

Fraudulent Use of Digital Radiography: Methods To Detect and Protect Digital Radiographs

Filip L.G. Calberson, DDS, MMS, Geert M. Hommez, DDS, MMS, PhD, and Roeland J. De Moor, DDS, MMS, PhD

Abstract

Digital radiography has become an indispensable diagnostic tool in dentistry today. To improve vision and diagnosis, dental x-ray software allows image enhancement (eg, adjusting color, density, sharpness, brightness, or contrast). Exporting digital radiographs to a file format compatible with commercial graphic software increases chances that information can be altered, added, or removed in an unethical manner. Dental radiographs are easily duplicated, stored, or distributed in digital format. It is difficult to guarantee the authenticity of digital images, which is especially important in insurance or juridic cases. Image-enhancement features applied to digital radiographs allow mishandling or potential abuse. This has been illustrated by several recently published studies. A standard authentication procedure for digital radiographs is needed. A number of manipulated radiographic images are presented to show concerns about security, reliability, and the potential for fraud. Antitampering techniques and methods of detecting manipulations in digital medical images are discussed. (*J Endod* 2008;34:530–536)

Key Words

Digital radiography, endodontics, image enhancement, image manipulation, radiographic authentication, radiographic images

From the Department of Operative Dentistry and Endodontology, Dental School, Ghent University Hospital, Ghent, Belgium.

Address requests for reprints to Dr Roeland De Moor, Department of Operative Dentistry and Endodontology, Dental School, Ghent University, Ghent University Hospital, De Pintelaan 185 (P8), B-9000 Ghent, Belgium. E-mail address: roeland.demoor@UGent.be.

0099-2399/\$0 - see front matter

Copyright © 2008 by the American Association of Endodontists.

doi:10.1016/j.joen.2008.01.019

The primary objective of endodontic treatment is the prevention or elimination of infection in the endodontium. This is achieved by means of a thorough chemomechanical cleaning and shaping before a dense, as hermetical as possible, obturation of the root canal system (1). Because the subjective complaints of the patient often indicate only the broad region within which the problem is situated, a profound clinical and radiographic examination is required to locate the causal tooth (or teeth). In most cases, a radiographic image will be decisive in revealing the endodontic pathosis.

Diagnoses of cases requiring an endodontic treatment are confirmed by means of a radiograph. In certain cases, several initial radiographs of the same tooth are required, not only for diagnosis but also to determine the treatment strategy and to assess the clinical approach and complexity of the treatment to be performed. In challenging endodontic or surgical situations demanding localization and characterization of roots, root canals, or anatomic structures, 3-dimensional digital imaging modalities like cone-beam volumetric tomography (CBVT) can be useful (2, 3). A CBVT image is mainly adopted for diagnosis, thus before treatment. Nevertheless, during and after the endodontic treatment, periapical radiographs are still required.

The success and outcome of the endodontic treatment can be assessed by additional radiographic exposures during the treatment (eg, length determination, location of canal, and gutta-percha cone fit). As a consequence, the number of radiographs can increase dramatically, especially in complex treatment cases, resulting in a higher patient exposure to radiation.

Digital radiography can, in this respect, offer an advantage. There is lower exposure to radiation (4, 5), and the time saved (6) by eliminating the development time can shorten the duration of an endodontic treatment considerably. Furthermore, errors in development are seemingly nonexistent because over- or underexposure can be corrected by adaptation of several parameters.

An additional advantage of direct digital radiography (which involves no intraoral storage phosphor plates but a captor linked by means of a cable directly to a computer), is the ease of taking several radiographs of the same teeth from various angles. When using indirect digital radiography or conventional radiography, a second or subsequent radiographic exposure requires the radiograph to be repositioned, whereas this is not necessary when using a direct digital technique. Here, the horizontal position of the cone can be moved to a different angle, and the captor preserves its original position. Therefore, a more precise analysis and comparison of two or more radiographs is obtained.

Aside from the advantages mentioned previously, the lack of standardized procedures that protect radiographic data against manipulation and that guarantee authentication is a major disadvantage of using digital images in dentistry. Particularly in juridic or insurance cases in which huge claims of damage or compensation are involved, there could be a temptation to manipulate digital radiographs by unethical means. Many useful solutions are found concerning image protection in digital photography, but only few reports in dental literature discuss how to deal with this problem in digital radiography. The development of radiographic authentication techniques is very complex and mathematically based and is therefore preferably left in the experienced hands of computer engineers. Nevertheless, dentists must be aware of the problem and its impact on the dental profession. The aim of this article was to address the potential of fraud on radiographic images and to discuss some recent general image authentication techniques that could be applicable to dentistry in the near future.

Review

Digital Images

A digital image is composed of small picture points, called pixels, each with a color value. Because pixel color values correspond with numeric values, computerized algorithms can be applied, by which pixel values in the (radiographic) picture may change according to certain mathematical regularities. These changes allow adaptation or alteration of the image brightness, contrast, sharpness, or color saturation (7). Likewise, certain regions on the radiograph with comparable pixel values, or values within a certain color range (eg, anatomic structures with the same radiodensity), can be emphasized or colored. This can clarify details in the radiograph and contribute to a better diagnosis. However, although some structures are enhanced, others may become less clear or blurred, and several reproductions of the same radiograph may be required. This may complicate interpretation of the whole image.

Software packages enable the dentist to manipulate digital radiographs without the patient being exposed to additional radiation (8). Once reference points are marked and calibration of the dimensions of the picture is performed, an accurate canal length can be determined on screen. The digital radiographs can easily be stored, linked to a patient's file, viewed, and sorted (9).

Manipulation of Digital Images

There are 2 types of image manipulation: malicious and nonmalicious image processing. In nonmalicious manipulation, pixel values in the digital radiograph may be altered (eg, to adjust the brightness or contrast of an image). This kind of processing does not alter the content of the image but makes it more easily accessible for the human eye (10); this process can be considered as image enhancement. Some articles clearly explain how imaging algorithms modify a dental radiograph (11, 12). Thus, dentists can understand the mechanisms of image enhancement and assess its impact on diagnostic quality and, hence, diagnosis and treatment. In malicious image manipulation, the content of the image is modified by deleting or adding data. Dental software packages allow for image enhancement but do not modify the content of the radiograph. Malicious alteration can, however, be performed in commercial photographic software.

As digital photography has gained popularity and interest in the use of conventional film has been lost, digital radiology has become a real alternative to conventional radiology in dentistry. Some studies even report that (direct) digital radiography provides equivalent (13, 14) or improved (15) diagnostic results compared with conventional film. Software to process digital images continues to become more and more sophisticated and user-friendly. Today, almost all images used for advertisement are digitally manipulated or corrected. The future of digital radiology may follow a similar path because digital radiographs are digital images. A few years ago, creating a convincingly altered digital image required the efforts of a specialist using sophisticated equipment, but nowadays it can be easily accomplished by anyone with a personal computer. As the procedure for exposing and modifying digital radiographs becomes easier, opportunities for abuse increase (16). When an original digital radiograph is exported from the dental software program in a certain format (eg, TIFF, JPEG, or BMP), it can be opened and modified in any other photographic software program (17). The same applies to a conventional radiograph that is scanned (eg, to duplicate and store a radiograph in digital format to avoid future discoloration or fading).

The potential to modify, remove, or add data in digital radiography using graphic software was pointed out in 1996 (18). In this publication, the authors suggested that a unique encrypted identification code

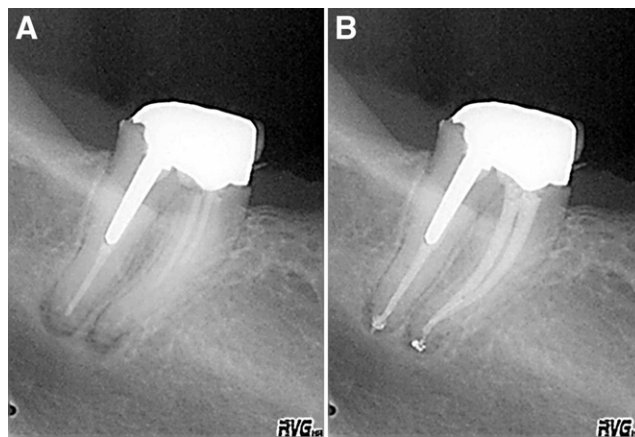


Figure 1. (A) Original radiograph: incomplete root canal filling, especially in the mesial root and (B) tampered-with image: now a more acceptable root canal filling is present.

could be embedded within each digital radiographic image. This code contains the name of the patient and date of exposure and is not attached to an imported or exported image. A study by Tsang et al. (19) proved that insurance companies could be deceived by means of fraudulent radiographs. The authors used a flatbed scanner to digitize conventional radiographs and simulated pathology on healthy teeth by adding carious lesions, large restorations, fractures, and periapical inflammation. These falsified images were printed and presented to the insurance companies as evidence for an expensive restorative treatment (root canal treatment + crown). Every submitted case got approval for treatment, resulting in compensation granted for a treatment that was not adequate or never would be performed. This study showed the possibilities for fraudulent use of modified radiographic images, alerting the scientific community to the importance of awareness and the need for measures to prevent such malicious practices.

A more recent publication explains how digitized pre- and post-operative radiographs of endodontic cases can be manipulated thoroughly with modern software (20). Figures 1 to 4 show manipulation of digital radiographs, highlighting the difficulty in distinguishing the original radiograph from the fraudulent one.

Recognition of Manipulated Digital Radiographs and the Need for Image Protection

A limited number of studies have examined the ability of dentists to distinguish modified radiographs from original ones and whether they could indicate where the modifications were made (21, 22). In the majority of cases, the original radiograph could not be distinguished from the altered image, few modified details were retrieved, or unaltered details were wrongly considered to be false. It appears that if a digital radiograph is altered with great care, it is extremely difficult to decipher where alterations have been made, even for persons with experience in the field of image enhancement. The authors of such studies highlight the need for methods other than visual inspection alone to protect digital data.

The incidence of fraud in medical claims for damage and compensation is high; in the United States alone, it accounts for 10% of cases of abuse or fraud (19), and it continues to increase (18). Insurance companies and experts could demand that digital radiographs are always evaluated in the original software and under predefined conditions (and not by means of exported images or outprints), but the lack of international standards in this respect is a major disadvantage (19).

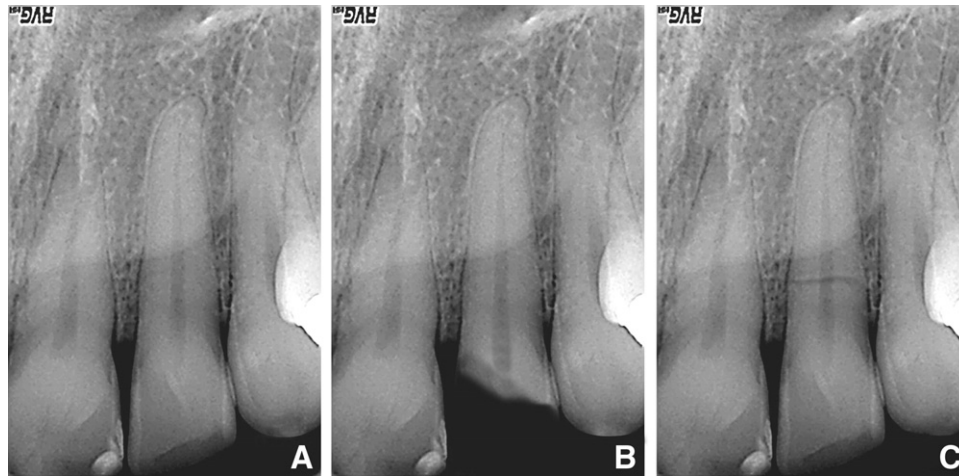


Figure 2. (A) Original radiograph: trauma with minor enamel fracture of the incisal edge; (B) tampered-with image: trauma with severe fracture of the crown (rehabilitation might require root canal treatment and a post-retained crown); and (C) tampered-with image: simulation of a horizontal root fracture in the coronal third of the root (with radiographic angulation parallel to the fracture line).

Methods To Secure Medical Digital Images

Most systems for digital radiography have a (built-in) software verification mechanism to guarantee the authenticity of original radiographs. Some software manufacturers do not allow the original radiograph to be opened or modified directly from within other “common” imaging software programs by encrypting the images or generating an uncommon image format. This renders the image incompatible with other software, allowing it to be processed only in the program in which it is generated. With certain systems, the original radiographic image may look blurry and can only be better examined after image enhancement in the associated software with which the radiograph has been made. To distribute the original picture or to examine it on another computer, the same software is necessary, or the image can be stored with an attached viewer tool (eg, Trophy Radiology, Marne-la-Vallée, France, now Eastman Kodak, Rochester, NY). Other dental software programs allow direct opening and modification of the original radiograph in photographic software but add an error mark on the image to indicate that the original picture has been modified (eg, Schick Technologies Inc, Long Island City, NY) (19), or the modified image is no longer

recognized by or cannot be reopened in the radiographic software in which it was generated or by the patient file to which it was linked (eg, Sidexis; Sirona, Bensheim, Germany). These incompatibilities between different dental software programs are rather to protect the manufacturer’s software than to protect the digital radiographic data.

The best approach to distributing original images is to export the image using dental software in its original software format. The image may then be opened and viewed on other computers but only using a software program from the same manufacturer. This ensures transparency so that the end user can be assured that only nonmalicious modifications have been made for the purpose of image enhancement.

However, if the appropriate software is not available to the end user, the radiograph must be exported in another compatible file format, which may be compatible with popular imaging software. In this case, there are several ways to protect the exported picture before it is distributed.

Digital radiographs can be exported to many formats. Some formats, like the Exif-JPEG and the digital imaging and communication in medicine (DICOM) format, export not only the image data but also incorporate metadata. Metadata describe other data, in this case the



Figure 3. (A) Original radiograph: a broken lentulo was left in the root canal and (B) tampered-with image: a normal pulp chamber and root canal; apparently, no endodontic treatment has yet been performed.

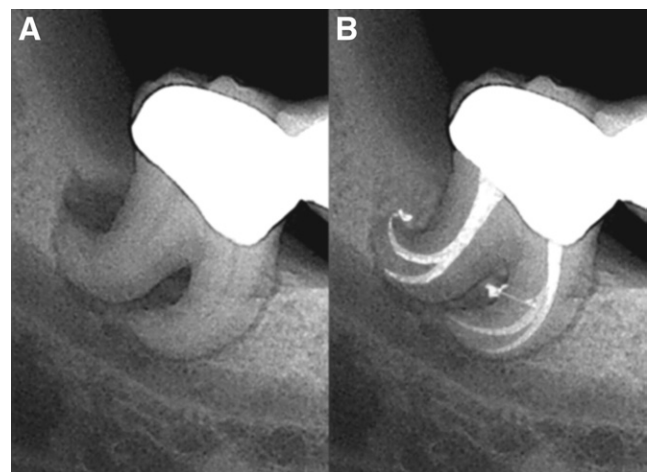


Figure 4. (A) Original radiograph: mandibular molar with severely curved roots and periapical and furcal lesion and (B) tampered-with radiograph: a root canal filling with lateral canal and healing of the bone lesions.

digital image data. Exif is an acronym for “exchangeable image file” and is used for digital camera photos. It records what is commonly called the “shooting data” (ie, the camera settings in use; in this case, the digital radiography captor) when the image was taken, and it specifies the way the image should be formatted so that it can be used by Exif-compliant devices such as printers. Most dental software programs support the Exif-JPEG format and the input of other metadata concerning patient identification, creation date, or file information. This might guarantee authentication, but commercial software is available to read and change the metadata (Exif-Reader © 1998-2002 Ryuji Yoshimoto, www.takenet.or.jp/~ryuuj/miniisoft/exifread/english/ and Exifer © 2001-2002 Friedemann Schmidt, www.friedemann.info). The DICOM image format is widely spread in medical imaging and is the standard for exchanging medical images between several users (23). Little information is available about the protection of the content of DICOM images. The majority of dental radiographic software supports this image format, and DICOM most likely will become the standard format for exchanging images in dentistry (24, 25). Ironically, newer versions of Photoshop (Adobe Systems Inc, San Jose, CA), the most commonly used image-editing software program, now fully support the manipulation of metadata image formats and the DICOM format.

DICOM defines protocols and mechanisms to manage and transfer medical data. A DICOM image combines patient data and image data. During the transportation process (eg, Internet and e-mail), a security issue arises because patient data cannot be distributed to unauthorized users.

Therefore, several techniques can provide encryption and decryption using hash codes, public keys, and private keys. These imagery-authentication techniques are based on cryptographic principles and digital signatures and protect the data against modification and retrieval of information during transmission. They do not, however, always offer protection when transmission is completed. Because the authentication codes or digital signature information are separate from the digital image, one could modify the image, recalculate the digital signature, and attach them together. Without knowledge of the original image data or original authentication information, it is difficult to contest the authenticity of the modified image.

A more secure way to protect image data is not to attach the authentication codes to the image but rather to embed verification data within the image. Sometimes referred to as “a watermark,” embedded data modify the image bits without changing the meaning of its content. Once the codes are embedded in the image content and the image is manipulated, these codes will also be modified so the authenticator can examine them and verify the integrity of the data.

The concept of hiding data in other data is called steganography. Different steganographic techniques can be divided into two main groups according to the embedding domain of the image: the spatial domain approach and the frequency domain approach. To understand the principles of steganography, some basic characteristics of pixels must be understood. A digital image consists of pixels, and each pixel has its own color value. The number of distinct colors that can be represented by a pixel depends on the number of bits per pixel (bpp). A single bit can have two values: one or zero (on or off). If one pixel is determined by one bit, that pixel can have only 2 different color values (eg, black and white), which is not enough to compose an image. The more bits per pixel, the more different color levels can be expressed. Because a digital dental radiograph consists of different levels of gray, 8 bpp are enough to compose a clear picture. For example, the pixel determined by the number 10010110 is 8 bits long and corresponds with a certain gray color. If the least significant bit (LSB) (on the right of the 8-digit number) is changed to 1 (10010111), the pixels' intensity changes slightly to the next level of gray. In an 8-bpp grayscale image, each pixel can have 2^8 , or 256, different levels of gray ranging from black to white. The human eye

can only distinguish 32 different levels of gray (26), so, when changing the LSBs, there will be a maximum of a $1/256$ change (0.39%) in pixel intensity. Thus, although the LSBs of the image are altered, the resulting image is perceptually equivalent to the original.

One approach to steganography, the spatial domain approach, is to embed checksums into the LSBs of the image (27). A secret numeric key, known by both the sender and the recipient, protects the 32-bit checksum, which is obtained by summing the seven most significant bits of every pixel in the image. Every single bit of the 32-bit checksum is inserted in binary form in the 32 LSBs determined by the key. Thus, a maximum of 32 pixels in the image (invisibly) change in color intensity. The image can then be saved and distributed. To check for authenticity, using the secret key, the recipient extracts the checksum and constructs a second checksum out of the seven most significant bits of each pixel. If the two checksums are different, the image has been tampered with. This simple technique has some disadvantages: it can detect tampering, but it cannot locate the manipulated pixels and exchanging the pixels in terms of location in the image will not always affect the resulting checksum and would not be detected. To overcome this, the image can be broken up into multiple small subblocks, each embedded with a checksum (28). The smaller the subblock size, the more precise the algorithm can pinpoint manipulated areas in an image. Because at least 32 pixels are needed to embed a 32-bit checksum, subblocks of at least $6 \times 6 = 36$ pixels are needed. To prevent exchanging subblocks, multiple checksums can be calculated by multiplying the pixel values by a function of their positions and then summing them. This way, exchanging subblocks will not go unnoticed, and every change in pixel value can be located within the range of the modified subblock (Fig. 5). Another solution is to divide the image into overlapping subblocks, which introduces an interblock relationship (29).

New anti-tampering techniques have been described that not only indicate which pixels or blocks have been tampered with but also retrieve the original content of the image (30). A highly compressed version of the original image is, to a certain level, embedded as a watermark in images with “self-correcting” capabilities. Therefore, two (instead of one) LSBs are used to incorporate information. These techniques have not yet been validated for practical applications, but practical self-embedding methods may be available in the near future.

Spatial domain authentication algorithms based on modifying LSBs can be effective but cannot distinguish between malicious and nonmalicious manipulation of a digital radiograph. The adjustment of brightness and contrast is a very common nonmalicious procedure in digital radiograph enhancement but will not be tolerated by the previously described verification techniques. An acceptable authentication method should protect all pixels in an image and distinguish between malicious and nonmalicious changes.

One way to make verification procedures less sensitive to (nonmalicious) minor changes is to embed the checksum into a more significant bit plane (ie, the third or fourth bit). Alternatively, embedding watermarks in the frequency domain rather than in the LSBs of pixels may be successful, while protecting the primary textures in the image, such as the edges. Edge information is the most important factor for our perception of the image. The embedded watermark should not satisfy the authentication process if such textures are tampered with or damaged, as in malicious manipulations. In most techniques, an image is decomposed into two different structural components: a texture component and a blurred version of the original image (Fig. 6). Because the texture image displays edges, which largely reflect the texture information of structures in the original image, the watermark can be embedded into this component and serve as an indicator of the authenticity of the watermarked image (31). This provides significant advantages for the authentication of biomedical images, which is strongly texture based (29). Because most common nonmalicious manipulations



Figure 5. (A) Original radiograph: no pathosis apparent; (B) tampered-with radiograph: periapical lesion caused by coronal leakage (rehabilitation would require endodontic treatment and new bridge); and (C) authenticity procedure by means of verification of embedded checksums in a watermarked image: small highlighted subblocks indicate where tampering was performed.

tend to preserve primary texture features of images, these embedding methods ensure that the watermark does not suffer significantly from such image-enhancement manipulations. The embedded watermark also uses (overlapped) subblocks, and some techniques provide recovery of the original image information.

Current and Future Image-Verification Applications

The image-verification techniques described earlier are new and continuously evolving. No standard yet exists because different image applications demand different protection algorithms, but authentication techniques in biomedical imaging are being investigated (32). Invisible digital watermarks can be classified as robust or fragile, depending on the requirements of the application. Robust watermarks are those designed to withstand accidental (and malicious) attacks, such as content alteration, compression, filtering, and cropping. Fragile watermarks will become drastically altered upon any alteration of the digital content. A semifragile watermark combines characteristics of both these types and would therefore be most suitable for dental radiography.

Little information is available concerning the protection of digital radiographs, but antitampering techniques are already used in a wide variety of applications. Digital watermarking is currently used in digital still cameras, video cameras, identity cards, scanners, printers, and

copiers. Applications include tamper detection, copyright protection, embedding descriptive information (metadata), and file access control by embedding access codes in image files.

Some of the newer photographic cameras (eg, Canon DVK-E2; Canon, Tokyo, Japan) produce images with an embedded image verification feature, which allows detection of the smallest (1 bit) discrepancy between two “identical” images. This feature is useful, for example, in insurance cases to guarantee the authenticity of clinical photographs of a dental trauma. In “digital ballistics,” algorithms are developed, by which an image can be traced to one specific camera, just as bullets may be traced to the pistol from which they are fired (33, 34).

Another possible verification procedure would be to incorporate a digital signature or watermark in the original, exported, or scanned image (Digimarc Corporation, Beaverton, OR). This watermark is a digital code that is added to the image under the form of noise, invisible to the naked eye, and can contain additional copyright information in the form of text. The watermark is preserved during conversion of file formats, printing, and rescanning of the image.

Some printers and scanners embed an invisible watermark on printed or scanned documents, which can also be used for copyright

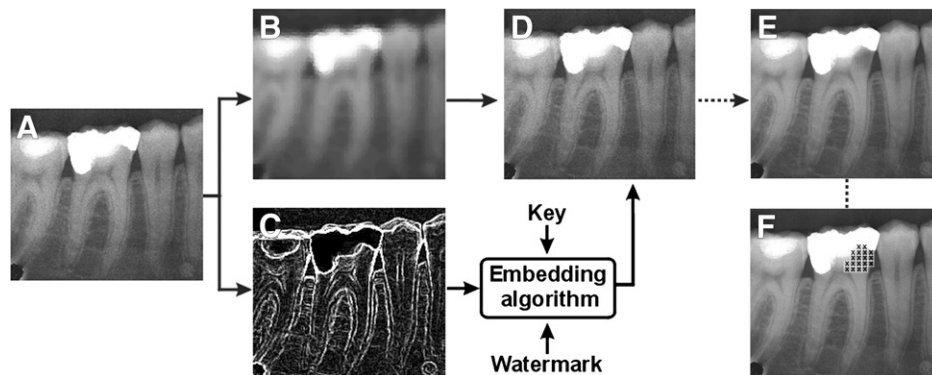


Figure 6. Watermark embedding process: the original image (A) is decomposed into a (B) blurry image field and (C) a texture field. A secret key determines the insertion of the watermark in the texture field by means of embedding algorithms. Composition into the (D) watermarked image, with no visible changes from the original image. (E) Tampered-with image: extensive carious lesion involving the pulp (root canal treatment and crown would be indicated). (F) Watermark detection and image authentication reveals the tampered-with parts of the image.

protection. In the near future, scanners or digital copying machines may detect these watermarks and use the information to refuse to replicate the documents, automatically alert the author, or charge extra costs.

Digital photograph verifier tools are available online that allow users to confirm the authenticity and ownership of digitally watermarked images on the Internet (35). Development of an authentication standard that is compatible with all digital radiographic manufacturers could be a simple and effective solution for dental radiography. If a radiograph is watermarked in the dental software upon exporting and distribution, the end user could verify its authenticity by uploading the image to a specific "verification" Web site.

Because of the high cost of computed tomography scan or CBVT machinery in general dental practice, patients are usually referred to an imaging center in which the 3-dimensional scan is performed and read by a dental radiologist. Digital computed tomography scan or CBVT computer models are distributed in digital format to the referring dentist. The 3-dimensional images are shown in an attached viewer tool. This software program ensures some authentication of the images. Nevertheless, 2-dimensional image "slices" or an image sequence compilation can be exported to compatible image (JPEG, TIFF, and BMP) and movie file formats (MPEG and AVI). These movies or digital clinical movies (from intraoral or dental microscope cameras) can also be manipulated with commercial video editing software. A security issue may arise, but several video-authentication techniques (eg, in the field of video surveillance cameras) are already existing or under construction (36, 37). Thus, an authentication for medical video files can be expected in the future.

A recent newspaper article (38) reported fraudulent use of microscopic images in published articles in leading medical journals like *Science* (concerning human embryonic cloning) (39, 40), the *New England Journal of Medicine* (concerning oral epithelium dysplasia) (41), and *The Lancet* (42). These previously unnoticed falsified results are unacceptable in medical science. The editors of these journals have expressed concern and call for improved authentication solutions for digital images. To limit the number of images in a scientific article, most (dental) journals instruct their authors to compose several images into one single image with sub-images or insets. This further complicates successful image-verification procedures. As yet, there is no ultimate solution, but as in medicine, dental journals and scientists should raise concerns on how to deal with this problem in the near future.

Conclusions

Several recent studies have speculated on the possibilities and impact of digital radiography fraud in the field of dentistry. The review presented here was not written to be provocative but rather to summarize the published literature, to increase awareness of the possibilities for fraud which are available, and to discuss possible authentication techniques. Alertness and awareness are recommended when digital radiographs are used in any context such as damage claims, medical evidence material, forensic dentistry, presentations, publications, or insurance cases.

Image-verification technologies will become standard features of digital cameras in the near future. The attention from industries that rely on highly reliable photographic or radiographic evidence (such as casualty insurance firms and medical institutions) will certainly cause these features to be incorporated, for instance, in radiographic machinery. The watermark should be applied in a controlled manner (already in the dental software, before manipu-

lations can be performed). This way, one could verify not only when and under what (shooting) conditions the image was taken but also with which radiographic device. The image-verification process will expose whether the image has been tampered with, what parts of the image or image pixels were manipulated, and (to some extent) what the original image looked like.

If law courts or insurance companies begin to demand standards for the authentication of digital images, manufacturers will have to comply to continue to sell their products. The future will tell if there is a real need for stricter policy or measures that retrieve, exclude, or avoid the fraudulent use of digital radiographs in dentistry.

References

- Ingle JI, Bakland LK. Endodontics 2002 (ed 5). Hamilton, Canada: BC Decker.
- Nair MK, Nair UP. Digital and advanced imaging in endodontics: a review. *J Endod* 2007;33:1-6.
- Cotton PT, Geisler TM, Holden DT, Schwartz SA, Schindler WG. Endodontic applications of cone-beam volumetric tomography. *J Endod* 2007;33:1121-32.
- Hayakawa Y, Shibuya H, Ota Y, Kuroyanagi K. Radiation dosage reduction in general dental practice using digital intraoral radiographic systems. *Bull Tokyo Dent Coll* 1997;38:21-5.
- Dula K, Sanderink G, van der Stelt PF, Mini R, Buser D. Effects of dose reduction on the detectability of standardized radiolucent lesions in digital panoramic radiography. *Oral Surg Oral Med Oral Pathol Oral Radiol Endod* 1998;86:227-33.
- Dunn SM, Kantor ML. Digital radiology. Facts and fictions. *J Am Dent Assoc* 1993;124:38-47.
- Wenzel A. Computer-aided image manipulation of intraoral radiographs to enhance diagnosis in dental practice: a review. *Int Dent J* 1993;43:99-108.
- Kerosuo E, Orstavik D. Application of computerized image analysis to monitoring endodontic therapy: reproducibility and comparison with visual assessment. *Dentomaxillofac Radiol* 1997;26:79-84.
- Analoui M, Buckwalter K. Digital radiographic image archival, retrieval, and management. *Dent Clin North Am* 2000;44:339-58.
- Mol A. Image processing tools for dental applications. *Dent Clin North Am* 2000;44:299-318.
- Analoui M. Radiographic image enhancement. Part I: spatial domain techniques. *Dentomaxillofac Radiol* 2001;30:1-9.
- Analoui M. Radiographic digital image enhancement. Part II: transform domain techniques. *Dentomaxillofac Radiol* 2001;30:65-77.
- Mistak EJ, Loushine RJ, Primack PD, West LA, Runyan DA. Interpretation of periapical lesions comparing conventional, direct digital, and telephonically transmitted radiographic images. *J Endod* 1998;24:262-6.
- Pass B, Furkart AJ, Dove SB, McDavid WD, Gregson PH. 6-bit and 8-bit digital radiography for detecting simulated periodontal lesions. *Oral Surg Oral Med Oral Pathol* 1994;77:406-11.
- Farman AG, Avant SL, Scarfe WC, Farman TT, Green DB. In vivo comparison of Visualix-2 and Ektaspeed plus in the assessment of periradicular lesion dimensions. *Oral Surg Oral Med Oral Pathol Oral Radiol Endod* 1998;85:203-9.
- Jones GA, Behrens RG, Bailey GP. Legal considerations for digitized images. *Gen Dent* 1996;44:242-4.
- Bruder GA, Casale J, Goren A, Friedman S. Alteration of computer dental radiography images. *J Endod* 1999;25:275-6.
- Horner K, Brett DS, Rushton VE. The potential medico-legal implications of computed radiography. *Br Dent J* 1996;180:271-3.
- Tsang A, Sweet D, Wood RE. Potential for fraudulent use of digital radiography. *J Am Dent Assoc* 1999;130:1325-9.
- Guneri P, Akdeniz BG. Fraudulent management of digital endodontic images. *I Endod J* 2004;37:214-20.
- Boscolo FN, Almeida SM, Haiter Neto F, Oliveira AE, Tuji FM. Fraudulent use of radiographic images. *J Forensic Odontostomatol* 2002;20:25-30.
- Visser H, Kruger W. Can dentists recognize manipulated digital radiographs? *Dentomaxillofac Radiol* 1997;26:67-9.
- Farman AG, Lapp RP. Image file interoperability for data protection, communication and trans-system connectivity. *Orthod Craniofac Res* 2003;6:151-5.
- Farman AG. Applying DICOM to dentistry. *J Digital Imaging* 2005;18:23-7.
- Chen SK. Integration of the digital imaging and communications in medicine standard into an oral and maxillofacial image management and communication system. *Oral Surg Oral Med Oral Pathol Oral Radiol Endod* 2001;91:235-8.
- Bushong SC. Radiologic Science for Technologists: Physics, Biology and Protection (ed 7). St. Louis: CV Mosby; 2001:374.
- Walton S. Information authentication for a slippery new age. *Dr Dobb's J* 1995;20:18-26.

28. Baldoza A, Sieffert M. Methods for detecting tampering in digital images. Air Force Research Laboratory, Information Directorate, Technology Transfer. Reference document IF-99-05. 1999. Available at: <http://www.afrlhorizons.com/Briefs/0001/IF9905.htm>. Accessed June 17, 2006.
29. Ho ATS, Zhu X, Woon WM. Semi-fragile pinned sine transform watermarking system for content authentication of satellite images. International Geoscience and Remote Sensing Symposium. Seoul, South Korea 25–29 July 2005.
30. Fridrich J, Goljan M. Images with self-correcting capabilities. International Conference on Image Processing. Kobe, Japan, 24–28 October 1999;792–6.
31. Zhu X, Ho ATS, Guan YL. Image content authentication using pinned sine transform. EURASIP J Appl Signal Processing 2004;14:2174–84.
32. Ho ATS, Zhu X, Shen J. Authentication of Biomedical Images Based on Zero Location Watermarking. International Conference on Control, Automation, Robotics and Vision. Kunming, China, 6–9 December 2004.
33. Lukas J, Fridrich J, Goljan M. Determining digital image origin using sensor imperfections. Proceedings of the SPIE (Society of Photographic Instrumentation Engineers) Electronic Imaging, San Jose, CA, 16–20 January 2005;249–60.
34. Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor noise. Trans Inform Security Forensics 2006;1:205–14.
35. Stegmark. Online digital photograph verification system. DataMark Technologies. Available at: <http://www.datamark.com.sg/onlinedemo/stegmark/index.htm>. Accessed June 20, 2006.
36. Chang SF, Lin CY. Issues and solutions for authenticating MPEG video. IEEE International Conference on Acoustics, Speech and Signal Processing. San Jose, CA. 15–19 Mar 1999;54–65.
37. Kalker T, Depovere G, Haitsma J, Maes MJ. Video watermarking system for broadcast monitoring. Proceedings of SPIE, Security and Watermarking of Multimedia Content 1999;3657:103–112.
38. Wade N, Sang-Hun C. Researcher faked evidence of human cloning, Koreans report. The New York Times. January 10, 2006.
39. Hwang WS, Ryu YJ, Park JH, et al. Evidence of a pluripotent human embryonic stem cell line derived from a cloned blastocyst [Retracted in: Science 2006;311:335]. Science 2004;303:1669–74.
40. Hwang WS, Roh SI, Lee BC, et al. Patient-specific embryonic stem cells derived from human SCNT blastocysts [Retracted in: Science 2006;311:335]. Science 2005;308:1777–83.
41. Sudbø J, Kildal W, Risberg B, et al. DNA content as a prognostic marker in patients with oral leukoplakia [Concern expressed in: N Engl J Med 2006;354:638] [Retracted in: N Engl J Med 2006;355:1927]. N Engl J Med 2001;344:1270–1278.
42. Sudbø J, Lee JJ, Lippman SM, et al. Non-steroidal anti-inflammatory drugs and the risk of oral cancer: a nested case-control study [Comment in: Lancet 2006;367:196] [Retracted in: Lancet 2006;367:382]. Lancet 2005;366:1359–66.