Preface

In the beginning: I first got interested in the question of photo authenticity in the most unlikely of ways. Nearly twenty years ago, I was waiting in line at a library, when I noticed an enormous book on a cart. Out of idle curiosity, I picked the book up. It was the Federal Rules of Evidence, and thumbing through it I came across Article X. Contents of Writing, Recordings, and Photographs, Rule 1001. In the article is the statement that a photograph is admissible as evidence if it is an original. The rule seemed straightforward, until I read the definition of original:

> (d) An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout – or other output readable by sight – if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.

I was struck that the definition of "original" included such a vague statement as "... or other output readable by sight." At the time, the digital revolution was still in its early days, digital cameras were still a novelty, and photo-editing software like Adobe Photoshop was relatively primitive. Nevertheless, the trajectory of digital advances was clear and it seemed likely that such advances would greatly complicate the introduction of photographic evidence in a court of law.

A first idea: This led me to start thinking about how one might authenticate a digital image. I'm a little embarrassed to say that nearly two years passed before I had my first solid idea on how to tackle the question of photo authentication. I was goofing around in Photoshop splicing the head of a friend onto the body of another person. My friend's head was too small to fit on the body and so I had to increase its size. As I performed this simple operation, I realized that Photoshop must use some type of interpolation to fill in the missing pixels and this interpolation would introduce correlations between neighboring pixels (Section 7.3). A graduate student, Alin Popescu, and I found a way to quantify and detect these correlations, and we submitted this work for publication.

A reviewer of our paper made an insightful comment that provided the fodder for our second forensic technique. This second technique exploited the fact that digital cameras do not record all of the pixels needed to generate a complete 3-channel color image. Instead, cameras record a subset of the required pixels and fill in the rest by interpolating them from their neighboring recorded

pixels. This led us to realize that *every* digital image has a hidden but discoverable pattern of pixel correlations, and, further, that this pattern will be disturbed if something is added to or removed from the image (Section 5.1).

A controversial photo inspired our third forensic technique. The photo was a composite of then presidential hopeful Senator John Kerry and actress and anti-war activist Jane Fonda sharing a stage at an anti-war rally. This photo was intended to draw attention to Kerry's involvement in the anti-war movement following his service in Vietnam. The pattern of illumination on the faces of Kerry and Fonda seemed inconsistent with them sharing an outdoor stage. Verifying this inconsistency led Kimo Johnson and I to develop a series of forensic techniques for measuring the properties of the surrounding illumination to detect photo composites (Section 2.5).

An emerging picture: As we gained traction on the problem of photo authentication, we started to think about the entire imaging pipeline – the physics and geometry of the interaction of light with the physical 3-D world (Chapters 2 and 3), the way light passes through a camera lens (Chapter 4), the conversion of light to pixel values in the electronic sensor (Chapter 5), the packaging of these pixel values into a digital image file (Chapter 6), and the pixel-level artifacts introduced by photo-editing software (Chapter 7).

By carefully modeling the path of light during image creation, we discovered physical, geometric, and statistical regularities in images that are disrupted during the creation of a fake. This allowed us to develop a suite of photo forensic techniques, each based on characterizing part of the image formation process, quantifying the regularities that arise because of this process, and then detecting deviations from these expected regularities.

This book: This book provides the intuition and background, as well as the mathematical and algorithmic details needed to understand, implement, and utilize a variety of photo forensic techniques. I wrote this book for students, researchers, and practitioners interested in digital forensics. I assume a certain amount of basic mathematical background (calculus, linear algebra, and basic probability theory). I also assume some experience with digital image processing. If you are a bit rusty in these fields, you may find the material in Chapter 9 helpful.

Throughout this book I use both photographic and computer-generated images to illustrate various forensic techniques. The computer-generated images were created using a physically-based renderer that produces accurate facsimiles of real-world photographic images. Using the renderer allowed me to create images of uncluttered scenes viewed from an ideal vantage point.

Throughout this book I use images downloaded from Flickr in which the photographer gave permission for the re-use of their image. I have credited each such image with the photographer's Flickr user name.

The techniques described in this book were developed with the invaluable help of many wonderful students and colleagues: Giulia Boato, Mary Bravo, Tiago Carvalho, Valentina Conotter, Olivia Holmes, Kimo Johnson, Eric Kee, Siwei Lyu, James O'Brien, Senthil Periaswamy, Alin Popescu, Weihong Wang, Emily Whiting, and Jeffrey Woodward. This book was masterfully edited by Mary Bravo who imbued every sentence with her special brand of clarity and conciseness.

Words of advice: Lastly, I have a few words of advice for anyone who uses these forensic techniques in a law enforcement or legal setting: work carefully and slowly. Double-, triple-, quadruple-check your work. Do not allow preconceived notions to affect what should be a purely data-driven analysis. Understand and respect the assumptions required by an analysis. When you are unsure, refrain from drawing conclusions.