COPY-MOVE IMAGE FORGERY DETECTION

By
Sandipan Roy
Supervised by Prof. Kaushik Roy
Department of Computer Science
West Bengal State University

INTRODUCTION

What is Image Forgery?

Image forgery means manipulation of digital image to conceal meaningful information of the image.

What is Copy-Paste Forgery?

Copy-Paste forgery is a type of image forgery in which a portion of the digital image is copied from one place and pasted somewhere in a another image.

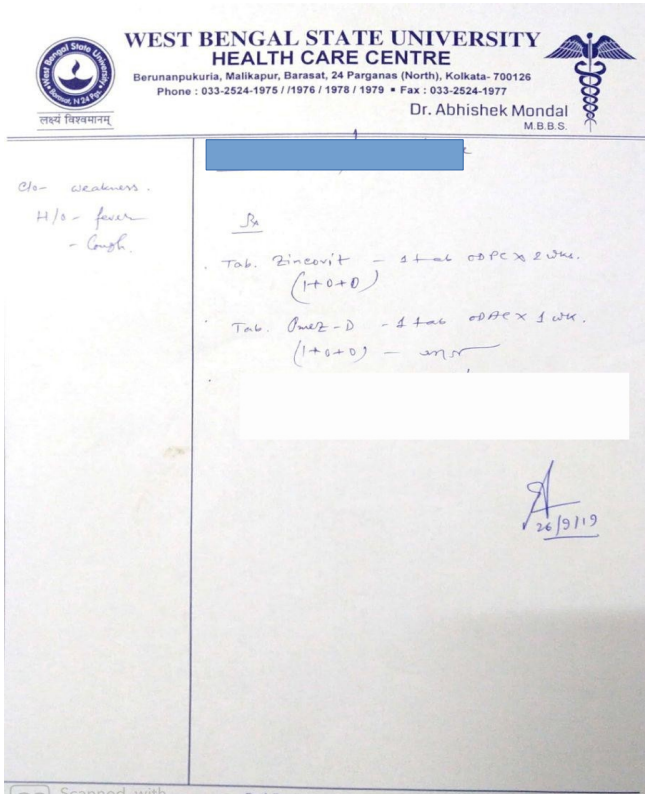
INTRODUCTION(Cont.)

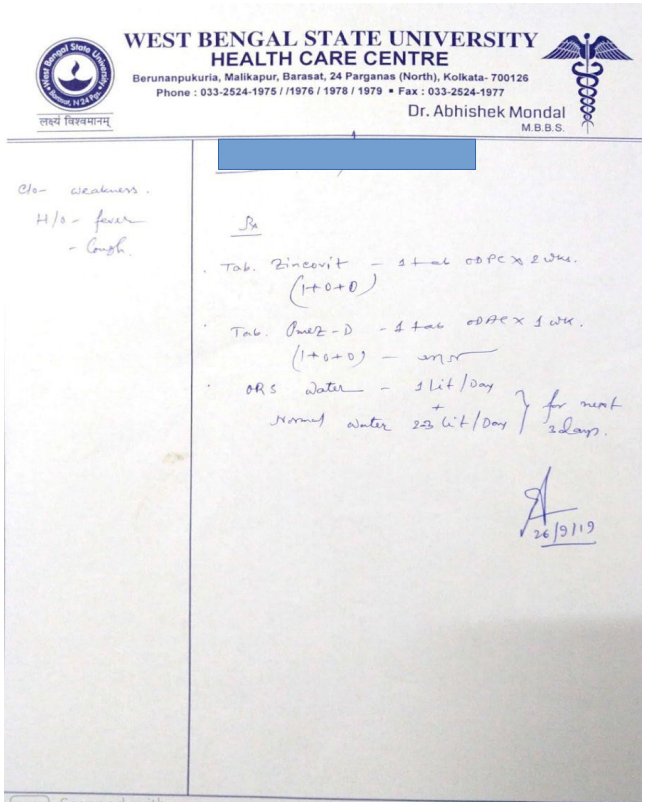
Why we need Copy-Paste Forgery Detection?

Image forgery detection is one of important activities of digital forensics. Forging an image has become very easy and visually confusing with the real one.One of the techniques most commonly used is the Copy-Paste forgery which proceeds by copying a part of an image and pasting it into the same image, in order to maliciously hide an object or a region.

Reason for Forgery Detection

- **Copyright Symbol**
- **Fake Face**
- **Fake Signature**
- **Fake News Image**
- **Fake Art**
- **Fake Medical Report**
- **Fake Documents**





Reason for Forgery Detection

I think this is Original.

My Mom think this is Original.

Forgery Detection Mechanisms

Can be Classified into Two Types

- Active Methods
- Passive Methods

Active Methods

1) **Hidden Information inside the Digital Image.**
2) **Done at the time of Data Acquisition or before disseminated to the public.**

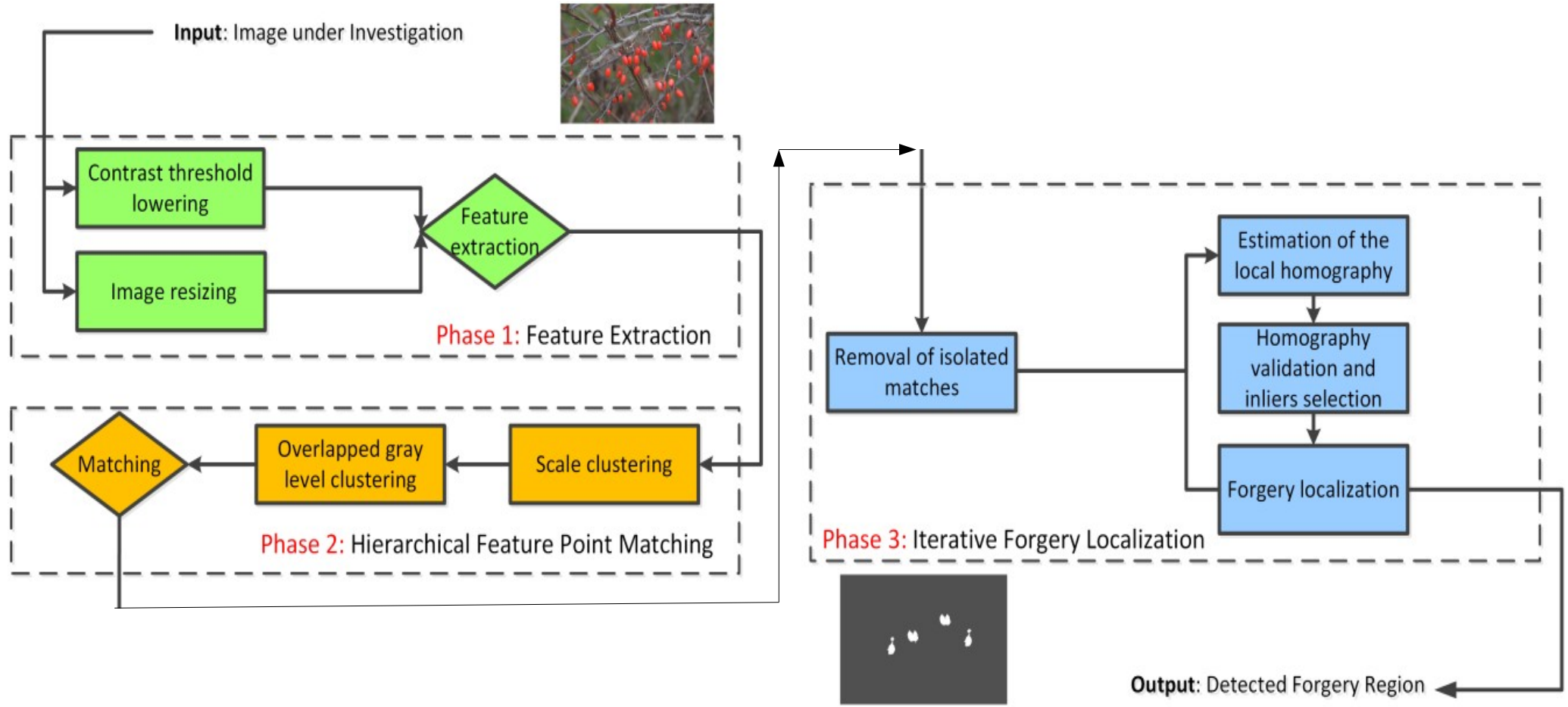
Passive Methods

1) **Use traces left by the processing steps in different phases of acquisition**
2) **They work by analyzing the binary information of digital image in order to detect forgery traces, if any.**

Now We can see some Passive Methods Proposed on Research Papers.

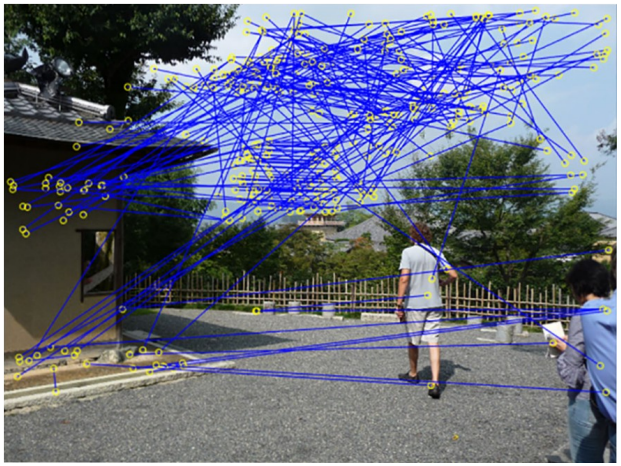
CASE STUDY 1

Hierarchical Feature Point Matching:



CASE STUDY 2

Adaptive Keypoints Extraction and Matching:



Input: The input image

Output: The image keypoints

STEP-1: Initialize parameters.

STEP-2: Partition the input image into sub-blocks.

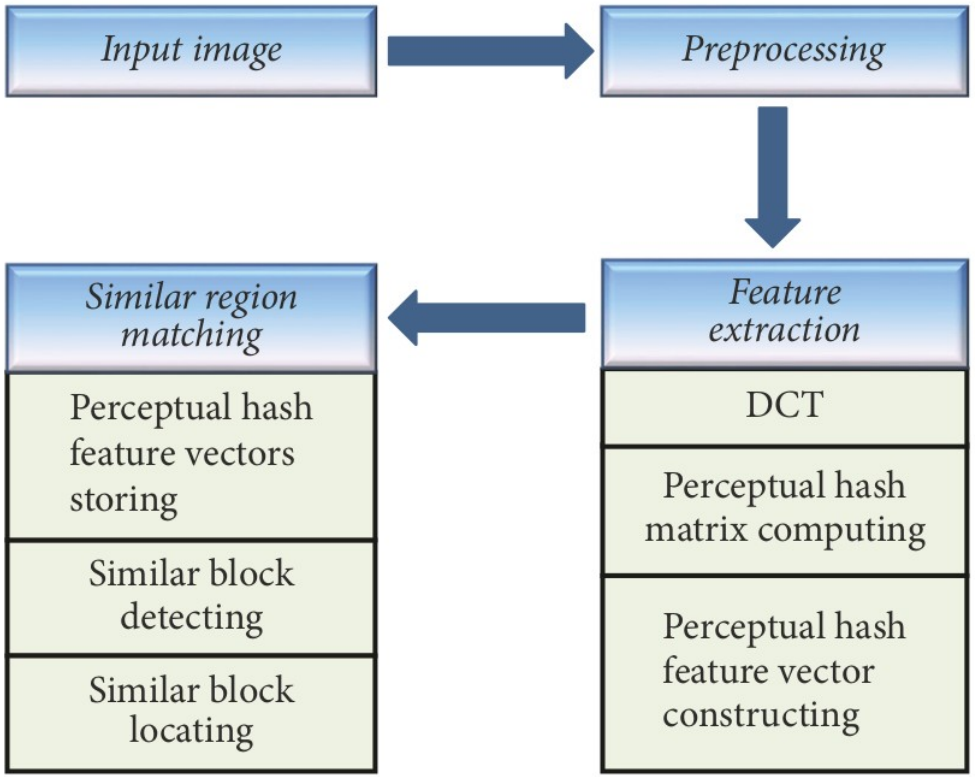
STEP-3: Detect SURF keypoints initially from the input image.

STEP-4: Detect SURF keypoints adaptively from the input image.

STEP-5: Homogenize processing on each sub-block.

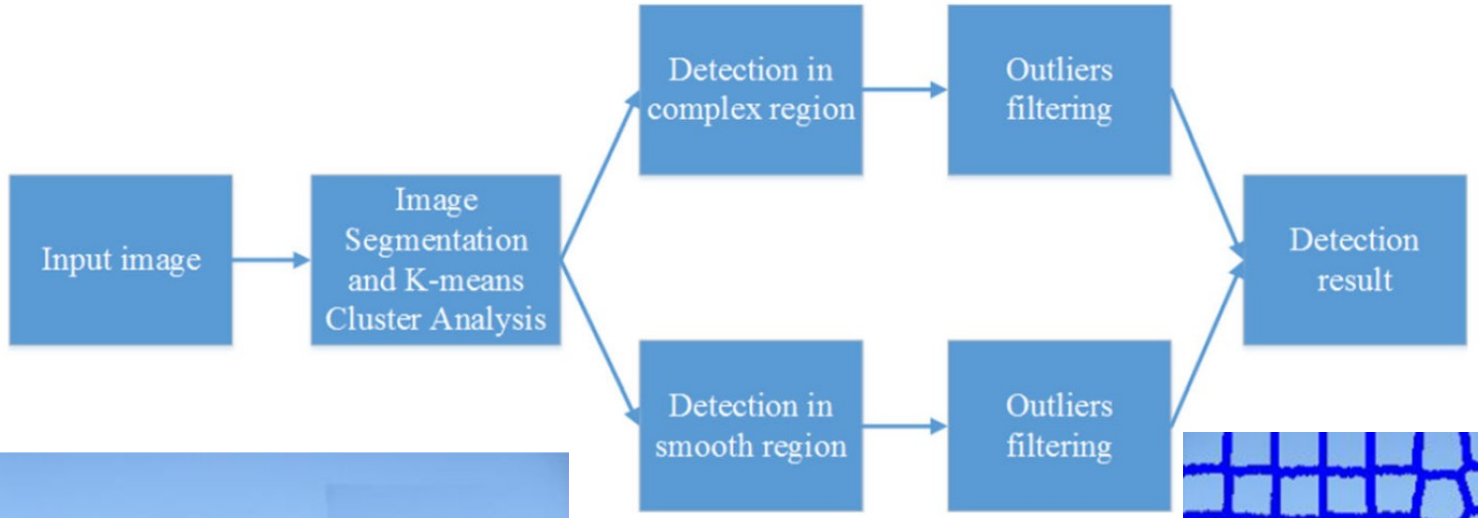
CASE STUDY 3

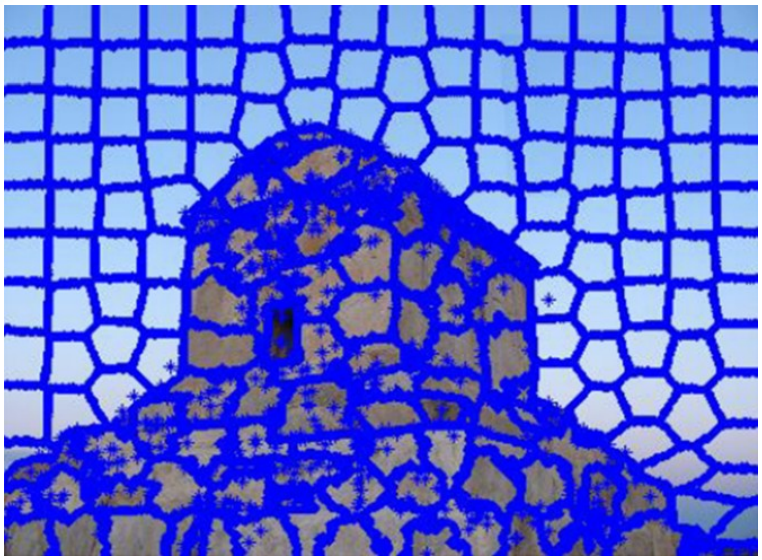
Perceptual Hashing-Based:



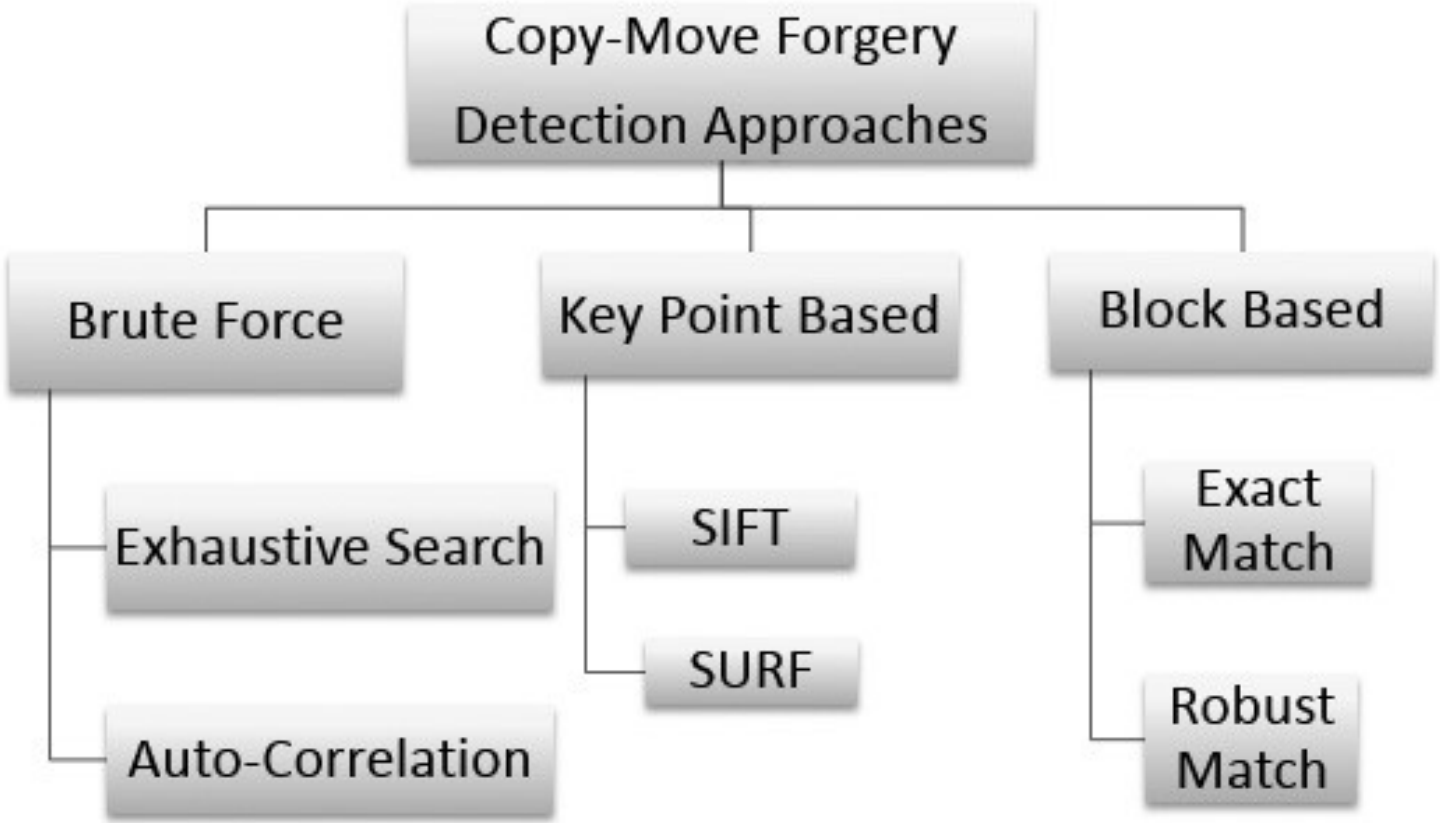
CASE STUDY 4

Pixel segmentation and K-means Clustering:





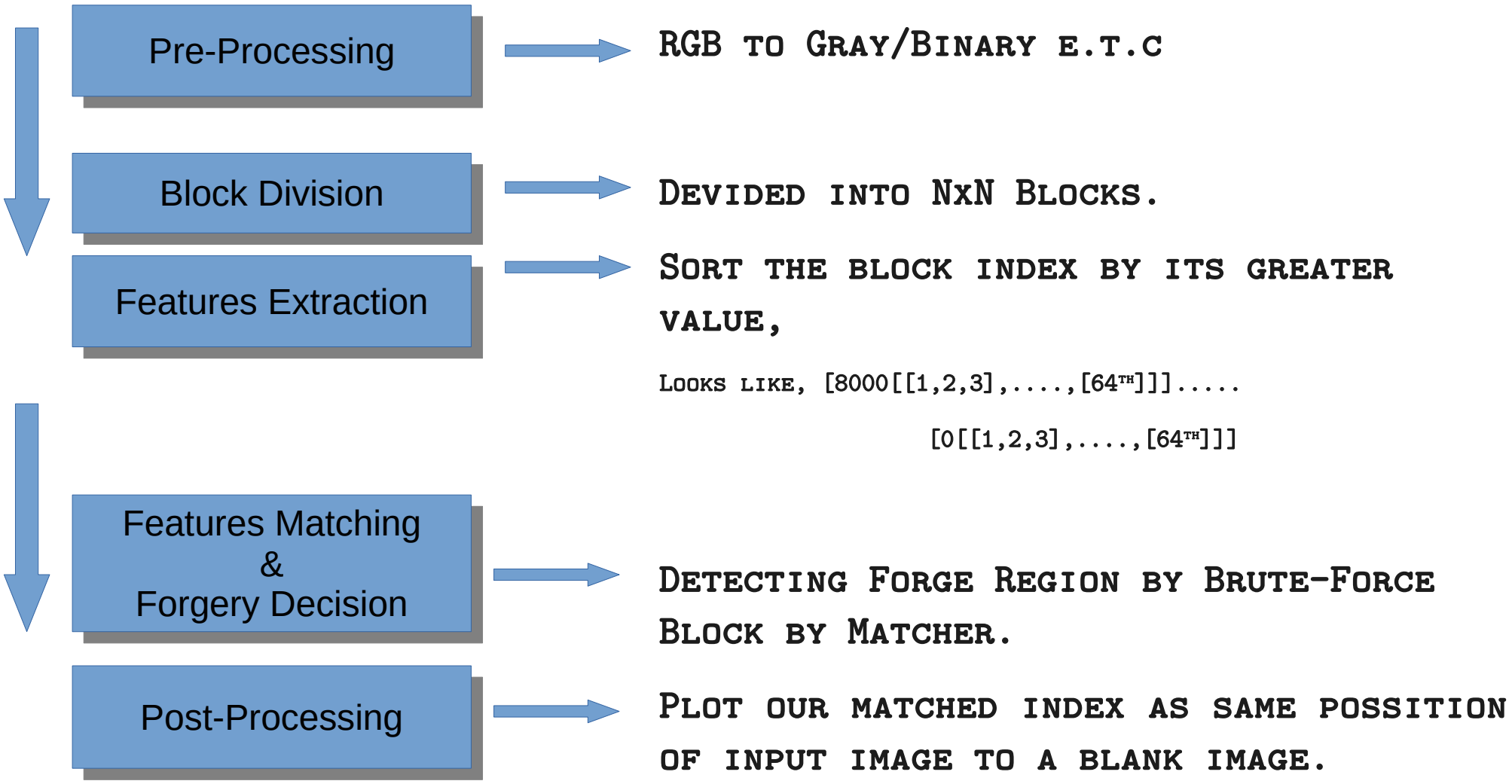
SUMMARY OF CASE STUDYS



PROBLEMS

- Lack of Labeled Samples and Certainty in Ground Truth
- Getting Bad Prediction
- Noise & False Positive
- Wrong Assumptions
- Imbalanced Data Sets

Our Approch


Pre-Processing
RGB to Gray/Binary e.t.c
Block Division
Devided into NxN Blocks.
Features Extraction
Sort the block index by its greater value,
Looks like, [8000[[1,2,3],....,[64TH]]].....
[0[[1,2,3],....,[64TH]]]
Features Matching & Forgery Decision
Detecting Forge Region by Brute-Force Block by Matcher.
Post-Processing
Plot our matched index as same possition of input image to a blank image.

Results & Evaluation

Dataset in Use:

1.CMFDdb_grip

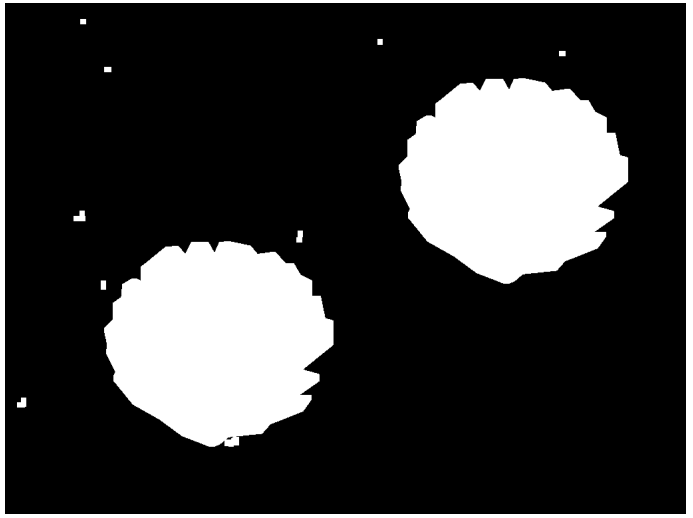
2.Image Manipulation Dataset

Used Evaluation Formula:

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

$$\text{Recall} = \frac{True\ Positive}{True\ Positive + False\ Negative}$$

$$F1 = 2 \times \frac{Precision * Recall}{Precision + Recall}$$



For this Example We Got,

Precision: 1 , Recall: 0.88732073753699 , F1 Score : 0.940296707272947

Examples

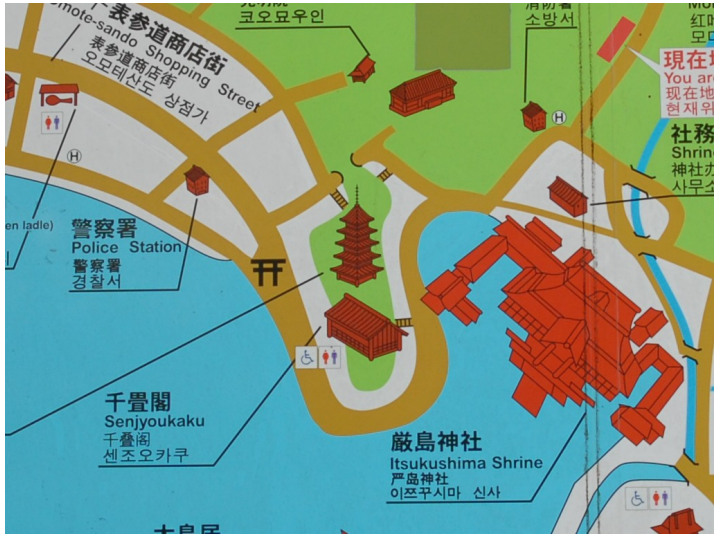
Original

Forged

Groud Truth

Our Result

Examples

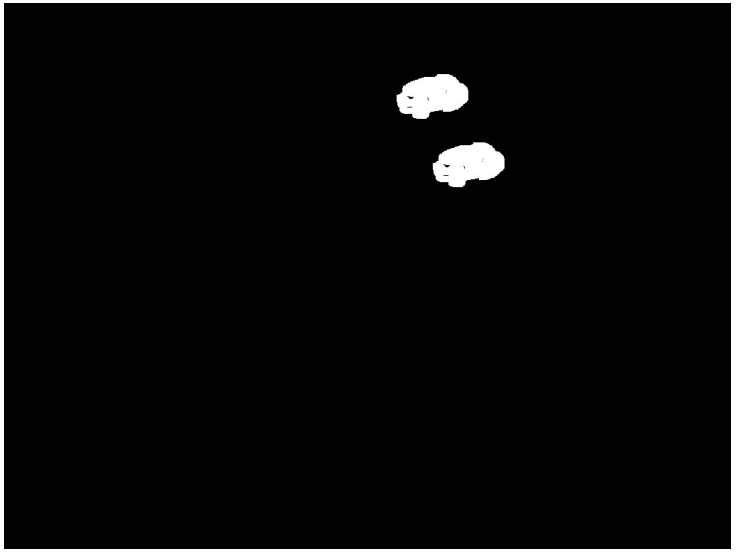


Original

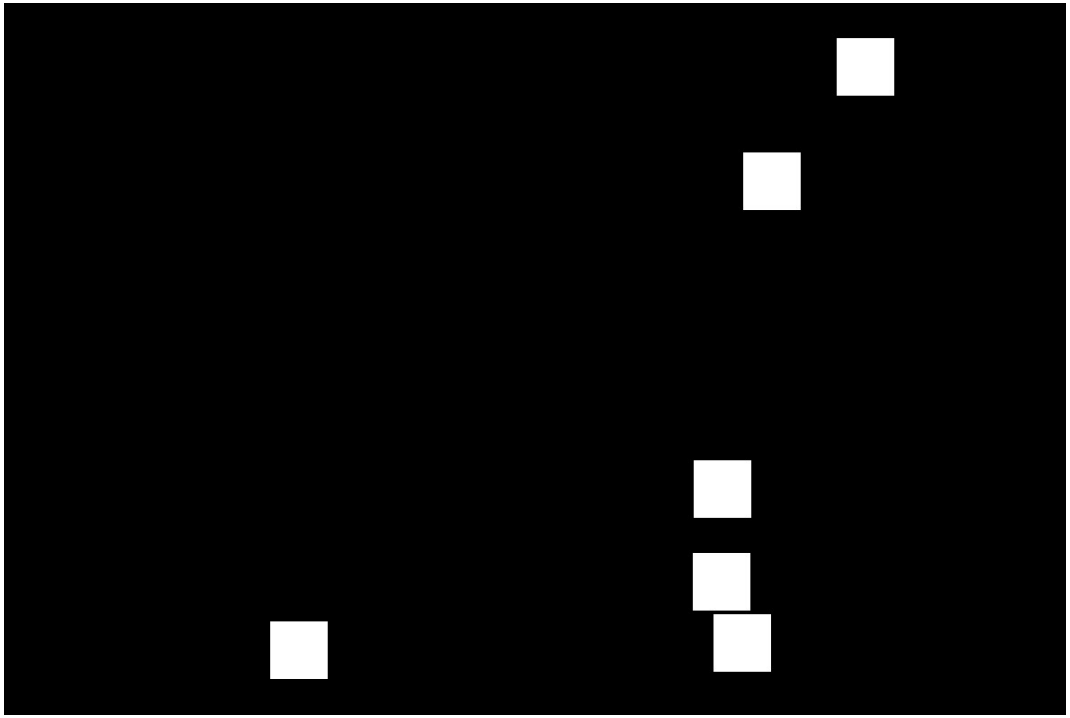
Forged

Groud Truth

Our Result

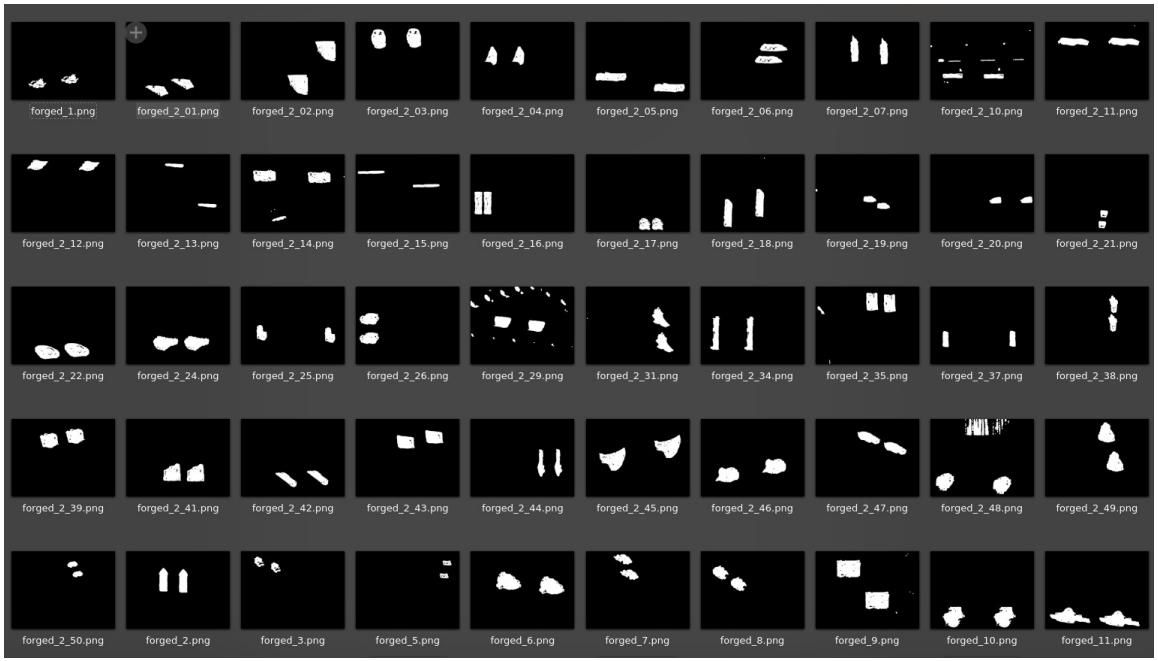


Examples of Multiple Forgery



Avarage Result

	Precision	Recall	f1 Score
Avarage	0.981701721	0.981570994	0.972077275



CONCLUSION

- In this work, we present a digital forensic technique for detection of image forgery.
- The proposed technique exploits the feature of double-compression, inherent in forged images.
- The proposed technique enables forgery detection to single copy-move forgery as well as multi copy-move forgery.

FUTURE WORK

- Automation of quality factor determination is a major future direction for this research.
- Reconstruction of forged image regions will also be investigated in the future.

REFERENCE

- H. Farid, “Exposing digital forgeries from JPEG ghosts,” IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.
- J. Wu, M.V. Kamath, S. Poehlman, "Detecting dierences between photographs and computer generated images", Proceedings of the 24th IASTED International conference on Signal Processing, Pattern Recognition, and Applications, pp 268273,2016.
- H.T. Sencar and N. Memon, (eds.), "Digital Image Forensics: There is More to a
- Picture than Meets the Eye", New York, NY, USA: Springer, 2013.
- G. Wallace, “The JPEG still picture compression standard", IEEE Transactions on Consumer Electronics, vol. 34, no. 4, pp. 30-44, 1991.
- D. Lowe, “Distinctive image features from scale-invariant key-points", International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.
- A. Srivastava, A.B. Lee, E.P. Simoncelli and S.C. Zhu, “On advances in statistical modeling of natural images", Journal of Mathematical Imaging, vol. 18, no. 1, pp.17-33, 2003.
- J. Redi, W. Taktak, and J.L. Dugelay, “Digital Image Forensics: A Booklet for Beginners", Multimedia Tools and Applications, vol. 51, no. 1, pp. 133 162, Jan. 2011.

THANK YOU

sandipan@parrotsec.org