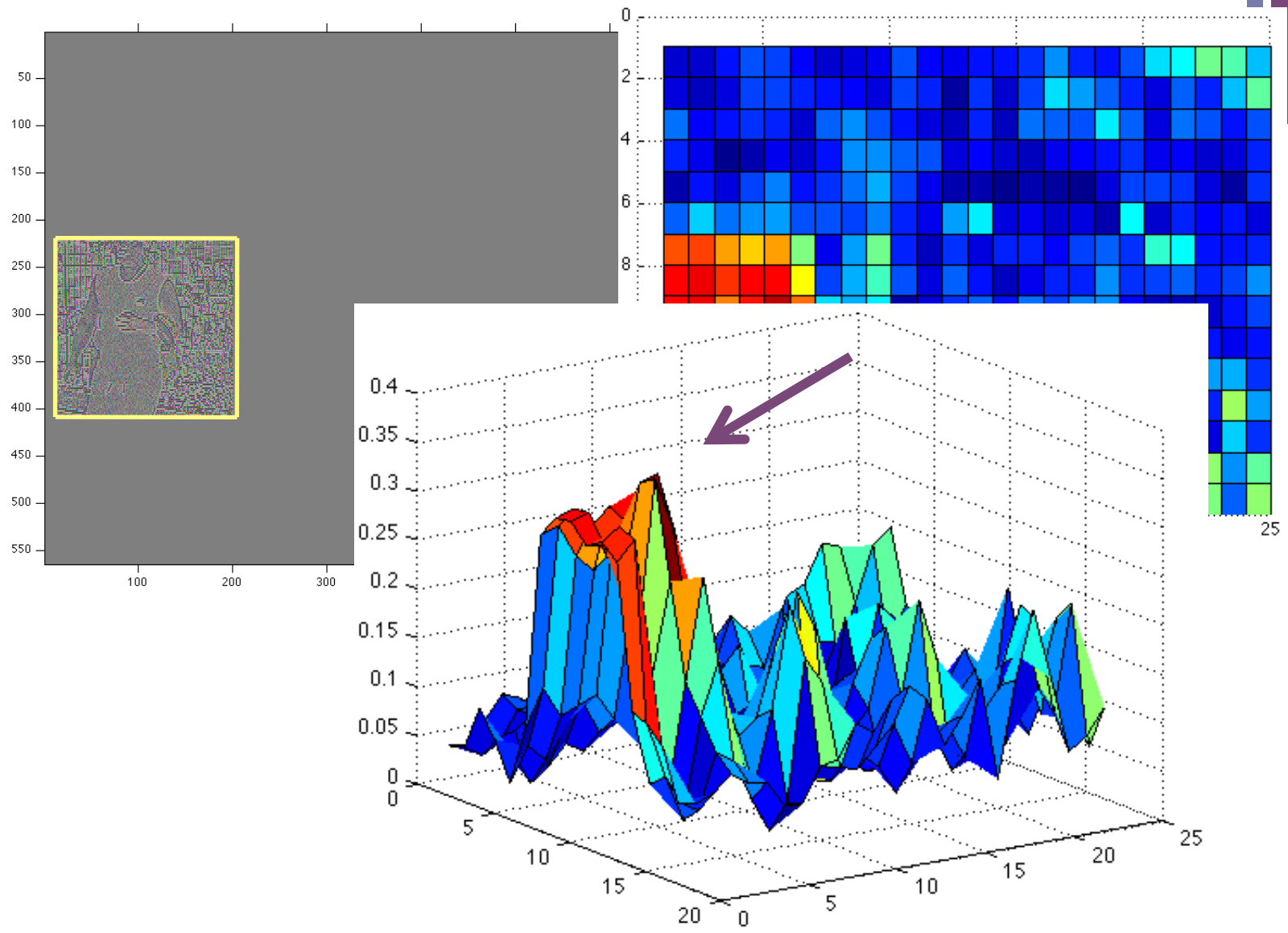

1
0.8
0.6
0.4
0.2
0
0
5
10
15
20
0
5
15
20
25


0
5
10
15
20
25

alphas

- alpha vector for every block
- Find median alpha vector of image
- Calculate the norm between alpha vector of each block with median
- Tampered region= large norm values

alphas

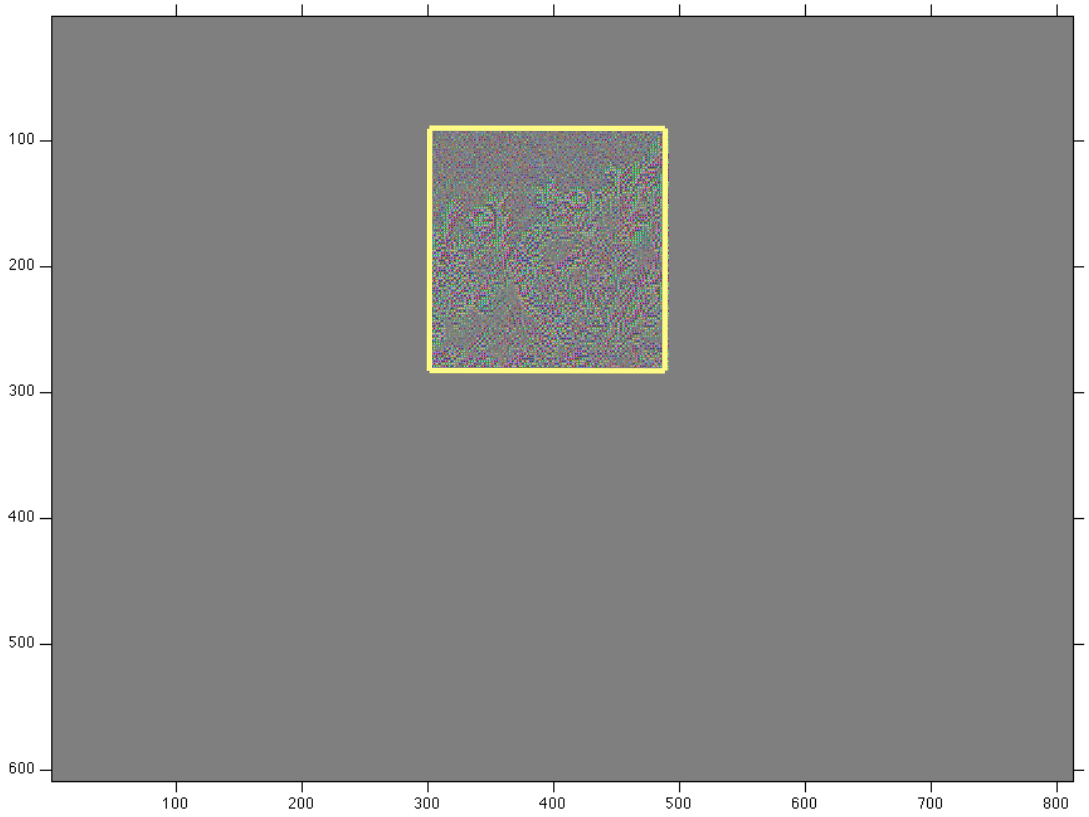

50
100
150
200
250
300
350
400
450
500
550
100
200
300
0
2
4
6
8
25
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
5
10
15
20
0
5
10
15
20
25

Algorithm: Clustering

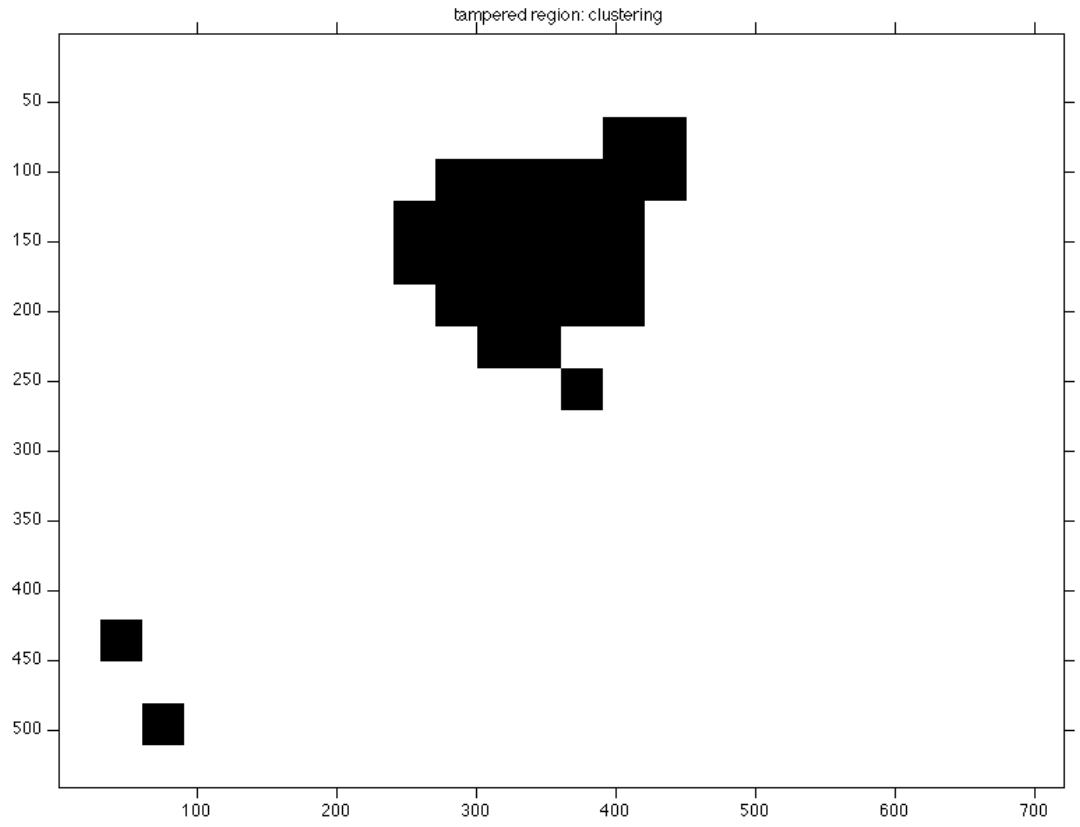
- 27-dim vector per block
- 2-cluster k-means
- Initialization
  - Use min FFT peak block as centroid for one cluster
  - Find other centroid far away
- Force one cluster to be smaller than the other
- Different weights between FFT peaks and alphas

Results: Clustering

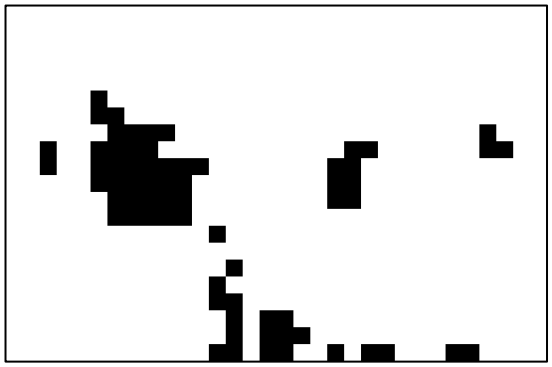
Results: Clustering



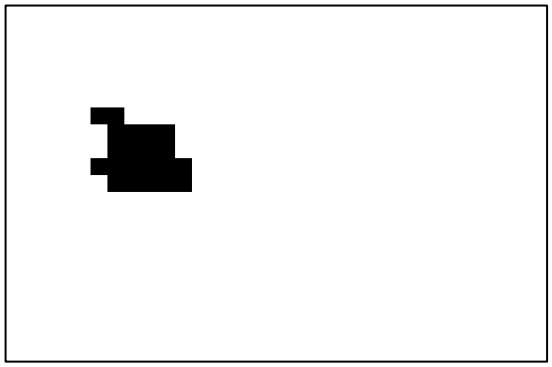
Results: Clustering



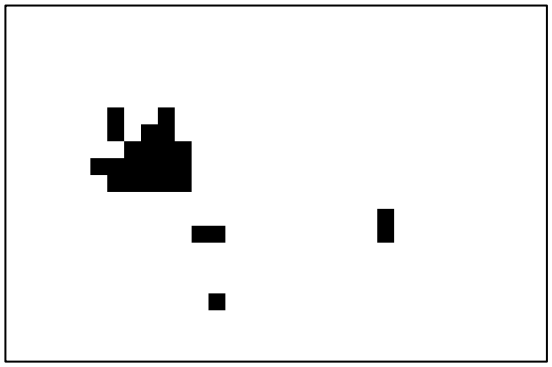
Weight sequence



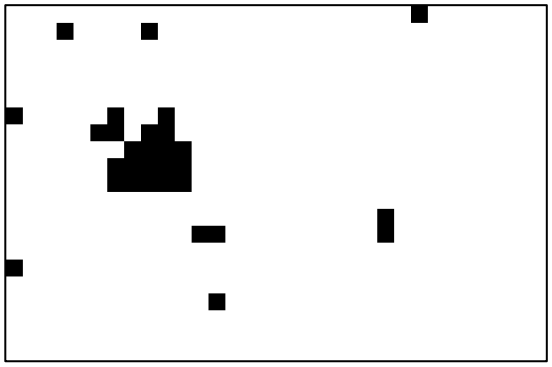
1



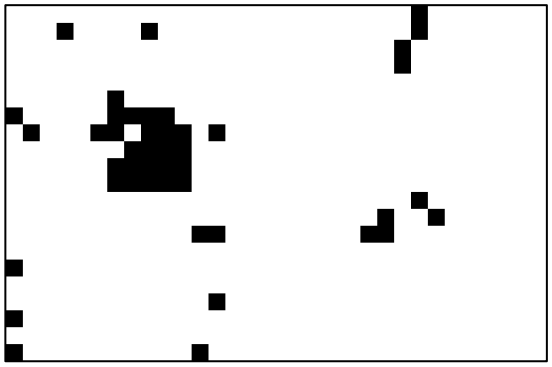
2



3



4



5

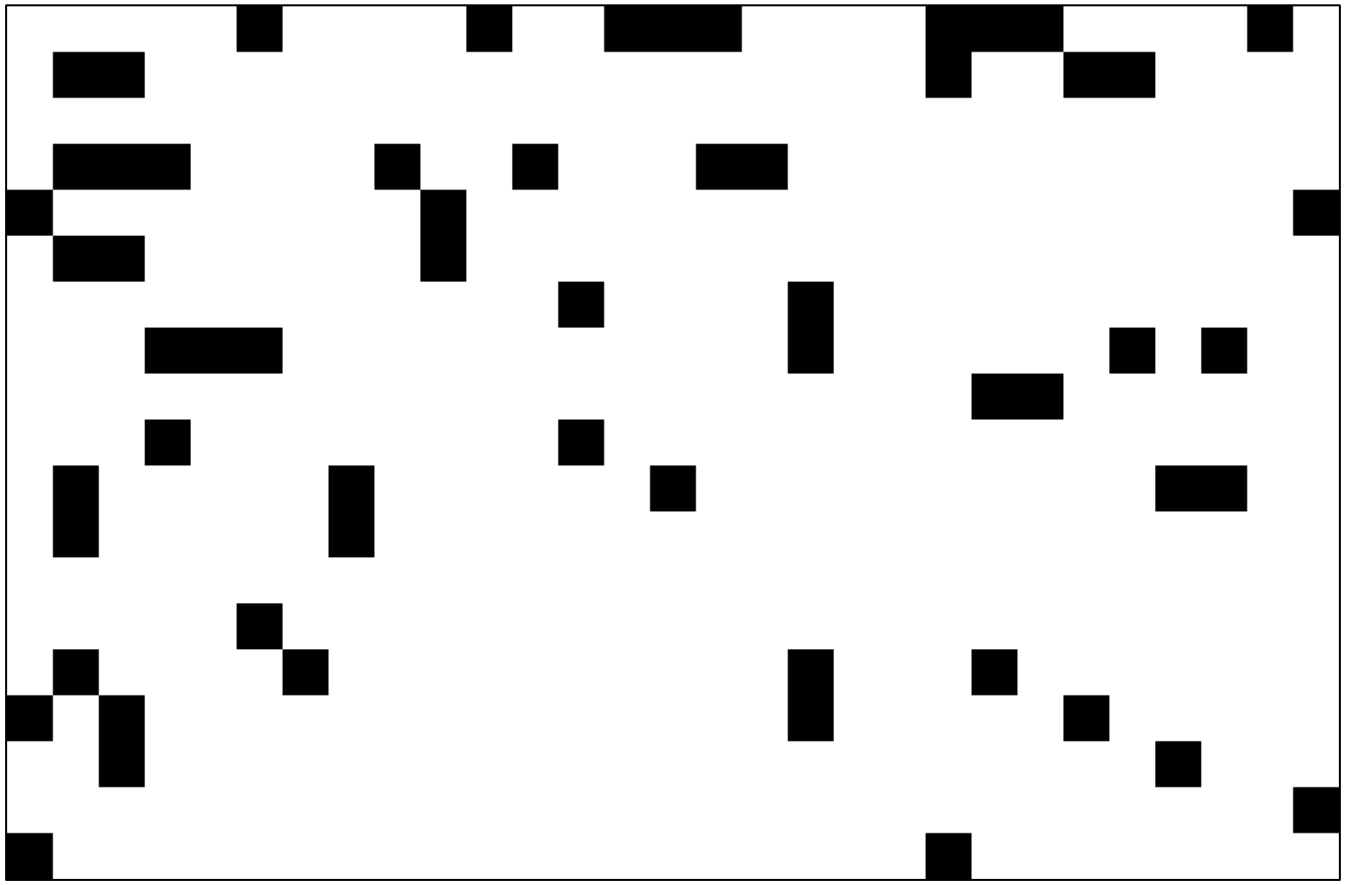
Assumptions

- Only one tampered zone
- Tampered zone is not too small
  - Block size = 64 x 64
  - Lower bound for detection
- Tampered zone is not too big
  - < 60 % of image size

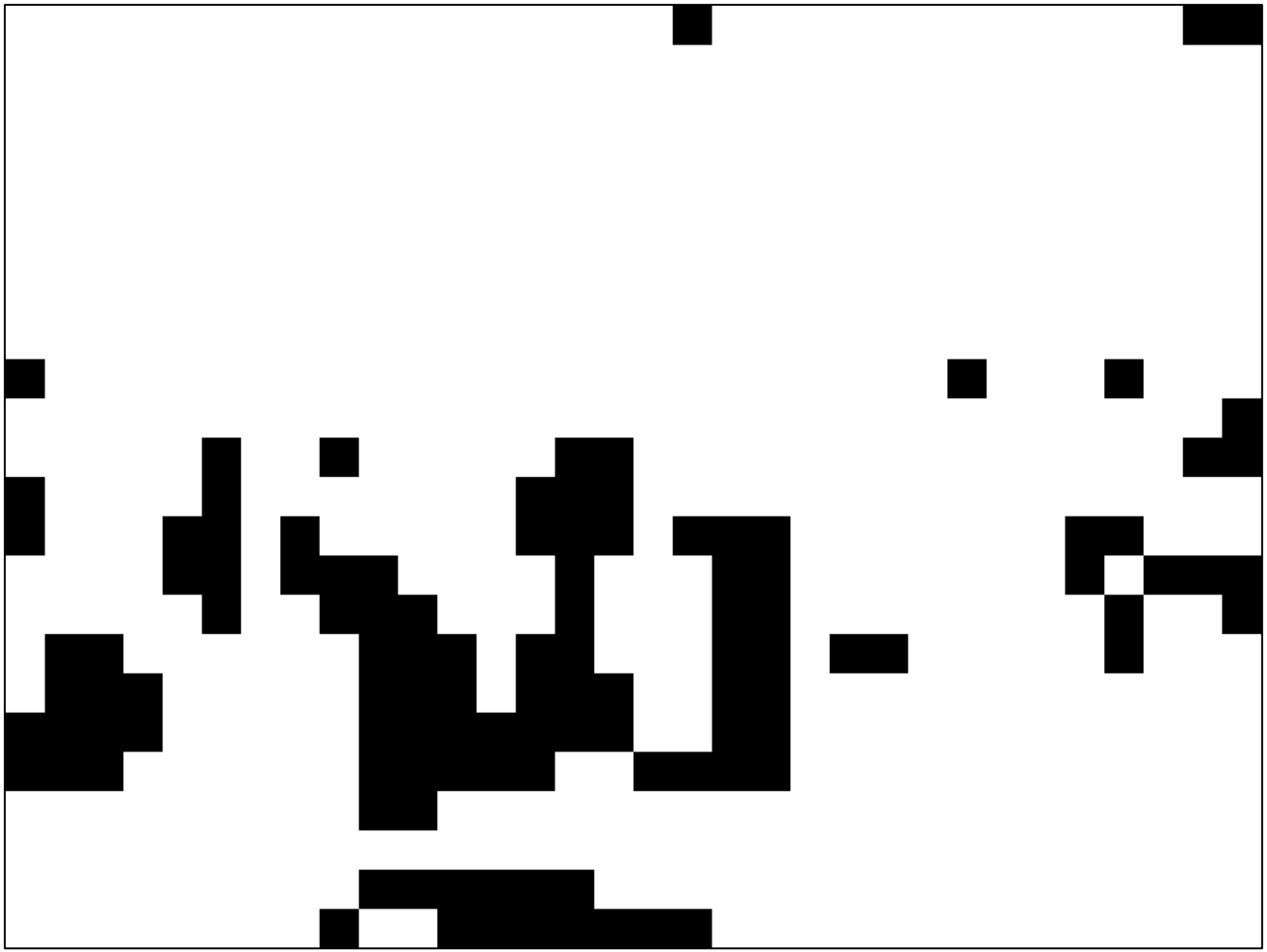
Algorithm: Classification

- Goal : separate signal from noise
- Properties of the signal
  - One connected component of moderate size
- Properties of the noise
  - Small multiple components or one very big (case of large uniform zones)
- Introduction of parameters to classify our map properly

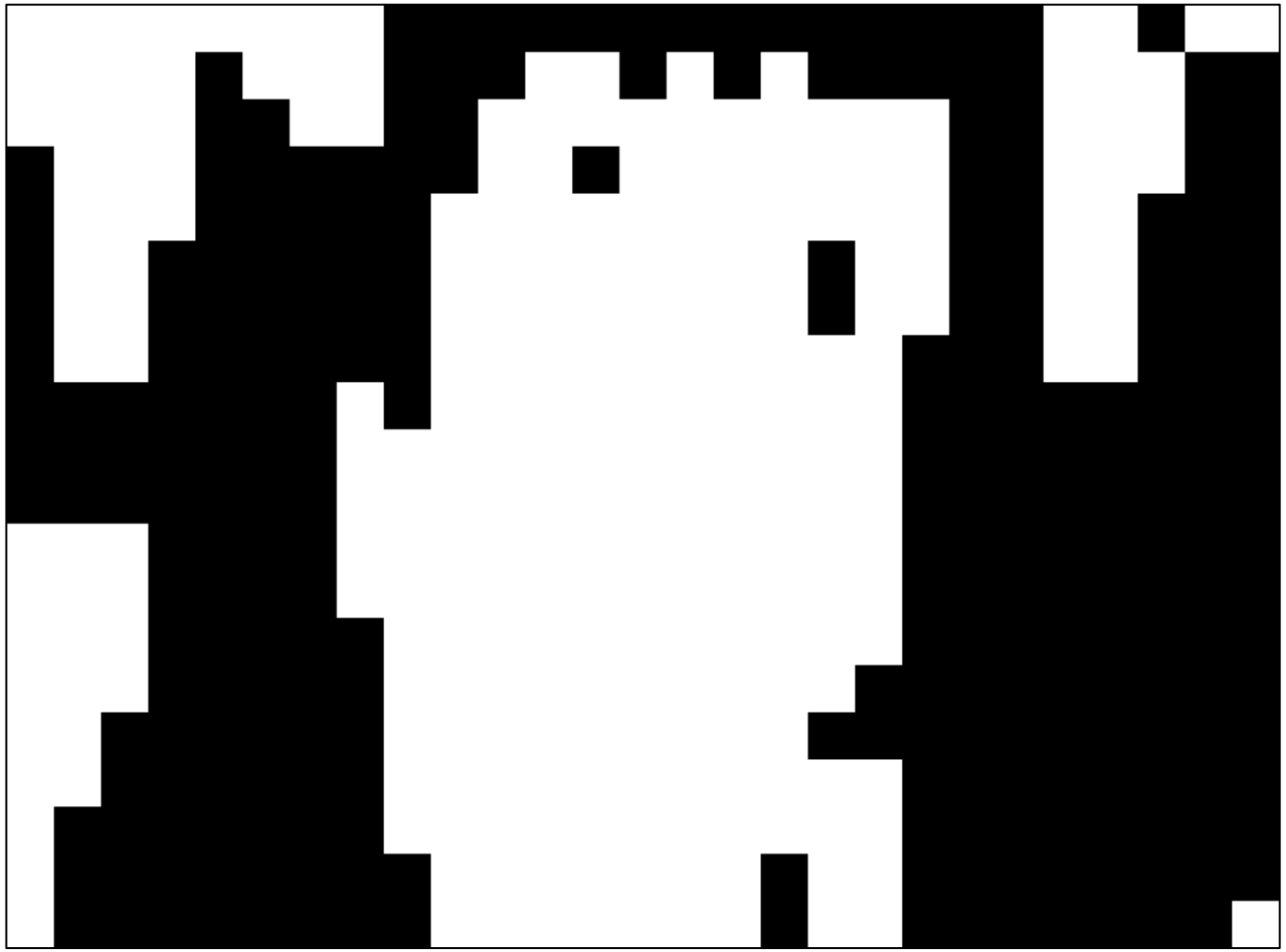
Results: Real Image 1



Results: Real Image 2



Results: Real Image 3

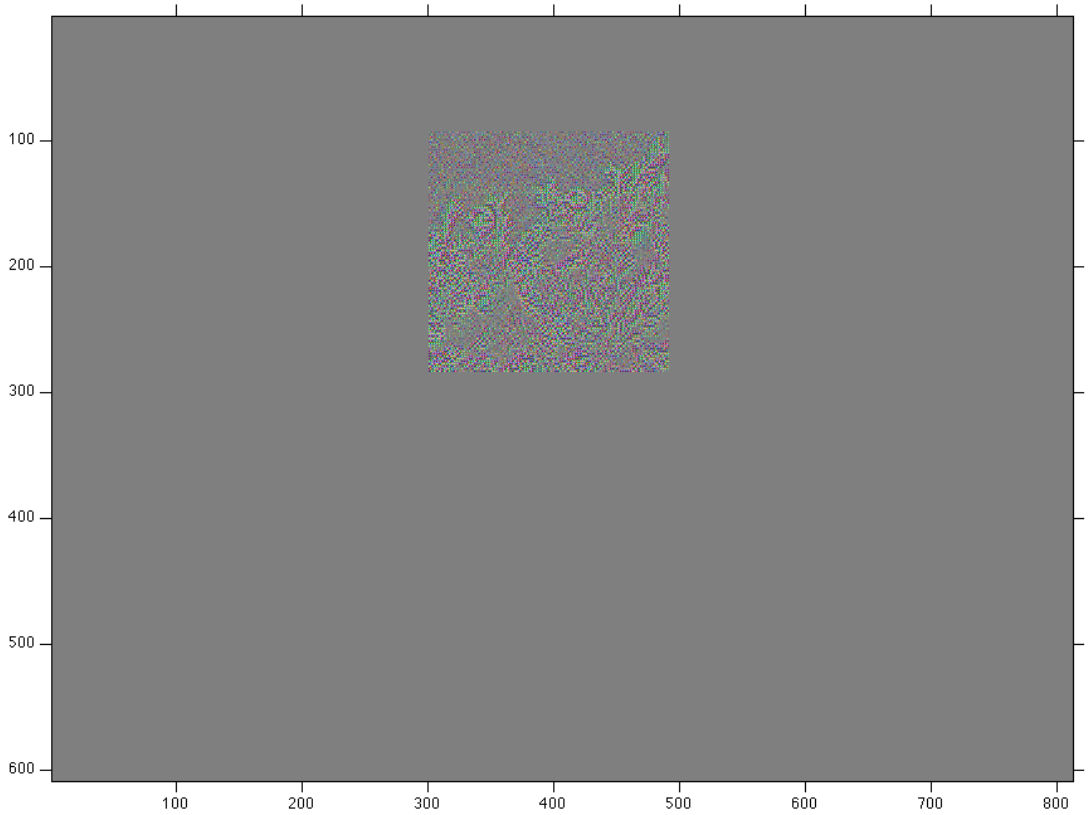


Algorithm: Classification

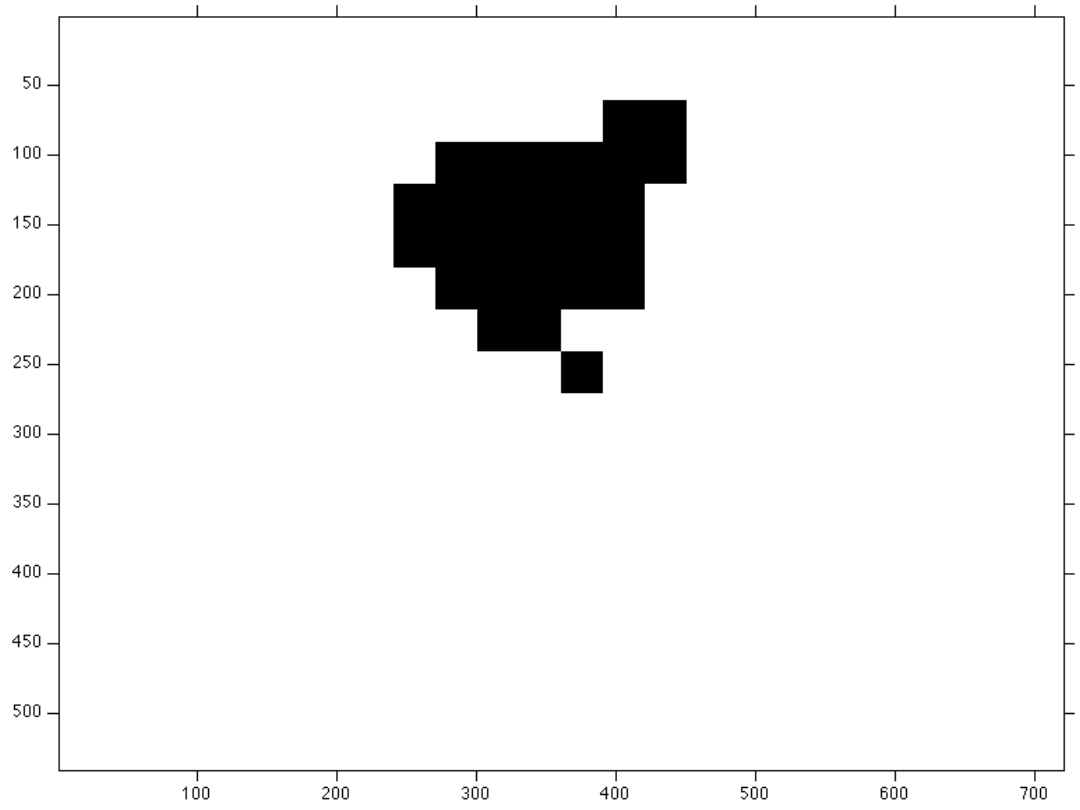
- Parameters
  - Smallest admissible noise
  - Comparison signal to total noise
  - Maximum size of our signal
- Apply for each of the 5 block maps
- Keep the only connected component that verifies our constraints
- If none of them does, the image is classified it as real

Results: Image 1

Results: Image 1

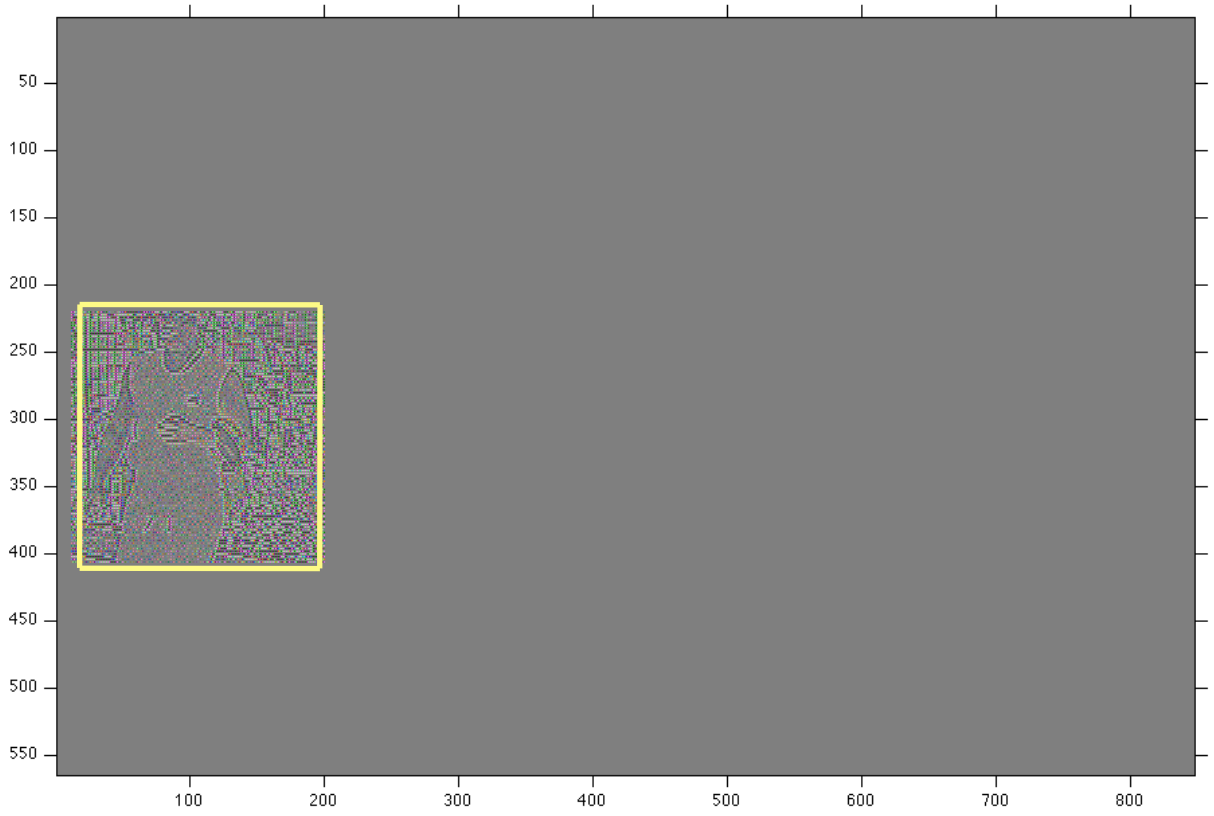


Results: Image 1

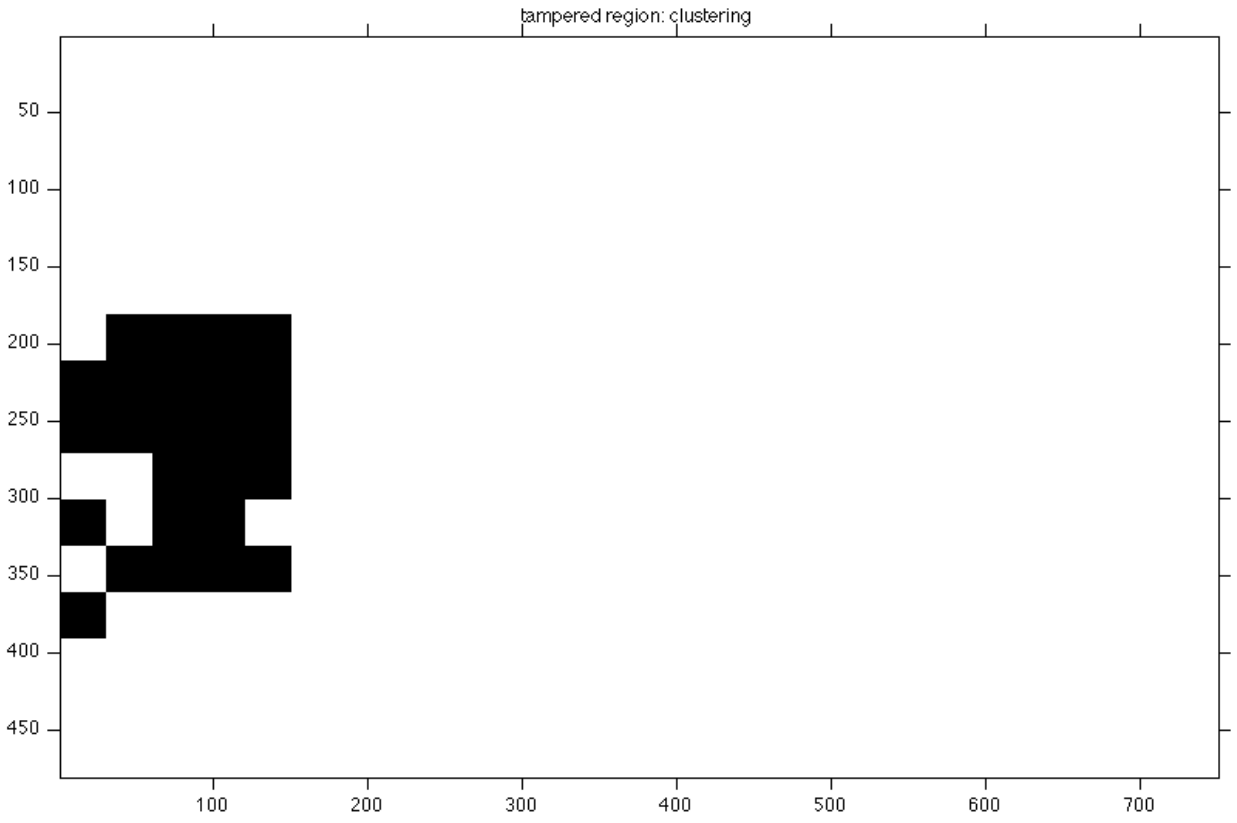


Results: Image 2

Results: Image 2

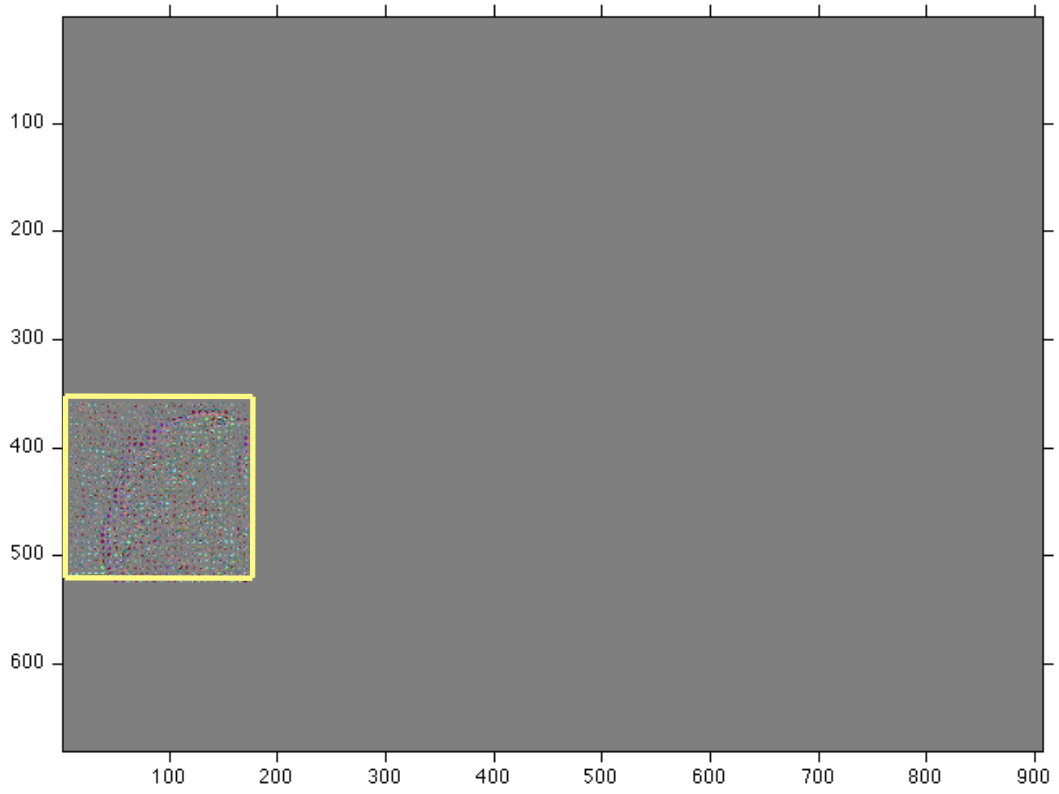


Results: Image 2

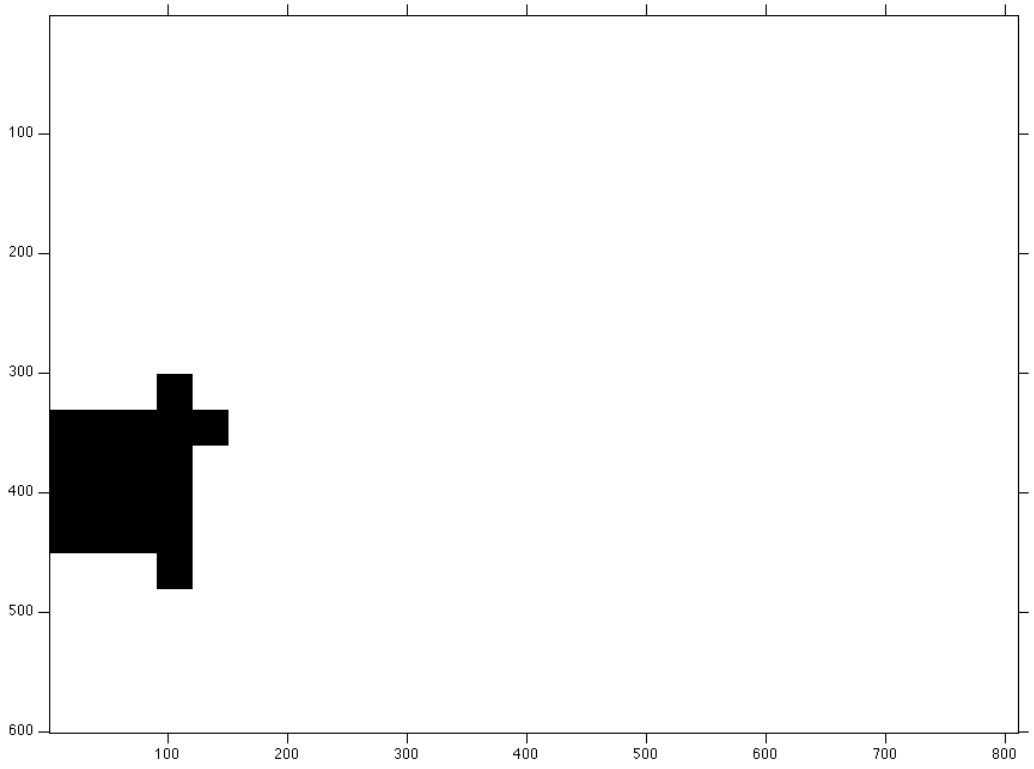


Results: Image 3

Results: Image 3



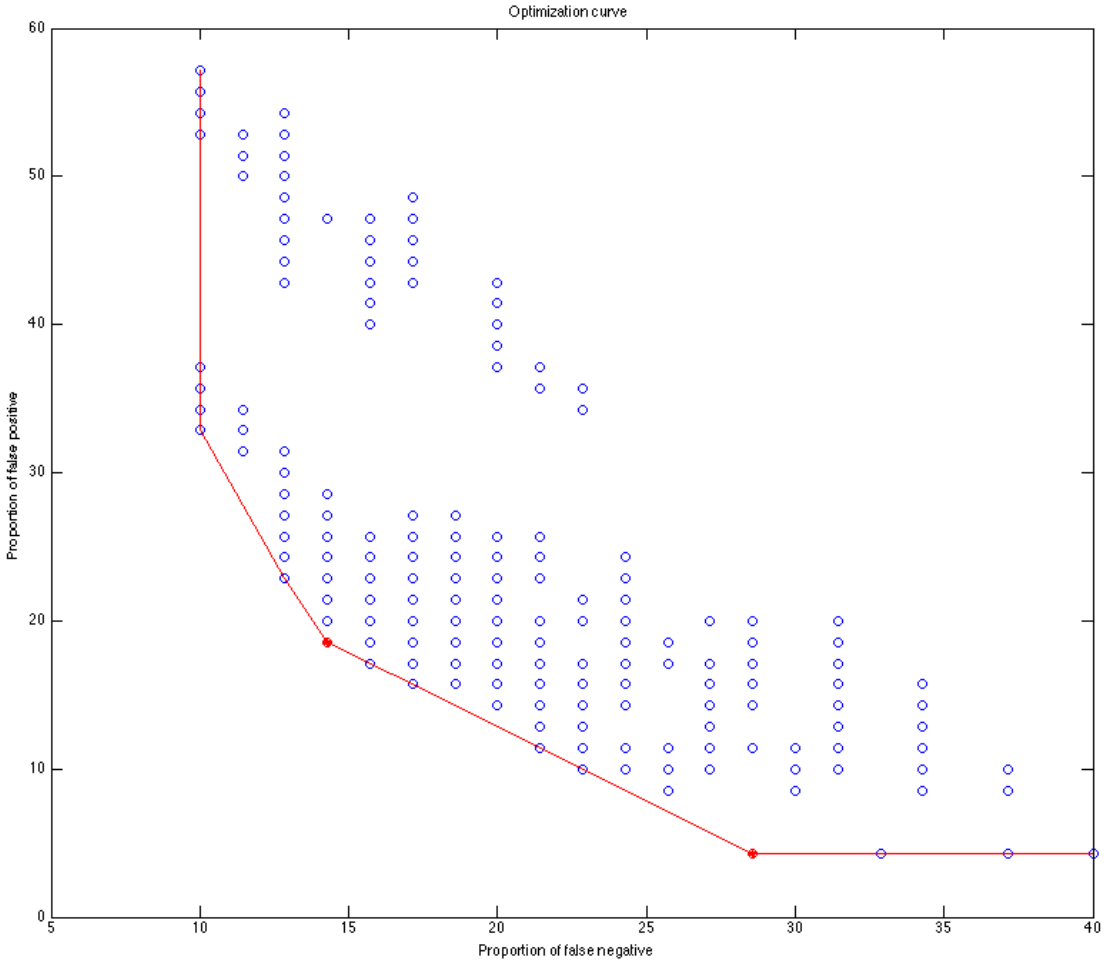
Results: Image 3



Results: Classification

- 140 given images (70 tampered, 70 untampered)
- Based on test images, we choose our parameters to achieve the best performances
- Degree of freedom on our sets of parameters depending on our priorities : Pareto curve

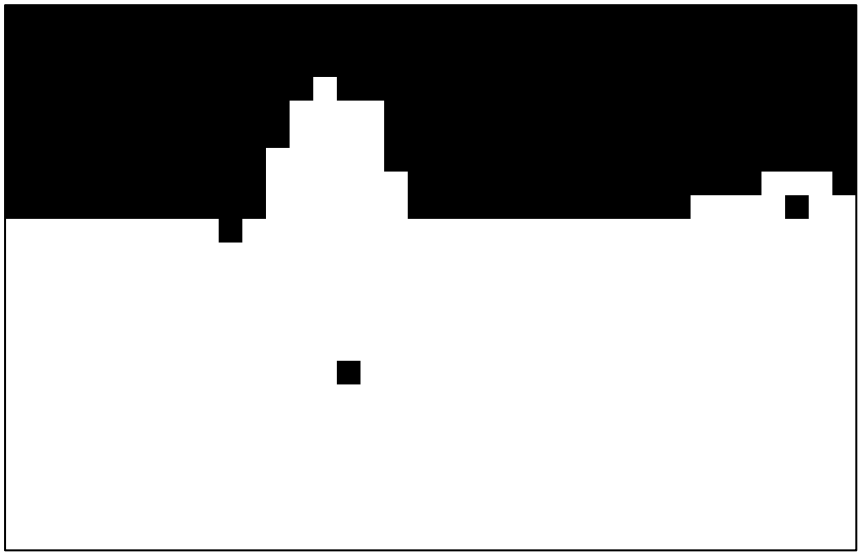
Results: Classification



Analysis - Reasons of failure

- Size of tampered region
- Sliding blocks of 64x64
- Large uniform zone in real images
  - No peaks, constant

Analysis - Reasons of failure



Ideas for Improvement

- Increase or decrease sliding block size
- Decrease sliding interval
  - More time
- Detect uniform regions
  - Process differently

Conclusion

- Main goal: detect local tampering in image
- For images that follow assumptions, classification & localization works well
- Classify between cameras
  - Use alpha values