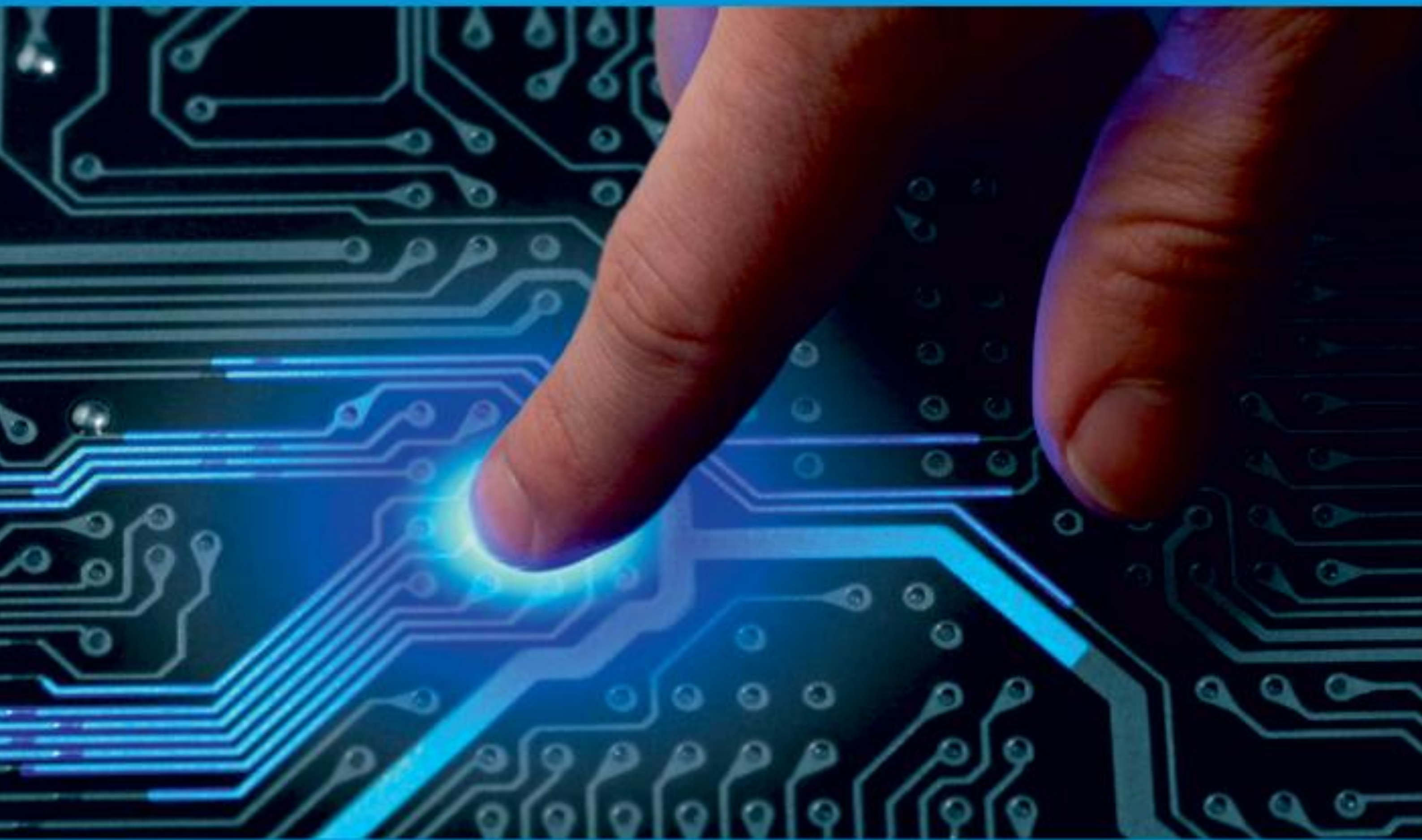
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

Pixel-Based Copy-Move Image Forgery Detection Analysis

B. Manikanth, Md. Rubeena Taj, K. Keerthi, M. Sandhya, M. Manasa

Assistant Professor, Department of ECE, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

UG Student, Department of ECE, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

UG Student, Department of ECE, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

UG Student, Department of ECE, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

UG Student, Department of ECE, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

ABSTRACT: Image forgery detection is widely used in various fields like crime investigations,medical fields etc.Copy-Move and splicing forgery is one of the major tampering techniques which is vastly used for copying a part of image and paste it in the place of original image.To perform tampering in this forgery is difficult because there will be too many similarities between original and forged one and in this we proposed an algorithm named Robust which gives accurate and efficient result for the forgery detection.This method works by applying principal component analysis for dimensionality reduction. This is a robust to minor variations in the image due to overlapping. Lexicographically sorting is used for detecting the forged region of all image blocks.We choose to implement an effectivealgorithm which classifies the given image asforged or not and this technique shows the efficiency on credible forgeries and quantity its robustness and sensitivity to additive noise and lossy JPEG compression.

KEYWORDS: Lexicographical sorting, Dimensionality reduction.

I.INTRODUCTION

The advancement in imaging technology has made easy to manipulate digital image. Digital cameras and computers of digital image forgery is potentially very serious. Digital image forgery has already appeared in manyforms. One of the specific forgery type is copy-move that can be done very easily by usingPhotoshop.This type usually aims to cover an unwanted scene in image ,by copying another scene from the same image i.e, a textured region and pasting it onto the unwanted region. The aim of copy-move forgery detection technique is used for detecting the duplicatedregions. However,these regions might not be the exact duplicates, since the tamperer could use tools to add noise to the resulting image.In real life copy-move is very likely for copying and moving a part to be subjected to slight rotation or blurring for better blending purposes .Hence, Copy-move forgery detection technique is robust to such operations as well.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

Fig1. Original image , tampered image

II.EXISTING METHODS

As various techniques are available to tamper images so there is availabilityof such techniques that can contribute in maintaining authenticityof images. Broadly Image forgery detection techniques can be categorized into two categories: Active and Passive.

1. Active: Digital signatures and watermarking are active techniques of forgery detection. These techniques are costly because only expensive cameras have such features to embed certain details in original image for identifying tampering.

2. Passive: Thisis also called blind image forgery technique.These techniques do not demand any prior information about original image. There are six types of techniques in passive approach, they are pixel-based, geometric-based, source camera identification-based, camera-based techniques, physics-based and format-based.In this technique we mainly focused on pixel-based copy-move image forgery detection.

III.PROPOSED METHOD

1. PIXEL-BASED TECHNIQUE

These are the most common techniques based on statistical changes happened at pixel-level due to forgery. These techniques also create a mutuality due to tampering in spatial or transformed domain. These methods are widely used for finding forgery of images. Usually, forgery detection is based on pixelvalues. These methods are focused on detecting the manipulation in the image on the basis of pixelcharacters. Usual pixel-based forgery detection techniques are image splicing, Resampling, Copy-move. In this we are focusing on copy-move forgery detection technique.

1.1COPY-MOVE FORGERY DETECTION

In copy-move forgery one segment of image is copied and pasted in the other part of same image. Mainintension of copy-move forgery is to hide some visual clues or replicating the things in image to mislead peoples. The reason behind the copy-move forgery is simple. In this we used principal component analysis methodology for forgery detection.

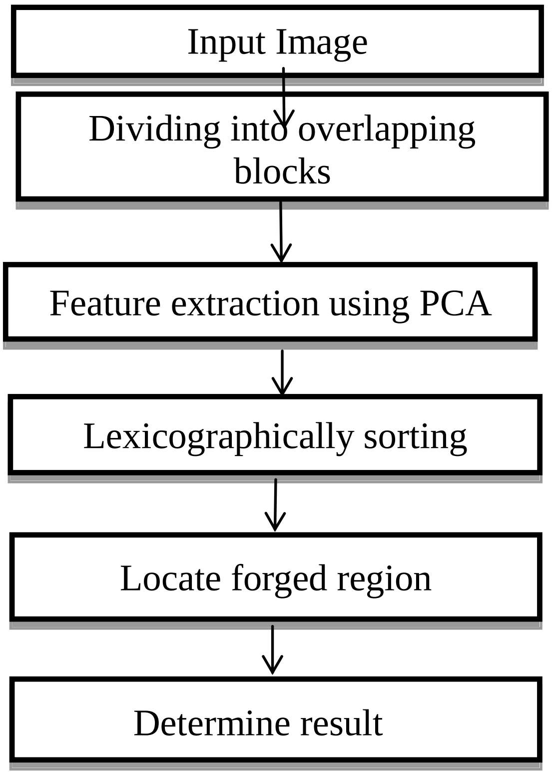
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

1.1.1 Methodology

Principal component analysis is a linear dimensionality reduction technique that can be utilized for extracting information from a high-dimensional space by bulging it into a low-dimensional sub-space. It tries to hold the essential parts that have more differencefrom the data and remove the non-essential parts with less variations.



Working

- The input tampered image is split into overlapping blocks of bxb pixels. Assuming that the image is an MxN color image, then there are (M-b+1)x(N-b+1) blocks and seven different characteristics are calculated.
- Using PCA the dimensionality reduction of all image blocks are reduced and search for the similar block pairs.
- Now, find the matched block pairs in the similar block pairs. Not all the similar block pairs are equally likely to come from two duplicated regions.
- Binary image is produced by setting tampered part to a white value and the rest set to a black value.
- Both the original and the tampered parts are detected by creating a line edge.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

IV.RESULTS

Here are some of the inputs of images that we have tested and obtained output

For Normal image:


Fig3.Original image


Fig4.tampered result

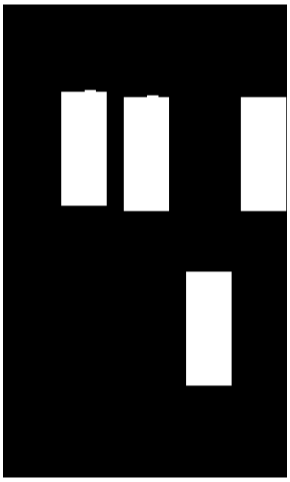


Fig5.binary output

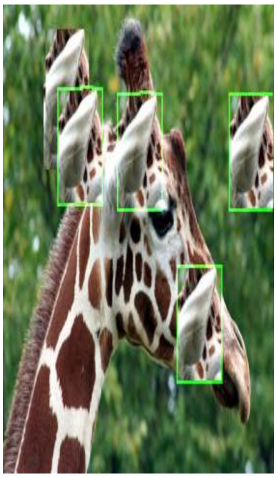


Fig6.detected result

blur images:

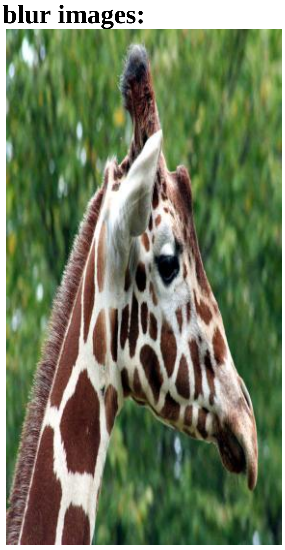


Fig 7.original image


Fig8.Blur image

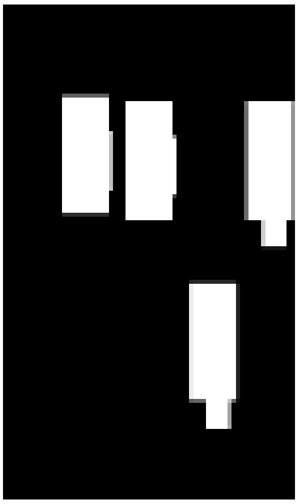


Fig9. Binary Image


Fig10.Detected output

For Rotation:


Fig11.Original


Fig12.Tampered result

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

Fig13. 90degreesRight

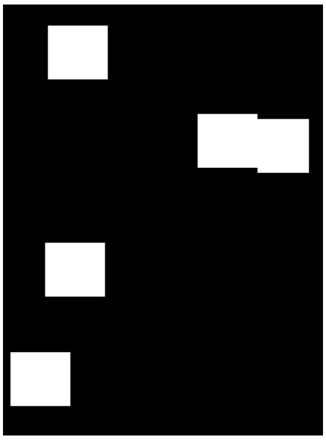


Fig14.Binary output

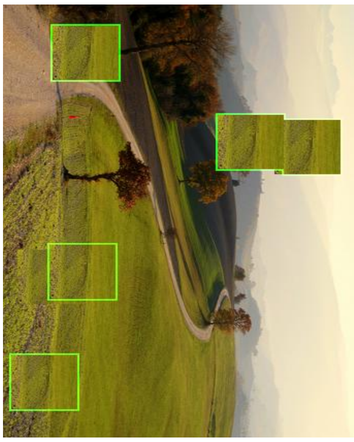


Fig15.Detected Output

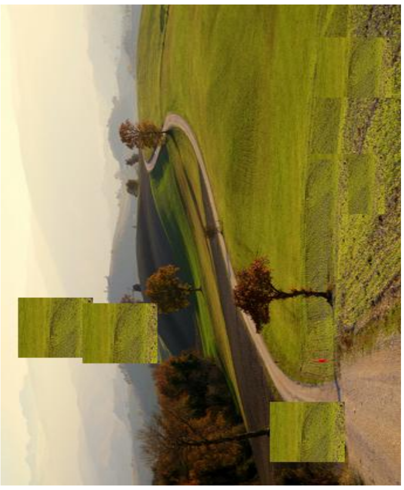


Fig16.Rotate 90degreesLeft

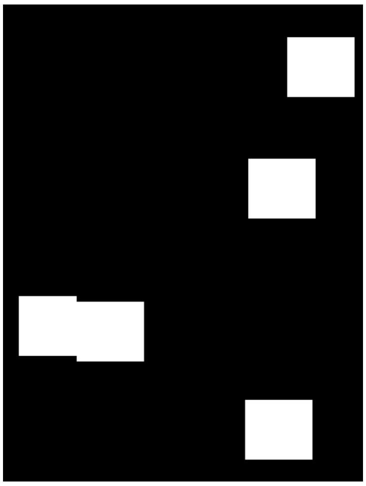


Fig17. Binary Image

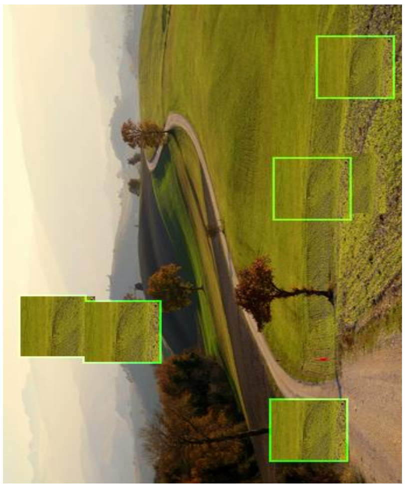


Fig18. Detected Output

Fig19.Rotate 180 degrees

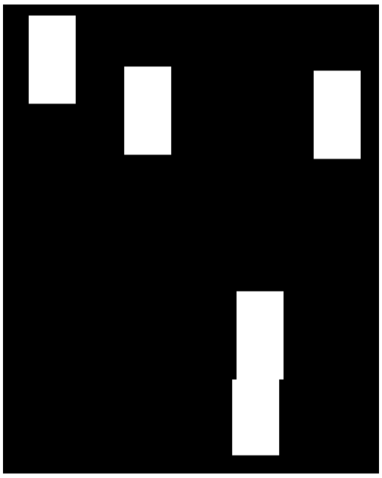


Fig20. Binary output

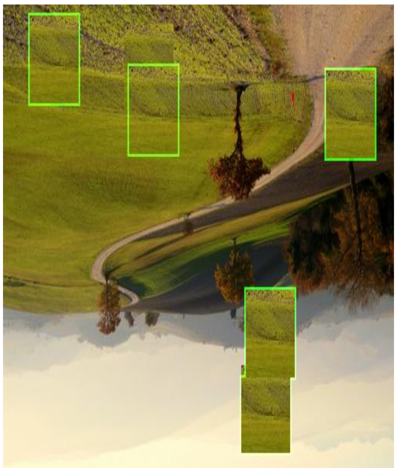


Fig21. Detected result

V.CONCLUSION

We have presented an efficient and robust technique that automatically detects duplicate regions in an image. Duplicated regions are detected by sorting all of the image blocks lexicographically. We have tested on different images by using CASIA 2.0 image tampering detection dataset and all the images are detected efficiently. We also

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005145|

found detection is applicable for blurred images and rotation etc. Although we have added a little amount of noise to the images and tested them, the algorithm gives the perfect result. We have seen that while this detection scheme improves the efficiency, the robustness of the method is reduced.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003.

[2] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Technical Report, TR2004-515, Dartmouth College, Computer Science, 2004.

[3] Guohui Li, Qiong Wu, Dan Tu, and ShaoJie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd," ICME, 2007.

[4] Yunlong Sheng and Henri H. Arsenault, "Experiments on pattern recognition using invariant fourier-mellin descriptors," J. Opt. Soc. Am. A, vol. 3, no. 6, pp. 771, 1986.

[5] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale,and translation resilient watermarking for images," IEEE Trans. Image Processing, vol. 10, pp. 767–782, 2001.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details