Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 9 (2014) 84 – 91

AASRI Procedia

www.elsevier.com/locate/procedia

2014 AASRI Conference on Circuit and Signal Processing (CSP 2014)

Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform

Mohammad Farukh Hashmi[a] *, Vijay Anand[b] , Avinas G. Keskar[c]

[a,b,c]*Department of Electronics Engineering, Visvesvaraya National Institute of Technology, Nagpur,440010, India.*

Abstract

In the present digital world, digital images and videos are the main carrier of information. However, these sources of information can be easily tampered by using readily available software thus making authenticity and integrity of the digital images an important issue of concern. And in most of the cases copy- move image forgery is used to tamper the digital images. Therefore, as a solution to the aforementioned problem we are going to propose a unique method for copy-move forgery detection which can sustained various pre-processing attacks using a combination of Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT). In this process first DyWT is applied on a given image to decompose it into four parts LL, LH, HL, and HH. Since LL part contains most of the information, we intended to apply SIFT on LL part only to extract the key features and find a descriptor vector of these key features and then find similarities between various descriptors vector to conclude that there has been some copy-move tampering done to the given image. And by using DyWT with SIFT we are able to extract more numbers of key points that are matched and thus able to detect copy-move forgery more efficiently.

Peer-review under responsibility of Scientific Committee of American Applied Science Research Institute

Keywords: Digital Image Forgery; DyWT (Dyadic Wavelet Transform); SIFT (Scale Invariant Feature Transfrom).

* Corresponding author: Mohammad Farukh Hashmi. Tel.: +91-712-280-1355.
E-mail address: farooq78699@gmail.com, vijjanand117@gmail.com,agkeskar@ece.vnit.ac.in.

Peer-review under responsibility of Scientific Committee of American Applied Science Research Institute
doi:10.1016/j.aasri.2014.09.015

1. Introduction

In this digital savvy world "seeing is no more believing". Most of the information is carried in a digital form especially in the form of either digital images or digital videos. Thus, they form the main stream of the information carrier. These sources can be manipulated very easily. In this paper, we will focus on image forgery, which has become a topic of serious concern. The image editing software such as Adobe Photoshop is readily available using which any given image can be easily doctored, which can lead to serious consequences, as these tampered images can be presented as a part of evidence in the court room leading to a wrong decision and creating the false belief in many real-world applications. Therefore the issue of authentication of the images has to be taken very seriously. Most of the forgery detection techniques are categorized into two major domains: intrusive/non-blind and non-intrusive/blind [1] as shown in the Fig.1

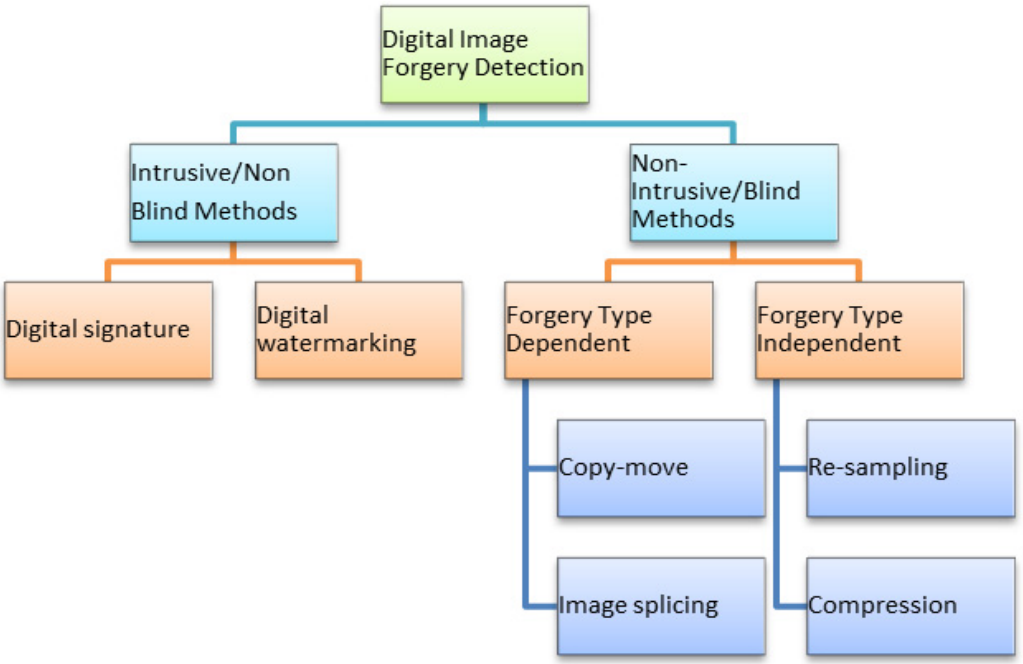

Fig.1. Classification of image forgery detection technique

Intrusive method which is also known as a non-blind method requires some digital information to be embedded in the original image when it is generated, and thus it has a limited scope. Some of the examples of these methods are watermarking and using digital signature of the camera and not all the digital devices can provide this feature. On the other hand, non-intrusive method which is also known as a blind method does not require any embedded information. A digital image is said to be forged when its original version is tampered by applying various transformations like that of rotation, scaling, resizing, etc. It may also happen that an image is tampered by adding noise or by removing or adding some objects to hide the real information [1]. Most commonly used image tampering method is copy-move image forgery in this a part of the original image is first copied and then pasted on other parts once or may be multiple times to hide some information.