Benemérita
Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

"IPCAM-CONNECTOR: Una componente para interactuar con una cámara IP"

Tesis Profesional

Que para obtener el título de:
Ingeniero en Ciencias de la Computación

Presenta

Benjamín Elías Sánchez Bonilla

Asesores

Dr. Manuel Martín Ortíz
Dr. Abraham Sánchez López

Otoño 2007

Resumen

En este documento se describe el desarrollo de una componente el cual nos da a los programadores la facilidad de interactuar con una cámara IP, esto quiere decir, poder realizar con facilidad una conexión y obtención de imágenes de la cámara. Por el momento sólo podrá ser usado para la línea de cámaras de Intellinet debido a que cada fabricante diseña de distinta forma sus cámaras.

Se explica una aplicación (Java Applet) usando la componente, dicha aplicación muestra las imágenes en forma de video, permite cambiar el tamaño de las imágenes, ver los frames por segundo en la transmisión, se puede cambiar de cámara proporcionando en la aplicación la dirección IP y puerto además de poder crear un video con formato **MOV** el cual puede ser reproducido en QuickTime, por último una interfaz la cual nos permite aplicar el filtro de negativo, como ejemplo (de la misma manera se pueden implementar otros filtros), sobre una imagen obtenida de la cámara.

La componente fue programada en Java bajo Windows Server 2003 utilizando un IDE de desarrollo NetBeans 3.5 para la interfaz gráfica (Applet) y JCreator 3.0 LE para el desarrollo del componente. La máquina en que se desarrolló y probó este componente fue en un Servidor Intel Xeon Dual de 2.8GHz, 1GB de memoria en RAM 1 tarjeta de video e-GeForce con 128 MB de memoria. La aplicación fue probada en la misma máquina así como en otras de características más pobres, la eficiencia de este componente depende de la conexión a Internet que se tenga si se desea probar a una distancia fuera del rango de la ubicación donde se encuentre.

INDICE

Planteamiento del Problema

El problema consiste en desarrollar un componente que permita al programador realizar una conexión a una cámara IP y a su vez obtener datos los cuales podrán ser usados para convertirlos a imágenes con formato JPG o GIF.

La idea es que con ayuda de este componente se pueda desarrollar un sistema como puede ser de monitoreo o de vigilancia sin que haya dificultad en usar una cámara IP.

Objetivo General

El objetivo general de este proyecto es crear un componente el cual permita una conexión y obtención de una imagen de una cámara IP.

Objetivo Específico

El objetivo específico es la construcción de una interfaz gráfica con el cual mostrar el funcionamiento de nuestro componente y así poder mostrar video desde una aplicación Java o una aplicación Web.

Capítulo I

El Video y sus Aplicaciones

Capítulo I. El Video y sus Aplicaciones

1.1 Introducción

Los negocios actuales, tanto los de las grandes como los de las pequeñas empresas, precisan facilidad de operación así como sistemas ajustados para la vigilancia de seguridad o la monitorización de procesos de producción, y aplicaciones avanzadas como la monitorización de la calidad de servicio y las transacciones del punto de venta. Estas empresas exigen más a sus sistemas de CCTV (circuito cerrado de TV): integración del equipamiento existente como cámaras analógicas, almacenamiento seguro, y la capacidad de monitorizar y gestionar sus sistemas en cualquier momento y desde cualquier lugar.

Desde la introducción de los sistemas de vídeo vigilancia analógicos a principios de los años 70, las ventas de sistemas de CCTV para ayudar en la investigación criminal y de seguridad han ido aumentando año tras año. En 2001, los ingresos del mercado de aplicaciones basadas en CCTV alcanzó los 4.700 millones de dólares según datos de Frost & Sullivan [1].

Según los datos de informes de la compañía de análisis de mercado J.P. Freeman and Co., hay más de 20 millones de cámaras analógicas instaladas sólo en los Estados Unidos. De estos 20 millones 1,5 millones de cámaras fueron vendidas en 2002. A pesar de estas impresionantes cifras de las cámaras analógicas, las cámaras de red han emergido como la categoría de producto de más rápido crecimiento, lo que indica claramente que los sistemas basados en IP están condenados a perdurar. Las cámaras de red se conectan directamente a una red IP y se integran en aplicaciones sobre la red, permitiendo a los usuarios tener cámaras en lugares remotos y visualizar, almacenar y analizar vídeo en directo de otra localización, o de múltiples localizaciones sobre la red o Internet. Las cámaras de red se prevé que representen más de la mitad del mercado de cámaras de seguridad en 2007.

A la vez que se está estableciendo la monitorización del vídeo para un puente o se está creando un sistema de vigilancia para la zona de estacionamiento de vehículos de la empresa, una solución emergente es la integración de los actuales sistemas de Vigilancia IP con la tecnología de redes inalámbricas.

Dada su escalabilidad, entre otras ventajas, la tecnología de Vigilancia IP está bien establecida no sólo para mejorar o revitalizar aplicaciones de vigilancia y monitorizaciones remotas existentes, sino también para un mayor número de aplicaciones. Y cuando añadimos la potencia de la transmisión inalámbrica a la Vigilancia IP creamos incluso una solución más robusta: Un cable Ethernet (conexión de red) que puede conectar fácilmente cámaras de red a una solución de conectividad punto-a-multipunto, creando instantáneamente una WAN (red de área extensa) inalámbrica capaz de transmitir vídeo de alta resolución a una estación base en tiempo real. La combinación de la Vigilancia IP con la tecnología Inalámbrica crea una aplicación de seguridad que va más allá que cualquiera de las tecnologías disponibles y proporciona además las siguientes características:

- Fácil de desplegar
- Alto grado de funcionalidad
- Proporciona ahorros en instalación y operación
- Totalmente escalable

Tanto si hay cámaras analógicas como digitales o una combinación de ambas, la Vigilancia IP inalámbrica ha demostrado ser atractiva para una amplia cantidad de aplicaciones como pueden ser:

1.2 Conteo de personas

En un comercio podría haber un dispositivo de vídeo IP instalado en cada una de las entradas del establecimiento.

Los dispositivos de vídeo IP pueden disponer de un módulo de recuento de personas que permite grabar el número de personas que pasan por cada puerta directamente en una unidad de negocios central. Cada uno de los dispositivos ofrece una visión de los expositores de puntos de venta. Las cámaras IP pueden activarse ante un movimiento y transmitirán ese vídeo a una unidad central y a un operador de vídeo inteligente que analizará los 'tiempos de permanencia'. Un hervidero de gente haciendo compras, en combinación con unos tiempos de permanencia largos, muestran una imagen del óptimo resultado de los expositores. Finalmente, esta información mejora la rentabilidad general del comercio.

Otras cuestiones importantes del comercio son: "¿En qué momento el nivel de las colas empieza a influir en la experiencia del cliente? ¿Hay una cola que va más rápida de lo esperado? ¿Se crea un clima de frustración ante una nueva disposición en el comercio?"

Por lo tanto, los sistemas de vídeo IP pueden lograr múltiples objetivos: para fines de inteligencia comercial, al ayudar a los minoristas a aumentar las ventas y la rentabilidad mediante el análisis del comportamiento de los clientes, mejorar la experiencia del cliente mediante el análisis de los tiempos de espera en la cola y observar las reacciones de los clientes que están haciendo cola, y ayudar a tomar decisiones para abrir nuevas cajas cuando los tiempos de espera en la cola alcanzan niveles que empiezan a arruinar la experiencia del cliente.

Figura 1.1 Sistema de Video IP

1.3 Reconocimiento de matrículas

El aparcamiento inteligente es una aplicación eficaz basada en el reconocimiento de matrículas. Puede resultar un problema que los clientes pierdan sus tickets de aparcamiento a largo plazo y pregunten a la administración sobre esta determinada plaza de aparcamiento. Se pierde mucho tiempo y energía en encontrar la tarifa correcta. El nuevo sistema ofrece una facturación mensual y unos tickets de aparcamiento que no generan dudas.

Otro problema es el uso de plazas de aparcamiento donde se dejan los vehículos robados hasta que se reduzca la intensidad de su búsqueda. Las autoridades policiales están muy satisfechas con los nuevos guardianes inteligentes que graban las horas de entrada y ofrecen estadísticas de los coches que están aparcados en cada plaza de aparcamiento. Esto evita depositar coches robados en otras ubicaciones de la ciudad así como intentar forzar las cerraduras de los coches aparcados en un "edificio inteligente". La aplicación del vídeo inteligente logra múltiples objetivos. Los propietarios de los coches, las autoridades y la administración de los aparcamientos salen ganando con esta aplicación.

1.4 Defensa o un sistema de detección de intrusiones

La aplicación del sistema de detección de intrusiones evita que se produzcan intentos de robo con pocos guardias de seguridad de servicio. Esta aplicación está diseñada para ofrecer una línea o líneas virtuales, restringiendo el paso en una dirección determinada. Dicho de otra manera, los empleados o el personal de seguridad pueden salir de un edificio, pero no pueden volver a entrar sin consultar el administrador de alarmas.

La adaptación de los sistemas de detección de intrusiones ofrece un sinfín de posibilidades. Esto significa que los sistemas de vídeo inteligente pueden configurar los sistemas de vigilancia para que sólo puedan recopilar datos de vídeo cuando existan determinados parámetros y al detectar movimientos anormales. El punto clave reside en

que los sistemas pueden configurarse para ofrecer una información más específica y focalizada.

1.5 Seguridad y Vigilancia

Las cámaras de red se usan en sistemas de seguridad profesionales y permiten vídeo en directo para que sea visualizado por personal autorizado. Las cámaras de red se integran fácilmente en sistemas mayores y más complejos, pero también pueden funcionar como soluciones aisladas en aplicaciones de vigilancia de bajo nivel.

- Las cámaras de red pueden usarse para vigilar áreas sensibles como pueden ser edificios, casinos, bancos y tiendas. Las imágenes en vídeo de estas áreas pueden ser monitorizadas desde salas de control, dependencias policiales y/o por directores de seguridad desde diferentes localizaciones.

- Las cámaras de red han mostrado igualmente ser efectivos sustitutos de las cámaras analógicas en aplicaciones tradicionales de refuerzo a las fuerzas de seguridad, como por ejemplo para mantener seguros determinados lugares públicos.

- Las cámaras de red pueden igualmente emplearse para el control de accesos. Las personas, al igual que los vehículos, pueden grabarse junto con la información de la fecha y la hora de entrada de forma que sea sencilla su revisión y localización. Las imágenes pueden almacenarse en un lugar remoto, imposibilitando el robo de esta valiosa información.

1.6 Monitorización Remota

Las cámaras de red se conectan fácilmente a las redes IP existentes y permiten actualizaciones en tiempo real de vídeo de alta calidad para que resulte accesible desde cada uno de los ordenadores de una red. Las áreas sensibles como son la sala de servidores, la recepción o cualquier lugar remoto pueden ser monitorizadas detalladamente de una forma única y económica, a través de la red de área local o de Internet.

- Las cámaras de red mejoran la monitorización de un establecimiento comercial para asegurar que todo está en orden. (Quality of Service)

- Una cámara de red es una herramienta útil en la oficina. Áreas como la recepción y las salas de conferencias pueden estar monitorizadas para controlar su actividad. Además los usuarios pueden hacer seguimiento de quién ha entrado en la sala de informática, por ejemplo, y tomar las acciones pertinentes cuando haya problemas.

- Las cámaras de red son herramientas útiles en la industria de la fabricación. Monitorizar robots, u otras máquinas, y las líneas de producción desde la

oficina o desde casa y permitir a los ingenieros de servicio acceder a las cámaras remotamente. Con cámaras con funcionalidad Pan/Tilt/Zoom es posible tomar, además, tanto vistas generales como detalladas.

1.7 Atracción Web

Las cámaras de red permiten vídeo en directo de alta calidad que puede ser mostrado a toda la comunidad en Internet. El vídeo en directo es un método efectivo para invitar a los visitantes a volver a un sitio web.

La tecnología de cámara de red puede utilizarse para atracción web, es decir, para hacer que un sitio web resulte más dinámico e interesante y, por tanto, atraer más visitas. Por estos motivos las cámaras para ver el estado meteorológico de una zona y otras cámaras en directo son fórmulas populares para generar tráfico de visitas a un sitio web. Las cámaras pueden colocarse en el centro de una ciudad, en la universidad, en las zonas montañosas o sobre el mar para mostrar vídeo en directo.

1.8 Aplicación en la Ciencia

En el área de la Robótica es fundamental la obtención de imágenes, tal es el ejemplo de la NASA en Marte: la tecnología Java juega un papel protagónico en la NASA y en su más reciente exploración en el planeta Marte. Desde que la nave del explorador se puso sobre suelo marciano, en el Jet Propultion Laboratory (JPL), Pasadena, California, científicos de la NASA usan Java como la tecnología base para las maniobras y el sistema de control del robot Spirit.

James Gosling, CTO para el Programa de Desarrolladores de Sun Microsystems, estuvo en el JPL y admitió que "fue grandioso ver el cuarto de control lleno de alegría cuando finalmente obtuvieron la confirmación de aterrizaje".

Java3D y Java Advanced Imaging Technology, son claves para la operación del software que utiliza el JPL para retener e interpretar las imágenes de tiempo real que captura el robot. La NASA ha creado una versión del software, disponible en la Red, que demuestra simulaciones en 3D del paisaje marciano, visión que les permite a los expertos en la Tierra manejar los movimientos del robot en ese agreste paisaje.

Existen múltiples razones por la cuales JPL se apoya en la tecnología Java para el control y el sistema de imágenes del robot: la NASA obtiene una grandiosa rentabilidad y productividad, al mismo tiempo que reconoce la habilidad de Java de correr en cualquier plataforma.

En la actualidad Sun y el JPL de la NASA suman esfuerzos para el desarrollo de un sistema de control de tecnología Java que proporcione a futuros robots la capacidad de tomar decisiones inteligentes e independientes mientras exploran el planeta rojo.

Otro tipo de sistema sería para la manipulación remota de robots móviles, dando al robot información necesaria (imágenes obtenidas de la Cámara IP) de su espacio y así pueda procesar la información y poder llevar a cabo sus tareas.

1.9 Aplicación en la Medicina

Un campo muy importante en la cual un servidor de video es altamente potencial es en la Medicina, a esto se le llama *Telemedicina.* La telemedicina puede ser definida como la transmisión de información médica y la prestación de servicios de salud a través de redes de telecomunicaciones. Esta incluye la transmisión de imágenes fijas, vídeo y otras formas de datos médicos.

Uno de los experimentos más tempranos en usar comunicaciones de vídeo y sonido con fines médicos, fueron llevados a cabo en las misiones espaciales de la década de los 60 por los programas espaciales Norteamericanos y Soviéticos.

Actualmente, la telemedicina es predominantemente vista como una manera de resolver problemas como: insuficiencia de especialistas, escasez y centralización de recursos, centros de salud rurales con servicios médicos limitados y dificultades geográficas de comunicación; de esta manera logrando el objetivo de proveer igualdad en servicios de salud, sin importar la localización geográfica.

1.10 Otras Aplicaciones

Vigilancia a los empleados de una fábrica, empresa o establecimiento comercial: El monitoreo mediante cámaras facilita a los jefes o supervisores de una empresa el monitoreo a los empleados, además de ser monitoreados, aumenta la eficiencia de trabajo por parte de ellos.

Empresas: Seguridad perimetral para edificios, monitorización de los muelles de carga.

Centros Comerciales: Seguridad para clientes en aparcamientos.

Instituciones bancarias y financieras: Aumento de la seguridad en cajeros automáticos.

Ayuntamientos: Monitorización de las intersecciones del tráfico.

Campus Universitarios: Monitorización de zonas para protección de los estudiantes.

Escuelas primarias: Actuar como monitores de salas virtuales o monitorización de aparcamientos para los padres que esperan a sus hijos y protección de los estudiantes frente a intrusos.

Gobierno: Sistemas de Vigilancia antiterrorista para la seguridad nacional.

Transporte: Seguridad en túneles, puentes, autopistas,…

Militar: Seguridad en los alrededores de las instalaciones militares.

Refuerzo legal: Reducción de crímenes y de la violencia en zonas de riesgo.

Capítulo II

Video Digital y en Red

Capítulo II. Video Digital y en Red

2.1 Video Digital

2.1.1 Introducción

El formato **Digital Video** o **DV** es un estándar de vídeo de gama doméstica, industrial y broadcast. Se basa en el algoritmo DCT y usa como protocolo de transmisión de datos el IEEE 1394 o *Firewire*. Generalmente graba en una cinta de 1/4 de pulgada - con tres variantes: Mini, M y L- [3].

Fue creado en 1996 como un estándar internacional según la norma IEC 61834, que define el codec y el tipo de cinta.

Fue desarrollado como formato digital de vídeo para un entorno industrial, pero su excelente relación calidad-precio provocó que se haya convertido en el formato predominante en el vídeo doméstico, como *Mini DV*, y que hayan surgido versiones profesionales, *DVCAM* y *DVCPRO*. Existe un formato tipo DV50, el Digital-S, basado en este estándar pero que graba en cinta de 1/2". Su popularidad ha provocado incluso que sea base comercial para un formato barato de alta definición, el HDV, que sólo comparte el tipo de cinta.

2.1.2 Características Técnicas

El **DV** es un sistema de vídeo digital por componentes que utiliza una frecuencia de muestreo 4:2:0 en PAL y NTSC. 4:2:0 explora las componentes de color en líneas alternas: en una línea recoge el rojo y en la siguiente, el azul, y así sucesivamente. Por lo tanto lo que ocurre finalmente es que hay cuatro veces más información de luminancia que de crominancia. La frecuencia de Y es 13,5 MHz y la de C, 6,75 MHz. El DV tiene una profundidad de color de 8 bits.

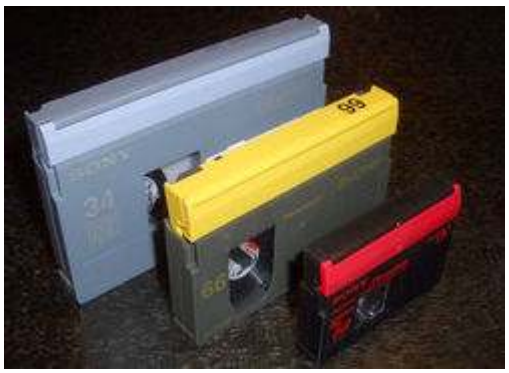


Figura 2.1 Cintas DV
De izq. a dch.: DVCAM-L, DVCPRO-M, MiniDV

Para la compresión de vídeo, DV usa el algoritmo DCT con una compresión intraframe y un ratio 5:1. DV es conocido como *DV25* porque el flujo de vídeo resultante es de 25 Mb/s -añadiendo audio, información de track y corrección de errores. El resultado de información es, aproximadamente, de 200 MB por minuto y unos 12 GB por hora.

El formato DV graba audio PCM sin compresión. Tiene dos configuraciones posibles de audio. Una permite grabar 2 canales de audio a 48 KHz y 16 bit, y la otra posibilidad 4 canales a 32 KHz y 12 bit; 2 canales de audio original y dos de doblado (audio dubbing) realizado a posteriori en posproducción. La calidad de la configuración de 2 canales, 48 KHz y 16 bit es ligeramente superior a la del disco compacto (CD).

Figura 2.2 Conector Firewire
Versión 6 pines (izq) y versión 4 pines (dch)

Para la conectividad el DV utiliza el interfaz IEEE 1394, también conocido como *Firewire* e *i.Link*, que si bien no es parte del formato en sí, está estrechamente ligado a éste. Cualquier equipo DV, tanto doméstico como profesional, lleva un conector Firewire, que puede tener conexión de 6 pines o de 4 pines. El Firewire también es usado como puerto serie para ordenadores -aparte del USB-. Equipos profesionales también pueden transportar la señal DV por SDI (digital) o por los conectores analógicos de vídeo en componentes, aunque en este caso habrá degradación de la señal por el paso digital-analógico.

La cinta usada para grabar DV tiene un ancho de 1/4" (6,35 mm). Este tipo de cinta tiene tres versiones distintas. La más conocida es la usada en la gama doméstica, la cinta *Mini DV*, que también usan algunos equipos profesionales y semiprofesionales. La rama profesional tiene otras dos variantes, el tamaño M y el tamaño L. La Mini DV tiene versiones de 30, 60 y 80 minutos. Las M y L tienen duraciones que van desde 12 a 276 minutos -siempre dependiendo de si se trata de DV, DVCAM, ProfessionalDV o DVCPRO.

El éxito de este formato y la búsqueda de nuevos soportes han llevado a JVC, Sony, Panasonic y otros fabricantes a desarrollar nuevas posibilidades de grabación. DV se graba sobre un disco duro portátil, en el propio camcorder o en un estacionario. Sony ha creado la gama XDCAM, que utiliza el Professional Disc como soporte. Se trata de un disco Blu-ray Disc con capacidad para 23 GB. XDCAM soporta los formatos DVCAM y MPEG IMX. Panasonic apuesta por la tarjeta de memoria con el modelo P2, un tipo de PCMCIA que aloja en su interior cuatro memorias SD. Las cámaras pueden llevar a la vez varias memorias e intercambiarse sobre la marcha.

2.1.3 Versiones

2.1.3.1 DVC

DVC DIGITAL VIDEO CASSETE v8 es la versión genérica del formato. Existen 2 tamaños de cinta: DV y MiniDV, la segunda más pequeña permite hacer los camcorders más compactos y ligeros de forma que se impone en el mercado. Las características del DVC: muestreo 4:2:0 con color a 8 bit, compresión 5:1 tipo DCT intraframe , flujo de vídeo de 25 Mb/s, 2 ó 4 canales de audio PCM a 32 ó 48 KHz y a 12 ó 16 bit. Es la versión no propietaria, el estándar acordado por la IEC. Todos los fabricantes distribuyen DVC con cinta pequeña MiniDV, quedando este nombre como la versión que se comercializa para uso doméstico.

Sólo graba señal en la cinta MiniDV o, en su defecto, en disco duro. Se diferencia de DVCpro y DVCam en el ancho de las pistas que graba la cinta, que tienen 10 micras.

Características técnicas de Mini DV		
Sistema	Digital SD. Por componentes	
Frecuencia de muestreo	4:2:0 (PAL & NTSC)	
Algoritmo	DCT intraframe	
Ratio de compresión	5:1	
Bitrate	25 Mb/s	
Profundidad de color	8 bits	
Soporte	cinta 1/4"	
Ancho de pistas	10 µm	
Canales de audio	2 canales PCM	4 canales PCM
Muestreo de audio	48 KHz / 16 bit	32 Khz / 12 bit

2.1.3.2 DVCAM

DVCAM es el nombre de la versión propia de Sony. Tiene las mismas características que el DV, pero Sony amplió el ancho de pista a 15 µm y aumentó en un 50 por ciento la velocidad de cinta. Esto repercute en mayor calidad, pero también en que las cintas duren un tercio que las del formato original. DVCAM puede grabar en cintas DVCAM y Mini DV y reproduce DV y DVCPRO -no desde el principio del formato-.

DVCAM se puede grabar, además de en cinta y disco duro, en Professional Disc.

Características técnicas de DVCAM		
Sistema	Digital SD. Por componentes	
Frecuencia de muestreo	4:2:0 (PAL)	4:1:1 (NTSC)

Algoritmo	DCT intraframe	
Ratio de compresión	5:1	
Bitrate	25 Mb/s	
Profundidad de color	8 bits	
Soporte	cinta 1/4"	Professional Disc
Ancho de pistas	15 µm	
Canales de audio	2 canales PCM	4 canales PCM
Muestreo de audio	48 KHz / 16 bit	32 KHz / 12 bit

2.1.3.3 DVCPRO

DVCPRO es la variante del DVC desarrollada por Panasonic. Al contrario que Sony, se apostó fuerte por este formato y se ha convertido en una importante franquicia con tres versiones desarrolladas hasta el año 2006. Su principal diferencia es que usa cinta con pistas de ancho de 18 µm y con otro tipo de emulsión, partículas de metal en lugar de metal evaporado -usado en DVC y DVCAM-. Además, cuenta con una pista longitudinal de audio y otra también longitudinal de control track para ayudar en edición, especialmente edición lineal. Otra característica respecto al audio es que sólo permite la opción de 2 pistas a 48 KHz y 16 bit.

DVCPRO o ***DVCPRO 25*** fue el primer DVCPRO desarrollado. Aparte de las pistas más anchas, de las cintas de partículas de metal y de las pistas longitudinales, DVCPRO 25 tiene un muestreo 4:1:1 en PAL y 4:2:0 en NTSC.

Características técnicas de DVCPRO 25		
Sistema	Digital SD. Por componentes	
Frecuencia de muestreo	4:1:1(PAL) 4:2:0 (NTSC)	
Algoritmo	DCT intraframe	
Ratio de compresión	5:1	
Bitrate	25 Mb/s	
Profundidad de color	8 bits	
Soporte	cinta 1/4"	tarjetas P2
Ancho de pistas	18 µm	
Canales de audio	2 canales PCM	
Muestreo de audio	48 KHz / 16 bit	

DV50 es una versión de mayor calidad que creó JVC en cinta de 1/2" pulgada llamada D9 (Digital S) con muestreo 4:2:2 a 50Mbps y compresión 3.3:1 utilizando dos codificadores de DV en paralelo con 4 pistas de audio PCM, y que posteriormente adoptó Panasonic como mejora de su DVCpro, pensando no sólo en cometidos ENG, sino en poder ofrecer aplicaciones de estudio. Lógicamente la capacidad de las cintas es la mitad de la proporcionada por DVCPRO 25.

Características técnicas de DVCPRO 50		
Sistema	Digital SD. Por componentes	
Frecuencia de muestreo	4:2:2	
Algoritmo	DCT intraframe	
Ratio de compresión	3,3:1	
Bitrate	50 Mb/s	
Profundidad de color	8 bits	
Soporte	cinta 1/4"	tarjetas P2
Canales de audio	4 canales PCM	
Muestreo de audio	48 KHz / 16 bit	

DVCPRO HD o *DV100* es una variación de DVCPRO 50 con resolución en Alta Definición. Usa el mismo muestreo 4:2:2, pero al ser HD permite resolución 1080 y 720, tanto en progresivo como en entrelazado -aunque el modo 1080/25p es falso, puesto que la captación es entrelazada y posteriormente hay un procesado-. Mediante una compresión hasta 1:6,7 se consigue un flujo de vídeo de 100 Mb/s. El formato admite además 8 pistas de audio.

Características técnicas de DVCPRO HD		
Sistema	Digital HD. Por componentes	
Frecuencia de muestreo	4:2:2	
Algoritmo	DCT intraframe	
Ratio de compresión	6,7:1	
Bitrate	100 Mb/s	
Profundidad de color	8 bits	
Soporte	cinta 1/4"	tarjetas P2
Canales de audio	8 canales PCM	
Muestreo de audio	48 KHz / 16 bit	

Toda la gama DVPCRO reproduce cintas DV y DVCAM, y algunos magnetoscopios también graban formato DV. También permite grabar en tarjetas de memoria P2 y en disco duro.

2.1.4 Importancia y Usos

El DVC fue creado para aplicaciones de vídeo digital para el mercado de consumo. Sony dominaba el mercado analógico con Betacam SP y dominaba en el mercado digital de postproducción con Betacam Digital aunque este formato era excesivamente caro para noticias ENG y necesitaba una solución para noticias ENG en formato digital creo el Betacam SX en M-PEG2 a 10Mbps. Panasonic, sin embargo, decidió aprovechar el formato DVC, sobre todo como formato más ligero en ENG (Electronics New Gat-

hering) para informativos. Creó su propia versión, el DVCPRO -a 25 Mbps -. Y JVC en las mismas fechas creo el D9 (ó Digital S) utilizando el doble procesado a 50Mbps con 4:2:2 y 3.3:1.

En 1997 el mercado industrial y broadcast nos encontramos compitiendo al unísono tres formatos: Betacam SX de SONY, DVCPro de Panasonic y D9 de JVC.

En 1998 tras un largo estudio la SMPTE/EBU task force recomiendan el formato digital ideal el del esquema de: 50 Mbps, 4:2:2 y 3.3:1 presentado por JVC.

A esto reaccionan rápidamente Panasonic creando el DVCPro50 y Sony el Betacam IMX, buscando los dos mantener la hegemonía del mercado de teledifusión y asimilando la lección del más pequeño JVC que no tiene su misma capacidad financiera.

Sony posteriormente para frenar la fuerte incursión de Panasonic en el mercado de informativos reaccionó apoyando el DVCAM, más allá de su cometido original como formato semiprofesional o para el mercado institucional. Al igual que DVCPRO 25, podía ser un sistema para informativos y para televisiones locales o con bajo presupuesto. El proceso de digitalización de las redacciones ha llevado a la gama DV, ya sea Sony o Panasonic, a casi todos los medios del mundo -aunque la primera también ha sabido vender su MPEG IMX-.

DV ha desde inicio un formato doméstico digital en componentes. La principal ventaja de cara al gran público fue la introducción de la cinta MiniDV, bastante más pequeña que sus competidores analógicos en el sector, el Hi8 y el VHS-C. JVC lanzó el primer modelo realmente compacto y con disposición vertical, varias veces más pequeño que sus competidores. La ventaja del tamaño, unido a su excelente calidad digital, ha permitido al MiniDV mantenerse desde mediados de la década de los 90 como el formato rey en el sector doméstico. Ha habido intentos por restarle fuerza, Sony hizo su propia apuesta mezclando su propio producto con el DV. Creó el Digital8, con las mismas características técnicas que el DV, pero aprovechando la cinta de 8 mm del Video8 y Hi8. O con el MicroMV de Sony -un formato MPEG-2-, la grabación en DVD -también MPEG-2- y la grabación con cámaras multiformato o cámaras fotográficas con tarjeta de memoria con una compresión de baja calidad en MPEG-4. Los últimos modelos domésticos permiten también grabar en disco duro, tanto en DV como en MPEG.

Entre medias de sector broadcast y sector doméstico, DV también se ha adaptado a vídeo industrial, su objetivo original. La mayoría de fabricantes ha mantenido MiniDV como el tipo de cinta a utilizar. Lo especial es que se ha apostado por un nuevo concepto de cámara. En lugar del clásico chasis ENG, se ha trabajado en una línea parecida a las videocámaras domésticas, de tamaño reducido y con visor al fondo, pero con sistema de 3CCD y controles profesionales. Canon y Sony son los fabricantes que más éxito han conseguido en esta línea, especialmente Canon y su modelo XL-1, que por contra se intenta parecer a las cámaras profesionales ENG en su disposición con visor en el lateral y montura al hombro.

El DV además ha tenido una importancia revolucionaria en cuanto a la democratización del vídeo. El sistema DV unido a una edición no lineal ha permitido que un usuario medio -en cuestión económica y de conocimientos técnicos- pueda acceder a una calidad profesional. Al mismo tiempo, Internet permite una difusión universal y

gratuita. Incluso el mundo del cine tiene la huella del formato digital: aunque ya se había grabado anteriormente en vídeo, el DV ha hecho que se produjesen películas sin apenas presupuesto que han llegado a estrenarse comercialmente -fragmentos de *El proyecto de la bruja de Blair* fueron grabados con cámaras de este tipo-, por otro lado cineastas de renombre se han acercado a él por su versatilidad, libertad de acción y estética propia, como Steven Soderbergh en *Full Frontal* y Lars Von Trier en *Bailar en la oscuridad* (*Dancer in the dark*).

2.2 Video en Red

2.2.1 Introducción

Un sistema de vídeo en red utiliza como red troncal (*backbone*) para el transporte de información redes LAN/MAN/WAN/Internet, en vez de las líneas punto a punto dedicadas que se utilizan en los sistemas de vídeo analógicos. Muchos negocios ya usan redes informáticas para una amplia cantidad de funciones. La tecnología de vídeo en red utiliza y amplía esta misma infraestructura para la monitorización remota y local.

Este capítulo proporcionará una introducción general a la composición, operación y beneficios de un verdadero sistema digital. En este sistema la transmisión de vídeo, del audio y de los paquetes de datos tiene lugar sin la presencia de una infraestructura física dedicada que conecte la cámara al monitor. El crecimiento del vídeo en red para tareas de vigilancia monitorización está siendo impulsado no sólo por un aumento general de la necesidad de seguridad, sino que también por su mayor rendimiento y los ahorros que proporciona, su flexibilidad en el acceso a la información y la facilidad de distribución de imágenes, por su capacidad de integración, escalabilidad y muchos otros factores.

2.2.2 Beneficios de la instalación de un sistema digital

El usuario final consigue una amplia variedad de beneficios al implementar un sistema de vídeo digital. Debajo encontrará un listado y la explicación de algunos de esos beneficios clave:

2.2.3 Flexibilidad en el acceso a la información

Las instalaciones ordinarias de CCTV operan en modo punto a punto, y precisan cableado dedicado para cada cámara. La visualización sólo puede llevarse a cabo desde monitores específicos y teclados de operarios conectados al sistema. Con una instalación de seguridad en red, el vídeo puede normalmente visualizarse desde cualquier punto de la red local, así como de forma remota desde cualquier parte del mundo. El acceso a la información del vídeo se controla a través de nombres de usuario y contraseña, en vez de restringir el acceso físico a un monitor y a un teclado de operario. Dado que se puede conectar a la red existe una excelente oportunidad para visualizar y gestionar la información que proviene de las cámaras. La mejora del acceso a través de una Intranet o de Internet proporciona un acceso más inmediato a las imágenes, a la vez que se redu-

cen considerablemente los gastos de viajes hacia y desde las localizaciones de monitorización. Además, por motivos de seguridad o conveniencia las imágenes pueden ser almacenadas automáticamente en lugares externos.

2.2.4 Facilidad en la distribución de la información visual

Uno de los mayores problemas con los sistemas analógicos es la falta de un sentido eficiente de la distribución de la información. La información está habitualmente disponible sólo en videocassete o en imágenes impresas. Ambos modos precisan un transporte público: mensajería, etc. para llevar la información de un lugar a otro. En el entorno del vídeo digital toda la información se trata como ficheros de datos, que pueden contener secuencias de vídeo o imágenes estáticas. Un fichero se puede distribuir fácilmente a un número ilimitado de receptores, o puede "colgarse" en una página web en pocos segundos. Esta distribución de la información visual puede realizarse sin degradación alguna de la calidad de las imágenes.

2.2.5 Utilización de una infraestructura existente

Frente a los sistemas analógicos que precisan cableado de propósito único o dedicado para enlazar dispositivos punto a punto, el sistema de vídeo digital precisa sólo una cantidad limitada de cableado para realizar la instalación. El sistema digital utiliza una red normal basada en IP para la transmisión y distribución de vídeo, con lo que se elimina la necesidad de una costosa instalación de cableado dedicado.

2.2.6 Funcionalidades de integración y preparación para el futuro

La tecnología de vídeo en red tiene la capacidad de proporcionar un mayor nivel de integración con otras funciones y servicios, lo que lo convierte en un sistema en continuo desarrollo. El uso de protocolos y redes estándares abiertos para la comunicación permiten una sencilla integración de sistemas con equipamiento de una amplia variedad de fabricantes. El cambio hacia la tecnología digital significa invertir en un sistema que tendrá continuidad en el futuro.

2.2.7 Escalabilidad

Un sistema digital es flexible y totalmente escalable para satisfacer las necesidades concretas de cualquier usuario. Lo digital ha sido diseñado para proporcionar funcionalidades de "contactar y funcionar" (*plug and play*) tanto para instalaciones pequeñas como para grandes aplicaciones profesionales. Frente a la mayoría de sistemas analógicos, un sistema de vídeo en red puede ser ampliado sin necesidad de reemplazar componentes del sistema.

2.2.8 Costo total de propiedad (TCO, Total Cost of Ownership)

Una cámara de red actualmente es más cara cuando se compara su precio con el de una cámara analógica "similar". Sin embargo un análisis que contemple todos los factores de la inversión total en el sistema hace que la decisión sea más favorable a la solución de vídeo digital. El vídeo en red puede aprovechar inversiones existentes en informática, redes y monitores. Los costes de instalación son generalmente inferiores dado que el cableado de red es mas económico que el coaxial. Además, se reducen los costes de mantenimiento al eliminar las cintas de vídeo y la necesidad de reparar y reemplazar los aparatos de vídeo (*VCR's*). Otro factor que impacta positivamente en el TCO se encuentra en el lado operativo. Las potentes herramientas de los sistemas digitales, tales como herramientas para buscar, localizar y distribuir imágenes de vídeo interesantes aumentan la eficiencia y la eficacia de los operadores. Cuando se incorporan todos estos factores de mantenimiento y operativos a la ecuación, el análisis de costes es aún más beneficioso para la solución digital, especialmente si se precisa grabación de vídeo.

2.2.9 Construir e instalar un sistema

Para diseñar con garantías de éxito un sistema de vídeo en red de alto rendimiento es necesario considerar múltiples factores antes de su instalación. Entre ellos habrá algunos que pueden ser controlados a través del diseño de sistemas, así como a través de factores externos como redes, rendimiento, entornos y otros que el diseñador debe considerar y sospesar adecuadamente.

2.2.9.1 Factores sobre redes

Dado que los sistemas digitales utilizan redes informáticas como medio de transporte para contenidos, el diseño de red afectará al rendimiento global del sistema de vídeo, así como al rendimiento global de la red. La gran mayoría de las redes nuevas que se instalan están basadas en Ethernet, están configuradas con una estructura de estrella y cuentan con una red troncal de comunicaciones entre diferentes switches. Para nuestro propósito las estructuras de estrella y de bus son las más relevantes. En las redes de bus todos los dispositivos están conectados a un cable central, denominado bus o *backbone*. En la estructura de estrella todos los dispositivos se conectan a un concentrador o *hub central*.

Cuando se comparan estructuras de redes Ethernet (bus) y de CCTV analógico (estrella) se encuentran diferencias importantes. Las redes Ethernet precisan una cantidad de cables relativamente pequeña y en ella varios dispositivos comparten el mismo cable (*bus*). Mientras que en las estructuras de estrella cada dispositivo necesita un cable separado para conectar al punto central. Una red Ethernet permite al usuario compartir el cable ente varios sistemas. La estructura de bus Ethernet no tiene un punto central en el sistema, lo que lo hace mucho más tolerante a los fallos que en la estructura de estrella y el cableado es más flexible y fácil de ampliar. En prácticamente todas las empresas el cableado Ethernet ya está instalado, y esta misma infraestructura puede ser también utilizada para aplicaciones de seguridad y vigilancia.

Una red Ethernet se integra fácilmente con intranets o Internet, permitiendo un acceso remoto controlado y supervisado a las cámaras y la cantidad de información que ofrecen. También permiten al usuario realizar en local las grabaciones o llevarlas a cabo en una localización remota a través de, por ejemplo una red privada virtual (VPN). Para

nuestros propósitos, la red Ethernet representada por la estructura de bus es superior a la actual estructura de red en estrella del CCTV.

En la figura 2.1 se muestra un ejemplo de un sistema de video en red.

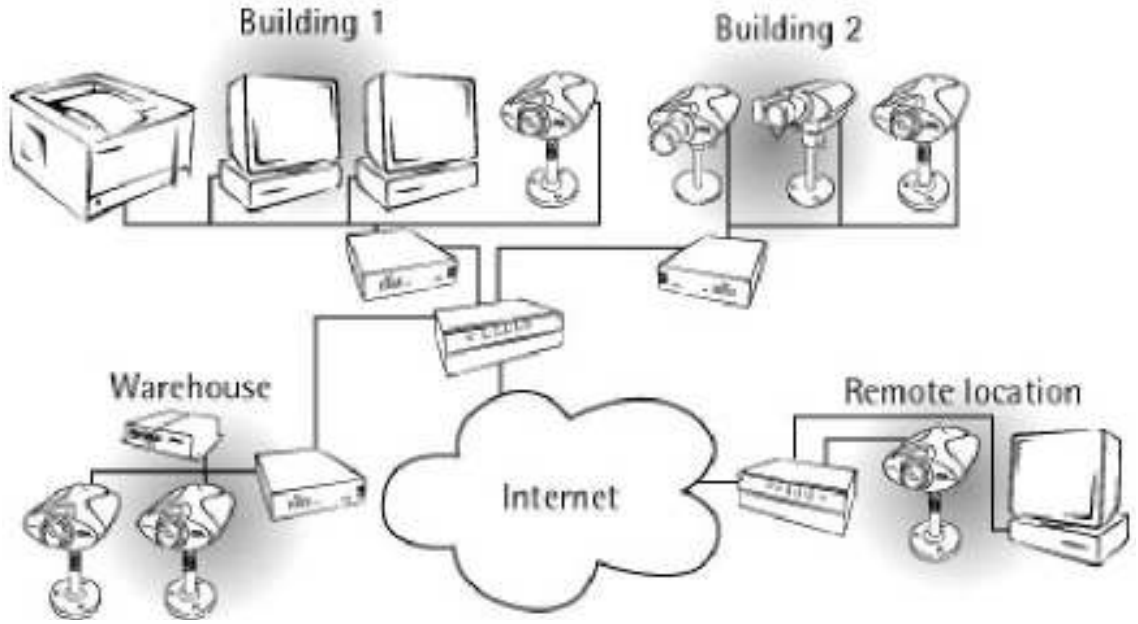


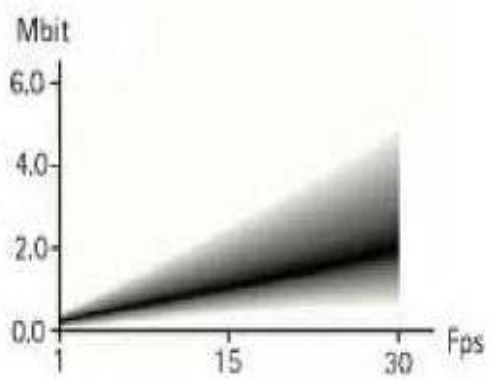
Figura 2.1 Ejemplo de un sistema de vídeo en red.

2.2.9.2 Capacidad de la red

Dependiendo de la configuración del sistema, el vídeo puede consumir grandes cantidades de ancho de banda de la red. En cualquier caso es importante comprender el rendimiento de la red actual: dónde hay cuellos de botella y dónde pueden ocurrir si se instala un sistema de vídeo digital. Esta labor suele realizarla el director de TI o al menos en cooperación con el departamento de sistemas.

Una red puede estar compuesta de segmentos con diferentes anchos de banda. Un único punto de conexión a un concentrador o a un conmutador puede ser una conexión a 10 o 100 Mbps, mientras que el *backbone* que comunica dos *switches* puede ser una conexión de 1 Gbps o incluso de 10Gbps. En esta situación la mejor solución es crear un plan para definir el ancho de banda disponible (mínimo ancho de banda disponible y máximo uso) para la aplicación.

Esto garantizará el nivel de rendimiento del que es preciso disponer para asegurar la operativa de un sistema de seguridad, y al mismo tiempo previene que el consumo sea superior a la capacidad, con la consecuente reducción del rendimiento de otros sistemas de la misma red.Es difícil definir el uso exacto del ancho de banda por parte de una cámara, debido a que dependerá de varios factores como:



- Tamaño de las imágenes
- Compresión
- Ratio de imágenes por segundo
- Resolución de la imagen

En relación a la gestión del ancho de banda es importante conocer que los productos de vídeo en red (basados en la compresión M-JPEG) utilizarán el ancho de banda en función de su configuración. Una imagen de alta resolución (4CIF) contiene cuatro veces más datos que una imagen a resolución normal (CIF). Una reducción del ratio de imágenes a la mitad (por ejemplo, pasar de 25 a 12.5 imágenes por segundo) reducirá también a la mitad la cantidad de datos. La figura anexa ofrece mayor información sobre este tema.

2.2.9.3 Soluciones de diseño de redes

Ahora nos centraremos en los diferentes elementos del diseño que pueden igualmente afectar al rendimiento y la gestión de la red. En la figura inferior izquierda vemos una solución que es vulnerable debido a que tiene demasiados puntos de potencial congestión en el tráfico de datos. En esta instalación todas las imágenes de todas las cámaras se envían del hub#1 al hub#2 a través de un único enlace. Este enlace ha de tener mucha capacidad para no correr riesgos de problemas potenciales de ancho de banda. Además, si por algún motivo el enlace falla no se tendrán imágenes de vídeo hasta que el problema haya sido solucionado.

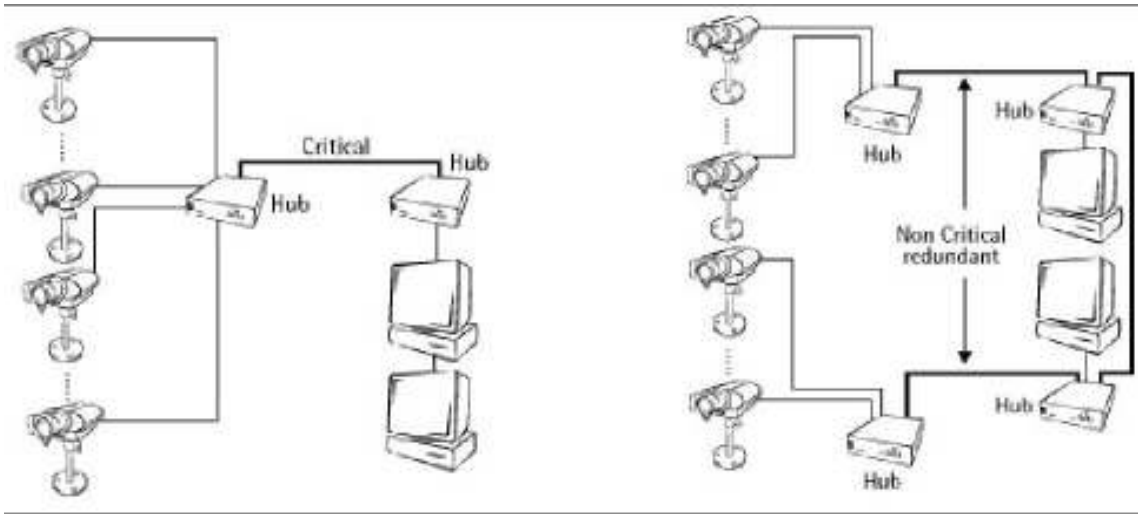


Figura 2.2 Dos diferentes conceptos de diseño de red

En la figura de la derecha (figura 2.2) las vulnerabilidades que mencionábamos sobre la de la izquierda se han gestionado y minimizado correctamente al incorporar dos nuevos hub/switches, y mediante la creación de un segundo enlace entre las cámaras y las áreas de monitorización.

Esta instalación tiene dos ventajas adicionales: Primero puede mejorar potencialmente el ancho de banda y eliminar el riesgo de congestiones. En segundo lugar, crea un sistema redundante de forma que incluso en el caso de fallos en un enlace el usuario seguirá teniendo acceso a alguna o todas las cámaras. Al diseñar los sistemas de forma prudente y dividir el número de cámaras en diferentes secciones o enlaces, el usuario consigue los beneficios de mayor fiabilidad y mejora del rendimiento.

2.2.9.4 Seguridad de la red

El proveedor de redes o el administrador, generalmente el departamento de TI, tendrá un conjunto de políticas asociadas al uso de la red. Estas políticas incluyen aspectos como credenciales para el log-on, procedimientos de back-up, y escaneo y filtrado de virus. Muchas de estas políticas pueden afectar al rendimiento del sistema. Por ejemplo, ¿Existen conexiones externas a máquinas no corporativas?, este tipo de conexiones serán necesarias si la organización planea usar servicios externos de monitorización de alarmas. Esto puede, a su vez, generar un gran número de cuestiones: ¿Tendrá el centro de monitorización de alarmas la capacidad para conectarse con el sitio local para realizar una ronda de vigilancia, tanto local como remotamente por parte de la compañía de alarmas? ¿Se va a almacenar el vídeo?, ¿De que forma? ¿Se deben incluir esas imágenes grabadas en los procedimientos de back-up? ¿El sistema actual de back-up es capaz de gestionar este volumen adicional de datos? Estos son sólo unos pocos ejemplos de preguntas y políticas que deben ser exploradas para valorar como los procedimientos de seguridad de la red pueden impactar en el rendimiento del sistema.

2.2.10 Factores externos de las aplicaciones

Además de los diversos factores relacionados con la red y cubiertos anteriormente existen varios factores externos que se relacionan directamente con la aplicación del sistema de vídeo en red. Estos factores, que son básicamente los mismos para un sistema digital que para un sistema de vídeo analógico precisan ser revisados.

2.2.10.1 Entorno

¿Las cámaras vas a ser usadas en exteriores o van a estar expuestas a condiciones adversas? Si es así las cámaras precisan estar instaladas en unas carcasas adecuadas que las protejan de las condiciones climatológicas, del polvo y de la humedad, de las temperaturas extremas, así como de otros factores ambientales no deseados. Las carcasas deben igualmente incorporar un sistema de calentamiento o enfriamiento para ofrecer una temperatura de operación adecuada. En este punto debemos también considerar el campo visual para la cámara. ¿Va a tener una visión clara y directa del área objetivo en todo momento?, ¿O puede la visión verse bloqueada (intencionalmente o no) por, por ejemplo, árboles que crecen, un camión aparcado o una puerta que se queda abierta?. Otro factor que afecta a la cámara, especialmente cuando se instala en exteriores, es la dirección hacia el área objetivo en relación a una luz fuerte, y en particular a la luz solar. Si una cámara está en la dirección hacia la que se pone el sol, las imágenes posiblemente sean completamente inútiles. Instalar la cámara en una localización diferente para visualizar la misma escena mejorará la calidad de las imágenes notablemente.

2.2.10.2 Iluminación

Uno de los factores a considerar más importantes cuando se instala un sistema de CCTV es la iluminación. ¿Habrá luz suficiente para poder contar con imágenes de alta calidad? Generalmente cuanta más luz haya mejor será la imagen. Si el nivel de luz es demasiado bajo las imágenes serán borrosas y los colores apagados. El nivel de luz se mide en Lux. Una luz solar fuerte tiene aproximadamente 10.000 lux y la luz de una vela es aproxi-

madamente 1 Lux. Habitualmente se precisan al menos 2000 lux para capturar imágenes de buena calidad.

Si la iluminación no es suficiente puede ser preciso instalar luces adicionales. Para asegurar una iluminación adecuada pueden usarse dispositivos externos de control como sensores de luz, detectores sensibles a movimientos en el área, etc.

Debemos igualmente considerar si la instalación es en un entorno de luz estática (por ejemplo en interiores) o en un entorno dinámico (generalmente en exteriores) donde los niveles de iluminación pueden variar considerablemente. Para compensar, en un entorno dinámico, los cambios de contraste y brillo, las cámaras deben ir equipadas con una lente que automáticamente ajuste el iris en función de la cantidad de luz circundante.

Deberían evitarse las áreas con mucho brillo ya que las imágenes pueden quedar sobre expuestas y que los objetos aparezcan muy oscuros. El contraste de colores entre objetos y fondos también afecta a la exposición. Un pequeño objeto oscuro debería mostrarse frente a un fondo oscuro para conseguir los colores correctos.

2.2.11 Factores operativos

Además de las consideraciones sobre redes y aplicaciones hay varios factores relacionados con la operativa de nuestro nuevo sistema de vídeo digital que también precisan ser examinados.

2.2.11.1 Visualización de vídeo

Hay dos tipos de sistemas cuando se precisa visualizar vídeo en directo. Primero existen instalaciones con operarios de seguridad dedicados a ver constantemente el vídeo y monitorizar activamente los objetos e incidentes de las imágenes. Ejemplos de este tipo de instalaciones incluyen establecimientos carcelarios, centros de vigilancia de ciudades y aeropuertos. El segundo tipo de sistemas es aquel en el que las imágenes de vídeo se visualizan sólo ocasionalmente. Estos sistemas son aquellos que se usan por ejemplo para dejar a alguien que pase a través de una puerta.

Un asunto fundamental con la visualización del vídeo es que alguien necesite estar allí para monitorizarlo y llevar a cabo acciones basándose en lo que está observando. La ventaja real de un sistema de vídeo en red es que la visualización se puede hacer desde cualquier punto de la red y simultáneamente desde varias localizaciones. Para proporcionar seguridad y una mejor gestión del sistema, el acceso al vídeo puede restringirse con protección por contraseñas en las cámaras. Un sistema de vídeo en red ofrece condiciones para asegurar que el vídeo puede ser monitorizado de la forma más eficiente y sencilla, consiguiendo mejores resultados.

2.2.11.2 Almacenamiento del vídeo

En la mayoría de las situaciones de seguridad es beneficioso, e incluso esencial, que el vídeo se grabe y almacene para su revisión posterior. Almacenar el vídeo permite que el usuario pueda revisar un incidente las veces que sea preciso, tanto imágenes aisladas

como secuencias de video interesantes, y después distribuirlas de la forma que precise la aplicación. Aunque el almacenamiento del vídeo proporciona numerosas ventajas para al gestión de la seguridad, es preciso ahondar, y lo haremos posteriormente, en las limitaciones de la grabación y su visualización posterior, basándose en las potenciales legislaciones gubernativas relacionadas con la grabación de imágenes en general y las restricciones a la grabación en función de la localización.

2.2.11.3 Acceso a la información

En el mundo analógico, la seguridad para el vídeo almacenado se consigue simplemente limitando el acceso a las cintas de vídeo grabadas, que normalmente se guardan en un armario al efecto o en una zona de almacenamiento. Con vídeo en red, toda la información se almacena como datos, sin limitaciones, y estos datos puede visualizarlos cualquiera que tenga acceso a la red. Dado que estamos hablando de sistemas que gestionan la seguridad de una operación, hay grandes incentivos para la limitación del acceso a esta información. La limitación del acceso puede dividirse en dos categorías o razones para la restricción: por motivos operativos y de gestión o por motivos legales.

Dado que la grabación del vídeo en muchas instancias está visto como una potencial intrusión en la privacidad de las personas, hay una gran motivación en la limitación del acceso a estos datos grabados o a la información. Los Gobiernos y las corporaciones tienen grandes intereses en poner límite y controlar el acceso al vídeo no sólo para evitar problemas o cuestiones futuras, sino también para conseguir la aprobación de individuos y organizaciones (Ej. sindicatos, empresas matrices,…) a la grabación del vídeo. Este tipo de limitaciones asegura que sólo el personal de seguridad tiene la capacidad de visualizar y trabajar con el vídeo.

Otro aspecto para restringir el acceso está en el lado operativo y este es para reducir el riesgo de que alguien intente borrar o manipular el material grabado. Las organizaciones tienen que controlar el acceso que la gente tiene a la información y a los pocos que tienen acceso para asegurar el mantenimiento de la integridad de los datos grabados. En muchos países e incluso municipios existen limitaciones específicas al acceso, que son legalmente necesarias si los datos grabados pretenden usarse como evidencia o como parte de los procedimientos de una investigación oficial.

En general es sólo este personal que tiene una necesidad real de esta información el que debería tener acceso completo. Para gestionar este tipo de acceso de forma efectiva muchas organizaciones registran el acceso por usuario, fecha y hora.

2.2.11.4 Integración

Dado que el vídeo reside en una red y la red se usa comúnmente para otras aplicaciones como control de accesos, de intrusos, gestión del edificio, etc. la base para las potenciales combinaciones y sinergias de integración está ya presente. En el pasado la integración se llevaba a cabo a nivel de relé/input, o entre dos PC’s que usen comunicación serie RS232.

Con un sistema de vídeo en red otras aplicaciones o sistemas pueden tener acceso directo a cámaras seleccionadas o al vídeo almacenado, sin necesidad de cableado o hardware adicionales. Al usar un API (Interfase de programación de aplicaciones) Win-

dows abierto, la capacidad de la tecnología de vídeo en red para proporcionar un mayor nivel de integración con otras funciones y servicios lo convierte en un sistema eficiente, en continuo desarrollo y preparado para el futuro.

2.2.11.5 Legislación existente

Como se ha mencionado anteriormente, otro factor que puede impactar en el rendimiento del sistema es la legislación aplicable. Hay un número de países que cuentan con regulaciones que protegen los derechos de privacidad individual. Estas leyes y regulaciones pueden en algunos casos restringir la visualización y/o el almacenamiento del vídeo. Los propietarios/operadores del sistema necesitan tener en cuenta estas regulaciones. En algunos casos el almacenamiento del vídeo puede verse particularmente afectado. Aunque la grabación actual no puede estar prohibida, la duración del vídeo puede verse restringida a poco más de 24 horas. En otros casos el almacenamiento del vídeo sólo se permite hasta 31 días después de la grabación y en cualquier caso la duración del almacenamiento está restringida y puede afectar a la manera en la que se pueden utilizar esos sistemas. En cada país suelen existir cuerpos gubernamentales que pueden proporcionar información adicional en relación a las restricciones de grabación y almacenamiento.

2.2.12 Componentes de un sistema de vídeo en red

2.2.12.1 Cámaras

Las cámaras son el componente esencial en todas las instalaciones de vídeo. Este dispositivo recoge la luz y la convierte en un conjunto de imágenes reconocible, que puede entonces enviarse a través de la red. Todas las cámaras generan imágenes estáticas que se envían a un visualizador con un ratio de imágenes por segundo. El ojo humano precisa aproximadamente 17 imágenes (o frames) por segundo para percibir el vídeo como en directo. La cámara en sí misma consiste en un chip que convierte la luz en señales eléctricas, y varios circuitos electrónicos como el DSP (procesador digital de imágenes) y otros que no son importantes para el tema que nos ocupa.

Como se ha mencionado brevemente antes las cámaras analógicas han sido el estándar durante muchos años. De forma creciente, cada vez hay más cámaras de red instaladas. Las cámaras de red proporcionan toda la funcionalidad de las cámaras analógicas y más, como veremos a continuación.

2.2.12.1.1 Cámaras de red fijas

Una cámara de red fija proporciona una visión estática del área que está frente a la cámara. Además de la unidad de cámara se necesita una lente para que la cámara opere correctamente. La lente ajusta la cantidad de luz que entra en la cámara, al igual que hace una cámara de fotos. La lente también enfoca la imagen en el sensor de imágenes (CCD). Antes de alcanzar el sensor, las imágenes pasan a través de un filtro óptico, que elimina cualquier luz infrarroja de manera que el color correcto (necesario para asegurar que sólo estamos usando una gama de color) sea el que se muestra. El sensor de imágenes convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales digitales eléctricas están ahora en un formato que pueden comprimirse y transferirse a través de la red.

Las cámaras de red proporcionan al usuario final muchos beneficios incluyendo una mayor funcionalidad respecto a las cámaras analógicas con un TCO (Coste total de propiedad) inferior. Las cámaras de red se conectan directamente a la red existente de manera que el cableado coaxial necesario para las cámaras analógicas ya no se precisa y los gastos de instalación son mínimos. Cuando existen ordenadores en el lugar ya no se precisa más equipamiento para ver las imágenes provistas por la cámara, y estas imágenes pueden visualizarse de la manera más simple desde un navegador Web en el monitor de un ordenador, y de forma más compleja usando soluciones de seguridad profesionales con la ayuda de un software dedicado.

2.2.12.1.2 Cámaras con movimiento horizontal, vertical y zoom (Cámaras PTZ)

Una cámara de red PTZ básicamente combina en un único producto una cámara fija, una lente de zoom, un dispositivo que permite a usuarios remotos mover la cámara para cambiar su campo de visión y un interfase de red. La cámara puede moverse tanto manual como automáticamente. En algunos casos se pueden usar lentes externas con las denominadas cámaras pan tilt (con movimiento horizontal y vertical).

2.2.12.1.3 Software

Aunque el vídeo se puede visualizar directamente desde un navegador Web normal sin la necesidad de software dedicado, se recomienda usar una aplicación de software en combinación con las cámaras. Este software puede ofrecer al usuario opciones de visualización más flexibles así como la posibilidad de almacenar y gestionar el vídeo. El software puede ser una solución autónoma para un único PC o una aplicación cliente/servidor más avanzada que proporcione soporte a múltiples usuarios simultáneos. En algunos casos el usuario final quiere seleccionar el software para implementar el soporte a múltiples sistemas como el de vídeo y el control de accesos. Seleccionar el paquete de software que permita unir los objetivos de la aplicación y del sistema es una de las claves en el diseño de un sistema útil y eficiente.

2.2.12.2 Otros componentes

Además de los componentes principales descritos anteriormente existen accesorios para los sistemas de vídeo en red que, en la mayoría de los casos, son útiles para otras aplicaciones y sistemas que también están en red. Estos sistemas incluyen impresoras, almacenamiento en red, unidades de CD/DVD-RW, servidores de correo electrónico y otros, que pueden añadir un valor sustancial a la instalación.

2.2.13 Un sistema de vídeo en red en acción

Tras evaluar la estructura de la red actual, el entorno de instalación y los componentes de un sistema de vídeo en red revisaremos el tipo de funcionalidad disponible en el sistema. Esto depende en gran medida del tipo de negocio que pretende asegurar la instalación. Las necesidades de un establecimiento comercial serán radicalmente diferentes a la s de la monitorización de un parking y ambas serán diferentes de las necesidades de un casino.

La tecnología de vídeo en red ha demostrado ser interesante en una amplia variedad de aplicaciones. Esta revolucionaria tecnología está reemplazando a los sistemas de estilo tradicional para reducir costes, aunque también está siendo usada por primera vez para crear y estimular nuevos y excitantes mercados. Hasta la fecha, la tecnología se ha desplegado con éxito en múltiples mercados. Como ejemplos sirvan el de Educación: para seguridad y monitorización remota de patios escolares, pasillos, salas y aulas; Transporte: para monitorización remota de estaciones ferroviarias, autopistas y aeropuertos; Banca: en aplicaciones de seguridad tradicional en bancos, sucursales y allá donde haya un cajero automático; Gobierno: con aplicaciones de vigilancia de seguridad, a menudo integradas en sistemas de control de accesos nuevos y existentes; Establecimientos comerciales (retail) para propósitos de seguridad y monitorización remota y para hacer más sencilla y efectiva la gestión del almacenamiento; Industria: para monitorización de procesos en la fabricación de automóviles, para la gestión del correo postal y para sistemas de control del almacenamiento y stocks.

Capítulo III

Ingeniería de Requisitos

Capítulo III. Ingeniería de Requisitos

3.1 Introducción

3.1.1 Propósito

El propósito del desarrollo de este trabajo es proveer un componente que facilite al usuario (programador) conectarse y obtener imágenes de una cámara IP, ya que en la actualidad no se cuenta con este tipo de componentes, los hay para otros dispositivos pero no para una cámara IP [12].

Este componente desarrollado está dirigido para los programadores, en especial aquellos que programan en el lenguaje JAVA.

Con este componente tendrán la facilidad de crear aplicaciones de vigilancia (pongo en primera mención la Vigilancia ya que en la actualidad es muy demandado un sistema de vigilancia, y ahora con la existencia de cámaras IP este componente es muy útil para desarrolladores), seguir con aplicaciones como son: enfocándonos en la medicina; la observación desde casa de una operación a algún familiar o vaya porque no el apoyo de un médico especialista situado en otro lugar que no sea en el hospital, este tipo de aplicaciones no son muy difundidas y sin embargo puede aportar mucho. En el campo de la robótica, este componente puede brindar la visión para hacer manipulación remota de robots, ya sean industriales, robots móviles, etc.

3.1.2 Alcance

Es importante recalcar los alcances de este componente, que tendrá la capacidad de conectarse y obtener imágenes de una cámara IP.

Tomando como objetivo de este componente es que el desarrollador tenga la facilidad de crear aplicaciones de escritorio o web para la manipulación de cámaras IP o tomar una cámara IP como herramienta de un proyecto de imágenes digitales o de robótica y hasta de vigilancia.

Para todo esto debe existir una meta, la cual es la creación de sistemas que exploten la existencia de estas cámaras y tengan un fuerte potencial en el mercado y la ciencia.

3.1.3 Limitantes

Este componente se reduce a manipular a una sola línea de cámaras, esa línea de cámaras es de la marca Intellinet, ya que en el mercado existen distintos tipos de cámaras IP y su funcionamiento varía por algunos parámetros.

3.2 Descripción General

3.2.1 Perspectiva del componente

Existen productos los cuales permiten una visualización de alguna o varias cámaras IP. Por ejemplo, **NetCam Watcher Pro,** con precio al público que tiene un número ilimitado de cámaras pero todo depende del paquete que compre el usuario, los hay desde 1 cámara hasta n-cámaras. Sus funciones van desde ver video hasta detección de movimiento y creación de video en formato AVI, todo eso pagando, desde la versión mas cara Professional desde 1 cámara hasta n-cámaras y en la versión Home pagando un precio mas económico hasta 2 cámaras.

Los beneficios y limitantes se ven reflejados en el precio.

Con este componente uno se pone su propia limitante tomando en cuenta la marca de la cámara. Además de que el programador puede extender este componente a más tipos de cámaras con tan solo estudiar las especificaciones de las demás marcas. Con este componente podemos crear múltiples sistemas agregando funciones como detección de movimiento, grabación de video en formato AVI o MOV, aplicación de técnicas de imágenes digitales y demás, el cual no contienen otros productos de cámaras IP.

3.2.1.1 Interfaces del Sistema

Algo importante de esto es como se hace la transferencia de la imagen desde la cámara a la PC, esto empieza desde la lente de la cámara que enfoca la imagen en el sensor de imagen (CCD). Antes de llegar al sensor, la imagen pasa por el filtro óptico que elimina cualquier luz infrarroja de forma que se muestren los colores correctos. El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de la red. Por otra parte en el componente se crea un mecanismo para hacer conexión a la cámara especificándole la dirección IP y el puerto, al realizar la conexión se procede al logueo al cual se le especifica un nombre de usuario y una contraseña de acceso a la cámara IP. Al ser aceptada la petición por parte del servidor de la cámara, se procede a la obtención de la imagen que más que nada son bytes los cuales posteriormente pueden ser manipulados por el programador para crear una imagen.

3.2.1.2 Interfaces con el Usuario

La manera de usar o programar con este componente y poder crear aplicaciones de vigilancia, etc., es usando un ID de programación adecuado o con lo que se adapte el programador, desde un JCreator, hasta un Eclipse o NetBeans para la creación de las interfaces gráficas es recomendable usar las últimas 2.

3.2.1.3 Interfaces con el Hardware

Este componente interactúa con cámaras IP de la serie Intellinet mediante el protocolo TCP/IP y una PC que los requisitos de memoria y reloj de procesador dependerán de que tan robusto sea el sistema creado con ayuda de este componente.

3.2.1.4 Interfaces de Comunicaciones

Este apartado es importante su mención ya que el componente se centra en este punto, puesto que existe comunicación de datos. Entiéndase como comunicación de datos al proceso de comunicar información en forma binaria entre dos o más puntos. Esto requiere 4 elementos básicos que son:

- **Emisor:** Dispositivo que transmite los datos.
- **Mensaje:** lo conforman los datos a ser transmitidos.
- **Canal o Medio:** consiste en el recorrido de los datos desde el origen hasta su destino.
- **Receptor:** Dispositivo de destino de los datos.

En este caso el receptor es la PC donde reside el componente o en su defecto el sistema creado en base a ese componente, el cual hace una petición (mediante un mensaje) al servidor de la cámara IP para realizar una conexión, y el emisor es la cámara IP que al recibir la petición del receptor y aceptarla, procede a enviar bytes de datos, esos bytes son la imagen, bytes que después serán procesados para una tarea a fin.

Una vez cumpliendo con estos 4 elementos básicos se dice que existe comunicación de datos, como se muestra en la figura 3.1 [7].

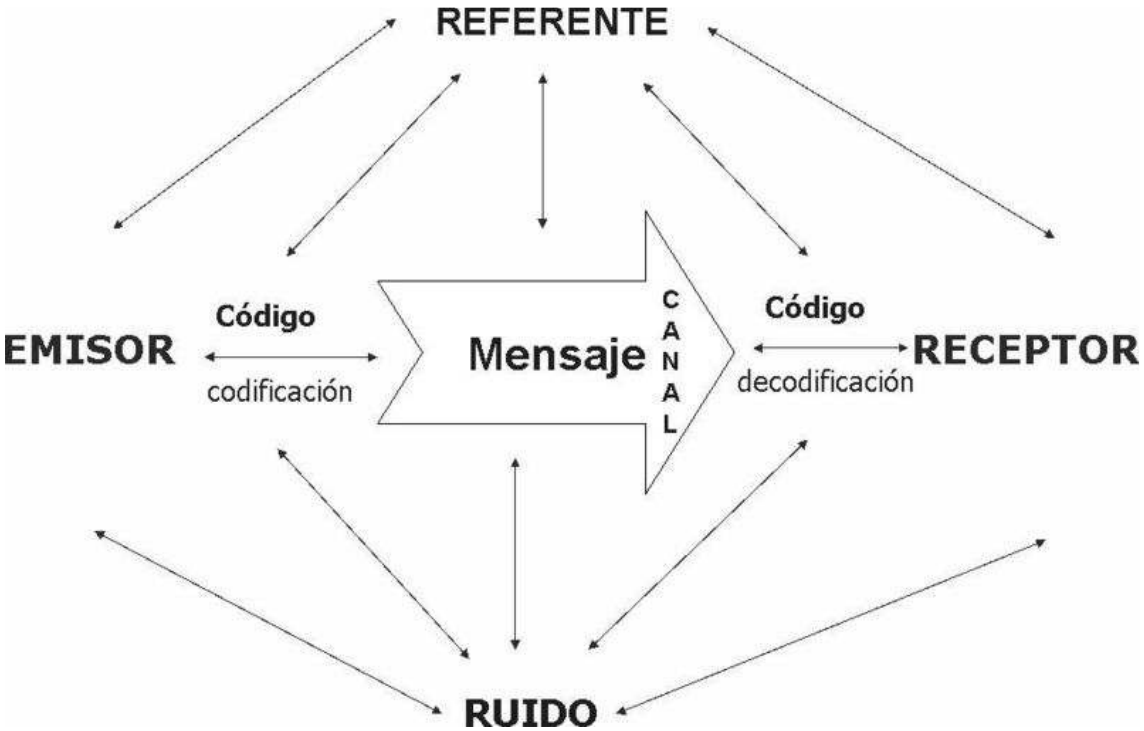


Figura 3.1 Elementos Básicos en la Comunicación de Datos

Una problemática que es muy importante para este tipo de transmisión, es la rapidez, cosa que depende por el ancho de banda por donde se transmite. Esto ya depende del tipo de conexión con el que se cuente para usar el sistema, normalmente sistemas de monitoreo son usados en redes LAN, en todo caso que sea usado en una WAN se deberá tener una buena conexión a Internet.

Memoria: Para el buen funcionamiento de un sistema que maneje este componente es necesario el uso de la memoria primaria y secundaria.

- **Memoria Primaria:** Son circuitos integrados capaces de almacenar información digital, a los que tiene acceso el microprocesador de una PC. Poseen una menor capacidad de almacenamiento que la memoria secundaria, pero una velocidad millones de veces superior. En la memoria primaria al momento de obtener los datos (bytes) de la cámara IP son almacenados en la memoria para ser procesados, ya sea para crear un formato de imagen válido o para realizar algún tipo de procesamiento digital, ya sea aplicar filtros o realizar operaciones diversas sobre esos datos y después transformarla a imagen y ver los resultados. Para este tipo de operaciones se necesita suficiente memoria para llevar a cabo este tipo de tareas, y no se alente el proceso. En mi caso utilizo una PC con 1GB de memoria primaria la cual es suficiente y de sobra, esto puede funcionar hasta con 256MB de memoria principal.

- **Memoria Secundaria:** Es un conjunto de dispositivos periféricos para el almacenamiento masivo de datos de un ordenador, con mayor capacidad que la memoria principal, pero más lenta que ésta. El disquete, el disco duro o disco fijo, las unidades ópticas, las unidades de memoria flash y los discos Zip, pertenecen a esta ca-

tegoría. Esta memoria será usada una vez obtenidos los bytes desde la cámara IP y esos bytes hayan sido usados para crear una imagen. La imagen o serie de imágenes creadas se podrán almacenar en el disco duro o algún otro medio y así poder crear un video en formato AVI, MOV, etc. La capacidad de almacenamiento requerido dependerá de el tipo de uso del sistema, ya que si se mantiene al sistema creando imágenes en el disco duro todo un día pues si ocupará mucho espacio, pero esos casos ocurre cuando el sistema es orientado a un sistema de vigilancia y al ser así se tendrá que crear un video a partir de esa serie de imágenes, ese video también ocupará bastante, pero eso se soluciona teniendo un disco duro con mucha capacidad que hoy en día no son muy caros.

3.2.2 Funciones del Componente

Este componente en función con la cámara IP es totalmente fácil ya que aleja al programador crear un mecanismo para realizar la conexión y obtención de los datos de la cámara IP.

Puesto que en otros casos para poder manejar una cámara desde un lenguaje de programación no es nada trivial, ya que luego el código creado o conseguido en la red no es autosuficiente y a veces no muy comprensible.

3.2.3 Características de los usuarios

Los usuarios, que en este caso deben ser programadores, deben tener conocimientos de el paradigma Orientado a Objetos y a su ves tener un conocimiento suficiente en el lenguaje JAVA. Tener amplios conocimientos en la creación de aplicaciones gráficas (aplicaciones swing o applets por lo menos) para poder desarrollar un sistema completamente gráfico y funcional.

3.2.4 Limitaciones

Para poder usar este componente se recomienda usar una cámara IP de la línea Intellinet puesto que fue con la que se trabajó y probó.

Se debe contar con una conexión de red al menos local.

Para el hardware se debe contar con una PC que soporte aplicaciones gráficas de JAVA, con al menos 128MB en RAM, recomendable para aplicaciones grandes 512 MB en RAM, el disco duro dependerá de que tipo de sistema se desee desarrollar.

Para desarrollar un sistema completo con ayuda de este componente se recomienda usar JDK 1.6 con el cual fue desarrollado este componente.

Para que un sistema sea seguro se maneja un login y un password para realizar la conexión a la cámara. En la cámara existe al menos una cuenta con password el cual puede ser modificado, y dentro del componente se especifica el login y password para poder acceder a la cámara. Esto puede mejorar dependiendo del programador del sistema implementando un sistema de seguridad extra, dependiendo el sistema a crear combinándolo con el login y password de la cámara.

3.2.5 Atenciones y Dependencias

Como este componente fue diseñado bajo Windows, talvez uno piensa que este componente no funcionaría en otro sistema operativo como Linux, eso no puede pasar ya que JAVA es multiplataforma por la capacidad de su máquina virtual. Todo dependería de que tan adaptable hagan un sistema con ayuda de este componente y ese sistema pueda funcionar tanto en Windows como en Linux.

3.2.6 Futuras Versiones

Este componente se puede extender a más versiones, todo depende de que tanto se avance en el estudio de otras cámaras y hacer pruebas como sucedió con esta versión y así poder tener un componente completo el cual pueda interactuar a cualquier cámara IP y no solo de la línea Intellinet.

Capítulo IV

Diagramas UML

Capítulo IV. Diagramas UML

4.1 Introducción

Todo gira en torno de una visión. Un sistema complejo toma forma cuando alguien tiene la visión de cómo la tecnología puede mejorar las cosas. Los desarrolladores tienen que entender completamente la idea y mantenerla en mente mientras crean el sistema que le dé forma [11].

El éxito de los proyectos de desarrollo de aplicaciones o sistemas se debe a que sirven como enlace entre quien tiene la idea y el desarrollador. El UML (Lenguaje Unificado de Modelado) es una herramienta que cumple con esta función, ya que nos ayuda a capturar la idea de un sistema para comunicarla posteriormente a quien esté involucrado en su proceso de desarrollo; esto se lleva a cabo mediante un conjunto de símbolos y diagramas. Cada diagrama tiene fines distintos dentro del proceso de desarrollo.

Es por esto que es necesario realizar diagramas entre los que se encuentra y usaremos son:

- Diagrama de casos de uso.
- Diagrama de secuencia.
- Diagrama de colaboración.
- Diagrama de estados.
- Diagrama de clases.

4.2 Diagrama de Casos de Uso

Un Diagrama de casos de uso es una descripción de las acciones de un sistema desde el punto de vista del usuario. Para los desarrolladores del sistema, ésta es una herramienta valiosa, ya que es una técnica de aciertos y errores para obtener los requerimientos del sistema desde el punto de vista del usuario.

En la figura 4.1 se muestra nuestro Diagrama de casos de uso el cual representa el funcionamiento utilizando actores y nuestros casos de uso. Nuestro primer actor es un programa el cual interactúa con el componente. Este componente hace la tarea de interactuar con la cámara IP que es nuestro segundo actor.

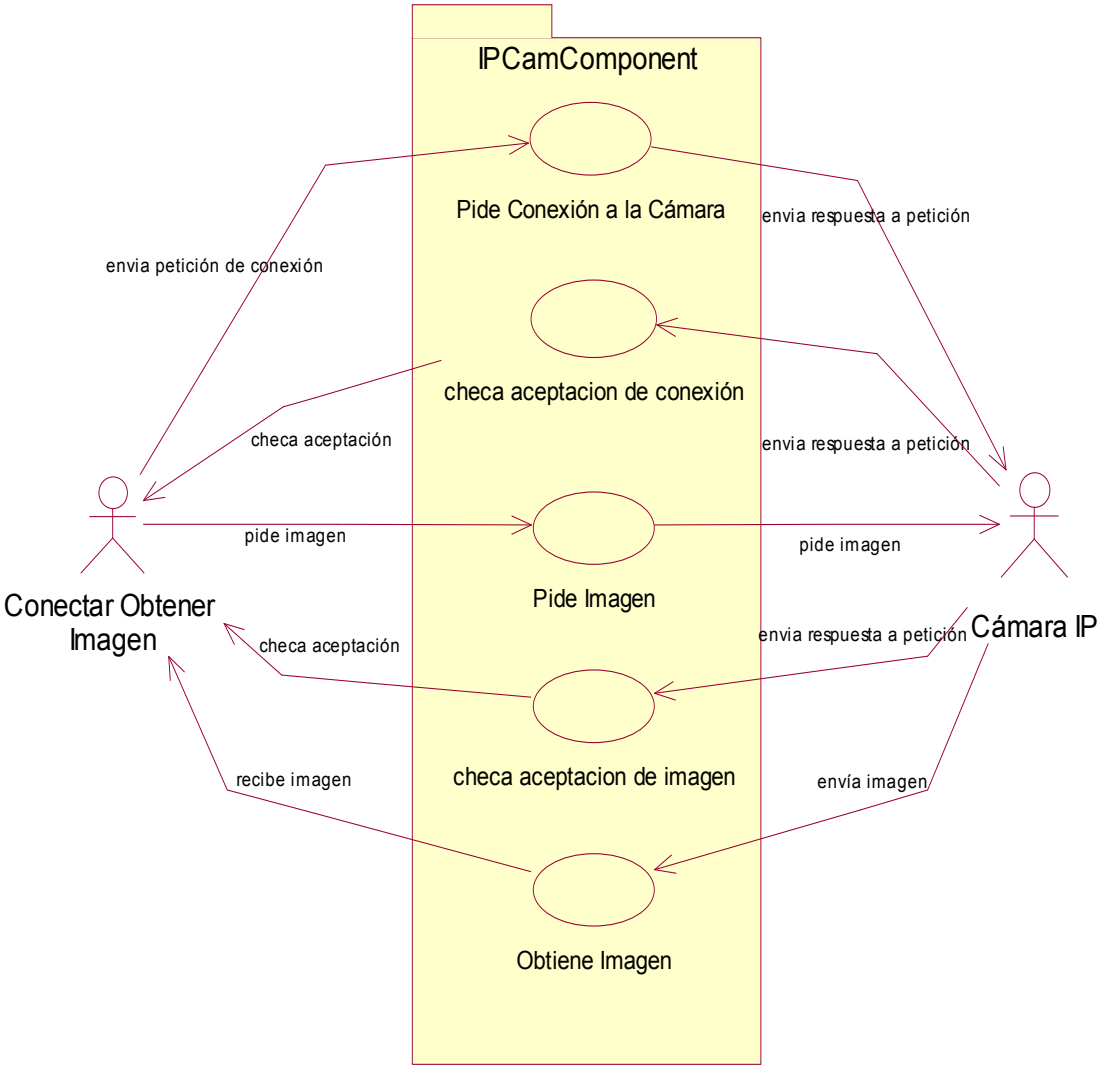


Figura 4.1 Diagrama de casos de uso

4.2 Diagrama de Secuencias

Un diagrama de secuencia muestra las interacciones entre objetos ordenadas en secuencia temporal. Muestra los objetos que se encuentran en el escenario y la secuencia de mensajes intercambiados entre los objetos para llevar a cabo la funcionalidad descrita por el escenario. En aplicaciones grandes además de los objetos se muestran también los componentes y casos de uso.

Los diagramas de secuencia, formalmente diagramas de traza de eventos o de interacción de objetos, se utilizan con frecuencia para validar los casos de uso. Documentan el diseño desde el punto de vista de los casos de uso. Observando qué mensajes se envían a los objetos, componentes o casos de uso y viendo a grosso modo cuanto tiempo consume el método invocado, los diagramas de secuencia y nos ayudan a comprender los cuellos de botella potenciales, para así poder eliminarlos. A la hora de documentar un diagrama de secuencia resulta importante mantener los enlaces de los mensajes a los métodos apropiados del diagrama de clases.

En la figura 4.2 se muestra el diagrama de secuencia correspondiente a nuestro componente desarrollado. Aquí se muestra claramente la secuencia que debe llevar este proceso de interacción con la cámara IP por medio de nuestro componente.

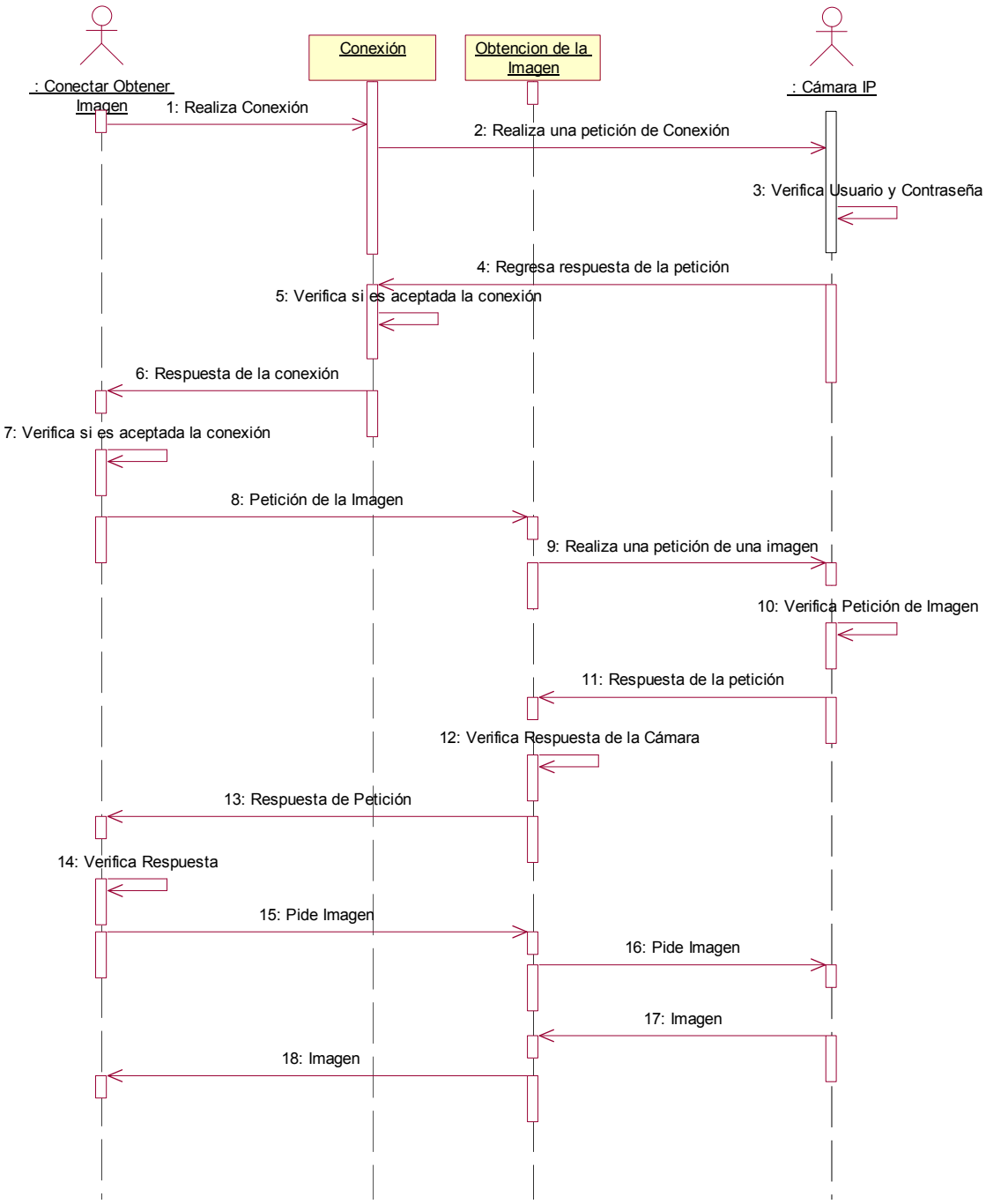


Figura 4.2 Diagrama de Secuencias

En este diagrama se muestra a nuestro primer actor que es el que va a utilizar el componente para poder interactuar con la cámara, el segundo actor es la cámara y se muestra un primer objeto el cual realiza la conexión a la cámara y un segundo objeto que es el que extrae las imágenes de la cámara.

4.2 Diagrama de Colaboración

Un diagrama de colaboración es una forma alternativa al diagrama de secuencia de mostrar un escenario. Este tipo de diagrama muestra las interacciones entre objetos organizados entorno a los objetos y los enlaces entre ellos.

Los diagramas de secuencia proporcionan una forma de ver el escenario en un orden temporal qué pasa primero, qué pasa después. Los clientes entienden fácilmente este tipo de diagramas, por lo que resultan útiles en las primeras fases de análisis. Por el contrario los diagramas de colaboración proporcionan la representación principal de un escenario, ya que las colaboraciones se organizan entorno a los enlaces de unos objetos con otros. Este tipo de diagramas se utilizan más frecuentemente en la fase de diseño, es decir, cuando estamos diseñando la implementación de las relaciones.

En la figura 4.3 se muestra el diagrama de colaboración correspondiente a este trabajo.

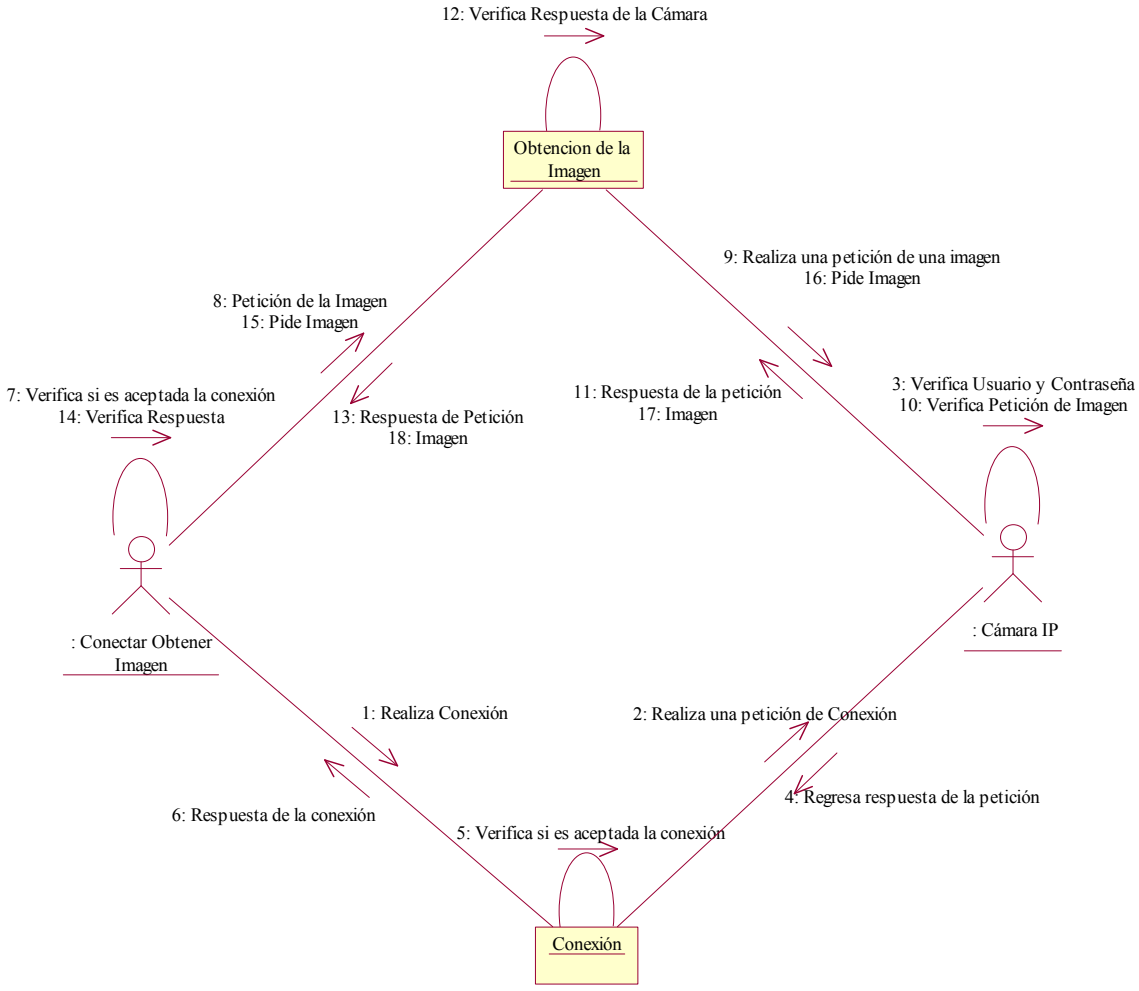


Figura 4.3 Diagrama de Colaboración

A diferencia de otras notaciones que muestran tanto el estado y el comportamiento de la clase en el diagrama de clases, UML separa el comportamiento de las clases en los diagramas de colaboración.

4.3 Diagrama de Estados

Un estado es una condición durante la vida de un objeto, de forma que cuando dicha condición se satisface se lleva a cabo alguna acción o se espera por un evento. El estado de un objeto se puede caracterizar por el valor de uno o varios de los atributos de su clase, además, el estado de un objeto también se puede caracterizar por la existencia de un enlace con otro objeto.

El diagrama de estados y transiciones engloba todos los mensajes que un objeto puede enviar o recibir. En un diagrama de estados, un escenario representa un camino dentro del diagrama. Dado que generalmente el intervalo entre dos envíos de mensajes representa un estado, se pueden utilizar los diagramas de secuencia para buscar los diferentes estados de un objeto.

En todo diagrama de estados existen por lo menos dos estados especiales inicial y final: Stara y stop. Cada diagrama debe tener uno y sólo un estado Stara para que el objeto se encuentre en estado consistente. Por el contrario, un diagrama puede tener varios estados stop.

En la figura 4.4 mostramos el diagrama de estados correspondiente.

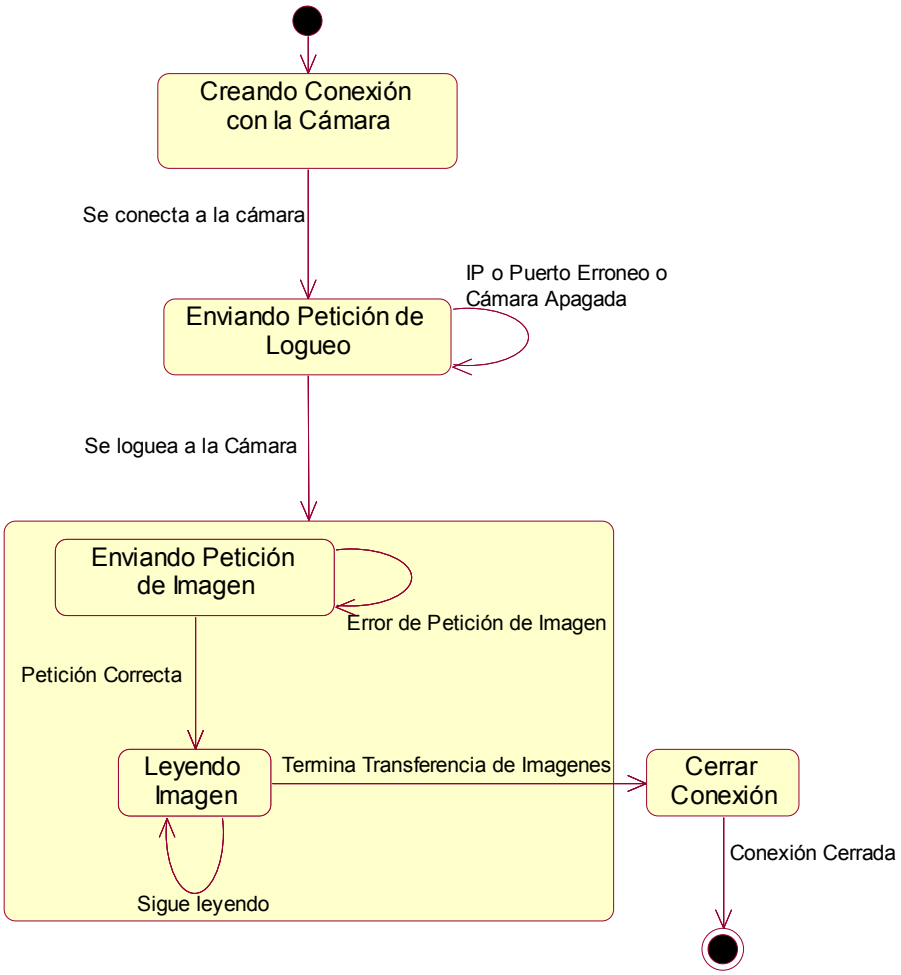


Figura 4.4 Diagrama de estados

Una transición en un diagrama de estados puede tener asociada una acción y/o una guarda, además, una transición puede disparar un evento. La acción será el comportamiento que se obtiene cuando ocurre la transición, y el evento será el mensaje que se envía a otro objeto del sistema. Por últimos, la guarda es una expresión booleana sobre los valores de los atributos que hace que la transición sólo se produzca si la condición evalúa a *trae*. Tanto las acciones como las guardas son comportamientos del objeto y generalmente se traducen en operaciones de alguna clase.

4.4 Diagrama de Clases

Los diagramas de clases son diagramas de estructura estática que muestran las clases del sistema y sus interrelaciones (incluyendo herencia, agregación, asociación, etc.). Los diagramas de clase son el pilar básico del modelado con UML, siendo utilizados tanto para mostrar cómo puede ser construido (diseño). El diagrama de clases de más alto nivel (*main class diagram*), será lógicamente un dibujo de los paquetes que componen el sistema. A su vez cada paquete tendrá un *main class diagram* que muestra las clases del paquete.

Las clases se documentan con una descripción de lo que hacen, sus métodos y sus atributos. Las relaciones entre clases se documentan con una descripción de su propósito, su cardinalidad (cuantos objetos intervienen en la relación) y su opcionalidad (cuando un objeto es opcional el que intervenga en una relación). La descripción de clases complejas se puede documentar con diagramas de estados.

En la figura 4.5 se muestra el diagrama de clases de nuestro componente, el cual está compuesto por dos clases: VariableSet y ReceiveSock.

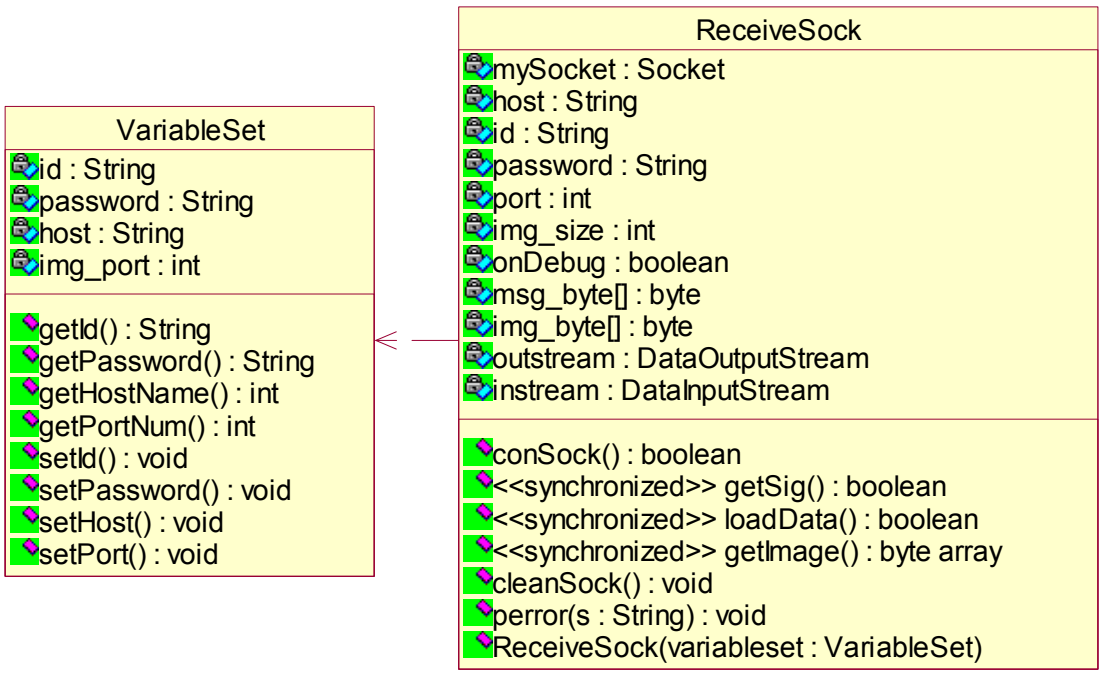


Figura 4.5 Diagrama de clases

Capítulo V

Implementación y Pruebas

Capítulo V. Implementación y Pruebas

5.1 Introducción

En este capítulo se explica la forma en que fue implementado el componente, los problemas que fueron surgiendo durante el desarrollo, así como los resultados de las pruebas realizadas para ver el buen funcionamiento del componente.

5.2 Proceso de Comunicación (Modelo Cliente-Servidor)

TCP es un protocolo orientado a conexión. No hay relaciones maestro/esclavo. Las aplicaciones, sin embargo, utilizan un modelo cliente/servidor en las comunicaciones.

Un servidor es una aplicación que ofrece un servicio a usuarios de Internet; un cliente es el que pide ese servicio. Una aplicación consta de una parte de servidor y una de cliente, que se pueden ejecutar en el mismo o en diferentes sistemas.

Los usuarios invocan la parte cliente de la aplicación, que construye una solicitud para ese servicio y se la envía al servidor de la aplicación que usa TCP/IP como transporte.

El servidor es un programa que recibe una solicitud, realiza el servicio requerido y devuelve los resultados en forma de una respuesta. Generalmente un servidor puede tratar múltiples peticiones (múltiples clientes) al mismo tiempo.

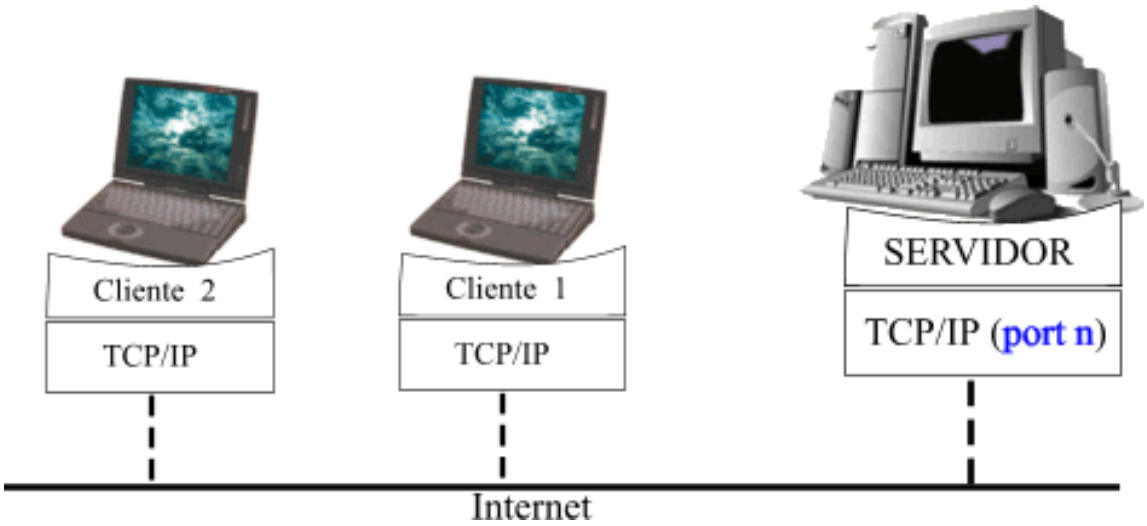


Figura 5.1 El modelo de aplicación cliente/servidor

Algunos servidores esperan las solicitudes en puertos bien conocidos de modo que sus clientes saben a que zócalo IP deben dirigir sus peticiones. El cliente emplea un puerto arbitrario para comunicarse. Los clientes que se quieren comunicar con un servi-

dor que no usa un puerto bien conocido tienen otro mecanismo para saber a qué puerto dirigirse. Este mecanismo podría usar un servicio de registro como Portmap, que utiliza un puerto bien conocido.

La arquitectura cliente-servidor sustituye a la arquitectura monolítica en la que no hay distribución, tanto a nivel físico como a nivel lógico.

5.2.1 Ventajas de la arquitectura cliente-servidor

- **Centralización del control**: los accesos, recursos y la integridad de los datos son controlados por el servidor de forma que un programa cliente defectuoso o no autorizado no pueda dañar el sistema.

- **Escalabilidad**: se puede aumentar la capacidad de clientes y servidores por separado.

El servidor de cliente es la arquitectura de red que separa al cliente (a menudo un uso que utiliza un interfaz utilizador gráfico) de un servidor. Cada caso del software del cliente puede enviar peticiones a un servidor. Los tipos específicos de servidores incluyen los servidores Web, los servidores del uso, los servidores de archivo, los servidores terminales, y los servidores del correo. Mientras que sus propósitos varían algo, la arquitectura básica sigue siendo igual.

Aunque esta idea se aplica en una variedad de maneras, en muchas diversas clases de usos, el ejemplo más fácil de visualizar es el uso actual de Web pages en el Internet. Por ejemplo, si estás leyendo un artículo en algún sitio Web como Discovery Channel, tu computadora y Web browser serían considerados un cliente, y las computadoras, las bases de datos, y los usos que componen Discovery Channel serían considerados el servidor. Cuando tu Web browser solicita un artículo particular de Discovery Channel, el servidor de ese sitio encuentra toda la información requerida para exhibir el artículo en la base de datos de Discovery, la monta en un Web page, y la envía de nuevo a tu Web browser.

5.2.2 Pasos a seguir de un Cliente y un Servidor

Para llevar a cabo este proyecto es necesario pensar en un mecanismo de comunicación entre el componente y la cámara IP, esto quiere decir, que vamos a utilizar el modelo Cliente-Servidor, el cual será explicado en esta sección.

5.2.2.1 Proceso Cliente

El programa cliente debe seguir varios pasos para comunicarse con un equipo homólogo o servidor. Estos pasos tienen que seguir una secuencia particular. Por supuesto, uno se puede preguntar: ¿Por qué no se reemplazan todos estos pasos con menos llamadas? En medio de cada paso, el programa puede seleccionar de muchas opciones. No obstante, algunos pasos son opcionales. Si el cliente omite algunos pasos, normalmente el sistema operativo rellena esas opciones con los valores predeterminados.

Puede seguir algunos de estos pasos básicos para crear un *socket*, configurar el *host* de destino, establecer el canal a otro programa de red y cerrarlo. La figura 5.2 muestra gráficamente los pass que el cliente toma para conectarse a un servidor.

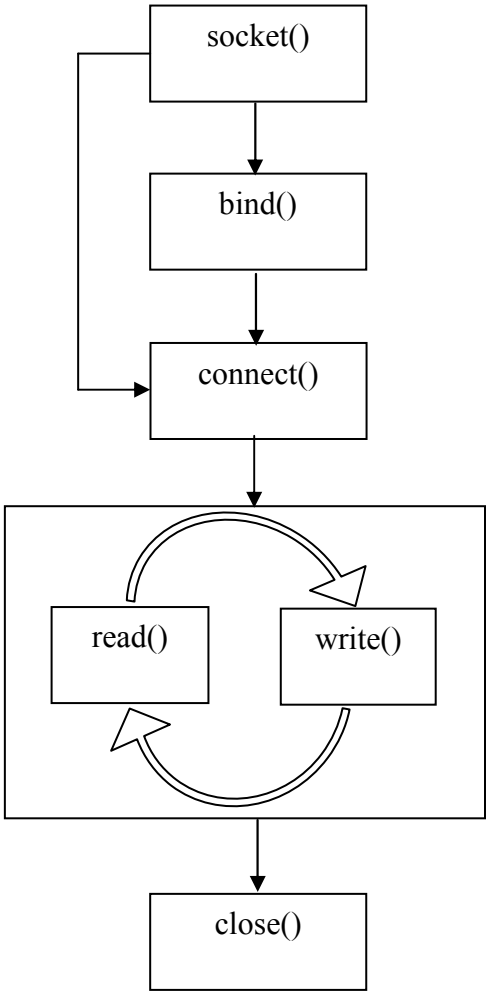


Figura 5.2 Proceso Cliente

En la siguiente lista se describe cada paso [13]:

1. Crear *socket.* Se selecciona de diversos dominios de red (por ejemplo, Internet) y clases de *socket* (como flujo).
2. Configurar las opciones del *socket* (opcional). Se dispone de muchas opciones que afectan al comportamiento del *socket.* Una vez abierto el *socket*, el programa puede cambiar estas opciones en cualquier momento.
3. Asociar con una dirección-puerto (opcional). Se aceptan conexiones de todos o de una sola dirección IP, y se establece un puerto de servicio. Si se omite, el sistema operativo asume cualquier dirección IP y asigna un número de puerto aleatorio.
4. Conectar a un equipo servidor (opcional). Se extiende y establece un canal bidireccional entre el programa local y otro programa de red. Si se omite, el programa utiliza una comunicación dirigida o sin conexión.
5. Cerrar la conexión parcialmente (opcional). Se restringe el canal de envío o de recepción. Se puede utilizar este paso después de la duplicación del canal.

6. Enviar-recibir mensajes (opcional). Una razón para prescindir de cualquier E/S podría incluir comprobación de disponibilidad de *host.*
7. Cerrar la conexión. Por supuesto este paso es importante si los programas no cierran las conexiones terminadas, los programas que consumen bastante tiempo de CPU pueden agotar casualmente los descriptores de archivo.

5.2.2.2 Proceso Servidor

El proceso para la conexión de un servidor siempre comienza con la creación del *socket.* Así como el cliente necesitaba llamadas específicas en determinados momentos, el servidor trabaja de un modo similar pero añade unas pocas llamadas extras al sistema. El servidor utiliza la llamada del sistema **socket(),** pero debe hacer un trabajo extra que ra opcional para el cliente, como puede verse ilustrado en la figura 5.3.

El programa cliente que se escribió anteriormente seguía el diagrama de cliente (figura 5.2). El orden de las llamadas que realizaba el cliente es: **socket(), connect(), read(), write() y close().** La llamada del sistema **blind()** no era necesario porque el sistema operativo realizó esa función en su lugar. El número de puerto no se necesitaba porque el programa llamaba al servidor. El cliente siempre realizaba una conexión activa porque la persigue enérgicamente.

Los servidores, por otro lado, necesitan proporcionar un número de puerto específico y consistente a los programas cliente si les va a prestar servicio. El diagrama de un servidor muestra unas pocas diferencias respecto al del cliente. El programa servidor que se escriba deberá utilizar las llamadas de sistema **socket(), blind(), listen(), accept(), y close().** Y mientras el programa cliente es una conexión activa, el servidor es una conexión pasiva. Las llamadas de sistema **listen() y accept()** crean una conexión sólo cuando el cliente pide una conexión (similar a la acción de responder al timbre de un teléfono).

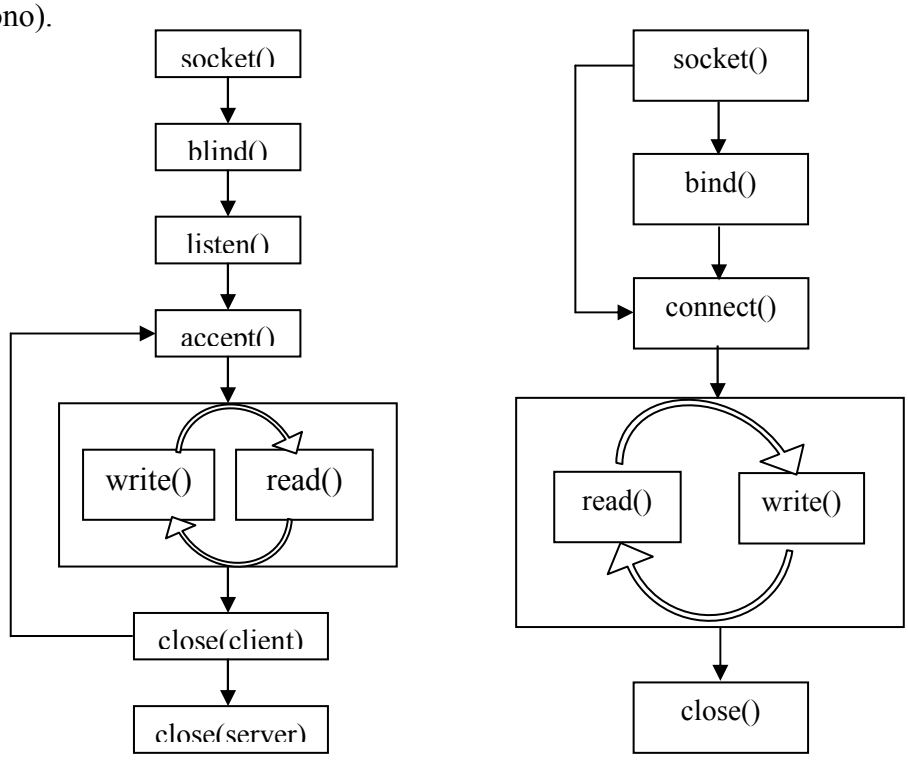


Figura 5.3 Proceso Servidor

Los flujos de programa para un cliente y un servidor son similares pero tienen diferencias muy dispares en el modo en que se conectan a la red. Éste es un esquema de las llamadas de sistema para los programas cliente servidor [13].

Los servidores pueden ser apátridas o stateful. Un servidor apátrida no guarda ninguna información entre las peticiones. Un servidor stateful puede recordar la información entre las peticiones. El alcance de esta información puede ser global o sesión-específico. Un servidor del HTTP para las páginas estáticas del HTML es un ejemplo de un servidor apátrida mientras que Apache Tomcat es un ejemplo de un servidor stateful.

La interacción entre el cliente y el servidor se describe a menudo usando diagramas de secuencia. Los diagramas de secuencia se estandardizan en el UML.

Otro tipo de arquitectura de red se conoce como arquitectura del par-a-par porque cada nodo o caso del programa es un "cliente" y un "servidor" y cada uno tiene responsabilidades equivalentes. Ambas arquitecturas están en uso amplio.

En nuestro caso el componente es el cliente el cual hará las peticiones a nuestro servidor que será nuestra cámara IP.

La comunicación se hará mediante sockets en java y se utilizarán algunos códigos de estado de respuesta del HTTP/1.1, todo esto explicado brevemente en otra sección.

5.3 Interacción con la Cámara IP

Para desarrollar con éxito el componente se optó por usar sockets para establecer la comunicación con la cámara, ya que, con los sockets es posible crear un cliente (que sería el componente) y hacer las peticiones al servidor (en este caso nuestro servidor es la cámara).

Para hacer posible esta comunicación es necesario utilizar los códigos de estado del HTTP/1.1

5.3.1 Sockets como parte de la solución

Los sockets son un sistema de comunicación entre procesos de diferentes máquinas de una red. Más exactamente, un socket es un punto de comunicación por el cual un proceso puede emitir o recibir información.

Fueron popularizados por Berkeley Software Distribution, de la Universidad Norteamericana de Berkeley. Los sockets han de ser capaces de utilizar el protocolo de streams TCP (Transfer Control Protocol) y el de datagramas UDP (User Datagram Protocol).

Utilizan una serie de primitivas para establecer el punto de comunicación, para conectarse a una máquina remota en un determinado puerto que esté disponible, para

escuchar en él, para leer o escribir y publicar información en él, y finalmente para desconectarse.

Con todas las primitivas se puede crear un sistema de diálogo muy completo.

En la figura 5.2 se muestra con un diagrama el funcionamiento de una conexión socket.

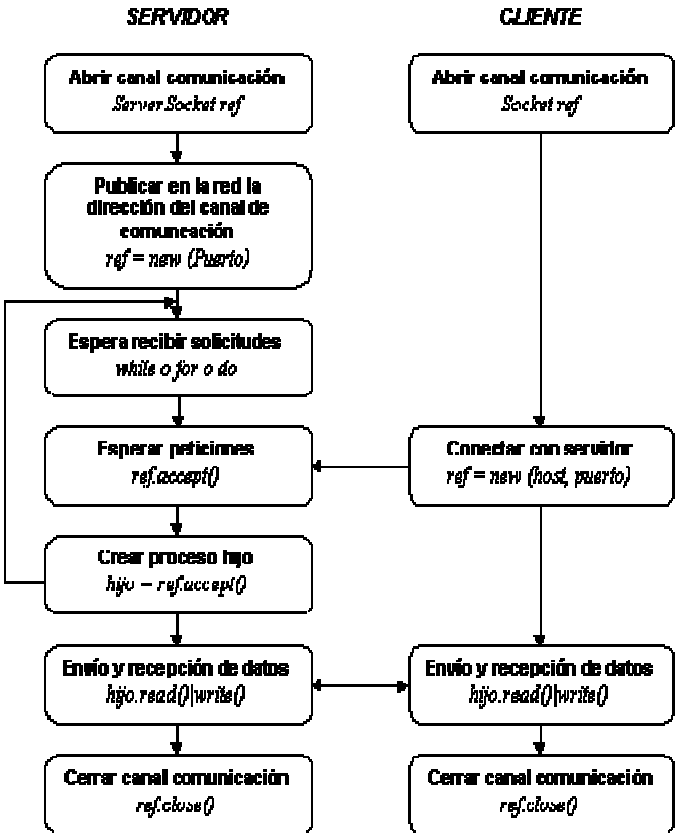


Figura 5.2 Funcionamiento de una conexión Socket [7]

5.3.2 Conexión con la Cámara IP

Para establecer una conexión con la cámara IP fue necesario estudiar sus características técnicas para poder programar adecuadamente, ya que cada cámara cuenta con una configuración diferente.

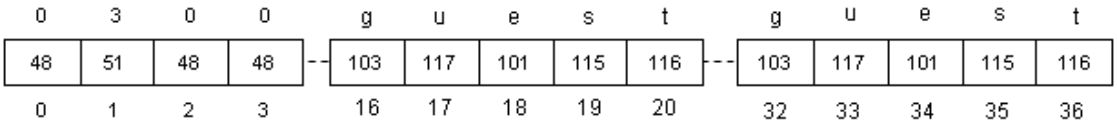
Dado que es una conexión IP, creamos un programa el cual funciona como cliente. El programa cliente hace lo siguiente:

1. Conexión a la cámara mediante un socket cliente especificándole la dirección IP y el puerto de la cámara. Un ejemplo de eso sería:

mySocket = new Socket(server, port);

Donde **server** es la dirección IP y **port** el número de puerto de la cámara.

2. Hacemos una comunicación mediante códigos de estado [14] (véase RFC 2616) para obtener el permiso de acceso al servidor de la cámara y agregando el **usuario** y **password** mediante la siguiente secuencia:
    - Se crea un arreglo de bytes de 48 casillas de la siguiente forma:



El número **0300** es un código de estado, el cual indica a la cámara que se desea iniciar una sesión dados un nombre de usuario con su respectiva contraseña que en este caso el usuario y contraseña es **guest**.

El código de estado, el usuario y la contraseña deberán ser transformados a bytes ya que la comunicación con la cámara es a base de bytes.

3. Se envía el arreglo de bytes a la cámara. La cámara lee el arreglo de 16 en 16 casillas, es por eso que se envía de esa forma.

4. Una vez que se envía la información, la cámara regresa una respuesta, el cual es un código de estado, este puede ser:

    - **301:** Indica que la autenticación del usuario fue con éxito.
    - **302:** Indica que la autenticación del usuario falló.
    - **9000:** El mensaje enviado a la cámara es inválido.

5.3.3 Obtención de las imágenes

Una vez obtenida una conexión estable con la cámara podemos obtener las imágenes que está captando. Esto se lleva a cabo con un intercambio de mensajes adecuado con la cámara, esto quiere decir, usando los códigos de estado correspondientes para esta acción.

1. Para empezar a interactuar es necesario realizar una petición de la imagen con el código de estado **0110.**

2. La cámara nos manda una respuesta la cual contiene lo siguiente:

    - Un código de estado como:
        - **120:** Mensaje de error *Server Full* que indica que está ocupado y no puede atender la petición.
        - **130:** Mensaje de éxito que indica que la imagen está disponible.
    - El tamaño de la imagen en bytes.

3. Se crea un arreglo de bytes con el tamaño ya obtenido anteriormente y se lee de la cámara la imagen. Para poder utilizar la imagen se debe crear a partir del arreglo de bytes.

Una vez que uno ya no desea más imágenes de la cámara se debe cerrar la conexión del socket antes realizada.

5.4 Pruebas

Hicimos pruebas con el componente desarrollado para verificar su grado de funcionalidad y efectividad.

Se hizo un Applet el cual se conecta a la cámara, obtiene las imágenes y las muestra en forma de video. Este Applet cuenta con un Panel de operaciones y un Visor de Sucesos, el Panel de Operaciones cuenta con lo siguiente (Figura 5.3):

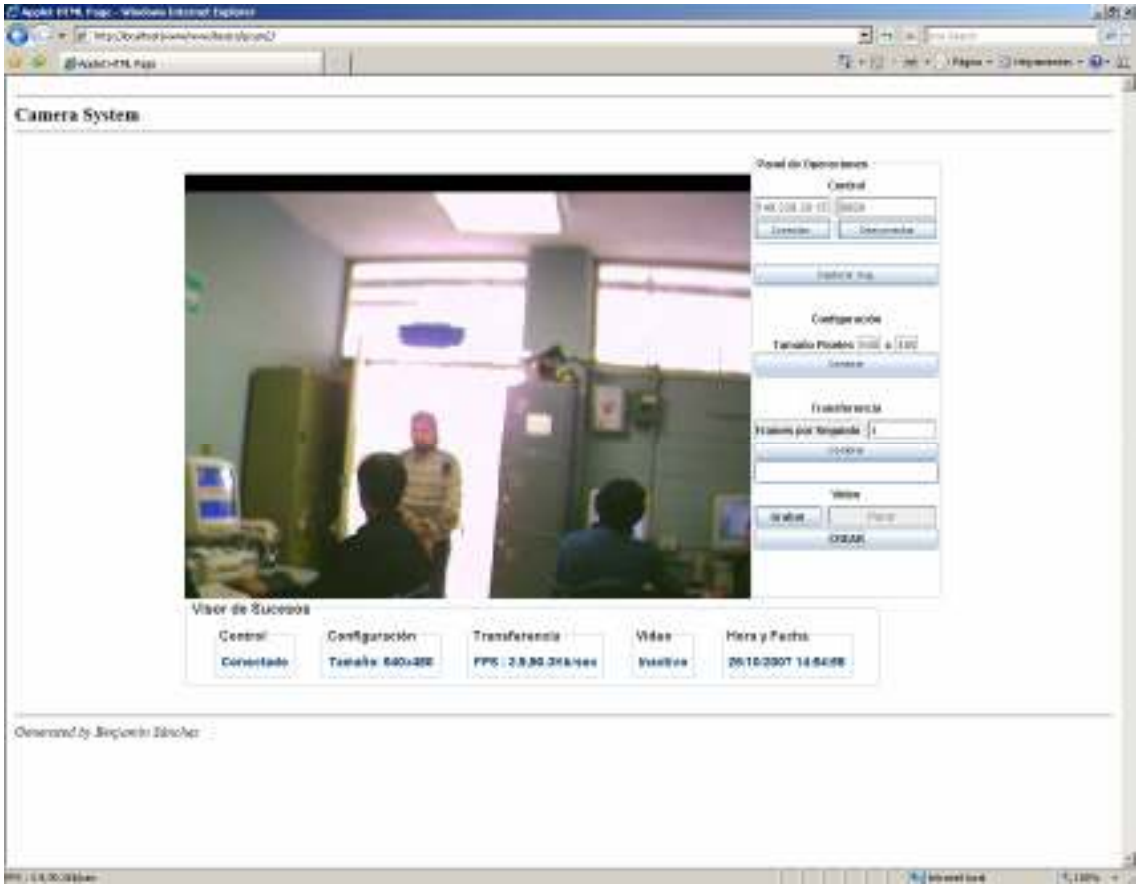


Figura 5.3 Applet usando una cámara IP

1. **Control:** Existe la posibilidad de dar la dirección IP y puerto de una de las cámaras. Hay 2 botones que tienen la función de Conectar y Desconectar a la cámara y un botón “Capturar Img.” el cual abre una aplicación que muestra una imagen dada por la cámara y que en este ejemplo le aplica un filtro de Negativo (Figura 5.4).

Figura 5.4 Aplicación Java que obtiene una imagen de la cámara y aplica el filtro de Negativo

2. **Configuración:** Nos ofrece la opción de cambiar el tamaño de la imagen en pixeles, recomendable usar como máximo un tamaño de 640x480 píxeles.

3. **Transferencia:** Permite cambiar los frames por segundo de transferencia de imágenes, normalizada a 4 fps.

4. **Video:** Nos permite guardas imágenes en disco duro y en base a eso crear un video en formato AVI para así visualizar en QuickTime como se muestra en la figura 5.6.

Figura 5.6 Video creado desde el Applet

En la parte de Visor de Sucesos simplemente se muestran las acciones que se hacen en el applet como:

- Conectar – Desconectar.
- Configuración: Muestra el tamaño actual de la imagen en píxeles.
- Transferencia: Muestra los frames por segundo.
- Video: Indica si está activa la grabación.
- Hora y Fecha: Muestra la hora y fecha del sistema.

El componente nos permite elegir un IP para conectarnos, en nuestro ejemplo eso nos permite abrir varias aplicaciones con diferentes IP de cámara (Figura 5.7)

Figura 5.7 Dos aplicaciones Applet con 2 cámaras distintas

Capítulo VI

Conclusiones y Perspectivas

Capítulo VI. Conclusiones y Perspectivas

Con la información recabada acerca de cámaras IP y sus aplicaciones como lo es en la medicina o en vigilancia IP, es claro que muchas instituciones pueden emigrar a este tipo de tecnologías y dejar atrás las WebCam y los sistemas de CCTV. Esto es porque el costo de inversión en esta tecnología de cámaras IP al paso del tiempo y con mejoras en la tecnología.

Se logró crear un componente que interactuara con una cámara IP (Cámara IP de la serie Intellinet), esto es, que se hiciera una conexión exitosa y la obtención de imágenes; imágenes que pueden ser procesadas según el problema a enfrentar.

Se logró crear una aplicación, el cual, utilizando el componente se pudiera obtener las imágenes y mostrarlas como si fuera video. En esta aplicación se puede cambiar de una cámara a otra, ya que el componente nos permite darle una dirección IP y un número de puerto donde esté la cámara. Y como se mencionó, las imágenes se pudieron procesar aplicando un filtro de negativo así como poder crear video con formato .MOV que puede ser reproducido en QuickTime.

Esto no es todo, sabemos que solo se puede utilizar el componente a una sola serie de cámaras IP (Intellinet) ya que cada fabricante define sus propios modos de interactuar con la cámara. Es por eso que este proyecto está abierto para seguir estudiando el funcionamiento de más cámaras y poder extender este componente para el uso con más series de cámaras.

Apéndice A

Cámara IP

Apéndice A. Cámara IP

¿No sería útil poder hacer seguimiento de cada una de las personas que atraviesa un punto de entrada de alta seguridad, o comprobar falsas alarmas en establecimientos desde el confort de su casa? Estas y muchas otras aplicaciones interesantes ahora son posibles gracias a la llegada de la tecnología de la cámara IP.

Comenzando con la primera WebCam del mundo en 1991, preparada para monitorizar remotamente el nivel de café en la cafetera de la Universidad de Cambridge, el mercado y el uso de la tecnología de la cámara IP ha crecido considerablemente. Soluciones de seguridad en bancos, aeropuertos y casinos son sólo unos pocos ejemplos o aplicaciones profesionales basadas en cámaras IP, que son algo común en nuestros días. La compañía de investigación Frost & Sullivan predice que para 2005 el mercado mundial de las cámaras IP alcanzará aproximadamente los 441 Millones de dólares, lo que representa un aumento de más de diez veces en tan sólo cinco años [1].

¿Por qué usar cámaras IP y dónde?

Los últimos avances han hecho posible conectar cámaras directamente a una red de ordenadores basada en el protocolo IP. La tecnología de las cámaras IP permite al usuario tener una cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de la red o de Internet. El acceso puede ser restringido, de manera que sólo las personas autorizadas puedan ver las imágenes, o el vídeo en directo puede ser incorporado al Web Site de una compañía para que todo el mundo pueda verlo.

Si un edificio está equipado con una red IP, entonces ya cuenta con la infraestructura necesaria para incorporar las cámaras IP. Una cámara de red realiza la mayoría de las funciones que lleva a cabo una cámara analógica estándar de circuito cerrado, pero proporciona más funcionalidades a un precio notablemente inferior. Dado que las cámaras IP se conectan directamente a la red existente a través de un puerto Ethernet, las empresas pueden ahorrar miles de Euros al no precisar en sus instalaciones un cableado coaxial adicional como necesitan las cámaras analógicas. Cuando se dispone de ordenadores, ya no se necesita ningún equipamiento adicional para ver las imágenes de la cámara de red. Las imágenes pueden verse de una forma muy sencilla desde un navegador Web y, en soluciones de seguridad más complejas, con la ayuda de un software dedicado.

Si la instalación cuenta además con cámaras analógicas, la adición de un servidor de video puede hacer que las imágenes estén disponibles en cualquier localización que fuera necesaria.

La Tecnología de la Cámara IP

Una cámara de red tiene su propia dirección IP y características propias de ordenador para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara IP puede describirse como una cámara y un ordenador combinados. Se conecta directamente a la red como cualquier otro dispositivo de red e incorpora software propio para

servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico. También incluye entradas para alarmas y salida de relé. Las cámaras IP más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.

El componente cámara de la cámara IP captura la imagen, que puede ser descrita como luz de diferentes longitudes de onda, y la transforma en señales eléctricas. Estas señales son entonces convertidas del formato analógico al digital y son transferidas al componente ordenador donde la imagen se comprime y se envía a través de la red.

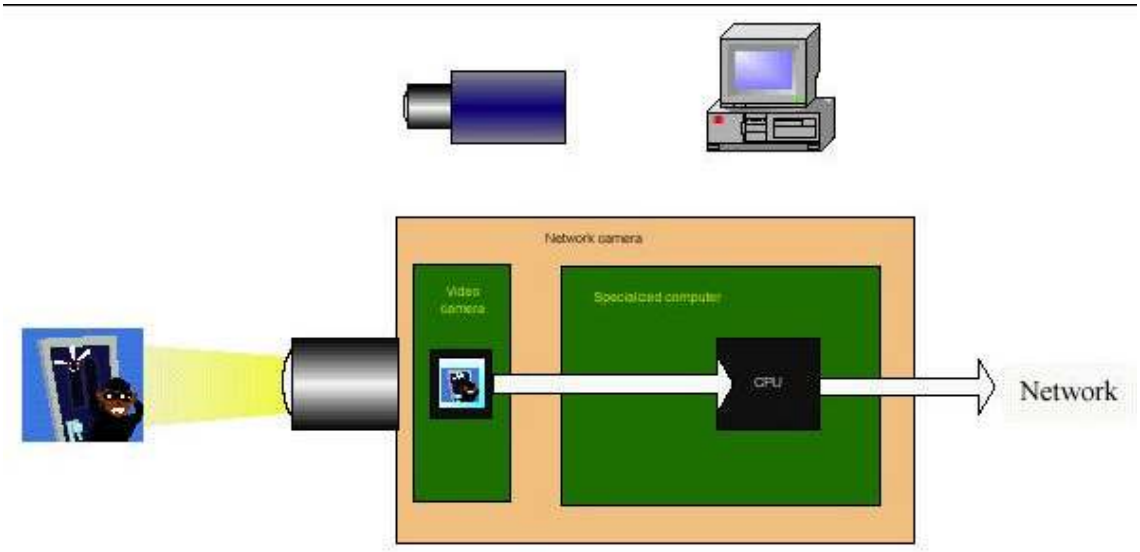


Figura 6.1 Interior de una Cámara IP

Examinemos más en profundidad los componentes de la cámara IP (Figura 6.2).

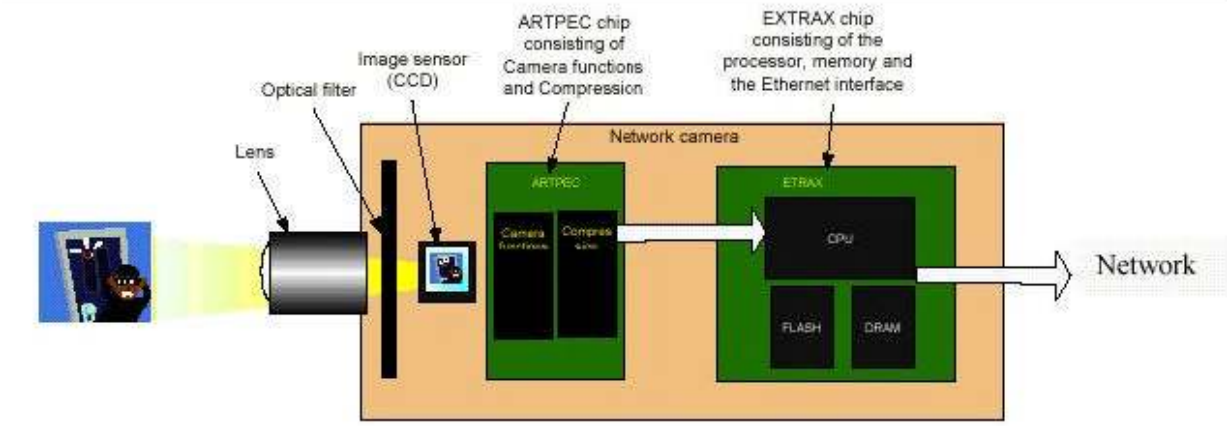


Figura 6.2 Funcionamiento de una Cámara IP

La **lente** de la cámara enfoca la imagen en el **sensor de imagen** (CCD). Antes de llegar al sensor la imagen pasa por el **filtro óptico** que elimina cualquier luz infrarroja de forma que se muestren los colores correctos. El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas seña-

les eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.

Las funciones de cámara gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las llevan a cabo el controlador de cámara y el chip de compresión de vídeo. La imagen digital se comprime en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la red.

La conexión Ethernet de la cámara, una solución optimizada para la conexión de periféricos a la red. Incluye una CPU de 32 bits, conectividad Ethernet 10/100 MB/s, funcionalidad de Acceso Directo a Memoria (DMA) y una amplia variedad de interfaces de entrada y salida. La CPU, y la memoria flash y DRAM representan los "cerebros" o funciones de ordenador de la cámara y están específicamente diseñados para su aplicación en redes.

Juntos, gestionan la comunicación con la red y el servidor Web.

La cámara IP en acción

Ya hemos visto las partes o componentes principales de la cámara IP. Pero, ¿Cómo funciona en términos de adquisición y compresión de imágenes, y de su posterior transferencia a través de una red para visualización remota?

Conectar la cámara a la red.

Para la mayoría de los sistemas de vigilancia de circuito cerrado es relativamente sencillo ampliar el número de cámaras y monitores dentro de un edificio, sin embargo ver esas imágenes desde otra localización es otra historia. En cualquier caso, si un edificio está equipado con una red ya existe la infraestructura necesaria para incorporar nuevas cámaras y de forma dinámica ampliar cuando y donde el vídeo puede ser visto.

Las redes IP

En la actualidad TCP/IP es el protocolo de comunicación más común, utilizado para Internet y para casi todas las redes que se instalan. En una oficina típica la mayoría de los ordenadores están conectados a través de una red Ethernet, por ejemplo en una Red de Área Local (LAN). Cada dispositivo de una LAN debe tener una dirección única, la dirección IP, que permite conectar directamente a Internet. Los ordenadores actuales y los dispositivos de red tienen una alta capacidad para comunicar simultáneamente con varias unidades diferentes. Una cámara IP de gama alta, puede enviar imágenes a diez o más ordenadores simultáneamente. Con una cámara IP enviar imágenes a un servidor Web externo, en vez de hacerlo directamente a los destinatarios, permite que se envíe video en tiempo real a un número ilimitado de espectadores.

Almacenar y transferir imágenes

Para conectar a Internet están disponibles actualmente muchos tipos diferentes de transmisión. Entre ellos se incluyen los módems estándar y RDSI, los módems de tele-

visión por cable, las conexiones dedicadas de alta velocidad, el ADSL y las conexiones Ethernet a 10, 100 y 1000 Megabites. Además, también pueden usarse los módems de los teléfonos móviles y otras opciones de redes inalámbricas. Las imágenes digitales pueden almacenarse en discos duros.

Habitualmente en un único disco duro pueden almacenarse millones de imágenes. Cuando el disco duro está lleno, el ordenador puede programarse para borrar automáticamente las imágenes más antiguas y liberar espacio para otras nuevas. Existen muchos sistemas de seguridad profesionales que gestionan las completas aplicaciones de seguridad disponibles actualmente en el mercado.

Técnicas de compresión y resolución de imagen

La resolución de las imágenes digitales se mide en píxeles. La imagen más detallada es la que tiene más datos y por tanto mayor número de píxeles. Las imágenes con más detalles ocupan más espacio en los discos duros y precisan mayor ancho de banda para su transmisión.

Para almacenar y transmitir imágenes a través de una red los datos deben estar comprimidos o consumirán mucho espacio en disco o mucho ancho de banda. Si el ancho de banda está limitado la cantidad de información que se envía debe ser reducida rebajando el número de frames por segundo o aceptando un nivel de calidad inferior. Existen múltiples estándares de compresión que resuelven los problemas de número de frames por segundo y calidad de imagen de diferentes formas. De los estándares más comunes tanto el JPEG como el MPEG transmiten vídeo de alta calidad, mientras que los estándares-H, usados normalmente en videoconferencia, no generan imágenes claras de objetos que se mueven a gran velocidad.

Requerimientos de luz de las cámaras

La razón más habitual de una calidad de imagen pobre es la insuficiencia de luz. Con un nivel de luz muy bajo el nivel de los colores será sombrío y las imágenes borrosas. El nivel de luz se mide en Lux. La luz solar fuerte tiene aproximadamente 100,000 Lux, la luz diurna tiene aproximadamente 10,000 Lux y la luz de una vela tiene aproximadamente 1 Lux.

Habitualmente se precisan al menos 200 Lux para capturar imágenes de buena calidad. Las áreas brillantes deben ser evitadas dado que las imágenes pueden resultar sobre-expuestas y que los objetos aparezcan muy oscuros. Este problema ocurre igualmente cuando se intenta capturar un objeto con luz negra. Una cámara ajusta la exposición para conseguir una buena media de nivel de luz para la imagen, pero el contraste de color entre el objeto y el fondo influye en la exposición. Para evitar este problema los objetos oscuros pequeños deberían disponerse delante de un fondo oscuro para conseguir el color y el contraste correctos.

Cómo reconocer una cámara IP

Para mucha gente una cámara IP y una WebCam son lo mismo, sin embargo son dos cosas muy diferentes. Como se muestra en la figura 6.3 una cámara IP tiene su propia

"inteligencia" y no necesita estar conectada a un ordenador para establecer una conexión a través de la red.

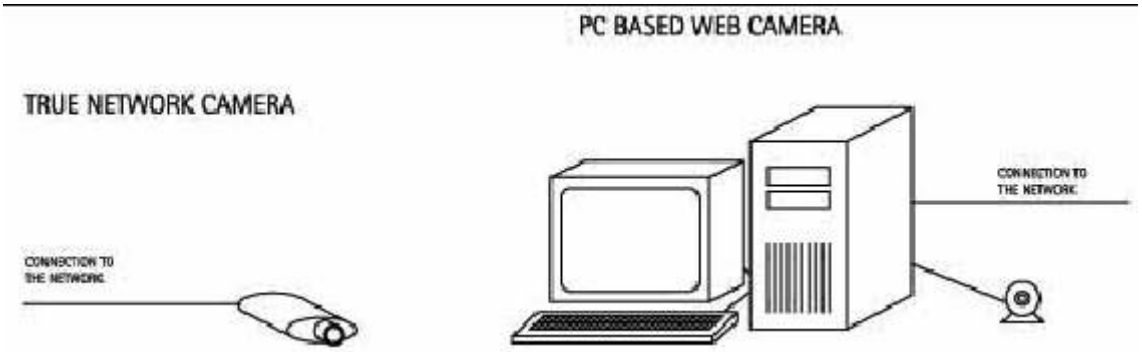


Figura 6.3 Cámara IP y WebCam

El futuro de las cámaras IP

Hace más de 10 años algunos profesores de la Universidad de Cambridge usaron un prototipo de tecnología de cámara IP para asegurar que podrían contar con una taza de café caliente.

Unos pocos años después, tras el nacimiento de la Web, pusieron imágenes de la cafetera a disposición de cualquiera que tuviera una conexión a Internet. Probablemente debido en parte a la falta de atractivo de los contenidos de la Web, la Cafetera de Cambridge fue un gran hito, recibió más de 2.4 millones de visitantes, y se convirtió en la primera aplicación popular para la tecnología de cámara IP: la atracción Web. La atracción Web permaneció como un gran mercado durante los primeros días de crecimiento de las cámaras IP. A medida que creció el conocimiento y el interés en ellas, las aplicaciones del mercado de la seguridad basadas en la monitorización remota y en la vigilancia se han convertido en el mayor mercado.

Al igual que 100 cámaras IP ofreciendo monitorización las 24 horas del día los 7 días de la semana a espectadores de todas partes del mundo está a años luz de la primera ***cafeteracam***, el futuro de las cámaras IP es ilimitado. En el futuro, cámaras "inteligentes" dotadas de sofisticadas CPU's no sólo constituirán los ojos de la gestión de la seguridad, sino que serán igualmente sus "cerebros". Estas cámaras inteligentes tendrán la capacidad de tomar decisiones a partir de determinados estímulos y llevarán a cabo acciones que aporten valor, aumenten la seguridad, o aquello que necesite la aplicación.

Apéndice B

Los 10 Principales Mitos sobre el Video en red

Apéndice B. Los 10 principales mitos sobre el video en red

¿Por qué hay percepciones erróneas acerca de la tecnología de Vigilancia IP?

Al igual que con cualquier nueva tecnología, siempre debe haber un periodo inicial de educación al mercado. Cuanto más complicada sea la tecnología o arraigada esté la tecnología actual y su modelo de negocio, más largo será el periodo de educación del mercado. Durante esta fase de aprendizaje es natural que existan vacíos de conocimiento y malas interpretaciones. Es en estas condiciones en las que las percepciones erróneas y los mitos pueden crecer y promoverse.

La tecnología de la Vigilancia IP no es especialmente complicada pero la parte IP no es natural en el entorno de la seguridad ya que entra en el mundo de las TI, territorio desconocido para muchos. En este sentido una nueva tecnología y unas condiciones totalmente nuevas pueden representar una amenaza para el status quo. El hecho de que la Vigilancia IP compita directamente con el Grabador Digital de Vídeo (DVR) crea un elevado número de conflictos, no inferiores al hecho de que desafía la asunción actual de que la tecnología del DVR y las cámaras analógicas representan un punto final, y por tanto la mejor tecnología. Afrontémoslo, existe una gran industria, desde fabricantes a instaladores e integradores acercándose a los usuarios y sus organizaciones, que tienen un especial interés en que el DVR sea la tecnología dominante. Además de estas condiciones de mercado "creadoras de mitos" considere que la industria de la seguridad es una en la que soluciones propietarias de una única marca son comunes y esperadas. Las soluciones de Vigilancia IP combinan productos y servicios de diferentes fabricantes. Este punto está empezando a interesar al usuario ya que se diferencía bastante en lo relativo a condiciones y expectativas. Ahora que comprendemos cuales son las razones de las malas interpretaciones y las medias verdades que han aparecido alrededor de la Vigilancia IP examinemos algunas de ellas más de cerca.

Los mayores mitos de la vigilancia IP

Hay un número de mitos, grandes y pequeños, alrededor de la tecnología de Vigilancia IP.

Se presentan 10 de los mitos más escuchados y los hemos organizado en dos categorías: generales y técnicos [1]. Primero se abordará los más generales y después algunas de las malas interpretaciones técnicas.

Mito 1: Los DVR's representan la última y mejor tecnología de CCTV de seguridad

Realidad: Además de haber gente que cree que los grabadores de vídeo digitales son la última y mejor tecnología, muchos piensan que en el DVR todo es digital y que es una tecnología de red, y no es así.

Un DVR tiene un importante número de ventajas si lo comparamos con un VCR (video casete recorder): no precisa cambios de cinta, proporciona una calidad de imagen constante y capacidades de búsqueda más rápidas. Sin embargo precisa cable analógico, que puede distorsionar la calidad de la imagen, además resultan bastante caros para equipar con ellos un edificio o una instalación industrial. La Vigilancia IP tiene todas las ventajas del DVR y además:

Escalabilidad: La Vigilancia IP escala de una a miles de cámaras en incrementos de una unidad. No tiene la limitación de los 16 canales. La Vigilancia IP ofrece cualquier ratio de imágenes por segundo en cualquier momento, no hay limitaciones.

Infraestructura más económica: La mayoría de los edificios de oficinas y otros tipos de instalaciones cuentan con infraestructura de cable de par trenzado (cable de red), de forma que la Vigilancia IP no precisa cableado adicional (uno de los gastos principales de una instalación de CCTV).

Sólo un tipo de red (IP) conecta y gestiona los datos, la voz, el vídeo, … de una empresa y hace que la gestión sea más sencilla y económica.

Accesibilidad remota: Cualquier secuencia de video, en directo o grabada, puede ser visualizada y controlada de forma segura desde cualquier localización del mundo a través de redes inalámbricas o con cable.

Inteligencia a nivel de cámara: Detección de movimiento, gestión de eventos, entrada para sensores, salida relé, fecha y hora y otras capacidades propias permiten a la cámara tomar decisiones inteligentes sobre cuándo enviar alarmas y a quién, cuándo enviar vídeo, e incluso a qué ratio de imágenes por segundo o con qué resolución debe enviar el vídeo.

Menores costes de sistema: Para muchas instalaciones, el sistema de Vigilancia IP ha demostrado ser una alternativa con un precio inferior. Redes estándares y abiertas, equipamiento de servidores y almacenamiento, permiten que haya competencia y opciones en el mercado frente a la aproximación de solución propietaria de un único fabricante que resulta el mundo del DVR. Y esto es sólo lo relacionado con el hardware, si añade los costes de instalación y mantenimiento y los beneficios del rendimiento, es claro que la Vigilancia IP ahorra grandes cantidades de dinero. Contrariamente a la opinión popular, el DVR no es una solución de punto final, sino un hito en el continuo desarrollo de la tecnología de CCTV. A medida que el mercado analice más detenidamente el DVR se dará cuenta de que representa un pensamiento basado en soluciones anticuadas y propietarias. La tecnología de la Vigilancia IP ha demostrado en poco tiempo que es superior a la tecnología del DVR. Hay una enorme diferencia entre las dos tecnologías y el mercado se encuentra en un momento en el que está empezando a comprender este punto crítico.

Mito 2: La tecnología IP no está suficientemente probada. Si es mejor ¿Por qué los proveedores de soluciones de seguridad no las venden más?

Realidad: Este mito está más relacionado con la estructura del mercado de la seguridad y con sus prácticas de compra que con el rendimiento y la fiabilidad de las soluciones de Vigilancia IP.

La Vigilancia IP es una tecnología relativamente nueva y algunos de los principales jugadores del mercado están actualmente ofreciendo una tecnología competidora, el DVR. Es natural que esas empresas quieran proteger sus inversiones en soluciones orientadas al DVR. En relación a esto la aparición de una nueva tecnología y una nueva mentalidad precisa construir un conocimiento y una infraestructura entre los integradores, consultores y otros agentes que influyen en la industria, con el fin de superar el status quo normal de pensamientos y procedimientos. Cuantos de nosotros recordamos que decíamos que las máquinas de escribir proporcionaban toda la tecnología necesaria, ¿Quién necesita un procesador de textos?, ¿Qué decir de los que todavía no han cambiado su VCR por un DVD? Es necesario que pase cierto tiempo para superar las tecnologías y los intereses arraigados.

El hecho es que el número de instalaciones de Vigilancia IP crece rápidamente, y el número de integradores y distribuidores crece cada día. No queda mucho para que el mercado reconozca la superioridad de la Vigilancia IP, y entonces veremos un rápido crecimiento en la base instalada y en la infraestructura para darle soporte.

Si este argumento no parece tener suficiente peso para nosotros es suficiente con comprobar como un gigante como IBM está entrando en el mercado de las redes de seguridad, así como el interés de jugadores como Cisco y Proxim en potenciar la educación del mercado.

Mito 3: La Vigilancia IP no satisface las demandas de aplicaciones a nivel corporativo

Realidad: Está probado que el concepto de Vigilancia IP permite llevar a cabo las instalaciones más grandes, las de mayor rendimiento, las más competitivas e impresionantes. De hecho de las muchas ventajas descritas anteriormente, la escalabilidad es una de las que apuntan los usuarios de alto nivel como la más impresionante. Por ejemplo, consultando con la empresa Axis, ellos a menudo reciben pedidos para instalaciones de 200, 300 o más cámaras algunas de las cuales son instalaciones de alta seguridad como aeropuertos internacionales y prisiones. Este mito es fácil de corregir: La Vigilancia IP ha demostrado que no tiene problemas para satisfacer las demandas a nivel corporativo. De hecho se ha comprobado que los principales negocios de Organizaciones de la Administración y de vigilancia de aeropuertos especifican IP como arquitectura de preferencia, algo que no ocurría hace tiempo.

Mito 4: La calidad de imagen del Vídeo IP no es tan buena como la del analógico

Realidad: Las cámaras IP de calidad tienen los mismos sensores de imagen (CCDs) de alta calidad y las mismas ópticas que las cámaras de seguridad analógicas. Además, con el uso de servidores de vídeo una cámara analógica o cámaras analógicas ya instaladas pueden incorporarse al sistema de Vigilancia IP. Al comparar las cámaras analógicas y las IP debemos poner énfasis en la buena calidad de las cámaras IP, que han sido diseñadas para un uso profesional. Estas cámaras IP de calidad profesional no deben confundirse con las cámaras de gama baja o las WebCam usadas para “atracción Web”. Estas cámaras no pueden proporcionar las mismas capacidades que una cámara con funcionalidades completas.

En breve, la tecnología de la cámara IP y la Vigilancia IP proporcionará una calidad de imagen superior, lo que se traducirá en una resolución de mega-píxeles. Las cámaras analógicas están limitadas por la resolución de 0.4 Mega pixeles de los estándares PAL y NTSC.

Las cámaras IP cuestan más que las analógicas, lo que hace que las soluciones de Vigilancia IP sean demasiado caras

Realidad: Es cierto que una cámara IP es más cara que una cámara analógica comparable, ya que incluye un número considerable de funcionalidades adicionales como son digitalización, compresión de imágenes e inteligencia. Si analizamos el coste total del hardware (cámaras, cableado y grabación), un sistema de Vigilancia IP suele ser mas económico que un sistema basado en DVR. Si incorporamos el componente de costes de instalación las ventajas del sistema de Vigilancia IP se hacen más obvias dado que la infraestructura IP es considerablemente más económica que la de cableado coaxial. Además los sistemas que usen controles PTZ precisan un cableado adicional, algo que no hace falta con IP. Power over Ethernet es otra característica que permite ahorrar costes al permitir conectar las líneas de alimentación energética a Sistemas de Alimentación Ininterrumpida en el centro de TI.

En una Instalación de alto nivel que Axis llevó a cabo en 2002 se desplegaron 300 cámaras de red. Era un entorno de misión crítica de un área de alta seguridad con necesidades de grabación a un alto ratio de imágenes por segundo. El coste total de la instalación del sistema completo de Vídeo vigilancia IP fue de 800.000 dólares o 2700 dólares por canal. Si se hubiera instalado un sistema similar basado en DVR el coste estimado hubiera sido de 1.800.000 dólares o 6000 dólares por canal, más del doble del coste del sistema de Vigilancia IP.

Mito 6: Si ya hay cámaras analógicas instaladas la Vigilancia IP no es una opción porque se necesita un DVR

Realidad: Puede que los proveedores de DVR quieran que creamos esto, sin embargo la tecnología de los servidores de vídeo existe para romper con este mito. Los fabricantes líderes de Vigilancia IP ofrecen servidores de vídeo con unos niveles de inversión razonables. Un servidor de vídeo convierte la señal de vídeo analógico en una secuencia de vídeo a través de una red, convirtiendo básicamente cualquier cámara analógica en una cámara de red. La mayoría de las instalaciones actuales de Vigilancia IP tiene una combinación de cámaras analógicas, servidores de vídeo en red, y secciones compuestas exclusivamente por cámaras IP. Una instalación con total funcionalidad basada en cámaras analógicas no representa una barrera para la utilización de una tecnología superior como la de la Vigilancia IP.

Ahora que hemos demolido algunos de los mitos generales que hemos oído sobre la Vigilancia IP, vamos a examinar algunos de los errores técnicos sobre los sistemas de vídeo en red.

Mito 7: Transferir todos los datos de vídeo sobrecargará mi red lo que hace que esta sea una tecnología impracticable

Realidad: Si usted tiene sólo unas pocas cámaras, una red Fast Ethernet (100 Mbit) como las de las oficinas actuales cubrirá normalmente cualquier demanda de transmisión. A nivel orientativo, una única cámara IP precisa aproximadamente entre 0.2 y 2 Megabits por segundo de ancho de banda, dependiendo de la compresión, el ratio de imágenes por segundo y el tamaño de las mismas. Para cualquier despliegue mayor de cámaras IP y servidores de vídeo recomendamos una red separada para el vídeo. Piense como si fuera una red ferroviaria, una vez que ciertos tramos de vía están congestionados, simplemente se construye otro tramo paralelo. A nivel corporativo el núcleo de la red local probablemente ya cuenta con tecnología Gigabit Ethernet. Con los routers y switches actuales separar redes es algo sencillo.

Además, se pueden dar otros pasos específicos para asegurar que la tecnología de Vigilancia IP puede integrarse en las operaciones de una organización sin que la red se resienta.

De forma adicional, dado que la inteligencia local está a nivel de la cámara, ésta puede tomar decisiones relacionadas con el ratio de imágenes a enviar sobre la red en función de eventos, movimiento, fecha u hora,… De modo que en muchos casos la cámara enviará sólo vídeo a través de la red si el vídeo merece la pena grabarlo, lo que significa sólo un 10% del tiempo. El 90% restante no habrá transferencia de vídeo a través de la red.

Mito 8: No es seguro transmitir vídeo sobre redes IP

Realidad: Aunque se usa principalmente como un dominio de información pública, Internet puede también usarse para transferir todos los tipos de información sensible, si se cuenta con las medidas de seguridad correctas como son firewalls, VPN's y se ha implementado la protección por contraseña. Actualmente los bancos y otras entidades financieras usan regularmente Internet como un medio para transacciones globales de dinero, y ha emergido como un medio probado para otras aplicaciones de seguridad como la vigilancia y la monitorización de seguridad. Por el contrario, los sistemas de vigilancia analógicos no tienen encriptación o autentificación y resulta relativamente sencillo acceder a los cables y de forma ilícita visualizar transmisiones de vídeo seguras, o incluso incorporar información de vídeo falsa en la red (Como en la película Ocean's 11). Esto es imposible en redes IP seguras.

Mito 9: La Vigilancia IP es menos fiable que otras tecnologías alternativas

Realidad: Cuando se desarrollaron las bases de la arquitectura de redes IP en los años 60 y 70, la capacidad para proporcionar redundancia fue la mayor demanda. De la misma forma en la actualidad los enlaces de transmisiones, los servidores de aplicaciones y almacenamiento y los switches pueden tener niveles paralelos de servicios y rutas alternativas de comunicaciones. El almacenamiento se puede consolidar en localizaciones externas seguras y se pueden usar servidores para hacer redundante el suministro eléctrico, usar RAID de discos hot-swap (que se pueden cambiar sin apagar el servidor), tarjetas de red duales y memoria correctora de errores.

Estos aspectos dependen del diseñador de redes y lo normal es que no se desplieguen todos los elementos de seguridad en una red de pequeñas dimensiones. Elegir componentes IT de alta calidad en una red significa que será una solución más fiable

que CCTV con DVR o DVR en caja negra. Y, no lo olvide, al usar equipos de servidor y de red estándares reemplazar hardware con fallos lleva menos tiempo y es más económico que con cualquier solución de DVR propietaria.

Mito 10: A la Vigilancia IP aun le quedan 5 años

Realidad: Este es el mayor mito de todos! Tenga en cuenta que las primeras cámaras IP fueron presentadas en 1996. La Empresa Axis Communications tiene instalados actualmente más de 200.000 canales de esta solución de "futuro" y el interés y los pedidos continúan creciendo.

Dados sus costes, rendimientos, fiabilidad o cualquier otra medida, la Vigilancia IP ha demostrado que es una solución para hoy, y que crecerá y mejorará para asegurar que es una solución también para el futuro.

En estos 10 Mitos se concluye repitiendo: que la Vigilancia IP es altamente escalable, a la vez que resulta efectiva y eficiente en la utilización de la capacidad de red de una compañía, y proporciona ventajas de rendimiento y costes sobre el modelo DVR que muchos piensan es la solución principal actualmente. También se ha comprobado que la Vigilancia IP es flexible, que basa sus funcionalidades en las cámaras IP y que es altamente fiable.

Apéndice C

API's para el manejo de Video en Tiempo Real

Apéndice C. API's para el manejo de Video en Tiempo Real

Con la introducción del scanner, cámaras digitales, y de otros dispositivos para adquisición de imágenes, los usuarios descubrieron el valor de incorporar imágenes en sus documentos y otros trabajos. Sin embargo, el soporte del muestreo y de la manipulación de estos datos puso un alto coste en las aplicaciones. Necesitaron crear interfaces de usuario y construir en dispositivos controladores para la variedad de dispositivos de imágenes disponibles. Una vez que su aplicación fuera preparada para apoyar a un dispositivo dado, hicieron frente a la realidad que desalentaba que los dispositivos continúan siendo actualizados con nuevas capacidades y características. Las aplicaciones se encuentran continuamente en revisión para permanecer actualizados.

Las aplicaciones de los dispositivos de adquisición de imágenes y de las aplicaciones de software reconocieron la necesidad de una comunicación estándar entre los dispositivos de imagen y las aplicaciones. Un estándar beneficiaría a ambos grupos así como los usuarios de sus productos. Permitiría que los productos de los vendedores del dispositivo fueran alcanzados por más aplicaciones y los vendedores de la aplicación podrían tener acceso a datos de esos dispositivos sin la preocupación de cual sea el tipo de dispositivo, o el dispositivo particular, con tal que él desea interactuar. JMF, TWAIN y otras fueron desarrollados debido a esta necesidad de la consistencia y de la simplificación.

JAVA MEDIA FRAMEWORK (JMF)

Java Media Framework [4] proporciona a los applets y aplicaciones Java la capacidad de reproducir, capturar y transmitir/recibir en tiempo real audio video y otros contenidos multimedia. Provee de una serie de codificadores y decodificadores para los formatos multimedia más relevantes siendo capaz además, de realizar transcodificación entre dichos formatos.

Introducción

Java™ Media Framework (JMF) es un API (Application Programming Interface), para la incorporación de medios basados en el tiempo (time-based medias) en aplicaciones Java y Applets. Los medios basados en el tiempo son medios tales como el audio, video, MIDI y animaciones que cambian con respecto al tiempo.

Inicialmente, el JMF 1.0 API, habilitaba a los programadores para desarrollar software de tipo Java que presentaban estos tipos de medios. Actualmente, el JMF 2.0 API, extiende el área de trabajo, para proveer soporte para captura y almacenaje de medios (basados en el tiempo), controlando el tipo de procesamiento que es efectuado durante la reproducción y para la personalización del procesamiento sobre flujos de medios.

Los objetivos principales del diseño de JMF 2.0 API son:

- Ser más fácil para programar.
- Soporte para la captura de medios.
- Habilita el desarrollo de aplicaciones para flujos de medios (media streaming) y conferencias en Java.
- Habilitación de tecnología y desarrollo avanzado que permita implementar soluciones personalizadas basadas en APIs ya existentes y nuevas características fácilmente integrables.
- Proveer el acceso a datos *Raw Media.*
- Habilitar el desarrollo de demultiplexores, codecs, procesadores de efectos, multiplexores, y renderers personalizables y descargables (JMF plug-ins).
- Mantener la compatibilidad con JMF 1.0 API.

Datos Basados En El Tiempo (Time-Based Media).

Toda información que tenga cambios significativos con respecto al tiempo puede ser catalogada como un medio basado en el tiempo, como lo son los clips de audio, secuencias MIDI, clips de video, etc. Estos medios pueden ser obtenidos de diversas fuentes, como archivos locales o remotos, cámaras, micrófonos y difusiones en vivo.

A continuación se presenta un modelo (figura 6.4) que describe las características de estos medios y la manipulación que a estos se les debe aplicar.

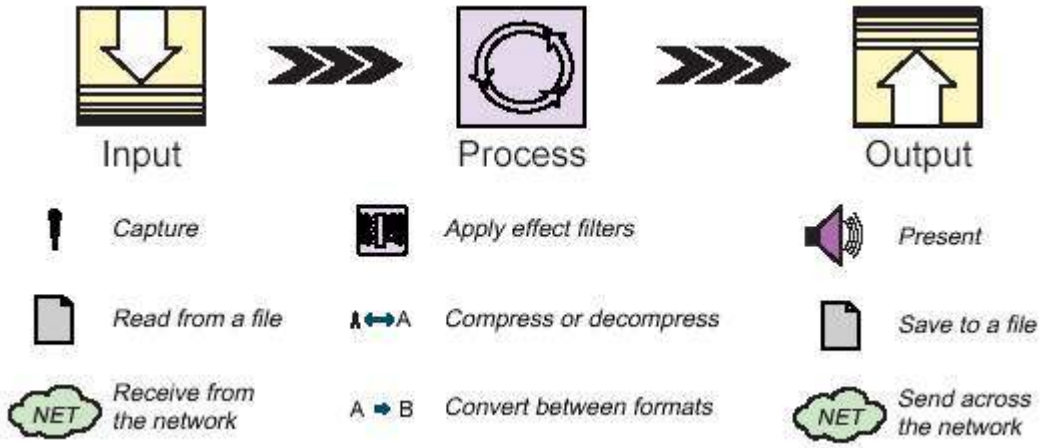


Figura 6.4
Modelo de Procesamiento de Medios

Las características claves de los medios basados en el tiempo son las siguientes:

- ***Flujo de Medios (Streaming Media).***
  La característica principal de este medio es que requiere de un tiempo de entrega y de procesamiento, y por esto se debe controlar, ya que una vez iniciado el flujo de datos, se deben satisfacer ciertos límites de tiempo.

- ***Presentación de Medios (Output).***

La mayoría de estos medios pueden ser presentados a través de dispositivos de salida tales como parlantes y monitores, u otras destinaciones (Ej.: a la red). Comúnmente a estos destinos de medios se le llaman D*ata-Sinks*.

- ***Procesamiento de Medios (Process).***
  En muchas instancias, la información contenida en un medio es manipulada antes de ser presentado al usuario, ya sea multiplexándola, filtrándola, comprimiéndola, o convirtiéndola en otro tipo de medio.

- ***Captura de Medios (Input).***
  Estos pueden ser capturados desde una fuente en vivo para procesarla y reproducirla o puede ser adquirida de un archivo de forma remota.

TWAIN

De manera no oficial **TWAIN** (Figura 6.5) es el acrónimo de Technology Without An Interesting Name (N.T. Tecnología sin un nombre interesante), sin embargo Kevin Bier uno de los autores originales dijo que eligió el nombre después de leer algunas obras de Mark Twain. Estándar industrial de un protocolo de software y una API que permite una integración sencilla de datos de imágenes entre los dispositivos de entrada, como los escáneres y las cámaras digitales de imágenes estáticas, además de las aplicaciones de software.

Figura 6.5 Twain

Introducción

En aplicaciones de imágenes bajo Windows, la API para escaneo mas usada es TWAIN www.twain.org. Desafortunadamente el nuevo .NET Framework no tiene ninguna ayuda incorporada para TWAIN. Tenemos que trabajar con los métodos del interop de .NET para tener acceso a esta API.

Los elementos de TWAIN

TWAIN define un protocolo de software Standard y una API (application programming interface) para la comunicación entre aplicaciones de software y dispositivos de adquisición de imágenes.

Los tres elementos dominantes en TWAIN son:

- **La Aplicación de Software:** Una aplicación debe ser modificada para usar TWAIN.

- **Software Manejador de Código** – Este software maneja las interacciones entre la aplicación y la fuente. Este código se proporciona en el TWAIN Developer's Toolkit y debe ser enviado gratis con cada fuente y aplicación TWAIN.

- **Código de software** – Este software controla el dispositivo de adquisición de imágenes y es escrito por el programador del dispositivo para cumplir con las especificaciones de TWAIN. Los drivers de dispositivo tradicionales ahora son incluidos en el código del software y no necesita ser enviado por aplicaciones.

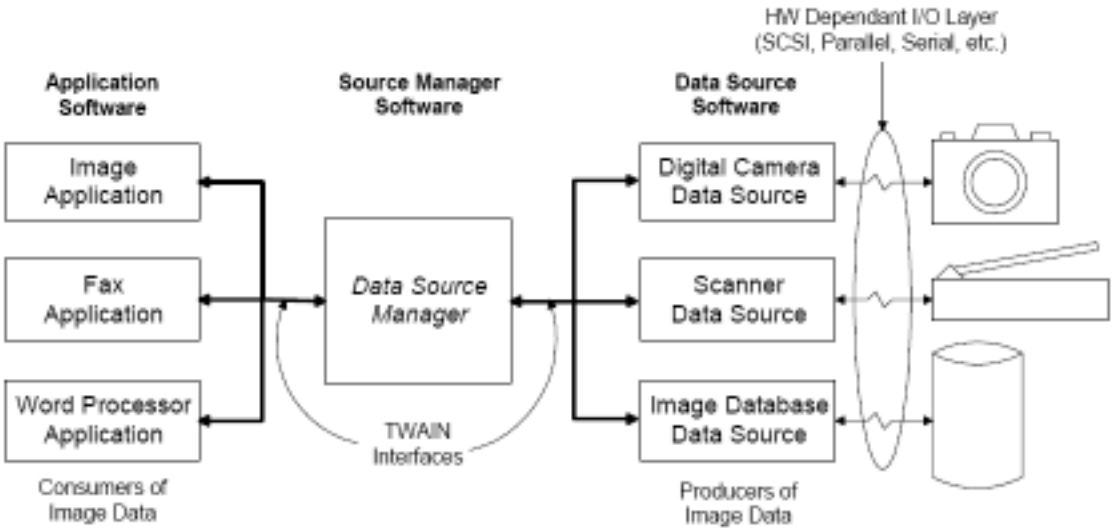


Figura 6.6 Elementos de TWAIN

Apéndice D

Uso del Componente IPCAM-CONNECTOR

Apéndice D. Uso del Componente IPCAM-CONNECTOR

Introducción

En este apartado se explica como es que se deben utilizar el componente, sus métodos y sus clases y un ejemplo sencillo para usar el componente.

Se cuenta con 2 clases: **VariableSet** y **ReceiveSock,** los métodos **conSock(), getSig()** y **loadData().**

Importar el Componente

El componente es un archivo JAR llamado **ipcamconnector.jar,** este puede ser colocado en cualquier parte. Para poder importar el JAR dentro de una clase creada se debe agregar en el CLASSPATH la dirección del componente y si se está usando algún IDE de desarrollo como JCreator o NetBeans agregarlos a su JDK Profiles, así, a la hora de compilar alguna clase que importe el componente reconozca las clases que contiene.

Para entender el uso del componente vamos a crear un ejemplo que haga la conexión y obtenga la imagen de la cámara y la guarde en disco.

Hagamos una clase que se llame **Obtener.java** y en la cabecera importamos las clases del componente, java.awt.image para la creación de la imagen a partir de los datos obtenidos de la cámara y el java.io para la creación del archivo (Figura 6.7):

```
import java.awt.image.*;
import java.io.*;
import com.intellinet.ipcamconnector.*;
```

Figura 6.7 Importar el Componente

Hacer Conexión Utilizando conSock() y logueo con getSig()

El método **conSock()** de la clase RecesiveSock es la encargada de realizar la conexión mediante sockets a la cámara.

Para poder hacer una conexión a la cámara se crea una instancia **VariableSet** pasándole el nombre de usuario, contraseña, ip y puerto de la cámara y crear una instancia ReceiveSock pasándole la instancia de VariavleSet (Figura 6.8).

```
VariableSet vset = new VariableSet("guest","guest","148.228.20.14",8080);
ReceiveSock rs = new ReceiveSock(vset);
```

Figura 6.8 Instancias VariableSet y ReceiveSock

En seguida se hace uso del método **conSock()** para realizar la conexión (figura 6.9) esta regresa un booleano; true si conecta, false si no conecta.

```
if(!rs.conSock()){
    rs = null;
    System.out.println("No Conecta!");
    System.exit(0);
}
```

Figura 6.9 Conectando a la cámara

Una vez conectado se procede al logueo utilizando el método **getSig()** (figura 6.10), este método regresa un **true** si lo hace con éxito de lo contrario regresa **false**.

```
if(!rs.getSig()){
    rs = null;
    System.out.println("No hay Señal!");
    System.exit(0);
}
```

Figura 6.10 Logueando a la cámara

Obtención de Imágenes utilizando loadData() y getImage()

Para la obtención de los datos se hace uso de los metodos ***loadData()*** y ***getImage().***

El método **loadData()** es para que el componente obtenga la imagen haciendo peticiones a la cámara, el método regresa ***true*** si el proceso fue exitoso y el componente guarda los datos en un arreglo de bytes, de lo contrario el método **loadData()** regresa ***false*** (figura 6.11)**.**

El método **getImage()** es para obtener los bytes de la imagen de la cámara (figura 6.11), este regresa un arreglo de bytes el cual ya se puede convertir a imagen con formato JPG.

```
for(int x=0;x<1;x++){
    if(rs.loadData()){
        InputStream in = new ByteArrayInputStream(rs.getImage());
        try {
            b_image = javax.imageio.ImageIO.read(in);
        }catch(IOException ioe){
            System.out.println("IOException:"+ioe);
         }
        try {
            image_video = new File("C:/temporal/video/"+"prueba"+x+".jpg");
            javax.imageio.ImageIO.write( b_image, "JPEG", image_video);
        } catch (Exception e){
            System.out.println("Exception:"+e);
          }
    }
    else System.out.println("no se pudo obtener imagen!");
    System.exit(0);
}
```

Figura 6.11 Obtención de la Imagen con loadData() y getImage()

Para poder obtener imágenes continuamente el **loadData()** y el **getImage()** van dentro de un ciclo, esto es posible porque se mantiene abierta la conexión con la cámara.

Una vez que no se quieran más imágenes se cierra la conexión con el método **cleanSock()**, siguiendo el ejemplo sería: **rs.cleanSock()**.

Bibliografía

[1] Axis Communications : http://www.axis.com

[2] The Code Proyect - http://www.codeproject.com/dotnet/twaindotnet.asp

[3] Wikipedia - http://es.wikipedia.org/wiki/

[4] Agustín J. González V. Ph.D. en Computer Science, Old Dominion University, U.S.A, 2000
http://profesores.elo.utfsm.cl/~agv/elo330/2s03/projects/JavaMediaFramework/main.htm

[5] The MathWorks - http://www.mathworks.com/access/helpdesk/help/toolbox/imaq/

[6] Networking and Emerging Optimization
http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/cliente-servidor.html

[7] Jean-Marie Rifflet "*Comunicaciones en UNIX*". McGraw Hill. 1998

[8] UML in a Nutshell". Sinan si Alhir. Ed. O'Reilly. 1998

[9] UML gota a gota". Martin Fowler. Ed. Prentice Hall. 1999

[10] UML Toolkit". Eriksson & Penker. Ed. John Wiley. 1998

[11] El Lenguaje Unificado de Modelado". Grady Booch, James Rumbaugh, Ivar Jacobson. Ed. Addison Wesley. 1999

[12] IEEE-STD-830-1998 Especificaciones de los Requisitos del Software

[13] Programación de Socket Linux. SEAN WALTON. Pearson Education, S.A., Madrid 2001

[14] Red Segura. http://fitxers.oriolrius.cat/1591/codishttp.html