Chapter 1
What's in This Book and Why?

Husrev Taha Sencar, Luisa Verdoliva, and Nasir Memon

1.1 Introduction

Multimedia forensics is a societally important and technically challenging research area that will need significant effort for the foreseeable future. While the research community is growing and work like that in this book demonstrates significant progress, many challenges remain. We expect that forensically tackling ever-improving media acquisition and generation methods and countering the pace of change in media manipulation will continue to require significant technical breakthroughs in defensive technologies.

Whether performed at the individual level or class level attribution is at the heart of multimedia forensics. This form of passive forensic analysis exploits traces introduced by the acquisition or generation pipeline and subsequent editing. These traces are often subtle and invisible to humans but can be detected currently by analysis algorithms and provide mechanisms by which generation or manipulation can be automatically detected. Despite significant achievements in this area of research, advances in imaging technologies and newly introduced approaches to media synthesis have a strong potential to render existing forensic capabilities ineffective.

More critically, media manipulation has now become a pressing problem with broad implications. In the past, it required significant skill to create compelling manipulations because editing tools, such as Adobe Photoshop, required experienced users to alter images convincingly. Over the last several years, the rise of machine learning-based technologies has dramatically lowered the skill necessary to create

H. T. Sencar (✉)
Qatar Computing Research Institute, HBKU, Ar-Rayyan, Qatar
e-mail: hsencar@hbku.edu.qa

L. Verdoliva
University Federico II of Naples, Naples, Italy

N. Memon
New York University Tandon School of Engineering, New York, NY, USA

H. T. Sencar et al. (eds.), *Multimedia Forensics*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-981-16-7621-5_1

compelling manipulations. For example, Generative Adversarial Networks (GANs) can create photo-realistic faces with no skill by an end-user other than the ability to refresh a web page. Deepfake algorithms, such as autoencoders to swap faces in a video, can create manipulations much more easily than previous generation video tools. While these machine learning techniques have many positive uses, they have also been misused for darker purposes such as to perpetrate fraud, to create false personas, and to attack personal reputations.

The asymmetry in the operational setting of digital forensics where attackers have access to details and inner workings of the involved methods and tools and thereby have the freedom to tailor their actions makes the task even more difficult. It won't be surprising to see these advanced capabilities being deployed to counter forensic methods. Clearly, these are all pressing and important problems for which technical solutions must play a role.

There are a number of significant challenges that must be addressed by forensics community. Imaging technologies are constantly being improved by manufacturers at both hardware and software levels with little public information about their specifics. This implies a black-box access to these technologies and involves a significant reverse engineering effort on the part of researchers. With rapid advancements in computational imaging, this task will only get more strenuous.

Further, new manipulation techniques are becoming available at a rapid pace and each generation improves on the previous. As a result, defenders must develop ways to limit the a priori knowledge and training samples required from an attack algorithm and should assume an open world scenario where they might not have knowledge of all the attack algorithms. Meta-learning approaches for developing detection algorithms more quickly would also be highly beneficial. Manipulations in the wild are propagated via noisy channels, like social media, and so there is a need for robust detection technologies that are not fooled by launderings such as simple compression or more sophisticated replay attacks. Finally, part of the task of forensics is unwinding how the media was manipulated and who manipulated it. Consequently, approaches to understanding the provenance of manipulated media are necessary.

All of these challenges motivated us to prepare this book on multimedia forensics. Our main objective was to discuss new research directions and also present some possible solutions to existing problems. In this regard, this book provides a timely vehicle for showcasing important research that has emerged in the last years addressing media attribution, authenticity verification, and counter-forensics. We hope our content also sparks new research efforts in the fight against forgeries and misinformation.

1.2 Overviews

Our book begins with an overview of the challenges posed by media manipulation as seen from today. In their chapter, Hendrix and Morozoff provide a comprehensive view of all aspects of the problem to better emphasize the increasing need for advanced media forensics capabilities. This is followed by an examination of forensics challenges that arise from the increased adoption of computational imaging. The chapter by McCloskey assesses the ability to detect automated focus manipulations performed by computational cameras. For this, it looks at cues that can be used to distinguish optical blur from synthetic blur. The chapter also covers computational imaging research with potential future implications on forensics.

This chapter is followed by a series of chapters focusing on different dimensions of the attribution problem. Undoubtedly, one of the breakthrough discoveries in multimedia forensics is that *Photo-Response Non-Uniformity* (PRNU) of an imaging sensor, which manifests as a unique and permanent pattern introduced to all media captured by the sensor, can be used for identification and verification of the source of digital media. Our book has three chapters covering different aspects PRNU-based source camera attribution. The first chapter by Kirchner reviews the rich body of literature on camera identification from sensor noise fingerprints with an emphasis on still images from digital cameras and the evolving challenges in this domain. The second chapter by Sencar examines extension of these capabilities to video domain and outlines recently developed methods for estimating the sensor's PRNU from videos. The third chapter on this topic by Taspinar et al. provides an overview of techniques proposed to perform source matching efficiently in the presence of a large collection of media.

Another vertical in attribution domain is the source camera model identification problem. Assuming that a picture or video has been digitally acquired with a camera, the goal of this research direction is to identify the brand and model of the device used at acquisition time without relying on metadata. The chapter by Mandelli et al. investigates source camera model identification through pixel analysis and discusses wide series of methodologies proposed to solve this problem.

The remarkable progress of deep learning, in particular Generative Adversarial Networks (GANs), has led to the generation of extremely realistic fake facial content. The potential for misuse of such capabilities opens up new problem in forensics that focuses on identification of GAN fingerprints used in face image synthesis. Neves et al. provide an in-depth literature analysis of state-of-the-art detection approaches for face synthesis and manipulation as well as spoofing those detectors.

The next part of our book involves several chapters focusing on integrity and authenticity of multimedia. This part starts with a review of physics-based methods that mainly analyzes the interaction of light and objects and the geometric mapping of light and objects onto the image sensor. In his chapter, Reese reviews the major lines of research on physics-based methods and discusses their strengths and limitations.

The following chapter investigates forensic applications of the *Electric Network Frequency* (ENF) signal. Since ENF serves as an environmental signature captured by audio and video recordings made in locations where there is electrical activity, it provides an additional dimension for time–location authentication and for inferring the grid in which a recording was made. The chapter by Hajj-Ahmad et al. provides an overview of the increasing amount of research work that has been done in this field.

The long-lasting problem of image and video manipulation is revisited in the subsequent four chapters. However, distinct from conventional manipulation detection methods, Cozzolino et al. focus on the data-driven deep learning-based methods proposed in recent years. This chapter discusses in detail forensics traces these methods rely on, and describes architectural solutions used for detection and localization, together with the associated training strategies. The next chapter features the new class of forgery known as DeepFakes that involve impersonating audios and videos generated by deep neural networks. In this chapter, Lyu surveys the state-of-the-art DeepFake detection methods and evaluates solutions proposed to tackle this problem along with their pros and cons. In the third chapter of the topic, Long et al. provide an overview of the work related to video frame deletion and duplication and introduce deep learning-based approaches to tackle these two types of manipulations.

A complementary integrity verification approach is presented next. Several work demonstrated that media manipulation not only leaves forensic traces in the audiovisual content but also in the file structure. The chapter authored by Piva covers proposed forensic methods devoted to the analysis of image and video file formats to validate multimedia integrity.

The last chapter on authenticity verification introduces the problem of provenance analysis. By jointly examining multiple multimedia files, instead of making individual assessments, and evaluating pairwise relationships between them, the provenance of multimedia files is more reliably determined. The chapter by Moreira et al. addresses this problem by covering state-of-the-art analysis techniques.

The last part of our book includes two chapters on counter-forensics complementing the advances brought by deep learning to forensics. The advances brought by deep learning have also significantly expanded the capabilities of anti-forensic attackers. The first chapter by Barni et al. focuses on adversarial examples in image forensics and how they can be used in creation of attacks. It also describes possible countermeasures against them, and discusses their effectiveness. The other chapter by Stamm et al. focuses on emerging threat posed by GAN-based anti-forensic attacks in creating realistic, but completely synthetic forensic traces.