Dossier to Support the

# Application for Tenure and Promotion


Matthew C. Stamm

Assistant Professor
Dept. of Electrical and Computer Engineering
Drexel University
3141 Chestnut St.
Philadelphia, PA 19104

mstamm@drexel.edu

This document may be periodically updated.
The most current version can be found at:
http://misl.ece.drexel.edu/tenure-dossier/

# Contents


**1 Highlights** **1**

**2 Education, Professional Experience, and Awards** **2**
2.1 Education . . . 2
2.2 Professional Experience . . . 2
2.3 Awards . . . 3

**3 Research Activities** **4**
3.1 Deep Learning Techniques for Image Editing and Forgery Detection . . . 5
3.2 Image Source Camera Identification . . . 7
3.3 Anti-Forensics and Adversarial Dynamics . . . 9
3.4 Image Forensics Using Lateral Chromatic Aberration . . . 11
3.5 Targeted Image Editing and Processing Detection . . . 12
3.6 Fundamental Limits and Trade-offs in Multimedia Forensics and Anti-Forensics . . . 14
3.7 Online Monitoring and Anomaly Detection for Datacenters . . . 15

**4 Funding** **17**
4.1 Funded Proposals . . . 17
4.2 Funded Proposals as Senior Personnel . . . 17
4.3 Research Proposals Currently Under Review . . . 18
4.4 Declined Research Proposals . . . 18
4.5 White Papers . . . 19

**5 Publications, Invited Talks, and Other Scholarly Material** **21**
5.1 Publications . . . 21
5.1.1 Journal Publications . . . 21
5.1.2 Journal Publications Currently Under Review . . . 22
5.1.3 Journal Publications in Preparation . . . 22
5.1.4 Conference Publications . . . 23
5.2 Citations . . . 26
5.3 Patents . . . 28
5.4 Software . . . 28
5.5 Datasets . . . 29
5.6 Invited Talks and Presentations . . . 29

**6 Teaching and Student Advising Activities** **31**
6.1 Courses Taught . . . 31
6.2 New Courses Developed . . . 32
6.2.1 ECES 301: Transform Methods and Filtering . . . 33
6.2.2 ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security . . . 34
6.2.3 ECES T680: Forensic Signal Processing . . . 34
6.3 Student Course Evaluations & Comments . . . 35
6.4 Graduate Student Supervision . . . 37

6.5 Undegraduate Student Supervision . . . . . 38

**7 Service Activities** **40**
7.1 University and Departmental Service . . . . . 40
7.1.1 College and Departmental Committee Membership . . . . . 40
7.1.2 Candidacy Examination, Thesis Proposal, and Thesis Defense Committee Membership . . . . . 41
7.1.3 Additional University and Departmental Service Activities . . . . . 42
7.2 External Service . . . . . 44
7.2.1 Leadership and Organization Activities . . . . . 44
7.2.2 Reviewing Activites . . . . . 44

**8 Curriculum Vitae** **46**

**Appendix A Unsolicited Letter From A Student Praising My Teaching** **62**

**Appendix B Course Syllabi** **64**
B.1 ECES 301: Transform Methods and Filtering . . . . . 65
B.2 ECES 435: Recent Advances in DSP - Multimedia Signal Processing and Information Security . . . . . 70
B.3 ECES T680: Forensic Signal Processing . . . . . 74

**Appendix C Sample Publications** **78**

# 1 Tenure and Promotion Dossier Highlights – Dr. Matthew C. Stamm

**Research**

- Made significant contributions to the field of multimedia forensics - most recently for helping pioneer the use of deep learning techniques in image editing/forgery detection and source identification.
- Winner of the 2017 Drexel College of Engineering Outstanding Early Career Research Achievement Award.
- Authored or co-authored 50 published papers (12 journal, 38 conference) along with 2 journal papers that are currently under review and 6 journal papers with planned submission dates within 1-3 months.
- Publications cited 1505 times (*h*-index of 18).
- Developed forensic camera model identification software currently in use by at least six governmental agencies.

**Funding**

- Recipient of 5 externally funded research grants (4 as PI, 1 as Co-I) totaling $2,404,514.
- Winner of a 2016 NSF CAREER Award.
- Funded by several organziations including the National Science Foundation (NSF), Defense Advanced Projects Research Agency (DARPA), Army Research Office (ARO), the Defense Forensics and Biometrics Agency (DFBA), and the National Security Agency (NSA).

**Teaching**

- Developed three new courses: (1) ECES 301: Transform Methods & Filtering, (2) ECES 435: Recent Advances in DSP - Multimedia Signal Processing & Information Security, and (3) ECES T680: Forensic Signal Processing.
- Consistently received strong student evaluations; one student has sent an unsolicited letter to the Senior Vice Provost of Academic Affairs praising my teaching.
- Advisor of 5 Ph.D. students (one graduated), 1 incoming Ph.D. student, and 2 M.S. Students.

**University and Departmental Service**

- Served on 47 Ph.D. candidacy, Ph.D. thesis proposal, Ph.D. thesis defense, and M.S. thesis defense committees.
- Member of 5 different departmental and college level committees including the ECE Department Head Search Committee and the ECE Planning and Development Committee.
- Volunteer or speaker at several departmental events including open houses, Advisory Council meetings, and other outreach events.

**External Service**

- General Chair of the 2017 ACM Workshop on Information Hiding and Multimedia Security.
- Elected member of the IEEE Signal Processing Society's Information Forensics and Security Technical Committee.
- Lead Organizer of the 2018 IEEE Signal Processing Cup.
- Organized special sessions at two conferences (EUSIPCO 2018, SPIE EI 2015).
- Editorial Board Member of IEEE SigPort.
- Regularly serve as invited reviewer for several journals and TPC member for several major conferences.

# 2 Education, Professional Experience, and Awards

## 2.1 Education

**Ph.D. Electrical Engineering** 2012
University of Maryland, College Park
*Thesis: Digital Multimedia Forensics and Anti-Forensics*
*Advisor: K. J. Ray Liu*

**M.S. Electrical Engineering** 2011
University of Maryland, College Park
*Advisor: K. J. Ray Liu*

**B.S. Electrical Engineering** 2004
University of Maryland, College Park
*University Honors*

## 2.2 Professional Experience

**Assistant Professor** August 2013 – Present
*Department of Electrical and Computer Engineering*
*Drexel University, Philadelphia, PA*

**Co-Instructor** June 2013 – July 2013
*Cybersecurity Leadership Program*
*Robert H. Smith School of Business*
*University of Maryland, College Park, MD*

**Post-Doctoral Research Associate** June 2012 – May 2013
*Department of Electrical and Computer Engineering*
*University of Maryland, College Park, MD*
*Supervisor: K. J. Ray Liu*

**Graduate Research Assistant** May 2008 – May 2012,
*Department of Electrical and Computer Engineering* May 2007 – August 2007
*University of Maryland, College Park, MD*
*Supervisor: K. J. Ray Liu*

**Graduate Teaching Assistant** September 2005 – May 2008
*Department of Electrical and Computer Engineering*
*University of Maryland, College Park, MD*

**Radar Systems Engineer** June 2004 – September 2005,
*Johns Hopkins University Applied Physics Lab* June 2006 – August 2006

## 2.3 Awards

**Drexel CoE Outstanding Early-Career Research Achievement Award** (2017) – Awarded annually to one assistant professor within Drexel University's College of Engineering (CoE) for outstanding research accomplishments.

**NSF CAREER Award** (2016) – Awarded for the proposal "CAREER: Scaling Multimedia Forensic Algorithms for Big Data and Adversarial Environments."

**Dean's Doctoral Dissertation Award** (2012) – Awarded annually to one graduating doctoral student in the A. James Clark School of Engineering at the University of Maryland for outstanding doctoral research.

**Ann G. Wylie Dissertation Fellowship** (2011) – Awarded annually to 40 outstanding doctoral students throughout the entire University of Maryland in the final stages of their dissertation.

**Future Faculty Fellowship** (2010) – Awarded annually by the A. James Clark School of Engineering to twenty Ph.D. students who show potential towards earning a faculty position at a major research university.

**Distinguished Teaching Assistant Award** (2006) – Awarded by the Department of Electrical and Computer Engineering at the University of Maryland, College Park.

## 3 Research Activities

As a researcher, I believe it is important to identify and study emerging problems facing society. Because of this, I have focused my research on a new branch of information security known as multimedia forensics. Multimedia forensics involves the development of techniques to identify multimedia forgeries such as falsified images and videos. Furthermore, it seeks to ascertain important information such as a multimedia file's origin and processing history. This research is particularly important because widely available editing software enables multimedia forgers to create perceptually realistic forgeries. A good example of this is the famous falsified image shown below of a missile test launch released by the Iranian government in 2008. This image was manipulated to hide the fact that one of the missiles being tested did not in fact launch.

Figure 1: Left: A digital image forgery of a missile test launch released by the Iranian government. The falsified image regions are outlined. Right: The unaltered image used to create the forgery.

My research seeks to provide information verification and security in cases such as this when an information source cannot be trusted. To do this, I make use of the fact that digital editing operations leave behind statistical traces in the same way that a criminal leaves behind fingerprints at a crime scene. Additionally, I perform research on anti-forensics, i.e. techniques designed to fool forensic algorithms. The study of anti-forensics is critically important because it enables security researchers to identify vulnerabilities in existing forensic techniques that forgers may attempt to secretly exploit. It also facilitates the development of methods to detect the use of anti-forensics in a forgery.

I have made several significant contributions to the field of multimedia forensics. Most recently, I have been a key figure in the development of deep learning techniques for multimedia forensics. My research group and I have created the first convolutional neural network (CNN) capable of detecting a wide variety of image manipulations and one of the first CNNs capable of performing camera model identification. As part of the DARPA MediFor project, we have also recently published one of the first anti-forensic attacks capable of leveraging generative adversarial networks (GANs) to falsify forensic traces within an image.

My research contributions have been recognized by both Drexel University and by my research community. I was the **recipient of an NSF CAREER Award in 2016** and the **winner of Drexel's College of Engineering Outstanding Early-Career Research Achievement Award in 2017**. Additionally, I currently serve as an elected member of the IEEE Signal Processing Society's Technical Committee on Information Forensics and Security and was the General Chair of the 2017 ACM Workshop on Information Forensics and Security.

In addition to my primary research, I have also engaged collaborative research on online monitoring and anomaly detection for datacenters with Nagarajan Kandasamy and Harish Sethu of Drexel University's Dept. of Electrical and Computer Engineering.

A description of my research activities since joining Drexel, as well as a list of publications associated with each topic are provided below.

## 3.1 Deep Learning Techniques for Image Editing and Forgery Detection

| | | |
|---|---|---|
| Students | Belhassen Bayar | |
| | Owen Mayer | |
| | Luca Bondi (*Visiting Student*) | Politecnico di Milano, Milan, Italy |
| Research Funding | NSF CAREER Award | |
| Years Active | 2015 - Present | |

A key element in identifying image forgeries is to detect evidence of image editing and manipulation. In the past, researchers have developed algorithms to accomplish this by first identifying traces left by individual editing operations, statistically characterizing these traces, then developing detectors targeted towards a single manipulation or editing operation. While this approach has led to the development of several important forensic algorithms, it also has several critical drawbacks: identifying a forensic trace is both difficult and time consuming, and a new trace must be identified and an accompanying detector must be designed for each different editing operation.

To address these issues, my research group and I have developed a set of deep learning techniques for multimedia forensics capable of automatically learning editing traces and performing forgery detection. Central to this research has been our development of convolutional neural networks (CNNs) specifically designed for multimedia forensics. While CNNs used in other research areas such as computer vision are able to directly learn classification features from training data, these traditional CNNs have the potential to learn features that capture an image's content instead of forensic traces. To overcome this problem, we developed a new form of convolutional layer, known as a *constrained convolutional layer*, in order to build CNNs for multimedia forensics. This new layer is capable of jointly suppressing an image's content (which we want to prevent the classifier from learning) and extracting low-level forensic traces. Building upon this research, we have performed research to systematically examine design choices for both this and higher layers of our forensic CNNs in order to maximize their performance. Experimental evaluations of our editing detection CNNs demonstrate that they can detect multiple different editing operations with up to 99.97% accuracy and outperform existing editing detection algorithms. Furthermore, we have been able to design a forensic CNN capable of differentiating between sequences of multiple editing operations and determining the order in which these editing operations were used. We have also created a forensic CNN framework capable of estimating parameters associated with a particular editing operation that was used to modify an image (e.g. scaling factor for resizing, blur kernel variance for Gaussian blurring, quality factor for JPEG recompression, etc.).

Additionally, my research group and I have also developed a variety of forgery detection algo-

rithms and systems that exploit forensic feature extractors learned by our CNNs. One particularly important result is our development of a system to learn a *forensic similarity metric* that can be used to identify inconsistencies in an image's source and/or processing history. This system compares forensic traces in two different small windows of an image by using a pre-trained portion of our CNN as a deep feature extractor (deep features correspond to a vector of the neuron activation levels in a pre-specified fully connected layer of our CNN), then passes the deep feature vectors to a "Siamese network" that has been trained to produce a score indicating whether these image windows have undergone the same or different processing. Manipulated and falsified image regions can be exposed by using this system to assess the forensic similarity of all regions throughout an image, then identifying dissimilar (i.e. falsified) regions. In collaboration with a visiting scholar from Politecnico di Milano, we exploited this forensic similarity metric to developed a new method of precisely localizing falsified regions within an image and plan to submit our results for publication in the near future. Additionally, we have studied the transference of deep forensic features between multiple forensic tasks (such as editing detection and source identification) and developed an approach to learn transferable forensic feature extractors.

**Publications On This Topic**


[1] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, **[#2 Most accessed article in IEEE TIFS during June 2018]**.

[2] O. Mayer, B. Bayar, and M. C. Stamm, "Learning unified deep features for multimedia forensic tasks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Innsbruck, Austria, Jun. 2018.

[3] O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.

[4] B. Bayar and M. C. Stamm, "Towards order of processing operations detection in JPEG-compressed images with convolutional neural networks," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics*, Burlingame, CA, Feb. 2018, pp. 211–1–211–9.

[5] B. Bayar and M. C. Stamm, "A generic approach towards image manipulation parameter estimation using convolutional neural networks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 5–10.

[6] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in *accepted for publication in IEEE International Conference on Accoustics, Speech, and Signal Processing (ICASSP)*, New Orleans, LA, Mar. 2017, pp. 2152–2156.

[7] B. Bayar and M. C. Stamm, "Design principles of convolutional neural networks for multimedia forensics," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking,*

*Security, and Forensics - Special Session on Deep Learning for Multimedia Security*, San Francisco, CA, Feb. 2017, pp. 77–86.

[8] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Vigo, Galicia, Spain, 2016, pp. 5–10.

**Publications In Preparation On This Topic**

[1] O. Mayer and M. C. Stamm, "Deep learning based forensic similarity for digital images," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[2] L. Bondi, P. Bestagini, S. Tubaro, and M. C. Stamm, "A new approach for performing falsified image region identification and localization using deep forensic feature inconsistencies," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Oct. 2018.

## 3.2 Image Source Camera Identification

| | | |
|---|---|---|
| Collaborators | Nagarajan Kandasamy | Drexel University |
| Students | Chen Chen<br>Xinwei Zhao<br>Belhassen Bayar<br>Owen Mayer | |
| Research Funding | Defense Forensics & Biometrics Agency<br>Army Research Office<br>NSF CAREER Award | |
| Years Active | 2014 - Present | |

Since digital images can be easily modified and redistributed, their authenticity and true origin are often unclear. Determining information about an image's source, such as the model and manufacturer of the camera that captured it, is an important task in multimedia forensics. This information can be used as evidence in criminal investigations and legal proceedings, or to verify the trustworthiness of information used in news reporting or strategic decision making. While information such as metadata can be easily falsified, forensic traces that can reveal an image's source are left in an image by both algorithmic and physical components inside the camera that captured it.

My research group and I have developed a broad set of algorithms capable of forensically determining an image's source camera model. Furthermore, we have adapted these algorithms to operate in realistic and challenging scenarios such as when an image is post-processed or when the set of all possible sources is unknown. **A software tool that we have built, named the *Source Camera***

***Model Identification Tool*, is currently in use by at least six government agencies**[1] including the Defense Forensic Science Center (DFSC), National Media Exploitation Center (NMEC), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Air Force Office of Scientific Research (AFOSR), and other governmental agencies.

Recently, we proposed one of the first forensic CNNs capable of performing camera model identification. Unlike classical camera model identification approaches which typically capture a forensic trace left by a single component inside a camera, our CNN is able to adaptively learn traces left cumulatively by the camera's internal processing pipeline. This has led to a camera model identification system that is able to identify an image's source camera model with greater than 98% accuracy. We have developed techniques to construct and train forensic CNNs such that they are robust to two of the most common post-processing operations: JPEG compression and image resizing. This is particularly important because both operations are known to be very forensically destructive (i.e. they can significantly degrade a forensic algorithm's ability to correctly identify an image's source) and they commonly applied to images when they are shared via social media. We have also developed a system that is capable of determining which social network an image was posted to, and is capable of determining if that image was reposted from a different social network.

Prior to our development of deep learning based methods, we developed several other approaches for performing forensic camera model identification. Many of these approaches relied on traces left by a camera's demosaicing algorithm, i.e. the process by which a camera converts the partially sampled color channels that are read directly off its imaging sensor into a full color image. In one approach, we capture these traces by grouping together a set of non-parameteric trace submodels designed to capture partial information of a camera's demosaicing traces. By enforcing diversity among these submodels, we are able to form a feature set that provides comprehensive representation of a camera's demosaicing algorithm. We then use an ensemble classifier to mine this large feature set for for good classification features and perform camera model identification. This approach can identify the correct make and model of an image's source camera with an average accuracy of 99.2%. In another approach, we developed a computationally efficient technique to compute a parametric estimate of a camera's demosaicing filter, then used these model parameters as camera model identification features. This algorithm is able to reach a target classification accuracy at a much lower computational cost than other algorithms that utilize similar features.

### Publications On This Topic


[1] B. Bayar and M. C. Stamm, "Accurate and robust source camera model identification via constrained convolutional neural networks," *currently under review in IEEE Transactions on Information Forensics and Security*, submitted Aug. 2018.

[2] B. Bayar and M. C. Stamm, "Towards open set camera model identification using a deep learning framework," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.


[1] This information can be verified by Dr. Stamm's PI on this project. Contact information can be provided upon request.

[3] O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.

[4] B. Bayar and M. C. Stamm, "Augmented convolutional feature maps for robust cnn-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4098–4102.

[5] C. Chen and M. C. Stamm, "Image filter identification using demosaicing residual features," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4103–4107.

[6] B. Bayar and M. C. Stamm, "Design principles of convolutional neural networks for multimedia forensics," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics - Special Session on Deep Learning for Multimedia Security*, San Francisco, CA, Feb. 2017, pp. 77–86.

[7] X. Zhao and M. C. Stamm, "Computationally efficient demosaicing filter estimation for forensic camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Sep. 2016, pp. 151–155.

[8] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Rome, Italy, Nov. 2015, pp. 1–6.

**Publications In Preparation On This Topic**

[1] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

## 3.3 Anti-Forensics and Adversarial Dynamics

| | |
|---|---|
| Students | Chen Chen<br>Xinwei Zhao<br>Owen Mayer |
| Research Funding | NSF CAREER AWARD<br>Defense Advanced Research Projects Agency (DARPA) |
| Years Active | 2014 - Present |

While forensic algorithms provide a variety of information security tools to authenticate multimedia content, an adversarial forger can devise *anti-forensic attacks* to disguise evidence of their forgeries or falsify an image's source. Furthermore, an intelligent forger will attempt to keep their anti-forensic capabilities secret so that vulnerabilities in forensic algorithms remain unknown. In

order to characterize and study a forger's anti-forensic capabilities, we have developed several new anti-forensic attacks that a forger may employ. Additionally, since anti-forensic attacks are processing operations, they can behind traces just like the editing operations they are designed to hide. My research group and I have examined several anti-forensic algorithms and developed new techniques to detect these anti-forensic attacks.

We have recently developed a series of anti-forensic attacks using tools from deep learning known as generative adversarial networks (GANs). GANs are a deep learning framework in which a two individual deep neural networks, a generator and a discriminator, are trained in a competing fashion. The generator tries to mimic the statistical distribution of training data while the discriminator tries to differentiate generated data from real data.

By altering the traditional GAN structure, we are able to train generators to anti-forensically remove traces of editing from an image as well as falsify forensic traces linked to an image's source camera model. To accomplish this, we integrate a trained forensic detector into the GAN training loop and create a new loss function that penalizes the generator if it is unable to fool the forensic classifier and the discriminator as well as if it introduces distortion into the attacked image. Our results show that we are able to fool sophisticated forensic algorithms designed to identify an image's source camera and algorithms designed to detect editing without introducing visually perceptible distortion into the attacked image.

We have also developed a set of techniques capable of detecting certain anti-forensic attacks. Many forensic algorithms have been developed to determine the model of an image's source camera by examining traces left by the camera's demosaicing algorithm. An anti-forensic attacker, however, can falsify these traces by maliciously using existing forensic techniques to estimate one camera's demosaicing filter, then use these estimates to re-demosaic an image captured by a different camera. We developed a new method to detect if an images source camera model has been anti-forensically attacked in this manner by characterizing the different content-independent local pixel relationships that are introduced by both authentic demosaicing algorithms and anti-forensic attacks. In separate work, we developed an attack to remove lateral chromatic aberration inconsistencies that can be used to expose cut-and-paste forgeries. We later showed that this attack can be detected by exploiting resizing differences between color channels which are induced by LCA anti-forensics and creating a set of features capable of quantitatively capturing these differences.

**Publications On This Topic**


[1] C. Chen, X. Zhao, and M. C. Stamm, "MISLGAN: An anti-forensic camera model falsification framework using a generative adversarial network," in *IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, Sep. 2018.

[2] M. Barni, M. C. Stamm, and B. Tondi, "Adversarial multimedia forensics: Overview and challenges ahead," in *European Signal Processing Conference (EUSIPCO)*, Rome, Italy, Sep. 2018.

[3] C. Chen, X. Zhao, and M. C. Stamm, "Detecting anti-forensic attacks on demosaicing-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 1512–1516.

[4] O. Mayer and M. C. Stamm, "Countering anti-forensics of lateral chromatic aberration," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 15–20.

[5] O. Mayer and M. C. Stamm, "Anti-forensics of chromatic aberration," in *Proc. IS&T SPIE Electronic Imaging, Media Watermarking, Security, and Forensics*, San Francisco, CA, Feb. 2015, pp. 94 090M–94 090M.

**Publications In Preparation On This Topic**

[1] X. Zhao, C. Chen, and M. C. Stamm, "Anti-forensically falsifying an image's processing history using a generative adversarial network," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[2] X. Zhao, C. Chen, and M. C. Stamm, "A generative adversarial network based attack to falsify an image's source camera model," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. / Sep. 2018.

## 3.4 Image Forensics Using Lateral Chromatic Aberration

| | |
|---|---|
| Students | Owen Mayer |
| Research Funding | NSF CAREER Award |
| Years Active | 2014 - Present |

Lateral chromatic aberration (LCA) is a form of color distortion in digital images that occurs due to a lens's inability to focus all wavelengths of light on the same point on the imaging sensor. In copy-and-paste image forgeries, where image content is copied from one image and pasted into another, inconsistencies in an imaging feature called lateral chromatic aberration (LCA) are intrinsically introduced.

We developed a new method to detecting cut-and-paste forgeries by identifying LCA inconsistencies. To do this, we developed a statistical model that captures the inconsistency between global and local estimates of LCA. We then used this model to pose forgery detection as a hypothesis testing problem and derive a detection statistic, which we show is optimal when certain conditions are met. This algorithm significantly outperforms existing LCA-based forgery detection algorithms. It also is able to detect forgeries in challenging scenarios where other algorithms fail, specifically when content is falsified by moving it radially inward or outward from the image's optical center. Additionally, to overcome the high computational cost of existing LCA estimation approaches, we developed a new and computationally efficient LCA estimation algorithm. To accomplish this we adapted a block matching algorithm, called diamond search, to efficiently measure the LCA in a localized region. Our improved LCA estimation algorithm reduces estimation time by two orders of magnitude without introducing additional estimation error.

We have also examined anti-forensic attacks to falsify LCA and defenses to detect these attacks. We created a new anti-forensic attack that demonstrates that an attacker can anti-forensically remove LCA inconsistencies that arise from cut-and-paste attacks. This attack operates by estimating the expected lateral chromatic aberration at an image location, then removing deviations from this estimate by independently geometrically distorting each color channel. We later developed an algorithm to detect anti-forensic attacks on LCA by identifying inconsistent resampling traces in an image's color channels that are introduced when LCA is falsified.

**Publications On This Topic**


[1] O. Mayer and M. C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762–1777, Jul. 2018.

[2] O. Mayer and M. C. Stamm, "Countering anti-forensics of lateral chromatic aberration," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 15–20.

[3] O. Mayer and M. C. Stamm, "Improved forgery detection with lateral chromatic aberration," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, Mar. 2016, pp. 2024–2028.

[4] O. Mayer and M. C. Stamm, "Anti-forensics of chromatic aberration," in *Proc. IS&T SPIE Electronic Imaging, Media Watermarking, Security, and Forensics*, San Francisco, CA, Feb. 2015, pp. 94 090M–94 090M.


## 3.5 Targeted Image Editing and Processing Detection

| | | |
|---|---|---|
| Collaborators | K. J. Ray Liu | University of Maryland, College Park |
| | Xiangui Kang | Sun Yat-Sen University, China |
| | Xiaoyu Chu | University of Maryland, College Park |
| Years Active | 2013 - 2015 | |

Different editing and processing operations typically introduce unique traces into an image. Prior to the development of deep learning techniques capable of automatically learning these traces, we identified the traces left by several different editing and processing operations through theoretical analysis. Using these traces, we formulated forensic algorithms targeted at specifically detecting each of these operations.

One editing operation that has received significant attention is median filtering, due to its ability to perform image smoothing as well as its use in many anti-forensic attacks. We developed a new median filtering detection algorithm capable of reliably operating when an image is JPEG compressed and when small image patches are independently analyzed - two scenarios that are problematic for previous median filtering detection algorithms. Our algorithm operates by building detection features an using an autoregressive model to capture statistical properties of an image's

median filter residual, which we define as the difference between an image in question and a median filtered version of itself. Our results show that our proposed forensic technique can achieve important performance gains over previous methods, particularly at low false-positive rates, with a very small dimension of features.

While several forensic techniques have been developed to detect individual editing operations, identifying a sequence of editing is a much more challenging task. This is made more difficult because some editing operations will alter the traces left by other operations that were previously applied to an image. We developed a framework to detect both the set of editing operations applied to an image as well as the order in which these operations were applied. This is important because it not only provides greater insight into a signal's processing history, but it can also be used to determine a forger's behavior patterns or provide insight into who manipulated a signal. To accomplish this, we introduced the notion of a conditional fingerprint to describe how an editing operation's fingerprints can change under subsequent processing. We identified the conditional fingerprints of contrast enhancement followed by resizing, and used our framework to develop an algorithm to determine the order in which resizing and contrast enhancement were applied to an image.

Additionally, identifying how a signal was acquired is an important forensic problem. Prior to our research, no forensic techniques were developed to determine if a signal was compressively sensed. We identified forensic traces left specifically by compressive sensing and developed two different algorithms to detect these traces in generic signals. Because compressive sensing traces appear very similar to traditional image compression traces, we developed a targeted detector designed specifically for use in images. In addition, we developed a technique to forensically estimate the number of compressive measurements used to acquire a signal.

**Publications On This Topic**


[1] X. Chu, M. C. Stamm, and K. J. R. Liu, "Compressive sensing forensics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1416–1431, Jul. 2015.

[2] M. C. Stamm, X. Chu, and K. J. R. Liu, "Forensically determining the order of signal processing operations," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Guangzhou, China, Nov. 2013, pp. 162–167.

[3] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1456–1468, Sep. 2013.

## 3.6 Fundamental Limits and Trade-offs in Multimedia Forensics and Anti-Forensics

| | | |
|---|---|---|
| Collaborators | K. J. Ray Liu | University of Maryland, College Park |
| | Xiaoyu Chu | University of Maryland, College Park |
| | Yan Chen | University of Maryland, College Park |
| Years Active | 2013 - 2016 | |

As the field of forensics continues to progress, questions have begun to arise regarding the existance of fundamental limits on the amount of information that can be forensically extracted from a signal. To address this question, we developed an information theoretical framework for identifying the number of manipulations and processing operations that can be detected by forensic algorithms. Within this framework, we proposed the concept of "forensicability" as mutual information between a forensic trace and a set of hypotheses about the operations that a signal has processed by. Building off this idea, our framework seeks to identify the error probability lower bound of forensic algorithms that make use of a particular forensic trace, and to identify the maximum number of hypotheses that can theoretically be distinguished between using a trace.

Similarly, we developed theoretical approaches to identify and characterize fundamental trade-offs present in anti-forensic attacks. We used these to study anti-forensic attacks on an image's compression history. These anti-forensic attacks have been developed to conceal compression-based evidence of image manipulation and of an its true origin.However, when anti-forensic techniques are applied to multimedia content, distortion may be introduced, or the data size may be increased. As a result, a trade-off between three factors exists when compressing an anti-forensically modified forgery: (1) the degree to which manipulation fingerprints can be forensically concealed, (2) the data rate, and (3) the distortion introduced. We characterized this trade-off by defining concealability and using it to measure the effectiveness of an anti-forensic attack. Then, to demonstrate this tradeoff in a realistic scenario, we examined the concealability-rate-distortion tradeoff in double JPEG compression antiforensics. To evaluate this tradeoff, we developed flexible anti-forensic dither as an attack that enables a forger to vary the strength of their anti-forensic attack. Through simulation, we identified two surprising results. One is that if a forger uses a lower quality factor in the second compression, applying anti-forensics can both increase concealability and decrease the data rate. The other is that for any pairing of concealability and distortion values, achieved using a higher secondary quality factor, can also be achieved using a lower secondary quality factor at a lower data rate. As a result, the forger has an incentive to always recompress using a lower secondary quality factor.

### Publications On This Topic

[1] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of media forensics: The forensicability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 774–788, Apr. 2016.

[2] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "On antiforensic concealability with rate-distortion tradeoff," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1087–1100, Mar. 2015.

[3] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of compression forensics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014, pp. 2689–2693.

## 3.7 Online Monitoring and Anomaly Detection for Datacenters

| | | |
|---|---|---|
| Collaborators | Nagarajan Kandasamy | Drexel University |
| | Harish Sethu | Drexel University |
| Students | Tingshan Huang | |
| | Salvador DeCelles | |
| Years Active | 2014 - Present | |

Performance monitoring of datacenters provides vital information for dynamic resource provisioning, anomaly detection, capacity planning, and metering decisions. Online monitoring, however, incurs a variety of costs: the very act of monitoring a system interferes with its performance, consuming network bandwidth and disk space. We have developed a variety of strategies aimed at reducing the computational and communication costs associated with performing online monitoring and anomaly detection for datacenters.

One approach exploits the fact that the signals of interest often can be sparsified under an appropriate representation basis and that the sampling rate can be tuned as a function of sparsity. We developed a basis selection algorithm called Best Basis that automatically adapts the representation basis to the structure of the underlying signal being sampled such that the information can be most concisely represented. Using the Best Basis algorithm, we developed a strategy that takes advantage of signal compressibility to reduce the data transfer and storage costs associated with online monitoring. Additionally, we developed adaptive rate compressive sampling where the key idea is to dynamically tune the sampling rate as the signal sparsity changes: in time windows where the signal is sparse we reduce the sampling rate and in windows where the signal is less concise the rate is increased, all the while ensuring that the chosen sampling rate guarantees a user- defined signal recovery quality.

We used the Trade6 application as our experimental platform and measure the signals of interest – in our case, signals pertaining to memory and disk I/O activity – using both of our adaptive sampling strategies. We then evaluated whether the reconstructed signals can be used for trend detection to track the gradual deterioration of system performance associated with software aging. Our experiments show that the signals recovered by our methods can be used to detect the existence of trends within the original signal with high confidence and that performance bottlenecks and anomalies that manifest themselves in portions of the signal where its magnitude exceeds a threshold value can also be detected. Most importantly, detection of these anomalies is achieved using a substantially reduced sample size – a reduction of more than 70% when compared to the

standard fixed-rate sampling method.

In a second approach, we developed a strategy based on exploiting the underlying structure of the signal being monitored to sparsify it prior to transmission to a monitoring station for analysis and logging. Specifically, predictive models are designed to estimate the signals of interest. These models are then used to obtain prediction errors, i.e. the error between the signal and the corresponding estimate, that are then treated as a sparse representation of the original signal while retaining key information. This transformation allows for far less data to be transmitted to the monitoring station, at which point the signal is reconstructed by simply using the prediction errors. We have shown that classical techniques such as principal component analysis (PCA) can be applied to the reconstructed signal for anomaly detection. Experimental results using the Trade6 and RuBBoS benchmarks indicate a significant reduction in overall transmission costs - greater that 95% in some cases - while retaining sufficient detection accuracy.

**Publications On This Topic**


[1] S. DeCelles, B. Bayar, M. C. Stamm, and N. Kandasamy, "Data reduction, compressed sampling, and recovery for online performance monitoring," *currently under review in IEEE Transactions on Network Service Management*, submitted Aug. 2018.

[2] S. DeCelles, , T. Huang, M. C. Stamm, and N. Kandasamy, "Detecting incipient faults in software systems: A compressed sampling-based approach," in *IEEE International Conference on Cloud Computing (CLOUD)* ***(15% acceptance rate)***, Jun. 2016, pp. 303–310.

[3] T. Huang, N. Kandasamy, H. Sethu, and M. C. Stamm, "An efficient strategy for online performance monitoring of datacenters via adaptive sampling," *IEEE Transactions on Cloud Computing*, Accepted and published on IEEEXplore in 2016, To appear in print.

[4] S. DeCelles, M. C. Stamm, and N. Kandasamy, "Efficient online performance monitoring of computing systems using predictive models," in *IEEE/ACM International Conference on Utility and Cloud Computing (UCC)* ***(27.5% acceptance rate)***, Limassol, Cyprus, Dec. 2015, pp. 152–161.

# 4 Funding

During my time as an Assistant Professor, I have secured more than **$2.4 million in external funding**.

I am the **Principal Investigator (PI) on four grants** totaling $2,149,085 including an **NSF CAREER Award** and a Co-Investigator on a fifth grant. In addition to my funding from the National Science Foundation (NSF), my work has also been funded by the Defense Advanced Research Projects Agency (DARPA), the Army Research Office (ARO), the Defense Forensics and Biometrics Agency (DFBA), and the National Security Agency (NSA).

In addition to my existing funding, I have also been selected as a finalist for an award from the 2018 Drexel Ventures Innovation Fund and expect to hear news of a funding decision by the end of the summer.

## 4.1 Funded Proposals - $2,404,514

[1] M. C. Stamm (PI), J. Shackleford, and N. Kandasamy, "High performance techniques to identify the source and authenticity of digital videos using multimedia forensics," *Army Research Office (ARO)*, July 1, 2017 – June 30, 2019,
Funded Amount: **$648,572**.

[2] S. Weber (PI), M. C. Stamm, and K. Dandekar, "Security by design: Drexel hands-on cybersecurity laboratory curriculum expansion," *National Security Agency (NSA)*, October 1, 2017 – September 30, 2018,
Funded Amount: **$255,429**.

[3] M. C. Stamm (Drexel University PI), with M. Kozak (PI - PAR Government), B. Klare (Rank One Computing), C. Sisson (Rochester Institute of Technology), and J. Corso (University of Michigan), "Project MediSphere," *Defense Advanced Research Projects Agency (DARPA) - MediFor Program*, May 2016 – February 2019,
Funded Amount: **$541,996.84** (Amount Awarded to Stamm/Drexel).

[4] M. C. Stamm (PI), "CAREER: Scaling multimedia forensic algorithms for big data and adversarial environments," *National Science Foundation – Faculty Early Career Development Program (NSF CAREER)*, March 2016 – February 2021,
Funded Amount: **$583,578**.

[5] M. C. Stamm (PI) and N. Kandasamy, "High performance techniques to identify source of digital images using multimedia forensics," *Defense Forensics & Biometrics Agency (DFBA) and Army Research Office (ARO)*, Feb. 1, 2015 – July 31, 2016,
Funded Amount: **$374,939**.

## 4.2 Funded Proposals as Senior Personnel - $206,165

[1] S. Weber (PI), C. Carroll, Senior Personnel: M. C. Stamm (SP), I. Savidis (SP), and K. Dandekar (SP), "Drexel cybersecurity for soldiers program (DCSP)," *National Security Agency*

*(NSA) and Army Research Office (ARO)*, Feb. 1, 2015 – July 31, 2016,
Funded Amount: **$206,165**.

## 4.3 Research Proposals Currently Under Review

[1] M. C. Stamm, "Seeing is believing - An image and video forgery detection software tool," *Drexel Ventures Innovation Fund*, September 2018 – August 2019, $99,780, Status: Selected as finalist, Final evaluation ongoing.

## 4.4 Declined Research Proposals

[1] N. Kandasamy (PI), H. Sethu, M. C. Stamm, and S. Weber, "SaTC: CORE: Medium: Dimensionality reduction techniques for online performance monitoring and anomaly detection," *National Science Foundation*, May 2017 – April 2021, $984,398.

[2] M. C. Stamm, "An image and video forgery detection software tool," *Drexel Ventures Innovation Fund*, July 2017 – June 2018, $99,880, Selected as finalist.

[3] J. Shackleford (PI), M. C. Stamm, B. Taskin, A. I. Pack, and D. C. Lim, "Collaborative research: CPS: Synergy: Developing next generation observation systems for animal studies," *National Science Foundation*, January 2017 – December 2020, $799,784.

[4] S. Weber (PI), M. C. Stamm, K. Dandekar, J. Shackleford, and A. Kontsos, "CICI: Secure and resilient architecture: Securing unmanned aerial system wireless sensor networks," *National Science Foundation*, January 2017 – December 2019, $1,000,000.

[5] K. R. Dandekar (PI), P. V. Abichandani, M. C. Stamm, and R. A. Greenstadt, "NeTS: Large: Real-time spectral and spatial processing for adversarial wireless networks," *National Science Foundation*, June 2016 – May 2018, $1,727,144.

[6] N. Kandasamy (PI), H. Sethu, and M. C. Stamm, "CSR: Small: Dimensionality reduction techniques for low-cost online performance monitoring and anomaly detection," *National Science Foundation*, July 2016 – June 2019, $499,440.

[7] K. R. Dandekar (PI), P. V. Abichandani, J. S. Stanford, M. C. Stamm, and S. Rank, "EDU: Software defined radio wars for cybersecurity and information assurance education," *National Science Foundation*, June 2016 – May 2018, $299,960.

[8] M. C. Stamm (PI) and N. Kandasamy, "Determining image and video integrity using convolutional neural networks," *Defense Advanced Research Projects Agency (DARPA) - MediFor Program*, May 2016 – February 2019, $936,036.

[9] M. C. Stamm and N. Kandasamy, "Software tool for determining image and video source and integrity," *Drexel Ventures Innovation Fund*, Submitted Dec. 2015, $100,000, Status: Selected as finalist, Full proposal due Mar. 2016.

[10] K. R. Dandekar (PI), P. V. Abichandani, N. Kandasamy, M. C. Stamm, and R. A. Greenstadt, "Nets: Medium: Real-time spatial and spectral processing for adversarial wireless networks," *National Science Foundation*, Apr. 2015 – Mar. 2019, $1,188,923.

[11] K. R. Dandekar (PI), P. V. Abichandani, M. C. Stamm, and S. Rank, "Edu: Software defined radio wars for cybersecurity and information assurance education," *National Science Foundation*, Jul. 2015 – Jun. 2017, $299,975.

[12] I. Savidis (PI), M. C. Stamm, and B. Taskin, "Satc:starss:securing integrated circuits against hardware trojans using information forensics," *National Science Foundation*, Nov. 2014 – Sep. 2017, $399,183.

## 4.5 White Papers

[1] M. C. Stamm (PI), J. Shackleford, and N. Kandasamy, "High performance techniques to identify the source and authenticity of digital videos using multimedia forensics," *Department of Defense Rapid Innovation Fund (DoD RIF), Army Research Office (ARO)*, Submitted May. 2016, Status: Invited to submit full proposal, Full proposal accepted.

[2] M. C. Stamm (PI), "Determining image heredity using information forensics," *National Security Agency (NSA)*, Submitted Oct. 2015, Status: No positive response indicated.

[3] M. C. Stamm (PI), "Project MediSphere," *Defense Advanced Research Projects Agency (DARPA) - MediFor Program*, Submitted Oct. 2015, Status: Full proposal submission encouraged, Full proposal accepted.

[4] M. C. Stamm (PI) and N. Kandasamy, "Robust and scalable techniques to determine image integrity and source using convolutional neural networks," *Defense Advanced Research Projects Agency (DARPA) - MediFor Program*, Submitted Oct. 2015, Status: Submission of full proposal encouraged, Full proposal declined in favor of Project MediSphere proposal.

[5] M. C. Stamm (PI) and J. A. Shackleford, "High performance techniques for multimedia forgery detection & source identification," *Combatting Terrorism Technical Support Office (CTTSO)*, Submitted Mar. 2015, Status: No positive response indicated.

[6] M. C. Stamm (PI) and N. Kandasamy, "High performance techniques to identify the origin of digital images using information forensics," *Defense Forensics and Biometrics Agency (DFBA)*, Submitted May 2014, Status: Submission of full proposal encouraged, Full proposal accepted.

[7] M. C. Stamm (PI), I. Savidis, and B. Taskin, "Securing integrated circuits against hardware trojans using information forensics," *Submitted through contact at the National Media Exploitation Center (NMEC) to be distributed throughout the Department of Defense*, Submitted May 2014, Status: No positive response indicated.

[8] M. C. Stamm (PI), "Determining multimedia heredity and authenticity using information forensics," *National Security Agency (NSA)*, Submitted Jan. 2014, Status: No positive response indicated.

[9] R. A. Greenstadt (PI), M. C. Stamm, M. Kam, and A. Fridman, "Open source verification via stylometry and image forgery detection," *National Security Agency (NSA)*, Submitted Jan. 2014, Status: No positive response indicated.

[10] M. C. Stamm (PI), "Multimedia information authentication using forensic decision fusion," *National Security Agency (NSA)*, Submitted Oct. 2013, Status: No positive response indicated.

# 5 Publications, Invited Talks, and Other Scholarly Material

This section contains information about my publications and efforts to disseminate my research.

In total, I have **authored or co-authored 50 papers** that are published. Additionally, I have authored 2 journal papers that are currently under review and am actively preparing 6 new journal papers with planned submission dates within the next 1-3 months. My publications have been **cited 1505 times** and my ***h*-index is 18**.

In addition to my published work, I have created and disseminated other scholarly material including one patent that is currently under review, a **software toolkit that is currently used by several governmental agencies**, a publicly available image dataset for multimedia forensics research, and have delivered several invited talks on multimedia forensics and information security.

## 5.1 Publications

### 5.1.1 Journal Publications

[1] M. C. Stamm, P. Bestagini, L. Marcenaro, and P. Campisi, "Forensic camera model identification: Highlights from the ieee signal processing cup 2018 student competition," *IEEE Transactions on Information Forensics and Security*, Sep. 2018.

[2] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, **[#2 Most accessed article in IEEE TIFS during June 2018]**.

[3] O. Mayer and M. C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762–1777, Jul. 2018.

[4] T. Huang, N. Kandasamy, H. Sethu, and M. C. Stamm, "An efficient strategy for online performance monitoring of datacenters via adaptive sampling," *IEEE Transactions on Cloud Computing*, Accepted and published on IEEEXplore in 2016, To appear in print.

[5] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of media forensics: The forensicability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 774–788, Apr. 2016.

[6] X. Chu, M. C. Stamm, and K. J. R. Liu, "Compressive sensing forensics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1416–1431, Jul. 2015.

[7] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "On antiforensic concealability with rate-distortion tradeoff," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1087–1100, Mar. 2015.

[8] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1456–1468, Sep. 2013.

[9] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, 2013, **[Nominated for the IEEE Signal Processing Society Overview Paper Award]**.

[10] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, Aug. 2012.

[11] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1050–1065, Sep. 2011.

[12] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010.

### 5.1.2 Journal Publications Currently Under Review

[1] B. Bayar and M. C. Stamm, "Accurate and robust source camera model identification via constrained convolutional neural networks," *currently under review in IEEE Transactions on Information Forensics and Security*, submitted Aug. 2018.

[2] S. DeCelles, B. Bayar, M. C. Stamm, and N. Kandasamy, "Data reduction, compressed sampling, and recovery for online performance monitoring," *currently under review in IEEE Transactions on Network Service Management*, submitted Aug. 2018.

### 5.1.3 Journal Publications in Preparation

[1] O. Mayer and M. C. Stamm, "Deep learning based forensic similarity for digital images," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[2] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[3] X. Zhao, C. Chen, and M. C. Stamm, "Anti-forensically falsifying an image's processing history using a generative adversarial network," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[4] B. Hosler and M. C. Stamm, "Forensic identification of an image's source social network," *in preparation for submission to IEEE Signal Processing Letters*, to be submitted Aug. / Sep. 2018.

[5] X. Zhao, C. Chen, and M. C. Stamm, "A generative adversarial network based attack to falsify an image's source camera model," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. / Sep. 2018.

[6] L. Bondi, P. Bestagini, S. Tubaro, and M. C. Stamm, "A new approach for performing falsified image region identification and localization using deep forensic feature inconsistencies," *in*

*preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Oct. 2018.

### 5.1.4 Conference Publications


[1] C. Chen, X. Zhao, and M. C. Stamm, "MISLGAN: An anti-forensic camera model falsification framework using a generative adversarial network," in *IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, Sep. 2018.

[2] M. Barni, M. C. Stamm, and B. Tondi, "Adversarial multimedia forensics: Overview and challenges ahead," in *European Signal Processing Conference (EUSIPCO)*, Rome, Italy, Sep. 2018.

[3] O. Mayer, B. Bayar, and M. C. Stamm, "Learning unified deep features for multimedia forensic tasks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Innsbruck, Austria, Jun. 2018.

[4] O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.

[5] B. Bayar and M. C. Stamm, "Towards open set camera model identification using a deep learning framework," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.

[6] B. Bayar and M. C. Stamm, "Towards order of processing operations detection in JPEG-compressed images with convolutional neural networks," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics*, Burlingame, CA, Feb. 2018, pp. 211–1–211–9.

[7] B. Bayar and M. C. Stamm, "Augmented convolutional feature maps for robust cnn-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4098–4102.

[8] C. Chen and M. C. Stamm, "Image filter identification using demosaicing residual features," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4103–4107.

[9] C. Chen, X. Zhao, and M. C. Stamm, "Detecting anti-forensic attacks on demosaicing-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 1512–1516.

[10] O. Mayer and M. C. Stamm, "Countering anti-forensics of lateral chromatic aberration," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 15–20.

[11] B. Bayar and M. C. Stamm, "A generic approach towards image manipulation parameter estimation using convolutional neural networks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 5–10.

[12] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in *accepted for publication in IEEE International Conference on Accoustics, Speech, and Signal Processing (ICASSP)*, New Orleans, LA, Mar. 2017, pp. 2152–2156.

[13] B. Bayar and M. C. Stamm, "Design principles of convolutional neural networks for multimedia forensics," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics - Special Session on Deep Learning for Multimedia Security*, San Francisco, CA, Feb. 2017, pp. 77–86.

[14] O. Mayer, D. C. Lim, A. I. Pack, and M. C. Stamm, "Classification of sleep states in mice using generic compression algorithms," in *EEE Signal Processing in Medicine and Biology Symposium (SPMB)*, Dec 2016, pp. 1–2.

[15] X. Zhao and M. C. Stamm, "Computationally efficient demosaicing filter estimation for forensic camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Sep. 2016, pp. 151–155.

[16] S. DeCelles, , T. Huang, M. C. Stamm, and N. Kandasamy, "Detecting incipient faults in software systems: A compressed sampling-based approach," in *IEEE International Conference on Cloud Computing (CLOUD) **(15% acceptance rate)***, Jun. 2016, pp. 303–310.

[17] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Vigo, Galicia, Spain, 2016, pp. 5–10.

[18] O. Mayer and M. C. Stamm, "Improved forgery detection with lateral chromatic aberration," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, Mar. 2016, pp. 2024–2028.

[19] S. DeCelles, M. C. Stamm, and N. Kandasamy, "Efficient online performance monitoring of computing systems using predictive models," in *IEEE/ACM International Conference on Utility and Cloud Computing (UCC) **(27.5% acceptance rate)***, Limassol, Cyprus, Dec. 2015, pp. 152–161.

[20] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Rome, Italy, Nov. 2015, pp. 1–6.

[21] O. Mayer and M. C. Stamm, "Anti-forensics of chromatic aberration," in *Proc. IS&T SPIE Electronic Imaging, Media Watermarking, Security, and Forensics*, San Francisco, CA, Feb. 2015, pp. 94 090M–94 090M.

[22] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of compression forensics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014, pp. 2689–2693.

[23] M. C. Stamm, X. Chu, and K. J. R. Liu, "Forensically determining the order of signal processing operations," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Guangzhou, China, Nov. 2013, pp. 162–167.

[24] M. C. Stamm and K. J. R. Liu, "Protection against reverse engineering in digital cameras," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Special Session on Adversarial Signal Processing*, Vancouver, Canada, May 2013, pp. 8702–8706.

[25] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "Concealability-rate-distortion tradeoff in image compression anti-forensics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013, pp. 3063–3067.

[26] Z.-H. Wu, M. Stamm, and K. Liu, "Anti-forensics of median filtering," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013, pp. 3043–3047.

[27] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics based on the autoregressive model of median filtered residual," in *Asia-Pacific Signal Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Hollywood, California, Dec. 2012, pp. 1–9.

[28] X. Chu, M. Stamm, and K. Liu, "Forensic identification of compressively sensed signals," in *IEEE International Conference on Image Processing (ICIP)*, Orlando, Florida, Sep. 2012, pp. 257–260.

[29] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensics vs. anti-forensics: A decision and game theoretic framework," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 1749–1752.

[30] X. Chu, M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensic identification of compressively sensed images," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 1837–1840.

[31] M. C. Stamm and K. J. R. Liu, "Anti-forensics for frame deletion/addition in MPEG video," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague, Czech Republic, May 2011, pp. 1876–1879.

[32] M. C. Stamm and K. J. R. Liu, "Wavelet-based image compression anti-forensics," in *IEEE International Conference on Image Processing (ICIP)*, Hong Kong, China, Sep. 2010, pp. 1737–1740.

[33] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *IEEE International Conference on Image Processing (ICIP)*, Hong Kong, China, Sep. 2010, pp. 2109–2112.

[34] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1698–1701.

[35] S. K. Tjoa, M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Harmonic variable-size dictionary learning for music source separation," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1698–1701.

[36] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Anti-forensics of jpeg compression," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1694–1697.

[37] M. C. Stamm and K. J. R. Liu, "Forensic detection of image tampering using intrinsic statistical fingerprints in histograms," in *Asia-Pacific Signal Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Sapporo, Japan, Oct. 2009, pp. 563–572.

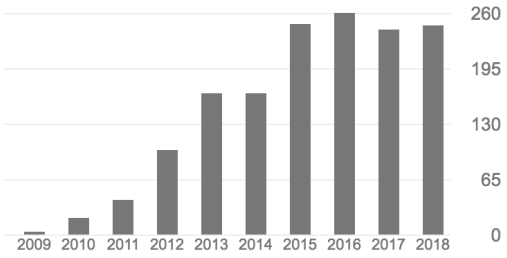
[38] M. C. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in *IEEE International Conference on Image Processing (ICIP)*, San Diego, CA, Oct. 2008, pp. 3112–3115.

## 5.2 Citations

I have been **cited 1505 times** and have an ***h*-index of 18**. My yearly citation counts are displayed below in Fig. 2 and the citations for my 20 most cited papers are shown on the next page in Table 1.

This citation information was retrieved from my Google Scholar profile on Aug. 15, 2018. Link available at:

https://scholar.google.com/citations?user=UE1rg1IAAAAJ&hl=en




| Year | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 (YTD) |
|---|---|---|---|---|---|---|---|---|---|---|
| Citations | 4 | 20 | 42 | 100 | 167 | 167 | 247 | 260 | 242 | 246 |

Figure 2: Yearly citation count information. Citations listed for 2018 are year-to-date figures current as of Aug. 15, 2018.

| Title & Publication Venue | Cited By | Year |
|---|---|---|
| "Forensic detection of image manipulation using statistical intrinsic fingerprints"<br>*IEEE Transactions on Information Forensics and Security* | 223 | 2010 |
| "Anti-forensics of digital image compression"<br>*IEEE Transactions on Information Forensics and Security* | 161 | 2011 |
| "Information forensics: An overview of the first decade"<br>*IEEE Access* | 159 | 2013 |
| "Temporal forensics and anti-forensics for motion compensated video"<br>*IEEE Transactions on Information Forensics and Security* | 106 | 2012 |
| "Anti-forensics of JPEG compression"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 99 | 2010 |
| "Robust median filtering forensics using an autoregressive model"<br>*IEEE Transactions on Information Forensics and Security* | 88 | 2013 |
| "Blind forensics of contrast enhancement in digital images"<br>*IEEE International Conference on Image Processing* | 87 | 2008 |
| "Undetectable image tampering through JPEG compression anti-forensics"<br>*IEEE International Conference on Image Processing* | 84 | 2010 |
| "A deep learning approach to universal image manipulation detection using a new convolutional layer"<br>*ACM International Workshop on Information Hiding and Multimedia Security* | 77 | 2016 |
| "Forensic estimation and reconstruction of a contrast enhancement mapping"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 64 | 2010 |
| "Forensics vs. anti-forensics: A decision and game theoretic framework"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 43 | 2012 |
| "Wavelet-based image compression anti-forensics"<br>*IEEE International Conference on Image Processing* | 32 | 2010 |
| "Anti-forensics for frame deletion/addition in MPEG video"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 31 | 2011 |
| "Anti-forensics of median filtering"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 29 | 2013 |
| "Robust median filtering forensics based on the autoregressive model of median filtered residual"<br>*APSIPA Annual Summit and Conference* | 25 | 2012 |
| "Forensic detection of image tampering using intrinsic statistical fingerprints in histograms"<br>*APSIPA Annual Summit and Conference* | 22 | 2010 |
| "Camera model identification framework using an ensemble of demosaicing features"<br>*IEEE International Workshop on Information Forensics and Security* | 22 | 2015 |
| "Forensically determining the order of signal processing operations"<br>*IEEE International Workshop on Information Forensics and Security* | 18 | 2013 |
| "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection"<br>*IEEE International Conference on Acoustics, Speech, and Signal Processing* | 16 | 2017 |
| "Design principles of convolutional neural networks for multimedia forensics"<br>*IS&T Electronic Imaging - Media Watermarking, Security, and Forensics* | 16 | 2017 |

Table 1: Citations for my 20 most cited publications (via Google Scholar, retrieved Aug. 15, 2018).

## 5.3 Patents

[1] O. Mayer and M. C. Stamm, "Learned forensic source system for identification of image capture device models," *U.S. Patent Application No. 62/652,651*, Provisional patent filed April 4, 2018.

## 5.4 Software

Source Camera Model Identification Tool

This software tool identifies the model and manufacturer of an image's source camera using forensic traces left in that image. It was developed as part of the grant "High-Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics" from the Defense Forensics and Biometrics Agencency (DFBA) and the Army Research Office (ARO).

**The *Source Camera Model Identification Tool* is currently in use by at least six government agencies**[2] including the Defense Forensic Science Center (DFSC), National Media Exploitation Center (NMEC), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Air Force Office of Scientific Research (AFOSR), and other governmental agencies. Copies of this software tool can be obtained from the Science Technology Integration Laboratory (STIL).

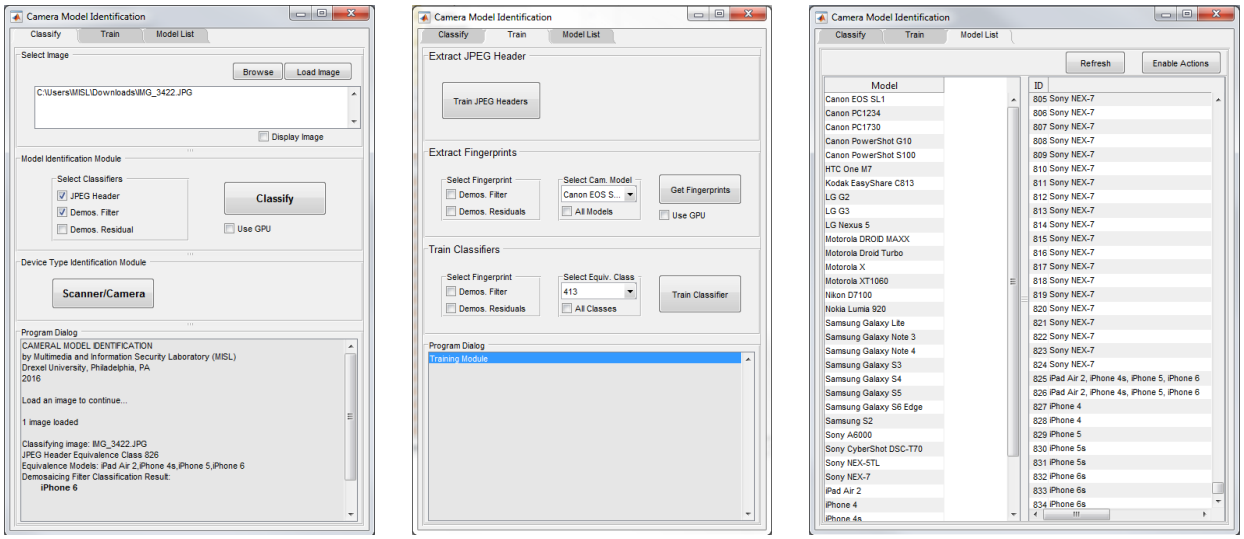



Figure 3: Screen capture of our *Source Camera Model Identification Tool* software pacakage's graphical user interface while performing classification and while performing training.

Screenshots of this software tool are shown in Fig. 3. This tool consists of both a graphical user interface and command line interface, software libraries implementing of all algorithms developed under this project including separate modules for feature extraction, training, and classification, binaries containing trained classifiers, and a 32 page user manual containing instructions on how

[2]This information can be verified by Dr. Stamm's PI on this project. Contact information can be provided upon request.

to install the software package, perform camera model identification, feature extraction, and classifier training as well as descriptions of all functions and subroutines invoked by this software package.

Research Source Code and Software

Source code, software implementations, and training data are available for several of the published papers and projects completed by my research group on the MISL gitlab page. These are provided to promote research reproducibility and aid in the dissemination of our results.

This code can be accessed on the MISL gitlab page using the link below:
https://gitlab.com/users/MISLgit/projects

## 5.5 Datasets

2018 IEEE Signal Processing Cup Dataset

This dataset was created to run the 2018 IEEE Signal Processing Cup (SP Cup) and has been made publicly available for research purposes. The 2018 SP Cup was a forensic camera model identification in which participants were challenged to develop a system correctly identify the make and model of an image's source camera using only the image itself.

This dataset consists of sets of images to be used for both training and evaluation purposes captured using 36 devices corresponding to 18 different camera models (different devices of the same manufacturer and model were used to capture images for the training and evaluation sets). All images were manually captured by members of my research group to control quality and ensure their provenance. This dataset is split into 10 known camera models used for Round 1 of the competition and 8 unknown camera models (whose identities were kept private) for use in Round 2 of the competition.

The 2018 IEEE Signal Processing Cup database can be accessed for free using IEEE Dataport:
http://ieee-dataport.org/995

## 5.6 Invited Talks and Presentations

- *Image Forgery Detection and Falsification Using Deep Learning*, Presented at meeting organized by WITNESS (human rights organization) & Harvard's Shorenstein Center to discuss malicious uses of Deepfakes and other AI-generated synthetic media, June 2018.
- *Multimedia Forensics: Using Mathematics and Machine Learning to Detect Image Forgeries*, Presented at Rowan University, April 2017.
- *Multimedia Forensics*, Presented at the Drexel Cybersecurity Symposium, November 2016.
- *Multimedia Forensics: Using Mathematics and Machine Learning to Determine an Image's Source and Authenticity*, Presented as an NSA Center of Academic Excellence Tech Talk, October 2016.

- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Closeout Meeting, August 2016.
- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Review Meeting, March 2016
- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Review Meeting, August 2015.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the IEEE Philadelphia Section, October 2014.
- *Information Forensics*, Presented at the West Philadelphia Science Showcase as part of the Philadelphia Science Festival, April 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the National Media Exploitation Center (NMEC), April 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), February 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the National Institute of Standards and Technology (NIST), March 2013.

# 6 Teaching and Student Advising Activities

Since joining Drexel, I have maintained a strong commitment to both undergraduate education, graduate education, and student mentoring. I have **developed three new courses** at the undergraduate and graduate levels; ( (1) ECES 301: Transform Methods and Filtering, (2) ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security, and (3) ECES T680 - Forensic Signal Processing. Particularly significant among these was the re-development of ECES 302 into a two quarter sequence (this was initiated in Fall 2013 however the course officially changed titles to ECES 301 in Fall 2014). This involved the creation of a comprehensive set of lecture notes and recitation scripts for ECES 301 that have been shared with and used by several Drexel faculty members, development of graded material (homeworks, quizes, midterms, and final exams), and coordination efforts for the development of Transform Methods II. Across the courses that I have taught, I have maintained high scores on my instructor evaluations - typically 4.5/5 or higher - and **in 2015 a student wrote an unsolicited letter to the Senior Vice Provost of Academic Affairs praising my teaching** (included in Appendix A).

In addition to my teaching duties, I have served as the **advisor to 5 Ph.D. students** (one co-advised with Nagarajan Kandasamy), 2 M.S. students (one also co-advised with Nagarajan Kandasamy), and three undergraduate students (one of which is completing his M.S. with me in the 2018-2019 academic year). I have also hosted a visiting Ph.D. student from Politecnico di Milano, Milan, Italy. One of my Ph.D. students has successfully defended his thesis and secured a position as an Applied Scientist at the Alexa Brain team of Amazon in Seattle. Additionally, I have successfully recruited one new incoming Ph.D. student who I will advise beginning in Fall 2018 and am working to recruit a second (who has indicated that he will likely commit to pursuing a Ph.D. with me fin Fall 2018).

## 6.1 Courses Taught

| Quarter | Course and Enrollment |
|---|---|
| Winter 17-18 | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security (Enrollment: 28 students) |
| Spring 16-17 | ECES 301: Transform Methods and Filtering<br>Enrollment: 44 students |
| Winter 16-17 | ECES T680: Forensic Signal Processing<br>Enrollment: 10 students |
| Fall 16-17 | ECES 301: Transform Methods and Filtering<br>Enrollment: 68 students |
| Spring 15-16 | ECES 301: Transform Methods and Filtering<br>Enrollment: 74 students |
| Winter 15-16 | ECES T680: Forensic Signal Processing<br>Enrollment: 42 students |

| | |
|---|---|
| Fall 15-16 | ECES 301: Transform Methods and Filtering<br>Enrollment: 85 students |
| Spring 14-15 | ECES 301: Transform Methods and Filtering<br>Enrollment: 84 students |
| Winter 14-15 | ECES T680: Forensic Signal Processing<br>Enrollment: 42 students |
| Fall 15-16 | ECES 301: Transform Methods and Filtering<br>Enrollment: 85 students |
| Spring 14-15 | ECES 301: Transform Methods and Filtering<br>Enrollment: 84 students |
| Winter 14-15 | ECES 690: Forensic Signal Processing<br>Enrollment: 27 students |
| | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security<br>Enrollment: 15 students |
| Fall 14-15 | ECES 301: Transform Methods and Filtering<br>Enrollment: 82 students |
| Spring 13-14 | ECES 302: Transform Methods and Filtering<br>Enrollment: 84 students |
| Winter 13-14 | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security<br>Enrollment: 13 students |
| Fall 13-14 | ECES 302: Transform Methods and Filtering<br>Enrollment: 83 students |

## 6.2 New Courses Developed

I have developed the following three courses:

- ECES 301: Transform Methods and Filtering
- ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security
- ECES T680: Forensic Signal Processing (Also listed as ECES 690)

Sample syllabi for each of these courses are provided as a reference in Appendix B.

### 6.2.1 ECES 301: Transform Methods and Filtering

Redevelopment Activities:

- Conducted complete redesign of course (previously ECES 302) including:
  - Development of new learning objectives
  - Revision of topics covered
  - Reformulation of order in which topics are presented
  - Creation of a complete set of lecture notes and recitation scripts
- Introduced new textbook (Signals and Systems (2nd Ed.) by Oppenheim and Willsky
- Developed new course material
- Organized and participated in course redevelopment meetings for Transform Methods ECES 301 and ECES 303 (Previously ECES 302 and ECES 390)
- Met with representatives from Pearson publishing to discuss customized textbook options for Transform Methods II

Topics Covered:

- Basic signal and system properties
- Continuous and discrete time convolution
- Continuous and discrete time Fourier series
- Continuous and discrete time Fourier transform
- Linear filtering
- Solving differential equations through Fourier analysis
- AM modulation (time permitting)
- Sampling theorem (time permitting)

New Materials Developed:

- Complete set of lecture notes
- Weekly homework assignments
- Weekly quizzes
- Three midterms plus comprehensive final exam
- Matlab excercises
- Recitation scripts
- Various handouts

### 6.2.2 ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security

Topics Covered:

- Digital image processing & compression
- Basic information hiding techniques
- Image watermarking (fragile and robust watermarking techniques)
- Image forensics (source camera identification and manipulation detection)
- Anti-forensics

New Materials Developed:

- Lecture slides and handouts
- Four bi-weekly projects
- Midterm exam
- Final project (in class presentation and final report)

### 6.2.3 ECES T680: Forensic Signal Processing

Topics Covered:

- Digital image processing & compression
- Image watermarking (fragile and robust watermarking techniques)
- Steganography and steganalysis
- Basics of decision theory (hypothesis testing, Bayes rule, Neyman-Pearson criteria, etc.)
- Introduction to machine learning
- Image forensics - editing and forgery detection
- Image forensics - source identification
- Anti-forensic attacks

New Materials Developed:

- Lecture slides and handouts
- Several projects
- Midterm exam
- Final project (in class presentation and final report)

## 6.3 Student Course Evaluations & Comments

Table 2 displays the average instructor and course ratings received (on a scale of 1 to 5) from student evaluations of my courses. Selected comments from these student evaluations are included below.

Additionally, James Esser, a student in my Spring 2015 ECES 301: Transform Methods & Filtering class, sent an unsolicited letter praising my teaching to Dr. John DiNardo, Senior Vice Provost of Academic Affairs in July 2015. This letter is included in Appendix A at the end of this dossier.

| Course | Course Name | Term | Level | Enroll | Instruct Eval | Course Eval |
|---|---|---|---|---|---|---|
| ECES 435 | Recent Advances in DSP | Winter 17-18 | U | 28 | 5.0 | 4.9 |
| ECES 301 | Transform Methods & Filtering | Spring 16-17 | U | 44 | 5.0 | 4.7 |
| ECES T680 | Forensic Signal Processing | Winter 16-17 | G | 10 | 4.7 | 4.7 |
| ECES 301 | Transform Methods & Filtering | Fall 16-17 | U | 68 | 4.5 | 4.3 |
| ECES 301 | Transform Methods & Filtering | Spring 15-16 | U | 74 | 4.9 | 4.4 |
| ECES T680 | Forensic Signal Processing | Winter 15-16 | G | 42 | 4.5 | 4.7 |
| ECES 301 | Transform Methods & Filtering | Fall 15-16 | U | 85 | 4.6 | 4.3 |
| ECES 301 | Transform Methods & Filtering | Spring 14-15 | U | 84 | 4.5 | 4.3 |
| ECES 690 | Forensic Signal Processing | Winter 14-15 | G | 27 | 4.4 | 4.4 |
| ECES 435 | Recent Advances in DSP | Winter 14-15 | U | 15 | 4.8 | 4.5 |
| ECES 301 | Transform Methods | Fall 14-15 | U | 82 | 3.5 | 3.4 |
| ECES 302 | Transform Methods & Filtering | Spring 13-14 | U | 84 | 4.2 | 4.1 |
| ECES 435 | Recent Advances in DSP | Winter 13-14 | U | 15 | 5.0 | 5.0 |
| ECES 302 | Transform Methods & Filtering | Fall 13-14 | U | 83 | 4.1 | 3.8 |

Table 2: Student Course Evaluations

Selected Comments from Student Evaluations

- "Dr. Stamm is one of the few instructors that everyone shows up to class for, and at every class. It's always a great lecture and keeps my attention span focused. I wish he had more free time to teach more classes." – ECES 435, Winter 17-18
- "Dr.Stamm gets me excited about literally anything he teaches. No apparent weaknesses." – ECES 435, Winter 17-18
- "The most outstanding lecturer I have had while attending Drexel. Understood the material, appreciated the material, and framed the material in an concise approachable way for the

student." – ECES 301, Spring 16-17

- "The instructor (Stamm) was incredibly charismatic and was visibly interested in the material he was teaching, which made learning the material very easy. He appears to take his job as a professor very seriously. He made no attempts to make the material "easy", but instead made sure all the students were able to understand and interpret the class material despite its inherent difficulty." – ECES 301, Spring 16-17
- "Amazing lecturer who always communicates his thoughts clearly. I can't recall any lecture where I was confused by the material and he was unable to provide a clear answer. No weaknesses, as far as I'm concerned." – ECES T680, Winter 16-17
- "I thought you taught really well. You worked through things really thoroughly, so I felt like I understood the material. No matter my grade, I feel confident in my understanding of everything we worked on, and my ability to use these skills in the real world. Overall, you were one of my favorite professors at Drexel so far! Thank you!!" – ECES 301, Fall 16-17
- "Professor Stamm is always full of enthusiasm and willingness to teach each and every lecture, and his deep interest in the class topics makes for an enjoyable class environment where motivation is avid. Professor Stamm knows the material by heart and is able to portray information and examples incredibly well and go into detail that truly does help grasp the material well. He's an excellent teacher and I hope he goes on to teach more of my systems classes!" – ECES 301, Spring 15-16
- "Stamm is a fantastic professor. He is very engaging and passionate about his field. He consistently checks in with students during lectures to make sure everyone is following and does not hesitate to explain things in greater detail when anyone is struggling. He also really knows his stuff." – ECES T680, Winter 15-16
- "Very engaging lectures. Explained concepts well. Clearly excited about the material covered. Overall one of the best lecturers I've had so far." – ECES 301, Fall 15-16
- "Dr. Stamm is one of the best professors I have had at Drexel so far. He puts in a lot of effort to make sure that students understand the material. He always comes prepared for lectures and goes through every single concept thoroughly. Very enthusiastic about what he teaches, and he does his best to keep everyone interested. I loved his class, and I just could not wait to go in. The only weakness that I can think of is his tendency to get deep into proofs occasionally, and that gets a bit confusing." – ECES 301, Fall 15-16
- "Extremely enthusiastic. Made me appreciate the material from week one. Had no plans on taking Transforms II since it is not a requirement for my major. Because of Professor Stamm I added the course into my schedule after three weeks. Absolutely fantastic instructor." – ECES 301, Spring 14-15
- "The teacher was able very prepared for class and ran the lectures very well. He is extremely knowledgeable on the topic and presented the material in a manner that was understandable and clear but not overwhelming. Much of the material covered could be very math intensive, which was not the purpose of this course, and I felt that he handled it rather well in class." – ECES 690, Winter 14-15

- "Professor did anything and everything he could to help students succeed. Out of all the years I have been here at Drexel, Dr. Stamm was perhaps the most caring and helpful professor I ever met. He truly LOVES the material and is passionate about what he is teaching, and you could easily see this every time you asked a question. In the end, he did everything in his power to share his love for this subject with students, and it was important for him to see students learning." –ECES 302, Spring 13-14
- "Dr. Stamm was definitely one of the best professors I have had at Drexel University. As a non ECE major (I am a Biomedical Engineering Major) I was able to understand the material he taught completely. He was able to engage the student's in class, while staying organized. His passion in education and the material topics as well as his profound knowledge in the material covered was clearly evident. Despite his seemingly young age, the professor's teaching style seemed well perfected, and almost natural. DREXEL NEEDS MORE PROFESSORS LIKE DR. STAMM." –ECES 302, Fall 13-14

## 6.4 Graduate Student Supervision

Upon arrive at Drexel in the Fall of 2013, I founded the Multimedia and Information Security Lab (MISL). I have worked to establish this research group by four Ph.D. students and one M.S. student who work under my supervision (all are currently funded by grants where I am the PI). Additionally, I co-supervise one Ph.D. student with Nagarajan Kadasamy (who is funded by the 2015 Koerner Family Dissertation Fellowship) and have recruited one new Ph.D. student (and likely a second) who will begin working with me in Fall 2018.

I have graduated one Ph.D. student, Belhassen Bayar, who has successfully secured a position as an Applied Scientist at the Alexa Brain team of Amazon. Additionally, my graduate students have successfully secured internships at prestigious employers (Chen Chen, Facebook - Spring 2018; Belhassen Bayar, Samsung Research Deep Learning Division - Summer 2015).

Ph.D. Students Under My Supervision

1. **Belhassen Bayar** (Graduated)
   Dissertation Title: *Deep Learning Techniques for Multimedia Forensics*
   Defense Date: August 6, 2018
   Internships: *Distributed Systems & Machine Learning Intern* - Samsung Research America, Summer 2015
   Awards: Lee Smith Travel Fellowship (2017)
   First Position: *Applied Scientist* - Alexa Brain Division, Amazon

2. **Chen Chen**
   Research Topics: Forensic camera model identification, Anti-forensics, Deep learning, Generative Adversarial Networks
   Internships: *Machine Learning Software Intern* - Facebook Engineering, Fall 2018

3. **Owen Mayer**
   Research Topics: Deep learning, Image editing and forgery detection, Image splicing detection using lateral chromatic aberration
   Awards: 2018 Koerner Family Fellowship, Provost's Award for Best Oral Presentation at the 2017 Drexel Emerging Graduate Scholars Conference, Drexel International Travel Award (2016)

4. **Xinwei Zhao**
   Research Topics: Anti-forensics, Deep learning, Generative adversarial networks, Forensic camera model identification
   Awards: IEEE Signal Processing Society Travel Grant - ICIP 2018, Lee Smith Travel Fellowship (2017)

5. **Salvador DeCelles** (Co-Supervised with Nagarajan Kandasamy)
   Research Topics: Online monitoring and anomaly detection for datacenters
   Expected Graduation: Fall 2018
   Awards: 2015 Koerner Family Fellowship

6. **Shengbang Fang** (Incoming Student - Fall 2018)
   Expected Research Topics: Deep learning techniques for multimedia forensics, Video source identification

Visiting Ph.D. Students Under My Supervision

1. **Luca Bondi**
   Visiting Period: February - April 2018
   Home Institution: Politecnico di Milano, Milan, Italy
   Research Topics: Image forgery localization, Deep learning techniques for multimedia forensics

M.S. Students Under My Supervision

1. **Hunter Kippen** (B.S./M.S. Student, beginning M.S. thesis work in Fall 2018)
   Research Topics: Deep learning techniques for video source identification

2. **Leland Machen** (Graduated, Co-Supervised with Nagarajan Kandasamy)
   Research Topics: Computationally efficient forensic algorithms, Forensic camera model identification
   Graduation Date: June 10, 2016
   First Position: *Software Engineer*, Lockheed Martin

## 6.5 Undegraduate Student Supervision

Undergraduate Student Volunteers Under My Supervision

1. Brian Hosler (2017-2018)

2. Hunter Kippen (2018)

3. George Slavin (2016)

Senior Design Groups Under My Supervision

1. Team: *Robust Mobile Object Tracking* (ECE-05)
   Academic Year: 2017-2018
   Co-Adivsor: James Shackleford
   Members: Nathan Schomer, Brian Hosler, Justin DeLisio, Marcus Iqbal

2. Team: *High Performance Digital Image Forensics* (ECE-29)
   Academic Year: 2015-2016
   Co-Adivsor: Nagarajan Kandasamy
   Members: Kevin Peters, Nathan Kline, Andrew Chau, Nicholas Tylek
   *** Chosen to represent ECE in the College of Engineering Senior Design Competition**

# 7 Service Activities

I have striven to be an active member of my department and my research community.

Within my department and college, I have **served on five committees** including the ECE Department's Planning and Development Committee and our recent Department Head Search Committee. As a member of the Planning and Development Committee, I led the effort to reform and standardize the procedures by which our department submits, considers, and votes upon motions. I have **served on 47 candidacy, thesis proposal, and thesis defense committees**, 12 of which I have chaired. Additionally, I have participated in several other departmental service activities such as creating research demonstrations for departmental outreach activities, speaking at several meetings and events such as our Advisory Council and Employer Circle meetings, volunteering at open houses and accepted student days, judging graduate student research competitions, and designing a session for the Drexel University Code Academy high school computing outreach program.

Within my research community, I served as the **General Chair of the 2017 ACM Workshop on Information Hiding and Multimedia Security** and currently serve as an **elected member of the IEEE Signal Processing Society's (IEEE SPS) Technical Committee on Information Forensics and Security** - the IEEE SPS body that oversees and organizes conferences, publications, awards, and educational activities related to information security. I was the **lead organizer of the 2018 IEEE Signal Processing Cup**, which is an annual international competition designed to challenge undergraduate students from around the world to tackle real problems in signal processing and machine learning. I have organized special sessions in two different conferences and serve as an editorial board member of IEEE SigPort. Additionally, I regularly review for several top journals within my field and serve on the technical program committees of several major conferences.

## 7.1 University and Departmental Service

### 7.1.1 College and Departmental Committee Membership

College-Level Committee Membership:

- ECE Department Head Search Committee, 2017 - 2018
- MS in Cybersecurity Degree Revision Committee, 2017 - Present

Departmental Committee Membership:

- Planning and Development Committee, 2017 - Present
- Assessment and Accreditation Committee, 2015 - Present
- Machine Learning Curricular Revision Committee, 2014 - 2015

### 7.1.2 Candidacy Examination, Thesis Proposal, and Thesis Defense Committee Membership

Ph.D. Qualifying Examination Committee Member - (Total: 17, Chair: 2)

- Chenxi Li (Adv. Cohen) - June 18, 2018
- Oday Bshara (Adv. Dandekar) - April 19, 2018
- Zhengqiao Zhao (Adv. Rosen) - September 7, 2017
- Yirui Liu (Adv. Walsh) - June 11, 2017
- Xinwei Zhao (Adv. Stamm) - June 1, 2017
- Chen Chen (Adv. Adv. Stamm) - May 31, 2017
- Owen Mayer (Adv. Stamm) - May 1, 2017
- Belhassen Bayar (Adv. Stamm) - April 25, 2017
- Kyle Juretus (Adv. Savidis) - June 15, 2016
- Stephen Woloszynek (Adv. Rosen) - September 29, 2015
- Jonathan Stokes (Adv. Weber) - September 16, 2015
- Yitian Shao (Adv. Visell) - May 27, 2015
- Solmaz Torabi (Adv. Walsh) - January 13, 2015
- Pingge Jiang (Adv. Shackleford) - September 23, 2014 **(Chair)**
- Ni An (Adv. Weber) - September 22, 2014
- Arjun Rajasekar (Adv. Hrebien & Kam) - July 2, 2014 **(Chair)**
- Michael Caro (Adv. Kim) - December 4, 2013

Ph.D. Thesis Proposal Committee Member - (Total: 15, Chair: 4)

- Owen Mayer (Adv. Stamm) - July 18, 2018
- Ni An (Adv. Weber) - December 4, 2017 **(Chair)**
- Pingge Jiang (Adv. Shackleford) - November 9, 2017 **(Chair)**
- Stephen Woloszynek (Adv. Rosen) - December 1, 2017 **(Chair)**
- Belhassen Bayar (Adv. Stamm) - July 11, 2017
- Rajath Soans (Adv. Shackleford) - April 21, 2017 **(Chair)**
- William Osei-Bonsu (Adv. Kandasamy, Co-Adv. Stamm) - February 15, 2017
- Jie Ren (Adv. Walsh) - April 1, 2016

- Marko Janko (Adv. Visell & Kam) - August 31, 2015
- Tingshan Huang (Adv. Sethu & Kandasamy) - June 18, 2015
- Brandon Morton (Adv. Kim) - June 4, 2015
- Matthew Prockup (Adv. Kim) - January 22, 2015
- Bradford Boyle (Adv. Weber) - August 13, 2014
- Zexi Liu (Adv. F. Cohen) - May 20, 2014
- Sayandeep Acharya (Adv. Kam) - January 16, 2014

Ph.D. Thesis Committee Member - (Total: 12, Chair: 4)

- Belhassen Bayar (Adv. Stamm) - August 6, 2018
- Pingge Jiang (Adv. Shackleford) - July 16, 2018 **(Chair)**
- Stephen Woloszynek (Adv. Rosen) - May 29, 2018 **(Chair)**
- Solmaz Torabi (Adv. Walsh) - May 14, 2018 **(Chair)**
- Rajath Soans (Adv. Shackleford) - December 1, 2017 **(Chair)**
- Marco Janko (Adv. Visell, Co-Adv. Kam, Acting Adv. Stamm) - September 12, 2017
- Brandon Morton (Adv. Kim) - April 22, 2016
- Matthew Prockup (Adv. Kim) - May 3, 2016
- Bradford Boyle (Adv. Weber) - May 27, 2015
- Donald Bucci (Adv. Kam) - February 13, 2015
- Sayandeep Acharya (Adv. Kam) - November 7, 2014
- Zexi Liu (Adv. F. Cohen) - September 24, 2014

M.S. Thesis Defense Committee Member - (Total: 3, Chair: 2)

- Jenna Schabdach (Adv. Shackleford) - May 24, 2016 **(Chair)**
- Andrew Benton (Adv. Shackleford) - June 8, 2015 **(Chair)**
- Daniel Zalkind (Adv. Kam) - May 15, 2014

### 7.1.3 Additional University and Departmental Service Activities

Other Departmental Service Activities

- Organized (with Gail Rosen) invited seminar by Dr. Min Wu, IEEE Signal Processing Society Distinguished Lecturer - October 18, 2016

- Served as Judge for the 8th annual Drexel IEEE Graduate student Forum's Research Symposium - February 26, 2016
- Developed a *Multimedia Forensics* session for the 2015 Drexel University Code Academy (DUCA) - A month-long program hosted by Drexel University for 25-30 high school juniors and seniors interested in computing
- Prepared and delivered presentation to the Freshmen Design Revision Committee on freshman engineering design projects utilized at other universities and how they could be adopted at Drexel - November 10, 2016
- Prepared and delivered presentation to the Senior Design Task Force on a Capstone Course alternative to the current Senior Design curriculum and how this is implemented at other universities - February 16, 2016
- Volunteer at Spring 2015 ECE Department Open House - March 5, 2015
- Volunteer at the 2014 ECE Deptartment Accepted Students Day - April 5, 2014
- Volunteer at Fall 2013 ECE Department. Open House - November 10, 2013

Research Demonstrations Presented on Behalf of the Drexel University ECE Department

- Created and administered two demonstrations for Drexel University's 2018 ECE Day - Feb 19, 2018
- Created a demonstration for ECE Open House events (presented by Ph.D. students Xinwei Zhao and Chen Chen) - August 20, 2017
- Created and administered two demonstrations for Drexel University's 2017 ECE Day - February 21, 2017
- Created a demonstration to represent Drexel at the Colloquium for Information Security and Education (CISSE) - June 12, 2016
- Created and administered two demonstrations for Drexel University's 2016 ECE Day - February 23, 2016

Speaker at the Following Events on Behalf of the Drexel University ECE Department

- Vanguard Innovation Team meeting as part of a session to build academic collaborations between Drexel and Vanguard - May 30, 2017
- Drexel University's meeting with Xinli Gu, Senior Director of DFX Technology of Huawei North America Network Division - December 2, 2015
- A. J. Drexel Cybersecurity Senior Advisory Board meeting - March 10, 2015
- ECE Employer Circle meeting - April 2014
- ECE Advisory Council meeting - October 4, 2013

## 7.2 External Service

### 7.2.1 Leadership and Organization Activities

General Chair of the Following Conferences:

- 2017 ACM Workshop on Information Hiding and Multimedia Security - Philadelphia, PA

Professional Society Leadership Activities:

- IEEE Signal Processing Society - Information Forensics and Security Technical Committee
  *Elected Member (2018-2020 Term)* - This committee oversees and organizes conferences, publications, awards, and educational activities related to information security, multimedia forensics, steganography, biometrics, cryptography, authentication, and other security related research.

Organizer of the Following International Competitions:

- 2018 IEEE Signal Processing Cup *(Lead Organizer)*
  This competition, held annually by IEEE Signal Processing Society, challenges teams of undergraduate students from around the world to tackle real problems in signal processing and machine learning. The competition I organized was a forensic camera model identification challenge in which teams designed systems to determine which type of camera was used to captured an image. The first round was run in conjunction with Kaggle and the final competition was held at the 2018 IEEE International Conference on Accoustics, Speech, and Signal Processing.

Editorial Board Membership

- IEEE SigPort

Special Session Organizer for the Following Conferences:

- 2018 European Signal Processing Conference (EUSIPCO)
  - Special Session on Adversarial Dynamics (Co-Organized with Benedetta Tondi and Mauro Barni)
- 2015 SPIE Electronic Imaging - Media Watermarking, Security, and Forensics
  - Special Session on Anti-Forensics (Co-Organized with H. Taha Sencar)

### 7.2.2 Reviewing Activites

Invited Reviewer for the Following Research Journals

- IEEE Transactions on Image Processing

- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Circuits and Systems for Video Technology
- IEEE Transactions on Multimedia
- IEEE Journal of Selected Topics in Signal Processing
- IEEE Transactions on Cybernetics (B)
- IEEE Signal Processing Letters
- Journal of Visual Communication and Image Representation (Elsevier)
- Signal Processing (Elsevier)
- Information Sciences (Elsevier)
- Computers & Security (Elsevier)

Technical Program Committee Member for the Following Conferences

- IEEE International Conference on Image Processing (ICIP) – 2014, 2015, 2016, 2017, 2018
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) – 2014, 2016, 2017, 2018
- IEEE Workshop on Information Forensics and Security (WIFS) – 2014, 2015, 2017, 2018
- ACM Workshop on Information Hiding & Mutimedia Security (IH&MMSec) –2017, 2018
- IEEE International Workshop on Multimedia Signal Processing (MMSP) – 2012

Reviewer or Subreviewer for the Following Conferences

- IEEE International Conference on Image Processing (ICIP) – 2008, 2009, 2010, 2012
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) – 2011, 2012
- IEEE Workshop on Information Forensics and Security (WIFS) – 2013
- European Signal Processing Conference (EUSIPCO) – 2012
- International Information Hiding Conference – 2011
- International Workshop on Digital Watermarking (IWDW) – 2011

Reviewer for the Following NSF Programs

- Ad-hoc reviewer for Secure and Trustworthy Cyberspace (SaTC) - 2015.

# 8 Curriculum Vitae

My curriculum vitae is included beginning on the following page.

# Matthew C. Stamm

Bossone Research Center • Room 413G
3120 Market Street • Philadelphia, PA 19104
mstamm@drexel.edu • 215-895-5894
misl.ece.drexel.edu

## EDUCATION

**Ph.D. Electrical Engineering** 2012
University of Maryland, College Park
*Thesis: Digital Multimedia Forensics and Anti-Forensics*
*Advisor: K. J. Ray Liu*

**M.S. Electrical Engineering** 2011
University of Maryland, College Park
*Advisor: K. J. Ray Liu*

**B.S. Electrical Engineering** 2004
University of Maryland, College Park
*University Honors*

## PROFESSIONAL EXPERIENCE

**Assistant Professor** August 2013 – Present
*Department of Electrical and Computer Engineering*
*Drexel University, Philadelphia, PA*

**Co-Instructor** June 2013 – July 2013
*Cybersecurity Leadership Program*
*Robert H. Smith School of Business*
*University of Maryland, College Park, MD*

**Post-Doctoral Research Associate** June 2012 – May 2013
*Department of Electrical and Computer Engineering*
*University of Maryland, College Park, MD*
*Supervisor: K. J. Ray Liu*

**Graduate Research Assistant** May 2008 – May 2012,
*Department of Electrical and Computer Engineering* May 2007 – August 2007
*University of Maryland, College Park, MD*
*Supervisor: K. J. Ray Liu*

**Graduate Teaching Assistant** September 2005 – May 2008
*Department of Electrical and Computer Engineering*
*University of Maryland, College Park, MD*

**Radar Systems Engineer** June 2004 – September 2005,
*Johns Hopkins University Applied Physics Lab* June 2006 – August 2006

## AWARDS AND FELLOWSHIPS

- **Drexel College of Engineering Outstanding Early-Career Research Achievement Award** (2017) - Awarded annually to one assistant professor within Drexel University's College of Engineering for outstanding research accomplishments.
- **NSF CAREER Award** (2016) - Awarded for the proposal "CAREER: Scaling Multimedia Forensic Algorithms for Big Data and Adversarial Environments"
- **Dean's Doctoral Dissertation Award** (2012) - Awarded annually to one graduating doctoral student in the A. James Clark School of Engineering at the University of Maryland for outstanding doctoral research.
- **Ann G. Wylie Dissertation Fellowship** (2011) - Awarded annually to 40 outstanding doctoral students throughout the entire University of Maryland in the final stages of their dissertation.
- **Future Faculty Fellowship** (2010) - Awarded annually by the A. James Clark School of Engineering to twenty Ph.D. students who show potential towards earning a faculty position at a major research university.
- **Distinguished Teaching Assistant Award** (2006) - Awarded by the Department of Electrical and Computer Engineering at the University of Maryland, College Park.

## TEACHING EXPERIENCE

**Drexel University**
*Assistant Professor*

| | |
|---|---|
| Winter 17-18 | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security (Enrollment: 28 students) |
| Spring 16-17 | ECES 301: Transform Methods and Filtering (Enrollment: 44 students) |
| Winter 16-17 | ECES T680: Forensic Signal Processing (Enrollment: 10 students) |
| Fall 16-17 | ECES 301: Transform Methods and Filtering (Enrollment: 68 students) |
| Spring 15-16 | ECES 301: Transform Methods and Filtering (Enrollment: 74 students) |
| Winter 15-16 | ECES T680: Forensic Signal Processing (Enrollment: 42 students) |
| Fall 15-16 | ECES 301: Transform Methods and Filtering (Enrollment: 85 students) |
| Spring 14-15 | ECES 301: Transform Methods and Filtering (Enrollment: 84 students) |

| | |
|---|---|
| Winter 14-15 | ECES 690: Forensic Signal Processing (Enrollment: 27 students) |
| | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security (Enrollment: 15 students) |
| Fall 14-15 | ECES 301: Transform Methods and Filtering (Enrollment: 82 students) |
| Spring 13-14 | ECES 302: Transform Methods and Filtering (Enrollment: 84 students) |
| Winter 13-14 | ECES 435: Recent Advances in Digital Signal Processing - Multimedia Signal Processing and Information Security (Enrollment: 13 students) |
| Fall 13-14 | ECES 302: Transform Methods and Filtering (Enrollment: 83 students) |

**University of Maryland, College Park**
*Co-Instructor, Cybersecurity Leadership Program*

| | |
|---|---|
| Summer 13 | Cybersecurity Leadership Capstone |

*Co-Instructor (One-Third Workload), Department of Electrical and Computer Engineering*

| | |
|---|---|
| Spring 11 | ENEE 324: Engineering Probability |

## INVITED TALKS

- *Image Forgery Detection and Falsification Using Deep Learning*, Presented at meeting organized by WITNESS (human rights organization) & Harvard's Shorenstein Center to discuss malicious uses of Deepfakes and other AI-generated synthetic media, June 2018.
- *Multimedia Forensics: Using Mathematics and Machine Learning to Detect Image Forgeries*, Presented at Rowan University, April 2017.
- *Multimedia Forensics*, Presented at the Drexel Cybersecurity Symposium, November 2016.
- *Multimedia Forensics: Using Mathematics and Machine Learning to Determine an Image's Source and Authenticity*, Presented as an NSA Center of Academic Excellence Tech Talk, October 2016.
- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Closeout Meeting, August 2016.
- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Review Meeting, March 2016
- *High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), Program Review Meeting, August 2015.

- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the IEEE Philadelphia Section, October 2014.
- *Information Forensics*, Presented at the West Philadelphia Science Showcase as part of the Philadelphia Science Festival, April 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the National Media Exploitation Center (NMEC), April 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the Defense Forensics and Biometrics Agency (DFBA), February 2014.
- *Digital Multimedia Forensics and Anti-Forensics*, Presented to the National Institute of Standards and Technology (NIST), March 2013.

## UNIVERSITY AND DEPARTMENTAL SERVICE

- *College-Level Committee Membership*
  - ECE Department Head Search Committee, 2017 - 2018
  - MS in Cybersecurity Degree Revision Committee, 2017 - Present
- *Departmental Committee Membership*
  - Planning and Development Committee, 2017 - Present
  - Assessment and Accreditation Committee, 2015 - Present
  - Machine Learning Curricular Revision Committee, 2014 - 2015
- *Ph.D. Qualifying Examination Committee Member* (Total: 17, Chair: 2)
  - Chenxi Li (Adv. Cohen) - June 18, 2018
  - Oday Bshara (Adv. Dandekar) - April 19, 2018
  - Zhengqiao Zhao (Adv. Rosen) - September 7, 2017
  - Yirui Liu (Adv. Walsh) - June 11, 2017
  - Xinwei Zhao (Adv. Stamm) - June 1, 2017
  - Chen Chen (Adv. Adv. Stamm) - May 31, 2107
  - Owen Mayer (Adv. Stamm) - May 1, 2017
  - Belhassen Bayar (Adv. Stamm) - April 25, 2017
  - Kyle Juretus (Adv. Savidis) - June 15, 2016
  - Stephen Woloszynek (Adv. Rosen) - September 29, 2015
  - Jonathan Stokes (Adv. Weber) - September 16, 2015
  - Yitian Shao (Adv. Visell) - May 27, 2015
  - Solmaz Torabi (Adv. Walsh) - January 13, 2015
  - Pingge Jiang (Adv. Shackleford) - September 23, 2014 **(Chair)**

  - Ni An (Adv. Weber) - September 22, 2014
  - Arjun Rajasekar (Adv. Hrebien & Kam) - July 2, 2014 **(Chair)**
  - Michael Caro (Adv. Kim) - December 4, 2013

- *Ph.D. Thesis Proposal Committee Member* (Total: 15, Chair: 4)
  - Owen Mayer (Adv. Stamm) - July 18, 2018
  - Ni An (Adv. Weber) - December 4, 2017 **(Chair)**
  - Pingge Jiang (Adv. Shackleford) - November 9, 2017 **(Chair)**
  - Stephen Woloszynek (Adv. Rosen) - December 1, 2017 **(Chair)**
  - Belhassen Bayar (Adv. Stamm) - July 11, 2017
  - Rajath Soans (Adv. Shackleford) - April 21, 2017 **(Chair)**
  - William Osei-Bonsu (Adv. Kandasamy, Co-Adv. Stamm) - February 15, 2017
  - Jie Ren (Adv. Walsh) - April 1, 2016
  - Marko Janko (Adv. Visell & Kam) - August 31, 2015
  - Tingshan Huang (Adv. Sethu & Kandasamy) - June 18, 2015
  - Brandon Morton (Adv. Kim) - June 4, 2015
  - Matthew Prockup (Adv. Kim) - January 22, 2015
  - Bradford Boyle (Adv. Weber) - August 13, 2014
  - Zexi Liu (Adv. F. Cohen) - May 20, 2014
  - Sayandeep Acharya (Adv. Kam) - January 16, 2014

- *Ph.D. Thesis Committee Member* (Total: 12, Chair: 4)
  - Belhassen Bayar (Adv. Stamm) - August 6, 2018
  - Pingge Jiang (Adv. Shackleford) - July 16, 2018 **(Chair)**
  - Stephen Woloszynek (Adv. Rosen) - May 29, 2018 **(Chair)**
  - Solmaz Torabi (Adv. Walsh) - May 14, 2018 **(Chair)**
  - Rajath Soans (Adv. Shackleford) - December 1, 2017 **(Chair)**
  - Marco Janko (Adv. Visell, Co-Adv. Kam, Acting Adv. Stamm) - September 12, 2017
  - Brandon Morton (Adv. Kim) - April 22, 2016
  - Matthew Prockup (Adv. Kim) - May 3, 2016
  - Bradford Boyle (Adv. Weber) - May 27, 2015
  - Donald Bucci (Adv. Kam) - February 13, 2015
  - Sayandeep Acharya (Adv. Kam) - November 7, 2014
  - Zexi Liu (Adv. F. Cohen) - September 24, 2014

- *M.S. Thesis Defense Committees* (Total: 3, Chair: 2)
  - Jenna Schabdach - (Adv. Shackleford) - May 24, 2016 **(Chair)**

  - Andrew Benton (Adv. Shackleford) - June 8, 2015 **(Chair)**
  - Daniel Zalkind (Adv. Kam) - May 15, 2014

- *Other Departmental Service Activities*
  - Organized (with Gail Rosen) invited seminar by Dr. Min Wu, IEEE Signal Processing Society Distinguished Lecturer - October 18, 2016
  - Served as Judge for the 8th annual Drexel IEEE Graduate student Forum's Research Symposium - February 26, 2016
  - Developed a *Multimedia Forensics* session for the 2015 Drexel University Code Academy (DUCA) - A month-long program hosted by Drexel University for 25-30 high school juniors and seniors interested in computing
  - Prepared and delivered presentation to the Freshmen Design Revision Committee on freshman engineering design projects utilized at other universities and how they could be adopted at Drexel - November 10, 2016
  - Prepared and delivered presentation to the Senior Design Task Force on a Capstone Course alternative to the current Senior Design curriculum and how this is implemented at other universities - February 16, 2016
  - Volunteer at Spring 2015 ECE Department Open House - March 5, 2015
  - Volunteer at the 2014 ECE Deptartment Accepted Students Day - April 5, 2014
  - Volunteer at Fall 2013 ECE Department. Open House - November 10, 2013

- *Research Demonstrations Presented on Behalf of the Drexel University ECE Department*
  - Created and administered two demonstrations for Drexel University's 2018 ECE Day - Feb 19, 2018
  - Created a demonstration for ECE Open House events (presented by Ph.D. students Xinwei Zhao and Chen Chen) - August 20, 2017
  - Created and administered two demonstrations for Drexel University's 2017 ECE Day - February 21, 2017
  - Created a demonstration to represent Drexel at the Colloquium for Information Security and Education (CISSE) - June 12, 2016
  - Created and administered two demonstrations for Drexel University's 2016 ECE Day - February 23, 2016

- *Speaker at the Following Events on Behalf of the Drexel University ECE Department*
  - Vanguard Innovation Team meeting as part of a session to build academic collaborations between Drexel and Vanguard - May 30, 2017
  - Drexel University's meeting with Xinli Gu, Senior Director of DFX Technology of Huawei North America Network Division - December 2, 2015
  - A. J. Drexel Cybersecurity Senior Advisory Board meeting - March 10, 2015
  - ECE Employer Circle meeting - April 2014
  - ECE Advisory Council meeting - October 4, 2013

## PROFESSIONAL SERVICE ACTIVITIES

*General Chair of the Following Conferences*:

- 2017 ACM Workshop on Information Hiding and Multimedia Security - Philadelphia, PA

*Professional Society Leadership Activities*:

- Information Forensics and Security Technical Committee, IEEE Signal Processing Society
  *Elected Member (2018-2020 Term)* - This committee oversees and organizes conferences, publications, awards, and educational activities related to information security, multimedia forensics, steganography, biometrics, cryptography, authentication, and other security related research.

*Organizer of the Following International Competitions*:

- 2018 IEEE Signal Processing Cup *(Lead Organizer)*
  This competition, held annually by IEEE Signal Processing Society, challenges teams of undergraduate students from around the world to tackle real problems in signal processing and machine learning. The first round was run in conjunction with Kaggle and the final competition was held at the 2018 IEEE International Conference on Accoustics, Speech, and Signal Processing.

*Editorial Board Membership*

- IEEE SigPort

*Special Session Organizer for the Following Conferences*:

- 2018 European Signal Processing Conference (EUSIPCO)
  - Special Session on Adversarial Dynamics (Co-Organized with Benedetta Tondi and Mauro Barni)
- 2015 SPIE Electronic Imaging - Media Watermarking, Security, and Forensics
  - Special Session on Anti-Forensics (Co-Organized with H. Taha Sencar)

*Invited Reviewer for the Following Research Journals*

- IEEE Transactions on Image Processing
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Circuits and Systems for Video Technology
- IEEE Transactions on Multimedia
- IEEE Journal of Selected Topics in Signal Processing
- IEEE Transactions on Cybernetics (B)
- IEEE Signal Processing Letters
- Journal of Visual Communication and Image Representation (Elsevier)
- Signal Processing (Elsevier)

- Information Sciences (Elsevier)
- Computers & Security (Elsevier)

*Technical Program Committee Member for the Following Conferences*

- IEEE International Conference on Image Processing (ICIP) – 2014, 2015, 2016, 2017, 2018
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) – 2014, 2016, 2017, 2018
- IEEE Workshop on Information Forensics and Security (WIFS) – 2014, 2015, 2017, 2018
- ACM Workshop on Information Hiding & Mutimedia Security (IH&MMSec) –2017, 2018
- IEEE International Workshop on Multimedia Signal Processing (MMSP) – 2012

*Reviewer or Subreviewer for the Following Conferences*

- IEEE International Conference on Image Processing (ICIP) – 2008, 2009, 2010, 2012
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) – 2011, 2012
- IEEE Workshop on Information Forensics and Security (WIFS) – 2013
- European Signal Processing Conference (EUSIPCO) – 2012
- International Information Hiding Conference – 2011
- International Workshop on Digital Watermarking (IWDW) – 2011

*Reviewer for the Following NSF Programs*

- Ad-hoc reviewer for Secure and Trustworthy Cyberspace (SaTC) - 2015

## FUNDED PROPOSALS - $2,404,514

[1] M. C. Stamm (PI), J. Shackleford, and N. Kandasamy, "High performance techniques to identify the source and authenticity of digital videos using multimedia forensics," *Army Research Office (ARO)*, July 1, 2017 – June 30, 2019,
Funded Amount: **$648,572**.

[2] S. Weber (PI), M. C. Stamm, and K. Dandekar, "Security by design: Drexel hands-on cybersecurity laboratory curriculum expansion," *National Security Agency (NSA)*, October 1, 2017 – September 30, 2018,
Funded Amount: **$255,429**.

[3] M. C. Stamm (Drexel University PI), with M. Kozak (PI - PAR Government), B. Klare (Rank One Computing), C. Sisson (Rochester Institute of Technology), and J. Corso (University of Michigan), "Project MediSphere," *Defense Advanced Research Projects Agency (DARPA) - MediFor Program*, May 2016 – February 2019,
Funded Amount: **$541,996.84** (Amount Awarded to Stamm/Drexel).

[4] M. C. Stamm (PI), "CAREER: Scaling multimedia forensic algorithms for big data and adversarial environments," *National Science Foundation – Faculty Early Career Development Program (NSF CAREER)*, March 2016 – February 2021,
Funded Amount: **$583,578**.

[5] M. C. Stamm (PI) and N. Kandasamy, "High performance techniques to identify source of digital images using multimedia forensics," *Defense Forensics & Biometrics Agency (DFBA) and Army Research Office (ARO)*, Feb. 1, 2015 – July 31, 2016,
Funded Amount: **$374,939**.

## CITATIONS

- Publications cited 1505 times, $h$-index of 18
- Citation information listed here and for individual publications retrieved via Google Scholar on August 15, 2018. Google Scholar profile available at the following url:

  `https://scholar.google.com/citations?hl=en&user=UE1rg1IAAAAJ`

## JOURNAL PUBLICATIONS

[1] M. C. Stamm, P. Bestagini, L. Marcenaro, and P. Campisi, "Forensic camera model identification: Highlights from the ieee signal processing cup 2018 student competition," *IEEE Transactions on Information Forensics and Security*, Sep. 2018.

[2] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, [**#2 Most accessed article in IEEE TIFS during June 2018**]
*Citations*: 1.

[3] O. Mayer and M. C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762–1777, Jul. 2018.

[4] T. Huang, N. Kandasamy, H. Sethu, and M. C. Stamm, "An efficient strategy for online performance monitoring of datacenters via adaptive sampling," *IEEE Transactions on Cloud Computing*, Accepted and published on IEEE Xplore in 2016, To appear in print,
*Citations*: 3.

[5] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of media forensics: The forensicability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 774–788, Apr. 2016,
*Citations*: 4.

[6] X. Chu, M. C. Stamm, and K. J. R. Liu, "Compressive sensing forensics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1416–1431, Jul. 2015,
*Citations*: 10.

[7] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "On antiforensic concealability with rate-distortion tradeoff," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1087–1100, Mar. 2015,
*Citations*: 8.

[8] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1456–1468, Sep. 2013,
*Citations*: 88.

[9] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, 2013, [**Nominated for the IEEE Signal Processing Society Overview Paper Award**]
*Citations*: 157.

[10] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, Aug. 2012,
*Citations*: 105.

[11] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1050–1065, Sep. 2011,
*Citations*: 158.

[12] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010,
*Citations*: 221.

## JOURNAL PUBLICATIONS UNDER REVIEW

[1] B. Bayar and M. C. Stamm, "Accurate and robust source camera model identification via constrained convolutional neural networks," *currently under review in IEEE Transactions on Information Forensics and Security*, submitted Jul. 2018.

[2] S. DeCelles, B. Bayar, M. C. Stamm, and N. Kandasamy, "Data reduction, compressed sampling, and recovery for online performance monitoring," *currently under review in IEEE Transactions on Network Service Management*, submitted Jul. 2018.

## JOURNAL PUBLICATIONS ACTIVELY IN PREP

[1] O. Mayer and M. C. Stamm, "Deep learning based forensic similarity for digital images," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[2] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[3] X. Zhao, C. Chen, and M. C. Stamm, "Anti-forensically falsifying an image's processing history using a generative adversarial network," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. 2018.

[4] B. Hosler and M. C. Stamm, "Forensic identification of an image's source social network," *in preparation for submission to IEEE Signal Processing Letters*, to be submitted Aug. / Sep. 2018.

[5] X. Zhao, C. Chen, and M. C. Stamm, "A generative adversarial network based attack to falsify an image's source camera model," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Aug. / Sep. 2018.

[6] L. Bondi, P. Bestagini, S. Tubaro, and M. C. Stamm, "A new approach for performing falsified image region identification and localization using deep forensic feature inconsistencies," *in preparation for submission to IEEE Transactions on Information Foresnics and Security*, to be submitted Oct. 2018.

## CONFERENCE PUBLICATIONS (PEER REVIEWED)

[1] C. Chen, X. Zhao, and M. C. Stamm, "MISLGAN: An anti-forensic camera model falsification framework using a generative adversarial network," in *IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, Sep. 2018.

[2] M. Barni, M. C. Stamm, and B. Tondi, "Adversarial multimedia forensics: Overview and challenges ahead," in *European Signal Processing Conference (EUSIPCO)*, Rome, Italy, Sep. 2018.

[3] O. Mayer, B. Bayar, and M. C. Stamm, "Learning unified deep features for multimedia forensic tasks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Innsbruck, Austria, Jun. 2018,
*Citations*: 1.

[4] O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018.

[5] B. Bayar and M. C. Stamm, "Towards open set camera model identification using a deep learning framework," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018,
*Citations*: 2.

[6] B. Bayar and M. C. Stamm, "Towards order of processing operations detection in JPEG-compressed images with convolutional neural networks," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics*, Burlingame, CA, Feb. 2018, pp. 211–1–211–9,
*Citations*: 3.

[7] B. Bayar and M. C. Stamm, "Augmented convolutional feature maps for robust cnn-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4098–4102,
*Citations*: 4.

[8] C. Chen and M. C. Stamm, "Image filter identification using demosaicing residual features," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 4103–4107.

[9] C. Chen, X. Zhao, and M. C. Stamm, "Detecting anti-forensic attacks on demosaicing-based camera model identification," in *IEEE International Conference on Image Processing (ICIP)*, Beijing, China, Sep. 2017, pp. 1512–1516,
*Citations*: 1.

[10] O. Mayer and M. C. Stamm, "Countering anti-forensics of lateral chromatic aberration," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 15–20,
*Citations*: 1.

[11] B. Bayar and M. C. Stamm, "A generic approach towards image manipulation parameter estimation using convolutional neural networks," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, 2017, pp. 5–10,
*Citations*: 4.

[12] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in *accepted for publication in IEEE International Conference on Accoustics, Speech, and Signal Processing (ICASSP)*, New Orleans, LA, Mar. 2017, pp. 2152–2156,
*Citations*: 16.

[13] B. Bayar and M. C. Stamm, "Design principles of convolutional neural networks for multimedia forensics," in *IS&T Symposium on Electronic Imaging (EI) - Media Watermarking, Security, and Forensics - Special Session on Deep Learning for Multimedia Security*, San Francisco, CA, Feb. 2017, pp. 77–86,
*Citations*: 16.

[14] O. Mayer, D. C. Lim, A. I. Pack, and M. C. Stamm, "Classification of sleep states in mice using generic compression algorithms," in *EEE Signal Processing in Medicine and Biology Symposium (SPMB)*, Dec 2016, pp. 1–2.

[15] X. Zhao and M. C. Stamm, "Computationally efficient demosaicing filter estimation for forensic camera model identification," in *IEEE International Conference on Image Processing*

*(ICIP)*, Sep. 2016, pp. 151–155,
*Citations*: 5.

[16] S. DeCelles, , T. Huang, M. C. Stamm, and N. Kandasamy, "Detecting incipient faults in software systems: A compressed sampling-based approach," in *IEEE International Conference on Cloud Computing (CLOUD)* ***(15% acceptance rate)***, Jun. 2016, pp. 303–310.

[17] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Vigo, Galicia, Spain, 2016, pp. 5–10,
*Citations*: 76.

[18] O. Mayer and M. C. Stamm, "Improved forgery detection with lateral chromatic aberration," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, Mar. 2016, pp. 2024–2028,
*Citations*: 4.

[19] S. DeCelles, M. C. Stamm, and N. Kandasamy, "Efficient online performance monitoring of computing systems using predictive models," in *IEEE/ACM International Conference on Utility and Cloud Computing (UCC)* ***(27.5% acceptance rate)***, Limassol, Cyprus, Dec. 2015, pp. 152–161.

[20] C. Chen and M. C. Stamm, "Camera model identification framework using an ensemble of demosaicing features," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Rome, Italy, Nov. 2015, pp. 1–6,
*Citations*: 20.

[21] O. Mayer and M. C. Stamm, "Anti-forensics of chromatic aberration," in *Proc. IS&T SPIE Electronic Imaging, Media Watermarking, Security, and Forensics*, San Francisco, CA, Feb. 2015, pp. 94 090M–94 090M,
*Citations*: 5.

[22] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of compression forensics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014, pp. 2689–2693,
*Citations*: 8.

[23] M. C. Stamm, X. Chu, and K. J. R. Liu, "Forensically determining the order of signal processing operations," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, Guangzhou, China, Nov. 2013, pp. 162–167,
*Citations*: 18.

[24] M. C. Stamm and K. J. R. Liu, "Protection against reverse engineering in digital cameras," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Special Session on Adversarial Signal Processing*, Vancouver, Canada, May 2013, pp. 8702–8706,
*Citations*: 3.

[25] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "Concealability-rate-distortion tradeoff in image compression anti-forensics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013, pp. 3063–3067,
*Citations*: 5.

[26] Z.-H. Wu, M. Stamm, and K. Liu, "Anti-forensics of median filtering," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013, pp. 3043–3047,
*Citations*: 29.

[27] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics based on the autoregressive model of median filtered residual," in *Asia-Pacific Signal Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Hollywood, California, Dec. 2012, pp. 1–9,
*Citations*: 25.

[28] X. Chu, M. Stamm, and K. Liu, "Forensic identification of compressively sensed signals," in *IEEE International Conference on Image Processing (ICIP)*, Orlando, Florida, Sep. 2012, pp. 257–260,
*Citations*: 3.

[29] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensics vs. anti-forensics: A decision and game theoretic framework," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 1749–1752,
*Citations*: 43.

[30] X. Chu, M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensic identification of compressively sensed images," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 1837–1840,
*Citations*: 10.

[31] M. C. Stamm and K. J. R. Liu, "Anti-forensics for frame deletion/addition in MPEG video," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague, Czech Republic, May 2011, pp. 1876–1879,
*Citations*: 31.

[32] M. C. Stamm and K. J. R. Liu, "Wavelet-based image compression anti-forensics," in *IEEE International Conference on Image Processing (ICIP)*, Hong Kong, China, Sep. 2010, pp. 1737–1740,
*Citations*: 32.

[33] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *IEEE International Conference on Image Processing (ICIP)*, Hong Kong, China, Sep. 2010, pp. 2109–2112,
*Citations*: 83.

[34] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *International Conference on Acoustics Speech and Signal Processing*

*(ICASSP)*, Mar. 2010, pp. 1698–1701,
*Citations*: 64.

[35] S. K. Tjoa, M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Harmonic variable-size dictionary learning for music source separation," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1698–1701,
*Citations*: 12.

[36] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Anti-forensics of jpeg compression," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1694–1697,
*Citations*: 99.

[37] M. C. Stamm and K. J. R. Liu, "Forensic detection of image tampering using intrinsic statistical fingerprints in histograms," in *Asia-Pacific Signal Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Sapporo, Japan, Oct. 2009, pp. 563–572,
*Citations*: 22.

[38] M. C. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in *IEEE International Conference on Image Processing (ICIP)*, San Diego, CA, Oct. 2008, pp. 3112–3115,
*Citations*: 87.

## PATENTS

[1] O. Mayer and M. C. Stamm, "Learned forensic source system for identification of image capture device models," *U.S. Patent Application No. 62/652,651*, Provisional patent filed April 4, 2018.

# Appendix A Unsolicited Letter From A Student Praising My Teaching

In July 2015, James Esser, a student in my Spring 2015 ECES 301: Transform Methods & Filtering class, sent an unsolicited letter praising my teaching to Dr. John DiNardo, Senior Vice Provost of Academic Affairs. This letter is included on the following page (this copy corresponds to an electronic copy shared with me after the printed and signed copy was shared with SVP DiNardo).

Dr. John DiNardo
Office of the Provost
Drexel University
3141 Chestnut St.
Philadelphia PA, 19104

To whom it may concern,

My name is James Esser, I am a junior computer engineering student and Drexel Men's Lacrosse Team player. The last three years of my academic career have been challenging and rewarding. And while my passions are driven by the academic subject matter, the true inspiration I have experienced during my studies has been the result of a few people who selflessly dedicate themselves to their students' futures. I would like to bring your attention to one such faculty member—Dr. Mathew Stamm.

I have been fortunate enough to study under Dr. Stamm for two terms; and I am not ashamed to say his curriculum has been the most difficult and challenging I have faced. However, his approach to these real-world challenges breeds contagious enthusiasm. I have witnessed his patient dedication motivate aspiring engineers to tackle these seemingly insurmountable engineering obstacles with growing confidence and pride. His uninhibited commitment to his students, his approachable nature, and his understanding that education is about relationships and not disimpassioned lecturing makes him an exceptional academic leader.

Many times I have struggled to understand how the collegiate coursework I am devoting myself to can be applied in a practical manner. Dr. Stamm's involvement in cutting edge defense research, and his willingness to bring those experiences and accomplishments into the classroom, provides students with invaluable insight into the possibilities of engineering today.

Dr. Stamm is an exceptionally honest individual. When unfortunate instances of academic dishonesty and honor code violations have occurred, Dr. Stamm has taken great strides to cultivate an environment that facilitates honesty, hard work, and collaboration. He has espoused a principled approach to learning centered on educational morality and fairness, and discouraged students from focusing merely on grade point averages. He is an inspiration for myself and many students like me.

Drexel University is an excellent academic institution with a wonderful history and precedent for educating some of the world's finest professionals. It is professors like Dr. Stamm that continue this tradition and deserve to be recognized for their tireless efforts on behalf of the University and its students.

Sincerely,

James Esser

Class of 2016

# Appendix B Course Syllabi

Syllabi for the following courses are included in this appendix on the subsequent pages:

- ECES 301: Transform Methods & Filtering
- ECES 435: Recent Advances in DSP - Multimedia Signal Processing and Information Security
- ECES T680: Forensic Signal Processing

# ECES 301: Transform Methods and Filtering I (Spring 2017)

---

**Course details**

| | |
|---|---|
| Lecture times | 12:30–1:50pm, Tuesdays and Thursdays |
| Lecture room | Curtis 340 |
| | |
| Instructor | Matthew Stamm (Dept. of ECE) |
| Instructor email | mstamm@coe.drexel.edu |
| Instructor office | Bossone 413G |
| Instructor office hours | Tuesdays 2-3pm |
| | |
| Recitation times | (Section 060) 9:00–10:50am, Fridays |
| | (Section 061) 11:00am–12:50pm, Fridays |
| | (Section 062) 1:00-2:50pm, Fridays |
| Recitation & Lab room | Randell 323 |
| | |
| Teaching Assistant | Alejandro Trofimoff |
| TA email | etrofimoff@hotmail.com |
| TA office hours | Thursdays 3-4pm |
| TA office hours location | Bossone 604B |
| | |
| Teaching Assistant | Zhuo Wang |
| TA email | spirit0607@gmail.com |
| TA office hours | Mondays 1-2pm |
| TA office hours location | Bossone 404 (Will likely change) |

**Course Description**

This course covers time and frequency domain analysis of both continuous and discrete time signals and systems. Topics covered include a discussion of fundamental signals and basic system properties, convolution, the Fourier series, the Fourier transform, and introductory filtering. Students will learn to design and analyze the input output relationships of linear time-invariant signals, and will discuss applications in the field of electrical engineering.

**Course Prerequisites**

- Either ENGR 232 or MATH 262
- ECE 201
- ECE 205 or BMES 372

**Course objectives / learning outcomes**

1. An understanding of various signal classifications, such as continuous-time vs. discrete-time and periodic vs. aperiodic, and of various system properties such as linearity, time-invariance, causality, and stability.
2. An understanding of how a linear, time invariant system's output can be determined by convolving its input with its impulse response.
3. An understanding of a how a periodic signal can be represented as the sum of a set of harmonically related complex exponentials using the Fourier Series.
4. An understanding of how to represent an aperiodic signal in the frequency domain using the Fourier Transform.

5. An understanding of how frequency domain methods can be used to determine a linear, time invariant system's output given its input and frequency response.

**Textbook**

- *Signals and Systems, 2nd Edition* by Alan V. Oppenheim and Alan S. Willsky with S. Hamid Nawab, Prentice Hall, 1996.
- The textbook is required. Homework problems will be assigned from this book, so please be sure to acquire a copy for yourself.

**Course logistics**

- Website
  - We will use Drexel's **Blackboard Learn** course management website for this class extensively.
  - I will mail you important information regarding the class through this system. Please make sure you setup the system to forward BB/Learn emails to an account you check regularly.
  - Homework, homework solutions, supplemental materials, etc. will be posted on the main course page.
  - The gradebook will hold your homework and midterm exam scores.
  - If you want to email me or the TAs, please do so at the email addresses listed above. This is preferred to emailing us from within BB/Learn.
- Lectures
  - **Laptops** are not to be used during lecture without prior approval by the instructor.
  - **Cell phones** are to be turned off. You should not be talking, web-surfing, or texting on your phone during class. If you need to use your phone in any way, please leave the classroom.
  - Please ask questions. If you are confused, then there is a very good chance someone else in the class is confused as well.
  - Read the indicated sections of the textbook for each lecture in advance. This will greatly improve your understanding of the material.
- Attendance
  - Attendance in lectures is not mandatory but is **strongly encouraged**.
  - Attendance in recitation **is mandatory**. Quizzes and exams will be held during your recitation section. This will be discussed in greater detail below.
- Homework
  - Working problems is the number one way to succeed in this class. Again: it is impossible to succeed in this class without dedicating substantial effort to the working of problems.
  - HW sets will be assigned every week.
  - HW is due at the **beginning of class** one week after it is assigned. HW may not be handed in late under any circumstance.
  - The lowest two HW grades will be dropped. If you are late with a HW submission, do not ask for an extension. We drop the lowest two HW grades to account for this.
  - HW may not be submitted electronically.

  - Your homework submission must be your own original work. You are allowed and encouraged to discuss the homework with other students, but the work and solutions you submit must be your own. **Copying homework solutions from another student is cheating**.
  - You must show your work in your homework submissions to receive credit for it. Unless the solution to a question is obvious, you will not receive credit for simply writing the answer to a problem, even if that answer is correct.
  - All homework submissions must meet following guidelines:
    * Homework should be neat and legible.
    * Your **full name** and **section number** must appear on the front page.
    * Each problem should be clearly numbered.
    * Problems should appear in the order in which they are assigned.
    * You must box your final answer.

    Homework that does not meet these guidelines may not be graded. Please understand we have a very large class and must insist on these requirements in order to expedite the grading process.
  - Due to the class size, the TAs may not thoroughly grade every problem. At least one question per homework will be graded closely for accuracy. Effort must be demonstrated on every problem in order to get full credit, even if not all answers are graded.

- Recitations
  - Recitations will reinforce the concepts introduced in lecture. They will focus on working problems and on applications of the theory discussed in lecture.
  - Recitations will consist of a quiz or exam, example problems worked on the board, a participation component where you may/will be asked to work problems on the board, as well as an opportunity to ask questions about the material.
  - In order to earn credit for your recitation grade, you must satisfactorily work through at least one problem on the board during the course.

- Quizzes
  - There will be weekly quizzes held during recitation on weeks in which an exam does not occur.
  - These quizzes will be similar to a question from the previous homework. If you completed each homework and reviewed the solutions, this should leave you well prepared for each quiz.
  - Quizzes are closed-book and closed notes. You may use a calculator with basic functionality. **You may NOT use a graphing calculator**, any device capable of advanced operations such as symbolic integration, or any device capable of accessing the Internet.

- Exams
  - There will be two different midterm exams held during recitation. These exams will tentatively occur on Friday 5/5 (Week 5), and Friday 6/2 (Week 9), though these dates may change. Historically, exams in this class have a nonzero chance of been pushed back one week. Please be prepared in case this occurs this quarter.
  - There will be a final exam during the week of June 12. The date, time, and location of the final exam will be announced at the site: http://drexel.edu/registrar/scheduling/exams/
  - The final exam is comprehensive; it will cover the entire course.

  - Exams are closed-book and closed notes. You may use a calculator with basic functionality. **You may NOT use a graphing calculator**, any device capable of advanced operations such as symbolic integration, or any device capable of accessing the Internet.
  - Exams may not be rescheduled. The final exam may not be rescheduled unless you have three exams scheduled in one day. Travel is not a justification for rescheduling the final exam.
  - For some exams, I **may** allow you to bring in one $8.5 \times 11$ inch page with notes on the front and back. If this is the case, I will let you know at least one class period in advance of the exam. This note sheet will be collected along with your exam and must be handwritten by you. Typed note sheets are grounds to fail the exam. Shared note sheets are grounds to fail the exam.

- Regrade Policy
  - If you feel that a quiz or exam was not graded properly, you may submit a written regrade request to me. Regrade requests submitted by email or delivered verbally will not be processed.
  - All regrade requests must contain the following:
    * Your name.
    * Your section number.
    * The date.
    * Your email address.
    * A clear description of what you believe was graded improperly, along with why you believe you deserve more credit.
  - All regrade requests must be submitted within one week of when the quiz or exam was returned.
  - No regrade requests may be submitted until you have had the quiz or assignment for at least 24 hours.
  - Please do not submit a regrade request unless you truly feel that there was an error in the grading of your quiz or exam. Frivolous regrade requests are very time consuming to process and will delay the grading of other material.

- Office hours
  - Office hours are available to you each week at the times listed above.
  - Please come to office hours. Office hours are always a very under-utilized resource.
  - If you have a question regarding a homework problem, I expect you to have attempted solving it before coming to office hours. I am happy to help you with any problem that you are stuck on, so long as you have first put forth an effort to solve the problem on your own.
  - Due to the size of the class and my other commitments I will not in general be able to schedule meetings with you outside of designated office hours, but please email me if you feel your concern merits an exception to this rule.

**Grading**

Your final numerical grade will be computed as follows:

| Option 1 | | Option 2 | |
|---|---|---|---|
| Homework (drop 2) | 10% | Homework (drop 2) | 10% |
| Recitation Participation | 5% | Recitation Participation | 5% |
| Quizzes (drop 1) | 15% | Quizzes (drop 1) | 15% |
| Midterm Exams | 40% | Highest Midterm Exam Grade | 30% |
| Final Exam | 30% | Final Exam | 40% |

I will compute final score under both options and assign your letter grade based on the highest of the two scores. Your final numerical score will be used to assign you a letter grade for the course as follows:

| | | |
|---|---|---|
| 93 | 100 | A |
| 90 | 92 | A- |
| 87 | 89 | B+ |
| 83 | 86 | B |
| 80 | 82 | B- |
| 77 | 79 | C+ |
| 73 | 76 | C |
| 70 | 72 | C- |
| 65 | 69 | D+ |
| 60 | 64 | D |
| 0 | 59 | F |

At my discretion I may curve course grades up (but not down). If this occurs, I will assign letter grades by examining the distribution of the final numerical scores. An A will likely correspond to the highest "cluster" of scores, followed by a B for the next "cluster", and so on.

I cannot tell you what your final letter grade in the class will be at the at the week 6 withdraw deadline, however, I will try to share the distribution of scores up to that point to give you some idea of your standing in class.

**Course Outline**

Below is a tentative outline of the topics we will cover in this course and the amount of time we will spend on them. The actual order in which these topics are covered and the amount of time spent on them may be changed as the course proceeds.

| Topic | Chapter | Week |
|---|---|---|
| Introduction to signals and systems | 1 | 1–3 |
| Linear time-invariant systems and convolution | 2 | 3–5 |
| Fourier series representation of periodic signals | 3 | 5–6 |
| The continuous time Fourier Transform & Applications | 4 | 7–9 |
| The discrete time Fourier Transform | 5 | 10 (Time Permitting) |

Note: The final exam will be during the week of XXX.

**Academic Policies**

Academic integrity, plagiarism, cheating policy:
http://www.drexel.edu/provost/policies/academic-integrity/

Students with Disability Statement:
http://drexel.edu/oed/disabilityResources/overview/

Course add/drop policy:
http://drexel.edu/provost/policies/course-add-drop/

Examinations:
http://www.drexel.edu/provost/policies/overview/~/media/Files/provost/policies/pdf/examinations_grading_options_v1.pdf

# ECES 435 (Winter 2018)
# Advances in DSP: Multimedia Signal Processing and Information Security

---

**Course details**

| | |
|---|---|
| Lecture times | Tuesdays & Thursdays, 12:30-1:50pm |
| Lecture room | Lebow Engineering Center 135 |
| Lab time | Fridays 11:00- 12:50 |
| Lab room (ECES 435) | Lebow Engineering Center 134 |
| Instructor | Matthew Stamm (Dept. of ECE) |
| Instructor email | mstamm@coe.drexel.edu |
| Instructor office | Bossone 413G |
| Instructor office hours | By Appointment |
| Teaching Assistant | Oday Bshara |
| TA email | ob67@drexel.edu |
| TA office hours | By Appointment |
| TA office hours location | T.B.D. |

**Course objectives / learning outcomes**

1. An understanding of digital images and how they are represented, processed, and stored.
2. An understanding of how information can be hidden in a digital signal, particularly a digital image.
3. Familiarity with how hidden information can be used for security purposes such as watermarking or image authentication.
4. An understanding of how image processing such as compression or contrast enhancement can be forensically detected.
5. An understanding of the source of a digital image can be determined without relying on easily falsifiable traces such as metadata.

**Textbook**

- There will be no required textbook for this course.
- Required and supplemental reading will be periodically posted to the course's Blackboard Learn website.

**Course logistics**

- Enrollment
  - It is **strongly recommended** that you have already taken or are currently taking ECE 361 – Probability & Statistics. Students should be familiar with probability theory, random variables, and statistics.
  - Students should have an appropriate familiarity with DSP and Matlab.
- Website
  - We will use Drexel's **Blackboard Learn** course management website for this class extensively.
  - I will mail you important information regarding the class through this system. Please make sure you setup the system to forward BB Learn emails to an account you check regularly.
  - Assignments, supplemental materials, etc. will be posted on the main course page.

  - The gradebook will hold your course assignment and midterm exam scores.
  - If you want to email me or the TAs, please do so at the email addresses listed above. This is preferred to emailing us from within BB Learn.

- Lectures
  - **Laptops** may not be used during lecture without prior approval by the instructor.
  - **Cell phones** should be set to silent and may not be used during lecture. You should not be talking, accessing the internet, or texting on your phone during class. If you need to use your phone in any way, please leave the classroom.
  - Please ask questions. If you are confused, then there is a very good chance someone else in the class is confused as well.
  - If reading is assigned, please read the material in advance of the corresponding lecture. This will greatly improve your understanding of the material.
- Attendance
  - Attendance in lectures is not required but is **strongly encouraged**. Part of your grade will be calculated from class participation. If you do not regularly attend lecture, you should expect your participation grade to be low.
- Course Assignments
  - Course assignments will be due periodically throughout the quarter. Detailed descriptions of each assignment along with their due dates will be posted on the BB Learn website.
  - A written report should be submitted for each assignment. A hard copy of this report should be turned in at the beginning of the class when the assignment is due.
  - Late assignments will not be accepted.
  - All assignments should be completed individually and your assignment report submission must be your own original work. You are allowed and encouraged to discuss assignments with other students, but the work and solutions you submit must be your own. **Copying assignment solutions or reports from another student is cheating.**
  - Code for each assignment should be written in Matlab. No other programming languages should be used to complete assignments (such as Python, C, etc) without permission of the instructor.
  - Unless explicitly noted, all code (or any other code) should be written by you. Proper attribution should be given to all code or software originating elsewhere and code from online sources should not be used without prior permission from the instructor.
  - If you are unsure if it acceptable to use software or code that you have found, please ask at least one full day before the assignment is due.
  - **Using another student's code or passing off existing code or software as your own is cheating and is strongly prohibited**.
- Midterm Exam
  - There will be one midterm exam held during this course.
  - The midterm will occur roughly half way through the quarter. More detail about this exam will given later in the quarter.

- Final Project
  - The course will culminate in a final design project. You will be allowed to choose the topic of this final project. This topic must be approved in advance by me.
  - At the end of the quarter, your team must give a presentation and a demo of your final project.
  - Your team will also prepare a final report documenting both technical details of your final project along with user documentation.
  - More detail will be given regarding the final project some time around the midpoint of the quarter.
- Office hours
  - Office hours are available to you each week at the times listed above.
  - Please come to office hours. Office hours are always a very under-utilized resource.
  - If you have a question regarding an assignment, I expect you to have attempted solving the problem before coming to office hours. I am happy to help you with any problem that you are stuck on, so long as you have first put forth an effort to solve the problem on your own.
  - Due to my other commitments I may not in general be able to schedule meetings with you outside of designated office hours. If you need to see me outside of office hours, please email me in advance. I will do best to accommodate reasonable requests to meet, but I may not always be able to meet with you due to time constraints.

**Grading**

Your final numerical grade will be computed as follows:

| | |
|---|---|
| Course assignments | 70% |
| Midterm Examination | 15% |
| Final project | 15% |

Minor adjustments to these weights may be made before the midpoint of the quarter. Any adjustments will be announced in class.

Your final numerical score will be used to assign you a letter grade for the course as follows:

| | | |
|---|---|---|
| 93 | 100 | A |
| 90 | 92 | A- |
| 87 | 89 | B+ |
| 83 | 86 | B |
| 80 | 82 | B- |
| 77 | 79 | C+ |
| 73 | 76 | C |
| 70 | 72 | C- |
| 65 | 69 | D+ |
| 60 | 64 | D |
| 0 | 59 | F |

At my discretion I may curve course grades up (but not down). If this occurs, I will assign letter grades by examining the distribution of the final numerical scores. An A will likely correspond to the highest "cluster" of scores, followed by a B for the next "cluster", and so on.

I cannot tell you what your final letter grade in the class will be at the at the week 6 withdraw deadline, however, I will try to share the distribution of scores up to that point to give you some idea of your standing in class.

**Course Outline**
Below is a tentative outline of the topics we will cover in this course. The actual order in which these topics are covered and the amount of time spent on them may be changed as the course proceeds.

| Topic |
|---|
| Introduction to image processing |
| Coding & compression |
| Information hiding, steganography & steganalysis (this may be skipped or shortened) |
| Introduction to decision theory & machine learning |
| Multimedia forensics - Manipulation detection |
| Multimedia forensics - Device identification |

**University Academic Policies**:
Missed Classes:
Absence from class will be based on the Universitys absence policy. Please review the link below.
http://drexel.edu/provost/policies/absence/

Academic Integrity, Plagiarism and Cheating Policy:
Please review the University policy regarding academic integrity:
http://drexel.edu/provost/policies/academic-integrity/
http://drexel.edu/studentlife/community_standards/studentHandbook/

Office of Equality and Diversity - Disability Resources:
Students requesting accommodations due to a disability at Drexel University need to request a current Accommodations Verification Letter (AVL) in the ClockWork database before accommodations can be made. These requests are received by Disability Resources (DR), who then issues the AVL to the appropriate contacts. For additional information, visit the DR website at drexel.edu/oed/disabilityResources/overview/, or contact DR for more information by phone at 215.895.1401, or by email at disability@drexel.edu.

Course Drop Policy:
http://drexel.edu/provost/policies/course-add-drop/

Course Withdrawal Policy:
http://drexel.edu/provost/policies/course-withdrawal/

Course Change Policy:
The instructor reserves the right to modify the course, as necessary, during the term: including policies, evaluations, due dates, course content, schedule, assignments or requirements. All changes will be communicated in lecture and/or via the course DrexelLearn page.

Weather, Emergencies and University Closing:
University closing or delayed opening information will be posted on www.drexel.edu. In the event of the need to close or delay the daily opening of a campus, the University will provide notice via Web, telephone, and the DrexelALERT system. Closing or delayed opening information will be announced at 215-895-MELT (6358).

The University determines whether to close or delay opening due to inclement weather, not the instructor. Therefore, please do not contact the instructor for this information.

# ECES T680 (Winter, 2016)
# Multimedia Forensics and Security

---

**Course details**

| | |
|---|---|
| Lecture times | 12:30-1:50pm, Mondays and Wednesdays |
| Lecture room | Drexel One Plaza Building GL13 |
| | |
| Instructor | Matthew Stamm (Dept. of ECE) |
| Instructor email | mstamm@coe.drexel.edu |
| Instructor office | Bossone 413G |
| Instructor office hours | Wednesdays 2–3 p.m. |
| | |
| Teaching Assistant | Owen Mayer |
| TA email | om82@drexel.edu |
| TA office hours | Thursdays 2-3 p.m |
| TA office hours location | Bossone 306 |

**Course objectives / learning outcomes**

1. An understanding of digital images and how they are represented, processed, and stored.
2. An understanding of how information can be hidden in a digital signal, particularly a digital image.
3. Familiarity with how hidden information can be used for security purposes such as watermarking or image authentication.
4. An understanding of how image processing such as compression or contrast enhancement can be forensically detected.
5. An understanding of the source of a digital image can be determined without relying on easily falsifiable traces such as metadata.

**Textbook**

- There will be no required textbook for this course.
- Required and supplemental reading will be periodically posted to the course's Blackboard Learn website.

**Course logistics**

- Enrollment
  - ECES 521 is a prerequisite for this course. As such, students should be familiar with probability theory, random variables, and statistics.
  - Students should have an appropriate familiarity with DSP and Matlab.
- Website
  - We will use Drexel's **Blackboard Learn** course management website for this class extensively.
  - I will mail you important information regarding the class through this system. Please make sure you setup the system to forward BB Learn emails to an account you check regularly.
  - Assignments, supplemental materials, etc. will be posted on the main course page.
  - The gradebook will hold your course assignment and midterm exam scores.
  - If you want to email me or the TAs, please do so at the email addresses listed above. This is preferred to emailing us from within BB Learn.

- Lectures
  - **Laptops** may not be used during lecture without prior approval by the instructor.
  - **Cell phones** should be set to silent and may not be used during lecture. You should not be talking, accessing the internet, or texting on your phone during class. If you need to use your phone in any way, please leave the classroom.
  - Please ask questions. If you are confused, then there is a very good chance someone else in the class is confused as well.
  - If reading is assigned, please read the material in advance of the corresponding lecture. This will greatly improve your understanding of the material.
- Attendance
  - Attendance in lectures is not required but is **strongly encouraged**. Part of your grade will be calculated from class participation. If you do not regularly attend lecture, you should expect your participation grade to be low.
- Course Assignments
  - Course assignments will be due periodically throughout the quarter. Detailed descriptions of each assignment along with their due dates will be posted on the BB Learn website.
  - A written report should be submitted for each assignment. A hard copy of this report should be turned in at the beginning of the class when the assignment is due.
  - Late assignments will not be accepted.
  - You will form groups to complete these assignments. Each group will only need to turn in one copy of the report for each assignment. Each group member should contribute approximately equally when completing each assignment.
  - Unless explicitly noted, all Matlab code should be written by you or a member of your group. Proper attribution should be given to all code or software originating elsewhere.
  - If you are unsure if it acceptable to use software or code that you have found, please ask at least one full day before the assignment is due.
  - Using another team's code or passing off existing software as your own is **strongly prohibited**.
- Midterm Exam
  - There will be one midterm exam held during this course.
  - The midterm will occur roughly half way through the quarter. More detail about this exam will given later in the quarter.
- Final Project
  - The course will culminate in a final design project. You will be allowed to choose the topic of this final project. This topic must be approved in advance by me.
  - At the end of the quarter, your team must give a presentation and a demo of your final project.
  - Your team will also prepare a final report documenting both technical details of your final project along with user documentation.
- Office hours

- Office hours are available to you each week at the times listed above.
- Please come to office hours. Office hours are always a very under-utilized resource.
- If you have a question regarding an assignment, I expect you to have attempted solving the problem before coming to office hours. I am happy to help you with any problem that you are stuck on, so long as you have first put forth an effort to solve the problem on your own.
- Due to my other commitments I may not in general be able to schedule meetings with you outside of designated office hours. If you need to see me outside of office hours, please email me in advance. I will do best to accommodate reasonable requests to meet, but I may not always be able to meet with you due to time constraints.

**Grading**

Your final numerical grade will be computed as follows:

| | |
|---|---|
| Course assignments | 50% |
| Midterm exam | 20% |
| Final project | 25% |
| Participation | 5% |

Minor adjustments to these weights may be made before the midpoint of the quarter. Any adjustments will be announced in class.

Your final numerical score will be used to assign you a letter grade for the course as follows:

| | | |
|---|---|---|
| 93 | 100 | A |
| 90 | 92 | A- |
| 87 | 89 | B+ |
| 83 | 86 | B |
| 80 | 82 | B- |
| 77 | 79 | C+ |
| 73 | 76 | C |
| 70 | 72 | C- |
| 65 | 69 | D+ |
| 60 | 64 | D |
| 0 | 59 | F |

At my discretion I may curve course grades up (but not down). If this occurs, I will assign letter grades by examining the distribution of the final numerical scores. An A will likely correspond to the highest "cluster" of scores, followed by a B for the next "cluster", and so on.

I cannot tell you what your final letter grade in the class will be at the at the week 6 withdraw deadline, however, I will try to share the distribution of scores up to that point to give you some idea of your standing in class.

**Academic Policies**

| | |
|---|---|
| Academic integrity, plagiarism, cheating policy: | www.drexel.edu/provost/policies/academic_dishonesty.asp<br>www.drexel.edu/studentlife/judicial/honesty.html |
| Students with Disability Statement: | www.drexel.edu/ods/student_reg.html |
| Course drop policy: | www.drexel.edu/provost/policies/course_drop.asp |
| Examinations: | www.drexel.edu/provost/policies/examinations.asp |

**Course Outline**

Below is a tentative outline of the topics we will cover in this course. The actual order in which these topics are covered and the amount of time spent on them may be changed as the course proceeds.

| Topic |
|---|
| Introduction to image processing |
| Coding & compression |
| Information hiding & digital watermarking |
| Introduction to decision theory & machine learning |
| Steganography & steganalysis |
| Multimedia forensics - Manipulation detection |
| Multimedia forensics - Device identification |

## Appendix C Sample Publications

The following publications are provided as a sample of my research efforts:


[1] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, **[#2 Most accessed article in IEEE TIFS during June 2018]**
http://misl.ece.drexel.edu/wp-content/uploads/2018/04/BayarStammTIFS01.pdf.

[2] O. Mayer and M. C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762–1777, Jul. 2018,
http://misl.ece.drexel.edu/wp-content/uploads/2018/02/Mayer_TIFS_2018.pdf.

[3] O. Mayer and M. C. Stamm, "Learned forensic source similarity for unknown camera models," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, Canada, Apr. 2018,
http://misl.ece.drexel.edu/wp-content/uploads/2018/05/Mayer_ICASSP18_CameraReady_13Feb2018.pdf.

[4] X. Chu, M. C. Stamm, Y. Chen, and K. J. R. Liu, "On antiforensic concealability with rate-distortion tradeoff," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1087–1100, Mar. 2015,
http://misl.ece.drexel.edu/wp-content/uploads/2017/07/Chu_TIP_2015.pdf.

[5] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1050–1065, Sep. 2011,
http://misl.ece.drexel.edu/wp-content/uploads/2017/07/Stamm_TIFS_2011.pdf.

[6] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010,
http://misl.ece.drexel.edu/wp-content/uploads/2017/07/Stamm_TIFS_2010.pdf.