Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 458 – 465

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics

Anil Dada Warbhe[a*], R. V. Dharaskar[b], V. M. Thakare[c]

[a]*Research Scholar, SGBAU, Amravati 444602, India*
[b]*Former Director, DES (Disha–DIMAT) Group of Institutes, Raipur 492101, India*
[c]*HOD, SBGAU (PG Dept. of Computer Science), Amravati 444602, India*

Abstract

It is crucial in image forensics to prove the authenticity of the digital images. Due to the availability of the using sophisticated image editing software programs, anyone can manipulate the images easily. There are various types of digital image manipulation or tampering possible; like image compositing, splicing, copy-paste, etc. In this paper, we propose a passive scaling robust algorithm for the detection of Copy-Paste tampering. Sometimes the copied region of an image is scaled before pasting to some other location in the image. In such cases, the normal Copy-Paste detection algorithm fails to detect the forgeries. We have implemented and used an improved customized Normalized Cross Correlation for detecting highly correlated areas from the image and the image blocks, thereby detecting the tampered regions from an image. The experimental results demonstrate that the proposed approach can be effectively used to detect copy-paste forgeries accurately and is scaling robust.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Digital Image Forensics; Image Forgery Detection; Image Tampering; Image Authentication.

1. Introduction

The internet has gifted us cost-effective approach to exchange and trade the data all over the world. Today's world almost entirely relays on internet technologies to communicate, doing businesses and governance. The main features of the technology, like Low cost, speedy access and ease of operation has made human lives easy going. However, all these advantages and the convenience, come at a cost. With increased sophistication of the

* Corresponding author. Tel.: +91-982-355-1869.
*E-mail address:*mtech2008@rediffmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.059

technologies, Internet crime has also increased tremendously around the world. The Internet has provided a stage for internet criminals to carry out criminal activities and posing a significant threat to Internet users.[1,2,3] These criminal activities are broad and diverse, for example, identity theft, a threat to nation's security, child pornography, copyright infringement is, to name a few. These crimes impose threats to individual safety and privacy. In such scenario, if the criminal get access to the confidential data of a person, such as or photos and videos, etc.; criminal can play with it as he wants, to satisfy his malice intents and poor victim, on the other hand, has to face serious consequences. Image forensics investigators need robust and efficient image authentication procedures to apprehend, detect and take legal action against criminals, involved in such acts.[4]

Digital forensics is a vast domain and covers many disciplines. The authors[5] have presented a complete ontology of digital forensics. The images are the rich source of information and are widespread in the cyberspace. The main concern with these digital images is that they are vulnerable to modifications very easily. Due to the availability of the sophisticated image editing software is on PCs, laptops, and mobile devices, one can easily carry out tampering with it. These attacks on images pose a great danger to the whole community, as one can easily change the meaning of the image by simply carrying out some operations on it. Once it becomes viral on the social networking sites can create havoc. Hence, it is imperative to authenticate the images for their originality. The authenticating the digital images for their content i.e. integrity, the source is the field of Digital Image Forensics (DIF). DIF has gained tremendous importance in last one and half decade among the research community. The fundamental problems digital image forensics techniques attempt to solve is the identification of the source and detecting the integrity of a digital image[6]. Identification of source involves determining the means by which the images are created like camera, scanner, and regenerative algorithm. Similarly, integrity can be confirmed by analyzing the images for its modification.

Digital image forensics can be classified broadly under two heads, as active forensics and passive forensics. Active forensics involves authenticating images by extracting the digital signature or watermark embedded in it. The digital watermarks are inserted into the images by the special cameras at the time of taking pictures. Any tampering operations done on the image can deteriorate the embedded watermark. This detected deterioration can be taken as an indication of the possible image tampering. However, the main limitation of the active forensics is that we need both original and the tampered image to authenticate and confirm tampering. Also, the need for special devices, such as special cameras, for example, makes it a costlier affair. Passive forensics, on the other hand, neither require special devices nor needs to have the original content available to prove tampering of the image. Passive forensics is also termed as blind forensics. It relies on the simple principle that the original natural image always owns some inherent pattern and statistics that are consistent. When some tampering operation occurs on the image, this change in the statistics of the image guarantees image tampering.[7]

Image Forensics or image tampering detection can be classified into different categories, like pixel base, a format based, camera based, etc.[8]. Copy-paste tampering detection comes under pixel based forensic detection tool. It is a most common type of tampering, in which forger copies some region from one place of an image and pastes it at some other location. Though copied and pasted regions in this class are identical; these tampering operations are so smartly done, that it leaves no obvious traces of tampering. It is sometimes easier to detect the pasted regions if it did not undergo any post processing operation. It becomes difficult if the copied part undergoes some sort of transformation such as scaling, rotation or both. In this paper, we introduce a scaling robust copy-paste detection scheme using Normalized cross correlation.

2. Literature Review

Copy-Paste tampering is also called as copy-move forgery. Copy-paste tampering detection can be carried out by two main approaches; either block based or by key-point detection[9,10]. As proposed technique uses the block based approach in this section, we review some of the techniques copy-paste tampering detection.

Fridrich et al.[11] have made the first attempt for copy-paste tampering detection. Popescu and Farid[12] have further improved the algorithm and presented a method using principal component analysis (PCA). Myna et al.[13] developed a method for detecting and localizing copy-move forgery using a log-polar coordinates and wavelet transforms. Bayram et al.[14] use the Fourier-Mellin Transform (FMT), which involves a log-polar mapping, to represent image blocks. Li and Yu[15] extended the work performed by Bayram et al.[14], which is based on FMT. The authors[16] have