Edward Delp, Nasir Memon,
and Min Wu

Digital Forensics

Today we find ourselves in a digital world, where most information is created, captured, transmitted, stored, and processed in digital form. Digital information permeates every aspect of our daily lives. Although representing information in digital form has many compelling technical and economic advantages, it has led to new issues and significant challenges when performing forensics analysis of digital evidence. These challenges stem from the following facts:

- Digital data is an abstract representation of information. It is just a sequence of bits and has no overtly obvious properties that point to its authenticity or its origin.
- There is a very diverse collection of devices used to create and store digital information, including cameras, audio recorders, personal digital assistants, cell phones, and computers. Reliably extracting evidence from such devices is challenging. The problem gets much harder if the information is hidden, encrypted, or fragmented.
- Given the low cost of digital storage, the sheer amount of data that one is typically confronted with in a forensics scenario is voluminous. Sifting through large collections of digital data while looking for the right piece of evidence can be a challenging task.
- Digital evidence often traverses different channels and may be found scattered across multiple devices and in multiple formats. Connecting the needed pieces of evidence together into a meaningful reconstruction of events becomes difficult.
- Digital data is malleable. There is an abundance of readily available anti-forensics tools that can be used to mask or erase present digital evidence.
- Digital data can be volatile and often requires timely analysis.

[DIGITAL FORENSICS IS INHERENTLY A MULTIDISCIPLINARY SUBJECT INVOLVING COMPUTER SCIENCE AND ENGINEERING, SIGNAL PROCESSING, AND CRIMINAL JUSTICE.]

In response to these challenges, there has been a slow-growing body of scientific techniques for recovering evidence from digital data. These techniques have come to be loosely coupled under the umbrella title of digital forensics. Digital forensics can be defined as the collection of scientific techniques for the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, usually of a criminal nature. The last few years have seen much research in this young and emerging subject.

Digital forensics is inherently a multidisciplinary subject involving computer science and engineering, signal processing, and criminal justice, at the very least. However, work in this area has been very fragmented. This pair of special issues represents an effort by the Signal Processing Society and the Computer Society to bring the two communities together and understand each others' contributions to the field of digital forensics.

This *IEEE Signal Processing Magazine* special issue provides a comprehensive overview of recent developments and open problems in digital forensics that are amenable to signal processing techniques. The first article in the issue is by Hany Farid, one of the pioneers of image forensics. He presents a comprehensive survey of image forgery detection. Although his discussion is focused on images, many of the techniques are general and can apply with suitable modifications to video and audio.

Jessica Fridrich describes her breakthrough discovery of photoresponse nonuniformity noise that can be used to identify individual cameras. She explains how this remarkable technique can also be used for detecting image tampering.

In the third article, Ashwin Swaminathan, Min Wu, and K.J. Ray Liu give a tutorial on how forensic information about different components in an imaging device can be computed by suitable analysis of the images taken by the device. The article refers to this line of work as component forensics and discusses methods, applications, and theory related to these forensic analyses.

The fourth article by Tian-Tsong Ng and Shih-Fu Chang examines different techniques for differentiating synthetic images from real images. Given the increasing sophistication of graphically rendered imagery, it is becoming more and more difficult to make such differentiations by visual inspection. Ng and Chang provide a succinct

Digital Object Identifier 10.1109/MSP.2008.931089

tutorial on different analytical techniques that can be used for this differentiation.

The first four articles show how various assertions on source and integrity of images (and video) can be made based on suitable analysis techniques. In the fifth article, Anandrabata Pal and Nasir Memon explore a totally different subject that is well known in the computer science forensics community but requires tools from signal processing for an effective solution. They provide a tutorial on file carving, which involves recovering and reassembling a digital file from its fragments. They discuss the diferenproblems that need to be solved to carve files and show how effective signal processing techniques can be used to carve image files.

> ALTHOUGH REPRESENTING INFORMATION IN DIGITAL FORM HAS MANY COMPELLING TECHNICAL AND ECONOMIC ADVANTAGES, IT HAS LED TO NEW ISSUES AND SIGNIFICANT CHALLENGES WHEN PERFORMING FORENSICS ANALYSIS OF DIGITAL EVIDENCE.

The sixth article addresses forensics of printed and scanned documents by the team of researchers who have done seminal work in this area. Pei-Ju Chiang, Nitin Khanna, Aravind K. Mikkilineni, Maria V. Ortiz Segovia, Sungjoo Suh, Jan P. Allebach, George T.-C. Chiu, and Edward J. Delp present a comprehensive survey on forensics analysis of printed documents. They first provide a tutorial on modern printing and scanning devices and then show how individual printers and scanners can be potentially identified by the tell-tale marks they leave on documents.

Robert Maher's tutorial focuses on signal processing techniques for audio forensics.

The article by Joseph P. Campbell, Wade Shen, William M. Campbell, Reva Schwartz, Jean-François Bonastre, and Driss Matrouf focuses on progress in speaker recognition and shows the need for its cautious use on audio evidence in forensic applications.

The last article in this special issue deals with the practical but very challenging aspects of presenting evidence extracted using signal processing techniques in a court of law. Using many anecdotes from their personal experience, authors Jo Tibbitts and YiBin Lu discuss the challenges that technical researchers need to address to make their work effective when produced in a court of law.

We hope you enjoy the articles in this special issue of *IEEE Signal Processing Magazine*.