IMAGE FORGERY DETECTION USING STATISTICAL ANALYSIS

Theja Voora, Thariq Shanavas, Varun Bandaru

IIT Bombay

Motivation

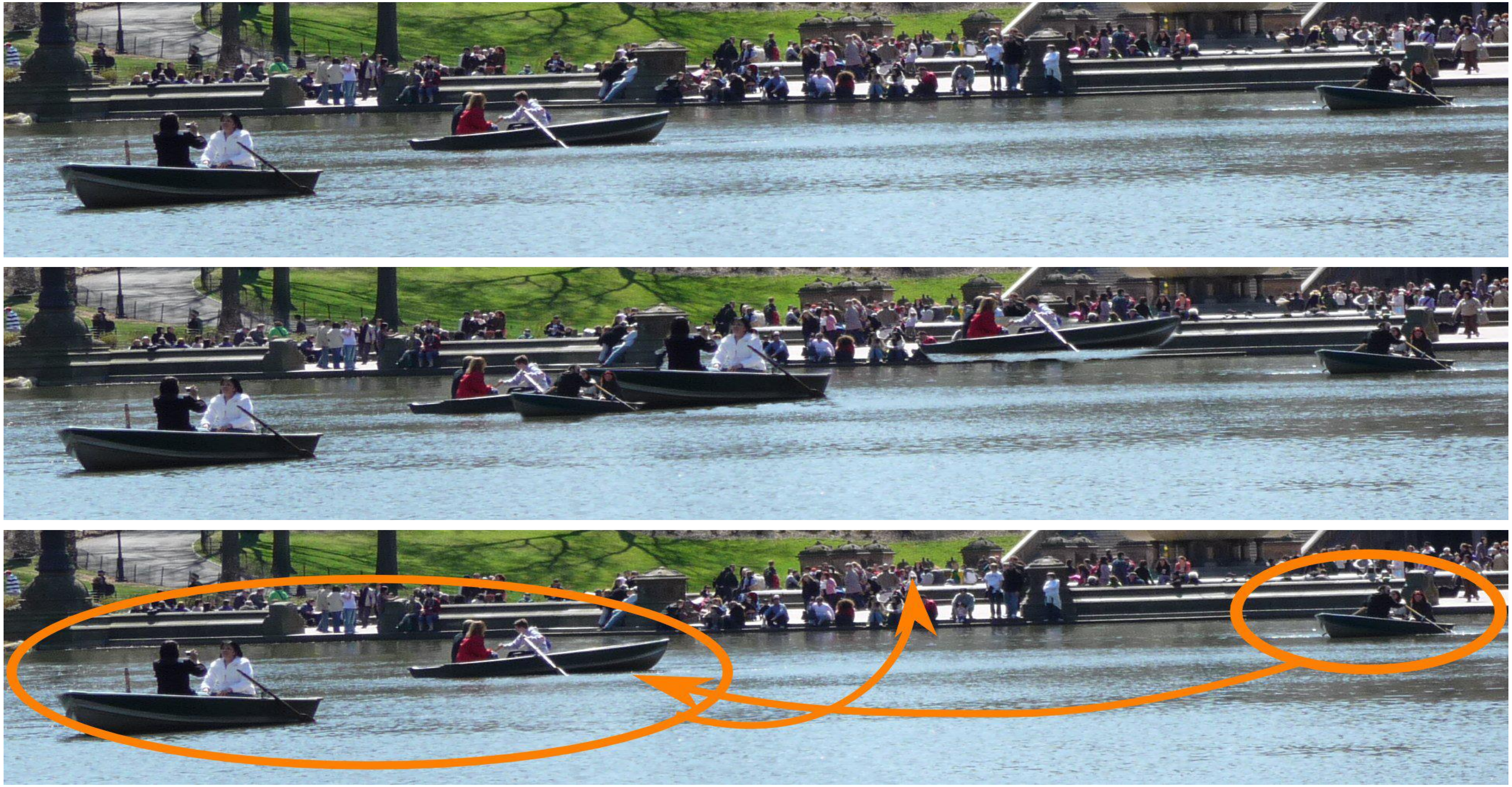
- We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery.
- In today’s world it is easy to develop the image by adding or removing some elements from the image.
- The trust we have had till now in believing what we see started eroding.
- Since extremely powerful technologies are now available to generate and process digital images, there is a concomitant need for developing techniques to distinguish the original images from the altered ones, the genuine ones from the doctored ones.

- The digital image forgery detection techniques are classified into active and passive approaches
- In active approach ,Digital watermarking has been proposed as a means by which an image can be authenticated
- The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach
- Passive techniques are used for detecting digital forgery based on Copy-Move and splicing
- In this work, we focus our interest on Copy-move forgery detection

Copy-Move Forgery

- In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object “disappear” from the image by covering it with a segment copied from another part of the image.
- Any Copy-Move forgery introduces a correlation between the original image segment and the pasted one. This correlation can be used as a basis for a successful detection of this type of forgery.

Other examples



Procedure

- The suspicious image is converted to greyscale to ease computation.
- Choose an optimum number of pixels for window dimension.
- Place the window at every possible position in the image.
- Extract the statistical features from the fourier transform of the extracted subcells and store in a matrix.

$$M = \frac{1}{p^2} \sum_{i=-(p-1)/2}^{(p-1)/2} \sum_{j=-(p-1)/2}^{(p-1)/2} I(x+i, y+j)$$

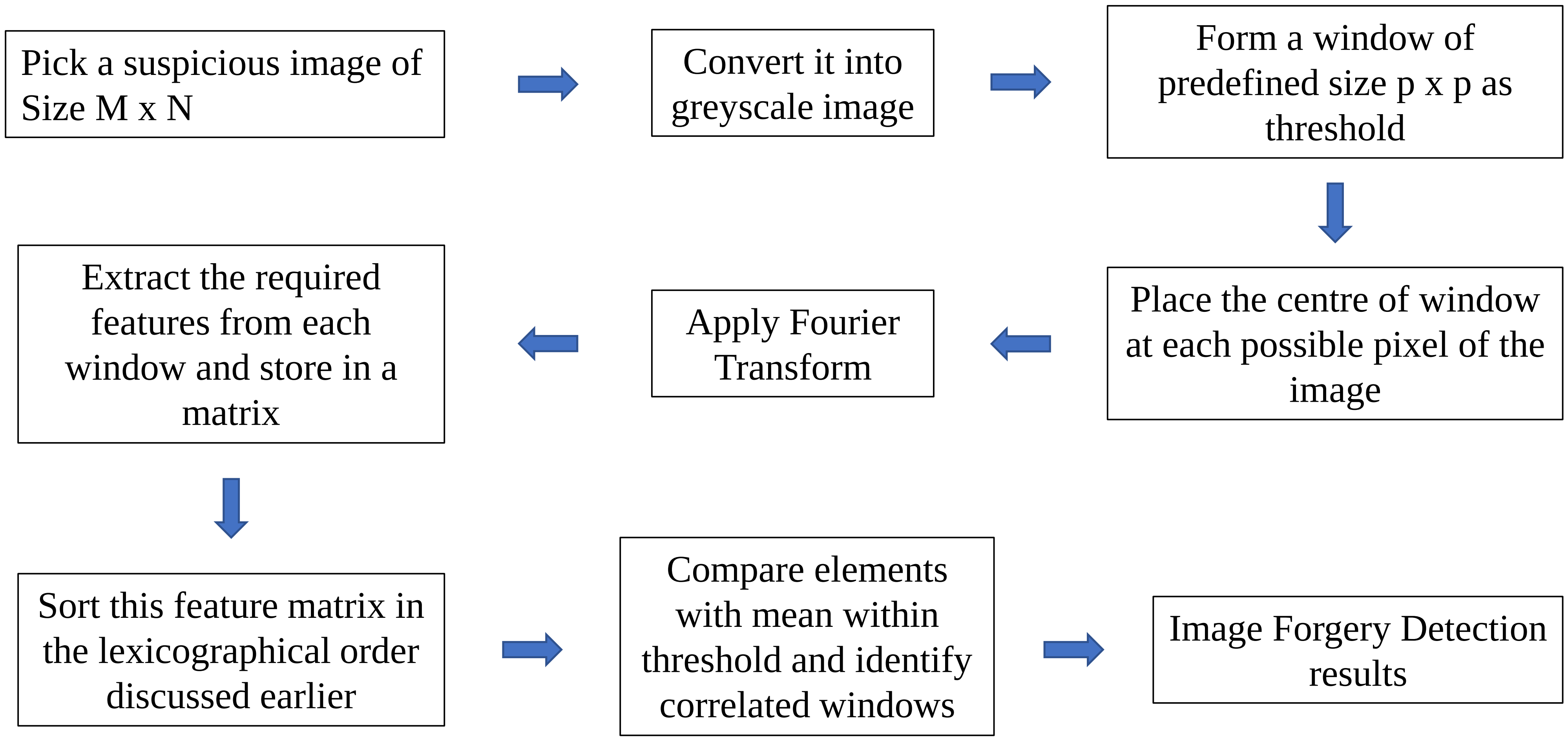
$$Var = \frac{1}{p^2} \sum_{i=-(p-1)/2}^{(p-1)/2} \sum_{j=-(p-1)/2}^{(p-1)/2} (I(x+i, y+j) - M)^2$$

$$Sk = \frac{1}{p^2} \sum_{i=-(p-1)/2}^{(p-1)/2} \sum_{j=-(p-1)/2}^{(p-1)/2} (I(x+i, y+j) - M)^3$$

$$Kr = \frac{1}{p^2} \sum_{i=-(p-1)/2}^{(p-1)/2} \sum_{j=-(p-1)/2}^{(p-1)/2} (I(x+i, y+j) - M)^4$$

- The rows of this Feature Matrix are rearranged in the increasing order of mean, and within cells of same mean, they are sorted in the order of variance, followed by skewness and kurtosis.
- Each element/row in the Feature Matrix is compared with all elements whose mean is within a pre-set threshold of the current element's mean.
- Within these, those elements which have variance, skewness and kurtosis each within a set of predetermined thresholds are marked as having strong correspondence.
- In the output figure, pixels corresponding to these elements are highlighted.

Algorithm



Pick a suspicious image of Size M x N
Convert it into greyscale image
Form a window of predefined size p x p as threshold
Place the centre of window at each possible pixel of the image
Apply Fourier Transform
Extract the required features from each window and store in a matrix
Sort this feature matrix in the lexicographical order discussed earlier
Compare elements with mean within threshold and identify correlated windows
Image Forgery Detection results

\\Code

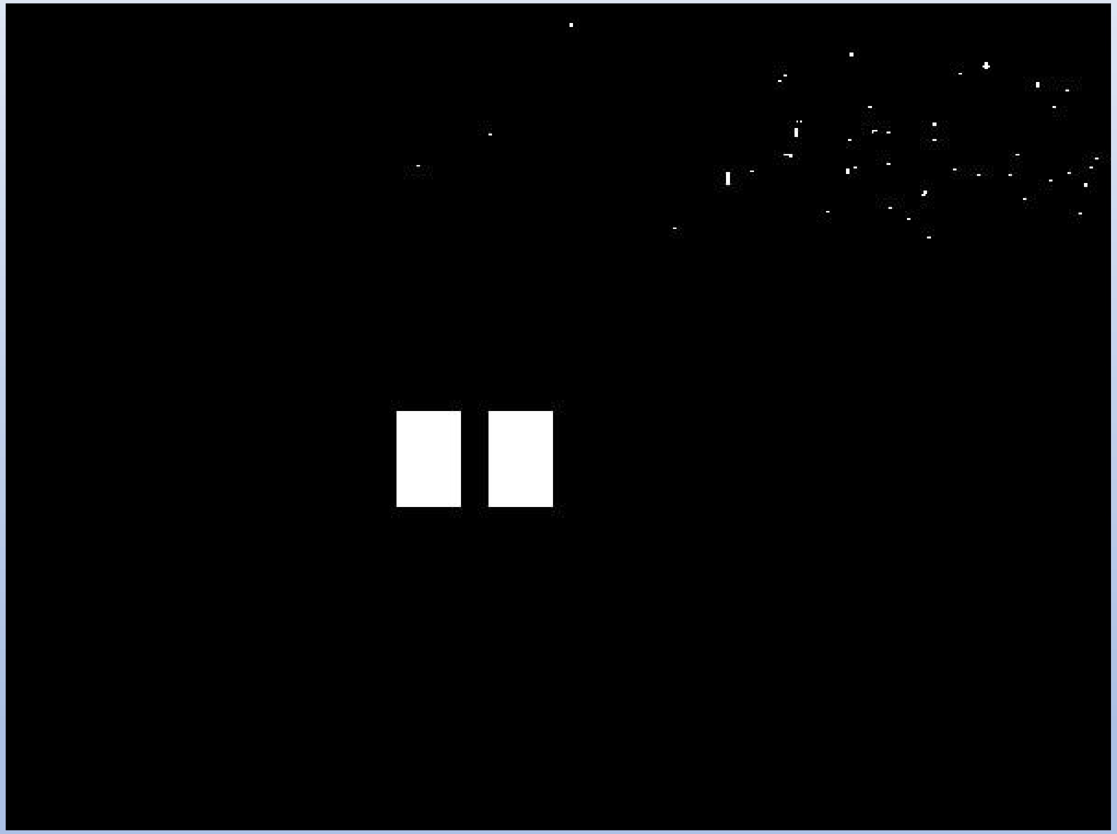
%We set the window threshold to 9 pixels.

%We used FFT to obtain the Fourier transform of the sub-images.

```
featurematrix2=sortrows(featurematrix2);
imout=zeros(len,wid);
l=numel(featurematrix);

for i=1:(numel(featurematrix)-1)
    temp=featurematrix2(i,:);
    j=0;
    while(1)
        j=j+1;

        if i+j>l
            break;
        end

        if abs(temp(1)-featurematrix2(i+j,1))<tm && abs(temp(2)-featurematrix2(i+j,2))<tv && abs(temp(3)-featurematrix2(i+j,3))<ts && abs(temp(4)-featurematrix2(i+j,4))<tk

                imout(temp(5),temp(6))=1;
                imout(featurematrix2(i+j,5),featurematrix2(i+j,6))=1;

        else
            break;
        end
    end
end

imshow(imout)
```

Results #1

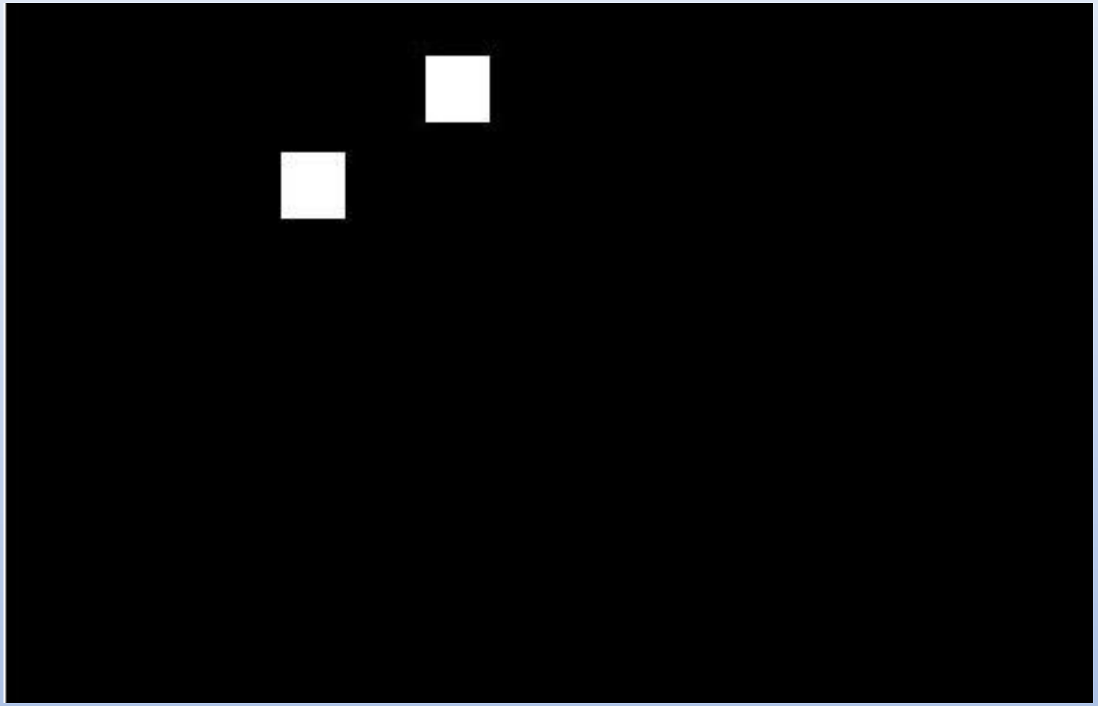
Suspicious image



Output

Original image

Results #1



Suspicious image

Output

Original image

References

[1] Sevinc Bayram, Ismail Avcibas, Bulent Sankur, Nasir D. Memon *Image manipulation detection with binary similarity measures*, Researchgate Jan 2005, 228937279

[2] Hany Farid *Image Forgery Detection*, IEEE Xplore, IEEE Signal Processing Magazine, March 2009, 10.1109/MSP.2008.931079

[3] Rajeev Kaushika, Rakesh Kumar Bajajb, Jimson Mathewc, *On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments*, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015.

thank you!