

# Image manipulation: Fraudulence in digital dental records: Study and review

Aman Chowdhry,  
Keya Sircar,  
Deepika Bablani Popli,  
Ankita Tandon  
*Department of Oral Pathology  
and Microbiology, Faculty of  
Dentistry, Jamia Millia Islamia,  
New Delhi, India*

**Address for correspondence:**  
*Dr. Aman Chowdhry,  
Department of Oral Pathology  
and Microbiology, Faculty of  
Dentistry, Jamia Millia Islamia,  
New Delhi - 110 025, India.  
E-mail: aman1rocks@gmail.com*

## Abstract

**Introduction:** In present-day times, freely available software allows dentists to tweak their digital records as never before. But, there is a fine line between acceptable enhancements and scientific delinquency. **Aims and Objective:** To manipulate digital images (used in forensic dentistry) of casts, lip prints, and bite marks in order to highlight tampering techniques and methods of detecting and preventing manipulation of digital images. **Materials and Methods:** Digital image records of forensic data (casts, lip prints, and bite marks photographed using Samsung Techwin L77 digital camera) were manipulated using freely available software. **Results:** Fake digital images can be created either by merging two or more digital images, or by altering an existing image. **Discussion and Conclusion:** Retouched digital images can be used for fraudulent purposes in forensic investigations. However, tools are available to detect such digital frauds, which are extremely difficult to assess visually. Thus, all digital content should mandatorily have attached metadata and preferably watermarking in order to avert their malicious re-use. Also, computer alertness, especially about imaging software's, should be promoted among forensic odontologists/dental professionals.

**Key words:** Digital images, detection, manipulation, validation


## Introduction

Forensic odontology/forensic dentistry is defined 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.”<sup>[1]</sup> Traditionally, forensic odontology covered human identification and injury analysis. However, tasks of forensic odontologists have broadened in recent years to cover issues related to child abuse and domestic violence, human rights protection, insurance claims, and professional ethics. For all the

above tasks, records have to be maintained through casts, radiographs etc. The storage of physical dental records like dental casts and radiographs is fraught with difficulties of space and is also very expensive. This has led to increasing dependence on digital photography and digital radiology for preservation and documentation of ante-mortem and post-mortem dental records.

The very nature of digital imaging makes it very easy for the operator to adjust or modify digital image files. Many such manipulations, however, constitute inappropriate changes to original data, and making such changes can be classified as scientific misconduct.<sup>[2]</sup> Skilled technical personnel can spot such manipulations using features in the imaging software.<sup>[3]</sup>

Good science requires reliable data. Consequently, to protect the integrity of research, the scientific community takes strong action against perceived scientific misconduct. In the current definition provided by the U.S. government, “Research misconduct is defined as fabrication, falsification, or plagiarism in proposing,

Access this article online	
<b>Website:</b> www.jfds.org	<b>Quick Response Code</b> 
<b>DOI:</b> 10.4103/0975-1475.127767	

performing, or reviewing research, or in reporting research results.”<sup>[3]</sup>

At the outset, it is imperative to define what constitutes digital image fraud. Any alteration of the original image in part or full with malicious intent of altering its implication constitutes digital fraud. It includes:<sup>[4]</sup>

- (a) Additions,
- (b) Removal or Masking,
- (c) Modifications of specific characteristics of image (color/contrast etc.),
- (d) Splicing, blending of multiple images into a single composite, and
- (e) Combination of any or all of the above. Being accused of misconduct initiates a painful process that can disrupt one’s research and career. To avoid such a situation, it is important to understand where the ethical lines are drawn between acceptable and unacceptable image adjustment.<sup>[3]</sup>

## Aims and objectives

In this article, we highlight some universal guidelines for the apposite handling of digital image data and provide some examples to exemplify pitfalls and inapt practices. This article also discusses anti-tampering techniques and methods of detecting and preventing manipulation of digital images.

## Materials and Methods

Digital image records of forensic data (casts, lip prints, bite marks) were manipulated using freely available softwares. Softwares used were Adobe® Photoshop® (Adobe Systems Inc, San Jose, CA, USA), Corel Draw® (Corel Corporation, Ottawa, Ontario, Canada), Picasa 3.9.1.535 version. To record digital images of casts, lip prints, bite marks, Samsung Techwin L77 digital camera (Samsung, Korea) was used. The tools employed on images for manipulation are listed together with their function in Table 1.<sup>[5]</sup>

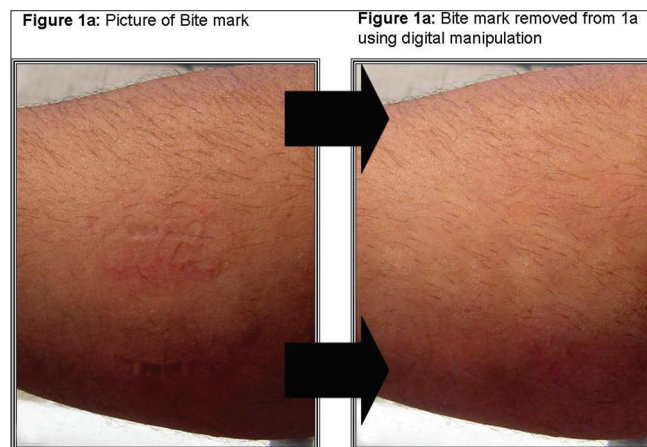
## Results and Observations

It was quite evident that ostentatious digital images can be created either by merging two or more digital images or by altering an existing image.

- Figure 1 shows use of merge tool on a bite mark photograph
- Figure 2 shows Tsuchihashis classification<sup>[6]</sup>
- Figure 3 shows original image of a lip print manipulated to another variety
- Figure 4 shows digital photographic records of palatal rugae on casts<sup>[7]</sup>
- Figure 5 shows multiplication of data in figure 4 using clone stamp tool.

**Table 1: Tools used for digital photo editing**

Name of tool	Uses
Pen tool/brush tool/pencil tool	To draw outlines, sketch etc.,
Eye dropper tool	Samples the color in image and makes it the foreground color
Paint bucket tool	Fills likewise colored pixels with color
Patch tool	This tool retouches image using sampled pixels or pattern and is used to repair flaws on a selected portion of an image
Lasso tool	To select and copy object out of image, which is need to be deleted or moved to different part of the image or even to a new document
Magic wand tool	Selection of similar colored pixels within a specified range
Clone stamp tool	Allows you to duplicate part of an image and can be use to multiply data.
Eraser tool	Wipes out pixels
Blur tool	Distorts pixels by diminishing the distinction between pixels
Smudge tool	Homogenize area in an image
Crop tool	To make the image size smaller to remove the area of interest
Toning tool (3 states)	
Dodge	Lighten an image
Burn	Opposite of the dodge tool, that is, This tool allows you to darken portions of the canvas
Sponge	This tool reduces the amount of saturation and contrast



**Figure 1:** Usage of merge tool on a bite mark photograph

## Discussion

The old adage of ‘publish or perish’ is very pertinent in the present scenario and it is not unexpected for sloppiness, plagiarism, and even fraud to find their way too easily in today’s intense research atmosphere. By far and away, the most significant problem is that scientists do not understand complex data-acquisition tools and occasionally seem to be duped by the ease of use of image-processing programs to manipulate data in a manner that amounts to misrepresentation.<sup>[8]</sup>

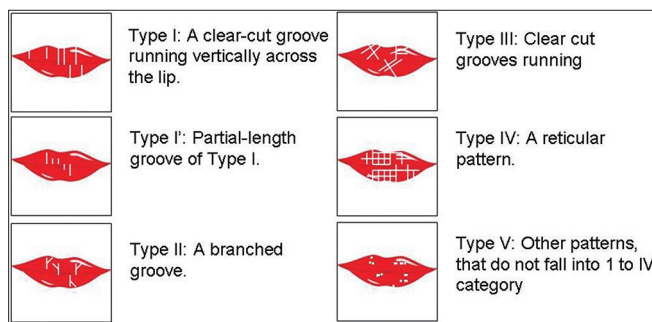


Figure 2: Tsuchihashi's classification



Figure 4: Digital photographic records of palatal rugae on casts

Procedural hindrances to objectionable image manipulation have been greatly reduced resulting in an ease of bringing about any change to an image with just the click of a mouse. Over the last 10-15 years, there have been a few highly public instances of falsified images (Abbott 1997;<sup>[9]</sup> Aldhous and Reich 2009;<sup>[10]</sup> Weissmann 2006;<sup>[11]</sup> Xin 2006;<sup>[12]</sup> Young 2008<sup>[13]</sup>), but most of the problem lies with the lack of a basic understanding of how to properly handle image data.<sup>[14]</sup> Digital image modification is done at a pixel level and makes it to a large extent undetectable when viewed with a naked eye. Several measures, such as few described below, help in detection of altered digital images:

### Cautious skepticism

Look for evident anomalies in the photo. This can comprise items not in the correct perspective, conflicting angles of reflection or unexpected discontinuities. Check for inconsistent gloom or features that seem slightly bigger or smaller than standard. Any inconsistencies may divulge the photo to be forged.<sup>[15]</sup>

### Scrutinize

With the assumption that tampering disturbs certain underlying statistical properties of an image, these forensic techniques can detect specific forms of tampering. Air-brushing or re-touching can be detected by measuring

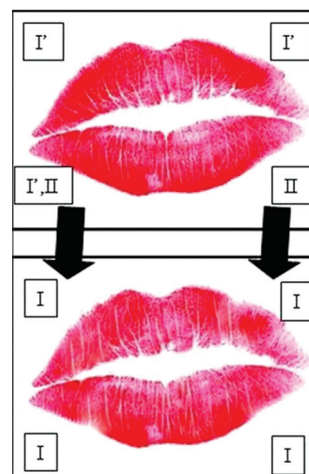


Figure 3: Original image of a lip print manipulated to another variety



Figure 5: Modification of Figure 4 showing how the same data was multiplied

deviations of the underlying color filter array correlations. A digital composite of two people can be detected by measuring differences in the direction to the illuminating light sources from their faces and body. Any inconsistencies in lighting can then be used as an evidence of tampering. Duplication or cloning can be detected by first partitioning an image into small blocks. The presence of identical and spatially coherent regions in an image can be used as an evidence of tampering.<sup>[16]</sup>

### Image analyzing software, tools, and Laboratory Investigation

If there is doubt about integrity of images and previous steps didn't detect the same, then the images can be submitted to a proficient image processing lab. Detection of altered images has also been made easier by forensic tools that scrutinize scientific images (available through the US Department of Health and Human Services Office of Research Integrity).<sup>[17,18]</sup> These tools have been used by some journals, and their routine use is currently being considered by many editors and publishers.<sup>[19]</sup>

The accuracy and reliability of digital dental records is very important when such records are considered as forensic evidence.



The knack of image fakery has a long history, and in today's digital age, it is possible to very easily change the information represented by an image without leaving any apparent traces of tampering. No method yet exists, which accomplishes efficiently and precisely the image forge recognition mission.

Considering that "prevention is better than cure," we propose that the person making a digital record should validate his data by taking certain steps to prevent the manipulation of the data by any third party for any spurious purpose. A few points for prevention of fraudulent use of digital images can be stated as:

### Meta data (data about data)

It is attaching of information in the form of data to digital image. (Figure 6 shows how an image metadata looks



Figure 6: Example for image metadata



Figure 7: Example for watermarking an image

like.) It's like a miniature text file appended to files only adding a few bytes to the total file size so as to discourage manipulation at an amateurish scale.<sup>[10,11]</sup> Most of the images are stored in Exchangeable Image File (EXIF) format, so that you can view it in any organizer that can speak EXIF format.<sup>[19]</sup>

### Digital watermarking

A digital watermark is a super impose on a digital photo (consisting of text/logo/copyright notice).

The purpose of a watermark is to recognize the work and discourage its unauthorized usage. Though a watermark can't thwart unauthorized use of digital image, it makes tampering more difficult and offer shield from manipulation. It can differentiate between malicious and non-malicious changes to a greater or lesser extent.<sup>[20]</sup> Figure 7 shows a superimposed water mark on previously used image [Figure 4] of casts.<sup>[7]</sup>

## Summary and 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. Computer alertness, especially about imaging software's, should be promoted among forensic odontologist/dental professionals. Anticipatory measures such as attached metadata and preferably water marking of digital images should be done in order 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.

## References

1. Keiser-Neilsen S. Person Identification by Means of Teeth. Bristol: John Wright and Sons; 1980.
2. Güneri P, Akdeniz BG. Fraudulent management of digital endodontic images. *Int Endod J* 2004;37:214-20.
3. Rossner M, Yamada KM. What's in a picture? The temptation of image manipulation. *J Cell Biol* 2004;166:11-5.
4. Fierte R. "Photo Fakery" oemagazine [Internet]. 2005 January. Available from: <http://spie.org/x16032.xml?highlight=x2410&ArticleID=x16032>. [Last cited on 2012 Dec 12].
5. Singbal KP, Chhabra N, Madan B. Digital Imagery: Reality or Fakery. *Int J Contemp Dent* 2010;1:93-8.
6. Tsuchihashi Y. Studies on personal identification by means of lip prints. *Forensic Sci* 1974;3:233-48.
7. Establishing the reliability of palatal rugae pattern in individual identification (following orthodontic treatment). *J Forensic Odontostomatol*. 2011;29:20-9.
8. Beautification and fraud. *Nat Cell Biol* 2006;8:101-2.
9. Abbott A. Forged images lead to German inquiry. *Nature* 1997;387:442.

10. Aldhous P, Reich ES. Further doubts over stem-cell images. *New Sci* 2008; 203:2.
11. Weissmann G. Science fraud: From patchwork mouse to patchwork data. *FASEB J* 2006;20:587-90.
12. Xin H. Scientific misconduct. Online sleuths challenge cell paper. *Science* 2006;314:1669.
13. Young JR. Journals find fakery in many images submitted to support research. *The Chronicle of Higher Education* (May 29, 2008). Available from: <http://chronicle.com/article/Journals-Find-Fakery-in-Man/846/>. [Last accessed on 2009 Apr 12].
14. Crome DW. Avoiding twisted pixels: ethical guidelines for the appropriate use and manipulation of scientific digital images. *Sci Eng Ethics* 2010;16:639-67.
15. O'Brien JF, Farid H. Exposing Photo Manipulation with Inconsistent Reflections. *ACM Trans Graph* 2012;31:1-11.
16. Farid H. Digital image forensics. *Sci Am* 2008;298:66-71.
17. Parrish D, Noonan B. Image manipulation as research misconduct. *Sci Eng Ethics* 2009;15:161-7.
18. Pearson H. Forensic software traces tweaks to images. *Nature* 2006;439:520-1.
19. 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.
20. Kutter M, Petitcolas FAP. Fair evaluation methods for image watermarking systems. *J Electron Imaging* 2000;9:445-55.

**How to cite this article:** 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.

**Source of Support:** Nil, **Conflict of Interest:** None declared