WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Dynamic Image Forensics and Forgery Analytics using Open Computer Vision Framework

Prof.Dr. j.k. Sumathi[1,*]

[1]Department of Computer Science, ITM University, Gwalior, India.

*Corresponding Author: Prof.Dr. j.k.Sumathi

DOI: https://doi.org/10.31185/wjcm.Vol1.Iss1.3
Received: December 2020; Accepted: February 2021; Available online: March 2021

ABSTRACT: The key advances in Computer Vision and Optical Image Processing are the emerging technologies nowadays in diverse fields including Facial Recognition, Biometric Verifications, Internet of Things (IoT), Criminal Investigation, Signature Identification in banking and several others. Thus, these applications use image and live video processing for facilitating different applications for analyzing and forecasting." Computer vision is used in tons of activities such as monitoring, face recognition, motion recognition, object detection, among many others. The development of social networking platforms such as Facebook and Instagram led to an increase in the volume of image data that was being generated. Use of image and video processing software is a major concern for Facebook because the photos and videos that people post to the social network are doctored images. These kind of images are frequently cited as fake and used in malevolent ways such as motivating violence and death. You need to authenticate the questionable images before take action. It is very hard to ensure photo authenticity due to the power of photo manipulations. Image formation can be determined by image forensic techniques. The technique of image duplication is used to conceal missing areas.

Keywords: Computer Vision, Digital Image Processing, Image Forensics, Image Forgery Analytics

1. INTRODUCTION

With the improvement of imaging technology, digital imaging sources are becoming the concrete information source. Meanwhile, the variety of image editing tools has made it possible for fake images to flood the Internet. "Image content forgery" by the mainstream media can be used for defamatory purposes and illegal activities. Bin Laden made his presence known through the social media in 2001 after 9/11. Also in 2007, an image of tiger in forest was proven as a tool to make the people believe in the existence of tigers in the Shanxi province of China. However, forensic investigation has revealed that the tiger was a “paper tiger.” In the same year, official images of four missiles were said to be doctored as one missile was found to be artificially duplicated [1]. The famous saying ’seeing is believing’ will not be effective in the future because of the inability to see. For this purpose, technology that ensures the image integrity is needed.

Changing the appearance of an image will affect the photo. There are various pieces of software that can alter picture parameters such as pixel, position, and size. Through the internet, newspaper, television and social media, there is a steep increase in the presence of fake news. Security of photograph forgery is a problem because this leads to severe vulnerabilities and loss of believability within digital photographs. Fraudulent photographs are often used as evidence in support of monetary claims. Cryptography for picture forensics is so helpful and efficient. These days, an outsized percentage of researchers specialise in the problematic of virtual photograph forgery. This is good case study of copy-pass image forgery where one or a multiple regions of the picture are substituted from different photographs. With photograph image manipulation techniques ranging from rotation, scaling, blurring, compression, and grain adding, credible forgeries

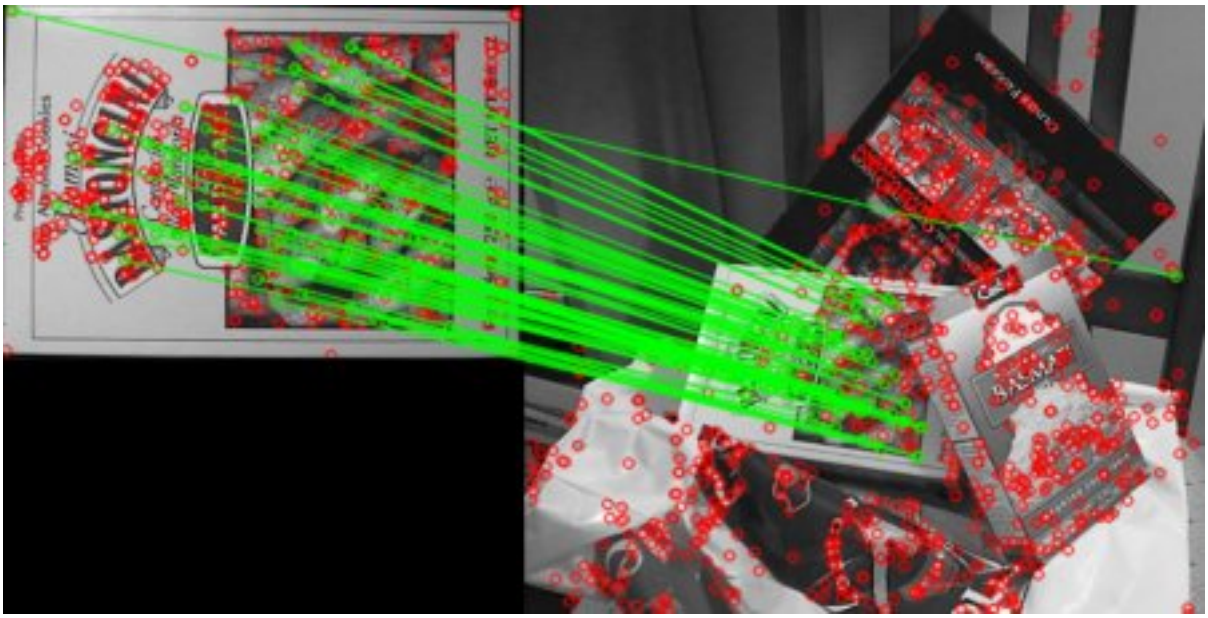

FIGURE 1. **Matching of Pixels from Image using Feature Extraction**

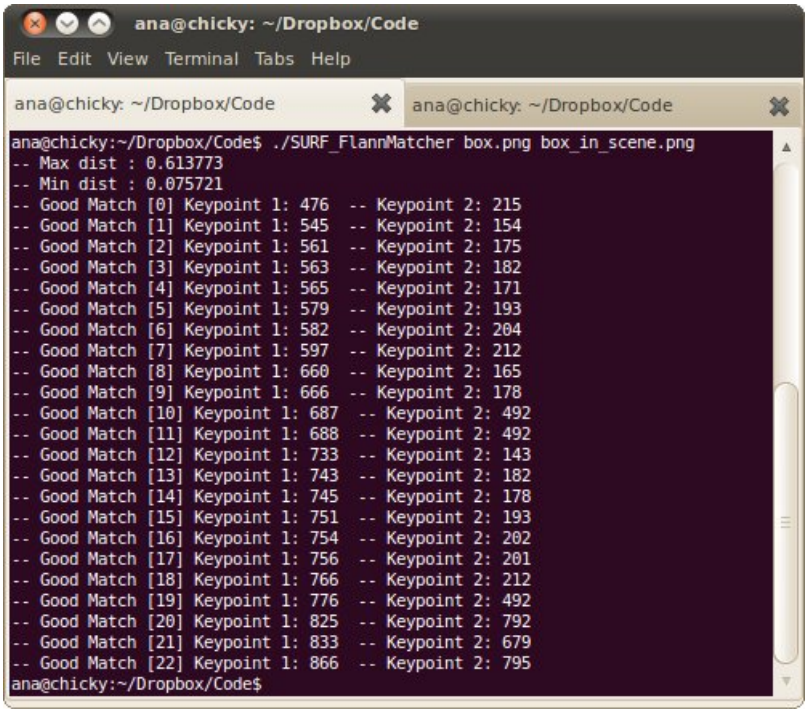

FIGURE 2. **Evaluation of Matching with Keypoints**

have been created. Copy flow forgery is prevalent because of the ease of use. There are at least two areas of duplication during the exposure period.

Artificial Intelligence is experiencing major advances and there are several development teams operating together to develop the architectures and methods. There are significant study fields concerning computer vision and image analytics by the professionals and scientist in this section [2]. There are popular methods for machine vision and image processing. A variety of resources and databases are required to do computer vision. Here are several popular innovations utilized in computer vision and image analytics.

Table 1. Technologies Integrated for Computer Vision and Image Processing

Tool	URL
OpenCV	http://www.opencv.org/
BoofCV	http://www.boofcv.org/)
NASA Vision Workbench	http://ti.arc.nasa.gov/tech/asr/intelligent-robotics/nasa-vision-workbench/
SimpleCV	http://simplecv.org/
Tesseract	https://github.com/tesseract-ocr/tesseract
SLIC Superpixels	http://ivrl.epfl.ch/supplementary_material/RK_SLICSuperpixels/
OpenMVG	https://github.com/openMVG/openMVG
LIBVISO	http://www.cvlibs.net/software/libviso/
VisualSFM	http://homes.cs.washington.edu/~ccwu/vsfm/
MeshLab	http://meshlab.sourceforge.net/
Bundler	http://phototour.cs.washington.edu/bundler/
Vid.stab	https://github.com/georgmartius/vid.stab
ViSP	https://visp.inria.fr/

OpenCV is an effective library for image recognition and computer vision. It has a high number of functions and algorithms for real-time machine vision and statistical mining. OpenCV was created by Intel, and currently OpenCV is funded by Sony. Garage and Invention culture. OpenCV was created for multiple use such as facial recognition and object detection [3].

OpenCV can be built in several programming languages such as Python, Java, C++, and so on. OpenCV will operate for other systems and programming languages such that the algorithm components can be applied without a problem. There are various installation procedures for OpenCV with different Oss [4].

2. IMAGE ANALYTICS USING OPEN COMPUTER VISION

In typical systems, photos and the computer vision files are stored on a pre-saved disc. This can be rendered more improved using OpenCV [5]. Developing a quick and powerful algorithm using OpenCV will guarantee real time identification of image attributes. This is the source code of OpenCV that is being executed in the Python framework that could be used for live real time identification from the web camera view [6].

```
import numpy as mnp
import opencv2
cap = opencv2.VideoCapture(0)
while(True):
    ret, frame = cap.read()
    MGray = opencv2.opencvtColor(frame,
opencv2.COLOR_BGR2MGRAY)
    MGray = mnp.float32(MGray)
    tdst = opencv2.cornerHarris(MGray,2,3,0.04)
    tdst = opencv2.dilate(tdst,None)
    frame[tdst>0.01*tdst.max()]=[0,0,255]
    opencv2.imshow('tdst',frame)
    if opencv2.waitKey(1) & 0xFF == ord('q'):
        break
cap.release()
opencv2.destroyAllWindows()
```

3. EVALUATION OF FORGERY IN BANKING INSTRUMENT

With the influence of automated authentications in different implementations, recognition of initial user experiences is one of the main challenges. There are several organizations who expect the documentation and certificates signed by the applicants as self-attestation. This is occurring now with the issuance of the latest smartphone SIM cards [7]. You should be careful because signatures are not readily collected. There are variety of photo editing applications accessible and used for the transformation of photographs to fresh images. This approach to patenting may be applied without the permission or consent of the original inventor [8, 9].

There is depiction of forgery in the latest text where the signatures are borrowed from another document.

FIGURE 3. Scanned Image of Original Cheque

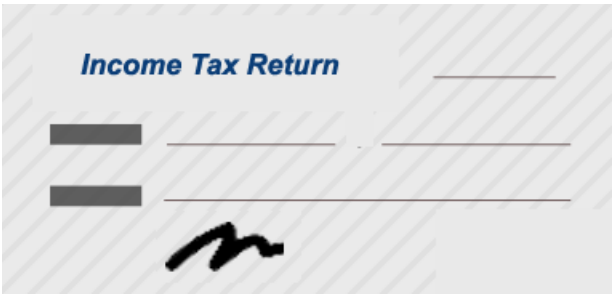

FIGURE 4. Signature used in other Document by Copying

```
  import numpy as tnp
  import opencv
  from matplotlib import pyplot as plot
  MIN_COUNT = 10
  timage1 = opencv.imread(''ChequewithCopiedSigna-
ture.png',0)
  timage2 = opencv.imread('OriginalCheque.png',0)
  sift = opencv.xfeatures2d.SIFT_create()
  # find the keypoints and descriptors with SIFT
  k1, im1 = sift.detectAndCompute(timage1,None)


 k2, im2 = sift.detectAndCompute(timage2,None)
 FLANN_INDEXG_KDTREE = 0
 indexg_params = dict(algorithm = FLANN_INDEXG_KDTREE,
trees = 5)
 search_params = dict(checks = 50)
 flann = opencv.FlannBasedMatcher(indexg_params,
search_params)
 matches = flann.knnMatch(im1,im2,k=2)
 # store all the good matches as per Lowe's ratio test.
 good = []
 for m,n in matches:
     if m.distance < 0.7*n.distance:
         good.append(m)
 if len(good)>MIN_COUNT:
     src_pts = tnp.float32([ k1[m.queryIdx].pt for m in
good ]).reshape(-1,1,2)
     dst_pts = tnp.float32([ k2[m.trainIdx].pt for m in
good ]).reshape(-1,1,2)
     M, mask = opencv.findHomography(src_pts, dst_pts,
opencv.RANSAC,5.0)
     matchesMask = mask.ravel().tolist()
     h,w = timage1.shape
     pts = tnp.float32([ [0,0],[0,h-1],[w-1,h-1],[w-1,0]
]).reshape(-1,1,2)
     dst = opencv.perspectiveTransform(pts,M)
     timage2 = opencv.pol-
ylines(timage2,[tnp.int32(dst)],True,255,3,
opencv.LINE_AA)
 else:
     print "Not enough matches are found - %d/%d" %
(len(good),MIN_COUNT)
     matchesMask = None
   draw_params = dict(matchColor = (0,255,0), # draw
matches in green color
                    singlePointColor = None,
                    matchesMask = matchesMask, # draw
only inliers
                    flags = 2)
 timg9 = opencv.draw-
Matches(timage1,k1,timage2,k2,good,None,**draw_params)
 plot.imshow(timg9, 'gray'),plot.show()
```

It is obvious from Figure that several pixels in the picture is the signature of another image. How machine learning is applied to pixel labeling can be achieved by utilizing machine learning in OpenCV [10, 11]. Through diligent forensic methods for detecting photos, the origin of the photo is possible to be discovered [12].

Image forgery is manipulating photographs to hide any detail. It can be difficult to distinguish between the modified and the initial media. This helps to preserve the image's trustworthiness and legitimacy. Today it is incredibly simple to create false photographs. Verifying the quality of photographs and identifying indicators of modification without needing

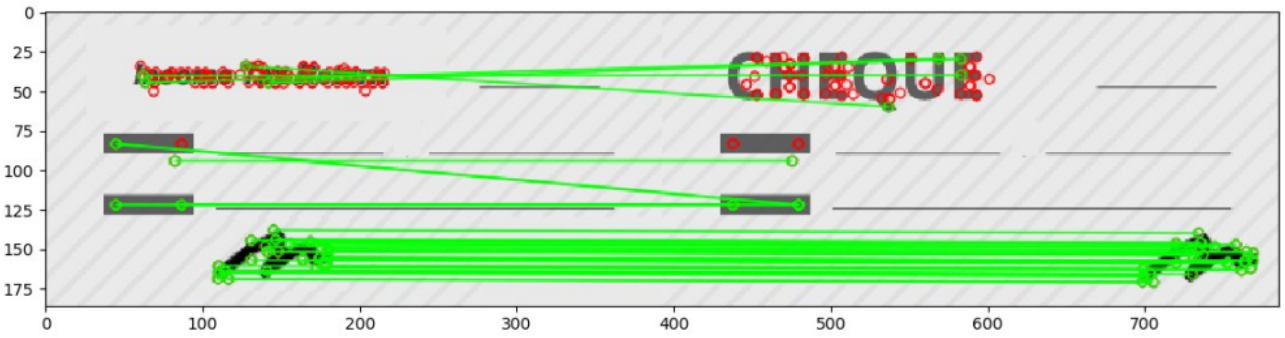

FIGURE 5. Copy Move Forgery Detection in Cheque

the pre-knowledge of the material is an essential area of study. A list is collected of recent publications linked to digital picture forgery. Passive input systems do not require any priori knowledge about the image. Firstly, different image forgery detection methods are defined and then their general framework is illustrated. This paper provides a short description of the current passive image authentication and briefly discusses the existing forgery detection strategies. The picture forgery detection strategy today is discussed, as well as studies for the future.

4. CONCLUSION

The area of digital image forensics has recently arisen and is currently forming an influence on planet. The primary aim of digital image forensics is to research photographs on whether they are original or false. Active methods such as watermarking and digital signature include details encoded in the photographs beforehand. However, the absence of accessible knowledge would impede the successful approaches of operation. Passive techniques are used to authenticate the two images which involve no prior knowledge of them. Photos are often duplicated via bogus picture shop editing process. When pictures are mixed, they generate a fascinating effect. But in plagiarism, field of copied job is strongly changed, if not total copying is performed. One downside is that it is difficult to evaluate which regions are legitimate and copied. The image forger applies sophisticated post-processing techniques to mask their behavior.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] A. F. Villán *Mastering OpenCV 4 with Python: a practical guide covering topics from image processing*, 2019.
[2] V. Janga, S. Kumar, and V. K. Enugala, "Advanced machine learning-based implementation patterns for computer vision and real-time multimedia applications," *Materials Today: Proceedings*, 2020.
[3] A. Talele, A. Patil, and B. Barse, "Detection of real time objects using TensorFlow and OpenCV," *Asian Journal For Convergence In Technology (AJCT)*, 2019.
[4] S. Taheri, A. Vedienbaum, A. Nicolau, N. Hu, and M. R. Haghighat, "OpenCV. js: Computer Vision processing for the open Web platform," *Proceedings of the 9th ACM Multimedia Systems Conference*, pp. 478–483, 2018.
[5] S. Sivkov, L. Novikov, G. Romanova, A. Romanova, D. Vaganov, M. Valitov, and S. Vasiliev, "The algorithm development for operation of a computer vision system via the OpenCV library," *Procedia Computer Science*, vol. 169, pp. 662–667, 2020.
[6] J. Sigut, M. Castro, R. Arnay, and M. Sigut, "OpenCV Basics: A Mobile Application to Support the Teaching of Computer Vision Concepts," *IEEE Transactions on Education*, vol. 63, no. 4, pp. 328–335, 2020.
[7] I. V. Kiselev, "Comparative analysis of libraries for computer vision OpenCV and AForge. NET for use in gesture recognition system," *Journal of Physics: Conference Series*, vol. 1661, pp. 12048–12048, 2020.

[8] V. Janga, S. Kumar, and V. K. Enugala, "Advanced machine learning-based implementation patterns for computer vision and real-time multimedia applications," *Materials Today: Proceedings*, 2020.
[9] L. Khurana, A. Chauhan, and P. Singh, "Comparative Analysis of OpenCV Recognisers for Face Recognition," in *2020 10th International Conference on Cloud Computing*, pp. 485–490, IEEE, 2020.
[10] J. S. Charlie and M. Wulandari, "Classification of Fertilizer Using OpenCV Based on Color Characteristic," *IOP Conference Series: Materials Science and Engineering*, vol. 1007, pp. 12053–12053, 2020.
[11] A. Brdjanin, N. Dardagan, D. Dzigal, and A. Akagic, "Single Object Trackers in OpenCV: A Benchmark," *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, pp. 1–6, 2020.
[12] I. H. Chen, Y. S. Lin, and M. B. Su, "Computer vision-based sensors for the tilt monitoring of an underground structure in a landslide area," *Landslides*, vol. 17, no. 4, pp. 1009–1017, 2020.