BOOK CHAPTER | Interpreting Images

Improving Image Interpretation in Digital Forensics

Jonathan Gasokpo Adjorlolo
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: adjonathan1017@gmail.com
Phone: +233242545875

ABSTRACT

Visual media has grown in importance as a means of communication in the digital space in recent years. The dependability of digital visual information has recently been called into question due to the ease of duplication in both content and origin. Digital image forensics is a new field of study that seeks to validate the authenticity of images by recovering information about their past. Identifying the imaging devices that captured the digital image and detecting forgery are two of the issues addressed. With the publication of study results and an increasing number of applications, digital image interpretation in digital forensics has emerged as an intriguing area for future research.

Keywords: Images, Forensic, Capturing, Visual Information, Interpretation.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Jonathan Gasokpo Adjorlolo (2022). Improving Image Interpretation in Digital Forensics . SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 23-28. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P4

1. INTRODUCTION

There is a paradigm shift in the way information is transmitted, via videos and images. They have served as both a source of evidence in our daily lives and as evidence in court. Because of the nature of videos and images, they are vulnerable to exploitation, distorting the information that the originals attempt to convey. There has been a setback in the absence of the undeniable benefit that digital visual media provides. With access to cheap, user-friendly editing tools, images and videos can be easily modified without leaving a trace and used for malicious purposes. These flaws in digital image forensics have raised more questions than answers about the use of digital images and videos as evidence. Before relying on digital images further, confirmation is required.

On September 24, 2002, a bogus photograph of George Walker Bush reading a book to schoolchildren was circulated. Because the photograph shows signs of digital editing, the true explanation is that someone took an existing photograph and flipped the image of the book in President Bush's hands.
For example, the image on the back of the book in the student's hands and the one on the back of the book President Bush is holding are mirrored, indicating that the image was manipulated.

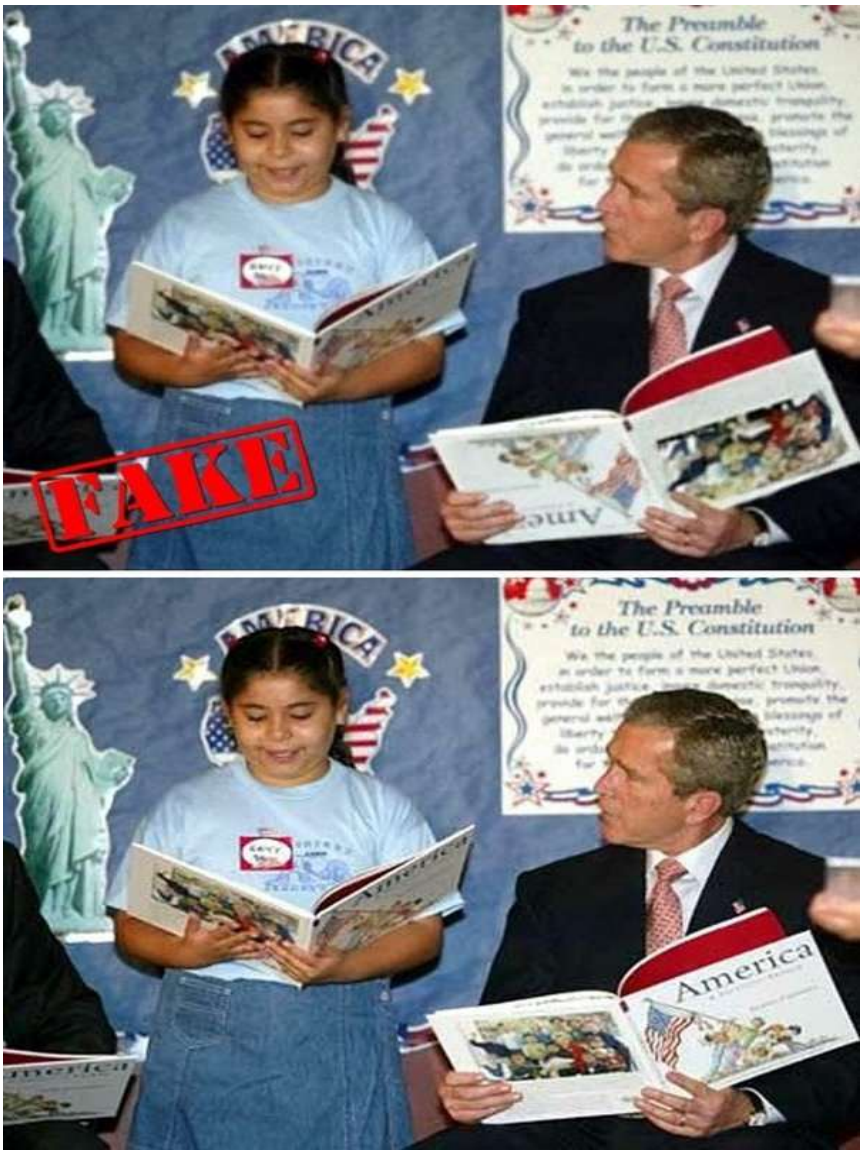

Fig 1: Original and Manipulated Image
Source: https://www.wired.com/2002/11/dubya-willya-turn-the-book-over/

The goal of digital image forensics is to provide tools to aid in blind investigation. This brand-new discipline derives from existing multimedia security-related research domains and uses image processing and analysis tools to recover information about an image's history. Under the umbrella of Digital Image Forensics, two major research paths emerge. The first category includes methods that attempt to answer question; ie by performing ballistic analysis to identify the device that captured the image or, at the very least, which devices did not capture it. These methods will be grouped together under the umbrella term "image source device identification techniques" in the sections that follow.

The second group of methods, on the other hand, seeks to uncover traces of semantic manipulation (i.e. forgeries) by examining inconsistencies in natural image statistics. These methods will be referred to as tampering detection techniques. In the era of highly digital cameras and the Internet, digital images have become one of the most popular information sources. Images, as opposed to textual information, provide an effective and natural communication medium for humans because their visual nature facilitates an effective understanding of the content.

The integrity of visual data has traditionally been accepted with confidence, such that a photographic image in a newspaper was commonly accepted as a certification of the news. Unfortunately, digital images are easily manipulated, particularly since the introduction of high-quality image-editing tools like Adobe Photoshop and Paintshop Pro. Furthermore, deep fake technology has posed a threat to the reality and integrity of image media as a result of the invention of generative adversarial networks, because this technology can easily generate photo-realistic fake images. As a result, digital-image forensics, the practice of detecting forgeries in digital images, has emerged as a significant field of study.

2. RELATED LITERATURE

Digital cameras are now very prevalent and can be found in a variety of devices such as smartphones, monitoring and surveillance cameras, and so on. Furthermore, powerful image editing software has become very common. Because digital images are so widely available, examiners, for example, can use them to assist in the resolution of crimes. However, manually analyzing a large volume of digital images is a time-consuming task. Furthermore, cognitive architecture and the brain, training and motivation, organizational factors, base rate expectations, irrelevant case information, reference material, and case evidence can all influence forensic decisions. In this context, digital image forensics (DIF) is a body of knowledge concerned with the recovery and analysis of digital evidence during the course of a criminal investigation.

DIF has primarily been used to address two issues: determining the provenance of an image and its integrity. Identifying the source of a digital image entails recognizing aspects such as the model of the camera that generated the image. To verify the integrity of a digital image, examine its contents to see if it has undergone one or more of the adulteration processes that result in a forged image. When operations on an image are performed to modify it, this is referred to as image manipulation. Image forgery considers the entire image to be maliciously exploited, whereas image tampering considers only parts of the image to be maliciously modified manipulated images. This has become more prevalent in social networks and messaging applications, providing a foundation for the phenomenon of fake news.

3. RESEARCH GAPS/ FINDINGS

We outline a number of findings and associated gaps

- How can image forgery be controlled in the digital domain and in Africa?
- How can visual images be effectively interpreted in the cyber world?
- How far can digital forensics influence the media space especially in Africa?
- How effective is image interpretation in making evidence admissible in court?

4. CONCLUSION

The exchange of digital images has become simple and widespread as imaging and communication technology has advanced. At the same time, instances of digital image manipulation have increased, necessitating a greater need for establishing ownership and authentication of the media. The community of digital image forensic researchers is constantly attempting to develop techniques for detecting the imaging device used for image acquisition, tracing the processing history of the digital image, and locating the region of tampering in digital images.

To achieve the goals, sensor, operational, and compression fingerprints were studied in conjunction with various image features. Many researcher is required to find the attempt to recover the tampered region details to be an appealing investigation domain. Many organizations' data fails to qualify for analysis using many existing techniques due to format discrepancies and the use of encryption. As a result, not only must robust forensic techniques be developed, but they must also be format independent and take encryption into account.

5. RECOMMENDATION FOR POLICY AND PRACTICE

The battle between forensic researchers and cybercriminals is never-ending, resulting in almost equal growth and development of anti-forensics techniques aimed at revealing and exploiting forensic technology weaknesses. As a result, anti-forensics techniques must be studied and investigated in order to determine which forensic techniques can be deceived. Researchers must also investigate whether these techniques leave behind any fingerprints that can be used to detect the use of anti-forensic operations.

This reduces the possibility of misclassifying anti-forensic processed images as true images, improving the reliability of existing and new forensic techniques. Anti-forensics can also be used to protect reverse engineering. The majority of image forensics research has focused on detecting the fingerprints of a specific type of interfering operation. However, in practice, a manipulated image is frequently the result of multiple such tampering operations carried out simultaneously. As a result, there is a need to develop a technique or framework capable of detecting multiple attacks and tampering.

6. DIRECTION FOR FUTURE WORKS

Many digital forensics tools designed to discover evidence are expected to reside on the suspect's device, but other features for investigating unknown and complex environments, including big data sources, are expected to be limited. As a result, the vast majority of forensic software is unsuitable for automatically or unattended detecting anomalies. As a result, one of the major challenges to be addressed in the near future is the development of tools and techniques to analyze large amounts of data and report potential digital clues to the examiner for further investigation. Engineering such tools and techniques, including appropriate visualization features to assist the forensic examiner, is a difficult task, especially given the lack of unified standards and the nontrivial computational requirements.

Fortunately, digital investigation can make use of cloud computing features, such as log analysis, data indexing, and multimedia processing, to offload the most demanding operations of digital forensics procedures. One of the most intriguing aspects of the cloud, from this perspective, is the opportunity to capitalize on a new paradigm in which forensics is provided as a utility.

Another advantage of pursuing a Function as a Service paradigm is the ability to concentrate the software in a single point, making updates and improvements easier. This can also hide complexity from end users, allowing professionals to focus on the investigation. Analogously, digital investigations can benefit from the proliferation of software-denied networking techniques, which provide additional layers of abstraction useful for analyzing attacks or infections without the need for resource-intensive traffic analysis campaigns.

Finally, digital forensics may become increasingly important in new and unexpected scenarios. The use of the Internet of things creates a point of interaction between the cyber and physical worlds, making digital Internet of things forensics an effective way to gather information about the no digital environment as well. For example, Internet of things nodes can investigate door presence sensor values to determine when a person was present in a room.

Obviously, such investigations raise additional privacy concerns, particularly because sensors may be influenced not only by a single user but by an undefined set of influencers; several people, not just the potential criminal, may trigger a presence sensor in a room each day. Because personal devices, appliances, and Internet of things nodes are beginning to "reverse the fate" of several court trials, we will look at how Internet of things and Click Per Second (CPS) can impact digital forensics in terms of both challenges and opportunities in the following section.

WEB REFERENCES

https://www.hindawi.com/journals/isrn/2013/496701/#abstract
https://www.sciencedirect.com/science/article/abs/pii/S0045790620305401
https://www.hindawi.com/journals/isrn/2013/496701/#abstract
https://link.springer.com/article/10.1007/s11042-010-0620-1