基于网络的语音加密通信系统设计

王海春[1] 邱寄帆[2] 银 河[2]
[1](成都信息工程学院网络工程系 四川 成都 610225)
[2](成都航空职业技术学院计算机工程系 四川 成都 610021)

摘 要 主要介绍应用声码器基于网络系统设计的语音加密通信系统方案,给出了硬件系统组成结构。在对加密算法实现过程进行可行性研究和分析的基础上,阐述了应用 ADPCM 编码调制技术和 UDP协议进行网络环境下实时多点语音通信的方法。给出了编程方法说明实现过程。

关键词 声码器 数字信号处理 语音加密

DESIGN OF VOICE ENCRYPTION COMMUNICATION SYSTEM BASED ON COMPUTER NETWORK

Wang Haichun[1] Qiu Jifan[2] Yin He[2]
[1](Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, Sichuan, China)
[2](Department of Computer Engineering, Chengdu Aeronautic Vocational & Technical College, Chengdu 610021, Sichuan, China)

Abstract This paper briefly described the voice encryption communication system design project which use sounder based on computer network. The hardware system constitution is shown in the paper. Based on the feasibility study and the analysis to the encryption algorithm, the paper presents a method of the real-time multi-point voice communication in network, which uses ADPCM and UDP. Some programming methods have been displayed in the paper.

Keywords Sounder Digital signal processing Voice encryption

0 引 言

某型号工程工作在网络环境,数据和语音信号均在网络上传输。设计的基于网络的语音加密通信系统由 3个模块组成,第 1个模块是语音数据采集与处理模块,用于对语音信号进行放大、模/数与数/模转换、压缩与合成和信号加密处理。第 2个模块是网络通信系统模块,是 1个在基于 802.3以太网络标准的网络系统上调用 API函数实现网络用户间通信的模块。第 3个模块是软件系统模块,采用 VC++编程,实现语音通信的系统调度和管理。

1 语音数据采集与处理模块设计

语音数据采集与处理模块主要用于对语音信号进行放大、模/数与数/模转换、压缩与合成和信号加密处理。模块通过 PC机与网络系统相连。系统组成如图 1所示。

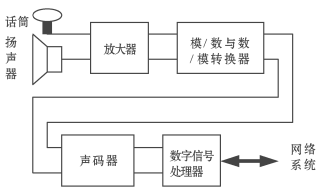

图 1 语音数据采集与处理模块

1.1 放大器

放大器采用 LM386音频功率放大器,主要用于扬声器的驱动。

1.2 模/数与数/模转换器

模/数与数/模转换器采用 ADI公司生产的 AD73311芯片,其内含 16位信噪比为 75dB的 A/D转换器和 16位信噪比为 70dB的 D/A转换器。

1.3 声码器

声码器采用美国 DVSI公司 AMBE-2000芯片[1],它是高性能、低功耗低速率编码/解码声码器,其主要特性为,语音质量高,压缩数据多,具有 2.0kbps、2.4kbps、3.6kbps、4.0kbps、4.8kbps、6.4kbps、8.0kbps、9.6 kbps等 8种压缩率,具有语音激活检测(vat)和插入舒适噪声(CNI)功能,能检测和产生双音多频(DTMF)信号,前向纠错功能可变速。

AMBE-2000工作时外接 16.384MHz的晶振,由于内部的 PLL电路,其内部工作频率达 66MHz。AMBE-2000的 A/D与 D/A语音接口信号可以是标准的 μ律或 A律压扩量化的 PCM信号,也可以是 16位线性量化的 PCM信号[2]。

收稿日期:2006-05-29。基金项目:四川省 2004年重点科技项目(项目号:04GG006-032)。王海春,副教授,主研领域:智能控制,语音处理,嵌入式应用。

1.4 数字信号处理器

数字信号处理器采用微低功耗、高性能的定点 DSP芯片 TMS320VC5416,用于控制和读写 AMBE-2000,负责控制话音的模/数与数/模转换,语音检测等算法的处理和加密算法等工作。系统加电正常工作后,微控制器复位 AMBE-2000芯片,开始进行语音编解码[3]。

AMBE-2000每 20ms完成 1帧语音数据的编码解码运算,并与控制器以标准串行方式交换一次数据,TMS320VC5416将编码后的语音加密后输出,同时将得到的要解码的数据送入 AMBE-2000进行解码。

2 网络系统模块设计

网络系统模块主要是利用现有的以太网络系统,考虑到系统的安全性要求高的特点,利用 Windows 2000 Server的网络安全管理功能,对用户身份和权限采取了严格的安全限制措施。在服务器上对数据进行了冗余备份并采取了严格的安全日志管理。

2.1 交换机

交换机采用锐捷的 STAR-1924F+可网管交换机,其端口具有 MAC、IP、用户名、帐号四元素绑定功能,从网络端口上限制了非法用户的接入。

2.2 通信传输协议

在网络上进行语音数据传输可采取 TCP(Transfer Control Protocol)协议和 UDP(User Datagram Protocol)协议。基于 UDP通信协议编制语音数据网络传输程序相对简单。为了传输数据,首先要设置双方的端口(Remote Port和 Local Port)属性,同时,要设置对方 IP(Remote Host IP)地址。这样,通过调用 Send Data方法就可以发送信息,有数据到来时会触发 Data Arrival事件,调用 Get Data方法接收已送来的信息。进行双向语音通信时,需要使用两个 Winsock控件。一个用于发送语音数据,另一个用于接收语音数据[4]。

3 语音数据加密算法设计

虽然网络系统采取了严格的安全管理措施,但网络连接的特点决定了在网络上采取某些办法仍然可以非法获取部分语音数据文件,为了加强语音数据通信的安全性,对经声码器处理后的语音数据还要进行加密处理。加密的算法是,让输入的语音信号与一个伪随机产生的加密序列进行模 2运算,解密算法是,让经加密处理后的语音数字信号与同样一个加密序列进行模 2运算,系统组成如图 2所示。

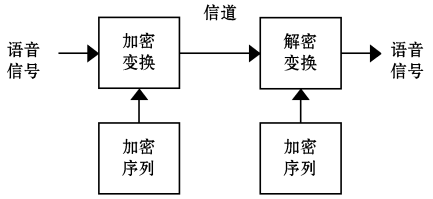

图 2 语音数字信号加密与解密处理系统

3.1 伪随机加密序列选取

为了保证语音信号传输的实时性,减少加密和解密的运算量,选择了在语音信号中加入伪随机密码序列的加密方法。

研究证明逻辑映射

$$X_{n+1}=1-2X^2n \qquad X\in(-1,1) \tag{1}$$

可以产生大量具有均值为零、自相关为 δ函数、互相关为零的统计特性的优良逻辑序列,因而可作为理想的密码序列,应用于语音信号的保密传输。Xn的码长选取非常关键,通过实验研究证明,当码长超过 64位时,语音信号的实时效果下降很快,当码长低于 8位时,保密效果明显降低。本系统 X的码长取 16位,取得了较好的效果。

3.2 语音信号加密系统设计

利用上述伪随机加密序列,采取逐位模 2加的计算方法,可以构成实时性良好的加密解密处理系统。语音输入端加密运算公式为:

$$Yn=Sn\oplus Xn \tag{2}$$

其中,Sn为声码器输出经压缩处理的语音数字信号,Xn为系统随机提供的密码序列,Yn为经加密后的输出信号,⊕为逐位模 2加运算符。

3.3 语音信号解密系统设计

接受端解密过程为加密过程的逆运算过程,解密运算公式为:

$$Sn=Yn\oplus Xn \tag{3}$$

其中,Yn为经加密处理的语音数字信号,Xn为系统随机提供的密码序列,⊕为逐位模 2加运算符,Sn为经解密后得到的语音信号。

4 语音通信调度与管理系统模块

语音通信调度与管理系统模块,采用 VC++编程,实现语音通信系统的综合调度与管理。系统分为服务器端软件系统和客户端软件系统。

4.1 服务器端软件系统

服务器端软件系统主要由 3个子模块组成。

系统设置子模块 主要负责系统初始化时要求客户提供相关初始信息。

通信监听子模块 为系统的主要工作模块,语音通信系统工作时,主要处于监听状态,负责收集用户要求通信的类型,例如是一对一还是一对多,并进行相应的设置和处理。

语音信箱管理子模块 主要负责管理由各用户发送给目标对象的语音文件,系统具有压缩、拷贝、删除、编辑等功能。

4.2 客户端软件系统

客户端软件系统主要由 2个子模块组成。

系统设置子模块 主要负责系统初始化时要求用户提供的相关初始信息。

通信子模块 语音通信系统工作时,主要工作于发送和监听状态,用户进行通信前要在菜单上选择是工作在一对一还是一对多状态,并将相应的信息传输给服务器管理系统。

5 结 论

基于网络的加密语音通信系统已经投入试运行,目前使用效果良好,达到了预期的设计目标。在 100Mb的以太网络上,同时使用人数在 20人以下时,通话质量和速度满足了用户要

求。但当同时使用的人数上升时,通话开始有明显的延时现象,这时只有降低语音的采样频率或加大声码器的数据压缩率才能达到要求,但同时话音质量下降很快。

本文提出的应用声码器硬件对语音信号进行压缩处理,应用 DSP对语音数字信号进行加密处理,利用以太网络系统进行语音通信调度管理的语音保密通信系统设计,较好地解决了网络多媒体应用中的带宽瓶颈问题和通信安全问题,非常适用于具有网络系统且对语音通信安全性要求较高的场合,具有推广和使用价值。

参 考 文 献

[1] 边会坤、苗杰光、丁铁夫、郑喜凤,"窄带宽有限距离语音通信系统设计分布式控制[J]",《电子技术应用》,2005(12):67~69.

[2] ITU-T Recommendation G.726 40,32,24 and 16 kb/s Adaptive Differential Pulse Code Modulation(ADPCM). 1990.

[3] 李朝青等. PC机与 DSP数据通信技术选编[M],北京:北京航空航天大学出版社,2004.

[4] 陈朝阳、薛峥,"基于以太网的可重配置数据与语音通信系统的设计[J]",《计算机工程与应用》,2004(10).

(上接第 25页)

② 非尖尾　它是相对于尖尾而言的,表示撇丝在到达尾部时并没有收缩为 1个像素。此时尾部的形状也可以有平尾、方尾、圆尾、光滑曲线尾等多种选择,具体的生成算法可以参见撇丝头部生成算法的描述,唯一的不同之处在于撇丝头部如果是根据撇丝的骨架向左扩展的话,撇丝尾部则向右扩展(头部与尾部总是相对而言的)[1]。

4 一组撇丝的生成算法

在图案创作或重描的过程中常常会用到一组有规律渐变的撇丝,这一组渐变的撇丝在规律渐变的同时又会随机地在指定的范围内变化,以满足快速便捷的创作要求[2]。

要产生一组带有随机范围的撇丝图案,先由创作者使用鼠标勾画出想要产生的一组撇丝的外部轮廓,它是由 *B* 样条曲线来描述的,这样算法就会根据一组撇丝中预定的参数自动产生一组形状和大小既相关又有随机性的撇丝。具体的算法如下:

① 用 B样条勾画出一组撇丝的外形曲线,存储于 FUR_UNIT数据结构中;

② 用 RandomPtArray函数产生一组带有随机性的控制点,存于 FLOWER数据结构中;

③ for(int i=0; i<flower.s_count; i++)用 CtrlPt函数产生一条随机撇丝所需的各个控制点;

④ 调用 FillFlower函数,在视图或在图像中实际画出这一组撇丝。

上述算法中用到的数据结构说明如下:

```
typedef struct{
    POINT    P_point_start[POINTS_COUNT];
    int      count;
    int      penWidth;
    int      clmum;
    int      mode;
} CURVE;        /每条 B样条曲线的信息

typedef struct{
    CURVE    s[MAXCURVES];
    int      s_count;
} FUR_UNIT;  /存放一组撇丝外形轮廓

typedef struct{
    CURVE    s[DETAILPOINTS+1];
    int      s_count;
} FLOWER;  /存放每条撇丝的控制点信息
```

实现一组撇丝功能的关键是 RandomPtArray这个函数的实现。由于一组撇丝必须有某种程度的形状相似性,同时在用户确定的边界上还必须和边界保持一致,因此我们在实现的过程中采用了旋转方法以保持一组撇丝的形状相似性,但是这样一来就不能做到同时与两边的边界完全保持一致,我们可以将两边同时相向进行旋转,两次旋转完成之后,再用两个函数进行融合,实际效果还是令人满意的。

实现旋转的公式如下:

$$x_1 = x\cos(angle) - y\sin(angle)$$

$$y_1 = x\sin(angle) + y\cos(angle)$$ [4]

旋转变换的正向角度是逆时针方向的。如果是顺时针方向旋转,则角度为负。

5 实验的效果图

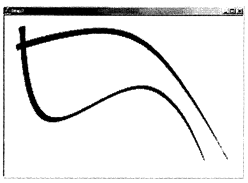

图 3　两根用 B样条曲线模拟的撇丝

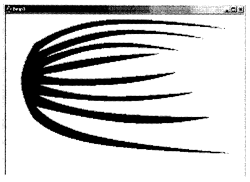

图 4　一组撇丝

6 结束语

本文就如何能够快速而有效的模拟纺织 CAD中有特色的撇丝工艺进行了算法方面的深入研究,用通过控制点控制的 B样条曲线来模拟撇丝,而且提供了详尽的算法,达到了非常好的效果,曲线非常自然圆滑,而且设计师可以用控制点自由的拉伸曲线而不会破坏撇丝的结构,可以创造出随心所欲的撇丝图案,让撇丝这种艺术风格发扬得淋漓尽致。最后还提出了如何用 B样条曲线算法实现一组撇丝,满足设计师对于一组撇丝灵活性的要求。

文中的算法已经成功地植入纹织和印花 CAD服务平台,此平台已经在《面向绍兴轻纺区域经济的网络化制造》中成功的应用,满足了绍兴中小纺织企业对于设计开发的要求,极大地提高了它们的生产力,而且将在今后的生产应用中进一步完善和发展。

参 考 文 献

[1] 陈纯、陈进勇著,纹织 CAD应用手册,北京,中国纺织出版社,2001.

[2] 马凌洲、许端清,"印花图案自动描稿系统的研制",《计算机工程》,2004,30(13):146~148.

[3] (美)David F. Rogers著,石教英、彭群生译,计算机图形学的算法基础,北京:机械工业出版社,2002.

[4] (美)Hearn D著,计算机图形学,第二版,北京:机械工业出版社,2002.