Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.8, 2013

Remote Surveillance System for Mobile Application

Sonali M. Diware
Dept. of Computer Engineering, Maharashtra Academy of Engineering, Alandi (D), Pune
E-mail: sonali.diware@gmail.com
Shweta A. Iskande
Dept. of Computer Engineering, Maharashtra Academy of Engineering, Alandi (D), Pune
E-mail: shweta.iskande@gmail.com

Abstract
Remote video surveillance is the use of cameras and other surveillance equipment to monitor properties and assets from a separate location. It is often used as a force multiplier or asset protection device for areas where it is not possible, practical, or affordable to install a cable network. It is commonly deployed in city and campus applications, or any place where it is difficult to monitor the surroundings using common means. Remote surveillance is a great opportunity to use wireless technologies for connectivity due to the flexibility they provide. A video surveillance system is only as reliable as the network it is connected to, so careful planning of the network technologies and equipment choices are crucial.
Keywords: camera control, change detection, computer vision, image processing, video surveillance.

1.Introduction

Security in residential complexes is restricted to limited geographical locations. Reason for this is the traditional devices and process used for securing any apartment or complexes. The on demand video surveillance and video capturing are accessed in a limited location from a central setup for surveillance. Users cannot afford to buy expensive surveillance devices for their personal use as they are expensive and need high setup and connections. It is difficult to keep a watch on security from different remote locations. As it need standard platform to access surveillance devices and secure connection protocol. This prevents the user for keeping a watch on security location from any remote place via a standard platform of accessing remote surveillance device. Today software is the most expensive element of virtually all computer-based systems. Software project estimates can be transformed from a black art of a series of systematic steps that provide estimate with acceptable risk. Lines of code and function point data are used in two ways doing software project estimation.
1.As an estimation variable to size each element of the software and,
2. As base line matrices collected from past projects and used in conjunction with estimation variable to develop cost and effort estimation.

2. Problem Definition

The mechanism for accessing surveillance devices should be capable of accessing devices from any remote location. This would allow user to keep a watch on security location from any remote location. The communication and the platform needed to access surveillance devices should be standard channel and device. The communicating and accessing device should be fully based on software. This will make easy for user to control and access surveillance devices. Accounts for all users should be maintained. This will make proper utilization of communication bandwidth using standard software based platform. This allows user to access surveillance devices from a standard user friendly platform like web portal or mobile devices.

3.Major Performance Objective

3.1 Video Streaming with High Bandwidth

Bandwidth is a key performance measure of remote communication. It defines how many bits can be transmitted every second, which means the more bandwidth available, the more data can be sent in a given period of time.Remote Surveillance Via Mobile uses IP networks that have the flexibility to allocate bandwidth as needed and reserve the unallocated bandwidth for other data using RTS protocol.

3.2 . Accessing Surveillance Device functions from remote location

Many of the function related to surveillance device like changing position of security camera's etc can be performed via remote procedure calls using data streaming between client and the server. It helps executing different functions of surveillance devices from remote location.

3.3. Compression of Capture Image

To achieve high communication speed and delay of frames in mobile devices, the image capture by the surveillance device is compressed to reduce the size of the image then it is send to mobile device via internet. This prevents of frame lagging and delay in communication.

3.4. Advanced Features

Through Remote surveillance we intend to spread security watch setups in a wider location. This will also make use of software based watch instead of using hardware. This will make user more comfortable to interact with the system. The software provides a bridge of communication between remote devices like mobile and web portal with the surveillance devices. The software will not perform communication between two remote devices or two desktop applications. The mobile application software will perform the task of connecting the wireless device with the server to get live video feeds. This will help user to keep a watch on security from remote place. The desktop application will perform interfacing with the surveillance devices and perform the task of transmitting video feeds to the web server. This will help user to get access to the surveillance device using software. User Database will perform the task of authentication of user accounts. This will help the system to marinating bandwidth of different users.

4. Literature Survey

Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people and often in a surreptitious manner. It most usually refers to observation of individuals or groups by government organization, but disease surveillance for example, is monitoring the progress in a disease in a community. The word *surveillance* comes from the French word for "watching over". The word *surveillance* may be applied to observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls). It may also refer to simple, relatively no- or low-technology methods such as human intelligence agents and postal interception. Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program and ADVISE, technologies such as high speed surveillance computers and biometric software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of their subjects. However, many civil rights and privacy groups such as the electronic frontier foundation and ACLU have expressed concern that by allowing continual increases in government surveillance of citizens that we will end up in a mass surveillance society, with extremely limited, or non-existent political and/or personal freedoms. Fears such as this have led to numerous lawsuits such as AT&T.

4.1. Existing System

4.1.1. *WiLife Digital Video Surveillance System*:

It is a wireless security system in a security location. The main advantage of wireless system is the hardware for connection is absent. The feeds from the security devices or cameras are capture at the central location. The surveillance devices are wireless and make use of radio transmitter. Radio transmitter are limited in scope and they cannot be extend to wider locations

4.1.2. 2M CCTV Video Surveillance System:

This is a traditional surveillance system where CC-TV is connected with the central monitoring device through cables. The captured imaged is examined by the central monitoring device.

4.1.3.Extreme Surveillance System:

This system uses smart chip based surveillance devices which are capable of interfacing directly with the computer through RS-232 cable. These systems have software GUI which controls the surveillance device.

5.Type of surveillance

5.1. Computer surveillance

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the united states for example under the communication Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies. There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups. Billions of dollars per year are spent, by agencies such as the Information Awareness Office, NSA, and the FBI, to develop, purchase, implement, and operate systems such as Carnivore, NarusInsight and ECHELON to intercept and analyze all of this data, and extract only the information which is useful to law enforcement and intelligence agencies. Computers are also a surveillance target because of the personal data stored on them. If someone is able to install software (either physically or remotely), such as the FBI's "Magic Lantern" and CIPAV, on a computer system, they can easily gain

unauthorized access to this data. Another form of computer surveillance, known as TEMPEST, involves reading electromagnetic emanations from computing devices in order to extract data from them at distances of hundreds of meters. The NSA also runs a database known as "Pinwale", which stores and indexes large numbers of emails of both American citizens and foreigners.

5.2. Telephones and mobile telephones

The official and unofficial tapping of telephone lines is widespread. In the United States for instance, the Communications Assistance for Law Enforcement Act (CALEA) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies. Two major telecommunications companies in the U.S. -- AT&T and Verizon—have contracts with the FBI, requiring them to keep their phone call records easily searchable and accessible for Federal agencies, in return for $1.8 million dollars per year. Between 2003 and 2005, the FBI sent out more than 140,000 "National Security Letters" ordering phone companies to hand over information about their customers' calling and Internet histories. About half of these letters requested information on U.S. citizens. Human agents are not required to monitor most calls. Speech-to-text software creates machine- readable text from intercepted audio, which is then processed by automated call-analysis programs, such as those developed by agencies such as the Information Awareness Office, or companies such as Verint , and Narus , which search for certain words or phrases, to decide whether to dedicate a human agent to the call. Law enforcement and intelligence services in the U.K. and the United States possess technology to remotely activate the microphones in cell phones, by accessing the phone's diagnostic/maintenance features, in order to listen to conversations that take place nearby the person who holds the phone.

Mobile phones are also commonly used to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily (whether it is being used or not), using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. A controversy has emerged in the United States over the legality of such techniques, and particularly whether a court warrant is required. Records for *one* carrier alone (Sprint), showed that in a given year federal law enforcement agencies requested customer location data 8 million times.

5.3 . Surveillance cameras

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device, IP network, and/or watched by a security guard/law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage. Now with cheaper production techniques, it is simple and inexpensive enough to be used in home security systems, and for everyday surveillance. Analysis of footage is made easier by automated software that organizes digital video footage into a searchable database, and by automated video analysis software's. The amount of footage is also drastically reduced by motion sensors which only record when motion is detected.

Figure 1. CCTV Camera.

Surveillance cameras such as these are installed by the millions in many countries, and are nowadays monitored by automated computer programs instead of humans. The use of surveillance cameras by governments and businesses has dramatically increased over the last 10 years. In the U.K., for example, there are about 4.2 million surveillance cameras—1 camera for every 14 people.

In the United States, the Department of Homeland Security gives billions of dollars per year in Homeland Security grants for local, state, and federal agencies to install modern video surveillance equipment. For example, the city of Chicago, IL recently used a $5.1 million Homeland Security grant to install an additional 250 surveillance cameras, and connect them to a centralized monitoring center, along with its preexisting network of over 2000 cameras in a program known as Operation Virtual Shield. Chicago Mayor Richard Daley stated that Chicago will have a surveillance camera on every street corner by the year 2016.

As part of China's Golden Shield Project, several U.S. corporations such as IBM, General Electric, and Honeywell have been working closely with the Chinese government to install millions of surveillance cameras throughout China, along with advanced video analytics and facial recognition software, which will identify and track individuals everywhere they go. They will be connected to a centralized database and monitoring station, which will, upon completion of the project, contain a picture of the face of every person in China: over 1.3 billion people. Lin Jiang Huai, the head of China's "Information Security Technology" office (which is in charge of the project), credits the surveillance systems in the United States and the U.K. as the inspiration for what he is doing with the Golden Shield project.

The Defense Advanced Research Projects Agency (DARPA) is funding a research project called Combat Zones That See that will link up cameras across a city to a centralized monitoring station, identify and track individuals and vehicles as they move through the city, and report "suspicious" activity (such as waving arms, looking side-to-side, standing in a group, etc).[33]

At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida, used Identix's facial recognition software, FaceIt, to scan the crowd for potential criminals and terrorists in attendance at the event.[34] (it found 19 people with pending arrest warrants)[35]

Governments often initially claim that cameras are meant to be used for traffic control, but many of them end up using them for general surveillance. For example, Washington, D.C. had 5000 "traffic" cameras installed under this premise, and then after they were all in place, networked them all together and then granted access to the Metropolitan Police Department, so that they could perform "day-to-day monitoring".[36]

The development of centralized networks of CCTV cameras watching public areas—linked to computer databases of people's pictures and identity (biometric data), able to track peoples' movements throughout the city, and identify who they have been with—has been argued by some to present a risk to civil liberties.[37]

5.4. Biometric surveillance

Biometric surveillance refers to technologies that measure and analyze human physical and/or behavioral characteristics for authentication, identification, or screening purposes. Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioral characteristics include gait (a person's manner of walking) or voice.

Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video. Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems. The Information Processing Technology Office ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft by their facial features.

Another form of behavioral biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioral traits. This might be used for instance to see if a person is acting "suspicious" (looking around furtively, "tense" or "angry" facial expressions, waving arms, etc.)

A more recent development is DNA fingerprinting, which looks at some of the major markers in the body's DNA to produce a match. The FBI is currently spending $1 billion to build a new biometric database, which will store DNA, facial recognition data, iris/retina (eye) data, fingerprints, palm prints, and other biometric data of people living in the United States. The computers running the database will be contained in an underground facility is about the size of a football field. The Los Angeles Police Department is currently installing automated facial recognition and license plate recognition devices in its squad cars, and providing handheld face scanners, which officers will use to identify people while on patrol.

Facial thermographs are currently in development, which allow machines to identify certain emotions in people such as fear or stress, by measuring the temperature generated by blood flow to different parts of their face. Law enforcement officers believe that this has potential for them to identify when a suspect is nervous, which might indicate that they are hiding something, lying, or worried about something.

5.5. Aerial surveillance

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle—such as a unmanned aerial vehicle, helicopter, or spy plane. Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper, a U.S. drone plane currently used for domestic operations by the Department of Homeland Security, carries cameras that are capable of identifying an object the size of a milk carton from altitudes of 60,000 feet, and has forward-looking infrared devices that can detect the heat from a human body at distances of up to 60 kilometers.

Figure 2. HART program concept drawing from official IPTO (DARPA) official website.

The United States Department of Homeland Security is in the process of testing UAVs to patrol the skies over the United States for the purposes of critical infrastructure protection, border patrol, "transit monitoring", and general surveillance of the U.S. population Miami-Dade police department ran tests with a vertical take-off and landing UAV from Honeywell, which is planned to be used in SWAT operations Houston's police department has been testing fixed-wing UAVs for use in "traffic control"

The U.K., as well, is currently working on plans to build up a fleet of surveillance UAVs ranging from micro-aerial vehicles to full-size drones, to be used by police forces throughout the U.K. In addition to their surveillance capabilities, MAVs are capable of carrying tasers for "crowd control", or weapons for killing enemy combatants. Programs such as the Heterogenous Aerial Reconnaissance Team program developed by DARPA have automated much of the aerial surveillance process. They have developed systems consisting of large teams drone planes that pilot themselves automatically decide who is "suspicious" and how to go about monitoring them, coordinate their activities with other drones nearby, and notify human operators if something suspicious is occurring. This greatly increases the amount of area that can be continuously monitored, while reducing the number of human operators required. Thus a swarm of automated, self-directing drones can automatically patrol a city and track suspicious individuals, reporting their activities back to a centralized monitoring station.

6.Proposed System Architecture

The architecture being used for this software is the Two Tier Architecture. In Two Tier Architecture, the client machine acts as a front end communicates with an application server. The application server in turn manipulates data with help of admin to access data. The business logic of the application, which says what actions to carry out under what condition, is embedded in the application server, instead of being distributed across multiple clients. Two tier applications are appropriate for large as well as small application, and for application that run on the World Wide Web.

Figure 3.Proposed system architecture.

6.1. Outdoor and Mobile Video Surveillance

*6.1.1.*Data Storage:

As today's security issues grow more complex, surveillance concerns often extend beyond closed doors and well into public spaces. To combat such evolving threats, outdoor and mobile surveillance has become a key element of comprehensive security solutions. While mobile surveillance is rapidly gaining prominence as an effective surveillance tool among specialist industries, such as law enforcement and the military, outdoor surveillance has become increasingly important in safeguarding public and organizational interests. These diverse video surveillance environments highlight the growing importance of HDDs, which enable vast quantities of critical video data to be stored efficiently, reliably and securely.

6.1.2. Advantages of HDD Technology

In Surveillance HDDs are a superior repository for video data compared to traditional media, such as videotapes, which are often plagued by hardware-based issues, such as generation loss and incompatibility with newer camera models. In addition, HDD-based video surveillance systems enable a broad range of functionalities not available with analog media.

6.1.3. Client/server architecture
Users can issue a variety of remote demands, permitting more than one client to view and control cameras simultaneously and more than one process to access data for more than one purpose, such as automatic remote archiving, searching and/or exporting data.
6.1.4. Data archiving
Data storage can be automated and distributed, enabling both public and private enterprises to utilize centralized data elements for security, control and convenience.
6.1.5. Easy integration
Quality digital video images streamed from high-definition cameras are easy to integrate with post-processing applications, such as facial recognition and object tracking.
6.1.6. Flexible controls for secure user-level access
Administrators can establish flexible controls for secure user-level access throughout an organization.
6.1.7. Image exporting
HDD-based surveillance systems can easily and securely transfer segments of video data for evidentiary purposes, training programs, or post-evaluation and reporting.
6.1.8. Higher image quality
Full-frame, high-resolution images delivered by modern high-end cameras are seamlessly archived on HDDs, enabling easy image viewing and authentication.
6.1.9. Plug and play on any network
All networked video servers can achieve plug-and-play status on any network using TCP/IP addresses; multiple cameras simply become addressable devices on an IP number.
6.1.10. Remote diagnostics and access
HDD-based video servers enable network assets to be remotely managed with network management software.
6.1.11. Smart search
HDD-equipped surveillance systems facilitate pixel-based searching of digital video, enabling an operator to highlight an area of interest with a camera view and search for pixel variations; such searches are completed in mere seconds. Video images are time- and date-stamped and can be accessed, replayed or copied with no detail loss. The multitude of additional functionalities enabled by HDD-based video surveillance systems translates into significant benefits, such as enhanced ease of use, greater flexibility and robust data security previously unavailable in the video surveillance industry. In addition, the combination of sophisticated high-definition cameras and HDD storage enables crisp, clear images that are valuable in various applications ranging from court evidence to forensics detailing.

7.Application
7.1. Security Applications
Application security encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application. Applications only control the use of resources granted to them, and not *which* resources are granted to them. They, in turn, determine the use of these resources by users of the application through application security.
7.2. iPhone surveillance system
CCTV Camera Pros sells iPhone surveillance system and iPhone compatible security cameras. All of the systems and security cameras are compatible with the Apple iPhone for remote camera viewing.
7.3. Audio in video surveillance system
While the use of audio in video surveillance systems is still not widespread, having audio can enhance a system's ability to detect and interpret events, as well as enable audio communication over an IP network.

References
P. R. Wolf and B. A. Dewitt, *Elements of Photogrammetry with Applications in GIS*, 3rd ed. New York: McGraw Hill, 2000.
P. Burt, P. Anandan, G. van der Wal, and R. Bassman, "A front-end vision processor for vehicle navigation," in *Proc. Int. Conf. Intelligent Autonomous Systems*, 1993.
P. Burt and E. Adelson, "The Laplacian pyramid as a compact image code," *IEEE Trans. Commun.*, vol. COM-31, pp. 532–540, Apr. 1983.
W. Freeman and E. Adelson, "The design and use of steerable filters," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 13, pp. 891–906, Sept. 1991.