Forensics project report

By

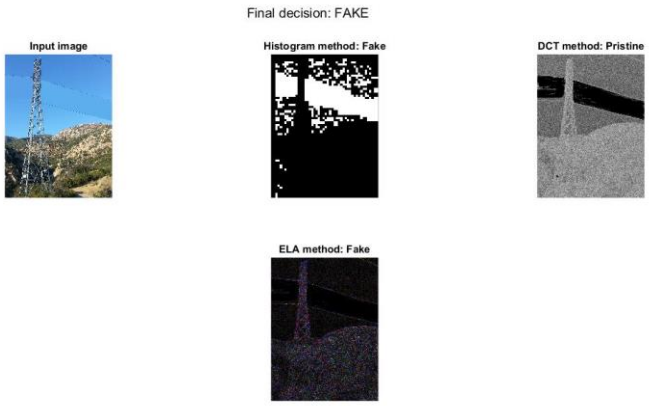
Shuyan
Aditya Jonnalagadda

4 strategies have been used.

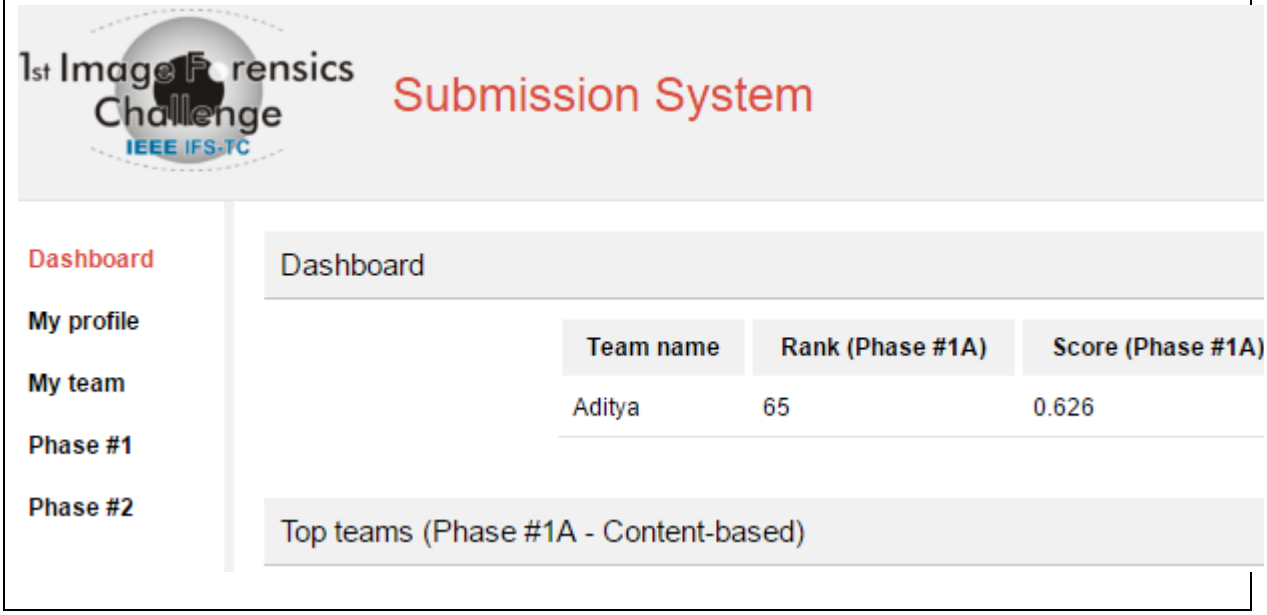
(1) Histogram based approach
(2) DCT based approach
(3) ELA based approach
(4) Copy-move based approach

(2), (3), (4) are standard methods and basic working of these algorithms were obtained online. We will explain about the changes that we did.

Sample output



Score for phase-1 : **62.6%**



- Inspiration for Histogram based approach is from “Forensic Detection of Image Manipulation using Statistical Intrinsic Fingerprints”
- The paper concentrated on the fact that there will some statistical fingerprints in the composite image due to slicing operation eg., because of contrast enhancement. It proposed that high frequency components can be observed in the transform of the histogram vector.
- Our analysis primarily hypothesized that if a splicing operation had been done, the lighting characteristics of the 2 regions will be of different nature. We wanted to capture this difference on the edges of the spliced image.
- **Approach #1:** We computed 100x100 block histograms on this edge and trained the SVM using transform of these histogram vectors. Negative (Pristine) samples were obtained from pristine images.
- One of our underlying assumptions is also that light intensity will be gradually varying over the images. Even if shadows are there, they will be soft in real scenes.
- **Approach #2:** We followed the approach from the paper. We computed the energy in high frequency components of the transform of histogram vector and classified the 100x100 block basing on this.
- Which means we had to find a local threshold for classifying each block as real or fake and a global threshold to classify the image as real or fake basing on number of real or fake blocks within the image.
- We tried various combinations of global and local thresholds using about 250 real and fake images, and came up with particular values for both. This seemed to give about 60-65% accuracy with about 100 real and fake images. But when we submitted this for score on phase-1 testing, score was only 0.5. Which pushed us to include other algorithms.
- DCT based algorithm only works if splicing is done on top of a jpeg image. Which were very few in the dataset, but this is quite trustworthy, which made us go for this.
- It gives an output image with foreign object highlighted.
- **Approach #3:** Now, as we need get a single output saying if its fake or real. Which made us think about block wise averaging. But we wanted to see if the inherent distribution within histogram is different between fake and real images as only a certain part of the fake image is highlighted.
- So we computed the histogram of the output of the algorithm output and trained the SVM basing on this. This worked. Then we went back to see what exactly SVM is doing. The ones which are being classified as fake have histograms biased to left and vice versa.
- In our testing, this method was giving about 50-55% because of very few jpeg source modifications. But this histogram method on top of algorithm output was working very well.
- Now in order to get better performance we used ELA and copy-move from the shared links on gauchospace.
- **Approach #4:** We thought it might be counterproductive to include the non-jpeg fake images as fake samples while training svm. So we manually went through all 900 fake images to come up with 75 fake images which were constructed from jpeg source image (concluded this basing one algorithm output for each of the 900 images).
- Then trained SVM only with confirmed fake examples, following table summarizes the effect of training SVM with x fake images and y real images (x-y)

	fake			real	
DCT (75 - 75)	17	183		168	33
DCT (75 - 60)	52	148		144	57
DCT (75- 75)	42	158		168	32
DCT (450- 450)	87	114		131	70

- **Approach #5:** For the ELA(error level analysis), algorithm outputs an image. Here also we needed to decide whether it is real or fake basing on that output image. We could have adapted the above histogram based approach, but we wanted to use global thresholding.
- We used about 300 real and fake images in order to determining this global threshold. This threshold is used differently. We separated the output image into three channels and we computed averages for each channel and then we took average of these averages and checked if that is above the global threshold or below to determine whether the image is real or fake. Following table summarizes the effect of choosing various thresholds over classifying the images as real or fake.

	Fake	Fake	Real	Real
Threshold	Correct	Wrong	Correct	Wrong
30	60	140	166	34
35	83	127	128	62
25	52	148	184	16
28	59	141	175	25
	104	346	912	138
25	93	357	968	82

- Finally, We decided an image to be fake if at least one of the algorithm says its fake.
- All our thresholds were such that, there will be high penalty if a real image is classified as fake. This constraint is due to the fact that we had 4 algorithms which could tell if an image is fake and on our decision to classify the image as fake even if one of them says that it is a fake.

Conclusion:

- It was a very interesting and thought provoking project as this field of forensics is completely new to both of us.
- Our main approach was to pick some idea and understand it and modify it basing on our intuition of what might work.
- We collaborated on most of the things. We divided reading papers as well. Initially we studied about 5-6 papers.
- Most of the DCT work was done by Shuyan and most of the histogram work was done by Aditya.
- Overall, we would say that 50% of the work was done by each of us.