COPY-MOVE IMAGE FORGERY DETECTION

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

Contents

INTRODUCTION

What is Image Forgery?

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

What is Copy-Move Forgery?

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

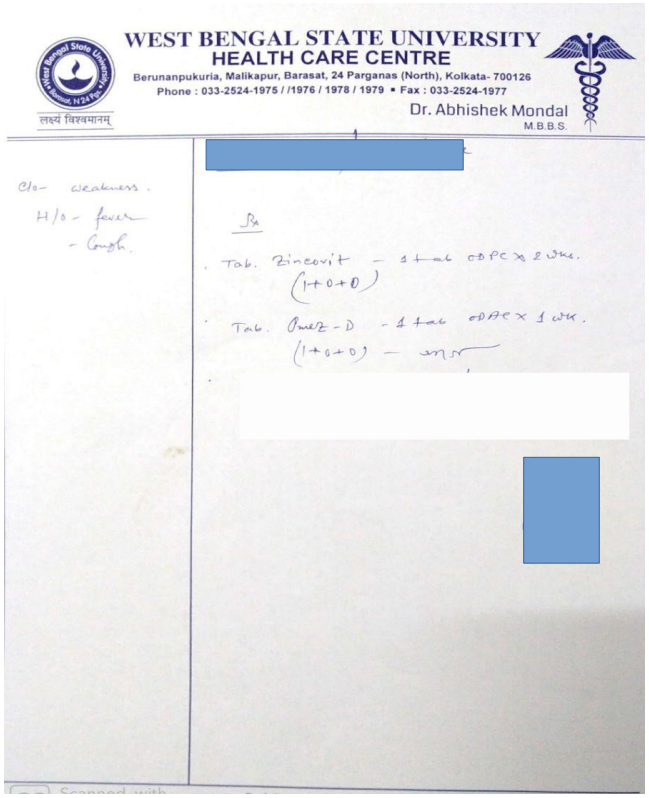
INTRODUCTION(CONT.)

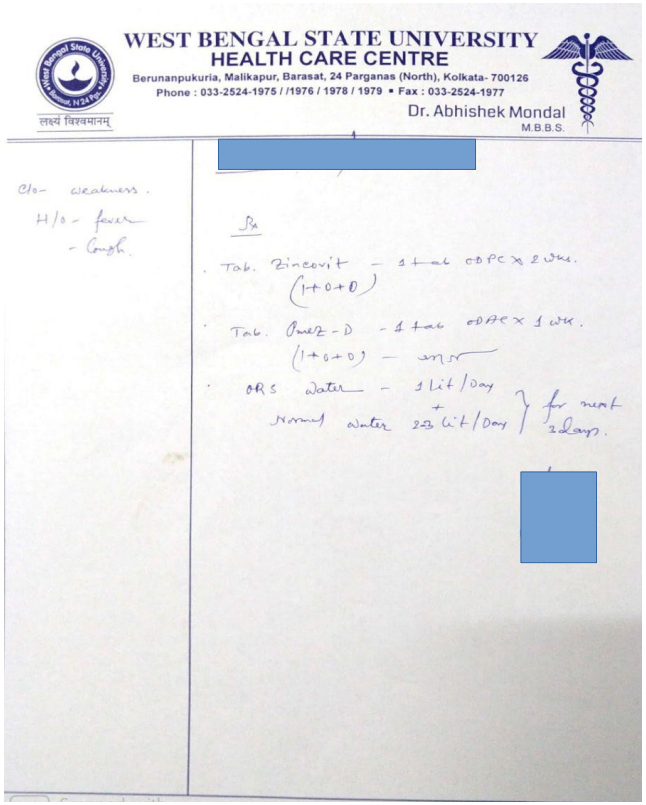
Why we need Copy-Paste Forgery Detection?

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-Move 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 Friends 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

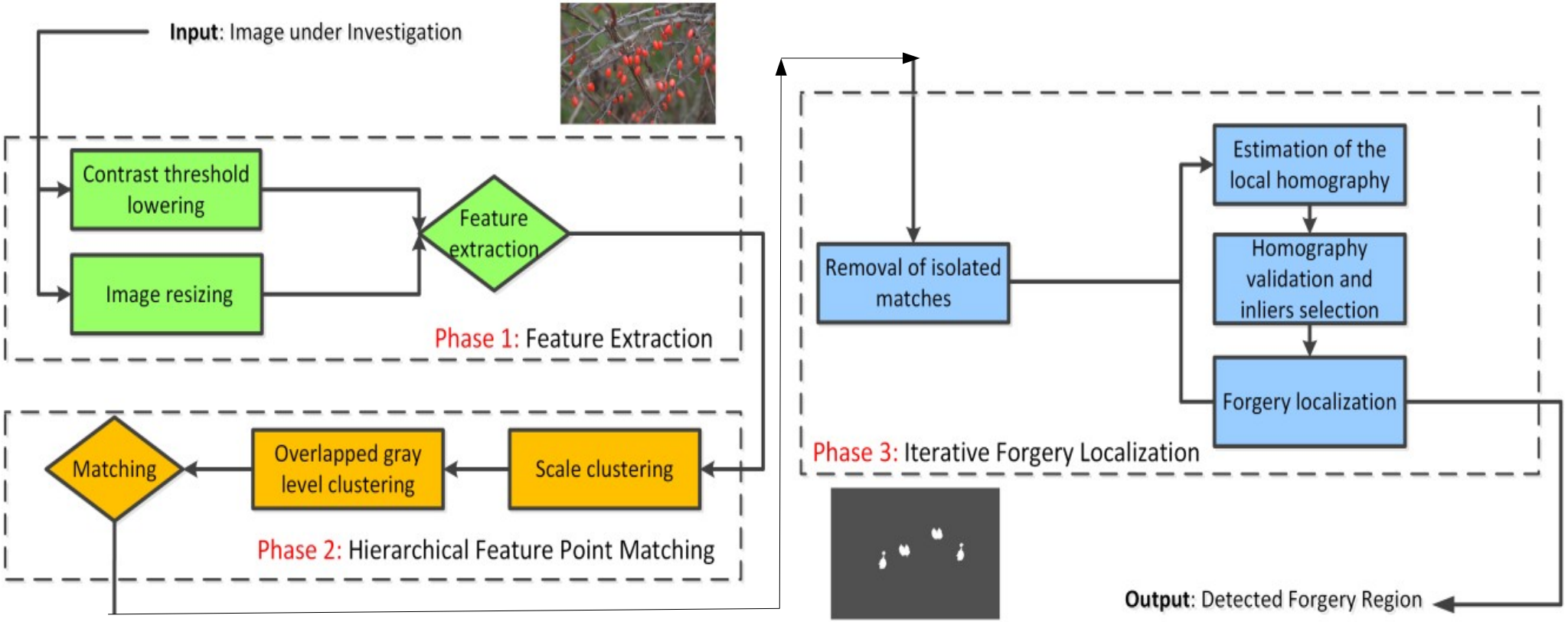
1) Use traces left by the processing steps in different phases of acquisition

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.

Literature Review 1

Hierarchical Feature Point Matching:

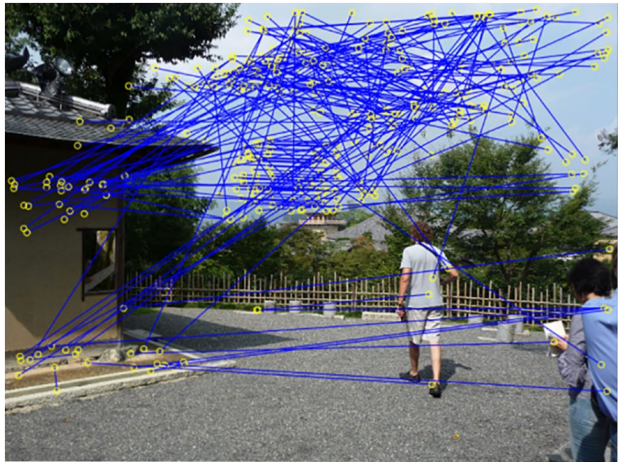


Limitations:

They got the forged points and very low false points but not getting the popper object.

Literature Review 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.

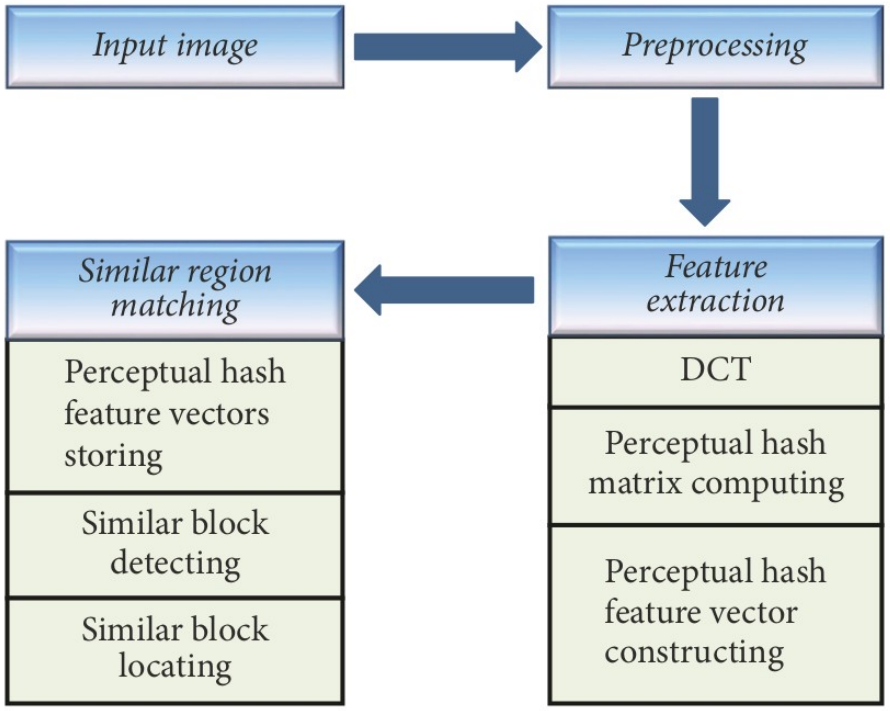
STEP-5: Homogenize processing on each sub-block.

Limitations:

With very high computational power they are not getting the popper object.

Literature Review 3

Perceptual Hashing-Based:

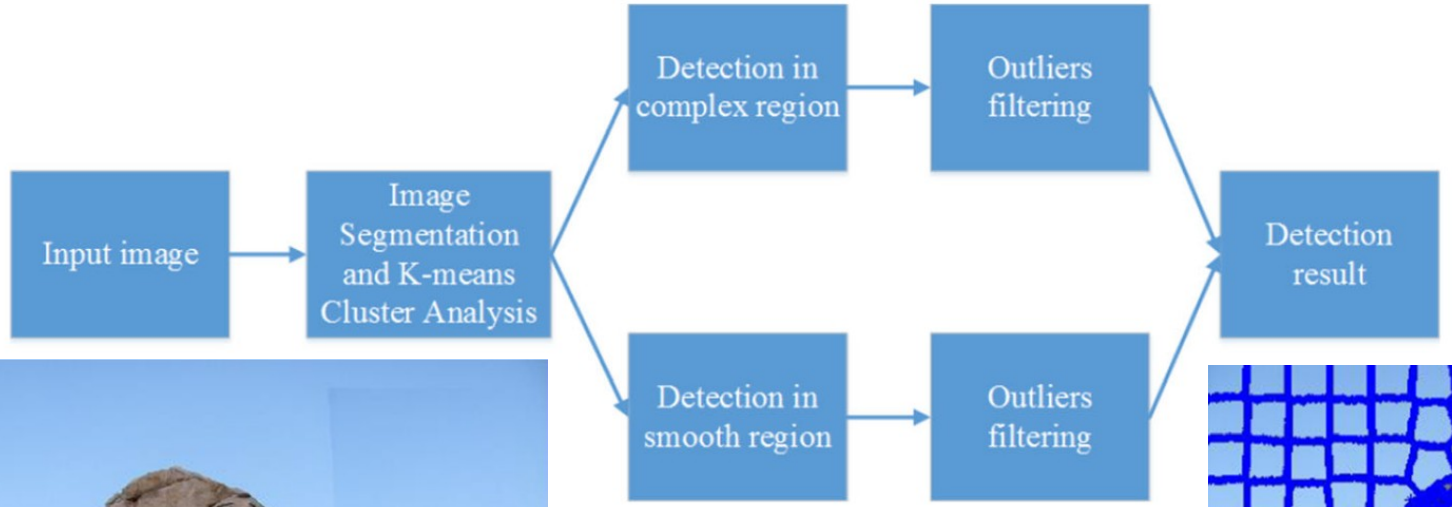


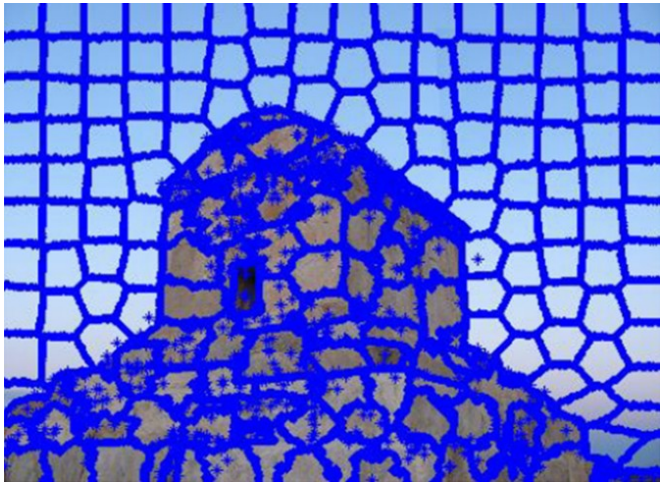
Limitations:

They get low accuracy in small copy-move regions.

Literature Review 4

Pixel segmentation and K-means Clustering:

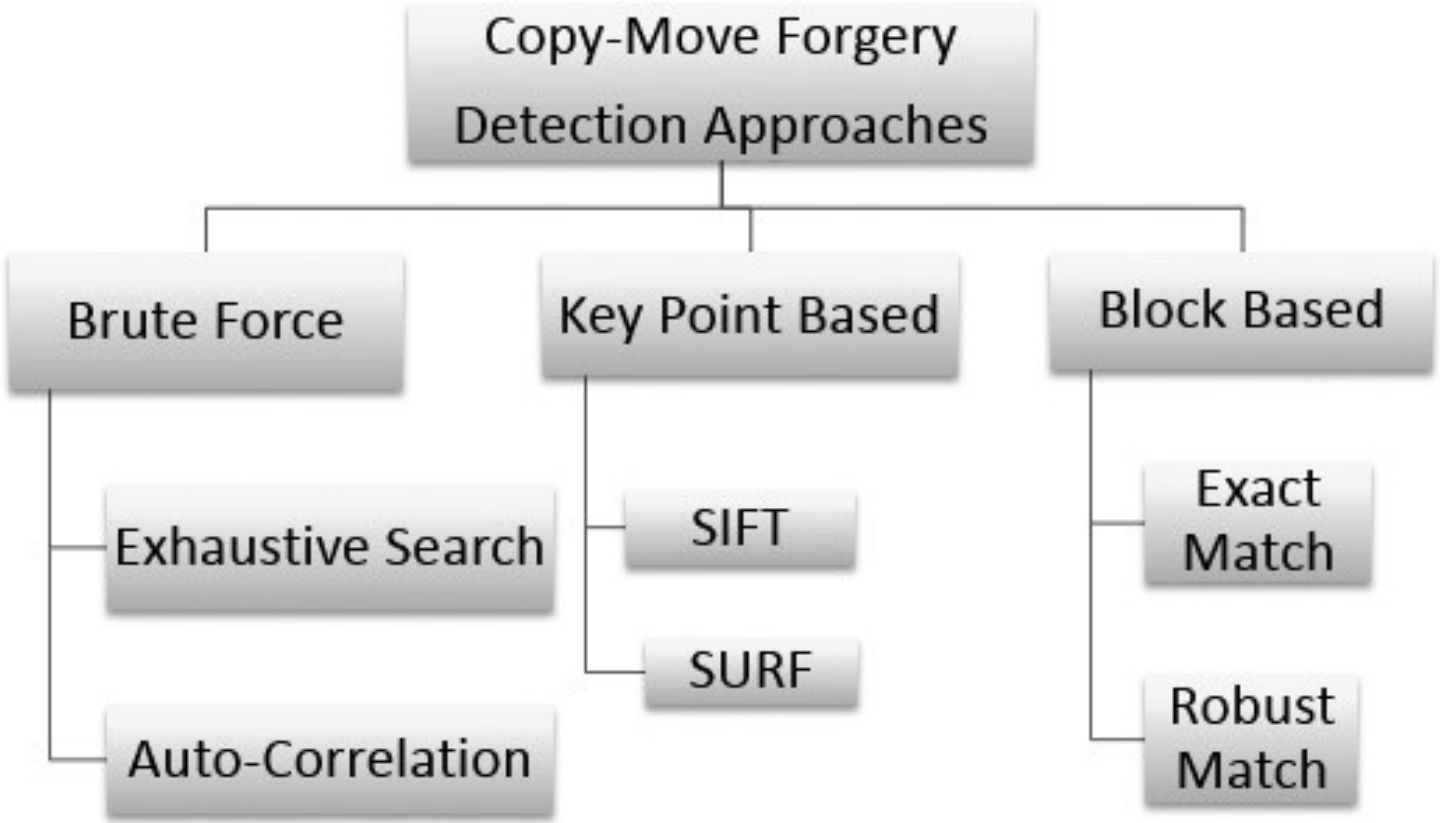




Limitations:

They can not detect which block or part is original and which is not.

SUMMARY OF LITERATURE REVIEW



PROBLEMS

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

Available Datasets

NO	Dataset	Forged Region	Image Size (in pixels)	No. of Images
1	CASIA 2.0	Single	384 × 256	700
2	CVIP Group	Single	1000 x 700	50
3	CoMoFoD_v2	Single	512 x 512	3000
4	CMFDdb-grip	Single	1080 x 786	80
5	Image Manipulation Dataset	Single	3264 × 2448	48
6	MICC-F220	Single	2048 x 1536	220
7	MICC-F8	Multi	2048 x 1536	8
8	COVERAGE	Single+Multi	Various Size	100

Available Dataset(Cont.)

Image Manipulation Dataset:

This dataset consist 48 forged images along with their original image and ground-truth, each image of size 3264 × 2448 pixels.

Available Dataset(Cont.)

CMFDdb-grip:

This dataset consist 80 forged images along with their original image and ground-truth, each image of size 1080 x 786 pixels.

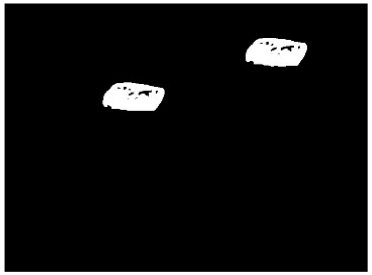
Proposed Approch

INPUT IMAGE

Pre-Processing

Block Division

Features Extraction



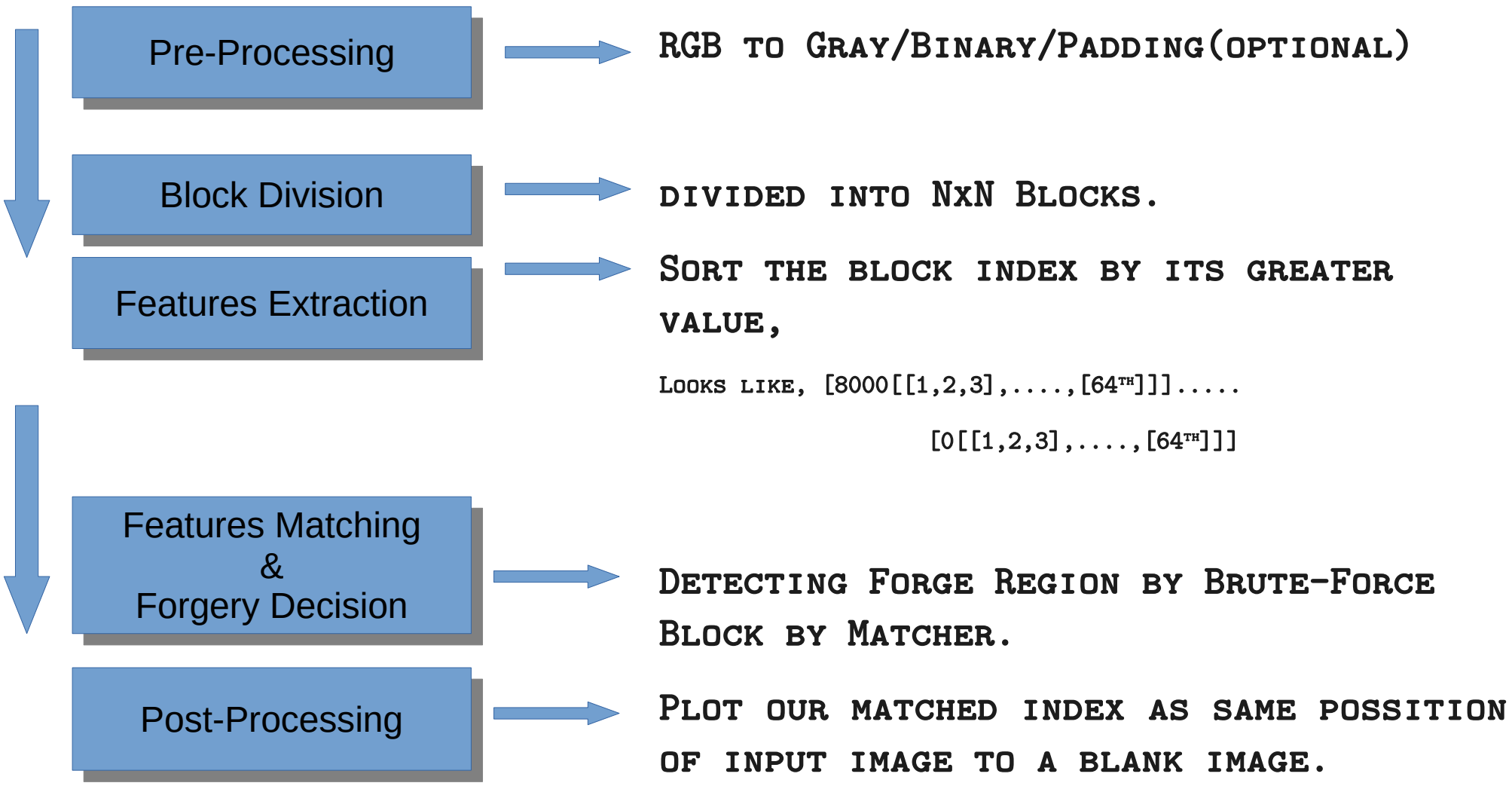
Features Matching

Forgery Decision

Post-Processing

OUTPUT IMAGE

Proposed Approch(Cont.)



Results & Evaluation

Dataset in Use:

1.CMFDdb_grip

2.Image Manipulation Dataset

3.CVIP Group

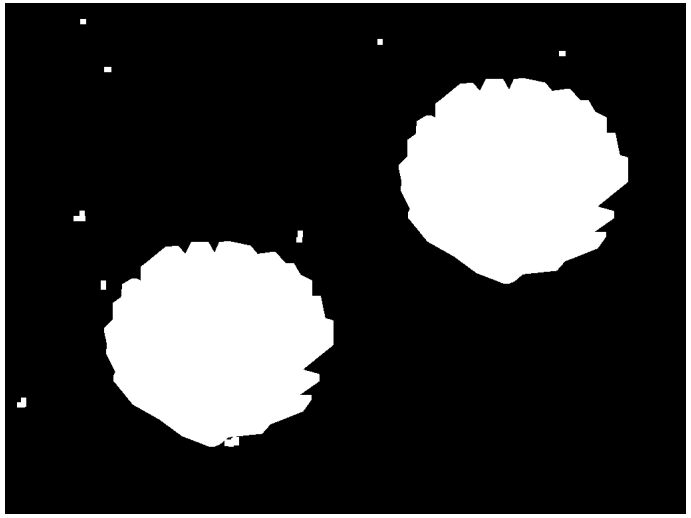
4.MICC-F8

Used Evaluation Formula:

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

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

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



Examples

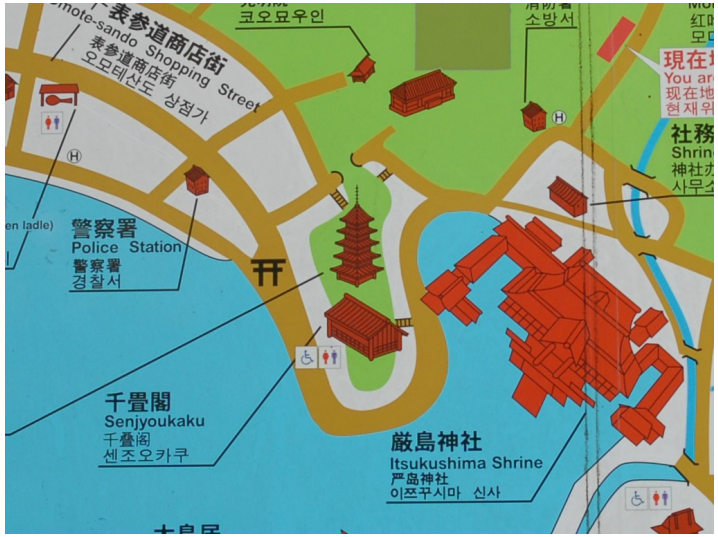
Original

Forged

Groud Truth

Our Result

Examples (Cont.)

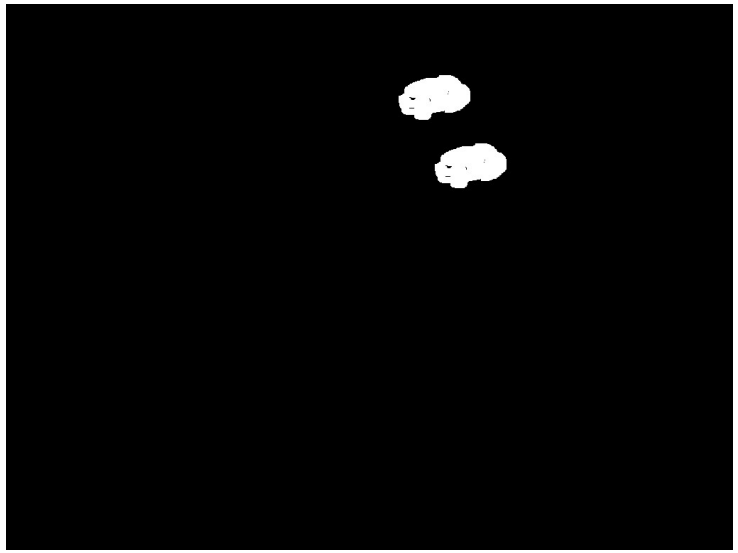


Original

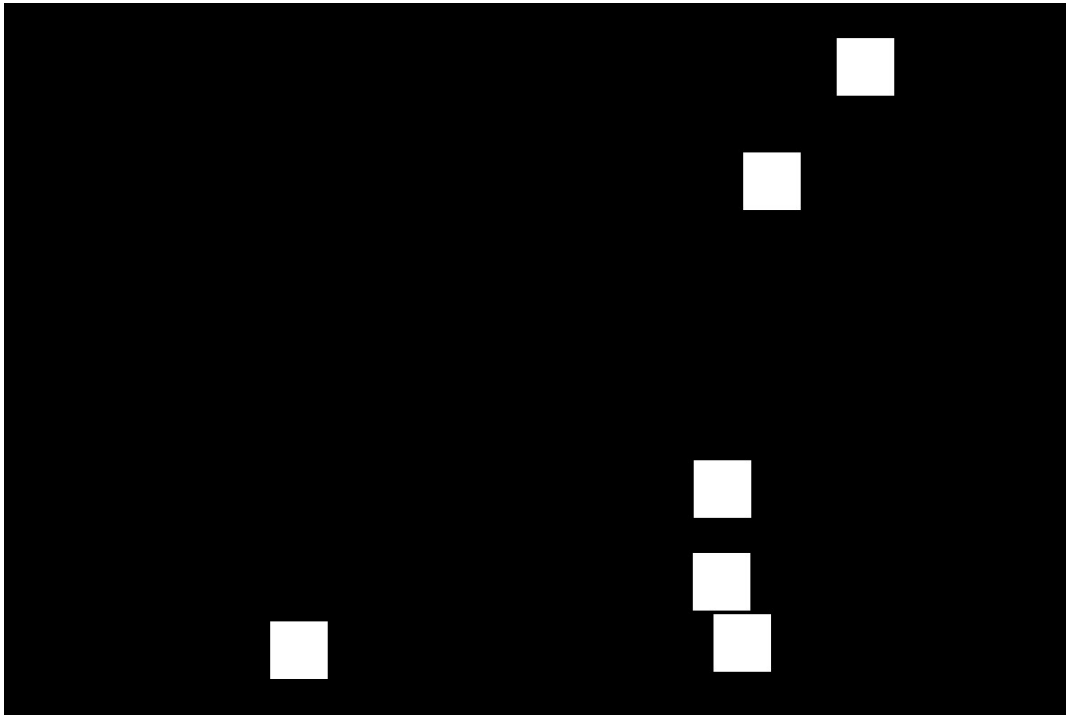
Forged

Groud Truth

Our Result



Examples of Multiple Forgery



Result

Our Result

Dataset	Precision	Recall	f1 Score
CMFDdb_grip	98.17%	98.15%	97.62%
CVIP Group	98.68%	98.25%	98.54%
Image Manipulation Dataset	97.85%	97.64%	97.03%
MICC-F8 Multi	98.84%	98.54%	97.93%

Comparison with Reviewed Literature

NO.	Dataset	Precision	Recall	f1 Score
Literature 2	CMFDdb_grip	95.9%	94.2%	96.05%
Literature 3	CVIP Group	87.68%	87.25%	87.54%

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