International Journal of Rough Sets and Data Analysis
Volume 4 • Issue 2 • April-June 2017

Tradeoffs Between Forensics and Anti-Forensics of Digital Images

Priya Makarand Shelke, Smt. Kashibai Navale College of Engineering, Pune and Savitribai Phule Pune University, Pune, India

Rajesh Shardanand Prasad, Computer Engineering Department, NBN Sinhgad School of Engineering (Savitribai Phule Pune University), Pune, India

ABSTRACT

Over past few years, we are the spectators of the evolution in the field of information technology, telecommunication and networking. Due to the advancement of smart phones, easy and inexpensive access to the internet and popularity of social networking, capture and use of digital images has increased drastically. Image processing techniques are getting developed at rapidly and at the same time easy to use image tampering soft-wares are also getting readily available. If tampered images are misused, big troubles having deep moral, ethical and lawful allegations may arise. Due to high potential of visual media and the ease in their capture, distribution and storage, we rarely find a field where digital visual data is not used. The value of image as evidence of event must be carefully assessed and it is a call for from different fields of applications. Therefore, in this age of fantasy, image authentication has become an issue of utmost importance.

KEYWORDS

Compression, Conceal Ability, Detectability, Digital Forensics, Distortion

INTRODUCTION

Due to the advancement and easy availability of digital editing soft wares, creating the forged contents is not a big deal, today. Because of this, one must verify the contents before using it. As a consequence, several forensic techniques have developed to detect various types of forgeries (Popescu & Farid, 2005; Farid, 2001; Kirchner & Fridrich, 2010; Farid, 2009). Staring from acquisition to fruition, image undergoes many steps and a forger can attack at any step. But, most image altering operations leave behind distinct, traceable "fingerprints" in the form of image alteration artifacts. As these fingerprints solely belong to that step/operation in which they get introduced, specific assessment to catch them must be designed. Such fingerprints are clues for forensic agents. They reveal the traces of fingerprints and present it to prove the presence of image altering operation. In order to study the flaws and limitations of current forensic tools and increase their strength with respect to current attacks, an intelligent forger must design techniques able to conceal the significant footprints left by typical image processing operation. In effort to conceal the footprints, distortion may get introduce, which results in poor image quality. Poor image quality is a vital parameter used by the forensic agents to detect forgeries. Thus, a trade-off between image quality and detectability gets introduced. If quality is preferred, footprints can be revealed and image alteration gets detected. On the contrast, if footprints are concealed, image gets distorted and thus image alteration can be detected. The main challenge in front of anti-forensic agents is to balance this tradeoff between image quality conceal ability of fingerprints and its un-detectability by forensic agents.

DOI: 10.4018/IJRSDA.2017040107

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Compressing the multimedia signal for storage and transmission is quite common. Forgers also need to compresses their forgeries for the same purpose. During compression, a famous tradeoff between the compression ratio and distortion into the signal must be balanced. Therefore, in the case of compressing anti-forensically forged signal, compression ratio, image distortion and probability that the forgery is concealed are all linked. A forger must balance a tradeoff between all three of these quantities. In this paper, we review recent techniques proposed to reduce these tradeoffs and propose a framework for the same.

RELATED WORK

Examples of Image Tampering

Though photo manipulation has become more common in the age of digital cameras and image editing software, it actually dates back almost as far as the invention of photography. Gathered below is an overview of some of the more notable instances of photo manipulation in history. For recent years, an exhaustive inventory of every photo manipulation would be nearly impossible, so we focus here on the instances that have been most controversial or notorious, or ones that raise the most interesting ethical questions.

Photographs do not always tell the truth. In fact, the first image1 forgeries appeared a long time ago, probably several years after Joseph Nipce produced the first photograph in 1825. For example, an iconic portrait of the US President Abraham Lincoln taken around 1860 is actually a forged image: the head of President Lincoln is depicted on the body of another person (see Figure 1). However, in the early days of photography, it was not easy to create forged images because making forgeries at that time required specific physical and chemical equipment and skills (Using www.fourandsix.com).

Image tampering has a long history and many examples of image tampering became known. For example, in a photograph made in circa 1865, General Francis P. Blair was added into the original photograph (Figure 2-a). Due to the influence of photographs, they are often doctored because of political motives. Another example is shown in Figure 2-b, where Po Ku had been removed from the left most position of the original photograph, after he fell out of favor with Mao Tse Tung (Using www.fourandsix.com).

In this doctored photo of Queen Elizabeth Bowes-Lyon — mother of Queen Elizabeth II — and Canadian Prime Minister William Lyon Mackenzie King in Banff, Alberta, King George VI was removed from the original photograph. This photo was used on an election poster for the Prime Minister in 1939. It is hypothesized that the Prime Minister had the photo altered because a photo of just him and the Queen painted him in a more powerful light (Figure 2-c).

A World War II photo (Figure 2-d) published in the Russian magazine Ogoniok in 1945 shows several Russian soldiers raising the Soviet flag atop the German Reichstag building. At the request of the editor-in-chief of the magazine, the photo was altered prior to publication to remove what appeared to be a watch from the right arm of the solider supporting the flag-bearer. Though in reality the object on his right arm was most likely a compass, there was concern that viewers would conclude that he had watches on both wrists, and take that as evidence that he had been looting (Using www.fourandsix.com).

Shortly after the death of Nelson Mandela, Kenyan politician Mike Sonko posted on Facebook (in Dec 2013) an image of himself being embraced by the revered statesman. Commentors quickly spotted the sloppy compositing work, however, and someone ultimately found the original photo, in which Mandela was actually embracing boxer Muhammad Ali against a completely different

12 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/article/tradeoffs-between-forensics-and-anti-forensics-of-digital-images/178165

Related Content

A Cross Layer Spoofing Detection Mechanism for Multimedia Communication Services
Nikos Vrakasand Costas Lambrinoudakis (2011). *International Journal of Information Technologies and Systems Approach (pp. 32-47).*
www.irma-international.org/article/cross-layer-spoofing-detection-mechanism/55802

A QoS-Enhanced Model for Inter-Site Backup Operations in Cloud SDN
Ammar AlSousand Jorge Marx Gómez (2019). *International Journal of Information Technologies and Systems Approach (pp. 20-36).*
www.irma-international.org/article/a-qos-enhanced-model-for-inter-site-backup-operations-in-cloud-sdn/218856

Defining an Iterative ISO/IEC 29110 Deployment Package for Game Developers
Jussi Kasurinenand Kari Smolander (2017). *International Journal of Information Technologies and Systems Approach (pp. 107-125).*
www.irma-international.org/article/defining-an-iterative-isoiec-29110-deployment-package-for-game-developers/169770

A Systematic Review on Prediction Techniques for Cardiac Disease
Savita Wadhawanand Raman Maini (2022). *International Journal of Information Technologies and Systems Approach (pp. 1-33).*
www.irma-international.org/article/a-systematic-review-on-prediction-techniques-for-cardiac-disease/290001

The Use of ICT in Researcher Development
Sam Hopkins, Erin A. Hensleeand Dawn C. Duke (2019). *Enhancing the Role of ICT in Doctoral Research Processes (pp. 209-233).*
www.irma-international.org/chapter/the-use-of-ict-in-researcher-development/219940