# The Illustrated Study of Detection of copy move Forgery of Digital image by Matching Triangle of Keypoint

Sayali Badge
#Department of Electronics Engineering
RGCER, Nagpur
sayalibadge859@gmail.com

***Abstract:-*** Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content, and detecting forgeries will only increase. Detection of malicious manipulation with digital images (digital forgeries) is the topic of this paper. In particular, we focus on detection of a special type of digital forgery – the copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. Copy–move forgery is one of the most common types of tampering for digital images. Detection methods generally use block-matching approaches, which first divide the image into overlapping blocks and then extract and compare features to find similar ones, or point-based approaches, in which relevant keypoints are extracted and matched to each other to find similar areas. we present a very novel hybrid approach, which compares triangles rather than blocks, or single points. Interest points are extracted from the image, and objects are modeled as a set of connected triangles built onto these points. Triangles are matched according to their shapes (inner angles), their content (color information), and the local feature vectors extracted onto the vertices of the triangles. Our methods are designed to be robust to geometric transformations. Results are compared with a state-of-the-art block matching method and a point-based method. Furthermore, our data set is available for use by academic researchers.

***Keywords:*** *Digital image forensics, copy-move forgery, SIFT,*

*****

## INTRODUCTION

Digital image forensics deals with the problem of certifying the authenticity of a picture, or its origin. an image has always implied the truth of what it represents. the advent of digital pictures and relative ease of digital image processing makes today this authenticity uncertain. the same tools, used to crop an image, eliminate “red-eye” or simply improve an image, can also be used to doctor images with despicable intent, creating an image that is not a representation of the reality.

Digital images can be manipulated in such a perfect way that the forgery cannot be visually perceived by naked eye. Nowadays, in our society, we can come in contact with a lot of tampered images, in news report, business, law, military affairs, academic research. More particularly, tampered images could be used to distort the truth in news reports, to destroy someone’s reputation and privacy, e.g. by changing a face of a person in a photo with someone else’s face. Law enforcement today uses emerging technological advances in the investigation of crimes. One of the main objectives of Image Forensics techniques is

to understand what kind of tampering has been applied. Images can be doctored in several ways [2]: photo-compositing, re-touching, enhancing are only some examples of typical image alterations. Although many tampering operations generate no visual artifacts in the image, they will nevertheless affect its inherent statistics. In this work we particularly intensified the study of copy-move tampering [3], that is one of the most common image manipulations. The goal of copy move forgery is to replicate a part of an image, often to hide an object, by copy-pasting a set of pixels from an area to another area of the same picture, and it is often very difficult to detect with the naked eye.

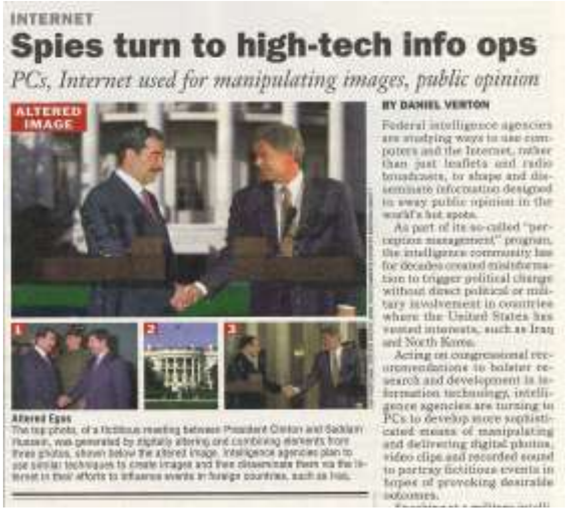
### The Need for Detection of Digital Forgeries:

The availability of powerful digital image processing programs, such as PhotoShop, makes it relatively easy to create digital forgeries from one or multiple images.

An example of a digital forgery is shown in Figure 1. As the newspaper cutout shows, three different photographs were used in creating the composite image: Image of the White House, Bill Clinton, and Saddam Hussein. The White House was rescaled and blurred to create an illusion of an out-of-focus background. Then, Bill Clinton and Saddam were cut off from two different images and pasted on the White House image. Care was taken to bring in the speaker stands with microphones while preserving the correct shadows and lighting. Figure 1 is, in fact, an example of a very realistic looking forgery.

.

The fact that one can use sophisticated tools to digitally manipulate images and video to create non-existing situations threatens to diminish the credibility and value of video tapes and images presented as evidence in court independently of the fact whether the video is in a digital or analog form. To tamper an analogue video, one can easily digitize the analog video stream, upload it into a computer, perform the forgeries, and then save the result in the NTSC format on an ordinary videotape. As one can expect, the situation will only get worse as the tools needed to perform the forgeries will move from research labs to commercial software.



INTERNET

Spies turn to high-tech info ops

*PCs, Internet used for manipulating images, public opinion*

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

**Figure 1 Example of a digital forgery.**

## COPY MOVE FORGERY:

Copy-Move image forgery is the widely used technique to edit the digital image. Copy-move forgery involves the pasting of image blocks in same image and conceal important information or object from the image. As a result of this the originality of the image is lost and puts at stake the authenticity of that digital image. In Copy-Move Forgery detection copied blocks are from same image so they sustain the same properties as the other blocks of image and therefore makes it very difficult to detect the forgery.

## FORGERY DETECTION METHODS:

To determine whether the digital image is authentic or not is a key purpose of image forensics. There are several different types of tampering attacks but the most common and the immediate one is the copy move forgery. Copy move forgery involves concealing or duplicating one region in an image by pasting certain portions of the same image on it. Digital forensics [1], deals with developing systems in the absence of watermarks [2] or signatures inserted in the image

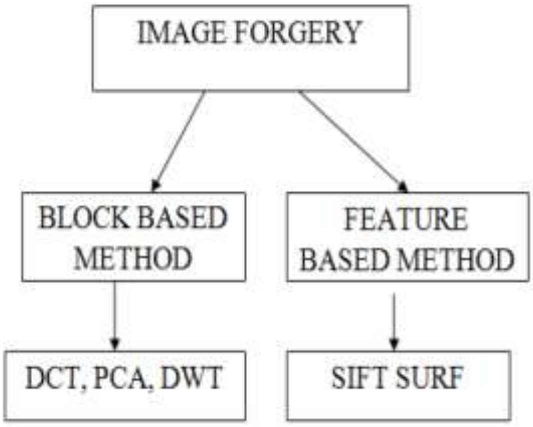


**Figure : Copy Move Forgery Detection Method**

## LITERATURE SURVEY:

Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Method In this paper ,As Copy-Move forgeries have become popular, the importance of forgery detection is much increased. Although many Copy-Move Forgery detection techniques have been proposed and have shown significant promise, robust forgery detection is still difficult. There are at least three major challenges: tampered images with compression, tampered images with noise, and tampered images with rotation. In this paper we reviewed several papers to know the recent development in the field of Copy-Move digital image forgery detection. Sophisticated tools and advanced manipulation techniques have made forgery detection a challenging one. Digital image forensic is still a growing area and lot of research needed to be done.
Published In September 2010, IEEE Global Journal of Computer Science and Technology

A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery in this paper, In this paper, the problem of detecting if an image has been forged is investigated; in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create a duplication or to cancel something that was awkward. Generally, to adapt the imagepatch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on scale invariant features transform (SIFT) is proposed. Such a method allows us to both understand if a copy–move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area

and, in addition, to estimate the geometric transformation parameters with high reliability. The method also deals with multiple cloning.
Published in
September 2011, IEEE transactions on information forensics and security

Copy-Move Forgery Detection using DCT,
In this paper novel approach is proposed to detect combination of different post-processing operations by single method. It is analyzed that block-based features method DCT is robust to Gaussian noise and JPEG compression, secondly the keypoint-based feature method SIFT is robust to rotation and scaling. Thus by combining SIFT and DCT we are able to detect forgery under post-processing operations of rotation, scaling, Gaussian noise, and JPEG compression and thus the efficiency to detect forgery improves but Results have shown that if one technique in method fails to detect forgery the other technique detects it and vice-versa and hence the detection rate is increased.
Published In
May 2013,IEEE International Journal of omputer Applications.

Contrast Enhancement-Based Forensics in Digital Images In this paper, we propose two novel algorithms to detect the contrast enhancement involved manipulations in digital images. First, we focus on the detection of global contrast enhancement applied to the previously JPEG-compressed images, which are widespread in real applications. The histogram peak/gap artifacts incurred by the JPEG compression and pixel value mappings are analyzed theoretically, and distinguished by identifying the zero-height gap fingerprints. Second, we propose to identify the composite image created by enforcing contrast adjustment on either one or both source regions. The proposed contrast enhancement based forensic methods could work particularly well when contrast enhancement is performed as the last step of manipulation.
Publised In
March 2014, IEEE transactions on information forensics and security

Image Forgery Detection Using Adaptive Oversegmentation and Feature Point MatchingIn this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in
each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Experimental results show that the proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, But They have better performance in case of complex scenes, while for images with regular background they typically find a lot of false matches .
Publised in
August 2015 ,ieee transactions on information forensics and security

## REFERENCES:-

[1] H. T. Sencar and N. Memon, “Overview of state-of-the-art in digital image forensics,” Algorithms, Archit. Inf. Syst. Secur., vol. 3, pp. 325–348, Dec. 2008 .

[2] H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.

[3] B. L. Shivakumar and S. S. Baboo, “Detecting copy-move forgery in digital images: A survey and analysis of current methods,” Global J. Comput. Sci. Technol., vol. 10, no. 7, pp. 61–65, 2010.

[4] J. Fridrich, D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, USA, Aug. 2003, pp. 342–358.

[5] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[6] G. Li, Q. Wu, D. Tu, and S. Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD,” in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 1750–1753.

[7] W. Luo, J. Huang, and G. Qiu, “Robust detection of region-duplication forgery in digital image,” in Proc. 18th Int. Conf. Pattern Recognit., 2006, pp. 746–749.

[8] W. Li and N. Yu, “Rotation robust detection of copy-move forgery,” in Proc. 17th IEEE Int. Conf. Image Process. (ICIP), Sep. 2010, pp. 2113–2116.

[9] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Proc. Inf. Hiding Conf., Jun. 2010, pp. 51–65.

[10] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in Proc. 2nd ACM Workshop Multimedia Forensics, Secur. Intell. (MiFor), 2010, pp. 59–64.