A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform

Toqeer Mahmood, Zahid Mehmood, Mohsin Shah, Tanzila Saba

PII: S1047-3203(18)30071-3
DOI: https://doi.org/10.1016/j.jvcir.2018.03.015
Reference: YJVCI 2162

To appear in: *J. Vis. Commun. Image R.*

Received Date: 12 September 2017
Revised Date: 13 March 2018
Accepted Date: 24 March 2018

Please cite this article as: T. Mahmood, Z. Mehmood, M. Shah, T. Saba, A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform, *J. Vis. Commun. Image R.* (2018), doi: https://doi.org/10.1016/j.jvcir.2018.03.015

A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform

Toqeer Mahmood[1], Zahid Mehmood[2], Mohsin Shah[3], Tanzila Saba[4]

[1] Department of Computer Science, University of Engineering and Technology Taxila-47050, Pakistan
Email: toqeer.mahmood@yahoo.com
[2] Department of Software Engineering, University of Engineering and Technology Taxila-47050, Pakistan
Email: zahid.mehmood@uettaxila.edu.pk
[3] School of Information Science and Technology, University of Science and Technology of China, Hefei-230027, China
Email: mohsin@mail.ustc.edu.cn
[4] College of Computer and Information Sciences, Prince Sultan University Riyadh-11586, Saudi Arabia
Email: tsaba@psu.edu.sa

Abstract

In this era, due to the widespread availability of digital devices, various open source and commercially available image editing tools have made authenticity of image contents questionable. Copy-move forgery (CMF) is a common technique to produce tampered images by concealing undesirable objects or replicating desirable objects in the same image. Therefore, means are required to authenticate image contents and identify the tampered areas. In this paper, a robust technique for CMF detection and localization in digital images is proposed. The technique extracts stationary wavelet transform (SWT) based features for exposing the forgeries in digital images. SWT is adopted because of its impressive localization properties, in both spectral and spatial domains. More specifically approximation subband of the stationary wavelet transform is utilized as this subband holds most of the information that is best suited for forgery detection. The dimension of the feature vectors is reduced by applying discrete cosine transform (DCT). To evaluate the proposed technique, we use two standard datasets namely, the CoMoFoD and the UCID for experimentations. The experimental results reveal that the proposed technique outperforms the existing techniques in terms of true and false detection rate. Consequently, the proposed forgery detection technique can be applied to detect the tampered areas and the benefits can be obtained in image forensic applications.

Key Words – Copy-move forgery; Tampered images; Forgery detection; Authenticity; Passive Authentication

1. Introduction

In this era, the users not only share many digital images in social media over the Internet but also in courtrooms as evidence, news reports, for insurance claims etc. The development of commercially available image editing tools are the basis of increasing use of digital images in our daily life. Ease of use of such tools has made manipulation of image contents easier. Image manipulation techniques can be classified as image steganography and image forgery. Both image steganography and image forgery manipulate an image but they differ from one another according to their practices [1-3]. Steganography manipulates a subject digital image for hiding secret information whereas image forgery changes the original semantic meaning of an image.

There have been a large number of steganographic techniques that utilize digital image for covert communication [4, 5]. At the same time, various steganalysis techniques have been devised to unveil secret messages in digital images [6]. The embedded data is restored during the authentication process by comparing the reference data. Thereafter, in the forensic investigation, the authenticated data is used to ensure the integrity of digital media whether forged or not [7]. Various existing stenographic tools have also been used to help forensic experts for the analysis of multimedia contents [8-10].

The tampering of digital images is very easy due to the accessibility of sophisticated and easy to use image manipulation and editing software. The tampered images can be used as a deceiving tool for hiding the