A Comparative Analysis on Three Duplication Elements in Copy-Move Forgery using PatchMatch-based Detection Method

Nur Izzati Nor Azaimi
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Johor, Malaysia
izzatiazaimi@gmail.com

Nor Bakiah Abd Warif, *IEEE Member*
Centre for Information Security Research, Faculty of Computer Science and Information Technology Universiti Tun Hussein Onn Malaysia
Johor, Malaysia
norbakiah@uthm.edu.my

Nor-Syahidatul N Ismail
Department of Computer System and Networking,
Faculty of Computing,
Universiti Malaysia Pahang Al-Sultan Abdullah,
Pekan, Pahang, Malaysia
nadiahismail@ump.edu.my

2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS) | 979-8-3503-1093-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSECS58457.2023.10256380

Abstract— **Image forgery is the alteration of a digital image to hide some of the important and useful information. Copy-move forgery (CMF) is one of the most difficult to detect because the copied part of the image has the same characteristics as the original image. Most of the existing datasets only highlight additional attacks in the copied part. Since there are no categories of duplication elements in the datasets, this research analyzed three categories of duplication elements in CMF which are animals, food and non-living things using DEFACTO and CoMo3Dataset. The analysis is performed on PatchMatch-based detection method and the results show that the method able to maintain at least 83% for all duplication elements in both DEFACTO and CoMo3Dataset. Furthermore, the method is able to detect a minimum 92% score for the food category in both datasets.**

Keywords—Copy-Move forgery, PatchMatch, DEFACTO, duplication regions

I. Introduction

Image forgery is a manipulation of the digital image to hide meaningful and useful information about the image. There are two types of image forgery: dependent and independent. Copy-move forgery (CMF) is a special type of image manipulation under dependent forgery in which a part of the image is copied and pasted elsewhere in the image to obscure an important image feature. Attacks including translation, rotation, scaling, and reflection may be added to the copied region to make the image even harder to detect. To detect the image, CMF detection methods are examined for their robustness not only against these attacks, but also Joint Photographic Experts Group (JPEG) compression, noise, and blur effects that occur after the copying process [1].

Many CMF datasets can be used for the evaluation of CMF detection. However, most of the dataset only categorized the image based on the attacks. No categories of duplication elements in the dataset, making it difficult for researchers to improve the CMF detection based on the duplication features. This research will focus on doing CMF detection based on the duplication elements categories other than CMF attacks.

This research will categorize three elements in duplication regions based on two existing datasets, specifically DEFACTO [2] and CoMo3Dataset. These categories are animals, food, and non-living things. The categories are selected based on the similarities of images in both datasets and categories of objects that people often see in their daily lives. The categories are then evaluated and compared using PatchMatch-based detection method [3]. PatchMatch is a randomized technique that finds matches of dense using approximate closest neighbors between image patches in a short amount of time. The objectives of this research are:

- To implement PatchMatch-based CMF detection method [3] on three categories of duplication elements in CMF dataset which are animal, food, and non-living things.
- To compare and analyze the results based on the categories.
- To identify the limitations of the PatchMatch-based CMF detection method based on the performance of the categories using F-score for pixel-level evaluation.

The rest of the paper is organized as follows: Section II explains the related work on CMF Detection. The explanation of the PatchMatch framework is given in Section III. The experiment results and discussions are presented in Section IV, and the conclusion is drawn in Section V.

II. RELATED WORK

A. *Image Forgery Detection*

To hide significant information in an image, people tend to apply image forgery. Image forgery detection is required to authenticate and to maintain the integrity of the image [1]. There are two types of approaches for image forgery detection: active approach and passive approach, as illustrated in Fig. 1.

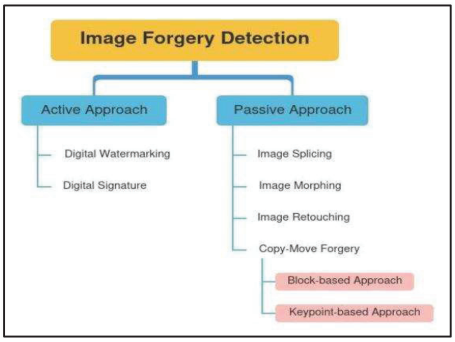

Fig. 1. A tree map of image forgery detection

1) *Active approach*

Active approach is an image authentication technique that uses the multimedia principle [4]. There are two types of active approaches in which a known authentication code is embedded in the image content before sending the images over an unreliable public channel. These types are Digital Watermarking and Digital Signature [5]. The concept of