Chapter 81
Copy–Move Forgery Localization Using Convolutional Neural Networks and CFA Features

Lu Liu

Institute of Information Science, Beijing Jiaotong University, Beijing, China

Yao Zhao

Institute of Information Science, Beijing Jiaotong University, Beijing, China

Rongrong Ni

Institute of Information Science, Beijing Jiaotong University, Beijing, China

Qi Tian

Department of Computer Science, University of Texas at San Antonio, San Antonio, US

ABSTRACT

This article describes how images could be forged using different techniques, and the most common forgery is copy-move forgery, in which a part of an image is duplicated and placed elsewhere in the same image. This article describes a convolutional neural network (CNN)-based method to accurately localize the tampered regions, which combines color filter array (CFA) features. The CFA interpolation algorithm introduces the correlation and consistency among the pixels, which can be easily destroyed by most image processing operations. The proposed CNN method can effectively distinguish the traces caused by copy-move forgeries and some post-processing operations. Additionally, it can utilize the classification result to guide the feature extraction, which can enhance the robustness of the learned features. This article, per the authors, tests the proposed method in several experiments. The results demonstrate the efficiency of the method on different forgeries and quantifies its robustness and sensitivity.
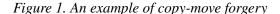
1. INTRODUCTION

As society develops, digital image plays a more and more important role in our daily life. Recently, digital image serves as carrier of information and medium of communication. A digital image not only can be used as evidences in court, but also can be used by doctors to diagnose the patients. In addition, digital images frequently occur in newspaper, magazine and television, which enable people to receive and understand information vividly.

With the development of image processing techniques, there are many tools, which can decorate an image easily without leaving obvious traces to the human eyes. Nowadays, people usually upload images that have been beautified to the Internet. It has brought a lot of benefits but has also brought some problems. Because not every image modification is performed for beauty, vicious tampering has forged realistic fake images. Once these manipulated images are maliciously used to mislead the public about the truth, it will be no doubt to seriously threaten stability and development of the society.

Copy-move forgery is one of the most common forgeries, where some parts of an image are copied and pasted to other parts of the same image. In order to harmonize the tampered regions with its surroundings, some other image processing operations, such as rotation, scaling, JPEG compression and blurring could be involved together with copy-move manipulation. Due to its effectiveness and simplicity, even a non-professional can deliberately tamper a digital image to obtain personal benefit or achieve personal intent. An example of copy-move forgery is shown in Figure 1, where a region was copied and pasted from the top right corner to the top left corner. This photo is tampered for beauty and variety. Even so, this is still not allowed in the photography competition. Actually, most images were tampered and were intended to hide an object in the image, or to emphasize a particular object. In consequence, it is urgent and important to research some methods to deal with the problem of authenticity and origin of digital images.

Figure 1. An example of copy-move forgery

To authenticate a digital image, many techniques have been developed. In general, these techniques can be divided into two types, active techniques and passive techniques. Active techniques usually use watermarks (Kundur & Hatzinakos, 1999) or digital signatures (Lu & Liao, 2003) as the authentication

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/copy-move-forgery-localization-using-convolutional-neural-networks-and-cfa-features/251498

Related Content

Securing the Supply Chain: Cybersecurity Strategies for Logistics Resilience
Siva Raja Sindiramutty, Chong Eng Tan, Wei Wei Goh, Sumathi Balakrishnan, Norhidayah Hamzahand Rehan Akbar (2024). *Navigating Cyber Threats and Cybersecurity in the Logistics Industry (pp. 300-365).*
www.irma-international.org/chapter/securing-the-supply-chain/341422

Supply Chain Management Security Issues and Challenges in the Context of AI Applications
Imdad Ali Shah, Raja Kumar Murugesanand Samina Rajper (2024). *Navigating Cyber Threats and Cybersecurity in the Logistics Industry (pp. 59-89).*
www.irma-international.org/chapter/supply-chain-management-security-issues-and-challenges-in-the-context-of-ai-applications/341413

Functioning of Terrorism
Dana Janbek (2019). *Violent Extremism: Breakthroughs in Research and Practice (pp. 1-14).*
www.irma-international.org/chapter/functioning-of-terrorism/213295

Challenges in Monitoring Cyberarms Compliance
Neil C. Rowe, Simson L. Garfinkel, Robert Beverlyand Panayotis Yannakogeorgos (2011). *International Journal of Cyber Warfare and Terrorism (pp. 35-48).*
www.irma-international.org/article/challenges-monitoring-cyberarms-compliance/64312

Cyber Counterintelligence: An Exploratory Proposition on a Conceptual Framework
Petrus Duvenage, Thenjiwe Sitholeand Basie von Solms (2019). *International Journal of Cyber Warfare and Terrorism (pp. 44-62).*
www.irma-international.org/article/cyber-counterintelligence/246333