IJCSI International Journal of Computer Science Issues, Volume 14, Issue 6, November 2017
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201706.17

Copy-Move Forgery Detection Based on Enhanced Patch-Match

Younis E. Abdalla[1], M. Tariq Iqbal[2] and M. Shehata[3]

[1] Faculty of Engineering and Applied Science, Memorial University of Newfoundland St. John's, Newfoundland A1B 2K6, Canada

[2] Faculty of Engineering and Applied Science, Memorial University of Newfoundland St. John's, Newfoundland A1B 2K6, Canada

[3] Faculty of Engineering and Applied Science, Memorial University of Newfoundland St. John's, Newfoundland A1B 2K6, Canada

Abstract

Image forgery detection approaches are varied and serve same objectives. However, the difference in image properties causes some limitations of most of these approaches. Integrate multiple forensic approaches to increase the efficiency of detecting and localize the forgery was proposed based on the same image input source. In this paper, we propose a new detector algorithm based on different image source format. We propose approach to detect a copy-move forgery based on PatchMatch enhanced by the dense field technique. The F-measure score used same evaluation function to make the system more robust. The output result shows high efficiency of detecting and localizing the forgery in different image formats, for passive forgery detection.

Keywords: *Copy-move detect; forgery localization; image forgery; score evaluation*

1. Introduction

One way to divide the professionals from the amateurs in any given field is to take a look at the equipment they use to accomplish their tasks. Advanced technology is currently the go-to equipment used by forgers via computer graphics and digital image processing. In fact, the use of digital imagery to create forgeries is one of the biggest problems emerging from the technology. However, experts working together with law enforcement are devising systems that employ advanced algorithms in order to ferret out the forgeries [1, 2]. What may be surprising to those not working in the field is that very few digital documents today (especially those produced from medical, legal and government sources) are entirely free of some aspect of forgery. Detecting forgery algorithms is possible but depends almost entirely on the image source. Digital photographs and documents are easily changed to suit the purposes of the user, with copy-move being the most popular approach to forgeries [3]. It is considered a type of passive forgery [4, 5] and is very widespread. Figure 1 below shows some different kinds of common forgeries [6].

One classic approach to digital image forgery is enhancing. This is the easiest approach and also is considered the least violating (that is, has the lowest repercussion if the forger is caught). To counteract these forgeries, active and passive detection mechanisms have been developed. In the active approach, digital watermarking or signatures are employed to make documentation more concise and genuine [6, 4].

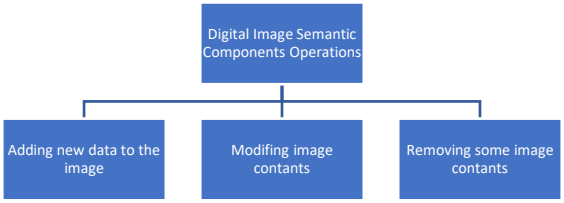

Fig. 1. Different types of forgeries.

The work is organized as follows. Following the introduction, we will provide an overview and revision of the algorithms used here. In the subsequent sections, we will delve deeper into the topics mentioned in the overview and also perform some tests to validate the methods.

2. Background

The history of forgery is as old as mankind. Throughout the centuries, it has primarily been used as a means to acquire access to power or money illegally [7]. Although this motivation persists, many cases of forgery today are focused instead on gaining access to systems for a variety of purposes. So, for instance, people engage in forgeries across fields as diverse as healthcare, surveillance, insurance, and even the media. To counteract forging activities, researchers are exploring algorithms as a means to detect image forgery. In the majority of the algorithms used thus far, lighting is analyzed to see whether or not copy-move forgery is present. During the forgery process, the image becomes "messy", and it is this "mess" that forgery detectors look for through the application of algorithms, as explained in [8]. The researchers in [8] also demonstrate how shadows can generate similar lighting artifacts within an image.

As touched on earlier, there are several different algorithm-based approaches for forgery detection, but the most popular techniques are block-based and feature-based. For block-based approaches, the detector needs access to the original image, whereas for feature-based strategies, the detector removes features by means of overlapping blocks