Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 464 – 470

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Computationally Efficient Digital Image Forensic Method for Image Authentication

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

The issue of the authenticity and integrity of digital images is getting critical. Nowadays it became easy to create image forgeries. Digital image forensics plays a vital role in proving authenticity and integrity of digital images. There are various types of image forgeries possible, and Copy-Paste is one of it. In this type of forgery, a region of an image is copied and afterward pasted to another part of the same picture. In this paper, we propose an effective and computationally efficient method for the detection of Copy-Paste forgery. The proposed forgery detection is based on a customized Normalized Cross Correlation (NCC). The experimental results show that the proposed approach can be effectively used to detect forgeries accurately and is robust to affine transform to a certain extent.

Peer-review under responsibility of organizing committee of the ICISP2015

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

1. Introduction

The internet has provided us a much sophisticated and convenient way to transfer and exchange the information all across the world. But at the same time, this cyberspace, has also provided a platform for criminals, to carry out criminal activities. With increased access to computers across the globe, cybercrime is becoming a major challenge

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

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.089

to law enforcement agencies. Cybercrime investigation process is still not fooled proof and has limited success in prosecuting the lawbreakers; therefore there is a strong need to understand and strengthen the existing investigation processes and systems for controlling the cybercrime.[1] Digital Image Forensics is one of it. The images are the rich source of information and are spread across the cyberspace.

Images are very vulnerable to modifications. Modifications in the images are carried out by attackers to change or conceal its meaning by using sophisticated image editing software. These software applications are easily available today; not only on personal computers and laptops but on handheld mobile devices as well.[2]This is a cause of great concern and poses threats to the public, government, and businesses. Hence, these images need to be authenticated. Authenticating the digital image for itscontent, i.e., integrity and the source is the field of Digital Image Forensics (DIF). DIF has gained tremendous importance in last one 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 digital images.[32] 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.

The tamper detection algorithms for the digital image forensics are classified as active tamper detection approaches and passive detection approaches. Passive tamper detection approach does not require the knowledge of any prior information about the content. The core assumption for this class of techniques is the assumption that original non-forged content owns some inherent patterns that are always consistent in the un-forged content, but they are very likely to be alteredby some tampering processes. Although visually imperceptible, such changes can be detecting by statistical analysis of the content itself, without the need of any apriori information. On the contrary, the active approach involves authenticating images by extracting the watermark and digital signature embedded in it. Special digital cameras are required to embed a digital watermark into an image at the time of their capture. So, any tampering operation done on images can deteriorate the embedded watermark and signature. This detected deterioration in the extracted watermark can help us confirming the authenticity of the images.[3]

The passive DIF techniques can be categorised into different domains such as 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artefacts introduced by the camera lens, sensor, or on-chip postprocessing; 4) physically based techniques, for detecting the forgery and authenticating the digital images.[4]

Further, these copy-paste image forensic techniques which are also called as image forgery detection techniques are categorized under two heads: 1) Block-based and 2) Keypoint based techniques. In this paper, we propose a common type of pixel based forensic technique called as copy-paste image forgery. We propose a blind digital image forensic method for image authentication so as to know whether the image is an authentic or a forged one. We have used block based approach to detect forgeries and used NCC as a basic tool to detect the forged regions.

2. Literature Review

Copy-Paste forgery is also known as copy-move forgery. In the last decade, copy-paste forgery has a profound impact on the authenticity of digital images. For this reason, researchers paid much attention detecting this kind of forgery. In this type of forgery creation, a part of the image is copied and/or moved to some other location in the same image.Because of this, a strong correlation exists between these copied and pasted parts which can be used as evidence for forgery detection. However, the main challenge is to find efficient algorithms to find features and matching these features for finding correlated segments. In these methods, first, characteristic features are calculated by two approaches: block based and keypoint based. In block based methods, the whole image is divided into the overlapping or non-overlapping blocks and then they are processed to extract the features whereas, in keypoint based approach the features are collected by calculating local keypoints for the whole image. The positions of each block or keypointare also stored in the feature vector. Then, the feature matching is performed to find similar features within the same image. The forgery localization is done by displaying the matched blocks or keypoints in colors corresponding to the locations of the matched features. As, in the proposed method, we have adopted the block based approach to detect forgeries; hence, in this section, we will review the literature based on the block processing approach.