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

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.2022.1005222 |

Digital Image Forensics Using Feature Extraction

Ch. Niteesh Kumar[1], B.Venu[2] , B.Mohan Vamsi[3], A. Surya Teja[4]

UG Student, Dept. of Electronics and Communications Engineering, Vasireddy Venkatadri Institute Of Technology, Nambur, Guntur, Andhra Pradesh, India [1-4]

ABSTRACT: Manipulation of digital images has become a major issue in recent years.Medical imaging, digital forensics, and journalism are just a few examples.Copy–move forgery is image tampering that involves copying one portion of an image and pasting it into another section of the same image.Because of the sophisticated image editing tools available, photographs are susceptible to a variety of modifications; as a result, their authenticity is being called into doubt, particularly where images have persuasive force, such as in a court of law, news stories, or insurance claims. Local visual cues are used to identify duplicated regions in key point-based forgery detection techniques. When the duplicated sections are close to each other and when dealing with highly textured areas, the performance of Key-Point based approaches diminishes.

This paper focuses on Copy-Move-Forgery detection technique based on feature extraction from images. The proposed method utilizes Difference of Gaussian (DoG) and blob detector for identifying alterations in a given image. The proposed technique is evaluated on benchmark datasets and the experimental results illustrates the superiority of the proposed technique over existing methods.

KEYWORDS: key-point, CMFD, Blobs, DOG, ORB, Feature Extraction.

I. INTRODUCTION

In today's environment, it is simple to edit an image by adding or removing parts, resulting in a significant number of image forgeries.In many applications, digital images as visual elements are a primary source of information, and one of the major Features of a digital image with a binary representation is its ease of manipulation.For a tamper detection method, digital photographs include various information such as brightness and hue of individual pixels.Image tampering is defined as changing some important properties of image for spiteful purpose. It can be divided into three categories such as

COPY MOVE Forgery: Copy move means taking one part of image and pasted to into other part of same image.

Fig1.1 Original Image

Fig 1.2 Forgery Image

CUT PASTE Forgery: Cut paste means merging of two images or merging of one part a image and paste it to the another image.

| 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.2022.1005222 |

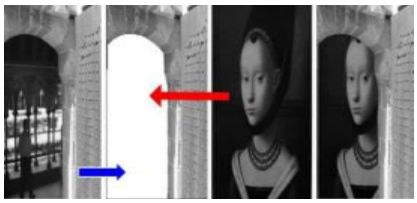

Figure 1.3 Cut Paste Forgery

Image Retouching: Image retouching forgery means enhancement of properties of original image byincreasingsaturation,brightness,hueetc.

Figure 1.4 Image Retouching

II. RELATED WORK

There are several methods for detecting tampering.We used ORB characteristics together with SVM to distinguish between fake and authentic photos (Support Vector Machine).ACC is used to extract feature vectors from the faked image (Auto Color Correlogram).ORB is a real-time application that combines an orientated fast key point detector and a rotating brief descriptor.It is substantially faster than SURF and SIFT.DOG (Difference of Gaussian) is also known as a blob detector because it detects blobs in the original image that differ in colour, brightness, and contrast from the surrounding areas.DCT(Discrete Cosine Transform) is a another method to find the tampering it exhibits a bounded series of data points as the addition of cosine functions vibrating at different frequencies.

III. EXISTING METHODS

Tosolvethetamperingintheimagewehave3methodsto solve them
1. Sobel Edge Detection
2. Feature Extraction
3. Feature Matching

Sobel Edge Detection: This detection method works through calculation of the gradient of the image intensity at every pixel within the image.When the detection process detects a high gradient area it basically represents it with white line on it.We apply this Sobel image to the blob detector for improving the blob localization purpose.

Fig 3.1 Sobel Edge Images

Feature Matching: In this stage we take the obtained blobs as a reference from the Sobel edge detection and we will try to extract the forged features in the image.This involves two techniques DOG and ORB.

| 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.2022.1005222 |

DOG(Difference Of Gaussian):

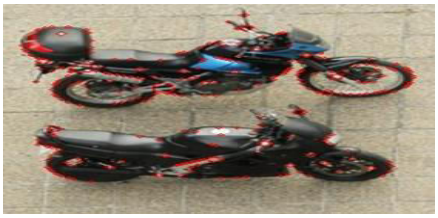

Fig 3.2 Shows the DOG

Which is used to detect blobs, In this we basically find the differences such as Brightness, Color and other properties in the image.To detect blobs we take Dog approach.

ORB(OrientedFastandRotatedBrief): They are actually two algorithms involved Fast and Brief. But we preferred as modified version of brief and that is combined with fast. It works on key point matching and it distinctive regions in an image like intensity variations we identify that we match them and we use for facial recognition.The use of Brief in normal facial recognition algorithm of SURF compares 16 pixels whereas in Brief algorithm we use an optimization technique we use only 4 pixels for comparison as shown in below figure.

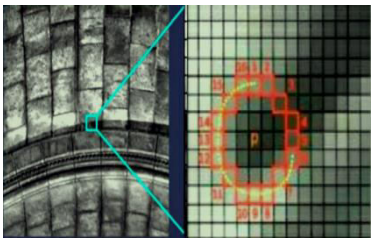

Fig 3.4 Key Point Detector

Fig 3.5 ORB Feature Detection

Feature Matching: Oncethefeatureextractionisdoneonthebothrealandforged images these images go under feature matchingtechnique where these compared and highlightedfeatures are marked with a straight line on the forgedimages so that we can find all the forged areas in theimage.

Fig 3.6 Feature Matching

IV. RESULTS

Therearemany methodsinimageforensics
1.DiscreteCosineTransform(DCT)
2.Scale Invariant Feature Transform(SIFT)
3.SpeedUpRobustFeatures(SURF)
4.AutoColourCorrelogram (ACC)

| 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.2022.1005222 |

5.DOGandORB

To compare this methods ,there are several parameters such as precision, recall,f1 score.

Extractionmethod	Pr(precision)%	Rc(recall)%	F1score%
DCT	77.78	99	87.06
SIFT	85.20	99	92.20
SURF	90.92	88.56	89.52
ACC	94.90	91	92.61
DoG& ORB	95.35	90.22	93.12

Table1:Shows thepercentagesofall extraction methods

Fig 4.1Results Of CMFD ByOR B and DoG

V. CONCLUSION

Copy move forgery detection approach is a novel model blob detector and orb feature detection. We can perform exact detection in Image forgery with this technique. In many cases, such as several forgeries in a single image or geometric alterations such as rotations, this detection technique will be as successful as feasible. Though forgeries are performed on the same image, the forged image is stored in distinct blobs, therefore we use the ORB feature to match it. As a result, the number of features to match and the number of false matches are significantly reduced. When both of these algorithms, DOG and ORB, are combined, feature matching becomes simple, allowing for easy detection of faked images.In future once this technique is improved there will be no need for human interference on these detection techniques.

REFERENCES

1. Rublee, E., Rabaud, V., Konolige, K., Bradski, G.: ORB: an effifffifficient alternative to SIFT or SURF. In: ICCV, pp. 2564–2571 (2011).
2. Shivakumar, B.L., SanthoshBaboo, S.: Detection of region duplication forgery in digital images using SURF. IJCSI Int. J. Comput. Sci. Issues 8(4), 199–205 (2011).
3. Gupta, C.S.: A review on splicing image forgery detection techniques. IJCSITS, **6**(2), 262–269, (2016).
4. Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012).

| 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.2022.1005222 |

5. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vis. **60**(2), 91–110 (2004).
6. Ng, T.-T., Chang, S.-F., Lin, C.-Y., Sun, Q.: Passive blind image forensics. In: Multimedia Security Technologies for Digital Rights Management, pp. 383–412 (2006).
7. Rublee, E., Rabaud, V., Konolige, K., Bradski, G.: ORB: an effifffifficient alternative to SIFT or SURF. In: ICCV, pp. 2564–2571 (2011).
8. Kong, H., Akakin, H.C., Sarma, S.E.: A generalized Laplacian of Gaussian fifilter for blob detection and its applications. IEEE Trans. Cybern. **43**(6), 1719–1733 (2013).
9. Al-Qershi, Osamah M., Khoo, Bee Ee, 2013. Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci. Int. 231 (1–3), 284–295.
10. Khan, Shaharyar, Saleem, Zahra, 2018. A comparative analysis of SIFT SURF KAZE AKAZE ORB and BRISK. Int. Conf. Comput. Math. Eng. Technol. 1–10.
11. Tralic, D., Zupancic, I., Grgic, S., Grgic, M.: CoMoFoD - new database for copymove forgery detection. In: Proceedings of 55th International Symposium ELMAR- 2013, pp. 49–54 (2013).
12. Yu, Liyang, Han, Qi, Niu, Xiamu, 2016. Feature point-based copy-move forgery detection: covering the non-textured areas. Multimedia Tools Appl. 75 (2), 1159–1176.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details