Review Article

Indian Journal of Forensic Odontology
Volume 6 Number 1, January - March 2013

Computer Based Review on Research and Development of Forensic Odontology

Mohit Dadu*

Pankaj Datta**

Dimple Arora***

Shivani Shokeen****

*PG Student, Department of Public Health Dentistry, I.T.S.-Dental College Muradnagar, Ghaziabad.

**Principal, Professor and HOD, Department of Public Health Dentistry I.T.S.-Dental College Muradnagar, Ghaziabad

***PG Student, Department of Public Health Dentistry I.T.S. -Dental College Muradnagar, Ghaziabad.

****PG Student, Department of Public Health Dentistry, I. T.S.-Dental College Muradnagar, Ghaziabad.

Abstract

We are living in the era of science and technology and it have infused with many aspects of our everyday life. With the advent of newer technologies the criminals have made full use of it which sometimes facade a challenging task to investigators such as forensic experts to catch the crime. An important observation in the field of Forensic Science is that most of the existing methods have been successful in certain crimes but these methods have not changed over the past few decades. Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information. Although it is most often associated with the investigation of a wide variety of computer crime. The use of computers in forensic dentistry has mirrored the use of computers in dentistry in general. There has been a rapid acceptance and use of computers for management of all front-office and many clinical procedures. Their use has presented new tools for solving difficult forensic problems and has created new concerns regarding their application in general dentistry. The accepted uses of computers in dentistry and forensic dentistry are presented along with suggestions for future directions. This review will discuss the need for computer forensics and application of technologies to be practiced in an effective and legal way, formalize basic technical issues, and point to references for further reading. It promotes the idea that the proficient practice of computer forensics and awareness of applicable laws is essential for today's networked organizations.

Keywords: Computer forensics; Criminal; Technology; Forensic dentistry; Dental records; Identification.

Introduction

Forensic Odontology is a vital branch of forensic science that involves that application of dental science to the identification of unknown human remains and bite marks, using both physical and biological dental evidence. Interest in forensic dentistry was relatively dormant until the 1960s when renewed interest was sparked by the first formal instructional program in forensic dentistry given in the United States at the Armed Forces Institute of Pathology. Over these years, technology has advanced in leaps and bounds and it certainly can be a good partner to find and evaluate better ways towards identification of individuals and to ensure that the correct persons are brought to justice for their actions. Computer technology can help to gather even more accurate evidence and therefore lead to a greater number of positive identifications with respect to possible identifications of an individual. Computer forensics emerged in response to the escalation

Corresponding author: Dr. Dimple Arora, H. No. - 399, Sector 21 - C, Faridabad - 121001, Haryana, India.

E-mail: dimple.dimplearora90@gmail.com

of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the Federation Bureau Investigation (FBI) laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations. The leveraging of computational techniques to aide in decision-making has been well established in the clinical arena for more than forty years.[1]

Today cyber forensics is a term used in conjunction with law enforcement, and is offered as courses at many colleges and universities worldwide." Computer forensics is the process of conducting an examination into the contents of the data on a computer system using state of the art techniques to determine if evidence exists that can aid in internal or legal investigations. Forensic specialists use a wide array of methods to discover data and recover deleted, encrypted, and damaged files.[2] In addition to a faulty legal system, the accessibility of advanced technology may be afflicting computer forensics. The North Atlantic Treaty Organization (NATO) defines cyber terrorism as "a cyber attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or to intimidate a society into an ideological goal" As computer systems grow more powerful, criminals may also abuse computer systems to commit crimes such as software theft, terrorism, and sexual harassment.[3]

The use of computers in forensic dentistry has mirrored the use of computers in dentistry in general. Although there are myriad definitions of digital forensics, network forensics, software forensics, computer forensics, etc., each is a sub-discipline of forensics, that is, "The use of science and technology to investigate and establish facts in criminal or civil courts of law" (American Heritage Dictionary of the English Language, 2000).[4]

Incidents of computer-related crime and telecommunications fraud have increased dramatically over the past decade. However, because of the esoteric nature of this crime, there have been very few prosecutions and even fewer convictions. The new technology that has allowed for the advancement and automation of many business processes has also opened the door to many new forms of computer abuse. Although some of these system attacks merely use contemporary methods to commit older, more familiar types of crime, others involve the use of completely new forms of criminal activity that has evolved along with the technology.[5]

Rules of evidence

Evidence in a computer crime case may differ from traditional forms of evidence in a much as most computer-related evidence is intangible-in the form of an electronic pulse or magnetic charge. Before delving into the investigative process and computer forensics, it is essential that the investigator have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceeding generally amounts to a significant challenge, but when computers are involved, the problems are intensified. Special knowledge is needed to locate and collect evidence and special care is required to preserve and transport the evidence. Before evidence can be presented in a case, it must be competent, relevant, and material to the issue, and it must be presented in compliance with the rules of evidence.

Digital Evidence

Digital evidence is any information of

probative value that is either stored or transmitted in a binary form (SWGDE 1998). This field includes not only computers in the traditional sense but also includes digital audio and video. It includes all facets of crime where evidence may be found in a digital form.[6]

Digital forensics

Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.[7]

Forensic engineering

Forensic systems engineering is the discipline investigating the history of Information Technology failures. It therefore focuses on the post-mortem analysis and study of project disasters.The work involves a detailed investigation of the project, the environment, decisions taken, politics, human errors and the relationship between subsystems.The work draws upon a multidisciplinary body of knowledge and assesses the project from several directions and viewpoints. The concept of systems is a central tool for understanding the delicate relationships and their implications in the overall project environment.[8]

Forensic odontology: Reaching the problem statement

Forensic Odontology is a specialized field of dentistry which deals with bite mark analysis and identification, mass disaster victim identification, missing person databases and identification, and other legal issues. The two main areas prominent to Forensic Odontology are Bite mark identification and Dental Identification.

Application of software technology in forensic odontology

In past decade it had been observed that software technology has emerged as an indispensable part of forensic odontology. Several research studies with application of software technology to identify an individual has been proposed and found to give very reliable results.

Bite mark identification

The teeth are an important part of our natural arsenal and are often used as a weapon in attack as well as defence. Various situations can force a person to bite another. Biting to inflict an injury can be the only means of defence for a victim.[9] In cases of violent crimes such as sexual homicide, rape, child sexual abuse, the assailant often bites the victim in an act of blind rage and ruthlessness.[10] There of course are cases of animals attacking humans leaving behind serious bite injuries which, at times can even be fatal. All these 'bites' leave certain 'marks' on the body of the person that is bitten. This mark is called a 'bite-mark' or 'bitemark' according to the recent odontology standards.[11] The standard techniques for examining bite marks are based upon interpreting photographic evidence in which a bite is compared with the models of the teeth of suspects.

Image perception software procedure

A photograph of a bite mark is opened with the image perception software, and a region of interest is then selected (Fig 1). After such selection, one can add colour to different greyscale areas of the image.

The assigning of selected colours to levels of grey values enables the forensic odontologist to select regions with similar grey values or to enhance subtle differences of grey values in the picture. The human eye can only distinguish about 40 shades of grey in a monochrome image, but can distinguish hundreds of different colours.[12] This will make it easier to establish which regions of pixel intensity is part of the bite mark and which are not. By omitting certain areas of pixel intensity, it is possible to isolate the region of the image which shows the bite mark.

Fig 1: Selected region of interest from original photograph

Fig 2: Image artificially coloured with image perception

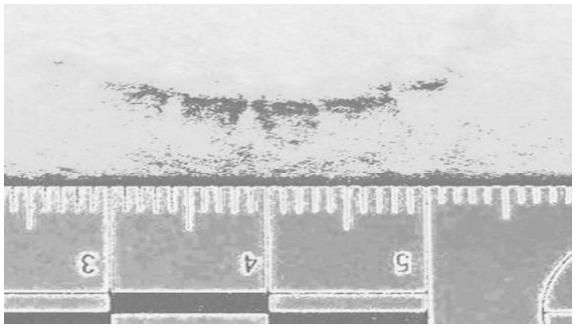
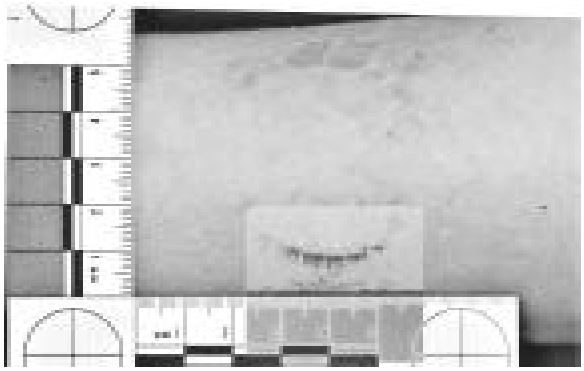


Fig 3: Image with visible incisal detail layered over original photograph technology software



A detailed image of the bite mark is produced (Fig 2) and the resolution of the image is then altered to be compatible with the resolution of the original photograph. Most bite mark images are scanned at 300dpi.

Part of the ABFO No. 2 scale has to be visible to accommodate the placement of the image over the original photograph with 100% exactitude.[13] The coloured image of the bite mark is now layered over the original bite mark photograph using Photoshop® of Adobe Systems. Manual methods to trace the images in order to generate the dental cast to identify an individual are sometimes problematic. So, special software have been devised which have reduced this problem and have provided high accuracy. With application of software technology it is possible to artificially colour areas with equal intensity values and depict a 2-D image as a pseudo- 3-D surface object. The use of image perception technology may allow visualization of a degree of detail unavailable with any other method.

Dental identification

Along with this, dental evidence is also used for the identification of human remains, medico-legal assessment of trauma to oral tissues, and testimony about dental malpractice. Teeth are highly resistant to destruction and decomposition, so dental identification can be made under extreme circumstances. It has become a popular and effective method to identify victims in cases of mass disasters like, fires, floods, plane crashes etc. when other methods of identification (fingerprints, physical etc.) are not available. Dental Identification involves comparison of one dentition with another and reaching a verdict. In most general cases the two dentitions compared being ante-mortem and post-mortem of the same person.[14]

Rugae pattern

Special software was designed called the Palatal Rugae Comparison Software (PR S Version 2.0) to match the clinical photographs taken using a SLR digital camera. The software recorded an accuracy of 99% in identification of individuals where as manual methods have shown high false positive and negative cases.[15]

Facial reconstruction

There are few studies which showed that with the application 3D Computed tomography scan and computer software

facial reconstruction can be done with low standard error of those measurements, from 0.85% to 3.09%. So, it can be used reliably in identification of individuals especially in mass disasters.[16]

Maxillary sinus in gender determination

Width, the length and the height of the maxillary sinuses were measured in Computerized Tomography scans with the application of software. Authors have concluded that Computerized Tomography measurements of maxillary sinuses may be useful to support gender determination in forensic medicine; however, with a relatively low-accuracy rate.[17]

Personal identification based on specific patterns of DMFS

Studies have been conducted to examine the overall utility of non-radiographic dental records for the establishment of individual identifications. It was found that even without radiographic lines of comparison, charts and notes that accurately detail a missing individual's antemortem dental condition can be essential for establishing an identification. Based on an analysis of two large datasets, individual dental patterns were determined using a special computer program (Odonto Search) and were found to be generally unique, or at least very uncommon.[18]

Computer crime investigation

The computer crime investigation should start immediately following the report of any alleged criminal activity. An incident response plan should be formulated, and a Computer Emergency Response Team (CERT) should be organized before the attack. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process. The use of a corporate GERT is invaluable. Due to the numerous complexities of any computer-related crime, it is extremely advantageous to have a single group, which is acutely familiar with the incident response plan, to call upon.[5]

Conclusion

For computer forensics to progress, the law must keep pace with technological advancements. Clear and consistent legal procedures regarding computer system searches must be developed so that police and investigators can be properly trained. An International Code of Ethics for Cyber Crime and Cyber Terrorism should also be established to develop protocols for "obtaining and preserving evidence, maintaining the chain of custody of that evidence across borders," and "clearing up any difference in language issues." Following these measures may be the first steps to resolving the technological and legal limitations afflicting computer forensics. Interpol, the International Criminal Police Organization, has developed a Computer Crime Manual with "training courses" and "a rapid information exchange system" that serves as a foundation for international cooperation. Lastly, the criminal abuse of technology can be limited by equipping the police department with state-of-the-art training and equipment for forensic analysis. Only then is the world safely prepared to face the future of technology. As one author predicts, "the next world war will be fought with bits and bytes, not bullets and bombs".

References

1. Michael GN, Mark MP, Lawrence AP. Recovering and Examining Computer Forensic Evidence. *Forensic Sci Comm.* 2000; 2(4): 32-5.
2. Digital Forensics of Texas, Inc. 2005. Available at http://home.swbell.net/txki dd/ forensics.html. Accessed Dec. 7, 2011.
3. Hoyte B. The need for Transnational and State-Sponsored Cyber Terrorism Laws and Code of Ethics (2012). Available at http:// articles.forensicfocus.com/2012/09/28/the-need-for-transnational-and-state-sponsored-

cyber-terrorism-laws-and-code-of-ethics/. Accessed Dec. 7, 2011.

4. Awson RD. Computers in forensic dentistry. *J Calif Dent Assoc.* 1996; 24(5): 58-61.
5. Computer crime investigation & Computer forensics. *Information Systems Security.* 1997; 6(2): 56-125.
6. National Center for Forensics Science 2005. Available from http://www.ncfs. org/ home.html. Accessed Dec. 7, 2011.
7. Kruse WG, Heiser JG. Computer Forensics: Incident Response Essentials. Amsterdam: Addison-Wesley longman; 2002.
8. Dalcher D. Forensic ECBS: The Way Forward. Eighth annual ieee international conference and workshop on the engineering of computer based systems, proceedings. Los alamitos. *IEEE Computer Soc.* 2001: 332-3365.
9. Furness J. A general review of bitemark evidence. *Am J Forensic Med Pathol.* 1981; 2: 49-52.
10. Webb DA, Pretty IA, Sweet D. Bitemarks: A psychological approach. Proceedings of the American Academy of Forensic Sciences. *Reno, NV.* 2000; 6: 147.
11. Bowers CM, Bell GL. ABFO Guidelines and Standards. Manual of Forensic Odontology; 3rd edition; American Society of Forensic Odontology. *Colorado Springs.* 1995; 299: 334-353.
12. Castleman KR. Digital Image Processing. Englewood Cliffs: Prentice-Hall Inc.; 1996, 556.
13. Hyzer WG, Krauss TC. The bitemark standard reference scale-ABFO No. 2. *J Forensic Sci.* 1988; 33(2): 498-506.
14. O'Connor T, Mark S. Course material for JUS425: 'Forensic Law' at the North Carolina Weslyan College, Rocky Mount, NC: 2006.
15. Hemanth M, Vidya M, Shetty N, Karkera BV. Identification of individuals using palatal rugae: Computerized method. *J Forensic Dent Sci.* 2010; 2(2): 86–90.
16. Sdos S, Ramos DL, Cavalcanti MG. Applicability of 3D-T facial reconstruction for forensic individual identification. *Pesqui Odontol Bras.* 2003; 17(1): 24-8.
17. Teke HY, Duran S, Canturk N, Canturk G. *Surg Radiol Anat.* 2007; 29(1): 9-13.
18. Adams BJ. Establishing personal identification based on specific patterns of missing, filled, and unrestored teeth. *J Forensic Sci.* 2003; 48(3): 487-96.