

基于小波图像压缩的远程医疗系统设计

余大勇(广州 421 医院信息科, 广东广州, 510000)

摘要: 介绍远程医疗系统的基本概念和发展状况。针对目前 421 医院现有网络和互联网情况, 提出了一种远程医疗系统的设计方案。利用 RSA 加密算法实现文字信息的加密, 利用小波分析技术实现图像压缩, 利用成熟的网络技术完成远程信息的传输。最后分析了系统的不足和发展方向。

关键词: 远程医疗; 小波变换; RSA 算法; 图像压缩

分类号: R444 TP873

文件标识符: A

The Design of Telemedicine System based on Wavelet Transformation Image Compression

YU Da-yong(Guangzhou 421 Hospital, Guangzhou, 510000)

Abstract: The basic concept and circumstance of telemedicine is introduced. According to the network of the hospital, a design of Telemedicine System is discussed. The encrypt method of text information is implement using RSA arithmetic. The image information is compressed using wavelet transformation. And the insufficiency of the system is analyzed.

Keywords: telemedicine; wavelet transformation; RSA arithmetic; image compression

计算机技术日新月异的进步推动着信息化事业的飞速发展, 信息作为知识经济时代的主体, 其重要性已引起社会普遍关注。目前, 421 医院已基本建立了较为完善的医院内部信息网络, 在医院管理中发挥着越来越重要的作用。同时, 为了保障驻岛边远地区战士的健康, 也建立了电子病历系统, 但是该系统对于急重症的治疗无法提供及时有效的信息传输和处理。作为军队中心医院, 很有必要利用先进的计算机技术给边远地区战士提供良好的医疗服务。

1 远程医疗系统概述

1.1 远程医疗

远程医疗是一种新兴的医疗服务方式。它利用现代通信网络, 结合计算机多媒体技术, 传输多媒体医疗信息来实现远距离的医疗活动。其主要应用形式有远程医疗诊断、远程医疗会议、远程医疗教育、远程医疗信息检索等, 主要着重于多媒体交互式服务。

远程医疗可减少边远地区病人求医的费用和求医诊治花费的时间, 节省医院医生往返各地的

费用和时间，也可以提供分散的医院之间的远程交流和协作，使医院能接触更广泛的病例，提高医疗水平，尤其对提高地广人稀地区的医疗水平可以起到重要的作用。所以，在国外，远程医疗应用得到了广泛的重视^[1]。

1.2 远程医疗系统的发展现状

国外远程医疗系统已发展到第三代远程医学，其主要特征为^[2]：传输界面主要以局域网和广域网相结合的模式，有线通信主要采用公共电话网技术(PBDN)，综合业务数字网技术(ISDN)，异步传输技术(ATM)和压缩电视技术等；无线通信主要依赖卫星的远距离传输；已实现实时动态图像和高分辨率静态图像的传输。在发达国家，远程医学已进入实际应用、普及、提高并使其更完善的阶段。已有不少商品化的系统出现。

远程医疗是我国在 80 年代中期才开始发展，发展初期的远程医疗存在着许多缺陷。由于大多采用电话线进行点时点的通信模式，成本高，而且覆盖面小。而开发在 Web 上的远程医疗会诊平台，可以方便地实现不同地域的医学专家进行医疗会诊，改变了原来电话线点对点的模式，节省了远程医疗的费用。1994 年在国家卫生部领导下国家信息网“金卫工程”建设。1994 年 10 月在上海科技节“人类已步入信息化时代”为主题的活动中，上海医科大学附属中山医院通过网络演示了远程医疗会诊，1995 年上海远程医疗会诊项目正式启动，1998 年，中国金药电子商务网”又开发成功并投入运营，为医药卫生行业的发展提供了科研、交流、销售、分析、管理等电子化远程模式。此外，中华医学会、中华医学基金会等单位也陆续开展了远程医疗服务。

2 远程医疗系统结构

2.1 远程医疗系统的要求

提供远程医疗服务的软硬件设备组成的系统称为远程医疗系统。虽然远程医疗有多种应用形式，但是对一个远程医疗系统来说，我们可以把需要实现的功能概括为以下几个方面：

无论是病人的病案还是远程医疗教育的内容都包含了不同形式的信，根据医疗信息的形式不同可以分为以下 4 类：

- ① 文字和数据信息，如病人的病史描述、医生的诊断结果和一些检查结果数据等；
- ② 音频信息，如病人的心音、诊断现场或会议现场的对话和远程教育中的旁白等；
- ③ 静止图象信息，如病人的 X 光片、CT 片和核磁共振片等；
- ④ 视频图象信息，如病人的超声、胃镜等活动视频等。

而且医用多媒体信息内容与其它多媒体信息不同之处在于：一旦取得了某种媒体的医疗信息内容(尤其是诊断信息和医疗检查信息)一般不允许做人为的修改。因此，医用多媒体信息内容具有不可修改性。

医用多媒体信息又具有一定的结构，例如病人的病案就可能包括一份病人个人信息表（文字），若干份就诊情况记录；每份就诊记录可能包括若干张 X 光片、cr 片（静止图象）、超声视频等等。远程医疗过程中，在一定程度上可以调整医疗信息的结构和显示方式，增加新的原始信息内容，但是一般不能改变医疗信息的原有内容。

医疗多媒体信息内容的不可修改性和信息结构的可调整性，构成了远程医疗多媒体应用与一般多媒体应用的差别。一个完整的远程医疗系统应当提供各种媒体内容的采集和存储的功能和医用媒体结构的编辑、检索和传送的功能。

2.2 远程医疗系统网络结构

远程医疗系统主要利用 Internet 网络来完成基本医疗信息的传输和完成医生和患者之间的语音交流等信息。

远程医疗系统应用的特点是实时性强、数据共享性强、数据类型多，既有一般数据又有多媒体影像数据，但应用点分散的特点。因此系统要求具有快速、准确、安全的运行能力。目前医院网络已经达到以下规模：

- ①提供 200 个以上的信息点；
- ②内部主干采用 1000M 以太网，100M 交换到桌面方案，并在将来能方便地升级到 ATM 主干；
- ③网络能方便地扩展，在扩展升级时能保证性能，且不浪费现有设备；
- ④网络不仅能支持联机大型数据库应用，还能很好地支持远程医疗等多媒体应用等等；
- ⑤提供功能强大、简单易用的网络管理软件。

根据上述目标，网络硬件设备采用朗讯的 Cajun 产品，具有高性能、多层交换、分布路由、堆叠、网络管理等优点。

住院楼、门诊楼、放射楼、医技楼、物资仓库、药厂通过交换机进行网络连接，用需要远程医疗服务的单位，可以使用微机通过电信线路 (PSTN / ISDN) 与总院连接。

网络结构如图 1 所示。

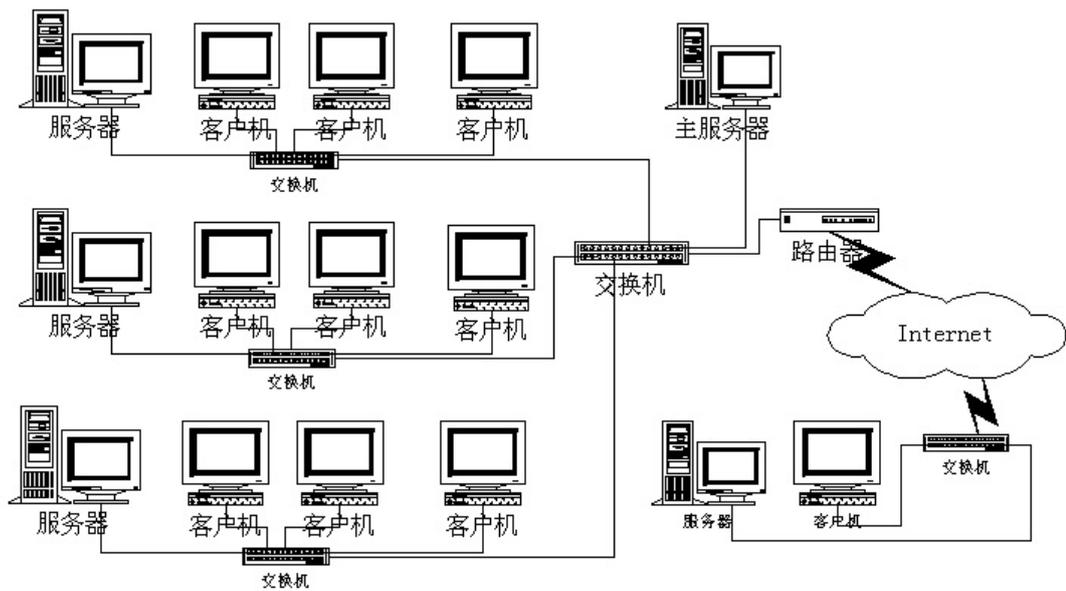


图 1 医院网络结构示意图

2.4 远程医疗系统结构

本远程医疗系统是以 Internet 作为传输媒体，借助其空间的异地性、系统的异构性以及各种基于 Internet 的规范和协议的通用性，来构建传输可靠、组建方便、分布广泛的远程医疗系统。

在该技术方案中主要利用了最基本的 TCP/IP(传输控制/Internet)协议中的 FTP(文件传输协议)和 TCP 传输协议，可以使用摄像头和便携式计算机，来构建系统。

对于文字和数据信息可以使用 FTP 协议来传输，考虑到部分信息信息不能公开传输，使用比较成熟的 MD5 加密算法进行加密，确保网络信息传输的安全。

对于图象信息（包括静止和动态图象）使用 TCP 协议传输，并使用小波压缩算法进行压缩，降低网络流量，提高传输效率。

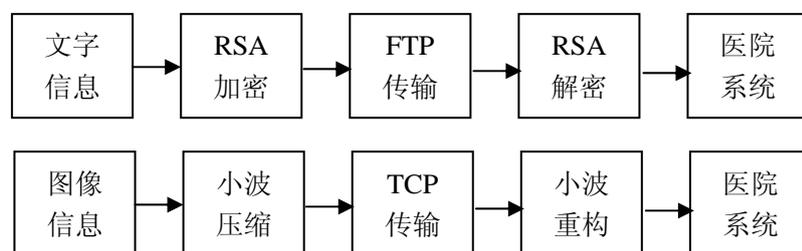


图 远程医疗系统处理过程

以下具体表述 FTP 传输和 TCP 传输的技术细节。

(1) Ftp 传输模块

Ftp 传输模块主要用于传输文字信息，包括患者姓名、单位等基本信息，还传输医师诊断后作出的最终病理报告信息。它的功能相对比较简单，基本上只是用于文件的上传、下载。在平台的模块设计上占的比重不大，设计上应集中精力于文件准确无误的存放到会诊双方的指定 Ftp 文件夹中，并由 Ftp 模块中的传输管理程序来自动完成。

(2) TCP 传输模块

TCP 传输是面向连接的传输，具有高可靠性、高稳定性。在系统中主要传输图像信息，考虑到边远地区的网络环境较差，因此，在满足图像分辨率要求的同时，需要尽可能减小文件大小。目前基于小波的图象压缩算法效果比较理想。

3 系统核心技术

3.1 小波图像压缩

为把小波变换用于图象处理，可以使用二维离散正交小波变换。二维Mallat算法公式如下^[3]：

$$D_{j+1} = H_c H_r D_j$$

$$C_{j+1}^1 = G_c H_r D_j$$

$$C_{j+1}^2 = H_c G_r D_j$$

$$C_{j+1}^3 = G_c G_r D_j$$

其中： $j = 0, 1, \dots, J - 1, J$

合成公式为：

$$D_j = H_c^* H_r^* C_{j+1} + G_c^* H_r^* C_{j+1}^1 + H_c^* G_r^* C_{j+1}^2 + G_c^* G_r^* C_{j+1}^3$$

重构信号为：

$$f(x, y) = \sum_{j=1}^J \sum_i \sum_m \sum_n C_j^i \Psi_{j,m,n}^{i*}(x, y) + \sum_m \sum_n D_j \varphi_{j,m,n}^*(x, y)$$

文献提出了一种小波压缩算法^[4]，步骤如下：

(1) 小波分解

将原图像进行 4 级小波分解，会得一个逼近子图像 LL4 和 12 个不同分解尺度上的高频子图像 LH_j、HL_j、HH_j (j=1, 2, 3, 4)。其中，LL4 为 4 级分解后的和原图像的逼近子图像，LH_j、HL_j、HH_j 为第 j 次分解后得到的该尺度上的水平、垂直、对角方向信息的细节子图像。

(2) LL4 量化编码

由于在子带 LL4 中集中了最多的能量，对恢复图像质量的影响最大，所以应采用无损压缩编

码，以减小失真；

(3) 计算统计特征量

计算 12 个高频子带的样本标准差 D；

(4) 量化系数

先取出各子带图像系数的符号，得到符号映射表，并对所编码的系数取绝对值。然后，根据上面的讨论，对不同的子带设置不同的系数量化范围，而范围的确定是以各子带的样本标准差 D 为依据。在不同的子带我们选择和它自身样本标准差 D 有关的阈值，把相应子带的系数与阈值比较；根据比较结果可以得到一映射表，映射表的元素 a 定义为

$$\begin{cases} a = 0 & |x| < T \\ a = 1 & |x| \geq T \end{cases}$$

其中：x 为子带图像系数；T 为阈值。然后，改变阈值，获取新的映射表。同时，T 的选择依赖于各子带小波系数的分布以及压缩比的要求[12]。

(5) 编码

因为映射表中 0 的比例很大，为提高编码效率，所有的量化映射表都采用游程编码，再进行 Huffman 编码。

3.2 加密算法

由于本远程系统将服务于部队，对一些比较敏感的信息必须采取加密手段才能利用开放的互联网络进行传输。RSA 加密算法是目前比较成熟、可靠的公开密钥算法，在本系统中使用 RSA 加密算法。

RSA 体制是 Rivest、Shamir 和 Adleman 在 1978 年提出的，其算法如下：

1. 选择两个质数 p 和 q；
2. 计算 $n=p*q$ 和 $z=(p-1)*(q-1)$ ；
3. 选择一个与 z 互质的数 d；
4. 找出 e，使得 $e*d=1 \pmod{z}$

对信息 P 加密，计算 $C = P^e \pmod{n}$ ，解密时计算 $P = C^d \pmod{n}$ ，可以证明，加密函数和解密函数互为反函数。公开密钥由 (e, n) 构成，而解密密钥由 (d, n) 构成^[3]。RSA 是目前公认比较安全的加密算法，其安全性分析可参见文献 5。

4 结束语

基于以上的分析和设计，实现了远程医疗系统的原型机，在互联网上方便地创建了节点，实

现了文本和图像的传输，效率较高，运行稳定。本系统的设计为低成本实现远程医疗系统提供了一定的参考。还将进一步完善该设计，增强医疗管理的功能，完善系统，为边远地区的病员提供更好的医疗保障。

参考资料：

- [1] 朱康辛,杨宇航,诸鸿文. 远程医疗系统结构模型研究. 计算机工程. 1999, 23(特刊): 126-128
- [2] 张巍,毛玉明. 远程医学和远程医疗野战化. 军事医学科学院院刊. 1999, 23(4):301-304
- [3] 姚天任,孙红. 现代数字信号处理. 华中科技大学出版社. 1999, 11:282-285
- [4] 侯文生,吴小鹰,彭承琳. 一种基于小波变换的医学图像量化编码算法的研究. 生物医学工程学杂志. 2002, 19(4): 657~659
- [5] 杨鹏,姚旺生. 微机上使用 RSA 加密算法的安全性初探. 计算机应用与软件. 2002, (5):57-59

作者简介：

余大勇，男，(1977-)，工程师，大学本科，广州 421 医院信息科，主要领域：医院信息管理、网络技术。