ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

CARRERA DE TECNOLOGÍA ELECTRÓNICA

"ANÁLISIS DE UN SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) CON TECNOLOGÍA INALÁMBRICA, PARA EL CONTROL Y SUPERVISIÓN EN OPERACIONES MILITARES"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO ELECTRÓNICO

CBOS. CUSSI CAJAS HENRY MANOLO
CBOS. MINGA AMAY PABLO FABIÁN

LATACUNGA, MARZO 2010

CERTIFICACIÓN

Se certifica que el presente trabajo de graduación fue desarrollado en su totalidad por los señores: CBOS. DE COM. CUSSI CAJAS HENRY MANOLO y CBOS. DE COM. MINGA AMAY PABLO FABIÁN, previo a la obtención de su Título de Tecnólogo Electrónico, bajo nuestra supervisión.

Latacunga, Marzo del 2010

Ing. César Naranjo

DIRECTOR

Ing. Katya Torres

CODIRECTOR

AUTORIZACIÓN

Yo, Cussi Cajas Henry Manolo, como autor del proyecto de grado “ANÁLISIS DE UN SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) CON TECNOLOGÍA INALÁMBRICA, PARA EL CONTROL Y SUPERVISIÓN EN OPERACIONES MILITARES” autorizo la publicación del presente proyecto de grado en la biblioteca virtual de la ESPE.

Latacunga, Marzo del 2010

_____

CUSSI CAJAS HENRY MANOLO
CBOS. DE COM.

DECLARACIÓN

Yo, Cussi Cajas Henry Manolo declaro que soy el autor y responsable del proyecto de grado “ANÁLISIS DE UN SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) CON TECNOLOGÍA INALÁMBRICA, PARA EL CONTROL Y SUPERVISIÓN EN OPERACIONES MILITARES”.

Latacunga, Marzo del 2010

_____

CUSSI CAJAS HENRY MANOLO
CBOS. DE COM.

AUTORIZACIÓN

Yo, Minga Amay Pablo Fabián, como autor del proyecto de grado “ANÁLISIS DE UN SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) CON TECNOLOGÍA INALÁMBRICA, PARA EL CONTROL Y SUPERVISIÓN EN OPERACIONES MILITARES” autorizo la publicación del presente proyecto de grado en la biblioteca virtual de la ESPE.

Latacunga, Marzo del 2010

_____

MINGA AMAY PABLO FABIÁN
CBOS. DE COM.

DECLARACIÓN

Yo, Minga Amay Pablo Fabián declaro que soy el autor y responsable del proyecto de grado “ANÁLISIS DE UN SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) CON TECNOLOGÍA INALÁMBRICA, PARA EL CONTROL Y SUPERVISIÓN EN OPERACIONES MILITARES”.

Latacunga, Marzo del 2010

_____

MINGA AMAY PABLO FABIÁN
CBOS. DE COM.

AGRADECIMIENTOS

Agradecemos a todos los ingenieros de la ESPE sede Latacunga, que en alguna u otra forma contribuyeron con nuestra formación para llegar a este punto de nuestra carrera, especialmente a nuestros Directores de tesis, Ing. César Naranjo e Ing. Katya Torres que nos ayudaron con sus conocimientos para la realización de este trabajo.

Henry Cussi y Pablo Minga.

DEDICATORIA

El presente trabajo fue posible gracias al apoyo incondicional de nuestras familias, a ellos les dedico el esfuerzo del presente proyecto.

Pablo Minga.

ÍNDICE

CAPÍTULO I

INTRODUCCIÓN

1.5. IMPORTANCIA DE UN CCTV

Los índices delictivos como son: robos, crímenes e inseguridad, han aumentado en forma considerable en los últimos años. Por razones de tipo económico, principalmente, no se dispone de los recursos suficientes para controlar la seguridad integral sea en domicilios e instituciones públicas o privadas, considerando como la necesidad primaria para justificar este proyecto, la seguridad, la misma que será para el beneficio y apoyo de los miembros de la Escuela Politécnica del Ejercito sede Latacunga así como también de apoyo a las operaciones de seguridad que necesite el Ejército Ecuatoriano.

En aplicaciones de video vigilancia, la tecnología inalámbrica es una manera flexible, viable, rentable y rápida de implantar cámaras; especialmente en sistemas que cubren grandes áreas como aparcamientos o centros de las ciudades, ya que elimina la necesidad de utilizar cables terrestres. Además, en edificios antiguos protegidos en los que no se permite la instalación de cables Ethernet, la tecnología inalámbrica pasa a ser la única alternativa.

1.6. DEFINICIÓN Y DESCRIPCIÓN DE UN CCTV.

El circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de video vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión

convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Para mejorar el sistema se suelen conectar directamente o en lazar por red otros componentes como vídeos u ordenadores, que se encuentran fijos en lugares determinados.

En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros. Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

1.7. TRANSMISIÓN Y RECEPCIÓN INALÁMBRICA DE VIDEO.

1.7.1. WIFI.

Existen varias tecnologías de transmisión inalámbrica; la más utilizada para armar redes locales es Wifi, que está basada en las especificaciones de IEEE[1] 802.11. Wifi es una marca registrada por la Wi-Fi Alliance (antes, la Wireless Ethernet Compatibility Alliance), la organización comercial que aprueba y certifica que los equipos cumplan con los estándares IEEE 802.11x.

[1] IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

Este estándar fue desarrollado por el IEEE, y define el uso de los dos niveles más bajos de la arquitectura OSI, especificando sus normas de funcionamiento en una WLAN (Wireless Local Area Network). Este estándar no es más que la parte de la norma 802 encargada de definir la capa de acceso físico (MAC) y de enlace, para entornos que usan ondas radioeléctricas como medio de comunicación.

1.7.1.1. Las normas WiFi.

La norma IEEE 802.11 ofrece tasas de 1 0 2 Mbps. Se han hecho algunas revisiones a la norma original para mejorar las prestaciones que ofrecen, se han creado las normas 802.11a, 802.11b y 802.11g, llamadas normas físicas de 802.11, también se han creado otras normas para asegurar la interoperabilidad de sus dispositivos detallados en la tabla 1.1.

Tabla 1.1 Estándares del WIFI

Nombre del estándar	Nombre	Descripción
802.11a	Wifi5	El estándar 802.11 (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mbps). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Wifi	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.

802.11c	Combinación del 802.11 y el 802.11d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.11d que permite combinar el 802.11d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

802.11g		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h		El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (Hiper LAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i		El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES*[2] y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir		El estándar 802.11r se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j		El estándar 802.11j es para la regulación japonesa lo que el 802.11h es para la regulación europea.

[2] ASE: Estándar De Cifrado Avanzado.

802.11n		Es una propuesta para mejorar significativamente el desempeño de la red de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz.

1.7.1.2. Portadoras y Ancho de Banda.

Las normas físicas 802.11, 802.11a, 802.11b y 802.11g, según sus modos de operación permiten conseguir rendimientos en cuanto a ancho de banda de acuerdo a su rango de trabajo, se definen en la tabla 1.2.

Tabla 1.2 Rendimiento en cuanto a ancho de banda de acuerdo al rango de trabajo

Estándar	Frecuencia	Tasa de transferencia	Rango
WiFi a (802.11a)	5 GHz	54 Mbps	10 m
WiFi b (802.11b)	2,4 GHz	11 Mbps	100 m
WiFi g (802.11g)	2,4 GHz	54 Mbps	100 m

1.7.1.3. Norma 802.11a.

El estándar 802.11 tiene en teoría un flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo a un rango de 30 metros aproximadamente. El estándar 802.11a se basa en la tecnología llamada OFDM (multiplicación por división de frecuencias ortogonales). Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos.

Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "banda dual".

1.7.1.4. Norma 802.11b.

El estándar 802.11b permite un máximo de transferencia de datos de 11 Mbps en un rango de 50 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales).

Tabla 1.3 Tasa de bits vs. Rango de la norma 802.11b

Tasa de bits teórico	Rango (en interiores)	Rango (exterior)
11 Mbps	50 m	200 m
5,5 Mbps	75 m	300 m
2 Mbps	100 m	400 m
1 Mbps	150 m	500 m

1.7.1.5. Norma 802.11g.

El estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM, es compatible con los dispositivos 802.11b.

Tabla 1.4 Tasa de bits vs. Rango de la norma 802.11g

Velocidad hipotética	Rango (interiores)	Rango (exteriores)
54 Mbps	27 m	75 m
48 Mbps	29 m	100 m

36 Mbps	30 m	120 m
24 Mbps	42 m	140 m
18 Mbps	55 m	180 m
12 Mbps	64 m	250 m
9 Mbps	75 m	350 m
6 Mbps	90 m	400 m

1.7.2. MODOS DE FUNCIONAMIENTO WIFI.

Existen diferentes dispositivos que se definen de acuerdo a su uso:

- **Los adaptadores inalámbricos o tarjetas de acceso inalámbrica (NIC).-** Son dispositivos bajo la norma 802.11 que le permiten a un equipo conectarse a una red inalámbrica. Los adaptadores inalámbricos están disponibles en diversos formatos, como tarjetas PCI[3], tarjetas PCMCIA[4], adaptadores USB, etc. Una estación es cualquier dispositivo que tenga este tipo de tarjeta.

- Los **puntos de acceso** (abreviado **PA** y a veces denominados zonas locales de cobertura) pueden permitirles a las estaciones equipadas con WiFi cercanas acceder a una red conectada a la que el punto de acceso se conecta directamente.

El estándar 802.11 define dos modos operativos:

- **El modo de infraestructura;** en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso. Éste es por lo general el modo predeterminado para las tarjetas 802.11b.

[3] PCI: Interconexión de Componentes Periféricos.
[4] PCMCIA: Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales.

- **El modo ad-hoc;** en el que los clientes se conectan entre sí sin ningún punto de acceso.

1.7.3. MODO DE INFRAESTRUCTURA.

En el modo de infraestructura, como se indica en la figura 1.1, cada estación informática se conecta a un punto de acceso a través de un enlace inalámbrico. La infraestructura formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). En el modo infraestructura el BSSID corresponde al punto de acceso de la dirección MAC.

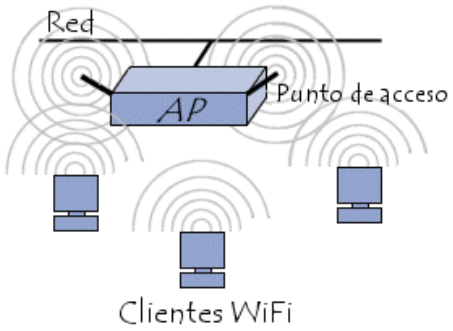


Figura 1. 1 Modo de infraestructura básico

Es posible vincular varios puntos de acceso juntos (o con más exactitud, varios BSS) con una conexión llamada sistema de distribución (o SD) para formar un conjunto de servicio extendido o ESS. El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica.

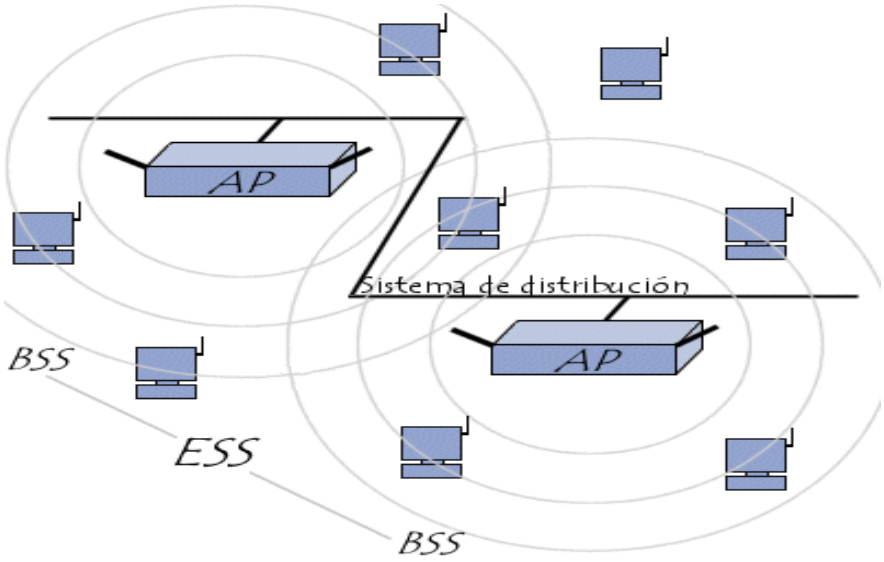


Figura 1.2 Definición de zona de cobertura de servicio.

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), que es un identificador de 32 caracteres en formato ASCII que actúa como su nombre en la red. El ESSID, a menudo abreviado SSID, muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el SSID para conectarse a la red extendida.

Cuando un usuario itinerante va desde un BSS a otro mientras se mueve dentro del ESS, el adaptador de la red inalámbrica de su equipo puede cambiarse de punto de acceso, según la calidad de la señal que reciba desde distintos puntos de acceso. Los puntos de acceso se comunican entre sí a través de un sistema de distribución con el fin de intercambiar información sobre las estaciones y, si es necesario, para transmitir datos desde estaciones móviles. Esta característica que permite a las estaciones moverse "de forma transparente" de un punto de acceso al otro se denomina itinerancia.

1.7.4. MODO AD HOC.

En el **modo ad hoc** los equipos cliente inalámbrico se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

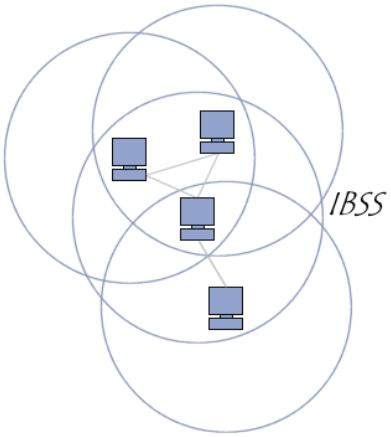


Figura 1.3 Definición de IBSS

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS.

Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red ad hoc, el rango del BSS independiente está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

1.7.5. TÉCNICAS DE TRANSMISIÓN DE DATOS.

1.7.5.1. Las tecnologías de transmisión.

Las redes locales radio eléctricas utilizan las ondas de radio o infrarrojo para transmitir algunos datos. La técnica usada en el transmisor para transmisores por radio se llama transmisión en banda angosta, consiste en pasar las comunicaciones en canales diferentes. Los transmisores de radio se someten a

numerosos apremios que hacen de esta transmisión un tipo de comunicación ineficiente. Estos apremios son básicamente los siguientes:

- El compartimiento de la banda de paso entre las diferentes estaciones presentes en una misma celda.

- La propagación por caminos múltiples de una onda de radio. Una onda de radio puede propagarse en una dirección diferente y posiblemente puede ser reflejado o refractado por los objetos del ambiente físico, para que un receptor pueda recibir a algunos instantes de información de dos intervalos parecidos realizados por dos diferentes ondas reflexivas.

La capa física de la norma 802.11 define varias técnicas de la transmisión que permiten limitar así inicialmente los problemas debido a las interferencias.

- Espectro ensanchado por saltos de frecuencia.
- Espectro ensanchado por secuencia directa.
- Tecnología infrarroja.

1.7.5.2. Banda angosta.

La técnica de banda estrecha consiste en el uso de una frecuencia de radio especificada para transmitir y recibir datos. La banda de frecuencia que se utilice debe ser lo más pequeña posible para no interferir con las bandas cercanas.

1.7.5.3. Espectro ensanchado.

El estándar IEEE 802.11 permite que dos técnicas de modulación de frecuencia desarrolladas para los militares transmitan datos. Estas técnicas, denominadas espectro ensanchado, consisten en utilizar una banda de frecuencia ancha para transmitir datos de baja potencia. Existen dos tecnologías de espectro ensanchado:

- Espectro ensanchado por saltos de frecuencia.
- Espectro ensanchado por secuencia directa.

Espectro ensanchado por saltos de frecuencia.

La técnica de espectro ensanchado por saltos de frecuencia o **FHSS** consiste en dividir la frecuencia de banda ancha por lo menos en 75 canales distintos (con "saltos" de 1 MHz de distancia entre sí) y después transmitirla a través de una combinación de canales que todas las estaciones en la célula conocen. En el estándar 802.11 la banda de frecuencia de 2.4 a 2.4835 GHz acepta 79 canales discretos de 1 MHz, la transmisión se lleva a cabo de un canal hacia otro y sólo se usa cada canal durante un período de tiempo corto (aproximadamente 400 milésimas de segundo), lo que permite que una señal más fácil de reconocer se transmita en un determinado momento y en una determinada frecuencia.

La técnica de espectro ensanchado por saltos de frecuencia se desarrolló originalmente para uso militar con el fin de prevenir que se escuchen las transmisiones radiales. La estación que no sabe qué combinación de frecuencia usar no puede escuchar la señal porque le sería imposible determinar la frecuencia en la que la señal fue transmitida y encontrar después la nueva frecuencia dentro de un período de tiempo corto.

Actualmente, las redes locales que usan esta tecnología son estándar. Debido a que la secuencia de frecuencias que se utiliza es conocida universalmente, esta técnica ya no es una forma segura de transmitir datos.

Sin embargo, FHSS todavía se utiliza en el estándar 802.11 para reducir la interferencia entre las distintas estaciones de una célula.

Espectro ensanchado por secuencia directa.

La técnica conocida como espectro ensanchado por secuencia directa (DSSS) consiste en transmitir para cada bit enviado una secuencia de Barker de bits (a veces llamado ruido pseudo aleatorio o PN). En esta operación, cada bit establecido en 1 es reemplazado por una secuencia de bit y cada secuencia de bit establecida en 0 es reemplazada por su complemento.

Como se indica en la figura 1.4 define una secuencia de 11 bits (10110111000) para representar un 1 y para codificar el 0 usa su complemento (01001000111). Cada bit que se codifica con esta secuencia se denomina chip o código de chip. Esta técnica (llamada chipping por "chip") modula cada bit que tenga la secuencia de Barker.

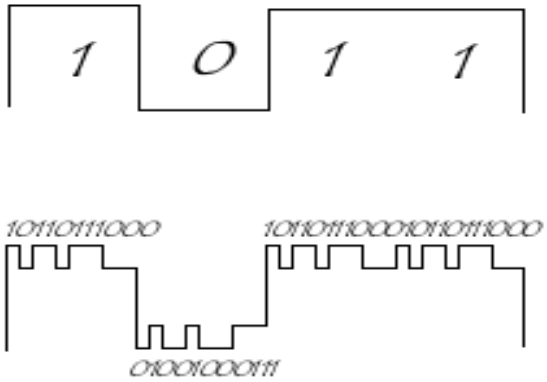


Figura 1.4 Secuencia de bits de la capa física de la norma 802.11

A través del chipping se envía información redundante y esto permite verificar errores e incluso corregirlos durante las transmisiones.

En la norma 802.11b, la banda de frecuencia 2.400-2.4835 GHz (83.5 MHz de ancho) se ha dividido en 14 canales distintos de 5 MHz cada uno. Sólo los primeros 11 se pueden usar en Estados unidos y Canadá. En el Reino Unido se pueden usar los canales del 1 al 13 solamente. Éstas son las frecuencias que se asocian a los 14 canales:

Tabla 1.6 Canales de la norma 802.11b con su respectiva frecuencia.

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Frecuencia (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

Sin embargo, para una correcta transmisión de 11 Mbps se debe transmitir en una banda de 22 MHz porque, de acuerdo al teorema de Shannon[5], la frecuencia de muestreo debe ser al menos el doble de la señal para que se digitalice. Algunos canales se superponen con canales cercanos. Es por ello que generalmente se utilizan canales aislados (1, 6 y 11) que están a 25 MHz de distancia.

Por lo tanto, cuando dos puntos de acceso que usan los mismos canales tienen áreas de transmisión que se superponen, las distorsiones de señal pueden afectar las transmisiones. Para evitar cualquiera de estas interferencias, se recomienda distribuir los puntos de acceso y seleccionar canales de forma tal que dos puntos de acceso que usen el mismo canal nunca estén cerca.

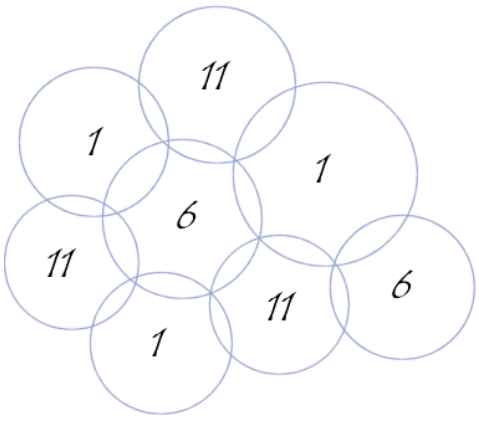


Figura 1.5 Zonas recomendadas de broadcast para los puntos de acceso.

El estándar 802.11a utiliza las bandas de frecuencia de 5.15 a 5.35 GHz y de 5.725 a 5.825 GHz, lo que le permite definir 8 canales diferentes de 20 MHz de ancho cada uno, una banda lo suficientemente ancha como para evitar que los canales interfieran unos con otros.

[5] Teorema de Shannon: es una aplicación del teorema de codificación para canales con ruido.

1.7.5.4. Tecnología infrarroja.

El estándar IEEE 802.11 también ofrece una alternativa a las ondas radiales: la luz infrarroja. La característica primordial de la tecnología infrarroja es el uso de una onda de luz para transmitir datos. Estas transmisiones viajan en una sola dirección, ya sea mediante una línea de visibilidad directa o al reflejarse en una superficie. Las ondas de luz ofrecen un alto nivel de seguridad debido a su naturaleza no difusa.

La tecnología infrarroja permite el envío de datos a una velocidad de 1 a 2 Mbps al usar una clase de modulación denominada PPM (modulación de posición de pulso).

La modulación PPM consiste en transmitir pulsos de amplitud constante y codificar información según la posición del pulso. Una velocidad de transferencia de 1 Mbps se alcanza con una modulación de 16 PPM y 2 Mbps se alcanzan con una modulación de 4 PPM, lo que permite que se codifiquen 2 bits de datos con cuatro posiciones posibles.

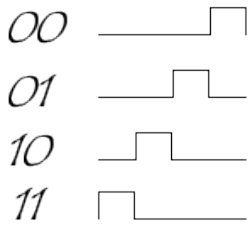


Figura 1.6 Bits de modulación 4 PPM

1.7.6. TÉCNICAS DE MODULACIÓN.

Mientras que la radio común utiliza una frecuencia modulada (FM) o una amplitud modulada (AM), el estándar 802.11b utiliza una técnica de modulación denominada PSK (modulación por desplazamiento de fase). Durante este proceso

cada bit sufre un desplazamiento de fase. Para transferir a velocidades bajas se usa un desplazamiento de 180 grados (es una técnica que se denomina BPSK, modulación por desplazamiento de fase binaria), mientras que una serie de cuatro desplazamientos de 90 grados permiten transferencias dos veces más rápidas (técnica llamada QPSK, modulación por desplazamiento de fase en cuadratura).

1.7.7. SEGURIDAD DE RED INALÁMBRICA WI-FI.

1.7.7.1. Una infraestructura adaptada.

Lo primero que hay que hacer cuando se instala una red inalámbrica es ubicar el punto de acceso en un lugar razonable dependiendo del área de cobertura que se desee. Sin embargo, es común que el área cubierta sea más grande que lo deseado. En este caso es posible reducir la solidez del terminal de acceso para que su rango de transmisión concuerde con el área de cobertura.

1.7.7.2. Para evitar los valores por defecto.

Cuando se instala un punto de acceso por primera vez, se configura con ciertos valores predeterminados, inclusive la contraseña del administrador. Muchos administradores principiantes suponen que como la red ya está funcionando, no tiene sentido cambiar la configuración del punto de acceso. Sin embargo, las configuraciones predeterminadas brindan sólo un nivel de seguridad mínimo. Por esta razón, es vital registrarse en la interfaz de administración (casi siempre a través de una interfaz Web o al usar un puerto en particular en el terminal de acceso) para establecer especialmente una contraseña administrativa.

Además, para conectarse a un punto de acceso es necesario conocer el identificador de red (SSID). Por ello se recomienda cambiar el nombre predeterminado de la red y desactivar la transmisión del nombre en la red. Cambiar el identificador de red predeterminado es muy importante, ya que de lo

contrario puede brindarles a los hackers información sobre la marca o el modelo del punto de acceso que se está usando.

1.7.7.3. Filtrado de direcciones MAC.

Todo adaptador de red (término genérico de la tarjeta de red) tiene su propia dirección física (que se denomina dirección MAC). Esta dirección está representada por 12 dígitos en formato hexadecimal divida en grupos de dos dígitos separados por guiones.

Las interfaces de configuración de los puntos de acceso les permiten, por lo general, mantener una lista de permisos de acceso (llamada ACL; Lista de control de acceso) que se basa en las direcciones MAC de los dispositivos autorizados para conectarse a la red inalámbrica.

Esta precaución algo restrictiva le permite a la red limitar el acceso a un número dado de equipos. Sin embargo, esto no soluciona el problema de la seguridad en las transferencias de datos.

1.7.7.4. WEP - Privacidad equivalente al cableado.

Para solucionar los problemas de seguridad de transferencia en redes inalámbricas, el estándar 802.11 incluye un sencillo mecanismo de cifrado llamado WEP (Privacidad equivalente al cableado).

WEP es un protocolo de cifrado de trama de datos 802.11 que utiliza el algoritmo simétrico RC4[6] con claves de 64 bits o 128 bits. El concepto de WEP consiste en establecer una clave secreta de 40 ó 128 bits con antelación.

Esta clave secreta se debe declarar tanto en el punto de acceso como en los equipos cliente. La clave se usa para crear un número que parece aleatorio y de

[6] RC4: Es un algoritmo de tamaño de clave variable con operaciones a nivel de byte. Se basa en el uso de una permutación aleatoria y tiene un periodo estimado de más de 10^{100}. Además, es un algoritmo de ejecución rápida en software.

la misma longitud que la trama de datos. Cada transmisión de datos se cifra de la siguiente manera: Al utilizar el número que parece aleatorio como una "máscara", se usa una operación "O excluyente" para combinar la trama y el número que parece aleatorio en un flujo de datos cifrado.

La clave de sesión que comparten todas las estaciones es estática, es decir que para poner en funcionamiento un número elevado de estaciones inalámbricas, éstas deben configurarse con la misma clave de sesión. Por lo tanto, con sólo saber la clave se pueden descifrar las señales.

Además, para la inicialización se usan sólo 24 bits de la clave, lo que implica que sólo 40 de 64 bits o 104 de 128 bits de la clave se utilizan realmente para el cifrado.

En el caso de una clave de 40 bits, con un ataque de fuerza bruta (que prueba todas las claves posibles) un hacker puede encontrar la clave de sesión con rapidez. Asimismo, una falla detectada por Fluhrer, Mantin y Shamir en la generación del flujo que parece aleatorio permite que se descubra la clave de sesión al almacenar y analizar de 100 MB a 1 GB de tráfico.

Por lo tanto, el WEP no es suficiente para garantizar verdaderamente la privacidad de los datos. Sin embargo, se recomienda utilizar al menos una clave WEP de 128 bits para garantizar un nivel de privacidad mínimo. Esto puede reducir el riesgo de una intrusión en un 90 por ciento.

1.7.7.5. Mejorar la autenticación.

Para administrar la autenticación, autorización y contabilidad (**AAA**) de manera más eficaz, se puede usar un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El protocolo RADIUS (definido por la RFC

2865 y la 2866[7]) es un sistema cliente/servidor que permite administrar de manera central cuentas de usuarios y permisos de acceso relacionados.

1.7.8. TÉCNICAS DE COMPRESIÓN.

Cuando se está desarrollando una aplicación de video-vigilancia digital los programadores consideran inicialmente los siguientes factores:

- ¿Son necesarias imágenes estáticas o en movimiento?
- ¿Cuál es el ancho de banda de la red?
- ¿Qué nivel de degradación de imágenes debido a la compresión resulta aceptable? (artifacts).
- ¿A cuánto asciende el presupuesto para el sistema?

Cuando se digitaliza una secuencia de vídeo analógica de acuerdo al estándar CCIR 601[8] puede consumir aproximadamente 165 Mbps (Megabites por segundo), es decir 165 millones de bits cada segundo. Aunque la mayoría de las aplicaciones de vigilancia rara vez comparte la red con otras aplicaciones intensivas en datos, es realmente infrecuente encontrar este ancho de banda disponible.

Para solventar este problema una serie de técnicas, denominadas técnicas de compresión de vídeo e imágenes, han sido creadas para reducir este elevado ratio de bits. Su capacidad para realizar esta tarea se cuantifica por el ratio de compresión, es decir, el menor consumo de ancho de banda que consigue.

En todo caso hay que pagar un precio por esta compresión ya que el aumento de la compresión genera una mayor degradación de la imagen. A esto se le denomina artifacts.

[7] RFC 2865 y 2866: Estándar para la Contabilidad (Protocolo RADIUS).
[8] CCIR 601: es el antiguo nombre de un estándar publicado por el CCIR (ahora UIT-R) para la codificación de señales de vídeo entrelazado analógica en formato digital.

Pero hay un dilema, la técnica de compresión más sofisticada y empleada es la más compleja y la más costosa para el sistema. Esto hace generalmente que una compresión sofisticada sea restrictiva en términos de mantener bajos los costes del sistema.

1.7.8.1. JPEG y MPEG, dos estándares básicos.

Los dos estándares de compresión básicos son JPEG y MPEG. En términos generales JPEG está asociado a imágenes digitales estáticas, mientras que el MPEG está dedicado a las secuencias de video. Sin embargo esos formatos de imágenes tradicionales JPEG y JPEG 2000 también tienen variantes que resultan apropiadas para video igualmente; los formatos Motion JPEG y Motion JPEG 2000.

El grupo de estándares MPEG que incluye los formatos MPEG-1, MPEG-2 y MPEG-4 comparten muchas similitudes, así como notables diferencias:

Una cosa en común es que todos han sido establecidos como estándares Internacionales por la ISO (Organización Internacional para la Estandarización) y la IEC (Comisión Electrotécnica Internacional), con contribuciones desde los EE.UU., Europa y Japón, entre otros. También son recomendaciones propuestas por la ITU (Unión Internacional de Telecomunicaciones), que ha ayudado a establecerlas como estándares de facto globalmente aceptados para la codificación de imágenes digitales estáticas y video.

La base de estos estándares se inició a mediados de los ochenta cuando se formó un grupo denominado Joint Photographic Experts Group (JPEG, Grupo de Expertos Fotográficos Unidos). Su misión era desarrollar un estándar para la compresión de imágenes en color y la primera contribución pública del grupo fue la presentación de la primera parte del estándar JPEG, en1991. Desde entonces, el grupo JPEG ha continuado trabajando tanto en el estándar JPEG original como en su último sucesor: el estándar JPEG 2000.

A finales de los 80, se formó el Motion Picture Expert Group (MPEG, Grupo de Expertos en Imágenes en Movimiento) con el propósito de definir un estándar para la codificación de imágenes en movimiento y audio. Desde entonces ha producido los estándares para MPEG-1, MPEG-2 y MPEG-4. El trabajo actual del grupo está centrado en la próxima generación de estándares, denominada MPEG-7 y MPEG-21. Debido a que estos estándares no están relacionados con la compresión de video no hay explicaciones posteriores de los mismos.

1.7.8.2. Reducción de datos en imágenes.

Como se ha mencionado previamente, una secuencia de video digitalizada puede ocupar 165 Mbps de velocidad en transmisión de datos. Para reducir las sobrecargas del medio en la distribución de esas secuencias y con el fin de conseguir la reducción deseada de los datos de las imágenes se emplean los siguientes criterios:

- Reducir matices de color en la imagen.
- Reducir la resolución de color respecto a la intensidad de luz prevaleciente.
- Reducir partes pequeñas, invisibles de la imagen.
- En el caso de una secuencia de video, las partes de una imagen que no cambian se deja como están.

Todas estas técnicas están basadas en un conocimiento preciso y exhaustivo de cómo el cerebro y los ojos trabajan en combinación para formar el complejo sistema visual humano.

Como resultado de estas sutiles modificaciones se produce una reducción significativa del tamaño del fichero para secuencias de video sin prácticamente ningún efecto para la calidad visual. La posibilidad de que esas modificaciones sean apreciables por el ojo humano depende típicamente del grado de la técnica de compresión que se utilice.

Figura 1.7 Imagen original

1.7.8.3. JPEG.

El estándar JPEG, ISO/IEC 10918[9], es sencillamente el formato de compresión actual más ampliamente utilizado. Ofrece la flexibilidad para seleccionar una imagen de alta calidad con un ratio de compresión razonablemente alto o conseguir un ratio de compresión muy alto con menor calidad de imagen. Se pueden crear sistemas como cámaras y visualizadores de forma económica dada la baja complejidad de la técnica.

Los artifacts muestran bloques como se puede apreciar en la Figura 1.8. Comparada con la imagen original en la figura 1.7 los bloques aparecen cuando se forza un ratio de compresión demasiado alto. En su uso normal una imagen comprimida con JPEG no muestra una diferencia visual con la imagen original sin comprimir.

La compresión de imágenes JPEG contiene una serie de técnicas avanzadas. La principal, la que hace la compresión real de la imagen es la denominada Discrete Cosine Transform (DCT) seguida por una cuantificación que elimina la información redundante (las partes “invisibles”).

[9] Extracto sacado de: www.axis.com

Figura 1.8 Una imagen comprimida con JPEG

1.7.8.4. Motion JPEG.

Una secuencia de video puede ser representada como una serie de imágenes JPEG. Las ventajas son las mismas que con imágenes estáticas JPEG-flexibilidad tanto en términos de calidad como en ratios de compresión.

La principal desventaja del Motion JPEG (también conocido como MJPEG) es que sólo utiliza una serie de imágenes estáticas sin hacer uso de técnicas de compresión de video. El resultado es un ratio de compresión ligeramente inferior para secuencias de video en comparación con las técnicas reales de compresión de video.

1.7.8.5. JPEG 2000.

Recientemente, el sucesor del exitoso estándar de compresión JPEG ha visto la luz. La base ha sido la incorporación de los nuevos avances en la investigación de la compresión de imágenes un estándar internacional. En vez de realizar la transformación DCT[10], JPEG 2000, ISO/ECT 15444, utiliza la transformación Wavelet[11].

[10] DCT: Transformada Coseno Discreta.
[11] Transformación Wavelet: Transformada óndula (tipo especial de transformada de Fourier).

La ventaja de JPEG 2000 es que los bloques de JPEG se eliminan y se remplazan con una imagen generalmente más difusa, como se puede apreciar en la figura 1.9.

Figura 1.9 Una imagen comprimida con JPEG 2000

Mientras que esta difusión de JPEG 2000 es preferible frente a los bloques de JPEG, en general es un asunto de preferencia personal. En cualquier caso el ratio de compresión de 2000 es más alto. Para ratios de compresión moderados, JPEG 2000 produce imágenes típicamente unos 25% inferiores en tamaño de fichero que JPEG con igual calidad de imagen.

El precio a pagar es trabajar con una técnica de compresión mucho más compleja.

1.7.8.6. Motion JPEG 2000

Al igual que JPEG y Motion JPEG, JPEG 2000 puede ser utilizado para representar una secuencia de video. Las ventajas son las mismas que con JPEG 2000, un ratio de compresión ligeramente superior comparado con JPEG y con el inconveniente de la complejidad.

Esta desventaja reaparece con Motion JPEG. Dado que es una técnica de compresión de imágenes estáticas no incorpora ninguna de las ventajas de la compresión de video. El resultado es un ratio de compresión inferior comparado con las técnicas reales de compresión de video.

1.7.8.7. H.261/H.263

El H.261 y el H-263 no son Estándares Internacionales sino recomendaciones de la ITU.

Ambos están basados en la misma técnica que los estándares MPEG y pueden ser interpretados como versiones simplificadas de la compresión de video MPEG. Fueron diseñados originalmente para video conferencia sobre líneas telefónicas con poco ancho de banda. En cualquier caso es un poco contradictorio que muestren carencia de alguna de las técnicas MPEG más avanzadas para ofrecer realmente un uso eficiente del ancho de banda.

La conclusión es que H.261 y H.263 no se adecuan al uso de codificación de video digital general.

1.7.8.8. MPEG-1

El primer estándar público del comité MPEG fue el MPEG-1, ISO/IEC 11172, cuya primera parte fue publicada en 1993. La compresión de video MPEG-1 está basada en la misma técnica que se usó para JPEG. Además incluye técnicas para la codificación eficiente de una secuencia de video.

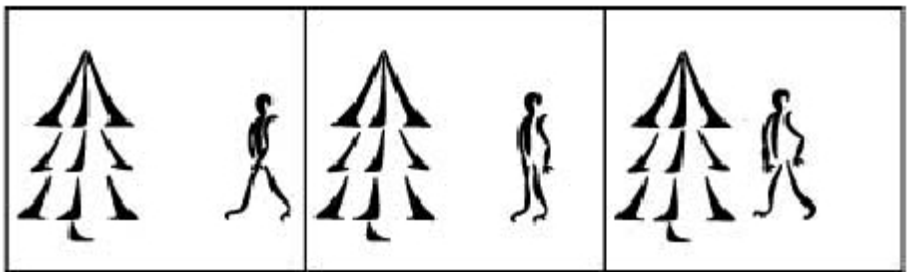


Figura 1.10 Una secuencia de vídeo JPEG de tres imágenes

Considere la secuencia de video mostrada en la Figura 1.10. La imagen de la izquierda es la primera imagen en la secuencia seguida por la imagen del medio y después la imagen de la derecha. Cuando se muestra, la secuencia de video

muestra a un hombre caminando de derecha a izquierda con un árbol que permanece estático.

En Motion JPEG/Motion JPEG 2000 cada imagen de la secuencia se codifica como una única imagen separada ofreciendo como resultado una secuencia igual a la original.

En MPEG video sólo las partes de la secuencia de video se incluye junto con la información de las partes que ofrecen movimiento. La secuencia de video de la Figura 1.10 aparecerá entonces como se muestra en la Figura 1.11. Sin embargo esto es sólo real durante la transmisión de la secuencia de video para limitar el consumo de ancho de banda.

Cuando se visualice aparecerá nuevamente como la secuencia de video original.

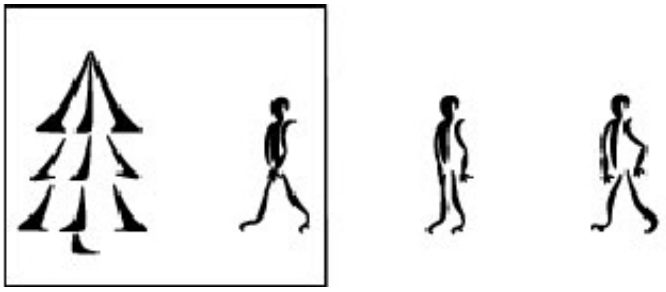


Figura 1.11 Una secuencia de video MPEG de tres imágenes.

MPEG-1 está centrado en streams de bits de aproximadamente 1,5 Mbps y originalmente para el almacenamiento de vídeo digital en CD's. El foco está en el ratio de compresión más que en la calidad de las imágenes. Puede ser considerado como la calidad tradicional del VCR pero en formato digital.

1.7.8.9. MPEG-2

El proyecto MPEG-2 se centró en la ampliación de la técnica de compresión MPEG-1 para cubrir imágenes más grandes y mayor calidad con un menor ratio de compresión y por consiguiente mayor uso de ancho de banda.

MPEG-2, ISO/IEC 13818, también ofrece técnicas más avanzadas para mejorar la calidad del video con el mismo ratio de bits. El inconveniente es la necesidad de un equipamiento más complejo. En cualquier caso estas características no suelen adaptarse a su uso en aplicaciones de vigilancia en tiempo real.

A nivel anecdótico, las películas en DVD están comprimidas utilizando las técnicas MPEG-2.

1.7.8.10. MPEG-4

También la tercera generación de MPEG está basada en la misma técnica. Una vez más, el nuevo proyecto se enfocó en los usos de nuevas aplicaciones.

Las características nuevas más importantes de MPEG-4, ISO/IEC 14496, relacionadas con la compresión de video son el soporte de aplicaciones con menor consumo de ancho de banda, por ejemplo: unidades móviles, y, por otro lado, para aplicaciones con una calidad extremadamente alta y sin casi limitación de ancho de banda. La realización de películas de estudio es sólo un ejemplo.

La mayoría de las diferencias entre MPEG-2 y MPEG-4 son características no relacionadas con codificación de video y por tanto no relacionadas con las aplicaciones de vigilancia.

1.7.8.11. Comparación MPEG

Todos los estándares MPEG ofrecen compatibilidad hacia atrás. Esto significa que una secuencia de video MPEG-1 también puede ser “empaquetada” como video MPEG-2 o MPEG-4. Del mismo modo, MPEG-2 puede ser “empaquetada” como una secuencia de video MPEG-4.

La diferencia entre un video MPEG-4 real y una secuencia MPEG-1 “empaquetada” como MPEG-4 es que los estándares más antiguos no hacen uso de las mejoras y nuevas características de los más actuales.

Dado que tanto MPEG-2 como MPEG-4 cubren una amplia variedad de tamaños de imágenes, ratios de imágenes y uso de ancho de banda, el MPEG-2 introdujo un concepto denominado Profile@Level[12].

La comparación de los MPEGs aparece en la Tabla 1.7, contiene el MPEG-1 con su limitación más utilizada (Constrained Paramenters Bitstream, CPB), MPEG-2 con su Main Profile at Main Level (MP@ML), y MPEG-4 con Main Profile at Level 3.

Tabla 1.7 Comparación de MPEGs

MPEG	**1**	**2**	**3**
Máx. ratio de bits (Mbps)	1,86	15	15
Ancho de imagen (píxeles)	352	720	720
Alto de imagen (píxeles)	288	576	576
Ratio de imágenes (fps)	30	30	30

Ni Motion JPEG ni Motion JPEG 2000 especifica el tamaño máximo de imagen ni el ratio de bits ni el ancho de banda.

1.7.8.12. Conclusión – Imágenes estáticas.

Para imágenes estáticas tanto JPEG como JPEG 2000 ofrecen bastante flexibilidad en términos de calidad de imagen y ratio de compresión. Mientras JPEG 2000 comprime ligeramente mejor que JPEG, especialmente a ratios de compresión muy altos, el momento de la ventaja comparada con el precio a pagar por la complejidad extra hace que hoy no sea la elección más habitual.

[12] Profile@Level: Es un perfil creado para hacer posible las capacidades de comunicación entre aplicaciones.

Para decirlo de otra forma; la ventaja de JPEG 2000 está en la compresión a un ratio muy alto.

Sin embargo las imágenes contienen muy poca información y por tanto no se adapta a las particularidades de la vigilancia.

Las ventajas de JPEG en términos de equipamiento económico tanto para codificación como para visualización lo convierten en la selección idónea para compresión de imágenes estáticas

1.7.8.13. Conclusión – Imágenes en movimiento.

Especialmente Motion JPEG es una buena elección cuando se utilizan múltiples aplicaciones debido a su simplicidad. Esto asegura un equipamiento económico y un consumo de ancho de banda ligeramente superior. Para un uso más eficiente del ancho de banda se recomienda el uso de alguno de los estándares de compresión de imágenes en movimiento.

MPEG-1 puede ser más efectivo que MJPEG, sin embargo por un precio ligeramente superior, MPEG-2 proporciona algunas ventajas y mayor calidad de imagen, comprimiendo el ratio de imágenes y la resolución, aunque tiene un mayor consumo de ancho de banda y es una técnica mucho más compleja. MPEG-4 está desarrollado para ofrecer una técnica de compresión para aplicaciones que necesitan menor calidad de imagen y ancho de banda.

También permite compresión de video similar a MPEG- y MPEG-2, mayor calidad de imagen con un mayor consumo de ancho de banda.

Dado que las recomendaciones H.261/H.263 no son estándares internacionales y que no ofrecen ninguna mejora de compresión en relación a los MPEG, no tienen ningún interés real.

1.8. CÁMARAS DE VIDEO.

Desde que los sistemas de CCTV se han convertido en algo muy popular en las últimas décadas, la tecnología ha mejorado y cada vez es más asequible. La mayoría de las cámaras de circuito cerrado de televisión en uso hoy en día suelen ser de vigilancia y seguridad. Se pueden encontrar sistemas de circuito cerrado de televisión en casi todos los bancos, casinos, centros comerciales y grandes almacenes. De hecho, los sistemas de circuito cerrado de televisión se han vuelto tan asequibles, la mayoría de pequeñas tiendas también tienen sistemas de circuito cerrado de televisión para fines de seguridad.

1.8.1. ANÁLISIS Y TIPOS.

Las cámaras inalámbricas se deben conectar a un punto de acceso, el punto de acceso debe ser de capa 3 y capaz de soportar QoS, para administrar la dirección IP y además de proporcionar acceso protegido WiFi (WPA) como característica mínima de seguridad.

La frecuencia de operación de las cámaras de video y puntos de acceso está en la banda 802.11g en una frecuencia de operación de 2,4 Ghz con una tasa de transmisión de datos desde 30 Mbps hasta 54 Mbps, y a una distancia máxima de operación sin obstáculos de 100 metros, y dado que también permite la compatibilidad con equipos 802.11b.

El tipo de características que se tendrán que definir son las siguientes: calidad de imagen, velocidad de trama, resolución, tipo de compresión, porcentaje compresión, tiempo de grabación.

Hay muchos tipos de cámaras de CCTV y pueden ser clasificados por: el tipo de imágenes que son capaces de capturar, la cantidad de fotogramas que pueden tomar por minuto, el tipo de conexión con el monitor o dispositivo de grabación de video, si están en condiciones de mover la posición y funciones especiales que pueden proporcionar.

Tipos de Imágenes: general, cámaras de circuito cerrado de televisión, tanto en blanco y negro o en color de imágenes de video. Además, muchas cámaras de circuito cerrado de televisión pueden tener la capacidad de visión nocturna que permite a una cámara de circuito cerrado de televisión para ver y grabar imágenes con poca luz usando una tecnología especial.

Fotogramas por segundo: Fotogramas por segundo significa que la cantidad de imágenes completas que una cámara de vídeo capta y envía a un dispositivo de grabación o monitor por segundo. Si bien la mayoría de sistemas de cámaras de CCTV son fácilmente capaces de capturar 30 o más fotogramas por segundo (30 fps se considera en tiempo real), la cantidad de cintas de vídeo o digital de almacenamiento sería enorme para registrar cada momento de cada día. Para la mayoría de las tiendas, las velocidades de 1 a 6 fotogramas por segundo son más que suficientes para capturar y grabar a un autor que haya cometido un delito.

Pan Inclinación Zoom (PTZ) Cámaras: Estos tipos de cámaras de CCTV permiten a una persona el control de la vigilancia de un espacio para mover la cámara a distancia, por lo general con un cable de RF o controlador. La mayoría de las cámaras móviles de vigilancia permitirá a la persona que mueva la cámara de izquierda a derecha (PAN), arriba y abajo (inclinación) y de un estrecho acercamiento (zoom).

Accesorios con cámaras especiales: Algunas cámaras de circuito cerrado de televisión tienen funciones especiales que se hacen para usos especiales. Por ejemplo, son extremadamente pequeñas cámaras de vigilancia que se utilizan para el espionaje (Nanny Cámaras[13]), hay cámaras que están hechos para ver de noche, las cámaras que son resistentes al vandalismo y las cámaras que son específicamente para uso en interiores o exteriores.

[13] Nanny Cámaras: Pequeñas cámaras para supervisar a niñeras abusivas.

1.8.2. CARACTERISTICAS GENERALES.

De acuerdo con las características de las cámaras para CCTV tenemos lo siguiente:

Para visualización:

- Velocidad de imagen 30 ips NTSC.
- Resolución de 352x240 CIF.
- Tipo de compresión MJPEG.
- Relación de compresión 10 %.

Para grabación continua:

- Tiempo de grabación 24 horas.
- Velocidad de grabación 30 ips NTSC.
- Resolución 352x240 CIF.
- Tipo de compresión MJPEG.
- Relación de compresión 10 %.

Para grabación de eventos:

- Alarma a una relación del 20 %.
- Velocidad de trama 30 ips NTSC.
- Resolución 704x5764 CIF.
- Tipo de compresión MJPEG.
- Relación de compresión 10 %.

1.8.3. CÁMARAS ESPECIALES.

En este apartado se va a referir a las cámaras que por su forma o prestaciones son aptas para ciertas aplicaciones muy específicas o se implantan con unos objetivos muy concretos.

- Microcámaras: se emplean fundamentalmente en aplicaciones cuya finalidad es la vigilancia discreta. En su categoría se pueden encontrar muy diversos

modelos, tanto monocromas como en color, en cuanto formas, tamaños, funcionamiento, cableadas o inalámbricas, resistentes, etc.

- Cámaras ocultas o camufladas: se instalan con la intención de pasar inadvertidas a las personas. Por lo general se trata de cámaras de muy reducidas dimensiones capaces de alojarse en objetos de lo más diverso: detectores de intrusión o de incendio, reloj, mirilla, libro, bolígrafo, teléfono, etc.

- Domo, esfera, semiesfera, microesfera: carcasas o elementos superficiales de diferentes formas y tamaños cuya función es proteger el elemento captador contenido en su interior. Por extensión se aplica el nombre a todo el conjunto, el cual se caracteriza por su diversidad en cuanto a formas, tamaños, materiales, cámaras contenidas, prestaciones, etc.

- Cámaras móviles emplazadas en vehículos (unidad móvil): equipo captador instalado en el techo de un vehículo mediante unos soportes especiales cuyas características son idénticas a las cámaras ubicadas en lugar fijo.

- Cámaras simuladas: diseños de óptica y cámara no operativos cuya función primordial es la disuasión. Para incrementar la credibilidad del conjunto se le añade el soporte oportuno, y, en ocasiones, un led o piloto indicador de operatividad.

- Cámaras para ambientes especiales: se trata de diseños específicos capaces de operar en condiciones adversas como puede ser la presencia de altas temperaturas, ambientes corrosivos o agresivos, atmósferas explosivas, bajo el agua, etc.

Así mismo, se indica las prestaciones de las cámaras, cuya activación o prioridad de transmisión está vinculada a sensores específicos o detectores (de intrusión,

incendio, etc.) con la intención de capturar imágenes cuando se produce una incidencia (intrusión, fuego,...).

1.8.3.1. Micro cámaras.

Son cámaras de video (color o B/N), de muy reducidas dimensiones al integrarse todos los componentes, incluido el audio, en pequeños dispositivos. Debido a esta característica se emplean fundamentalmente en aplicaciones cuya finalidad es la vigilancia discreta, siendo factible disimularlas u ocultarse en elementos del entorno de emplazamiento.

Las características y requisitos propios de estos dispositivos son:

- Tamaños y formas muy diversas: cilíndricas, rectangulares, cuadrangulares, en placa, etc.
- Modelos con elevada resolución y sensibilidad.
- Sincronización interna o externa.
- Carcasas especiales: plástico, metálicas, aluminio,...
- Diferentes ópticas.
- Posicionamiento manual, aunque pueden admitir control remoto.
- Minisoportes especiales orientables: en función del tamaño y forma de la cámara.
- Ubicación e instalación sencilla e inmediata ("plug and play") motivada por su reducido peso y tamaño, pudiendo adaptarse a cualquier tipo de superficie, mobiliario, pared, etc.
- Posibilidad de llevar incorporada la iluminación con el fin de optimizar la captación en condiciones de escasa luminosidad.
- También se dispone de modelos inalámbricos.
- Posibilidad de incorporar audio, para captar los sonidos en la zona de vigilancia.
- Ciertos modelos incorporan desplazamiento horizontal, vertical, zoom, etc.

En cuanto al resto de características y requisitos son similares a las cámaras convencionales de superior tamaño. Sus reducidas dimensiones avalan su rendimiento en instalaciones necesitadas de vigilancia discreta, oculta o encubierta.

1.8.3.2. Cámaras ocultas o camufladas.

Se refiere a cámaras de muy reducido tamaño alojadas en diversos dispositivos u objetos habituales en las instalaciones a controlar.
Los objetos más habituales para contener las cámaras son:

- Detector de intrusión o de incendio: pueden ser operativos o falsos (solo la carcasa). Puede vincularse la captación de imágenes a la causa desencadenante de la alarma e incorporar leds de infrarrojos para visión nocturna.
- Reloj operativo, cuadro, espejo,... permiten una vigilancia discreta de las instalaciones al mantenerse ocultas o invisibles.
- Otros objetos que faciliten el enmascaramiento e integración estética en el entorno, por ejemplo como mirilla de una puerta, libro, caja de pañuelos, cinta de video,…
- Otras posibilidades de ocultación en objetos desplazables o transportables como puede ser un teléfono móvil, un cajetilla de tabaco, un bolígrafo, un maletín,…
- Igualmente es factible instalar, exclusivamente un micrófono o circuito de audio para captar los ruidos que se originen.

Entre las características comunes a estos elementos se destacan:

- Todos los dispositivos son aptos para integrarse en sistemas de CCTV convencionales.
- En función del objeto contendor, la instalación puede ser cableada o inalámbrica, debiendo, en tal caso disponer de transmisor y fuente de alimentación propia.

- Vinculación a sistemas de alarma, activación manual o automática, etc.
- Montaje e instalación sencilla (conectores "plug and play").

1.8.3.3. Cámara oculta en detector.

Una de las técnicas de ocultación más corrientes consiste en instalar la microcámara de televisión en el interior del detector de intrusión o de incendio, los cuales pueden ser operativos o falsos (solo la carcasa).

Como ventaja complementaria puede vincularse la captación de imágenes a la causa desencadenante (fuego o intrusión) de la alarma e incorporar leds de infrarrojos para visión nocturna.

Otra forma de operación consiste en captar imágenes constantemente y enviar señales al puesto de control para advertir la incidencia (zumbador, mensaje en pantalla, ampliación o preferencia automática de visualización, etc.) o activar un equipo grabador de imágenes.

Entre sus características se destacan las siguientes:

- Cada elemento (cámara y detector) cumple los requisitos características y funciones para las que ha sido diseñado.
- Empleo de cámaras color o en blanco y negro.
- Posibilidad de incorporar micrófono para la captación de los sonidos ambientales.
- Modelos resistentes al agua, lo cual posibilita su instalación en el exterior, al aire libre.
- Aplicaciones para pequeñas instalaciones (domicilio, comercio,...) y para complejos sistemas de protección.

1.8.3.4. Domos.

Estos elementos o carcasas son los cuerpos contenedores de una cámara de vigilancia que se instala en su interior con la intención de proteger el elemento captador contenido en su interior y, en ocasiones, pasar desapercibida a la visión de las personas.

La denominación de los cuerpos contenedores está basada en la forma, aunque cada una de ellas admite tamaños muy diferentes en función de las dimensiones de la cámara que contiene.

Las características más destacables son:

- Cámaras en color o monocromas, con sus características propias.
- La instalación de la cámara puede hacerse de forma fija o gobernada por control remoto (desde teclados, matrices, multiplexores, etc.), pudiendo programar ciertos movimientos repetitivos (preposicionamientos) tanto en sentido horizontal como vertical.
- Posibilidad de ajuste vertical y horizontal de la cámara.
- Color de la burbuja o carcasa: claro, oscuro (tintado o ahumado) o combinado (claro, sólo en el espacio de desplazamiento y el resto oscuro).
- Materiales: base de aluminio y, como elemento transparente, metacrilato, plástico, policarbonato,...
- Muy utilizadas en interiores (también en exteriores), donde se mimetizan fácilmente con cualquier entorno (industrial, comercial, bancario, etc.).
- Montaje en superficie o empotrado, sobre techo o pared. Las esferas pueden verse colgantes y sobre mástil o soportes específicos.
- Posibilidad de equiparlas con calefactor y de acoplarles un posicionador.
- Las conexiones se efectúan por la base del soporte.
- Integración sencilla en sistemas de CCTV implantados.
- Grado de protección (IP) que garantice la estanqueidad al polvo y agua.

- Resistencia al vandalismo y sabotaje (golpes, manipulaciones, perforaciones,...).
- Aunque la mayoría se instalan con cables, también es posible las instalaciones inalámbricas.
- Pueden ir equipadas con iluminación infrarroja para dotar al equipo de iluminación cuando ésta se atenúa.
- Modelos día/noche: cambian de funcionamiento en color a blanco y negro cuando la iluminación disminuye.

1.8.3.5. Cámaras móviles.

Los sistemas de CCTV móviles van emplazados en vehículos (unidad móvil) y constan de un equipo captador montado en el techo de un vehículo, mediante unos soportes especiales, y sus características son idénticas a las cámaras emplazadas en lugar fijo.

Estas son algunas de las características exigibles a estos equipos:

- Su mayor ventaja es la posibilidad de captar imágenes de varias zonas e incidir sobre aquellas que más interesa.
- La cámara podrá desplazarse sobre los 360º del horizontal (pan) y 180º en el plano vertical (tilt).
- Dispondrá de zoom y estabilizador de vídeo.
- Cambio automático de color a blanco y negro en condiciones de escasa iluminación.
- Equipamiento accesorio de iluminación mediante focos de luz visible o infrarroja, o visor nocturno.
- Posibilidad de añadir un monitor y control del sistema desde el interior del vehículo o mediante control remoto.

Entre sus aplicaciones principales se tiene: las unidades montadas en vehículos patrulla para la vigilancia instalaciones privadas o para espacios de competencia de la seguridad pública, vigilancia de zonas específicas, etc.

CAPÍTULO II

ANÁLISIS

2.5. ANÁLISIS DE LOS DIFIRENTES TRANSMISORES Y RECEPTORES INALÁMBRICOS DE VIDEO.

2.5.1. SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN CON TRANSMISIÓ ANALÓGICA.

Los circuitos cerrados de televisión (CCTV, Closed Circuit Television Systems) son los primeros sistemas de video-vigilancia, su origen se remonta a los años 50's, sus características analógicas encarecen su precio y proporcionan: flexibilidad, escalabilidad, redundancia y tolerancia a fallas.

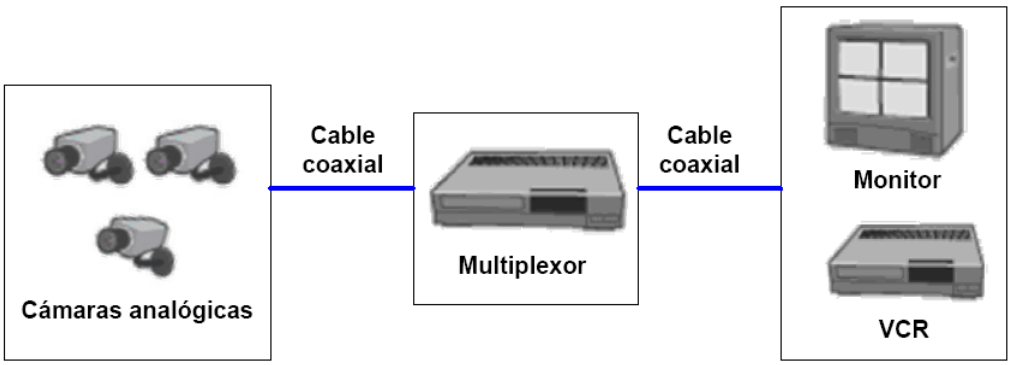


Figura 2.1 Esquema de la plataforma de video-vigilancia analógica

La Figura 2.1 muestra un sistema CCTV que emplea cable coaxial, las conexiones punto a punto desde las cámaras analógicas hasta el multiplexor (MUX) o concentrador de las señales de video, constituyen un reto al momento de implementar el cableado, las grabadoras de video (VCR, Video Camera Recorder) almacenan las secuencias en cintas magnéticas[14], se puede conectar un

[14] Cintas casi fuera del mercado actual.

multiplexor entre la cámara y el VCR para grabar video proveniente de cualquier cámara.

2.5.1.1. CCTV usando DVR.

En estos sistemas CCTV, se usa un grabador de video digital (DVR, Digital Video Recorder) encargado de almacenar el video digitalizado de las cámaras analógicas. Figura 2.2. El disco duro reemplaza a las cintas magnéticas y es necesario comprimir el video para almacenar la máxima cantidad de imágenes en un día. En los primeros DVR el espacio del disco duro era limitado y representaba un inconveniente.

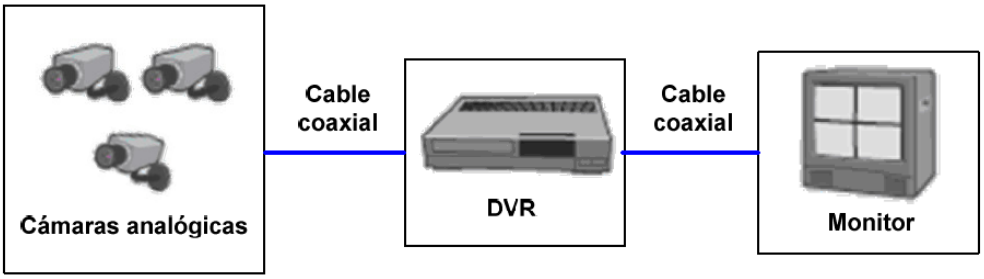


Figura 2.2 Sistema analógico que incluye un DVR para grabar y gestionar, la información de video digital.

El DVR puede incluir características IP y mediante una conexión a Internet, el video digital se puede monitorizar remotamente.

2.5.1.2. Los beneficios de ir hacia lo digital.

En los últimos 20 años, las aplicaciones de monitorización y vigilancia han estado basadas en la tecnología analógica. Los sistemas de circuito cerrado de televisión han sido tradicionalmente grabados en VCRs (Grabadores de Video en Cinta, Video Cassette Recorder, VCR), y dado que la percepción es que resultan fáciles de manejar y que tienen un precio razonable, la tecnología analógica fue, probablemente, la elección adecuada en el momento de la compra. De todas formas, el alcance actual de la tecnología digital ha cubierto muchas de las limitaciones de la tecnología analógica. Los sistemas de CCTV analógicos generalmente precisan un mantenimiento intensivo, no ofrecen accesibilidad remota y son notablemente difíciles de integrar con otros sistemas. Independientemente de estas deficiencias obvias.

El sistema de video vigilancia digital ofrece toda una serie de ventajas y funcionalidades avanzadas que no puede proporcionar un sistema de video vigilancia analógica. Entre las ventajas se incluyen la accesibilidad remota, la alta calidad de imagen, la gestión de eventos y las capacidades de vídeo inteligente, así como las posibilidades de una integración sencilla y una escalabilidad, flexibilidad y rentabilidad mejoradas.

Accesibilidad remota.

Se pueden configurar las cámaras de red y los codificadores y acceder a ellos de forma remota, lo que permite a diferentes usuarios autorizados visualizar video en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación del mundo tan solo accediendo a la red. Esto resulta ventajoso si los usuarios quisieran que otra empresa, como por ejemplo una empresa de seguridad, tuviera también acceso al video.

En un sistema CCTV analógico tradicional, los usuarios necesitarían encontrarse en una ubicación de supervisión para ver y gestionar video, y el acceso al video desde fuera del centro no sería posible sin un equipo como un codificador de vídeo o un grabador de video digital (DVR) de red. Un DVR es el sustituto digital de la grabadora de cintas de video.

Alta calidad de imagen.

En una aplicación de video vigilancia, es esencial una alta calidad de imagen para poder capturar con claridad un incidente en curso e identificar a las personas u objetos implicados. Con las tecnologías de barrido progresivo y megapíxel, una cámara de red puede producir una mejor calidad de imagen y una resolución más alta que una cámara CCTV analógica.

Asimismo, la calidad de la imagen se puede mantener más fácilmente en un sistema de video en red que en uno de vigilancia analógica. Con los sistemas analógicos actuales que utilizan un DVR como medio de grabación, se realizan muchas conversiones analógicas a digitales: en primer lugar, se convierten en la cámara las señales analógicas a digitales y después otra vez a analógicas para su transporte; después, las señales analógicas se digitalizan para su grabación. Las imágenes capturadas se degradan con cada conversión entre

los formatos analógico y digital, así como con la distancia de los cables. Cuanto más lejos tienen que viajar las señales de video, tanto más débiles se vuelven.

Gestión de eventos y video inteligente.

A menudo existe demasiado material de video grabado y una falta de tiempo suficiente para analizarlo adecuadamente. Las cámaras de red y los codificadores de video avanzados con inteligencia o análisis integrado pueden ocuparse de este problema al reducir la cantidad de grabaciones sin interés y permitir respuestas pro gramadas. Este tipo de funcionalidad no está disponible en un sistema analógico.

2.5.1.3. El DVR.

El Grabador de Video Digital o Grabador de Video Personal (PVR o DVR por sus siglas en inglés) es un dispositivo interactivo de grabación de televisión en formato digital. Se podría considerar como un set-top box más sofisticado y capacidad de grabación.

Un DVR se compone, por una parte, del hardware, que consiste principalmente en un disco duro de gran capacidad, un procesador y los buses de comunicación; y por otra, del software, que proporciona diversas funcionalidades para el tratamiento de las secuencias de video recibidas, acceso a guías de programación y búsqueda avanzada de contenidos.

El DVR nace gracias al nuevo formato digital de la televisión, este hecho permite almacenar la información y manipularla posteriormente con un procesador. De modo que se podría calificar al DVR como un ordenador especializado en el tratamiento de imágenes digitales.

Así el DVR se ha diferenciado de su predecesor analógico el VCR (Video Cassette Recording) en el cual tan solo se podían almacenar imágenes de forma pasiva, con la posibilidad de rebobinarlas hacia delante o hacia atrás, y por supuesto pausarlas.

Figura. 2.3. DVR

2.5.1.4. Circuito cerrado de televisión con transmisión digital.

La solución digital es más sencilla y económica de lo que se suele pensar. Incluso con el crecimiento del CCTV y la reciente aceleración de la migración hacia la tecnología de video digital, aun existen muchos obstáculos para una mayoría de usuarios a la hora de cambiar de la grabación de video analógica a la digital. Muchos usuarios finales no son aun conscientes de que hay un camino paso a paso disponible para transformar los actuales sistemas de seguridad analógicos a la tecnología digital.

En términos de educación, la mayoría de los usuarios finales aun precisan un conocimiento más profundo de los beneficios y posibilidades de los sistemas de vigilancia digitales basados en redes. También es importante saber que en la transición de un sistema de vigilancia analógico a uno digital, ningún sistema es demasiado pequeño o demasiado asociado a tecnología analógica, para beneficiarse de la tecnología digital. Incluso una sola cámara conectada a un servidor de video proporcionará al usuario final todo el rango de beneficios que vienen asociados a la vigilancia digital en red.

Considere la sencillez y el ahorro de costes de una migración progresiva y paso a paso hacia la Vigilancia IP. Ahora es el momento adecuado para dar el paso digital.

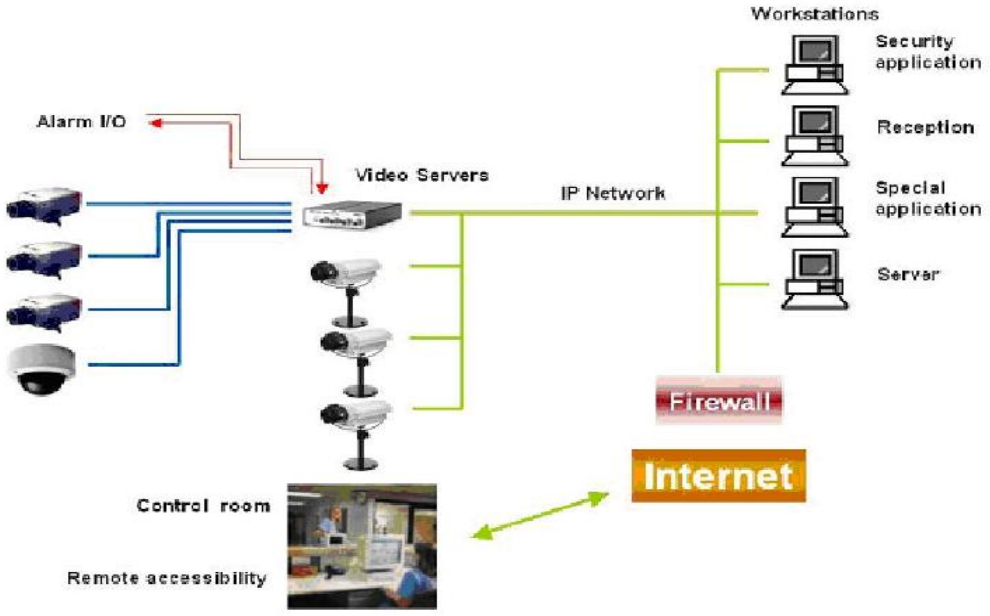


Figura 2.4. La revolución digital.

La actualización de la revolución digital: la tecnología de servidor de vídeo en la configuración de la figura 2.4, el servidor de vídeo proporciona la conexión entre las cámaras y la red. Con la simple incorporación de esta tecnología, están disponibles una amplia lista de nuevas características y funciones:

- Acceso remoto a las imágenes usando la red informática, lo que además elimina la necesidad de monitores de seguridad dedicados en la oficina central.

- Acceso protegido por contraseña allá donde haya una conexión a Internet.

- Conexión a una estación de control remoto para visualizar lo que está ocurriendo y controlar las cámaras y otros aspectos del sistema de vigilancia.

- Fácil integración con otros sistemas y aplicaciones.

- Menor Coste total de propiedad (Total Cost of Ownership, TCO) al aprovechar la infraestructura y equipamiento heredado.

- Crear sistemas preparados para el futuro, de manera que se terminaron las revisiones completas del sistema.

El estándar más habitual para redes inalámbricas de área local (WLAN) es la norma IEEE 802.11. Si bien existen otros estándares y otras tecnologías patentadas, la ventaja de utilizar los estándares inalámbricos 802.11 es que funcionan en un ámbito sin licencia, de manera que no implican ningún coste asociado a la configuración y al funcionamiento de la red. Las extensiones más relevantes del estándar son 802.11b, 802.11g, 802.11a y 802.11n.

La extensión 802.11b, aprobada en 1999, funciona a 2,4 GHz y proporciona velocidades de hasta 11 Mbit/s. Hasta el año 2004, la mayoría de productos WLAN que se vendían se basaban en 802.11b.

La extensión 802.11g, aprobada en 2003, es la variedad más común de 802.11 del mercado. Funciona a 2.4 GHz y proporciona velocidades de hasta 54 Mbit/s. En general, los productos WLAN son compatibles con 802.11b/g.

La extensión 802.11a, aprobada en 1999, funciona en la frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbit/s. En algunas partes de Europa, la banda de frecuencia de 5 GHz no está disponible, ya que se utiliza para sistemas de radar militares. En estas áreas, los componentes WLAN a 5 GHz deben cumplir el estándar 802.11a/h. Otra desventaja de la extensión 802.11a es que la cobertura de la señal es inferior a la de 802.11g, ya que funciona en una frecuencia superior. Así, se requieren muchos más puntos de acceso para la transmisión en la banda de 5 GHz que en la de 2.4 GHz.

Al configurar una red inalámbrica, es importante tener en cuenta la capacidad de ancho de banda del punto de acceso y los requisitos de ancho de banda de los dispositivos de red. Normalmente, el caudal de datos útil admitido por un estándar WLAN específico es aproximadamente la mitad de la tasa de bits estipulada por el mismo debido a la sobrecarga de la señal y del protocolo. En el caso de las cámaras compatibles con 802.11g, no se deben conectar más de cuatro o cinco cámaras a un punto de acceso inalámbrico.

El estándar más habitual para redes inalámbricas de área local (WLAN) es la norma IEEE 802.11. Si bien existen otros estándares y otras tecnologías patentadas, la ventaja de utilizar los estándares inalámbricos 802.11 es que funcionan en un ámbito sin licencia, de manera que no implican ningún coste

asociado a la configuración y al funcionamiento de la red. Las extensiones más relevantes del estándar son 802.11b, 802.11g, 802.11a y 802.11n.

2.6. ESTUDIO DEL DESEMPEÑO DE LA TECNOLOGÍA WIFI EN LOS DIFERENTES AMBIENTES POSIBLES PARA SU DESEMPEÑO.

La claridad de señal es la clave para la realización de una comunicación Wireless. Algunos de los factores que afectan la claridad son:

- **Potencia de la señal**: Obviamente, una señal fuerte permite una mejor recepción en largas distancias. La normativa en España para el nivel de señal en transmisión Wireless es de 100mW para la frecuencia de 2'4GHz y de 1W para la frecuencia de 5'4GHz.

- **Distancia**: La potencia de la señal de radiofrecuencia (RF) disminuye con la distancia. Además se pueden sumar interferencias no deseadas con lo que se consiguen distancias menores. Como se verá más adelante, la señal puede ser modificada de diferentes formas para adecuarla a la distancia que tenga que recorrer (tipos de antenas).

- **Interferencias**: Los factores atmosféricos, como la nieve, la lluvia o el granizo, pueden interferir en la señal. Es un dato a tener en cuenta cuando se quieren realizar enlaces wireless en exteriores. Normalmente las interferencias de RF son causadas por aparatos que están emitendo cerca, en la misma banda y mismo canal que nosotros. También se consideran interferencias a las transmisiónes wifi que esten en el mismo canal que nuestra señal, por lo que siempre es conveniente utilizar el canal menos utilizado. Incluso otros sistemas de RF como puede ser microondas o cualquier otro sistema también puede interferir y degradar el nivel de nuestra señal.

- **Línea de visión**: La señal necesita visión directa para realizar bien la comunicación. Si hay obstáculos en la línea de visión, no se podrá realizar la conexión. La transmisión Wifi está sólo es válida para enlaces con visión directa. Aunque en interiores es posible que aprovechando los rebotes de la señal en paredes u otros objetos, pero en ningún caso se ofrece una garantia

de señal al traspasar un objeto por fino que pueda ser este, se podría conseguir un enlace wireless.[15]

Para el presente proyecto se debe tomar en cuenta la probabilidad de utilizarlo en los siguientes ambientes:

- En oficinas.
- En edificaciones y en instalaciones donde haya equipos de transmisión (radiofrecuencia para la comunicación).
- En el Terreno. (Vegetación)

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debida a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

2.7. ANÁLISIS DE LA APLICABILIDAD DE UN SISTEMA DE VIDEO VIGILANCIA A UNA UNIDAD DE COMBATE.

Los militares siempre han utilizado dispositivos de vigilancia de una forma u otra, la diferencia es que hoy se pueden implementar para una gran variedad de propósitos y así avanzar hacia sistemas mucho más complejos como los sistemas semi-inteligentes. Los acontecimientos ocurridos el 11 de septiembre del 2001 en los EE UU son un claro ejemplo de la fragilidad de la seguridad nacional de un país y es justificación absoluta para reforzarla de manera drástica y con todas las herramientas necesarias, para ello la revolución tecnológica militar es uno de los caminos a seguir.

Los sistemas militares cibernéticos donde las armas son simplemente el músculo desplegado por un sistema nervioso basado en un inteligente manejo de datos a través de comunicaciones, mando y control (C3I2[16]); es el futuro de la seguridad

[15] Extracto sacado de: http://www.wifisafe.com/conceptos_wireless.php
[16] Comando control comunicaciones, inteligencia e informática del Comando conjunto de las FFAA.

nacional en Ecuador. Por todo esto se optó por realizar un análisis para adaptar la tecnología inalámbrica de un CCTV a una unidad de combate.

Figura 2.5. Parte de un núcleo de combate en un ambiente abierto

Entonces se empieza por conocer, ¿qué es una Unidad de Combate?. La Unidad de Combate es la mínima cantidad de hombres, armados y equipados que se desenvuelve de manera completa en cualquier situación de combate ya sea este especial[17] o regular[18].

Para un combate especial la Unidad de Combate se puede dividir en equipos de combate y estos a su vez en núcleos de combate conformados por 8 o 10 personas dependiendo la situación.

En la figura 2.5 se observa parte del núcleo de combate realizando sus maniobras en un terreno abierto y en donde se podría utilizar un CCTV.

Si se pudiera realizar la supervisión de toda la operación a tiempo real, las condiciones de control y el desenvolvimiento de cada uno de los miembros de esta unidad serían excelentes. La supervisión de la operación se la realizaría desde un punto cercano a las operaciones y en donde se encontrarían los equipos de visualización.

[17] Combate Especial: Combate Urbano, Combate a Guerrillas ó Combate a grupos armados organizados.
[18] Combate Regular: Combate entre Ejércitos.

Para esto se tendría que utilizar una cámara por individuo, pero esta cámara debería ser lo suficientemente liviana y pequeña para que no estorbe al desempeño del soldado y también de suficiente resolución como para grabar imágenes en movimiento y también estar diseñada para soportar el movimiento del personal que la porta.

Además si se emplea en operaciones especiales, podría utilizarse en la noche, así que debería tener funciones especiales como por ejemplo: ser infrarroja.

Las mini cámaras con Motion JPEG son una buena elección debido a su simplicidad. Esto asegura un equipamiento económico y un consumo de ancho de banda ligeramente superior que con JPEG. Para un uso más eficiente del ancho de banda es recomendable el uso de alguno de los estándares de compresión de imágenes en movimiento: MPEG-1, MPEG-2 que proporciona algunas ventajas y mayor calidad de imagen o, MPG-4 si se necesita mayor calidad de imagen.

Así los transmisores, algunos ya incorporados en las cámaras, también deben ajustarse a las necesidades del núcleo de combate. Un transmisor con tecnología Wifi es lo ideal, por su fácil acceso a una mayor variedad de tecnología y porque no se necesita transmitir a grandes distancias, sino a un puesto de mando cercano a la operación en desarrollo.

También se podrían utilizar transmisores FM o AM, pero son transmisores grandes y que le quitarían la movilidad al núcleo de combate a demás de consumir mucha energía, con lo cual implicaría llevar más fuentes de energía (baterías de mayor duración).

La tecnología Wifi necesita de línea de vista para una óptima transmisión, es por esto que se resta la movilidad y la aplicabilidad en sectores donde haya objetos que obstruyen la conexión, aunque se podría aprovechar el rebote de la señal en los objetos, la transmisión no se la podría garantizar. Un transmisor con tecnología Bluetooth[19], es poco recomendable por su alcance sobre todo y por su interrupción ante los obstáculos.

Para la visualización se debe tomar en consideración la energía, lo más recomendable es utilizar una PC portátil equipada con tarjeta de captura de video, por su versatilidad y además porque no necesita energía de la red eléctrica. Una PC portátil nos brinda muchas más ventajas y su batería dura de 2 a 3 horas, en

[19] Bluetooth: Especificación industrial para Redes Inalámbricas de Área Personal (WPANs).

algunas llegando hasta las 4 a 5 horas si se les optimiza el consumo de energía. Y con esto se tendría una unidad móvil.

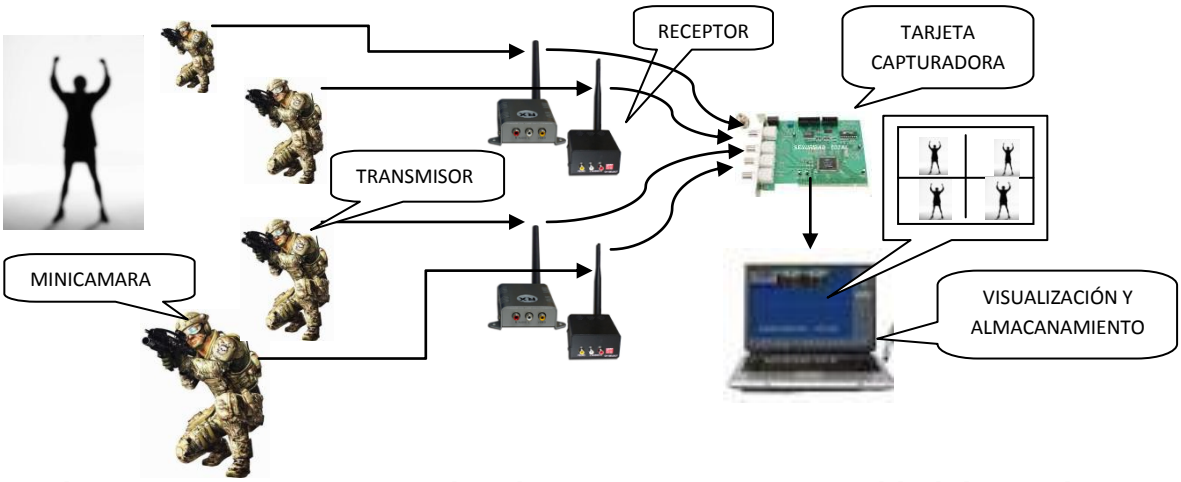


Figura 2.6. Esquema tentativo de un CCTV para una unidad de combate.

2.8. ANÁLISIS COMPARATIVO DE UN CCTV.

Toda la industria dedicada al CCTV habla acerca de la tecnología IP; incluso hay quien se aventura a predecir una muerte prematura de las cámaras análogas. Si bien algunas cámaras IP pueden ofrecer resoluciones en mega píxeles, las cámaras análogas siguen ofreciendo una mayor eficiencia, menor costo y mayor confiabilidad.

Antes de decidir entre cámaras IP o análogas, es necesario entender cómo funcionan estas tecnologías. Las diferencias entre ambas cámaras, sus tecnologías y los métodos de transmisión, son cruciales para el desarrollo de una solución de CCTV bien planeada.

2.8.1. FUNCIONAMIENTO DE UNA CÁMARA DE CCTV.

De inicio, las cámaras IP y las análogas, pueden parecer mas similares de lo que realmente son; ambas emplean sensores CCD[20] o CMOS[21]. Mientras que prácticamente todas las cámaras análogas usan lectores CCD, la mayoría de las cámaras IP actuales utilizan lectores CCD o CMOS indiferentemente. La señal

[20] CCD dispositivo de carga acoplada
[21] CMOS semiconductor complementario de oxido metálico.

análoga del sensor se convertirá a digital por medio de un conversor análogo - digital y luego al procesador de imagen a bordo de la cámara. En la cámara IP, la imagen será comprimida internamente (codificada) y transmitida por medio de protocolos IP en redes Ethernet hacia los grabadores (NVR); en la cámara análoga, el video se reconvierte nuevamente a análogo mediante un convertidor digital - análogo de forma que la imagen pueda ser transmitida hacia los grabadores (DVR) donde la señal es codificada y almacenada.

Hasta este punto, pareciera que la diferencia entre estos tipos de cámaras no es importante; la diferencia es donde se comprime o codifica el video y que componentes utiliza. Hay diferencias significativas de calidad entre los sensores CCD y CMOS con una demostrable superioridad de los sensores CCD.

Funcionamiento de los sensores.

Los sensores CCD contienen cientos de miles (o millones en el caso de las cámaras con resolución en mega píxeles) de elementos de imagen llamados pixeles; cada pixel contiene un elemento sensible y un capacitor. El capacitor mantiene una carga que es proporcional a la cantidad de luz que incide en la superficie del pixel, que es luego transferida esa carga de voltaje y la digitaliza.

Un sensor CMOS está construido de arreglos similares de pixeles, pero tiene el capacitor que retiene la carga para cada pixel; las filas de pixeles son activadas secuencialmente y la cantidad de luz que incide en la superficie del pixel es convertida en voltaje y leída directamente al tiempo de la exposición.

Es de especial atención para la video vigilancia, mantener la calidad de la imagen en todo el espectro de condiciones de iluminación; en este aspecto, los sensores CMOS tienen debilidades significativas comparados con los de CCD. Como la tecnología CMOS tiende a tener menor habilidad en el manejo de la luz, no compensa adecuadamente en condiciones de iluminación frontal y es propenso a generar sombras y ruido en condiciones de baja iluminación

Para intentar solventar estos problemas, una tecnología nueva llamada WDR[22], ha evolucionado y promete mucho. Una cámara WDR escanea el mismo cuadro dos veces, uno por un sensor lento y luego por uno de alta velocidad; los dos cuadros son entonces procesados pixel por pixel y resulta en un único cuadro de salida. La tecnología WDR compensa en condiciones de fondos brillantes o de baja iluminación, produciendo imágenes claras con bajo nivel de ruido y con buen contraste. A la fecha, la tecnología WDR no ha sido aplicada a ninguna cámara IP mega pixel de alta definición.

[22] WDR amplio rango dinámico.

Otra área de preocupación para la video vigilancia son las distorsiones conocidas como “artefactos de movimiento”; nuevamente, los sensores CCD se desempeñan mejor que los CMOS en condiciones de mucho movimiento debido al diferente tipo de disparador utilizado.

El disparador se refiere a la manera en la cual una videocámara presenta la luz al sensor; un sensor CCD usa un disparador global que significa que el sensor entero es habilitado en un mismo momento, tomando así una foto o cuadro por vez. Cada pixel de salida es almacenado en su capacitor y es leído por el circuito antes de tomar el siguiente cuadro.

Los sensores CMOS usan un disparador secuencial; debido a la falta de almacenamiento de carga, la información de cada pixel es leída secuencialmente en pequeños grupos de pixeles, comenzando desde arriba y descendiendo por todo el arreglo de pixeles, exponiendo solo una porción del arreglo por vez, como el sensor lee diferentes porciones del cuadro en diferentes momentos mientras es capturado, esto provoca artefactos de movimiento como manchones, temblor de la imagen y en algunos casos, la exposición parcial.

Ambos tipos de cámaras son más similares que diferentes en la captura de la imágenes; sin embargo, en el tema de los métodos de transmisión del video, las diferencias son significativas.

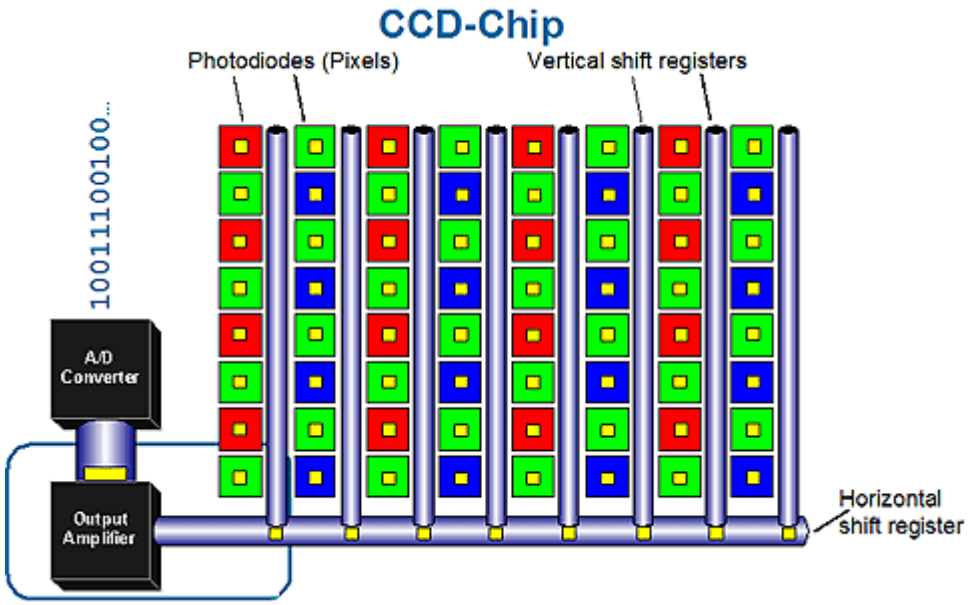


Fig. 2.7 Tecnología de sensores en las cámaras.

2.8.2. CÁMARA IP.

Lo que comúnmente se conoce como cámara IP, es una cámara que digitaliza y procesa imágenes análogas, que después codifica internamente para ser enviadas por medio de conexiones Ethernet hacia computadoras o equipos similares. Las cámaras IP pueden tener sensores CCD o CMOS y están disponibles en los mismos estilos que las cámaras tradicionales de vigilancia, algunas incluyen movimiento vertical, movimiento lateral y acercamiento en forma de domos, tipo bala, con iluminación infrarroja, camufladas y en ocasiones con conexión WiFi[23].

Típicamente están equipadas con un servidor web integrado y se pueden accesar y controlar por medio de cualquier red IP como WAN[24], LAN[25], Intranet o Internet; ya que se utilizan navegadores web estándar o clientes de software, los usuarios pueden ver sus imágenes desde cualquier ubicación local o remota. Las cámaras IP combinan las capacidades de una cámara con las de una computadora; no requieren una conexión directa o dedicada a una computadora y pueden ser colocadas en cualquier lugar dentro de la red, justo como se haría con cualquier computadora. Una cámara IP es un dispositivo de red, tiene su propia dirección IP, se conectan por cable o WiFi a la red y requieren mantenimiento.

2.8.3. CÁMARA ANALÓGICA.

Una cámara de vigilancia análoga comienza con un sensor CCD y luego digitaliza la imagen para ser procesada posteriormente, pero antes de que el video sea enviado, deberá volver a convertirse en análogo para que pueda ser recibido por un equipo análogo como un monitor o grabador. Diferente a las cámaras IP, las cámaras análogas no tienen ningún tipo de servidor interno o codificadores y no requieren de mantenimiento técnico; estas funciones son implementadas en el equipo de control y grabación.

2.8.4. DIFERENCIAS ENTRE LAS CARACTERÍSTICAS DE UNA CÁMARA DIGITAL Y UNA CÁMARA ANALÓGICA.

La principal diferencia entre las cámaras análogas y las IP es el método por el cual la señal de video es transmitida codificado.

[23] WIFI fidelidad inalámbrica.
[24] WAN redes de área amplia.
[25] LAN redes de área local.

Calidad de video:

Tecnología IP.

Las cámaras IP pueden capturar imágenes de alta resolución en mega píxeles, pero tienen problemas en condiciones de baja iluminación. Cuadros perdidos y artefactos de movimiento son muy comunes en las cámaras IP con lector CMOS. Las cámaras IP están limitadas en sus recursos de codificación, como resultado, se tiene que hacer una meticulosa selección con respecto a la codificación, velocidad de captura y calidad; donde la preferencia de una decrementa a otra característica. Desde que el video sea comprimido antes de ser monitoreado o almacenado, nunca podrá tener la mejor calidad de imagen o video en tiempo real. Codificar el video en la cámara agrega retrasos que son un problema cuando un operador necesita seguir algo mediante los controles de movimiento.

Tecnología analógica.

Las cámaras análogas se desempeñan muy bien en casi cualquier condición de iluminación y manejan de forma correcta la captura del movimiento, no tienen capacidades diferentes a los estándares PAL[26] / NTSC[27], el video es comprimido en el grabador (DVR) donde muchos más recursos de software y hardware están disponibles, lo cual resulta en una mayor calidad de video y mas cuadros por segundo. Las cámaras análogas transmiten video al DVR sin comprimir, donde puede ser monitoreado en vivo sin el retraso que genera la compresión previa.

Infraestructura de cableado:

Tecnología digital.

Una ventaja que se percibe de las cámaras IP es la habilidad de usar el cableado de red existente para soportar un sistema de video vigilancia, pero también limita la distancia total a 330 pies según las normas TIA/EIA-568-B[28]. El cableado estructurado es capaz de transmitir alimentación eléctrica, video, voz y datos.

Tecnología analógica.

El cableado común para cámaras análogas utiliza cable coaxial, que es algo anticuado; los integradores actualizados utilizan convertidores para transmitir video análogo, alimentación eléctrica y datos sobre infraestructura de cableado de red por encima de las limitaciones TIA/EIA. Utilizando estos convertidores, el video análogo puede ser transmitido de forma eficiente a más de 2 km y la

[26] Línea de fase alternada, sistema de codificación utilizado en la transmisión de señales de tv. Analógica.
[27] Comité nacional de estándares de televisión.
[28] Tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones.

alimentación eléctrica cerca de 300 metros. También existen convertidores activos que pueden extender dicha transmisión usando cable Cat 5.

Una complicación son los límites del estándar PoE[29] a 12.9W, que son insuficientes para muchas de las cámaras con iluminadores infrarrojos o que requieren calentadores o ventiladores para su operación. Incluso con el nuevo estándar PoE+, el límite de 25W resulta insuficiente; cuando menos se requieren 70W para operar una cámara exterior PTZ[30] de alto desempeño, así que será necesario correr un cableado adicional para la alimentación eléctrica.

Video transmisión:

Tecnología digital.

Mientras que algunas cámaras IP pueden almacenar cantidades limitadas de video internamente, una falla en la infraestructura de red resultara en la pérdida de la imagen en vivo y su posible almacenamiento. Intentar limitar las fallas en la infraestructura de red usando sofisticados equipos de triple capa, redes redundantes u otros, puede resultar una tarea significativamente compleja y costosa. También, las redes pueden resultar infectadas por virus o software mal intencionado con consecuencias catastróficas. Las cámaras IP son dispositivos de red y como tales, requieren de administración y manejo, lo cual las vuelve vulnerables.

Tecnología analógica.

Las cámaras análogas están limitadas a las fallas propias de cada uno de los equipos del sistema y la pérdida de una sola pieza de equipo no causara la degradación o pérdida total del sistema. La transmisión usualmente es pasiva y ya instalada, prácticamente no requiere de ningún mantenimiento. Las cámaras análogas son una tecnología muy madura y tienen un largo historial de servicio.

Seguridad:

Tecnología digital.

Los envíos de video IP pueden ser encriptados y son difíciles de interceptar; por otro lado, la red está sujeta a la infección de virus y otro tipo de ataques. En una red, cada cámara (y puede haber miles en un mismo sistema) y los todos los dispositivos que se comunican en ella, son sujeto de ataques de hackers en cualquier lugar del mundo.

[29] Alimentación a través de Ethernet, fuente de alimentación inteligente.
[30] Las cámaras PTZ pueden moverse horizontalmente, verticalmente de forma manual o automática.

Tecnología analógica.

Las señales análogas son menos seguras y pueden ser interceptadas o visualizadas por cualquiera que tenga acceso a la infraestructura de cableado. Con la posible excepción del DVR, todo el sistema es inmune a virus y otros tipos de ataques; para accesar o interferir con el sistema, es necesario tener contacto físico con los equipos o la infraestructura de cableado.

Mantenimiento:

Tecnología digital.

Una cámara IP es un dispositivo de red que requiere de cierto nivel de conocimiento para su manejo y administración. El costo estimado del mantenimiento de un dispositivo de red (por dirección IP) está en el rango entre los $100 y los $400 USD anuales.

Tecnología analógica.

Las cámaras análogas no requieren de ningún tipo de administración, no existen direcciones IP, no hay programación de por medio, no involucra software, ningún tipo de conocimiento adicional, etc. Toda vez instaladas, virtualmente no requieren mantenimiento alguno.

Inalámbrico:

Tecnología digital.

Una clara ventaja de las cámaras IP es la flexibilidad de integración con las redes WiFi, que son prácticamente ilimitadas en términos de expansión; el ancho de banda, y la topología siguen siendo un punto de preocupación.

Tecnología analógica.

El número de cámaras análogas usando radio frecuencias para transmitir el video de forma inalámbrica, están limitadas a una docena antes de llegar al límite de capacidad del espectro en las bandas libres de radio.

Instalación:

Tecnología digital.

Las cámaras IP requieren de un nivel básico de conocimientos de integración de redes en instalaciones pequeñas y significativamente mayores capacidades técnicas mientras el tamaño del sistema sea incrementado.

Tecnología analógica.

Las cámaras análogas requieren de un mínimo o ningún conocimiento de redes y configuración; solo alimente, apunte y enfoque, sin importar el tamaño total del sistema.

Compatibilidad:

Tecnología digital.

Las cámaras IP requieren un grabador de video en red (NVR) o navegador para comunicar cada cámara en particular, que puede ser propietario o único. Cada vez que se agrega una cámara, tendrá que asegurarse que el NVR soporte ese modelo en particular. Un NVR puede soportar un número limitado de cámaras de un fabricante específico; muchos productores tienen una gran variedad de protocolos de comunicación en sus líneas de modelos.

Tecnología analógica.

Cualquier cámara análoga puede ser conectada a cualquier DVR, no hay diferencias de compatibilidad cuando se sustituye o agrega una cámara o DVR al sistema. Como nota adicional, muchos de los DVR actuales son híbridos y permiten una comunicación y administración transparente con cámaras análogas e IP en una misma interfaz de software.

Vigencia:

Tecnología digital.

Mientras que las cámaras IP tienen en el mercado cerca de una década, aun representan solo el 15% del total instalado. La tecnología IP aun es inmadura y aun tiene mucho camino por recorrer; los modelos actuales serán rápidamente reemplazados por otros con mejor calidad, más eficiencia, mayores características, más baratas y más confiables.

Tecnología analógica.

Las cámaras análogas son estables y maduras, tienen un historial de servicio bien definido así como sus aplicaciones y propósitos; continuaran siendo importantes en el mercado gracias a su dominio.

Escalabilidad:

Tecnología IP.

Una de las ventajas de las cámaras IP es la habilidad de agregar cámaras conectándolas a la infraestructura de red; cuando se escala un sistema de cámaras IP a nivel empresarial, hay requerimientos substanciales de manejo y administración de redes, equipamiento y un ancho de banda importante.

Tecnología analógica.

Los sistemas análogos pueden ser expandidos prácticamente sin requerimientos adicionales de ancho de banda o transmisión de datos entre cámaras y grabadores. Mientras que las cámaras análogas no requieren de ancho de banda, pueden ser escaladas de forma exponencial con un mínimo de compromisos ya que son conectadas directamente a los DVR sin pasar por transmisión por red.

Costo:
Tecnología IP.

Las cámaras IP pueden ser hasta 3 veces más caras que sus equivalentes análogos; adicionalmente, puede haber costos de licenciamiento por cámara para conectarlas al NVR[31]. En algunas instancias, las cámaras IP pueden ser más efectivas en relación a su costo en situaciones donde la infraestructura de cableado llegue a representar un problema mayor. Instalaciones grandes requieren de equipamiento administrador de redes y periféricos que pueden resultar en altos costos.

Tecnología analógica.

Las cámaras análogas y sus equipos periféricos son significativamente más económicos que sus contrapartes de tecnología IP, requieren muy poco o ningún equipo de administración de señales, lo que reduce costos, especialmente en instalaciones grandes. Para las aplicaciones típicas, cuando se contabiliza el equipamiento, software y la instalación, la tecnología análoga es una propuesta más valiosa.

Mientras que las cámaras IP son más caras, no deben ser juzgadas solo por su costo; no es una competencia entre tecnologías. El uso apropiado y la combinación de ambas como una solución programada para brindar beneficios al cliente y solventar sus necesidades de video vigilancia, deberá ser el factor

[31] Video grabadores en red.

determinante.

Idealmente, el usuario final debería ser capaz de conectar cualquier cámara IP o análoga a cualquier equipo de grabación, NVR o DVR, sin complicaciones, sin preocuparse por su vigencia, o temer por la operatividad del sistema; esto es utópico en el mercado actual, se tiene que impulsar la propuesta de aplicación de estándares abiertos en la industria de CCTV.

Mientras tanto, las grandes aplicaciones inalámbricas en mega píxeles es el área fuerte de la tecnología IP, para la mayoría de las demás aplicaciones, el uso de cámaras análogas es más adecuado, más práctico, confiable, fácil de operar, fácil de instalar, más confiable y con una mejor relación costo - beneficio.

CAPÍTULO III

RESULTADOS

3.1. APLICABILIDAD DE UN CCTV A TECNOLOGÍA PORTÁTIL PARA USOS GENERALES.

Se ha visto que la tecnología wifi es muy versátil y que también los diferentes aparatos wifi pueden llegar a utilizar poca energía, por lo que es muy fácil de utilizarla con baterías, como es el caso de las laptops o también de los transmisores y receptores indicados en los capítulos anteriores.

Es así que se puede afirmar que sí es factible adaptar un CCTV a tecnología portátil. Por ejemplo: para una bodega militar en la que siempre se está modificando y actualizando, según las necesidades, la distribución de las diferentes secciones; sería muy útil que todo el CCTV a utilizar, sea portátil para poder adaptarlo a estas necesidades y los cambios, muy necesarios, para mantener la optimización propia de una unidad militar.

Lo que en realidad garantiza que todo un equipo de CCTV sea portátil, es la posibilidad de montarlo y desmontarlo sin la necesidad utilizar cables, para que sea flexible de cambiar de lugar a sus dispositivos, sin tener que romper paredes, tuberías, regletas y cables. Únicamente tendríamos que tomar en cuenta que los transmisores garanticen la señal hacia el receptor.

Entonces un CCTV portátil para aplicaciones generales, tendría la siguiente estructura:

- Cámaras:
    - Mini cámaras inalámbricas.
    - Cámaras domo.
    - Cámaras infrarrojas.
    - Cámaras con movimiento y Zoom.

- Transmisores:
    - Transmisores incorporados en las cámaras.
    - Transmisores de audio y video de gran alcance.
    - Amplificadores de señal para mayores distancias.

- Receptores:
    - Receptores de varios canales.
    - Receptores de un solo canal.

- Tarjeta capturadora de video (DVR):
    - Tarjetas internas para slots y zócalos DDR.
    - Tarjetas externas para conexión USB.
    - Tarjetas con varias entradas de Video y Audio (2, 4, 8, …).
    - Pequeña consola con conexión a PC.

- Software para manejar y gestionar las cámaras:
    - Software de la tarjeta capturadora.
    - Software de consola.
    - Software para gestionar y manejar las cámaras. (movimiento y zoom)

- PC para visualización y almacenamiento.
    - Laptop.
    - Discos duros externos.

3.2. DESARROLLO DE UN PROTOTIPO.

3.3.1. LUGAR DE IMPLEMENTACIÓN.

El presente prototipo de CCTV inalámbrico se implementó en el Laboratorio de Comunicaciones de la ESPE sede Latacunga. El dispositivo de las cámaras se encuentra detallado en el ANEXO A.

3.3.2. INSTALACIÓN.

Primero se selecciona la tarjeta de video (DVR) de acuerdo a las necesidades de seguridad. La tarjeta ha ocuparse es la DR3004F de la marca Surveillance System.

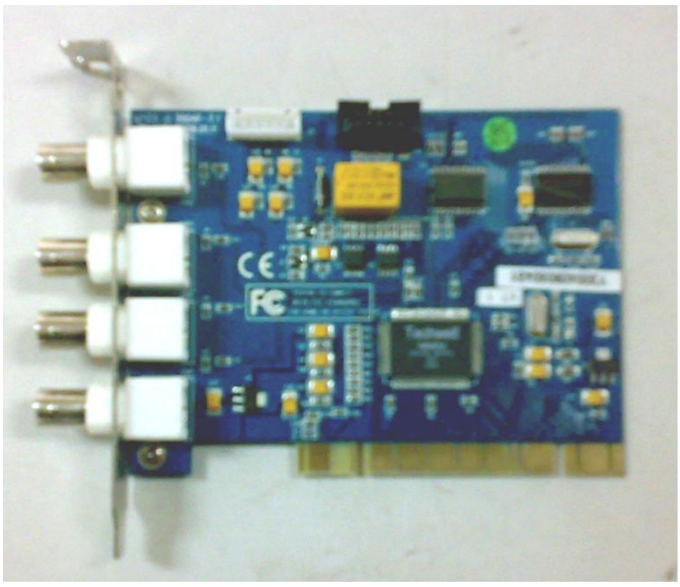


Figura 3.4 Tarjeta DR3004F

Para instalar esta tarjeta se destapa el keys y se la inserta en uno de los slots de expansión, como se observa en la figura 3.5.

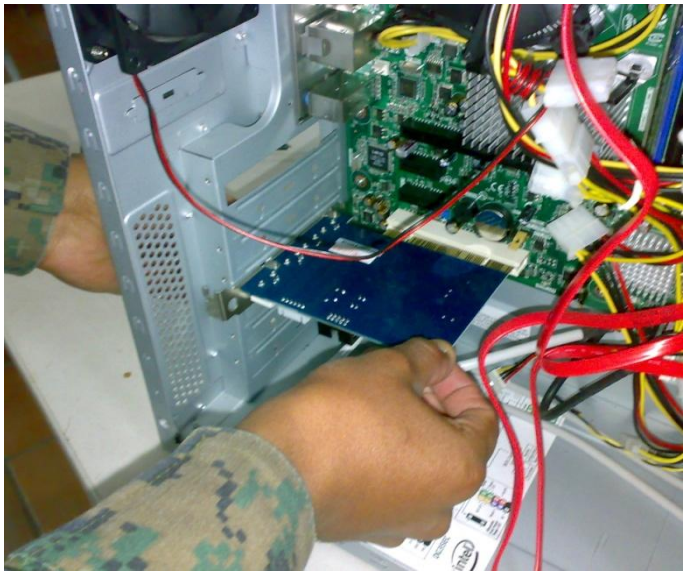


Figura 3.5 Instalación de la Tarjeta DVR

Se debe asegurar bien la tarjeta para evitar cualquier falla de funcionamiento. Una vez insertada la tarjeta, se coloca la taba del keys para luego encender la PC e instalar el software de la tarjeta.

Instalación del Software.

Desde el menú que se despliega en la pantalla al momento de insertar el CD de la tarjeta Ejecutar setup.exe, y la interfaz de instalación aparece como se indica en la siguiente pantalla:

Figura 3.6 Setup.exe

Luego aparece un cuadro como en la figura 3.7. Se debe seleccionar siguiente.

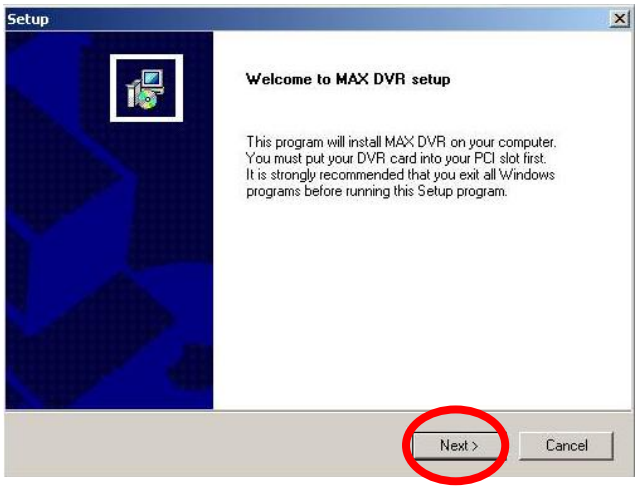


Figura 3.7 Inicio setup

A continuación se escoge el formato de video haciendo clic en NTSC y seleccionar siguiente. Figura 3.8.

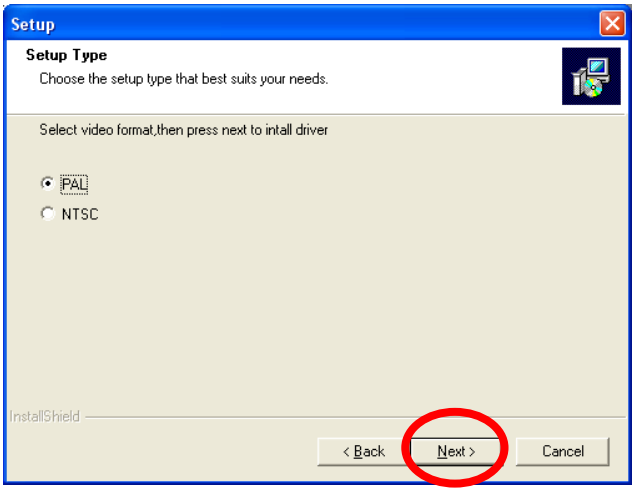


Figura 3.8 Selección de formato de video

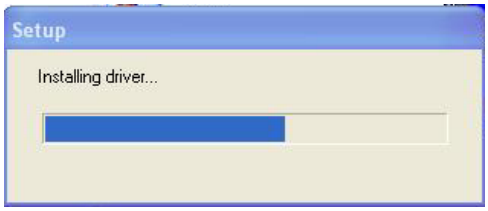


Figura 3.9 Progreso de la instalación.

Después de estos pasos, comienza la instalación como en la figura 3.9, de la aplicación del paquete MAX DVR.

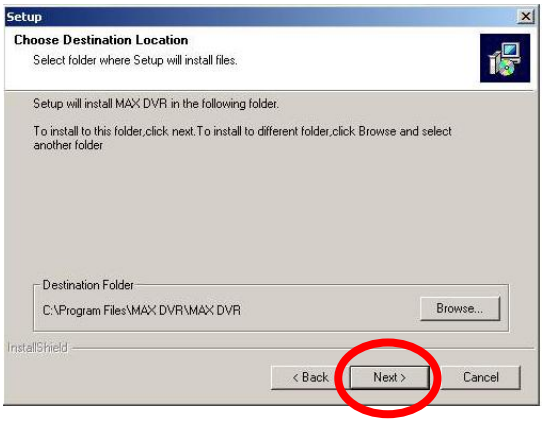


Figura 3.10 Paso de la instalación.

Luego se selecciona la dirección en donde se desee instalar la aplicación y haga clic en siguiente. Figura 3.10.

Haga clic en siguiente. Figura 3.11.

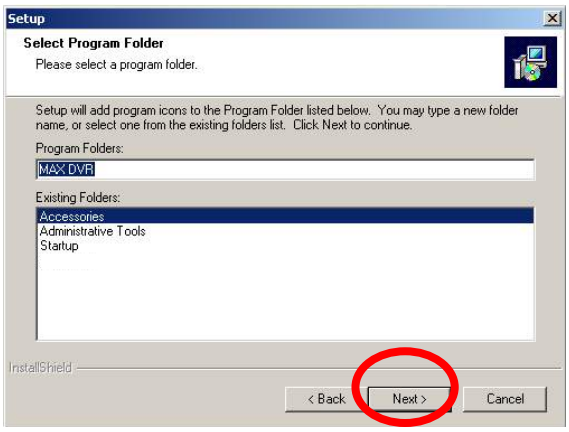


Figura 3.11 Registro de aplicación.

Por último hacer clic en finalizar como se muestra en la figura 3.12.

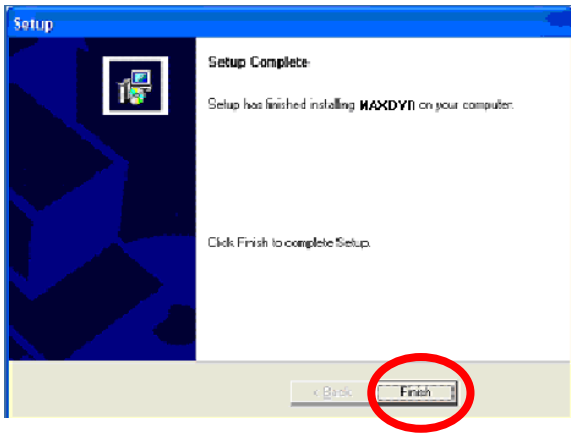


Figura 3.12 Instalación de aplicaciones terminada.

Después de haber terminado todo el proceso, reinicie el ordenador. Se creará un acceso directo en el escritorio como en la figura 3.13.

Figura 3.13 Acceso directo de MAX DVR

Instalación de las Cámaras.

Para la instalación se ocupó la cámara Wireless PPW-245UK, cuyas características se detallan en el ANEXO B, tomando en cuenta el dispositivo de la figura 3.14 pero con la diferencia de que se va a visualizar en una PC.

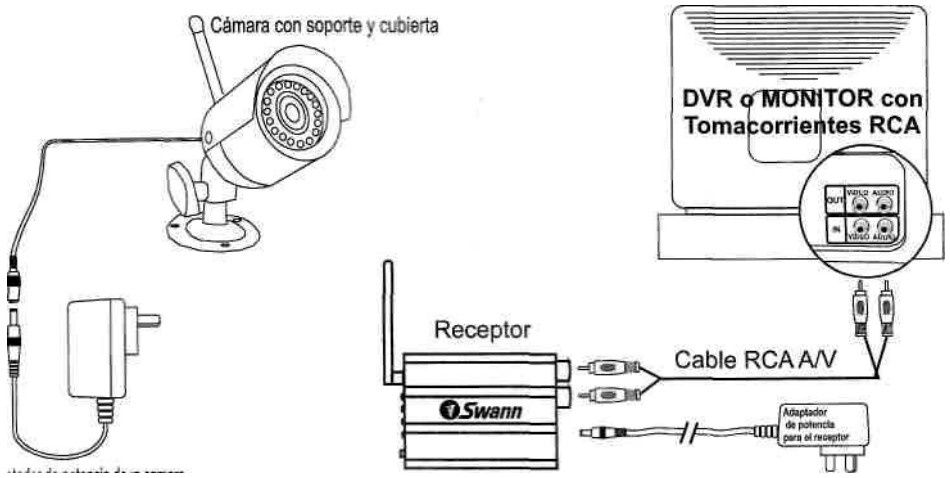


Figura 3.14 Instalación de las cámaras.

La cámara posee una antena omnidireccional que es más efectiva cuando se usa en posición VERTICAL. Tomando en cuenta esto se procede de la siguiente forma:

1.- Conectar la Cámara y el Receptor a sus adaptadores de potencia respectivos (los Adaptadores tienen una etiqueta al final del cable para indicar con qué unidad deben usarse).

Figura 3.15 Conjunto Transmisor-Receptor

2.- Conectar el Receptor al equipo en el que desea visualizar la cámara (monitor, AV TV, VCR, DVR, etc) utilizando el cable RCA A/V suministrado. Si se tiene una

TV A/V con tomacorrientes RCA, necesitará encender la TV en el canal AV para visualizar la cámara. Para visualizar el receptor en su VCR, deberá colocar el VCR a la selección de entrada AV y encender la TV en el canal que normalmente utilizaría para ver una tintado película en el VCR. En este caso se va a visualizar en una PC con una tarjeta de entradas BNC, para lo cual es necesario utilizar un adaptador de conector RCA A/V a BNC. (Figura 3.15)

Figura 3.16 Adaptaros de RCA A/V a BNC

3.- Luego de conectar la cámara y el receptor, se debe asegurar de que el receptor se encuentre sintonizado en el mismo canal que la cámara. (Figura 3.17) Presionar el botón Selección de Canal del receptor hasta que se encienda el LED. Se obtiene la mejor imagen ajustando la posición de la cámara y el receptor.

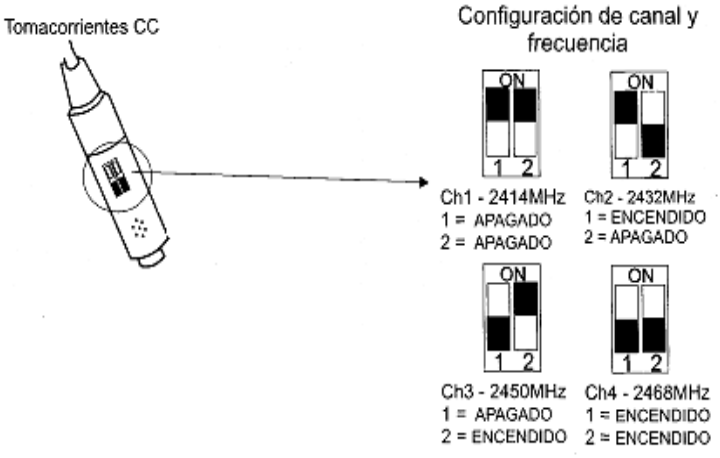


Figura 3.17 Partes de la cámara y configuración del canal.

El receptor está equipado con funciones de Bloqueo y Bucle.

Los interruptores están enumerados 1,2,3,4 (Figura 3.18), representando 4 canales de cámara. Cuando el interruptor está en la posición ARRIBA, el canal de la cámara está APAGADO.

Al cambiar entre los canales, el receptor automáticamente salteará el canal fijado en APAGADO.

El modo Bucle le permite ver todos los canales activos de la cámara fijados en ENCENDIDOS, pasando cíclicamente por los canales cada cierto tiempo.

Esta función es útil para monitorear cámaras o grabaciones de VCR.

Mueva el interruptor L a ENCENDIDO para ciclar los canales activos. Figura 3.18.

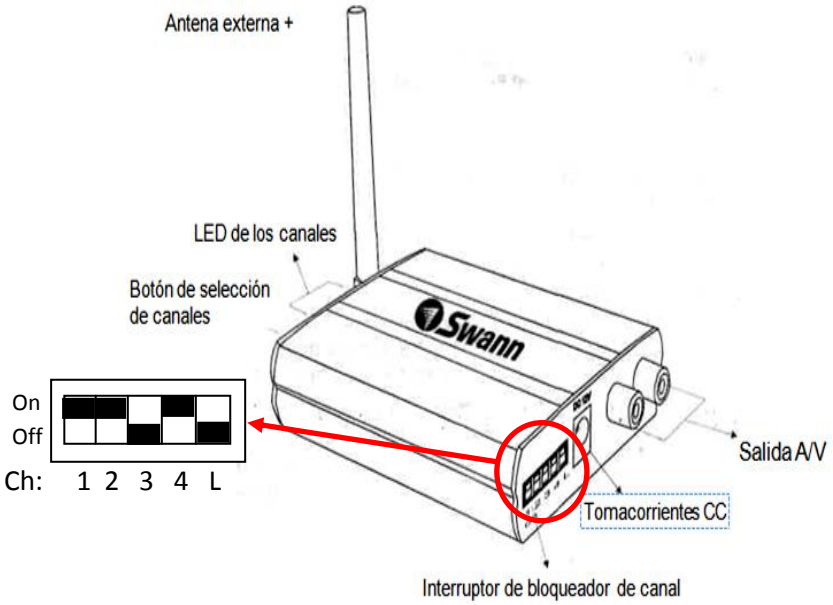


Figura 3.18 Partes del receptor.

3.3.3. MANEJO DEL SISTEMA.

Una vez instalado todo el CCTV inalámbrico, se detalla el funcionamiento a continuación:

En la figura 3.19 se puede apreciar las imágenes emitidas por las cámaras del circuito. Como la tarjeta es para cuatro canales se observa que las cámaras 3 y 4 no están funcionando ya que solamente se instalo 2 cámaras.

Figura 3.19 Imágenes en Software MAXDVR.

Las funciones de los botones para el manejo del software se detallan en la Figura 3.20. Para la llave se puede configurar un clave de acceso, pero se puede acceder sin configurar esto.

Figura 3.20 Nombre de las funciones de los botones.

El control PTZ se la realiza con cámaras alámbricas, esta función no está disponible ya que se instaló sólo cámaras inalámbricas en el circuito.

En el momento de la instalación se crea automáticamente una carpeta en donde se almacena los videos grabados, esta carpeta está en la dirección C:/DVR_DATA/VIDEO y de donde se puede extraer y observar las grabaciones.

También se puede acceder a las grabaciones dando clic en el botón Búsqueda y Reproducción, apareciendo un cuadro (Figura 3.21) en el cual se puede ver todas las grabaciones realizadas por cada cámara y la fecha que se desee ver, además se puede sacar respaldos en un CD o DVD desde este mismo cuadro de dialogo, dando clic en Resguardo como en la figura 3.21. El formato en el que se graba permite reproducir en el Windows Media Player.

Para el presente proyecto la resolución con la que se está grabando es de 320x240 píxeles y se comprime en MS-MPEG4 V2.

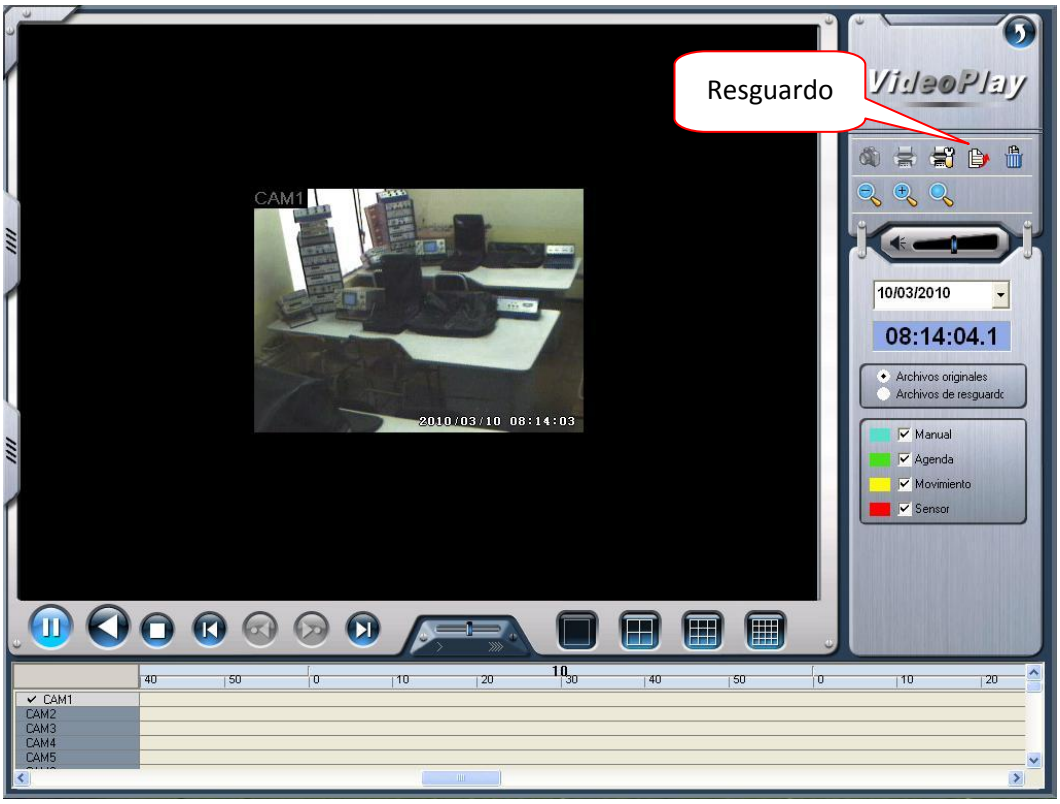


Figura 3.21 Visualización de las grabaciones.

Para una mejor visualización se puede mejorar el video utilizando el software de la tarjeta, para ello primero se ingresa en el botón Configuración y luego se da clic en el botón Video Avanzado, aparecerá el cuadro de la Figura 3.22.

En este cuadro se manipulará el contraste, el brillo y la saturación en el caso de las cámaras inalámbricas, y en el caso de cámaras alámbricas se puede manipular la ganancia.

Si el video no está lo suficientemente claro esta opción ayudará a mejorar la calidad, pero hasta cierto punto, ya que la nitidez del video depende de la resolución que tenga cada cámara, es decir de sus características técnicas.

Figura 3.22 Configuración de video.

La configuración predeterminada es la mejor opción para deshacer cualquier cambio que se realice y que no esté acorde con las expectativas, pues esta configuración es neutra.

Se ha realizado un manual de bolsillo para un mejor manejo del software, este manual consta en el ANEXO C.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES.

De acuerdo al análisis realizado en el Capítulo II, un CCTV inalámbrico es bastante sencillo de implementarlo, gracias a que sus elementos se instalan independientemente y sin los molestosos cables, pero con la dificultad de estar limitados al alcance inalámbrico y a interrupción de la señal.

La mejor cámara para un CCTV inalámbrico es la cámara IP, gracias a que se la puede conectar como un host más en una red interna o en el internet, dependiendo del diseño y las necesidades. Una cámara IP es la única cámara inalámbrica que permite gestionar el video en forma remota, es decir, manipular el paneo (movimientos horizontales y/o verticales) y el zoom, que son ventajas muy notorias frente a una simple cámara wireless. El consto de una cámara IP es muy superior a una wireless debido a estas características, esto se puede concluir de la tabla del ANEXO C, en donde se detalla la el estudio comparativo de Costo-Beneficio de algunas cámaras.

Del análisis del capítulo II, acerca de la aplicabilidad de un sistema de video vigilancia a una unidad de combate, se puede decir que la tecnología inalámbrica es tan flexible que se la puede adaptar a móvil, pero en inconveniente se da al momento de utilizarlo por períodos de más de 2 horas. Este problema se genera porque los transmisores y receptores consumen bastante energía para trabajar y si el sistema es móvil solamente trabaja con baterías, lo que no garantiza una duración de trabajo eficaz de más de 2 horas.

Para la implementación de un sistema económico, sencillo y de fácil instalación la mejor alternativa es utilizar cámaras wireless y una tarjeta DVR para visualizar en una PC. Este sistema puede ser instalado por personas con poco conocimeinto técnico.

Para la implementación de un sistema de video vigilancia más complejo se debe ocupar cámaras IP. Este sistema debe ser instalado por técnicos con conocimiento profundo en el tema.

4.2. RECOMENDACIONES

Para el diseño de un CCTV inalámbrico es necesario realizar un estudio de la ubicación de los diferentes dispositivos tomando en cuenta lo siguiente:

- Cobertura de la cámara.
- Obstrucción para la señal inalámbrica.
- Dificultad de acceso a los equipos para personas extrañas al sistema.
- Alcance de la señal.
- Reacción eficaz ente cualquier situación sospechosa, desde el equipo de monitoreo.

La interface del sistema deberá ser sencilla de manejar y tendrá que contar con un manual amigable y comprensible, debido a que no siempre será manejado por técnicos.

Un parámetro de diseño que se debe considerar es la saturación del medio de los equipos wifi, por lo que se debe tomar en cuenta la presencia de redes wireless u otros dispositivos inalámbricos que afecten al sistema.

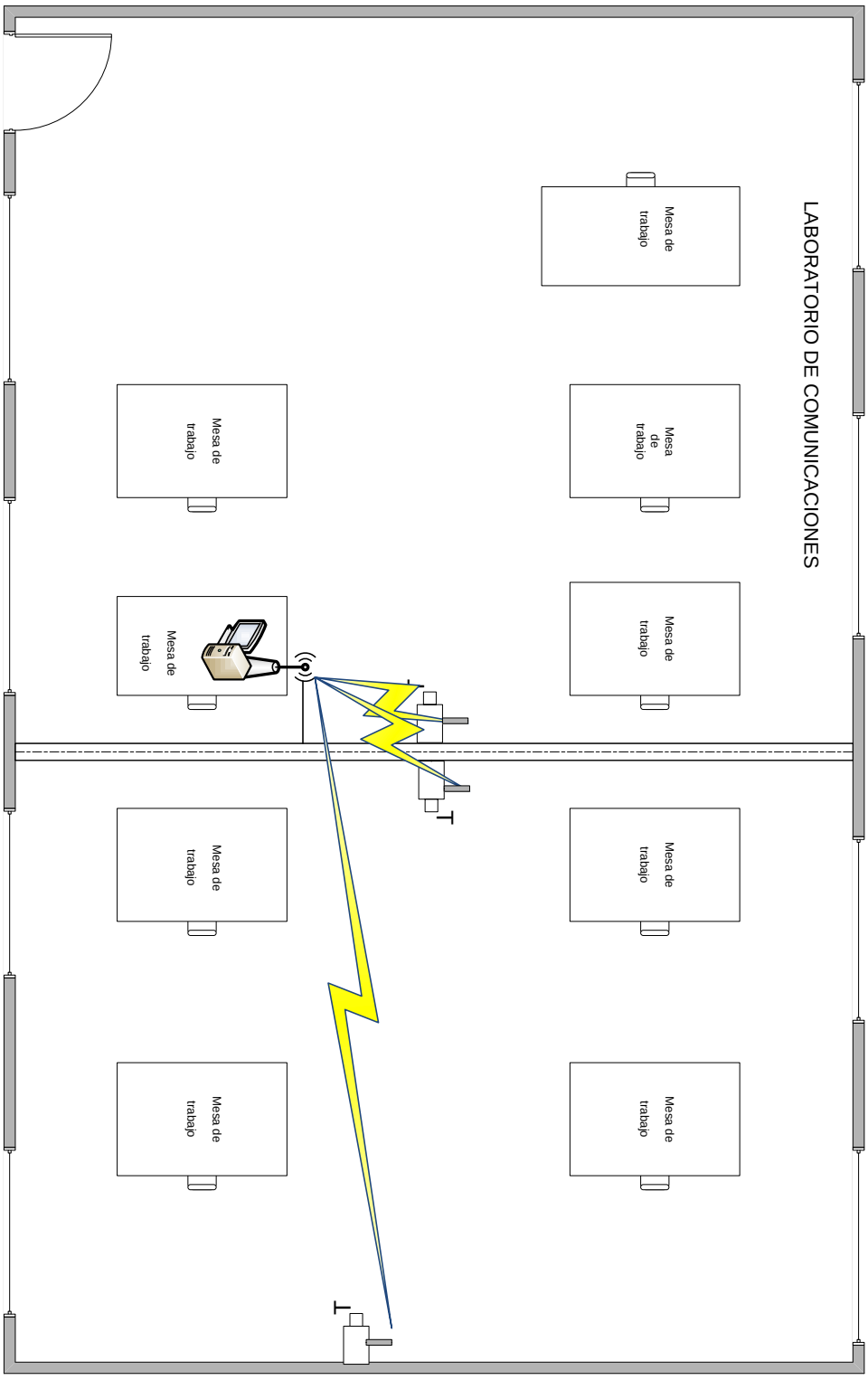
Antes de utilizar cualquier cámara para cualquier propósito, se tiene la responsabilidad de enterarse de cuáles son las leyes y regulaciones que prohíben o limitan el uso de cámaras y cumplir con las leyes y regulaciones que apliquen.

ENLACES BIBLIOGRAFICOS.

- http://www.wifisafe.com/conceptos_wireless.php
- http://articulo.mercadolibre.com.mx/MLM-39410952-capturadora-de-video-y-audio-usb-20-por-rca-y-s-video-_JM
- http://www.softworld.es/gr/grabador_de_dvd_usb_2_0_hi_speed
- http://www.wcctv.co.uk
- http://www.superinventos.com/inalambricas.htm
- http://www.axis.com/products/video/video_server/index.htm
- http://www.intercron.com/cctv.htm - Argentina
- http://www.cctv-seguridad.com.mx/
- http://www.promatco.com.ec/tv.html#2
- http://www.video-surveillance-guide.com/ip-versus-analog-cameras.
- http://www.www.axis.com/.../Del%20CCTV%20analogico%20a%20la%20Vigilancia%20IP.pdf.
- http://www.swann.com.au/.
- http://es.kioskea.net/s/cctv.
- http://www.swannsecurity.com/s/products/view/?product=1040.
- *http://www.voxdata.com.ar/voxcursocctv.html* -

ANEXO A

UBICACIÓN DE LAS CAMARAS



ANEXO B

CARACTERISTICAS DE LAS CAMARAS Y RECEPTOR

	Video
Image Sensor	1/3" CMOS
Video Quality	380 TV Lines
Number of Effective Pixels	NTSC: 510 x 492 PAL: 628 x 582
Minimum Illumination	0 Lux (IR on)
Day/Night Mode	Color during day / switches to B&W at night
White Balance	Automatic
Signal / Noise Ratio	> 48dB
Electronic Shutter	1/60 - 1/15,000 NTSC 1/50 - 1/15,000 PAL
Gain Control	Automatic
Backlight Compensation	Yes
Wide Dynamic Range	No
Lens	6mm
Viewing Angle	53°
	Audio
Microphone	Yes
Audio Range	9ft / 3m
	Night Vision
Night Vision Distance	Up to 26ft / 8m
IR Cut Filter	No
Number of Infra-Red LEDs	11
Infra-Red Wavelength	850nm
Infra-Red LED Life	10,000 hours
	General
Operating Power	DC 12V
Operating Temperature	-14°F ~ 122°F / -10°C ~ +50°C
Body Construction	Aluminum

Dimensions - Camera & Stand	5.1" x 2.0" x 2.0" 130mm x 50mm x 50mm
Weight – Camera & Stand	8.6oz / 245g
Dimensions - Receiver	1.0" x 3.1" x 4.3" 25mm x 80mm x 110mm
Weight - Receiver	6.5oz / 185g
Remote Control	Yes
	Wireless
Digital or Analog	Analog
Max. Transmission Range	Up to 165ft / 50m
Typical Range	65ft / 20m
Frequency	2.4 GHz
Transmission Channels	4
Batttery Power Option	No

ANEXO C

CUADRO COMPARATIVO COSTO vs BENEFICIO DE LAS CÀMARAS A UTILIZARSE

CÀMARA (COSTO) / CARACTERÌSTICAS	SWANN* PPW-245UK 2Càm+Rx $ 245	TRENDNET TV-IP110W $ 298	D-LINK DCS-3420 $ 652	IP MPEG4 MOTORIZADA $ 926
TIPO	Wireless	Wifi (IP)	IP	IP
SENSOR	CMOS 1/3”	CMOS 1/4”		CCD color 1/4”
VIDEO	380 TV Lines NTSC:510x492 PAL: 628 x 582	30 imágenes por segundo 640 x 480 pixeles	25 imágenes por segundo	Hasta 25 img. en 176 x 144. Hasta 25 img. en 320 x 240 Hasta 10 img. en 704 x 576
ZOOM	NO	NO	digital 4x	óptico 10X Lente 4.2 - 42 mm F 1.8 -290
ALCANCE	100 m.	100 m.	100 m	150 m.
AUDIO	Mic. integrado	Mic. integrado	Mic. integrado	micròfono integrado y micròfono externo
MANEJO REMOTO	NO	NO	SI	SI
SOFTWARE DE GESTION	NO	SI	SI	SI
ALIMENTACIÓN	9-12V	12V	12V	12V
PANEO	NO	NO	NO	Mov. horizontal: 270º; Velocidad 15º ~ 50º/sg. Mov. vertical: +90º~ -45º; 15º ~ 25º/sg.

*Se eligió la cámara Swann para desarrollar el prototipo por ser la más económica, con la suficiente resolución como para un pequeño laboratorio. En realidad el costo es casi parecido a una cámara IP sencilla, pero con la diferencia de que tenemos con este pack dos cámaras y así cubrimos el doble de espacio.

ANEXO D

MANUAL BASICO PARA LA OPERACIÓN DE UN CIRCUITO CERRADO DE TELEVISIÓN (CCTV), CON EL PROGRAMA MAX DVR.

1. Arreglo del Sistema

Haga clic  y entre en el interfaz que aparece en la pantalla como lo indica la figura 1.

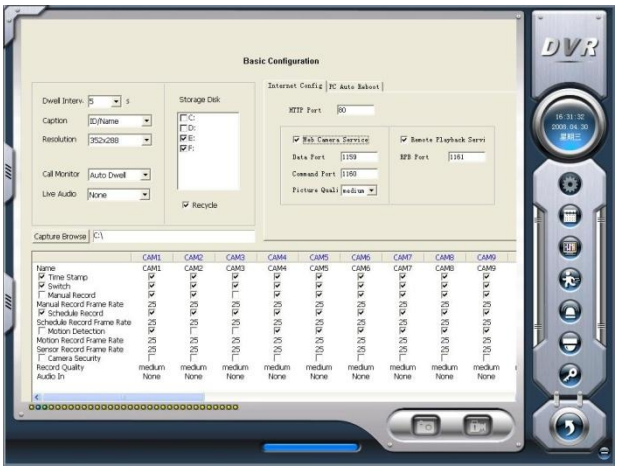


Figura 1

Las definiciones de los botones son los siguientes.

 La Configuración básica

 Fije la configuración

 La configuración de video.

 Configuración de Deteccion de movimiento

 Configuración de la alarma

 Configuración de P.T.Z

 Configuración del usuario

 Retorno

Figura 2

Configuración básica.

Haga clic en y entre en la página de la configuración básica dónde los usuarios pueden instalar el sistema o simplemente pueden usar los valores predeterminados.

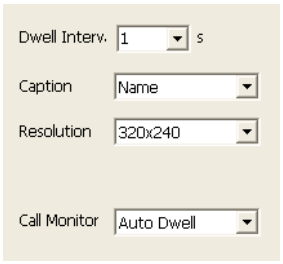


Figura 3

Sobre el almacenamiento de datos de registro. Verificar la figura 4.

Figura 4.

Anteriormente, el sistema de MAXDVR muestra que todo el HDD disponible se divide para los usuarios. Los usuarios pueden seleccionar uno o más de las particiones que se agotarán en la sucesión de basar.

En la siguiente área en la página de la configuración básica, los usuarios pueden entrar el nombre del usuario y la contraseña en las ventanas relativas. Entonces al reiniciar el sistema, manda el acceso al sistema con el nombre del usuario y la contraseña.

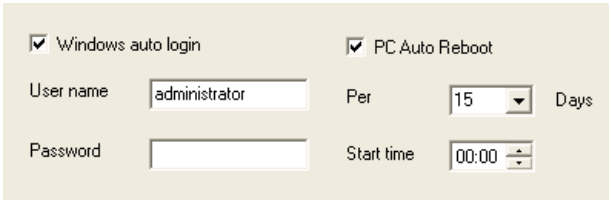


Figura 5.

2. Configuración del video.

Haga clic en y entre en la página de la configuración de video como se indica en la figura 6. Los usuarios pueden cambiar los valores de los artículos correspondientes, es decir el contraste, el brillo, el color, la saturación, la ganancia, dibujando las palancas en las barras, de clic en Predefinido, y todos los valores volverán al valor predefinido.

Figura 6.

3. Configuración de detección de movimiento.

Haga clic en  y entre en la configuración de detección de movimiento.

Figura 7.

La definición de los artículos del arreglo:

La sensibilidad: los usuarios pueden poner la sensibilidad de descubrimiento de movimiento aquí.

La velocidad: Sensibilidad de descubrimiento de movimiento

El Número del bloque: El número de reja fija.

Los valores predeterminados: Ponga como predefinido.

Seleccione todos: seleccione todas las áreas del cauce como el área de descubrimiento

Claro: aclare todas las áreas de descubrimiento y entonces los usuarios pueden seleccionar las áreas de descubrimiento personalizadas por el cursor.

4. Fije la configuración.

Haga clic en  y entre en la página de Configuración de horario como se indica en figura 8.

Figura 8.

El DR series sistema, ofrece a los usuarios las opciones de configuración de horario. Cada cauce tiene tres tipos los modos protocolados, es decir el registro del horario, registro de descubrimiento de movimiento y registro de alarma de sensor. El usuario puede poner los horarios separadamente de domingo a lunes para todos los tres modos del registro. El sensor alarma registro modo tiene la prioridad más alta entre todos los modos del registro. Aquí los usuarios pueden poner los horarios para él.

Cuando los usuarios necesitan revisar el horario para un cauce, primero seleccione el nombre de la cámara en los tres modos del registro agrúpe, y seleccione las barras coloridas en el lado correcto, entonces seleccione ‘Edit selecto ' para revisar los horarios. Dar clic en ‘Add ' para agregar el horario para un cierto cauce.

De clic en ‘Delete ' para anular el horario. De clic en ‘Clear ' para anular todos los horarios de un cierto cauce.

Revise la figura 9 y aprenda a revisar los horarios para un cauce:

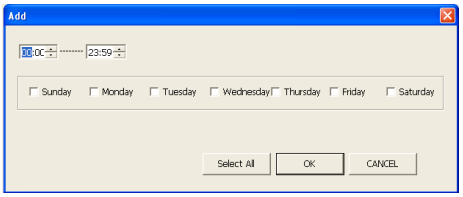


Figura 9.

3. Configuración de la alarma para la detección de movimiento.

El sistema puede recibir la alarma de dos formas de forma local o desde cualquier parte de la red.

Configuración de forma local.

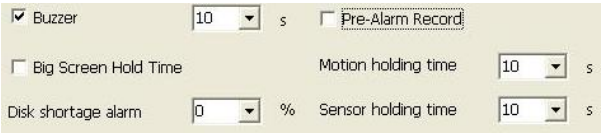


Figura 10.

Las Explicaciones relativas:

El zumbador: Los usuarios pueden seleccionar si para abrir el zumbador del sistema si las alarmas se han activado y también se han seleccionado cuánto tiempo los anillos del zumbador

El Registro de la pre-alarma: Los usuarios pueden seleccionar si para habilitar el pre-registro de la alarma y también el tiempo del pre-registro.

Pantalla grande que sostiene el tiempo: El cauce correspondiente será la pantalla llena cuando la alarma activó. Ponga el tiempo de sostenimiento de pantalla lleno aquí.

Movimiento que Sostiene el tiempo: El sensor del movimiento puede descubrir algún movimiento, sólo si el movimiento dura para un período que excede el tiempo predefinido, entonces el registro de la alarma empezará y pitidos del zumbador.

Sensor que Sostiene Time: El tiempo magnetofónico continuo después de que el sensor detuvo.

La Alarma de Escasez de disco: Si el HDD el espacio disponible es entonces menos el valor fijo, el zumbador emitirá una señal sonora si el Zumbador de '' ha sido seleccionado.

Rendimiento de la alarma.

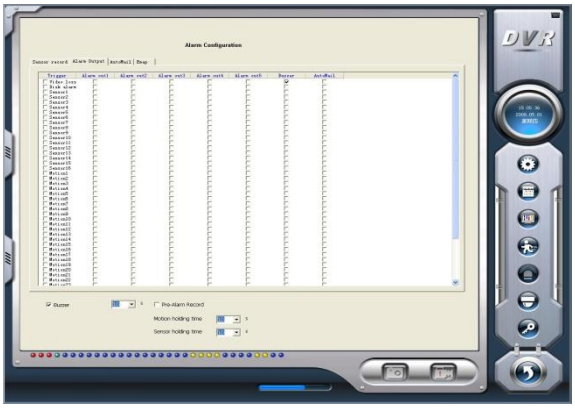


Figura 11.

Presione  en el interfaz principal y acceda a la área de Configuración de alarmas dónde los usuarios pueden hacer un arreglo para la alarma de descubrimiento de movimiento, arreglo de alarma de sensor y corto de HDD.

4. Configuración para el control P.T.Z.

Haga clic en  y entre en el área de configuración como se indica en la figura 12.

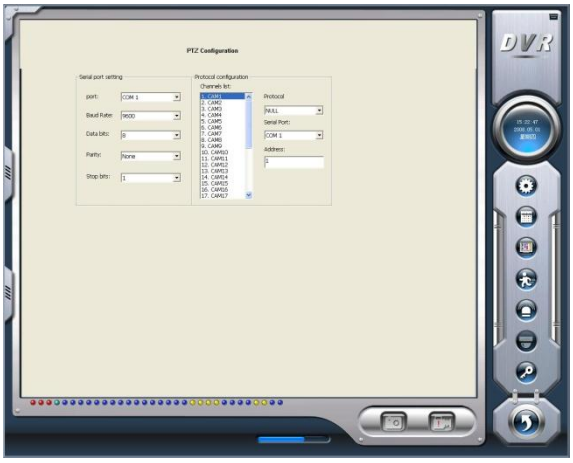


Figura 12.

Arreglo del protocolo.

Los usuarios pueden seleccionar protocolos diferentes, el número del puerto en serie para los dispositivos de P.T.Z, como se indica en la figura 13.

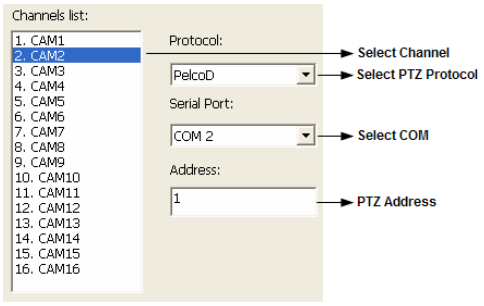


Figura 13.

Configuración de los usuarios.

Haga clic en  y acceda al área de configuración como se indica en la figura 14.

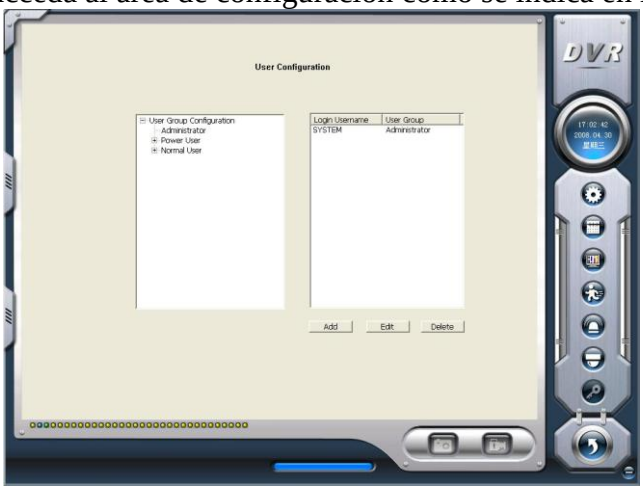


Figura 14.

Después de instalar el sistema de MAXDVR, se creará un usuario y un administrador.

Derechos de Usuario de cambio.

Seleccione a un usuario en el área de Configuración de Usuario y pulsar el botón ‘Edit ' para luego revisar el área del usuario, como se indica en la figura 15.

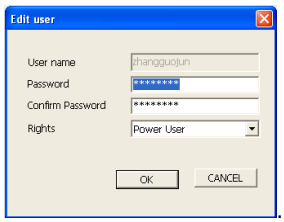


Figura 15.

5. Control P.T.Z.

Haga clic en y el MAXDVR le proporcionara la pantalla que se indica en la figura 16.

Figura 16.

Los usuarios pueden controlar los dispositivos de P.T.Z con los siguientes botones que se indican en la figura 17.

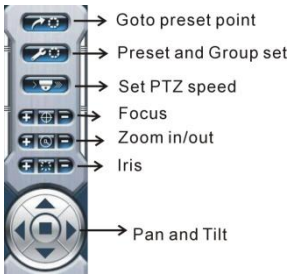


Figura 17.

6. Búsqueda del registro y cinta.

Haga clic en y el MAXDVR le proporcionara la pantalla que se indica en la figura 18.

Figura 18.

Búsqueda del registro.

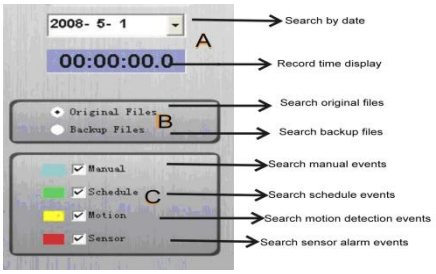


Figura 19.

A, B y C marcan las áreas de tres métodos de la búsqueda.

- A: Investigue por la fecha (ENE ,1, 1971)
- B: Investigue en el archivo del apoyo y el archivo original.
- C: Investigue por el modo del registro.

7. El control del video.

función de los botones:

-  : Juegue
-  : Parada
-  : Juegue al revés. Este botón es válido al jugar atrás por el solo cauce
-  : La Sección anterior. Este botón es válido al jugar atrás por el solo cauce
-  : Luego la Sección. Este botón es válido al jugar atrás por el solo cauce
-  : Marco anterior.
-  : Marco siguiente.