eForensics Magazine

ONLINE COURSE INTRODUCTORY MATERIAL

Raahat Devender Singh

DIGITAL VIDEO FORENSICS

Uncovering the Truth in a World of Distorted Realities

Table of contents

About the course

Digital Video Forensics: Uncovering the Truth in a World of Distorted Realities

>> VISIT THE COURSE <<

DVF is a multifaceted research domain where each facet is an elaborate study in its own. The course entitled Digital Video Forensics: Uncovering the Truth in a World of Distorted Realities has been designed to offer comprehensive understanding of the digital video forensics domain, beginning with the fundamental concepts of digital videos and the technical issues related to digital video processing, to the basic knowledge of a wide range of issues associated with the evidential use and forensic analysis of video evidence, followed by the practical knowledge of various video forensic investigation procedures (including both rudimentary and specialized video content authentication and forgery detection scheme), all of which will help develop crucial analytical, problem-solving, and research skills. The participants will also gain a deep understanding of the current research gaps, open issue and future research avenues in the video forensics domain, which will act as a platform for further career and personal development. Altogether, this course will enable the participants to establish a strong foundation for the eventual development of a meaningful career in the tremendously exciting domain of video forensics.

The course has been divided into four basic modules, where each module acts as a compendium of self-contained yet cognate aspects of the domain of digital video forensics.

Module 1 (Fundamentals of Digital Videos and Digital Video Processing) provides an overview of the basic attributes of digital videos including frame-rate, bit-rate, resolution, visual quality, and essential concepts associated with digital video processing, such as spatio-temporal sampling, motion estimation, motion compensation, video encoding, data losses and impairments, noise reduction and compression. This module also presents a succinct analysis of different kinds of digital videos, where the categorization is based on the kind of acquisition device, recording parameters and environmental conditions prevalent during the acquisition process. The primary objective of this module is to

familiarize the participants with those aspects of digital videos and digital video processing which are apposite to the video forensics domain.

Module 2 (Video Evidence: Basic Concepts and Principles) presents a detailed account of the ascension of digital videos to the status of "forensic evidence", including particulars of the principles and practice of CCTV and the impact it has had on modern day surveillance. To help illustrate the significance and inculpatory nature of video evidence, the module provides examples of real-life cases of use of video evidence during criminal investigations and court proceedings. Real-life instances of footage tampering and basic principles and issues related to content authenticity and admissibility are also discussed, along with a thorough analysis of the principles and procedures involved in the collection, recovery, enhancement and authentication of forensic evidence.

Module 3 (Content Authentication and Tamper Detection in Digital Videos: Part 1 (Basic)) is geared towards the rigorous exposition of the fundamental tools and techniques used to authenticate digital videos and detect tampering therein. This module comprises of detailed study of basic active and passive forensic schemes including content authentication measures, such as source camera identification, timestamp analysis, and digital signature and watermark analysis, types of video forgeries and their creation, and basic tamper detection techniques including hash value analysis, metadata and hex editor analysis, dubbed video test, and Video Error Level Analysis (VELA).

Module 4 (Content Authentication and Tamper Detection in Digital Videos: Part 2 (Advanced)) covers the advanced topics related to digital video forensics, including evaluation of the limitations of basic tamper detection techniques discussed in Module 3, followed by thorough analysis of specialized forgery detection techniques and various forensic artifacts utilized by these techniques. Important concepts related to the effects of environmental factors and recording conditions on the content authentication process are also discussed, along with a comprehensive study of the issues, challenges and future research avenues in the domain of digital video forensics.

An essential component of all the modules is a set of unconventional and stimulating exercises that will present themselves as an opportunity for the participants to explore the various engaging aspects of video forensics, and inspire them to fully comprehend not only the societal significance of this research domain but also the extent to which it has become an integral part of today's world.

Raahat Devender Singh

The instructor

Raahat Devender Singh is a PhD research scholar and a guest lecturer working in the Department of Computer Science and Engineering in University Institute of Engineering and Technology, and the Forensics Department in Panjab University, Chandigarh, India. She has been actively working in the Digital Video Forensics domain for over three years, and her fields of specialization include digital signal processing, digital image and video content authentication and forgery detection, and forensic analysis and interpretation of digital visual media evidence. She has participated in a number of national and international conferences, and has written several articles and research papers for magazines and scientific journals of various publishing houses including Springer, World Scientific, and Elsevier

>> VISIT THE COURSE <<

DIGITAL VIDEO FORENSICS

UNCOVERING THE TRUTH IN A WORLD OF DISTORTED REALITIES

The most dangerous of all falsehoods is a slightly distorted truth.

— Georg Christoph Lichtenberg

When French inventor Nicéphore Niépce created the world's first permanent photograph in 1826, he set in motion what could only be described as a revolution of epic proportions, and though the art of photography has changed over the centuries, our fascination with the 'captured image' never did.

Our eternal preoccupation with multimedia technology has caused us to become a civilization replete with astonishing miscellanea of digital audio-visual information, and in today's world, this information is not just a source of entertainment. The endless proliferation of multimedia content in our everyday lives has been conducive to our eventual dependence on this content to the extent where our perception of reality has become strongly linked to the contents of digital images and videos, and where we expect this digital information to serve as universal, objective, and infallible records of occurrence of events.

From Video to Video Evidence

One eye-witness weighs more than ten hearsays.

— Plautus

In a world with constant surveillance and a plethora of digital multimedia capture devices, not many events of significant worth escape the watchful eye of a camera. For quite some time now, we have been relying on the visual content acquired from surveillance and intelligence systems to form the basis of countless critical and highly consequential decisions in the fields of journalism, politics, and defense planning. In the court of law, digital videos make for some of the most inculpatory evidence, simply because we as humans find it very difficult not to trust the evidence of our own eyes; it's in our biology to believe what we see. So, unlike other forms of forensic evidence, like DNA and fingerprints, which are circumstantial in nature and require further inference, digital videos provide a first-hand account of an event, and as Sherlock Holmes once remarked in A Study in Scarlet, "There is nothing like first hand evidence".

The very first instance where video footage led to a successful conviction was the James Bulger murder case of 1993. On February 12th, 1993, a CCTV camera captured fuzzy images of two-year old James being led out of the New Strand Shopping Center in Bootle, Merseyside, England by his two ten-year old killers. The surveillance video images led to the subsequent apprehension of the culprits (Joh Venables and Robert Thompson), and ever since then, there has been a steady increase in the expansion of CCTV as a surveillance technique.

Fig.1 CCTV showed James Bulger being led away from a Bootle shopping center on February 12th, 1993
BBC News http://www.bbc.co.uk/liverpool/content/articles/2006/12/04/local_history_bulger_feature.shtml

Aside from the inceptive Bulger case, there have been numerous cases where surveillance footage has led to successful convictions; some of the most notable cases include the David Copeland (London nail bomber) case of 1999, the 7/7 suicide attacks in London in 2005, the 2008 Mumbai attacks, the 2011 England riots, the Boston marathon bomber case of 2013, Carlesha Freeland-Gaither, Hannah Graham, and Levar Jones cases of 2014, the November 2015 Paris attacks, and the 2016 Brussels bombing.

The Failings of Digital Visual Content

A lie that is half-truth is the darkest of all lies.

— Alfred Tennyson

The tendency to distort the truth for personal gains is not a trait we acquire, it is a predilection ingrained deep in our consciousness. In his book 'Why We Lie: The Evolutionary Roots of Deception and the Unconscious Mind', Professor David Livingstone Smith states, "Evolutionary biology teaches us that the tendency to deceive has an ancient pedigree. We find it in many forms, at all levels, throughout the natural kingdom... ".

Digital images and videos have an incontrovertible influence on our perception of reality, and as with any technology that is powerful enough to affect society's belief system, visual media too is far from immune to man's propensity to manipulate and falsify reality for the sake of his own personal gains.

Content tampering is not a recent trend. Within half a century of the invention of photography, instances of photo tampering began to emerge. Shown below are some of the earliest examples of image tampering found in history.

Fig.2 One of the earliest examples of pre-digital photo tampering in history. (a) An iconic portrait of Abraham Lincoln (Circa 1860), was revealed to be a forgery. This image was found to have been composed by placing Lincoln's head atop South Carolina politician John Calhoun's body from (b). Another instance of photo tampering is (c), where a commissar was removed from the original photograph (d) after falling out of favor with Stalin (Circa 1930) .

Updated archive of image tampering instances throughout history: http://www.fourandsix.com/photo-tampering-history/.

(a) (b) (c) (d)

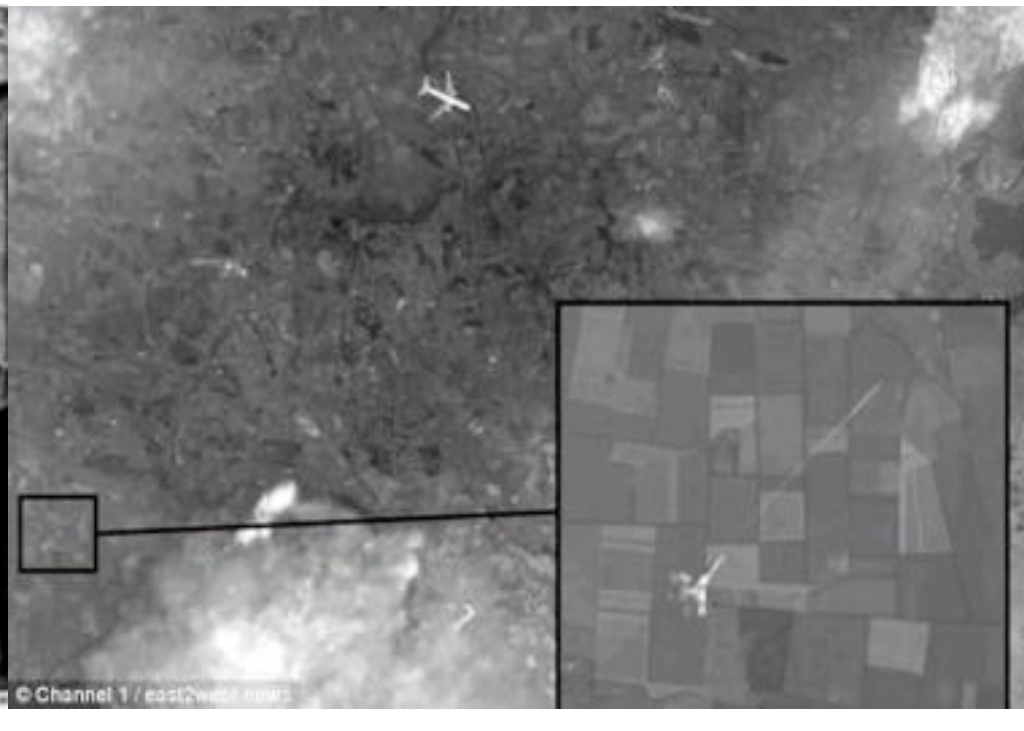
Note: Technically, a 'forgery' refers to something that is falsely made with the intent to deceive whereas 'tampering' refers to the intentional modification of structure or composition of something that would render it harmful. Despite the subtle difference, in the context of digital forensics, these terms are used synonymously.

As uncomplicated as it was to manipulate pre-digital photographs, digital images are even easier to tamper with. Following are a few instances of tampered visual content that have surfaced in the media and information world over the recent years.

These real-life examples of visual content manipulation bring to pass the somber realization that while a picture may still be worth a thousand words, those words may not necessarily be true.

Furthermore, in the wake of widespread proliferation of high-resolution digital cameras, powerful personal computers and inexpensive yet sophisticated content editing software, like Adobe Photoshop and Premier, Lightworks, Video Edit Magic, and Cinelerra, we have become aware of the fact that digital videos too can be altered without any significant effort, even by non-darkroom experts.

(a)



(b)

Fig.3 More recent examples of image tampering. (a) In November 2014, a pro-Palestinian Facebook group posted a doctored photograph of gaunt inmates of Nazi concentration camp holding signs with messages that castigated Israel and demonstrated support for Palestinians in Gaza. (b) After months of denying any involvement in the downing of Malaysian Air's flight MH17 over Ukraine, Russian state media ran a story in November 2014, calling attention to allegedly new satellite imagery it claimed substantiated that MH17 (top of the picture) had been shot down by a Ukrainian fighter jet (bottom left). Experts, however, didn't take much time to debunk the photo which was found to have been composed of pieces of Google Earth imagery from 2012 and a stock photo of a Boeing jet. It was also confirmed that the location of the plane shown in the photo did not exactly correspond to the actual path that MH17 took.

An infamous case of footage tampering came to light in January 2013, when Kendrick Johnson, a student of the Lowndes High School in Georgia, was found dead in the school gymnasium. Upon analysis of the footage from all the CCTV cameras in the vicinity of the gym, forensic investigators found that four cameras installed inside the gym were missing portions of their footage. While two cameras in the gym were missing an hour and five minutes of video, another pair of cameras was missing two hours and ten minutes each.

In yet another infamous case of footage tampering, a police car dash cam video of a citizen arrest was alleged to have been edited before its public release. In July 2015, Sandra Bland, a civil rights activist, was pulled over by the Texas Department of Public Safety trooper, and was later arrested after engaging in a heated argument with the trooper. Following her controversial death in custody three days later, the dash cam video of the arrest was publicly released. This video, however, exhibited several continuity issues (such as sudden appearance and disappearance of vehicles and people on the road, while the audio continues uninterruptedly), which made it evident that the footage was edited prior to its release.

The relative inexperience on the part of the forgers, as exhibited in the aforementioned examples, neither precludes nor undermines the very tangible threat that content tampering poses in our society today. Dutch scholar Desiderius Erasmus once said, “Man's mind is so formed that it is far more susceptible to falsehood than to truth.” In a world where video evidence has the power to make the difference between a justified conviction and an unjust acquittal, or the faculty to allow for the exoneration of defendants who might otherwise have been wrongfully convicted, judgments based on manipulated data is a travesty that we as a civilized society can ill-afford.

Video Evidence: Vulnerable yet Indispensable

Vulnerability is the birthplace of innovation, creativity and change.

— Brené Brown

While the pliability of digital visual media and its innate vulnerability to unobtrusive alterations has caused us to become skeptical of its validity, their usefulness in today's world remains incontrovertible. Fallibility of digital videos notwithstanding, it does not preclude it from being admitted as evidence. The issue of authenticity challenges faced by digital evidence is best illustrated with two pertinent rulings: "Merely raising the possibility of tampering is insufficient to render evidence inadmissible" (United States vs Allen 106 F.3d 695, 700 - 6th Cir. 1997) and "The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness" (US v. Bonallo, 858 F. 2d 1427, 1436 - 9th Cir. 1998).

Therefore, in situations where reliance on a distorted version of reality can have dangerous repercussions, it becomes paramount to validate the integrity of digital content prior to the acceptance of their content as an accurate depiction of reality. Since subjective inspection fails to provide the desired degree of conviction regarding content authenticity, specialized digital forensic techniques have to be relied upon.

Digital Video Forensics (DVF) is a branch of digital forensics that aims to provide tools and techniques that support digital video authentication and integrity verification. DVF stems from existing multimedia security related research domains (such as digital signatures and watermarking, steganography, video phylogeny and video recapture detection) and exploits image and video processing techniques to enable interpretation and investigation of digital content. The primary goal is to preserve any evidence in its most original form, all the while conducting a structured investigation to validate the digital information so as to be able to reconstruct its entire processing history, from the time it was created to its current form.

Digital Content Authentication

General Course of Action

DVF techniques help establish trustworthiness of digital content by providing answers to two crucial questions:

1) Was the video captured by the device it is claimed to have been acquired with?

2) Does the video still portray its original content?

The first question is of major interest when the source of the video is the evidence itself. This pertains to scenarios where the ownership of the acquisition device is incriminating or when the digital content can be considered accusatory or culpatory only if it was recorded by a particular device, like a surveillance camera. The techniques that attempt to identify the acquisition device are collectively referred to as Source Camera Identification Techniques.

The second question is of more general interest, the answer to which finds pertinence in everyday cases of content manipulation, and to answer this question, a rather different set of techniques is required that focus on uncovering evidence of semantic manipulations, i.e. forgeries. These are referred to as Tamper or Forgery Detection Techniques. The foundation of all such techniques is the basic fact that even if a forgery remains completely inconspicuous to the naked eye, it will undoubtedly disturb the underlying attributes and properties of the digital content. These disturbances are irreversible and emerge as certain detectable traces in the resulting content, and are generally known as "forensic artifacts" or "footprints/fingerprints of the forgery." Much like a human fingerprint, every alteration leaves its own uniquely characteristic fingerprint on the given content. Careful detection of these fingerprints or artifacts helps reverse engineer this content, so as to identify the type and order of the alterations that it underwent. Subsequent analysis enables further classification of the corresponding alteration process as malicious or innocuous.

Concluding Remarks

The truth is incontrovertible. Malice may attack it, ignorance may deride it, but in the end, there it is.

— Winston Churchill

Ubiquitous surveillance cameras that inhabit convenience stores, restaurants, malls, parks, traffic intersections, public transit systems, banks, ATMs, schools, and businesses, coupled with our cell phone cameras that extend a watchful eye to nearly every corner of every town, have engendered a plethora of digital images and videos. Constant exposure to all this visual information has led us to become dependent on its contents as a reliable portrait of 'reality' in almost every aspect of our daily lives. The significance and influence of this visual content increases considerably when it is used as evidence in making sensitive and consequential decisions that have long term effects on our society. The innate susceptibility of digital content to alterations combined with the eternal desire of humans to distort reality, the motivation for which could be to either invoke a change for the good (as in Fig. 3a) or to satisfy a malicious purpose (as in Fig. 3b), strengthen the need to devise specialized investigative procedures that are capable of establishing the trustworthiness of digital images and videos, before we decide to place our faith in the legitimacy of their contents. In the field of digital video forensics, we may have come a long way over the last two decades, but the struggle is not nearly over.

References

1. Willfried Baatz, Photography: An Illustrated Historical Overview, New York: Barron's, 1997.

2. D Smith, The Sleep of Reason: The James Bulger Case, London: Century Arrow Books, 1994.

3. David Copeland: a quiet introvert, obsessed with Hitler and bombs, Nick Hopkins and Sarah Hall, June 30th, 2000. https://www.theguardian.com/uk/2000/jun/30/uksecurity.sarahhall.

4. Intelligence and Security Committee (May 2006). "Report into the London Terrorist Attacks on 7 July 2005" (PDF). BBC News.

5. 3 witnesses identify Kasab, court takes on record CCTV footage. The Economic Times. India. June 17th, 2009.

6. London riots: Police release more CCTV suspect images, August 19th, 2011. http://www.bbc.com/news/uk-england-london-14589732.

7. Boston bomber caught on CCTV: FBI close in on suspect seen dropping bag in street, Christopher Bucktin, April 18th, 2013. http://www.mirror.co.uk/news/world-news/boston-marathon-bomber-caught-cctv-1838523

8. Found! How FBI saved Philly nurse after a citizen reported litter at kidnapper's hideout - and thanks to a GPS tracker that was put on his car because his credit was so bad, Wills Robinson, November 6th, 2014. http://www.dailymail.co.uk/news/article-2823104/Abducted-Philadelphia-woman-rescued-man-arrested.html

9. Hannah Graham: Police charge Jesse Matthew with abduction, September 24th, 2014. http://www.bbc.com/news/world-us-canada-29339013

10. Levar Jones shooting: South Carolina trooper charged in death. September 25th, 2014. http://www.foxnews.com/us/2014/09/25/sc-trooper-faces-felony-assault-charge-after-shooting-unarmed-man-during.html

11. Paris attacks suspect Abdeslam 'caught on CCTV' in French petrol station, January 11th, 2016. http://www.bbc.com/news/world-europe-35286647

12. What Happened at Each Location in the Brussels Attacks, New York Times, March 22nd, 2016. https://www.nytimes.com/interactive/2016/03/22/world/europe/brussels-attacks-graphic.html

13. Why We Lie: The Evolutionary Roots of Deception and the Unconscious Mind, David Livingstone Smith, St. Martin's Press, New York, July 1st, 2004

14. Kendrick Johnson footage released; expert finds it 'highly suspicious', Victor Blackwell, CNN, November 22nd, 2013. http://edition.cnn.com/2013/11/21/justice/kendrick-johnson-surveillance-videos/.

15. Sandra Bland Arrest Video Appears Edited, Justin Worland, July 22nd, 2015. http://time.com/3967329/sandra-bland-video-continuity/.

16. Irregularities in Sandra Bland Arrest Video Point to Tampering, July 22nd, 2015. https://sputniknews.com/us/201507221024914204/

17. Sandra Bland dashcam video: A side-by-side comparison, https://www.youtube.com/watch?v=hFXItgzLZQQ

eForensics Magazine

Written for eForensics Magazine by Raahat Devender Singh

Cover Design & DTP by Marta Strzelec

Proofreading and editing by Lee McKenzie