Deep Learning on Digital Image Splicing Detection Using CFA Artifacts

Nadheer Younus Hussien, Benha University, Banha, Egypt
Rasha O. Mahmoud, Benha University, Banha, Egypt
Hala Helmi Zayed, Benha University, Banha, Egypt

ABSTRACT

Digital image forgery is a serious problem of an increasing attention from the research society. Image splicing is a well-known type of digital image forgery in which the forged image is synthesized from two or more images. Splicing forgery detection is more challenging when compared with other forgery types because the forged image does not contain any duplicated regions. In addition, unavailability of source images introduces no evidence about the forgery process. In this study, an automated image splicing forgery detection scheme is presented. It depends on extracting the feature of images based on the analysis of color filter array (CFA). A feature reduction process is performed using principal component analysis (PCA) to reduce the dimensionality of the resulting feature vectors. A deep belief network-based classifier is built and trained to classify the tested images as authentic or spliced images. The proposed scheme is evaluated through a set of experiments on Columbia Image Splicing Detection Evaluation Dataset (CISDED) under different scenarios including adding postprocessing on the spliced images such JPEG compression and Gaussian Noise. The obtained results reveal that the proposed scheme exhibits a promising performance with 95.05% precision, 94.05% recall, 94.05% true positive rate, and 98.197% accuracy. Moreover, the obtained results show the superiority of the proposed scheme compared to other recent splicing detection method.

KEYWORDS

Color Filter Array, Deep Belief Network, Deep Learning, Digital Image Forgery, Splicing Forgery

1. INTRODUCTION

The usage of images is increasing every day in modern societies. However, that role of images is only possible if the images’ contents can be trusted to be true (Zampoglou et al., 2017). Nowadays, digital images exist everywhere such as magazine covers, newspapers, in courtrooms as clues, and all over the pages of the World Wide Web (WWW) to be one of the popular ways of communication among people. Therefore, the motivation to make forged images increases simultaneously. In addition, the great advancements in digital images manipulation tools such as Photoshop simplified the forgery process and made it hard to be discovered (Qu et al., 2009). On the other side, image forgery detection techniques have been developed to check the integrity and authenticity of images (Pan et al., 2011).

Generally, there exist many kinds of digital images forgery techniques such as splicing forgery, copy-move forgery, retouching forgery, etc. However, splicing forgery detection is more challenging when compared with other forgery types because the forged image does not contain any duplicated regions. In addition, the absence of source images introduces no evidence about the forgery process.
Image splicing is one of the commonly adopted approaches to make forged images. As depicted in Figure 1, through copying parts from the original images and pasting them into a target image, the forger is able to build a synthesized scene to deceive others. With the help of the widely available image processing tools, even non-expert individual can easily create forged images based on the splicing approach. Although professional experts are still able to discover non-perfect forgeries, it is still a difficult matter to fully automate the process of forgery detection, particularly, when the splicing forgery is followed by post-processing step which may include blurring addition, noise addition, image compression, etc., to hide the clues of the forgery process (Zhan et al., 2016).

Many feature extraction approaches have been used in the different splicing forgery detection methods proposed in the literature. However, few works have benefited from the features based on color filter array interpolation which can be easily disrupted by the splicing process, yielding features that can be used effectively to differentiate between authentic and spliced images (Fernandez et al., 2018; Zampoglou et al., 2017). In addition, deep learning approach succeeded in solving many difficult problems in several fields such as computer vision, machine learning, and object recognition. Hence, it can play an effective role in building splicing forgery detection techniques. In this study, an automated splicing forgery detection scheme is introduced that benefits form the inconsistency of color filter array interpolation and the powerful classification ability of deep neural networks. The proposed method comprises three steps: image preprocessing in which a number of processes are done to prepare the images for the next step, feature extraction where a group of features are obtained via estimating the color filter array (CFA) patterns, and classification in which a deep belief network based classifier is built and trained to differentiate between authentic and spliced images. Intensive experiments are conducted to evaluate the performance of proposed method under different scenarios using a standard dataset. In addition, the performance of proposed method is evaluated in case of postprocessing such as noise and JPEG compression.

The rest of the study is structured as follow: Sec. 2 reviews some of the recently proposed splicing forgery detection methods. Sec. 3 presents the proposed splicing forgery detection scheme. Sec. 4 includes the implementation and experimentation. Finally, the study is concluded and recommendations for extending the proposed work are given in Sec. 5.

2. RELATED WORK

Numerous approaches have been proposed to automatically detect the image forgery process. An automated passive splicing forgery detection scheme was presented by Hsu et al. (Hsu et al., 2007). It depends on detecting the differences of the camera characteristics in different areas of a given image. The obtained results reveal that the suggested method has 70% precision and 70% recall.

Shi et al. (Shi et al., 2007) introduced another splicing forgery detection approach that employs a natural image model. The obtained results using the Columbia Image Splicing Detection Evaluation

Figure 1. Creating a forged image using splicing technique
DeLone & McLean IS Success Model in Evaluating Knowledge Transfer in a Virtual Learning Environment
www.igi-global.com/chapter/delone-mclean-success-model-evaluating/65005?camid=4v1a