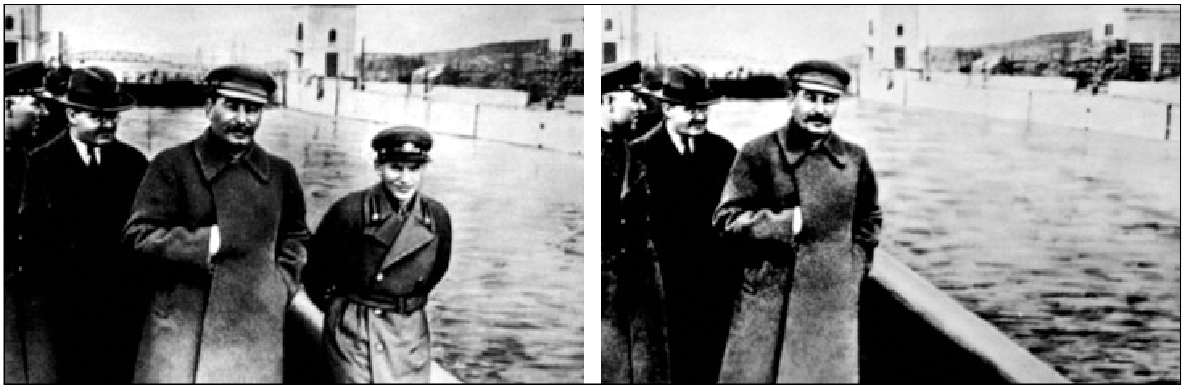
Chapter 1

Introduction

Stalin, Mao, Hitler, Mussolini, Castro, Brezhnev, and many others had photographs manipulated in an attempt to rewrite history. These men understood the power of photography and that if they changed photographs they could change history. In this photograph, for example, a commissar was removed from the original photograph after falling out of favor with Stalin.



Cumbersome and time-consuming darkroom techniques were required to alter the historical record on behalf of Stalin and others. Today, powerful and low-cost digital technology has made it far easier for nearly anyone to alter digital images. And the resulting fakes are often very difficult to detect. This photographic fakery is having a significant impact in many different areas of society.

Doctored photographs are appearing in tabloid and fashion magazines, government media, mainstream media, social media, on-line auctions sites, on-line dating sites, political ad campaigns, and scientific journals. The technology that can distort and manipulate digital media is developing at break-neck speeds, and it is imperative that the technology that can detect such alterations develop just as quickly. The field of photo forensics has emerged to restore some trust to photography. This book describes techniques that can be used to authenticate photos. These techniques can also be used to extract image information that might be useful in a forensic setting. Here are several examples of the applications for photo forensics:

Photo Tampering: A political candidate attempts to stir up controversy by creating a photographic composite showing her opponent sharing a stage with a controversial figure. Even if the composite is visually compelling, the creation of such a fake often leaves behind telltale clues. The goal of photo forensics is to exploit these clues. A common clue is a discrepancy in lighting direction. Two photos are rarely taken under identical lighting conditions, and an analysis of shadows, shading, and specularities can reveal lighting inconsistencies. Another clue emerges when one person in the composite photo is digitally enlarged or shrunk to fit the scene. An analysis of the pixel values in the composite may reveal traces of digital manipulation. Yet another clue is produced if the photos are taken with different quality cameras. In this case, differences in certain photo characteristics may reveal the existence and location of the inserted image. Chapters 2, 5, and 7 describe a variety of forensic techniques for detecting the inconsistencies that arise when some region of a photo has been digitally spliced, air-brushed, or altered.

Camera Ballistics: Analogous to gun ballistics, which links a bullet to a handgun using distinctive markings left by grooves in the handgun barrel, a photo may be linked to a specific digital camera because of distinctive digital markings left by the imaging device. JPEG images – by far the most common type of image – are packaged using a code that bears little resemblance to the pixels that we typically associate with an image. Different cameras use different versions of this code, and so the specific JPEG code can reveal the make and model of the camera that recorded the image. Moreover, when a digital image is opened and re-saved with photo-editing software, the original file formatting is likely to change. If the original file formatting is intact, this indicates that an image has not been altered after it was recorded. Even more precise than this JPEG technique, is a technique that exploits the slight imperfections that exist in every camera's electronic sensor. These imperfections vary from camera to camera and can be used to link a digital image to a single digital camera. Such links may allow, for example, a forensic examiner to demonstrate that pornographic images of children were taken with a particular camera. Parts of Chapter 5 and Chapter 6 describe forensic techniques for verifying and identifying the source of a digital image.

Counter-Forensics: To avoid detection, a clever forger might display a fake photo on a high quality monitor and then re-photograph it. The resulting image may still exhibit lighting inconsistencies, but it will foil forensic techniques that check for inconsistencies in the camera properties. However, this *re-capture* method of producing forgeries may introduce a new type of inconsistency. The camera settings, which are often stored alongside the image data, will be consistent with an indoor scene taken at close range.

The scene characteristics implied by the data may be in stark contrast to the contents of the photo. Parts of Chapters 3 and 4 describe forensic techniques for detecting, among other types of manipulations, re-captured images.

Enhance: In movies and television, scenes of digital forensic science usually involve someone exhorting an analyst to, “zoom and enhance that!”. Then, after some furious typing, the analyst leans back and the computer screen shows a handful of pixels miraculously resolving into a high-resolution image. Despite this clichéd and unrealistic depiction, modern forensic technique are capable of some forms of digital enhancement and 3-D analysis that may be useful to a forensic examiner. Chapter 3 describes several enhancement and analysis techniques.

Although growing quickly, the field of photo forensics is still in its infancy, and many of its applications have yet to be imagined. At their foundation, all current and future photo forensic techniques rely on a solid understanding of the imaging pipeline from the interaction of light with the physical 3-D world, the refraction of light as it passes through the camera lenses, the transformation of light to electrical signals in the camera sensor, and, finally, the conversion of electrical signals into a digital image file. This book is organized according to this pipeline, with each chapter describing a set of forensic techniques built on understanding and modeling some aspect of the imaging process.