基于数字水印和数字签名技术的医学影像存储与传输系统安全机制研究*

曾 旭 司马宇

（遵义医学院医学信息工程系 遵义 563003）

〔摘要〕 针对目前未引入安全机制的医学影像存储与传输系统，提出基于数字水印和数字签名技术的安全机制方案。数字水印技术对医学图像进行有效的版权等信息认证，数字签名技术对医学图像的发送方与接收方进行身份等信息的认证，为远程医疗的发展提供支持。

〔关键词〕 医学影像存储与传输系统；数字水印；数字签名；仲裁；远程医疗

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2016.07.010

Research on the Security Mechanism of Medical Picture Archiving and Communication System Based on Digital Watermarking and Digital Signature Technology

ZENG Xu, SIMA Yu, Department of Information Engineering, Zunyi Medical College Zunyi 563003, China

〔**Abstract**〕 Regarding the medical picture archiving and communication systems without the security mechanism, the paper proposes the solution based on the digital watermarking and digital signature technology. The digital watermarking system can validly authenticate such information as the copyright of medical pictures, while the digital signature technology can authenticate such information as the identities of senders and receivers of medical pictures. The paper provides support for the development of telemedicine.

〔**Keywords**〕 Picture Archiving and Communication System (PACS); Digital watermarking; Digital signature; Arbitration; Remote medical

1 引言

随着现代医院数字化进程的推进，传统的医学图像保存介质已由胶片转变为数字图像、光盘、磁盘等。新技术无疑为临床诊断带来很多便利，但由于数字图像容易被修改，所以医学数字图像的认证显得尤为重要。将数字水印技术和数字签名技术引入到医学影像存储与传输系统[1]中将在较大程度上保证病患个人资料的安全，为及时治疗提供便利。该技术在确保图像准确真实基础上，也使医生避免误诊，进而减少医院与患者之间的医疗纠纷，对于保证远程诊疗安全性具有积极意义。

2 医学影像存储与传输系统安全性分析

医学影像存储与传输系统（Picture Archiving and Communication System，PACS）是近年来随着数

〔收稿日期〕 2016－02－25

〔作者简介〕 曾旭，副教授，发表论文 7 篇；通讯作者：司马宇，副教授。

〔基金项目〕 贵州省科学技术基金资助项目（项目编号：LKZ［2011］22）；国家自然科学基金资助项目（项目编号：61463053）。

字成像、计算机和网络技术的进步迅速发展起来，旨在全面解决医学图像的获取、显示、存储、传送和管理的综合系统。它主要分为图像获取、大容量数据存储以及图像显示。医学图像必须遵循数字成像和通信标准，这使得医学影像存档通信系统可以兼容不同厂家生产的各种医学成像设备。由于医学影像存储与传输系统的广泛通用性，所以医生用于诊断的医学图像的安全认证也成为了关键性的问题。医学图像在不同用户之间的传输要求实现的安全性有：(1) 医学图像数据的保密性。由于医学图像显示病患的个人身体特征属个人隐私，院方有责任保护病患的身体特征的相关数据。(2) 传输医学图像双方身份的确定性。由于远程诊断或者病患转院等原因所引起的医学图像数据在公共信道上传输，均需要网络系统提供方便且安全的确认对方身份的保障措施。(3) 不可否认性。无论是在公共信道还是传统的医学图像交互过程中，信息是瞬息万变的。医学图像一旦顺利交互则不可否认，否则必将导致信息传输的双方以及病患的利益受损。(4) 不可修改性。如果医学图像在公共信道传输的过程中被修改，结果必定造成医生赖以诊断的医学图像数据出现差错，最终可能导致病患得不到合理正确的治疗，有可能引发医疗纠纷。

3 基于数字水印和数字签名技术的医学影像存储与传输系统

3.1 数字水印技术

3.1.1 原理 数字水印技术 (Digital Watermarking Technology)[2-4]是一种有效的数字产品版权保护和数据安全维护技术，是信息隐藏技术研究领域的一个重要分支，它将具有特定意义的水印标记，利用数字嵌入的方法隐藏在数字图像、声音、文档、视频等数字产品中，用以证明创作者及其作品的所有权，作为鉴定、起诉非法侵权的证据，同时通过对水印的检测和分析保证数字信息的完整可靠性，从而成为知识产权保护、多媒体防伪和安全认证的有效手段。目前大多数水印制作方案都采用密码学中的加密体系来加强，在水印的嵌入、提取时采用一种甚至多种密钥联合使用的方式达到信息的隐蔽性和完整性要求。

3.1.2 本系统应用 本系统中通过置乱算法[5-7]将院方特定的印章数据进行置乱后，将得到的置乱印章嵌入到原始的医学图像中，嵌入过程需要院方提供特有的水印密钥。原始医学图像在院方的印章数据、水印密钥以及特定的置乱算法干预下，得到带有版权等水印信息的医学图像，操作流程，见图 1、图 2。

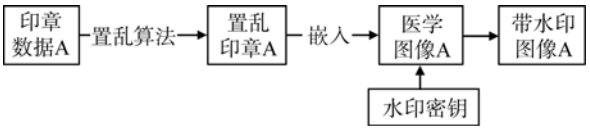

图 1 水印嵌入过程

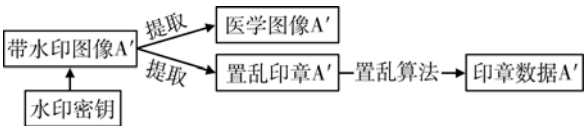

图 2 水印提取过程

3.1.3 具体实现过程 (1) 发送方利用置乱算法将自己特有的印章数据 A 进行置乱处理，得到置乱印章 A。(2) 将置乱印章 A 嵌入到医学图像 A 中，得到带水印的医学图像 A。该嵌入过程需要发送方的水印密钥。(3) 接收方可以直接根据接收到的带水印的医学图像进行临床诊断。(4) 若需要对接收到的带水印医学图像 A′进行仲裁，则需要发送方提供水印密钥。根据发送方提供的水印密钥可以在带水印的医学图像中提取置乱印章 A′和医学图像 A′。(5) 若印章数据 A 与印章数据 A′相吻合，则说明医学图像的版权等信息认证成功，否则失败。

3.2 数字签名技术

3.2.1 原理 数字签名技术 (Digital Signature Technology) 的发展目前较为成熟，其主要功能是使数据发送方无法否认自己的发送行为。目前的数字签名技术均是基于非对称的公钥密码体制，即该系统中应该包括医学图像发送方、医学图像接收方以及第 3 方权威认证机构 (Certification Authority, CA)。系统中用户的身份凭证是数字证书，数字证书对于用户是唯一的，且由用户预先申请。CA 负责发放和管理数字证书，用户在建立会话之前，首先通过数字证书经由 CA 建立彼此信任关系，在此

基础上，数字签名以及密文形式的会话过程确保合法接收内容的真实性，操作流程，见图 3、图 4。

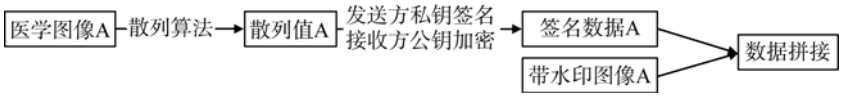

图 3 添加签名过程

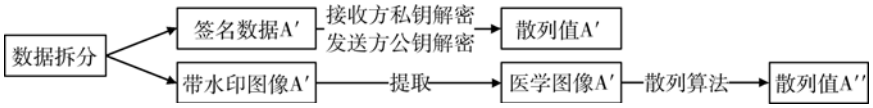

图 4 验证签名过程

3.2.2 具体实现过程 （1）双方决定使用公共信道传输医学图像，通过 CA 确定双方身份。（2）发送方用自己的私有密钥将传输医学图像的散列值 A 进行数字签名，然后使用接收方的公钥再次进行加密，使得接收方为唯一合法的接收者。（3）通过公共信道将进行数字签名后的散列值 A 和带水印医学图像 A 传输给接收方。（4）接收方用自己的私有密钥和发送方的公钥解密医学图像并获得散列值 A′，同时接收带水印医学图像 A′。（5）若医学图像 A′的散列值 A″等同于接收到的散列值 A′，则通信双方签名验证，否则失败。

4 整体框架

医学图像是医生赖以诊断的临床数据，要求较高的精确度。所以在公共信道进行传输的所有数据最终选择加解密效率较高的对称密钥，对称密钥的协商方式已经较为成熟。具体的发送与接收流程，见图 5、图 6。

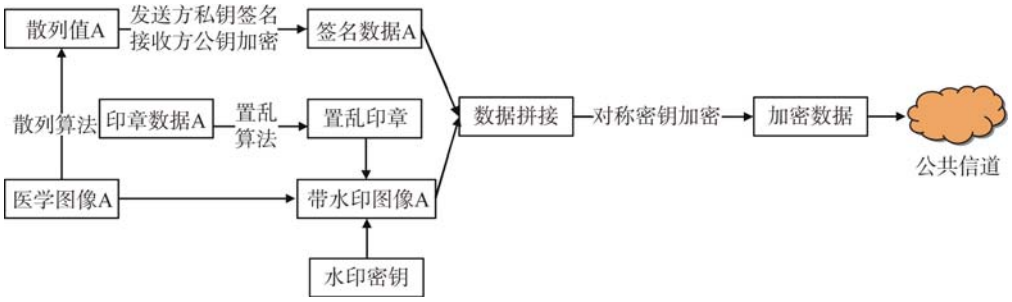

图 5 发送端流程

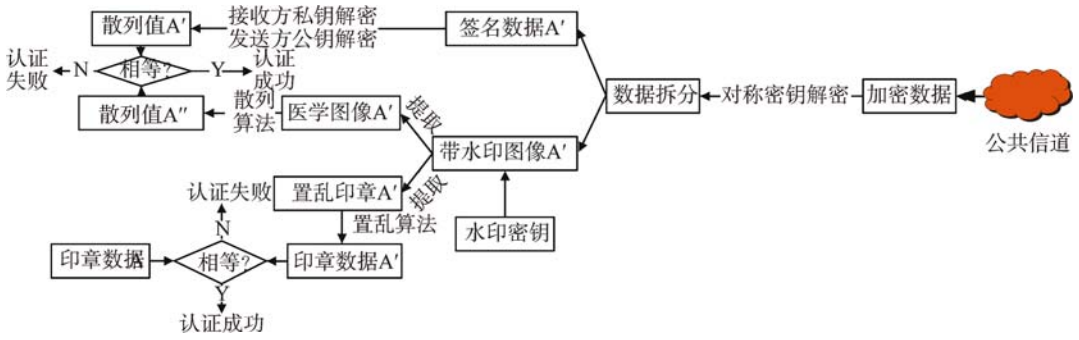

图 6 接收端流程

（下转第 50 页）

完成无线传输层安全协议 3 级加密，签名密钥设备以毫秒为单位，在无线传输层安全协议，主要用于握手时加/解密操作，保证长期无线传输层安全协议会话安全，客户端身份验证和数字签名。

4 结语

随着科技的发展，医院移动电子商务已初具规模，其安全问题也亟待解决。从接入终端层、通信层、网关协议层、应用服务层 4 层分析了医院移动电子商务的安全问题。在此基础上提出了一种基于无线传输层安全协议的医院移动电子商务安全解决方案，可以为医院服务器提供保密、完整、不可否认的识别服务。

参考文献

1 秦成德，王汝林. 移动电子商务［M］. 北京：人民邮电出版社，2012：223 - 227.

2 吴民. 移动医疗的应用［J］. 医学信息学杂志，2012，33（11）：2 - 5.

3 吕晓娟，仇保跃，王晓勇，等. 数字化医院建设热点难点分析［J］. 医学信息学杂志，2013，34（5）：21 - 24.

4 徐洪峰，徐曦，曾杰. 移动电子商务安全问题研究［J］. 计算机技术与发展，2011，21（11）：237.

5 贾末，王永刚，沈韬，等. 医院信息系统性能优化策略探讨［J］. 医学信息学杂志，2014，35（9）：28 - 31.

6 赵长超. WPKI 在移动电子商务中的研究和实现［D］. 济南：山东大学，2011：26 - 29.

7 姚志洪. 跨入移动健康时代［J］. 医学信息学杂志，2014，35（5）：2 - 7，24.

8 郑西川，孙宇，于广军，等. 基于物联网的智慧医疗信息化 10 大关键技术研究［J］. 医学信息学杂志，2013，34（1）：10 - 14.

9 吕福春，陈特放. 基于 WAP 的移动电子商务安全研究［J］. 福建电脑，2011，（12）：15 - 16.

10 张海燕. 移动商务的安全技术研究［D］. 长春：吉林大学，2012：25 - 27.

（上接第 46 页）

5 结语

在未引入安全机制的 PACS 中加入数字水印和数字签名技术能够解决安全性问题。数字水印技术能够保护医学图像数据的完整性，任何人不能对图像进行篡改和替换；水印也由于其透明性，攻击者不易发现其存在，同时也不影响医生对医学图像进行判断；数字签名技术能够同时保障医患双方的利益，发生争端时得到公正的仲裁。虽然数字水印和数字签名技术的引入在一定程度上降低了工作效率，但其提高医学图像保存、传输、显示的安全性，为远程医疗的积极发展提供了较好的保障。

参考文献

1 梁思宇，李继宏. 关于 PACS 与 HIS 的协同问题研究［J］. 中国医院管理，2010，（5）：70 - 71.

2 杨义先，钮心忻. 数字水印理论与技术［M］. 北京：高等教育出版社，2006.

3 J Fridrich，M Golijan，R Du. Distortion - free Data Embedding for Image［C］. Proc. 4th Information Hiding Workshop，Pittsburgh，Pennsylvania，2001：25 - 27.

4 刘瑞祯，谭铁牛. 数字图像水印研究综述［J］. 通信学报，2000，21（8）：40 - 49.

5 顾成喜. 一种改进的数字图像置乱方法［J］. 计算机仿真，2011，28（1）：261 - 264.

6 李子臣，杨义先，吴伟陵. 一类基于数字签名的密钥认证方案［J］. 电子学报，2000，28（4）：1 - 2.

7 郭小涛. 面向医学对象的无损数字水印系统的研究［D］. 上海：上海交通大学，2008.