Identification of Tampered Image by SIFT Detection

Prof. Mayur Tembhurney[1], Anjali Patil[2], Anjali Sharma[3], Ashi Dahat[4], Gunjan Badade[5]

[1,2,3,4,5]S. B. Jain Institute of Technology, Management & Research, Nagpur

ABSTRACT

Fake or altered photos are a challenge for everyone in today's digital environment. According to research, digital photos play a key role in industries such as medicine, paperwork, law, and social media, and tampering with such vital information is simple with programmes like Photoshop and other altering tools. Many photographs are tampered with on social media for amusement, however tampering with images that play a critical function and might cause major concerns must first be recognised. We employed the SIFT (scale-Invariant feature transform) detection approach in this work, which is one of the most widely used and has a 93.87 percent accuracy.

INTRODUCTION

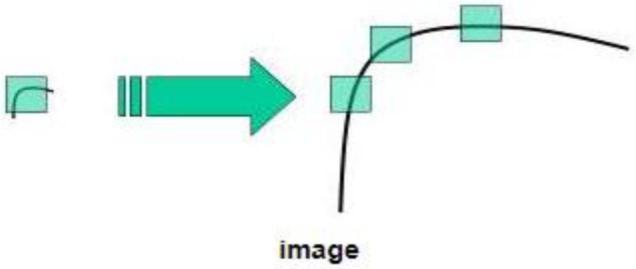
In today's digital environment, the digital image is a valuable and practical source of information. They transmit information at the highest speed because to their simplicity of capture and storage. Images can be used as evidence or proof in a court of law. From military to paperwork, from art to medical, digital pictures have a wide range of applications. Digital picture forensics is becoming an increasingly important requirement in society. It's crucial that the picture is genuine. Because of the evolution of computers and the ease with which low-cost hardware and software are available these days.

It becomes relatively easy to change a digital image without leaving any obvious indications of manipulation, and tracing it gets more difficult. As a result, the digital image's integrity, authenticity, and privacy are compromised. The goal of this change is to obscure some of an image's most critical traces, such photos provide incorrect information. Any modifications in the image must be identified in order to determine the validity of the photos.

Digital image forensic is an area of research that focuses on uncovering picture tampering. The photos are matched using SIFT based on feature key points. This is one of the most extensively used picture feature extraction algorithms. The method identifies the image's main features, such as the SIFT description and SIFT descriptor. The SIFT method is used to eliminate low-response features. Copy move is a frequently used technique for editing digital photographs**.** forging of an image Copying a section of a picture into an input image and concealing certain key information or elements from the image is all that is required. Hence the image's originality is compromised, and the image's authenticity gets compromised.

When cloned areas of the same picture exhibit comparable qualities to the initial image, it becomes highly difficult to identify forgeries. Snapshot is the duplicated piece of a picture that is used to fake the image. A copy move forgery introduces correlation between the original picture region and the duplicated content. The post-processing of the sample is required before pasting to generate a realistic fake. A good forgery detection technique should be resistant to procedures such as post-processing rotation and scaling there are a number of algorithms available that focus on snippet post-processing.

Some corner detectors, such as Harris, are rotation-invariant, which means they can discover the same corners regardless of how the picture is rotated. It's clear since the corners of the rotated image remain the same. What about scalability, though? If the picture is resized, a corner may no longer be a corner. Take a look at the image below for an example. When zoomed in the same window, a corner of a small picture within a small window appears flat. As a result, the Harris corner isn't scale invariant.



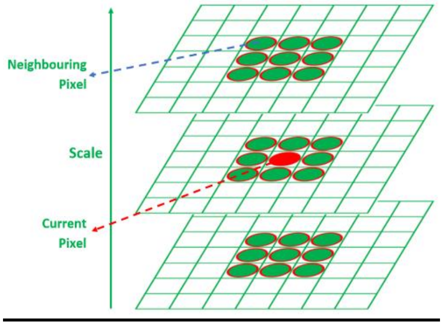
It is self-evident that we cannot detect key-points of different scales using the same window. With a minor corner, it's fine. However, wider windows are required to identify greater corners. Scale-space filtering is used for this. Let’s begin by detecting key-points and drawing them. We must first create a SIFT object.

A four-stage filtering method is employed in the SIFT algorithm.

a. Detection of the interest key points that is scale space extreme.
b. By considering only the stable key points, localization of key points takes place.
c. Orientation assignment is performed to the selected key points.
d. Key point Descriptor

Phase I: Scale Space Peak Selection

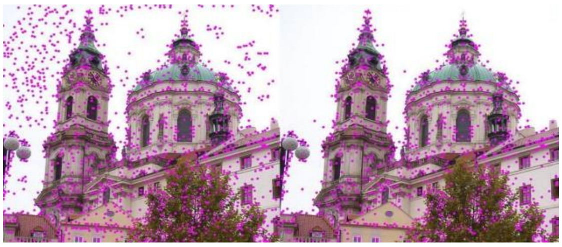
Scale Space refers to the process of adding a constant set of Gaussian Filters to a target image with varying sigma values. The Scale Space is the plot that results from this. The Spatial Coincidence Assumption is used to select the scale space peak. According to this, we classify an edge as an actual edge if it is discovered at the same place at various scales (as shown by zero crossings in the scale space).



The local maxima/minima in Scale Space of laplacianof Gaussian can be used to discover Interest Points in 2D pictures. For a particular sigma value, a prospective SIFT interest point is determined by selecting the potential interest point and taking into account the pixels in the level above (with greater sigma), the same level, and the level below (with lower sigma than current sigma level). It is a possible SIFT interest point if the point is the maximum/minimum of all 26 nearby points – and it serves as a starting point for interest point detection.

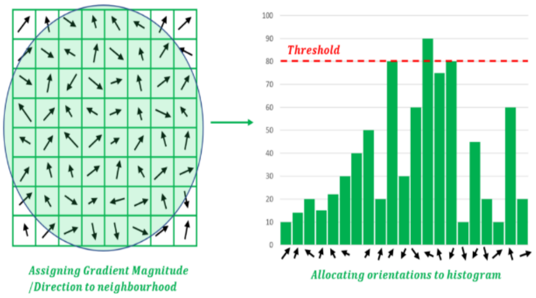
Phase II: Key Point Localization

The refining of key-points identified in the preceding step is called key point localization. Low-contrast key-points, shaky key-points, and key-points on the edges are all deleted. Calculating the Laplacian of the key-points identified in the previous stage accomplishes this.



Phase III: Assigning Orientation to Key-points

The orientation of the key-points must be computed in order to accomplish detection that is invariant with regard to the rotation of the picture. This is accomplished by considering the key-point's neighbourhood and estimating the magnitude and direction of the neighborhood's gradients. A histogram with 36 bins is generated based on the values gathered to represent 360 degrees of orientation (10 degrees per bin). As an example, if a point's gradient direction is 67.8 degrees, a value proportional to the point's gradient magnitude is added to the bin representing 60-70 degrees. Histogram peaks over 80% are turned into a new key-point and utilised to determine the original key-point's orientation.


Assigning Gradient Magnitude /Direction to neighbourhood
100
90
80
70
60
50
40
30
20
10
0
Threshold
Allocating orientations to histogram

Phase IV: Key Point Descriptor

Finally, utilising the key-point’s neighbourhood, a description is constructed for each key-point. These descriptors are used to compare key-points in different pictures. The description of that key-point is defined using a 16×16 neighbourhood of the key-point. The neighbourhood of 16×16 is broken into sub-blocks. Each of these sub-blocks is a 44-neighborhood that is non-overlapping and continuous. Following that, an 8 bin orientation is constructed for each sub-block, as described in Orientation Assignment. To produce the key-point descriptor, these 128 bin values (16 sub-blocks * 8 bins per block) are expressed as a vector.

REFERENCES

[1]. Hold E. Sitting pretty in the post-mobile era. https://www.npd.com/wps/portal/npd/us/blog/2017/ 955 sitting-pretty-in-the-post-mobile-era/; 2017.

[2]. Magazine MTSTO. Here’s how many digital photos will be taken in 2017. http://mylio.com/true-stories/tech-today/ how-many-digital-photos-will-be-taken-2017-repost; 2016.

[3]. J. Fridrich, D. Soukal, and J. Lukas, “Detection of Copy-Move Forgery in Digital Images,” in Proceedings of Digital Forensic Research Workshop, August 2003.

[4]. Shivani Thakur, Ramanpreet Kaur, Dr. Raman Chadha ,Jasmeet Kaur, “A Review Paper on Image Forgery Detection In Image Processing”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 86-89

[5]. Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, 300 Liu-Ho Road, Makung City, Penghu 2019

[6]. Katzenbeisser S, Petitcolas F. Information hiding techniques for steganography and digital watermarking. Artech house; 2000.

[7]. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on information forensics and security 2012;7(6):1841–54.

[8]. I Amerini, L Ballan, R Caldelli, A DelBimbo, L D Tongo, Giuseppe Serra, Copy Move Forgery Detection And Localization By Means Of Robust Clustering with J Linkage.

[9]. T Bianchi and A Piva, Image Forgery Localization via Block- Grained Analysis of JPEG Artifacts IEEE Transactions on Information Forensics And Security

[10]. A Langille and M. Gong, & quot. An efficient match-based duplication detection algorithm & quot;, IEEE CRV, p. 64, 2006.

[11]. A. K. Yadav, D. Singha and V. Kumar, Forgery (Copy-Move) Detection In Digital Images using Block Method, International Journal of Collaborative Research in Engineering Sciences, (2014), April.

[12]. D.G. Lowe, & quot Distinctive Image Features from Scale-Invariant Key points & quot. International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.

[13]. Tang, and H-V Shum, Detecting Doctored Images using Camera Response Normality and Consistency.

[14]. S.-F. Chang Hsu, Y.-F, and, Image splicing detection using camera response function consistency and automatic segmentation.

[15]. A. Swaminathan, M. Wu, and K. J. R. Liu, Digital Image Forensics via Intrinsic Fingerprints.

[16]. Andrea Costanzo, Irene Amerini, Roberto Caldelli, and Mauro Barni, Forensic Analysis of SIFT Keypoint Removal and Injection, IEEE Transactions on Information Forensics and Security.