

Digital image fraudulence: A curse to forensic odontology

Geeta Karyakarte,
Alka Dive,
Ashish Bodhade,
Shubhangi Khandekar
*Department of Oral and
Maxillofacial Pathology, VSPM
Dental College and Research
Centre, Nagpur, Maharashtra,
India*

Address for correspondence:
*Dr. Geeta Karyakarte,
Department of Oral and
Maxillofacial Pathology, VSPM
Dental College and Research
Centre, Nagpur, Maharashtra,
India.
E-mail: geetakaryakarte@
hotmail.com*

Introduction


Keiser-Neilson in 1970 defined Forensic Odontology as “that branch of forensic medicine which in the interest of justice deals with the proper handling and examination of dental evidence and with the proper evaluation and presentation of the dental findings.”^[1] Conventionally, forensic odontology always covered human identification and injury analysis. However, tasks of forensic odontologists have broadened in recent years to cover issues related to child abuse, domestic violence, human rights protection, insurance claims, and professional ethics. For all the above tasks, records have to be maintained through casts, radiographs, and other forms. The storage of physical dental records such as dental casts and radiographs is burdened with difficulties

Abstract

In today's era of forensic investigations, hard copies of forensic data have been replaced by digital records. However, wide availability of image processing software makes digital image manipulation an easy and low-cost way to distort or conceal facts. This review article aims to understand fraudulence in the digital records in forensic odontology and the various ways to detect as well as prevent it to an appreciable extent. Types of image fraudulence, ways to detect this fraudulence, and measures to prevent it to an appreciable extent have been discussed. Knowledge about digital image fraudulence, detection, and prevention is the desperate need of the hour in today's technology-driven forensic investigations. This review article attempts to focus on this pestering issue and aid the evolving technologies driven by great needs for valid forensic technique trying to claw out their way through the malignant fraudulence rooted in today's evolving digitization.

Key words: Digital image, fraudulence, forensic odontology, investigations

of space and proves to be very expensive. This has led to increasing dependence on digital photography and digital radiology for preservation and documentation of antemortem and postmortem dental records.^[2] Images and videos have become the main information carriers in the digital era. The expressive potential of visual media as well as the ease in their acquisition, distribution, and storage is such that they are more and more exploited to convey information, even sensible. As a consequence, today images and videos represent a common source of evidence, both in everyday life controversies and in trials.^[3] Along with indubitable advantages, the accessibility of digital visual media brings a foremost shortcoming. The very nature of digital imaging makes it very easy for the operator to adjust or modify digital image files. Many such

Access this article online	
Website: www.jfds.org	Quick Response Code 
DOI: 10.4103/jfo.jfds_16_18	

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

For reprints contact: reprints@medknow.com

How to cite this article: Karyakarte G, Dive A, Bodhade A, Khandekar S. Digital image fraudulence: A curse to forensic odontology. *J Forensic Dent Sci* 2018;10:67-70.

manipulations, however, constitute inappropriate changes to the original data. Making such changes can be classified as scientific misconduct.^[4] Moreover, with the spread of low-cost, user-friendly editing tools, the art of tampering and counterfeiting visual content is no more restricted to experts. As a consequence, the modification of images for malicious purposes is now more common than ever.^[3,5] This article focuses on understanding the types of image forgery, the methods to detect them, and methods to prevent image forgery to an appreciable extent.

Types of Image Forgery

To understand the methods to detect image forgery, an understanding about the types of image forgery^[6] is necessary. Following is a short description of the ways in which a digital image can be manipulated:

Image retouching

This is the least harmful method of image manipulation. Image retouching does not lead to loss of any details of the image but may lead to enhancement of certain features, whereas diminution of others in the original image. The only aim of image retouching is to make the subject in the image more attractive and thus is the most common method of image manipulation used in magazines and hoardings. Even if the intention of this manipulation is not fraudulence, image retouching is considered unethical [Figure 1].

Image splicing or photomontage

This method refers to a pastep produced by sticking together images using digital tools available such as Photoshop. Image splicing technique involves composition of two or more images, which are combined to create a fake image^[6] [Figure 2].

Copy-move attack

In this technique, one covers a part of the image to add or remove information. A part of the same image is copied and pasted into another part of that image itself.^[6] In a copy-move attack, the intention is to hide or add something in the original image using some other part of the same image^[7] [Figure 3].

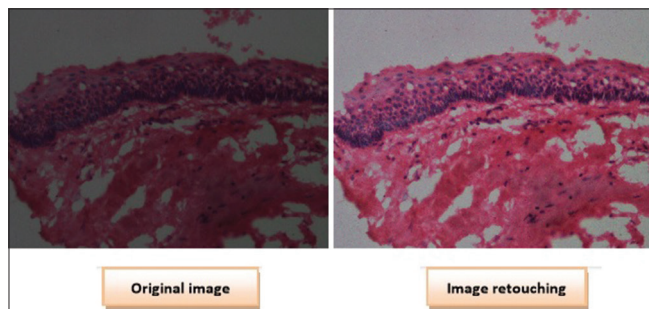


Figure 1: Original image. Image retouching

Methods to Detect Image Forgery

Joint photographic expert group format analysis

The joint photographic expert group (JPEG) format is an endless source of data that can be used for the purposes of detecting forged images. The JPEG Format Analysis algorithm makes use of information stored in the abundant technical meta-tags available in the beginning of each JPEG file. These tags contain information about quantization matrixes, Huffman code tables, chroma subsampling, and many other parameters as well as a miniature version (thumbnail) of the full image. The content and sequence of those tags, as well as which particular tags are available, depend on the image itself as well as the device that captured it or software that modified it.^[8]

In addition to technical information, JPEG tags contain important information about the photo, including shooting conditions and parameters such as ambient light levels, aperture and shutter speed information, make and model of the camera, lens with which the image was taken, focal length of the lens, whether or not flash has been used, and color profile information.^[8]

Image forgery can be detected by analyzing the discrepancies between the actual image and available exchangeable image file (EXIF) information, comparing the actual EXIF tags against tags that are typically used by a certain device (one that is specified as a capturing device in the corresponding EXIF tag).^[8]

Double-quantization effect

This algorithm is based on certain quantization artifacts appearing when applying JPEG compression more than once. If a JPEG file is opened, edited, and then saved, certain compression artifacts will inevitably appear.^[8]

To determine the double-quantization effect, the algorithm creates 192 histograms containing discrete cosine transform values. Certain quantization effects will only appear on these histograms if an image was saved in JPEG format more than once. If the effect is discovered, we can definitely tell that the image has been edited (or at least saved by a graphic editor) at least once. However, if this effect is not discovered, we cannot make any definite conclusions about the image as it could, for example, be developed from a RAW file, edited in a graphic editor, and saved to a JPEG file just once.^[8]

Error level analysis

This algorithm detects foreign objects injected into the original image by analyzing quantization tables of blocks of pixels across the image. Quantization of certain pasted objects (as well as objects drawn in an editor) may differ significantly from other parts of the image, especially if either (or both) the original image or injected objects were previously compressed in JPEG format.^[8]



Figure 2: Original image. Photomontage image description: A set of casts is duplicated by photomontage creating an illusion of more cast samples

Copy-move forgery detection

The copy-move fraudulence can be detected using various methods enlisted below:^[6]

Copy-move forgery detection using pixel-based approach

This algorithm is based on pixel-based approach. Mathematical morphological operations are used.^[6]

The partition-based copy-move forgery detection approaches

Most of the partition-based copy-move forgery detection approaches are classified as block-based approaches and nonblock-based approaches.^[6]

- Block-based approaches
- Nonblock-based approaches.

Since these complex algorithms use mathematical formulae-based computer programs, they have to be analyzed by a computer expert.

Inconsistent image quality

Every time the same image is opened and saved in the JPEG format, some apparent visual quality is lost and some artifacts appear. Different JPEG compression algorithms may produce vastly different files even when set to their highest quality setting. The simplest way to estimate the apparent visual quality of an existing JPEG file would be applying certain formulas to channel quantization tables specified in the file's tags.^[6]

Methods to Prevent Image Forgery to an Appreciable Extent

Metadata (data about data)

Metadata involves attaching information in the form of data to a digital image.^[2] It is a miniature text file appended to files which adds only a few bytes to the total file size so as to discourage manipulation at an amateurish scale.^[9,10] Most of the images are stored in EXIF format so that it can be viewed in any organizer that can identify EXIF format^[11] [Figure 4].

Digital watermarking

A digital watermark is superimposing a text or a logo on a digital photo.^[2] The purpose of a watermark is to recognize the work and discourage its unauthorized usage. Although a watermark cannot thwart

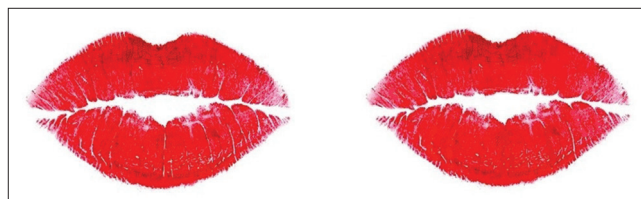


Figure 3: Original image. Copy-move attack image description: An image of a lip print sample is manipulated using copy-move attack to create the illusion of an entirely different lip print

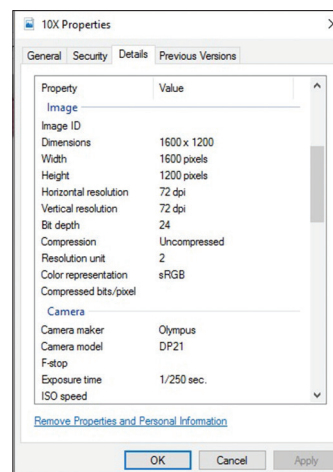


Figure 4: Original image. Metadata in exchangeable image file format

unauthorized use of digital image, it makes tampering more difficult and offers shield from manipulation. It can differentiate between malicious and nonmalicious changes to a greater or lesser extent.^[12] However, digital watermarking meets with a disadvantage that some expert software experts may edit the watermark and remove it [Figure 5].

Conclusion

Digital imaging has provided scientists with new prospects to obtain and manipulate data using techniques that were difficult or impossible to employ in the past. There is a possible use of retouched images for fraudulent purposes even in forensic investigations. As it is the vital need to make trust in all images and photographs, we further studied the techniques for detection of any kind of image forgery, which are based on different approaches. To ensure

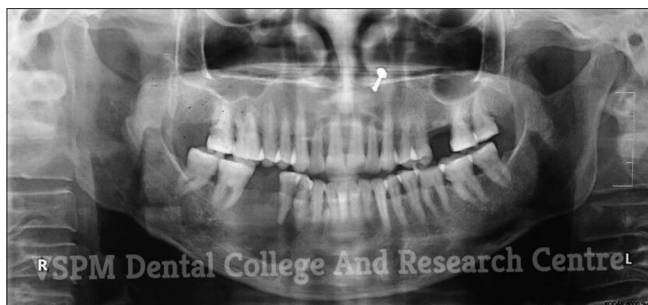


Figure 5: Original image. Digital watermarking

trustworthiness, multimedia authentication techniques have emerged to verify content integrity and prevent forgery of images. Computer alertness, especially about imaging software, should be promoted among forensic odontologist/dental professionals. Anticipatory measures should be done to avert their malicious reuse. Until there is an integrated response from the research community as to what constitutes appropriate image manipulation, the problem of “data beautification” will continue to plague science.^[2]

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

References

1. Leung C. Forensic odontology. *Hong Kong Med Diary* 2008;13:16-20.
2. Chowdhry A, Sircar K, Popli DB, Tandon A. Image manipulation: Fraudulence in digital dental records: Study and review. *J Forensic Dent Sci* 2014;6:31-5.
3. Redi JA, Taktak W, Dugelay JL. Digital image forensics: A booklet for beginners. *Multimedia Tools and Applications*. 2011;51:133-62.
4. Güneri P, Akdeniz BG. Fraudulent management of digital endodontic images. *Int Endod J* 2004;37:214-20.
5. Farid H. Exposing digital forgeries in scientific images. *Int J Sci Res Publ* 2006;12:122-9.
6. Mankar S, Gurjar P. Image forgery types and their detection : A review. *Int J Adv Res Comp Sci Softw Eng* 2015;5:174-8.
7. Gupta A, Saxena N, Vasistha S. Detecting copy move forgery using DCT. *Int J Sci Res Publ* 2013;3:2250-3153.
8. Detecting Forged (Altered) Images. *Forensic Focus*; 2017. Available from: [http://www.file:///C:/Users/dell/Desktop/Forensic%20odontology/Detecting%20Forged%20\(Altered\)%20Images%20_%20Forensic%20Focus%20-%20Articles.html](http://www.file:///C:/Users/dell/Desktop/Forensic%20odontology/Detecting%20Forged%20(Altered)%20Images%20_%20Forensic%20Focus%20-%20Articles.html). [Last cited on 2018 Jan 30].
9. Weissmann G. Science fraud: From patchwork mouse to patchwork data. *FASEB J* 2006;20:587-90.
10. Aldhous, P., & Reich, E. S. (2009). Further doubts over stem cell images. *New Scientist*, 203(2720).
11. Kutter M. Petitcolas FAP fair evaluation methods for image watermarking systems. *J Electron Imaging* 2000;9:445-55.
12. Benos DJ, Vollmer SH. Generalizing on best practices in image processing: A model for promoting research integrity: Commentary on: Avoiding twisted pixels: Ethical guidelines for the appropriate use and manipulation of scientific digital images. *Sci Eng Ethics* 2010;16:669-73.