IMAGE FORGERY DETECTION USING CNN AND SVM

G.L. Bajaj Institute of Technology and Management Greater Noida

Shubham Jha(1901920130167)

Vinayak Basant (1901920130190)

SUPERVISED BY :

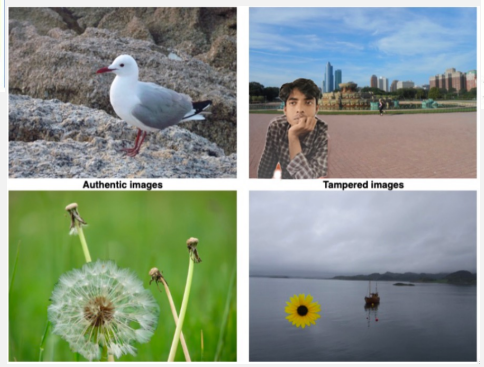
Ms. Pragati Gupta

INTRODUCTION

- The use of digital photography has increased over the past few years, a trend which opens the door for new and creative ways to forge images. Now-a-days several software are available that are used to manipulate image so that the image is look like as original. Images are used as authenticated proof for any crime and if these image does not remain genuine than it will create a problem.
- In particular, some of these images are tampered in such a way that it is impossible to detect even by humans. Over and above, social media platforms, such as Facebook, Instagram, and Twitter have turned the distribution of those images to the mass into a trivial task. While tampering processes, such as image contrast adjustment and skin smoothing, are harmless, there are others that could create serious business or political issues.
- Three of the most common manipulations in literature are:
    1. Copy-move: a specific region from the image is copy pasted within the same image.
    2. Splicing: a region from an authentic image is copied into a different image.
    3. Removal: an image region is removed oved and the removed part is then in-painted.

EXAMPLE OF FORGED IMAGE

(a) original image (b) forgery image



Example of Image Forgery showing forged and authentic image

PROBLEM STATEMENT

- The boom of digital images coupled with the development of approachable image manipulation software has made image tampering easier than ever. As a result, serious issues can emerge if the matter is not tackled accordingly.

- we develop a CNN network answer this question by comparing its performance on two separate datasets. Moreover, we measure the effect of a data augmentation technique and different hyperparameters on classification performance

- Our experiments show that dataset difficulty can significantly influence the performance obtained.

TECHNOLOGY USED

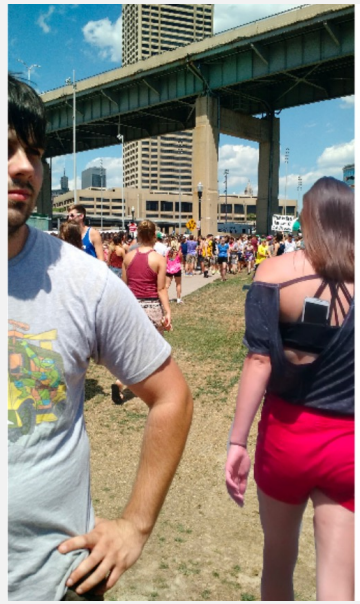
- **PYTHON**
  - PYtorch
  - scikit-learn
- **Convolutional neural network** For feature extraction
- **Support vector machine** For Classification

DATASETS

The **CASIA v2.0** dataset contains 12,622 images distributed 60-40 amongst authentic-tampered

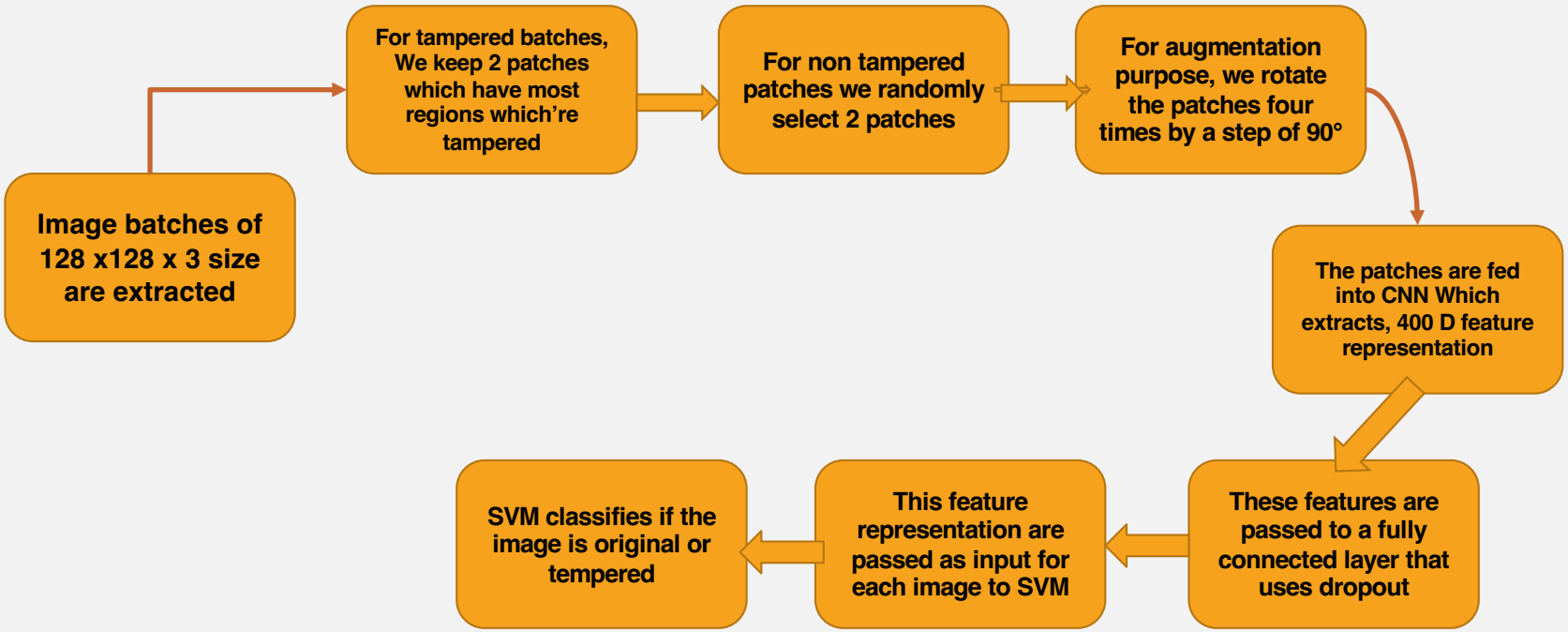
The **NC16** dataset contains 1,124 images with a 50-50 distribution

CASIA - Example of tampered image



NC16 - Example of tampered image

METHODOLOGY



USE CASES

- With over 4.5 billion active internet users, the amount of multimedia content being shared every day has surpassed everyone's imagination.
- Large-scale and pervading social media platforms, along with easily accessible smartphones, have given rise to huge visual data such as images, videos, etc.
- One of the perils accompanying this huge amount of data is manipulation and malicious intent to remove the authenticity of these media.
- The availability of various image-editing software and tools such as Photoshop, GIMP, etc., has made it possible to create forgeries with minimal effort.
- Today, it is quite easy to produce a manipulated media that looks indifferent to the human eyes.
- Various types of digital image forgeries have evolved, the major ones include copy-move, splicing, morphing, watermarking, etc.
- Copy-move manipulation means cutting and pasting a portion of the same image onto itself. Splicing involves cutting and pasting from different sources.

CONCLUSION

In this work we experimented with using a CNN in the image forgery detection task. More specifically, we used a CNN network to extract features from two datasets of varying difficulty, namely CASIA v2.0 and NC16. These results validate our intuition that the classification performance decreases the more challenging the samples are. our study has shown that image tampering can be detected with an accuracy of more than 84% even if done by professionals.

However, according to our findings the implemented architecture does not easily generalize to datasets with different underlying distributions. To conclude, while there is surely a lot of work still to be done in the image forgery detection domain, we believe that neural networks will be able to detect tampered images regardless of their difficulty..

REFERENCE

1. Weiqi Luo, Jiwu Huang, and Guoping Qiu. Robust detection of region-duplication forgery in digital age
2. Yuan Rao and JiangqunNi. A deep learning approach to detection of splicing and copy-move forgeries in images.
3. https://www.kaggle.com/datasets/sophatvathana/casia-dataset
4. https://ieeexplore.ieee.org/document/7823911
5. https://www.nist.gov/itl/iad/mig/open-media-forensics-challenge
6. https://pytorch.org/
7. https://www.youtube.com/watch?v=XE5TCGVMZO8&t=1s

THANK YOU