文章编号:1002-8692(2009)09-0033-02

远程医疗中的图像加密系统

·实用设计·

胡 蓉,王 玲

(湖南大学 电气与信息工程学院,湖南 长沙 410082)

【摘 要】介绍了一种基于TI公司的TMS320DM642 DSP的图像加密系统。该系统直接从医疗仪器(如CT、核磁共振等)中读取已生成的数字图像信号,通过网络接口将其输入到DSP处理模块,并使用图像加密算法对图像进行计算和变换,最后通过TMS320DM642独有的EMAC模块对数据进行传输,实现医学图像的远程传输。

【关键词】TMS320DM642;远程医疗;图像加密

【中图分类号】TP277 【文献标识码】A

Image Encryption in Remote Diagnosis System

HU Rong, WANG Ling

(College of Electrical and Information Engineering, Hunan University, Changsha 410082, China)

【Abstract】 An image encryption system based on TI TMS320DM642 chip is introduced in this paper. These medical images are gained from the physic instrument (CT or nuclear magnetic resonance), and transmitted through the module of network to DSP. Then image encryption algorithm is used to transform and calculate the signal, making the images invisible. Making use of TMS320DM642's peculiar function, EMAC module transmits the data to network to realize the remote diagnosis.

【Key words】 TMS320DM642; remote diagnosis system; image encryption

1 引言

近年来,放射学、影像医学、数字化图像技术与计算机技术及通信技术的结合,形成了图像存储与传输系统(Picture Archiving and Communication System,PACS)[1-2]。PACS系统已成为现代及未来的医学图像影像信息管理利用的主流趋势,也已成为了医院信息系统的重要组成部分。在未来的远程医疗中,医学影像资料的采集与交换,远程医疗中传输图像信号的频率也越来越高,法律要求患者的资料都要进行加密再进行传输,其安全性及隐蔽性也开始受到关注。

2 系统硬件设计

2.1 系统概述

整个远程医疗图像加密系统由两部分组成:DSP图像处理系统和数据的网络输入输出模块。主要功能模块有DSP存储器模块,DSP时钟和中断模块,DSP核心处理模块和网络输入输出设备。系统框图如图1所示。

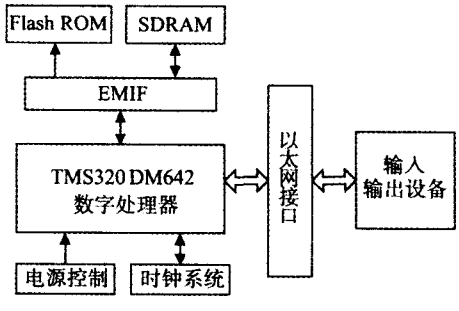

图1 远程医疗图像加密系统框图

系统工作原理是:由CT等医疗影像仪器得到的数字图像信号,经过网络接口进入DSP核心处理模块,由DSP模块对采集到的数字图像信号进行加密处理,最后通过网络传输实现远程医疗。

2.2 DSP核心系统设计

2.2.1 系统设计要求

本系统的总体设计要求为:具有高速处理能力,能满足高灰度级别的医学图像大运算量的要求,同时要求存储容量大,便于图像管理,采集的灰度图像为1 024×1 024,灰度级别为2 048~4 096。该系统的主控芯片选择TI公司针对多媒体处理领域应用的高性能的TMS320DM642(以下简称DM642)。

2.2.2 EMIF内存扩展模块

本系统主要用于高精度的灰度医学图像,所以在处理中会产生大量的数据,需要扩展大容量的外部存储器才能满足数据处理的需要。DM642通过EMIF访问片外存储器,可配置为SRAM,Flash,SDRAM等各类存储器接口。

DM642的EMIF支持对同步设备的直接接口,最常用的是同步动态存储器(Synchronous Dynamic RAM,SDRAM)。采用MICRON公司的MT48LC16M16A2,与DM642的连接示意图如2所示。DM642还需要扩展一个Flash存储器,用于保存程序代码和掉电后仍需要保存的用户数据。本设计中选用的是AMD公司的8 Mbit(1M×8 bit)的MBM29DL800TA芯片,图3为MBM29DL800TA

与 DSP 的接口示意图。

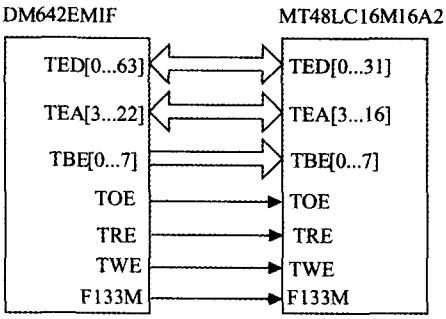

图 2 MT48LC16M16A2 与 DM642 的连接图

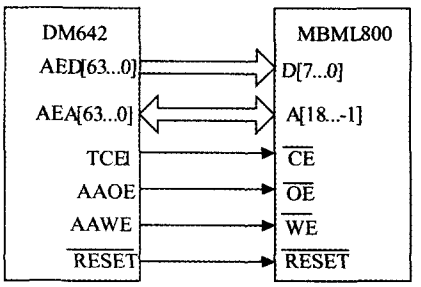

图 3 MBM29DL800TA 与 DM642 的连接图

2.3 输入输出系统的设计

本系统输入的信号为 CT 或核磁等医疗仪器中的数字信号，由于一般的医疗器械数据外部接口的输出方式为网络接口，所以采用 DM642 的网络功能。

针对 DM642 内嵌了一个以太网控制器，这里采用 Intel 公司的 LXT971ALC 芯片。连接电路如图 4 所示，从 DM642 传输过来的数据通过 LXT971A 转换为以太网物理层能够接受到的数据信号后，通过隔离变压器再经过 RJ-45 传输到以太网上去。

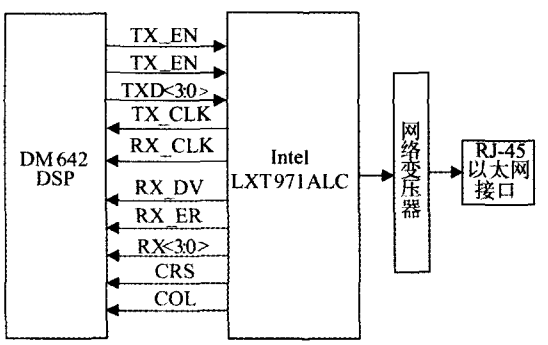

图 4 DM642 网络接口电路

由于传输的是专用医学图像，不采用 BMP，JPEG 等一般格式，而是以 DICOM 格式存放。本设计采用 DICOM3 标准，标准的第 8 部分提供消息交换的网络支持，说明 DICOM 实体之间在网络环境中通信服务和必要的上层协议的支持。DICOM 中使用的是 OSI 和 TCP/IP 两类协议[3]。

3 系统软件设计及核心算法分析

3.1 系统整体软件设计

整个远程医疗图像加密系统的软件设计流程如图 5 所示。

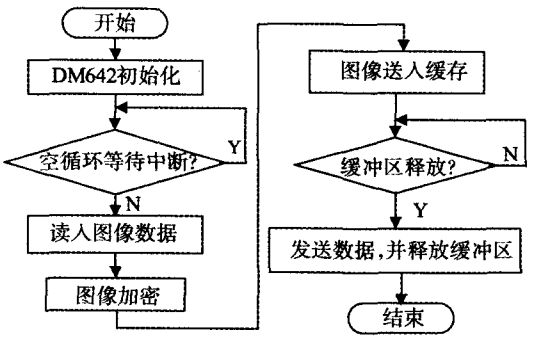

图 5 图像加密系统软件流程图

首先初始化系统各个模块，开始空循环等待中断，然后从医学影像仪器采集原始图像，DSP 对读取的数据进行加密，之后将数据送入缓存等待发送[4]，发送完毕后释放缓冲区。

3.2 网络模块流程

从医学影像仪器采集图像信号时，等系统和网络口初始化后，开始扫描并进行 AD 采样，待 FIFO 存储完毕后 DSP 开始读取数据，DSP 算法对数据进行处理后送入以太网处理，结束后停止 AD 采样。

加密后的数据经过网络端口传输时，先读取状态寄存器，等待寄存器接收完毕再检测缓冲区的状态，若正在释放则等待释放完毕，将待发送的数据写入发送缓冲区，发送完毕后释放缓冲区。

经过图像加密处理后的数据还是 1 024×1 024 的数字格式的图像，FIFO 数据存满时，会通过硬件中断通知 DM642，开始 EDMA 方式的数据传输，在不占用 CPU 资源的情况下将 FIFO 数据传入内存中指定的位置[5]，然后将数据打包发送。

3.3 核心算法

本文采用将混沌映射和模映射相结合的方法对图像进行加密，充分利用混沌的加密性能和模运算的置乱功能，在加密图像的同时尽量减少计算复杂度和运算时间，节约时间来处理下一幅图像。

3.3.1 混沌加密原理

混沌现象是一种复杂的非线性、非平衡的动力学过程，对初始条件极为敏感，对于两个相同的混沌系统，若使其处于稍异的初态都会迅速变成完全不同的状态，同时运动的无规则性及具有宽 Fourier 功率谱及类似噪声的特性，使其具有天然的屏蔽性，十分适合保密通信。

常见的混沌系统为 Logistic 混沌

（下转第 41 页）

4 小结

本文讨论了一种平面视频立体化技术，并针对直接使用商业软件提取深度后合成视频存在的闪烁问题提出了两个改进方法：一是在同一段视频中以某一帧图像的深度图为模板，相邻帧根据实际情况作相应的微调，这对于背景保持相对静止的视频效果较为明显，但对于运动物体效果不明显。二是在提取深度之前使用 Canny 算子进行边缘提取预分割，便于深度分层的同时，也使相邻帧的运动变化更为连贯，较好地解决了视频的闪烁问题。对两组立体化视频作主观测试评价的结果验证了方法的有效性，立体显示效果得到了改善。

参考文献：

[1] SCHREER O,KAUFF P,SIKORA T.3D videocommunication:algorithms, concepts, and real-time systems in human centred communication [M].Chichester,England:Wiley,2005.

[2] BARNARD S,FISCHLER M.Computational stereo[J].ACM Computing Servegs,1982,14(4):552-572.

[3] 唐志健.基于立体视觉的深度信息回复技术研究[D].大庆：大庆石油学院，2006.

[4] CANNY J. A computational approach to edge detection[J]. IEEE Trans. Pattern Analysis and Machine Intelligence,1986 (8):679-714.

[5] 王娜，李霞.一种新的改进 Canny 边缘检测算法[J].深圳大学学报，2005,4(2):149-152.

[6] TONY L. Edge detection and ridge detection with automatic scale selection[J]. International Journal of Computer Vision,1998,30(2):117-154.

[7] 侯春萍，俞斯乐.一种平面图像立体化的新方法[J].电子学报，2002,12 (12):1862-1863.

[8] ROBERTS L G. Machine perception of 3-dimensional solids, Optical and electro-optical information processing [M]. Cambridge: MIT Press,1965.

[9] SONKA M,HLAVAC V,BOYLE R. Image processing, analysis and machine vision[M]. [S.l.]:PWS Publishing,1999.

[10] 陆杰，赵旭忠.图像质量评价的发展[J].计算机工程，2000,26(11):4-5,49.

[11] 汪孔桥，KANGAS J A. 数字图像的质量评价[J].测控技术，2002,19(5):14-16.

责任编辑：许 盈 收稿日期：2009-07-04

(上接第 34 页)

$x(k+1)=1-ax^2(k)$，$a\in(1.401\ 15\cdots 2]$，$x(k)\in(-1,1)$，$k=0,1,\cdots$ (1)

式中：a 成为分枝参数。当 $a\in(1.401\ 15\cdots 2]$ 时，Logistic 映射工作于混沌状态。

3.3.2 模运算置乱

图像置乱是利用某种运算有效地打乱输入明文的次序，但变换后像素的总个数不变，直方图不变，进而能有效掩盖明文的统计特性，抵御统计分析。目前提出的置乱方法有 Arnold 变换和幻方变换，Fass 曲线，Hilbert 曲线等。本文采用的是新型的置乱——模运算。

设图像为 $f(x,y)$，$x\in\{0,1,\cdots,M-1\}$，$y\in\{0,1,\cdots,N-1\}$，其相平面上的任意一点 (x_n,y_n) 经过(4)映射变到另一点 (x_{n+1},y_{n+1})

$$\begin{cases}x_{n+1}=K_1\cdot x_n(modM)\\ y_{n+1}=K_2\cdot y_n(modN)\end{cases} \quad (2)$$

式中：K_1,K_2 分别是 $(2,M)$ 和 $(2,N)$ 范围内的范数，且 M 不能被 K_1 整除，N 不能被 K_2 整除，式(2)是一一映射，其逆变换为

$$\begin{cases}x_n=\dfrac{x_{n+1}+k_1M}{K_1},\ k_1\in\{0,1,\cdots,k_1-1\}\\ y_n=\dfrac{y_{n+1}+k_2N}{K_2},\ k_2\in\{0,1,\cdots,k_2-1\}\end{cases} \quad (3)$$

式中：x_n 和 y_n 变换应当满足的条件 $x_{n+1}+k_1M(modK_1)=0$，$y_{n+1}+k_2N(modK_2)=0$。

所用时间以及计算量都远远小于 Arnold 等置乱方法。这是因为 Arnold 等置乱的每次横坐标或纵坐标变换都有 2 次乘法，而模运算只要 1 次乘法运算，每一点的置乱都节约了 2 次乘法运算，计算时耗时最大的即乘法运算，所以采用此模运算节约了 $2N^2$ 次乘法计算。

4 小结

DM642 作为专用数字多媒体处理器，具有强大的图像处理功能、强大的配置及以太网硬件接口功能，同时经过混沌加密算法处理，保护了医学图像。在本系统中，以太网和 DSP 的通信技术可以广泛应用到远程医疗系统中其他医学信号的传输，在远程医疗的网络普及化方面具有一定的参考价值。

参考文献：

[1] 孙婷娇，刘谦. 远程医疗系统的信息采集与交换方法[J].中华医药管理杂志，2003(4):232-233.

[2] 何宇，郭建明. 基于 TMS320DM642 单芯片的网络接入系统研究与实现[J]. 武汉理工大学学报：交通科学与工程版，2005(10):770-773.

[3] 赵贵军，张大波. PACS 系统中的 DICOM 标准[J].微计算机信息，2006(6):259-262.

[4] 尹显东，李在铭，姚军，等. 图像加密传送系统的设计与实现[J]. 信息与电子工程，2004(3):1-4.

[5] 梁讯，熊水东. DM642 嵌入式网络接口开发设计[J].计算机工程，2007(8):277-279.

责任编辑：任健男 收稿日期：2009-06-29