International Journal of Advances in Scientific Research and Engineering (ijasre)
ISSN: 2454-8006 [Vol. 03, Issue 4, May -2017]
www.ijasre.net

DIGITAL FORGERY

M. N. O. Sadiku[1], Sarhan M. Musa[1], and S. R. Nelatury[2]

[1]College of Engineering

Prairie View A&M University

Prairie View, TX 77446

[2]School of Engineering and Engineering Technology

Pennsylvania State University

Erie, PA 16563-1701

U.S.A

ABSTRACT

Forgery is the criminal act that provides misleading information about a product or service. It is the process of making, adapting, or imitating documents or objects with the intent to deceive. Digital forgery (or digital tampering) is the process of manipulating documents or images for the intent of financial, social or political gain. This paper provides a brief introduction to the digital forgery.

Key words: Digital forgery, Digital tampering, Electronic forgery, Online forgery

1. INTRODUCTION

Forgery has been defined as the crime of falsely altering or manipulating a document with the intension of misleading others. It may include the production of falsified documents or counterfeited items. Today, we live in the digital era, where digital technology has become predominant technology for creating, processing, transmitting, and storing information [1].

Digital forgery is falsely altering digital contents such as pictures, images, documents, and music perhaps for economic gain. It may involve electronic forgery and identity theft. The majority of digital forgery occurs because digitally altered pictures often appeal to the viewers' eyes. And with the availability of powerful, affordable picture-processing software (such as Adobe Photoshop, Adobe Premiere, Corel Draw, or GIMP), one can alter almost anything in a photo. For example, images of children (child pornography) involved in sexually explicit conduct can be created from innocent images, or even without the involvement of an actual child [2]. Digital techniques are notoriously more precise than conventional means of retouching because any area of the photo can be changed pixel by pixel. It is hard for humans to spot images that have been doctored in some way. Thus the common saying “seeing is believing” is no longer true in this digital age.

2. FUNDAMENTALS

The digital image has become one of the most important means of sending and receiving information. It is the foremost source of evidence for any event in the court of law. It is also used in forensics investigations, military, medical records, insurance, and other fields.

There are three types of image forgery: image retouching, splicing forgery, copy-move image forgery. They are illustrated in Figure 1 [3]. Regardless of the camera used to take pictures, image retouching can be used to get rid of any flaws later on. Retouching manipulates the image by changing its features without making noticeable modifications of the content. Splicing (i.e. copy paste) is a form of photographic tampering in which there is digital splicing of two or more images into a single composite. Perhaps the most common type of forgeries is the copy-move (i.e. cloning) forgery. In this forgery type, a part of the image itself is copied and pasted into another part of the same image with the aim of concealing certain features in the original images [4].

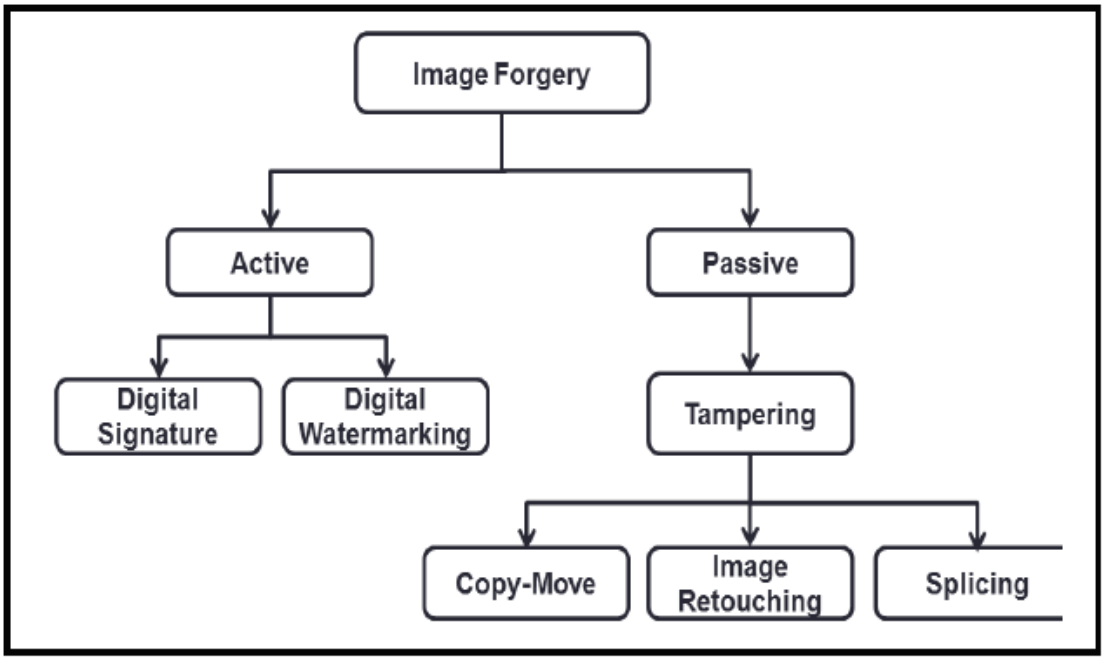

Figure 1 Classification of image forgery [3].

3. FORGERY DETECTION

As digital cameras replace analog ones, the need for authenticating digital images and detecting forgeries increases. Recent advances in technology have provided methods for detecting unethical uses of digital forgery. These include techniques for detecting cloning, splicing, resampling artifacts, color filter-array aberrations, and chromatic aberrations [5].

Forgery detection techniques can be classified into two broad categories [6]: active and passive or blind. Typical examples of active technique are watermarking and steganography . Copy move forgery detection is a common example of passive technique. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are popular algorithms for effective transformation of an image. They are both used for copy-move forgery detection [7].

Lighting inconsistencies in digital images can be used for revealing traces of digital tampering. Artificial blurring is another common process in digital image manipulation; it is used to generate plausible digital image forensics.

4. CHALLENGES

Technological advancement particularly in the area of digital imaging has posed substantial challenges for the law. Digital forgery weakens the evidentiary value of images. For digital images, security and authenticity were major issues. Computational complexity is also a major problem due to the required image processing operations.

Digitally altered images are ethically allowed as long as they lack malicious intent. But certain types of forgery may be considered felonies in all fifty states and under federal law. For example, identity theft, where a person forges the signature of another, is a felony and is punishable by a fine and some years of imprisonment.

5. CONCLUSION

Digital forgery involves changing elements of a document or image and representing the changes as true copies of the original. A number of image forgery detection schemes have been developed to compensate for human visual inspection, which is subjective and unreliable. Digital image forensics is a growing research field that supports the struggle against digital forgery and tampering.

REFERENCES

[1] S. Math and R. C. Tripathi, "Digital forgeries: Problems and challenges,"
International Journal of Computer Applications, vol. 5, no. 12, August 2010, pp. 9-12.
[2] J. A. Silversmith, "Photographic evidence, naked children, and dead celebrities: Digital forgery and the law," Harvard Law School, 1998.
[3] P. Nampoothiri and N. Sugitha, "Digital image forgery - A threaten to digital
Forensics," *Proceedings of International Conference on Circuit, Power and Computing Technologies*, 2016.
[4] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," *Proceedings of Digital Forensic Research Workshop*, 2003.

[5] H. Farid, "Exposing digital forgeries from JPEG ghosts," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, March 2009, pp. 154-160.

[6] S. Kumar, J. V. Desai, and S. Mukherjee, "Copy move forgery detection in contrast variant environment using binary DCT vectors," *I.J. Image, Graphics and Signal Processing*, vol. 6, 2015, pp. 38-44.

[7] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences*, vol. 49, no. 3, 2017, pp. 281-307.

About the authors

Matthew N.O. Sadiku, is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is an IEEE fellow. His research interests include computational electromagnetics and computer networks.

Sarhan M. Musa , is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. Dr. Musa is LTD Spring and Boeing Welliver Fellow.

Sudarshan R. Nelatury, is an associate professor at Penn State University, The Behrend College, Erie, Pennsylvania. His teaching and research
interests lie in electromagnetics and signal processing.