静态现场的远程实时可视化安全监控系统的研究

缪克华　李茂青
（厦门大学自动化系，厦门 361005）
E-mail：zxkd@jingxian.xmu.edu.cn

摘　要　传统的安全监控系统存在很多问题，如需要建设高速视频网络，需要人工实时看守智能化低、并且会涉及隐私问题。该文讲述了如何利用摄像机、计算机、极低速传输线路 PSTN（公用电话交换网）及互联网络构建一种智能型的、远程分布式的、实时可视化基于静态现场的监控系统。该系统结合了 Socket 技术、火灾探测技术、人形物体识别技术、M-JPEG 图像压缩技术。

关键词　安全监控　火灾探测　图象压缩

文章编号 1002-8331-（2003）05-0223-04　**文献标识码** A　**中图分类号** TP391.41

Research on Visible Security Monitor System of Remoter Stactic Scense

Miao Kehua Li Maoqing
（Departmen of Automation，Xiamen University，Xiamen 361005）

Abstract：There exist many problems in the traditional security monitor system.For example：it needs a Wide-Band Video Network，monitored by man，and the involved private problem.This article represents how to construct a intelligent，visible，distributed security monitor system of remote static scene by using video camera，computer，low-band network PSTN（Public System of Telephone Network）and Internet.This system combined Socket Technology，Fire Detection Technology，Human body Recognition Technology，and M-JPEG technology.

Keywords：security monitor，fire detection，Image Compression

1　引言

分布实时可视化安全监控系统广泛应用于工业生产、交通、电力和智能办公大楼、住宅小区的监控。传统的分布式可视化监控系统必须建立宽带视频线路网络，然后建立监控中心，实行人员看守监护。这种系统在各监控点分布十分远时，就要投入大量的资金建立视频线路网络。另外传统的人工看守监控还存在着涉及隐私问题，例如在住宅小区的监控系统，被监控现场（住家）中的主人并不希望监控者每时每刻监控他们的一举一动，而只有出现异常情况时例如在有非法闯入者或发生火灾等异常情况时，才需要向监控中心传送图像信息。而且现场的主人却可能需要在随时随地的查看现场的情况。而互联网的发展和图像压缩与智能识别技术的发展为大家提供了这种可能。如何利用摄像机、计算机、极低速传输线路 PSTN（公用电话交换网）及互联网络构建一种智能型的、远程分布式的、实时可视化监控系统，已经成为重要课题。

在实时监控中，当监控现场画面中的监控对象与背景图像都随时间不断变化而变化时，称之为动态现场。如交通违章状况监控系统、超市售货防盗监控系统等实时监控系统。在这一类系统中监控系统所监控的现场时刻都在发生变化，在这种动态环境对现场的变化状况作出智能识别是比较困难的。当监控现场画面中的监控对象与背景图像不变或有规律变化时则为静态现场，如无人看守仓库、家居、下班后的厂房、办公室、实验室等。相对于动态现场而言静态现场实时监控系统的智能化程度就可以做得很高。

下面提供构造这样系统的一种模型（如图 1）。

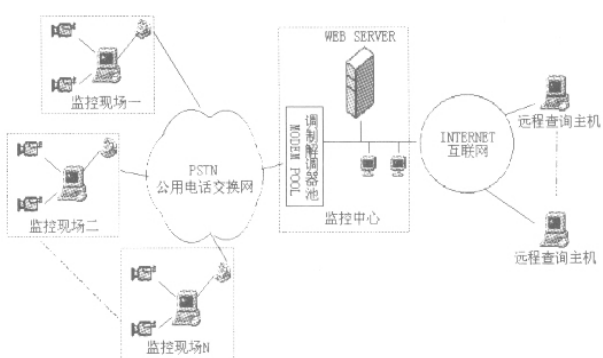

图 1　系统模型

2　工作原理

该系统由监控现场、监控中心、远程查询三个子系统组成。系统的工作原理如下（见图 2）。

2.1　监控现场

监控现场子系统由三个组件组成。三个组件分别是图像采集、异常情况智能识别（以下简称识别）和网络传输。图像采集组件利用可用多个摄像机等图像采集设备采集多个监控现场图像数据，智能识别系统对现场图像数据进行分析识别并作出

基金项目：教育部与福建省和厦门市共建厦门大学"211 工程"基金资助（部级）编号：Y09001）
作者简介：缪克华，研究生，厦门大学计算机与信息工程学院自动化系。李茂青，教授，厦门大学计算机与信息工程学院付院长，自动化系主任。

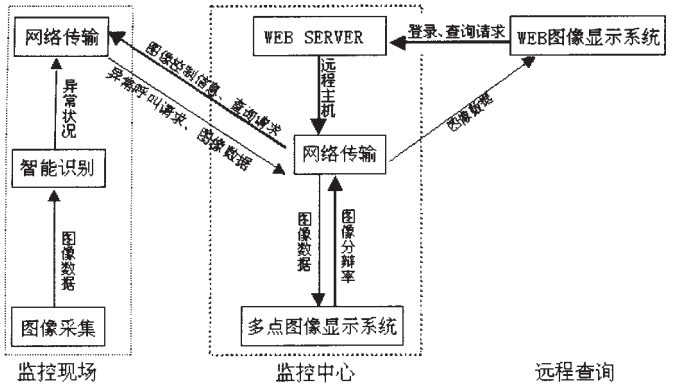

图 2　系统工作原理图

判断,如果发现有异常情况,网络传输组件利用电话线路通过 PPP 协议连接监控中心,建立网络连接后发送图像数据并接受监控中心的控制。另外网络传输系统还处于自动应答状态,能够接受监控中心的电话查询呼叫,并且自动建立网络连接,经核对查询者身份后,可发送现场图像数据并接受查询者的控制。

2.2　监控中心

监控中心子系统由三个组件组成:三个组件分别是 WEB SERVER、网络传输、多点图像显示。主要有两个方面的功能:(1)等待并接受监控现场的异常情况的呼叫,当收到监控现场有异常状况的电话呼叫,与呼叫主机自动建立网络连接。并且多点图像显示系统立即自动显示监控现场图像。监控中心工作人员观察监控现场实时图像,可以按实际要求改变监控现场图像的分辨率(分辨率与图像连续性成反比),根据现场的异常情况,可通知各职能部门或通知现场主人进行处理。(2)接受远程 INTERNET 用户查询,经核对远程查询用户身份后可通过电话线路与监控现场主机建立网络连接。这样监控现场主机与远程用户的查询主机之间能够借助监控中心建立网络连接。

2.3　远程查询系统

远程查询利用远程计算机通过 WEB 浏览器登录监控中心 WEB 服务器,经核对身份后通过监控中心建立与监控现场的网络连接,远程用户通过 WEB 查看监控现场的实时图像。

2.4　实际运作方式

在实际运作中监控中心可以以网站的形式存在,例如一个城市只需要一个提供这种服务的网站。监控现场可以设在各个企业单位、家庭、仓库等静态的现场中,用户在离开现场时把计算机设于监控状态,进入现场时解除监控状态。网站没有主动获取监控现场图像的权利,而只有在发生异常情况时才获取现场图像,另外用户通过 INTERNET 查询现场情况时,要通过现场计算机的身份认证才能接收到图像数据。这样用户的隐私权利也就得到了保护。

3　关键技术

通过以上的原理分析可以知道在整个系统中最关键的技术是互联网技术、图像的压缩技术和静态现场的异常情况的智能识别技术。以下就三个方面分别讨论。

3.1　互联网技术

从图 2 中可以看出为了实现实时图像数据以及实时控制信息的传输,必须在监控现场主机与监控中心之间、监控现场主机与远程查询主机之间必须建立一条稳定的数据流。Socket 解决了这样的问题。

3.1.1　Socket 简介

Sockets 是一种网络应用编程接口,它采用客户机/服务器的通讯机制,使网络客户机方和服务器方通过 socket 实现网络之间的连接和数据交换而不用考虑网络的具体协议。Socket 提供了一系列的系统调用,使用这些系统调用就可以实现网络通讯。为了实现通讯,客户机与服务器必须先定义三个属性:①网络地址。(TCP/IP 协议中即为 IP 地址)。②端口号(PostNumber):表示同一主机上的不同进程。③Socket 类型:分为流式套接口(StreamSocket)和数据报套接口(DatagramSocket)两种。具体地讲,IP 地址标识某一网络节点,而端口号标识此节点上的某一具体应用。Socket 类型确定数据交换形式,它有两种形式针对不同的应用。

(1)流式套接口:它是可靠的、双向的、顺序的、包长度不限的、非重复的面向连接的服务,适合于一次交换大量数据或需要可靠数据交换的应用。

(2)数据报套接口:它是不可靠但高效的无连接服务,一般应用在高可靠、低延迟的局域网上。主要用于一次交换少量数据(如网络对弈程序)或对数据传递可靠性和传递次序没有具体要求的应用。

3.1.2　具体应用

在实际应用中,在监控现场主机(设为 A)中预设了监控中心监控主机(B)网络地址和端口号。B 的指定的端口处于监听状态。当监控现场发生异常情况时,主机 A 自动与监控中心建立网络连接。接着 A 向 B 发送的含有 A 的网络地址的数据报。B 检测到后,B 和 A 各自建立流式套接口,两主机之间就可以建立可靠的、双向的、顺序的、包长度不限的连接。A 就可向 B 发送图像数据,B 接到数据后就可以在多点图像显示系统中显示出来。当然 B 不仅要与 A 连,而且要与所有发生异常情况的监控现场主机建立 Socket,这时只要在建立流式套接口时指定不同的端口号(PostNumber)就可以了。这样 B 的多点图像显示系统可以连续不断地显示多个监控点的图像。

与此类似,当远程查询者需要查询监控现场情况时,远程主机(设为 C)利用 WEB 浏览器登录监控中心网址,下载 WEB 图像显示系统(用 Java 编制的客户端程序)。用户核对身份后,监控中心利用电话线路建立与监控现场的网络连接。建立连接后 WEB SERVER 把监控现场主机 A 的网络地址和端口号送给 C,这样 C 和 A 之间就可以建立流式 Socket。A 可以实时地向 C 传送现场图像。

还有一种情况,当 B 与 A 连接时,C 同时需要查询,或监控中心的其它多台主机需要同时查看 A 的现场图像时,这时需要利用一种 IP 多播的技术(IP MULTICAST)。是指在互联网上对一组 IP 站点进行数据传送,这一组 IP 站点是动态形成的,每一站点都可以动态地加入或退出这个组。当某个 IP 站点向互联网中的多个 IP 站点发送同一数据时,多播可以减少不必要的重叠发送,与使用多次点对点的单播及广播相比,减轻了网络负载,提高了网络带宽的使用率及数据传输的实时性。所以只要把任何一个想查看现场图像的主机的网络地址加入到 A 的多播组中就行了,当然首先要经过身份认证。

3.2　静态现场异常情况的智能识别

对于安全监控而言,智能识别的目的是识别出可能的火灾和可能的非法闯入者。火灾图像识别的研究已经达到可以应用的程度了。对有非法闯入者的识别则采用密码和人形物体识别的方法来实现。下面分别讨论火灾识别和非法闯入者的识别。

3.2.1 火灾识别

3.2.1.1 早期火灾火焰的图象特性

(1)面积变化:早期火灾是着火后火灾不断发展的过程。在这个阶段,火灾火争的面积呈现连续的、扩展性的增加趋势。

(2)边缘变化:早期火灾火焰的边缘变化有一定的规律,同其它的高温物体及稳定火焰的边缘变化不同。

(3)形体变化:早期火灾火焰的形体变化反映了火焰在空间分布的变化。

(4)闪动规律:火焰的闪动规律,即亮度在空间的分布随时间变化的规律,火焰在燃烧过程中会按某种频率闪烁。

(5)分层变化:火焰内部的温度是不均匀的,并且表现出一定的规律。

(6)整体移动:早期火灾火焰是不断发展的火焰,随着旧的燃烧物燃尽和新的燃烧物被点燃,火焰不断移动着位置。所以火焰的整体移动是连续的、非跳跃性的。

3.2.1.2 火灾识别步骤

在火灾图像探测方法中,对每一帧图象做以下操作:(1)对图象上的每个目标,根据一定的算法来判断他们同前一帧中目标的匹配关系,从而得到各个目标的连续变化规律。(2)提取本帧图象的特征信息。即提取如上所述的面积、边缘等信息。(3)以采用一定算法对最近几帧图象的特征信息进行综合处理,最后得出有火灾发生的概率。

3.2.1.3 火灾 BP 神经网络探测算法

中国科学技术大学火灾科学国家重点实验室提出一种基于 BP 神经网络算法对图象的特征信息进行综合处理。效果如下:在一个尺度为 3m(宽)×4.5m(高)的空间中进行的,摄象机安装在空间的顶部,向下俯瞰探测区。当火焰距离为 10m 时,对所有实验样本都在 10 秒以内给出了准确判断,没有发生误报现象。当火焰距离为 30m 时,实验样本的准确判断为 80%。因而完全符合静态现场火灾监控的要求。

3.2.2 非法闯入者的识别

3.2.2.1 人脸识别研究的现状

当然对是否为非法闯入者的识别的最好方法是人脸的识别,也就是每一个进入监控现场的人,都要经过人脸识别系统的识别。人脸识别是目前非常活跃的研究领域,在识别效果的准确率、容错性和健壮性等方面取得了一定的进展。但是现今人脸识别系统的缺点是:(1)系统必须具备大容量的人脸数据库;(2)增加识别对象时要重新训练整个系统;(3)系统需求硬件平台较高;(4)单纯从图像无法对真假人脸的识别。因而对于本监控系统采取了人形物体的识别和密码相结合的手段。

3.2.2.2 人形物体的识别

相对于人脸的识别,人形物体的识别的识别率要高的多,而且算法简单。有点类似于手写字体机器识别。而人体的头肩部的特征是相当明显。算法非常多,限于篇幅,就不在此陈述了。

3.2.2.3 识别过程

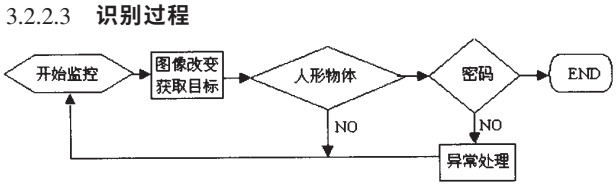

图 3 识别过程

3.3 低速线路图像传输技术

3.3.1 静态监控现场图象信号的特点

(1)静态监控现场电视整体图象变化小,帧相关性极大。可以将整屏监控现场图像划分为 2 个区域:背景区、运动物体运动区。摄像头一般安装在固定地点,照明灯光一般不变,帧与帧背景区的数据基本相同。因此背景区只要传输一次。

(2)视频图象信号中的细节、灰度及运动等 3 个分辨率参数之间实质上是相互依赖的。考虑到监控的目的主要是防火与防盗。当出现火警时,监控者需要看清的是细节和灰度,而不大需要火的运动。当出现闯入者时监控者需要看清的是细节和动作不大考虑灰度。因此可以根据相应的情况,采用分辨率参数来降低编码率。

(3)只对传输图像,不传输声音。

3.3.2 极低码速率的压缩技术研究现状

在多媒体系统中常用的 3 个图像处理标准是:

(1)JPEG 标准(ISOCD 10918)适用于连续色调静止图象的数字压缩编码;可以按要求实现不同的压缩率。

(2)MPEG 标准(ISO/IEC 11172),适用于数字存储媒体上活动图象及其伴音的压缩编码;适用于传输率在 1-10M 的广播级图像。

(3)CCITTH.261、H.263 标准,适用于可视电话和会议电视等应用系统中的数字压缩编码。

适应于普通模拟电话网上的 64kbps 以下的可视电话。

虽然 JPEG 标准起初是为静止图像而设立,但它也被一些视频和多媒体系统采用并取得了相当好的效果,它已逐步演化成为一种非正式标准-运动 JPEG(M- JPEG)。在某些方面它比 MPEG 系统性能低一些,但它有自己的优点,系统成本低、结构简单、压缩率可灵活改变。

3.3.3 系统采取的图像压缩传输策略

根据以上的情况分析,系统采用下述策略:(1)采用标准的 NTSC 制式信号分辨率 320*240。(2)采用 M-JPEG 压缩技术。(3)根据现场发生异常具体的情况,当判断为火警时采用 16 位灰度,当判断为有闯入者时应用 8 位灰度。(4)只传送运动物体区的图像。5、监控者可按要求改变图像的压缩率以改变图像的连续性。经过以上策略可以看看下列试验结果:

这是在一个人从镜头 7 米远处走到镜头 2 米处 3.30 秒钟的片段。第一为背景图全部传输。其余的只传输运动目标(白线内的部分)。

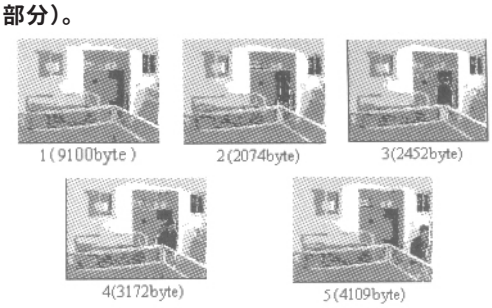

图 4

从以上可以看出当运动目标占据整个图像的面积较大时,所要传送的字节也相对增高,这样会导致图像传输的不稳定,时快时慢。但是不会低于 1 帧/2 秒(100/5K),实验表明一般为 1.5 帧/秒。(以上数据以 56.6K 的 MODEM 计算)。

4 结束语

上面从四个方面阐述了一种构造基于静态现场的实时监控系统的方法，它有智能型的、远程分布式的优点。但是这个系统也还存在有不足之处，如图像的连续性还不够稳定、另外监控现场通过 MODEM 与监控中心建立网络连接的过程需要一定的时间，这对于安全监控是非常不利的。但是随着 ISDN 电话线路的推广，这些不足之处就会得到大大的改善。

（收稿日期：2002 年 1 月）

参考文献

1.宋卫国等.基于人工神经网络的火灾图象探测方法[J].火灾科学，1999；8(3)

2.[美]BONNERP.Network Programming with WindowsSockets[M].New-Jersey，Prentice Hall，1996

3.马小虎.多媒体数据压缩标准及实现[M].北京：清华大学出版社，1996：119~171

（上接 186 页）

中，增加一个外挂第三方厂商杀毒软件的功能，利用专业杀毒软件对缓存进行查毒、杀毒。杀毒软件处于实时监控状态，一有新的文件进入缓存，就用杀毒软件查杀病毒。之所以用外挂第三方杀毒软件的方法，是因为专业杀毒软件厂商能及时提供升级服务，并且可以外挂多个杀毒软件，以提高可靠性。目前杀毒软件也可以查杀木马程序，但对于网页中有害的 Applet 代码还无能为力。因此，对网页中有“document.applets”等语句时，发给用户一个警告信息，由用户决定是否执行。

4.2 邮件服务器

前文已谈到，目前邮件病毒泛滥，其危害程度已经大超过传统的病毒。但用户接收邮件使用的是 POP3 协议，而 POP3 协议需要使用套接字服务器（Sockets Server）进行代理。这需要修改客户的底层协议文件。普通的 POP3 协议在一个给定的端口上进行通信，而不是与具体的 IP 地址通信。而使用套接字服务器进行代理后，客户机将代理服务器看作最终目的地，而由代理服务器与原来请求的目的地进行对话，并把邮件转发给客户。完整的 Email 系统由收集报文的输出队列，客户处理，服务器处理以及接收邮件的邮箱组成。每封 Email 报文由邮件体和邮件头两部分组成，邮件头包含了邮件的发送者、接收者、时间以及其它完成 Email 传递所需的各种信息。邮件由用户用 SMTP 协议发到本地邮件服务器，在经过一系列邮件服务器之后，到达接收方本地的邮件服务器，最后接收者用邮局协议（POP 协议）从其邮箱中取出邮件。因此在所设计的改进型应用网关防火墙中增加一个邮件网关，由防火墙作内部网邮件的接收者，一旦因特网的邮件服务器建立了一条到防火墙的连接，防火墙就在同一个端口上建立一条与内部网客户的连接。客户端通过监听防火墙 IP 地址有无一条返回连接，让防火墙知道它正等待一条返回连接。此时，防火墙建立虚拟邮件服务器将 Email 接收到邮件网关上，同样经过外挂第三方杀毒软件对邮件进行处理后，再通过防火墙同客户端的连接将邮件分发给用户（如图 2）。在这一过程中，修改过的客户端 Sockets 程序能区分是否是本地的 Email 请求，并还需要考虑邮件的保密性的问题。

在应用网关防火墙中针对不同的应用而增加专用目的代码，看起来有些浪费，但却比任何其他方法安全得多，也简便得多。一则不必担心不同过滤策略之间的交互影响，另一方面不必担心内部网数百台主机防病毒能力的不一致性而带来的危害。同时这种改进的应用网关还有另一个优点，可以进行双向代理。不但可以制定“进”的访问策略，还可以制定“出”的策略。可以制定检查发出的邮件和上传的文件的规则，检查文件是否包含有公司的程序或数据，从而防止公司内有价值的程序和数据被盗。

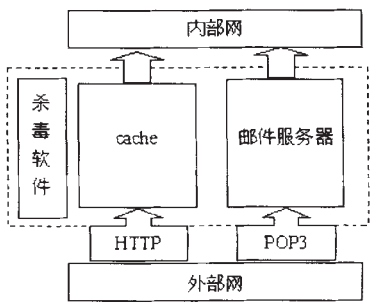

图 2 改进的应用网关

5 结束语

该文针对传统防火墙的不足，提出了在防火墙上增加虚拟邮件服务器，并且将第三方杀毒软件与防火墙紧密结合起来抵御邮件病毒的方案。但是杀毒软件是属于被动式的安全措施，总是当病毒流行后，才出现相应的杀毒软件。因此，提高网络的安全性，除使用防火墙技术外，还应综合使用其它安全技术。该文提出的改进的应用网关，对较大的网络访问量会产生延迟，使用户感觉访问网络变慢，这可以通过提高服务器性能和增加网络带宽来解决。

目前，整体的安全集中在网络的边缘上，坚固的外表与柔弱的中央是一种普遍存在的现象。坚固的外表是防火墙，虚拟专用网，虚拟局域网等将网络分隔的方法。而内部的安全管理则令人担忧。一个长期不改变，简短易猜的超级用户口令，无论口令认证机制如何安全，都无济于事。因此，制定一整套完善的安全策略，并严格地执行它，才能最终达到系统的整体安全。

（收稿日期：2002 年 1 月）

参考文献

1.宋书民，朱智强，徐开勇等译.防火墙技术指南[M].北京：机械工业出版社，2000

2.刘克龙，蒙杨，卿斯汉.一种新型的防火墙系统[J].计算机学报，2000；(3)：231~236

3.谢琳，胡刚，沈雁.一个安全邮件系统的设计与实现[J].计算机工程与科学，2000；(1)：48~51

4.前导工作室译.网络安全技术内幕[M].北京：机械工业出版社，1999

5.原菁，卿斯汉.基于安全数据结构的防火墙[J].计算机科学，2001；(6)：56~59