UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGON

ANÁLISIS DE TÉCNICAS DE COMPRESIÓN Y ENCRIPTAMIENTO DE VIDEO

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO MECANICO ELECTRICISTA

P R E S E N T A N:
JACINTO HECTOR HERNÁNDEZ DELGADILLO
CARLOS ALBERTO CALDERON BANDA

ASESOR: ING. DAVID ESTOPIER BERMUDEZ

MÉXICO **2000.**

Agradecemos infinitamente a nuestra Universidad por todas las facilidades que nos brindaron para la realización del presente trabajo, así cómo a nuestros profesores por todo el apoyo tanto profesional como personal.

El presente trabajo no hubiera sido posible sin las facilidades que nos fueron otorgadas, por nuestra gloriosa Universidad Nacional Autónoma de México

INDICE GENERAL Pag

INTRODUCCION 1

CAPITULO 1

CONCEPTOS BASICOS DE DIGITALIZACION DE VIDEO

1.1 Transmisión de información desde el punto de vista transmision digital 3
1.2 Campos binarios 3
1.3 Capacidad de un canal de comunicación 4
1.3.1 Capacidad máxima 4
1 4 Medios de comunicación 5
1.5 Señales de video, audio y televisión 8
1.5.1 Señales de banda base video y audio 9
1 6 Procesamiento básico de las señales de televisión 10

CAPITULO 2

MEDIOS DE TRANSMISION PARA VIDEO DIGITAL

2.1 Medios de transmisión 16
2.2 Características de un medio de transmisión 16
2 3 Cables de cobre 17
2.3.1 Líneas aéreas de cobre desnudo 17
2 3 2 Cable multipar subterráneo 17
2.4 Carácteristicas de propagación 18
2.5 Características eléctricas de los cables 19
2.6 Cable de par trenzado 19
2.6.1 Ventajas del par trenzado 20
2.6.2 Desventajas del par trenzado 20
2.7 Especificaciones para cable UTP 20
2.8 Cable coaxial 22
2.8.1 Conductores 22
2.8.2 Dieléctrico 22
2.8.3 Aislamiento 22
2.8.4 Armadura 22
2.8.5 Aplicación del cable coaxial 23
2.8.6 Ventajas del cable coaxial 23

2.8.7 Desventajas del cable coaxial 23

2.9 Fibra optica 23
2.9.1 Propagacion 25
2.9.2 Reflexion 26
2.9.3 Refraccion 27
2.10 Ley de Snell 27

2.11 Ventajas de la fibra óptica 28
2.11.1 Desventajas 28
2.12 Microondas 28
2.12.1 Ventajas 28
2.12.2 Desventajas 28
2.13 Satélites 30
2.13.1 Ventajas 30
2.13.2 Desventajas 30
2.14 Red Digital de Servicios Integrados 30
2.15 Enlace digital DS-0 30
2.16 Dataenlace 31

CAPITULO 3

OPTIMIZACION DE RECURSOS PARA TRANSMISION DE VIDEO

3.1 Compresión de video 33
3.2 Señal de video 35
3.3 Ancho de banda de las señales portadoras en video 37
3.4 Lo que ve el ojo 38
3.5 Necesidades de la compresión digital 39
3.6 Capacidad de almacenamiento 43
3.7 Efectos de los parámetros de digitalización en la compresión de imagen 43
3.8 Entropía 44
3.9 Codificación 44
3.10 Tipos de compresión en señales digitales 45
3.11 Técnicas de compresión 46
3.11.1 Técnicas de compresión sin pérdidas 47
3.11.1 a Codificación del plano de bits 48
3.11.1 b Codificación predictiva sin pérdidas 49
3.11.2 Técnicas de compresión con pérdidas 49
3.11.2.a Características principales 49

3.11.2.b Codificacion predictiva con perdidas 52
3.12 Codificacion por transformacion 54
3.13 Codificacion por bloques truncados 57
3.14 Dimensiones aplicables a la compresion 58
3.15 Categoria de la compresion 58
3.16 El proceso DPCM 58
3.17 Proceso de codificación DCT y reduccion de la entropia 60
3.18 Compresión MPEG 66
3.19 Estándar del JPEG 67
3.20 Requerimiento de MPEG para el video 67
3.20.1 Acceso aleatorio 68
3.20.2 Búsqueda rápida en adelanto/atraso 68
3.20.3 Lector de regreso 68
3.20.4 Sincronía de audio y video 68
3.20.5 Retraso en la codificación/decodificación 69
3.21 Algoritmo de compresión MPEG 69
3.21.1 Reducción de la información espacial 70
3.21.2 Reducción de la redundancia temporal 71
3.22 Desempeño de la compresión en el mundo real 72
3.23 Escogiendo una técnica de compresión 72
3.24 Aplicaciones 74
3.24.a Videoconferencia 74
3.24.b Video- Codec 76
3.24.c Cientific Atlanta 82
3.24.d El sistema codificador 83
3.24.e VT34A3Dc 84

CAPITULO 4

SEGURIDAD EN LA TRANSMISION DE VIDEO

4.1 Modelos, objetivos y sistema de codificación 88
4.2 Códigos 94
4.3 Cifradores de transposición 95
4.4 La norma del cifrado de datos 96
4.5 Técnicas de encriptamiento 97
4.5.1 Algoritmo DES 97
4.5.2 Cifrador de flujo 99
4.5.3 Protección de clave 101

4.6 Modelo matematico 101
4.6.1 Métodos 104
4.7 Identificación de usuario 105
4.8 Seguridad en redes 107

CAPITULO 5

APLICACIONES

5.1 S-HTTP 111
5.2 SSL 111
5.3 Unidad móvil 112
5.3.1 Descripción 112
5.4 Video conferencia sobre redes LAN 115
5.4.1 Beneficios 118
5.4.2 Aplicaciones 118
5.4.3 Tarifas video enlace digital (Digital Link) 120

INTRODUCCION

El comunicarse ha sido una de las necesidades primarias del hombre El proceso de entablar una comunicación, puede tener varias vertientes una ellas, y tal vez, la más importante es la comunicación a distancia.

Dentro de la evolución de los medios de comunicación existen diferentes formas de comunicación. Uno de los grandes avances en los sistemas de comunicación fue la transmisión de imágenes, misma que fue creada en el año de 1927, cuando los laboratorios Bell hicieron la primera transmisión de televisión entre Nueva York y Washington.

En Estados Unidos en 1939 se transmitieron regularmente programas de televisión, pero durante la segunda guerra mundial el desarrollo de ésta se vió afectada y no fue sino hasta después de 1945 cuando se empezaron a desarrollar nuevos métodos para mejorar la transmisión.

Más aún, con la evolución de los dispositivos y los medios de transmisión se vió la digitalización de las señales, permitiendo con esto, entre otras cosas integrar voz, datos y vídeo

Cabe mencionar que los sistemas de comunicación han evolucionado conforme a las necesidades del hombre, por que estas cada vez son más complejas.

Hoy en día los sistemas de comunicación deben tener principalmente características específicas como. confiabilidad, velocidad y versatilidad; esto es, sistemas que permitan transmitir información a altas velocidades y que esta misma no se pierda, la información a transmitir puede ser voz, datos e imágenes.

Como ya se ha mencionado estos logros se dieron gracias en gran medida a la digitalización de las señales; uno de los sistemas más difundidos actualmente es el último, es el de la transmisión de imagen o vídeo. El vídeo es un sistema tan versátil que integra conjuntamente voz y datos, es por eso que el estudio y comprensión de la forma en que trabaja es muy importante.

La señal usada para la transmisión de televisión en blanco y negro es una señal muy compleja, en la cual la información esta formada de varias partes o componentes individuales. Básicamente la señal transmitida en televisión consiste de dos portadoras separadas: una modulada con la parte de audio y la otra modulada con la parte visual.

Un receptor de television recibe ambas portadoras, simultaneamente, refuerza o simplifica su nivel de ambas y luego las separa para su modulación. La parte de sonido o audio de la señal de la television es una onda estándar.

Asi, la parte de sonido de una señal de televisión se transmite en una portadora modulada en frecuencia, y para la de video de emplea otra portadora que la modula en amplitud; mas adelante se verán los detalles técnicos correspondientes

A lo largo del desarrollo de este trabajo, comprobaremos, que el video es uno de los sistemas más confiables y fácil de interpretar ya que facilita la transmisión de aspectos especificos de información por medio de la imagen.

Es por esto que los avances que se den dentro del ámbito de video son dignos de un estudio en particular.

La seguridad en la transmisión de información es sin lugar a dudas una prioridad dentro de las mismas, además de que día a día el tamaño de la información tiende a ser más grande, es por esto que se buscan métodos para transmitir información sin saturar los medios, ni los equipos.

Estos conceptos se aplican al video digital y es por eso que se han desarrollado métodos de compresión de vídeo y encriptamiento, que sin lugar a dudas cubren las expectativas en cuanto a estas necesidades se refieren

El presente trabajo se centra en el estudio de estos conceptos; de acuerdo a los avances tecnológicos que hoy en día se han convertido en cotidianos en ciertos ambientes y que posteriormente serán más difundidos en la vida cotidiana.

CAPITULO I

ELEMENTOS DE TRANSMISIÓN Y CONCEPTOS BASICOS DE DIGITALIZACION DE VIDEO

1.1 TRANSMISION DE INFORMACION DESDE EL PUNTO DE VISTA TRANSMISION DIGITAL

Es la transferencia de información discontinua que ha sido procesada y codificada, generalmente en forma binaria, sobre un medio de comunicación con el auxilio de equipos para esta función. Será preciso la existencia de una fuente de información, un destinatario de los mismos, y una unión entre ambas

1.2 CAMPOS BINARIOS

Un sistema de transmisión de datos tiene como finalidad llevar la información del medio transmisor a uno receptor, donde la información se refiere al número de simbolos binarios que son los necesarios para la transmisión y recepcion de un mensaje.

La transmisión de información es el envío de simbolos que cambian impredecíblemente con el tiempo, los cuales deben de ser interpretados, tener un sentido y un valor. Y para facilidad de esto se utiliza una secuencia binaria. La cual es correspondiente al mensaje a transmitir.

Mensaje

Es la transmisión de información de un usuario a otro

Bit

Es la cantidad mínima de información

Byte

Es un carácter o letra que esta formado por ocho bits

BPS (Bit Por Segundo)

Es el número de elementos de señalización por segundo o unidad de tiempo. Dicha unidad se utiliza para representar la velocidad de transmisión o velocidad binaria.

1 baudio = 1 Bit por segundo (bps), si cada elemento de señal transporta un bit

En general si hay "m" elementos, un bps = (log 2 * m) baudios

Un baudio es la unidad de medición en la velocidad de señalización.

1.3 CAPACIDAD DE UN CANAL DE COMUNICACIONES

Esta dado por el numero de bits por segundo que un canal de comunicaciones puede transportar, el cual a su vez es proporcional al ancho de banda

1.3.1 CAPACIDAD MÁXIMA (LEY DE SHANNON)

$$CAPACIDAD = W/\log 2\ (1+s/n)$$

donde: W = ancho de banda
s/n = señal a ruido

Banda de paso

Es representado por dos números que indican las frecuencias máximas y mínima en los cuales el canal de comunicaciones trabaja en optimas condiciones, es decir es un segmento en cierto lugar del espectro electromagnético que deja pasar determinadas frecuencias.

Ancho de Banda (BW)

Es el número que expresa la capacidad de transmisión de una línea, se obtiene restando la frecuencia mas baja que contenga una señal, de la frecuencia más alta que contenga esa misma señal. En otras palabras, es una medida de la amplitud de la señal en el espectro de frecuencias

Modulación

Es la modificación de una señal periódica para transportar datos. Esta señal periódica es lo que se conoce como portadora. Los datos que modulan la portadora (es decir la información que procede de la fuente) constituyen una señal en banda base, que es un término que suele referirse a las señales que no están moduladas

1.4 MEDIOS DE COMUNICACION

Definiremos los principales medios de comunicacion, ya que el medio de comunicación es usado para interconectar estaciones de usuario y dispositivos

La selección del medio a utilizar depende de:

- Tipo de ambiente donde se va a instalar.
- Tipo de equipo a usar
- Tipo de aplicación y requerimientos
- Capacidad económica (relación costo/beneficio esperado)

Enlaces físicos terrestres

- Par de cables trenzados
- Cable coaxial de banda angosta
- Cable coaxial de banda ancha
- Fibras ópticas

Espacio aéreo

- Microondas
- Infrarrojos.
- Láser
- Radiofrecuencia.

Par de cables trenzados

Es el medio más común, usado también en PBX (Private Branch Exchange). A continuación se describen sus principales características.

- Puede transportar tanto señales digitales como analógicas
- Alcance, hasta de tres kilómetros dependiendo del producto.
- Permiten trabajar en transmisiones Half Duplex y Full Duplex
- Alta taza de errores a grandes velocidades.

- Baja inmunidad al ruido, interferencia etc
- Requiere protección especial· blindaje, ductos, etc
- Bajo costo

Cable coaxial de banda angosta (Base Band).

- Transmiten una señal digital simple, en Half Duplex
- No hay modulación en frecuencia
- Diseñado principalmente para comunicación de datos. Pero pueden acomodar aplicaciones de voz y video los cuales se transmiten en forma digital.
- Emplea conectores especiales para conexión física
- Alcanza de 1 a 10 Km.
- BW 10 Mbps.
- Poca inmunidad al ruido.
- Bajo costo.

Cable coaxial de banda ancha

- Se puede combinar voz, datos y video simultáneamente, pero en diferentes frecuencias.
- Todas las señales se transmiten en forma Half Duplex.
- Mejor inmunidad al ruido que el de banda base.
- BW de 400 Mhz.

Fibras ópticas

Consiste de un núcleo central, muy fino de vidrio o plástico, que tiene un alto índice de refracción. Este núcleo está rodeado por otro medio que tiene un índice algo mas bajo, que lo aísla del medio ambiente. Cada fila provee un camino de transmisión único de extremo a extremo, unidireccional.

Transmiten la señal cuando pulsos de luz se introducen en un extremo, usando un láser o LED. La reflexión de los pulsos viaja sobre todo el largo del conductor llevando consigo la información de datos. La transmisión es generalmente, punto a punto sin modulación, una característica importante es que no es afectada por interferencia eléctrica, ruidos, problemas energéticos, temperatura radiación o agentes químicos, el ancho de banda es mucho más alto que con cualquier otro medio. Actualmente 50 Mbps a 10 Km. Experimentalmente 1 Gbps.

Es capaz de transmitir voz, datos y video, por lo que el cable es altamente confiable, es muy difícil de bifurcar y presenta muy poca perdida de velocidad Físicamente la fibra es muy fina, liviana, durable y por lo tanto instalable en muy poco espacio, sin embargo todavía es muy cara, no se puede reparar y su capacidad multipunto es muy baja.

Microondas

Este sistema de comunicación emplea el espacio aéreo como medio físico de transmisión La información se transmite en forma digital a través de ondas de radio de muy corta longitud Pueden direccionarse múltiples canales a múltiples estaciones dentro de un enlace dado

Las estaciones consisten de una antena tipo plato y de circuitos que interconectan la antena con la terminal del usuario. La transmisión es en línea recta y por lo tanto se ve afectada por los accidentes geográficos, edificios, bosques, mal tiempo, etc. El enlace promedio es de 40 Km.

Una de las ventajas importantes es la capacidad de poder transportar miles de canales de servicio a grandes distancias a través de repetidoras, a la vez que permiten la transmisión de información en forma natural.

Satélites

Este dispositivo que actúa principalmente como "reflector" de las emisoras terrenas. Podríamos, decir que es la extensión al espacio del concepto de torre de microondas. Al igual que estas los satélites reflejan un haz de microondas que transportan información codificada. Realmente la función de reflexión se compone de un receptor y un emisor, que opera a diferentes frecuencias: recibe a 6 Ghz y envía o refleja a 4 Ghz, por ejemplo:

Físicamente, los satélites giran alrededor de la tierra en forma sincronía con ésta a una altura de 35680 Km, en un arco directamente ubicado sobre el ecuador. Como ejemplo digamos que un satélite esta ubicado en el ecuador a cualquier punto latinoamericano, actuaría como una altísima torre de microondas que permitiría interconectar todo el continente.

1 5 SEÑALES DE VIDEO, AUDIO Y TELEVISION

Hay tantos usos de estas señales que está justificado considerar el proposito especifico de cada una Video es una palabra que proviene del latin que significa "yo veo" Analogamente, audio significa "yo oigo" Los dos términos corresponden respectivamente, video a luz y audio a sonido. El microfono es el sistema de audio más conocido, este convierte las ondas de sonido en variaciones eléctricas de la señal de audio El altavoz recibe esta señal audio en las terminales de entrada, ya sea por conexión directa o como parte de un sistema de radiodifusión. Luego el altavoz reproduce el sonido original captado por el micrófono.

En el caso de la transmision de video se requiere de un dispositivo que capte la imagen para posteriormente ser transmitida, la primera fase se lleva a acabo en una cámara de televisión, que se compone de cuatro secciones principales. Uno de estos es el sistema óptico, que consiste en varias lentes (ordinariamente tres o cuatro) que captan la luz reflejada por el objeto y proyectan una imagen exactamente enfocada sobre la superficie especialmente preparada del tubo de cámara La segunda porción es el tubo de cámara que convierte la energia luminosa en energia eléctrica. La tercera sección esta compuesta por los amplificadores necesarios para el correcto funcionamiento del tubo de cámara y para la amplificación de la salida de señal de imagen (vídeo) de la cámara antes de que sea alimentada a los otros amplificadores exteriores a la cámara. La cuarta porcion de la cámara del tipo de estudio es el sistema monitor de imagen, mediante el cual el operador puede ver la imagen captada por su cámara. Se compone de un tubo de imagen análogo al montado en los receptores domésticos, pero más pequeño, y sus amplificadores asociados.

En la fase del tubo de cámara, para ser más especificos, convierte en su entrada la luz en las correspondientes variaciones eléctricas de la señal de vídeo. El tubo de cámara es para la señal de vídeo lo que el micrófono es para la señal de audio. Al final del sistema vídeo, el tubo de imagen convierte la tensión de la señal vídeo de la entrada en la luz de la salida La información vídeo, es producida en la pantalla del tubo de imagen tal como seria en la escena del tubo de cámara.

Diferencias entre la señal de vídeo y la señal de audio.

La imagen luminosa se convierte en una señal eléctrica

1.5.1 Señales de banda base vídeo y audio

Para las señales vídeo o audio, el rango de frecuencias es lo que se le llama banda base Esas frecuencias corresponden realmente a la información visual o acústica deseada, sin complicaciones adicionales

tal como codificación o modulacion para funciones especiales En los sistemas audio, las frecuencias de las bandas base son de 20 hz a 20 khz, aunque comúnmente para sonido de alta fidelidad se utiliza la banda de 50 hz a 15 khz En los sistemas video, las frecuencias de la banda base son de 0 hz para corriente continua hasta 4 Mhz. Las señales de la banda base pueden ser aplicadas a un reproductor con altavoz para reproducir el sonido deseado. También puede ser alimentada la señal de la banda base de video a un tubo de imagen para producir la imagen deseada.

La razón de convertir la información de sonido y visual en señales electricas de la banda base es que si pueden ser amplificadas convenientemente Por lo demás, el proceso de la señal por los circuitos electrónicos es el adecuado para varios usos.

Para señales de radiodifusión, en la transmisión por radio o inalámbrica, la señal de la banda base de audio se utiliza para modular una onda portadora de radiofrecuencias (RF). La modulación es necesaria por que las frecuencias audio son demasiado bajas para que su radiación sea eficiente. Por otra parte para diferentes estaciones se utilizan diferentes frecuencias portadoras. El receptor puede ser sintonizado a cada frecuencia portadora. En el receptor la señal de RF modulada es detectada para recuperar la información original de audio

En la difusión de televisión se aplica la misma idea que en la de radio. La señal de la banda base de video modula una portadora de alta frecuencia para su transmisión inalámbrica. En el receptor el detector video recupera la señal original

En la teledifusión, o difusión de televisión, se utiliza modulación de amplitud (AM) para la señal de imagen y modulación de frecuencia (FM) para la señal de sonido asociada.

Elementos de imagen

Una imagen fija es fundamentalmente una ordenación de muchas áreas pequeñas oscuras y luminosas. En una impresión fotográfica los granos finos de plata proporcionan las diferencias en cuanto a luz y sombra necesarias para producir la imagen. Un ejemplo son las fotografías de los periódicos, cuando se imprime una imagen en el proceso de fotograbado, hay muchos puntos negros que forman la imagen y se puede observar que la imagen impresa esta compuesta de pequeñas áreas elementales de blanco y negro. Si se las examina detenidamente, se verán los puntos a causa de que los elementos de imagen son relativamente grandes.

Cada área pequeña de luz o sombra es un elemento de imagen o detalle de imagen llamado pixel Todos los elementos juntos contienen la información visual de la escena

Si son transmitidos o reproducidos con un mismo grado de luz y sombra que el original y en la posición correcta, se producirá la imagen

1.6 PROCESAMIENTO BÁSICO DE LAS SEÑALES DE TELEVISIÓN

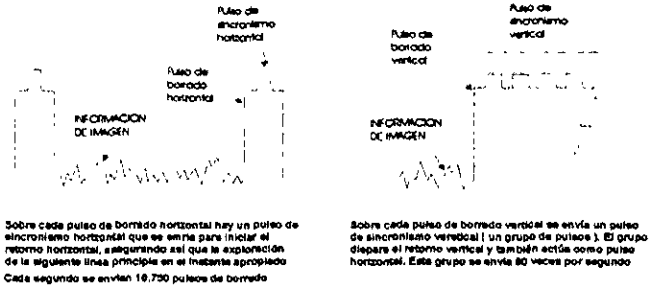
La señal usada para la transmisión de televisión en blanco y negro es una señal muy compleja, en la cual la información esta formada de varias partes o componentes individuales Básicamente, la señal transmitida en televisión consiste de dos portadoras separadas. una modulada de acuerdo con la parte de audio y la otra con la parte visual o de vídeo. Un receptor de televisión recibe ambas portadoras, simultáneamente, refuerza o amplifica su nivel de ambas y luego las separa para su demodulación. La parte de sonido o de audio de la señal de televisión es una onda estándar

Así, la parte de sonido de una señal de televisión se transmite en una portadora modulada en frecuencia, y para la de vídeo se utiliza otra portadora que se modula en amplitud.

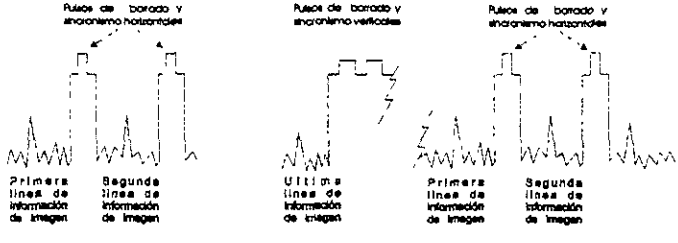
En una señal compuesta de televisión, la portadora de sonido se encuentra a 4.5 Mhz por encima de la portadora de vídeo, como se dijo anteriormente. La información de sonido la lleva una portadora normal de banda lateral derecha (BLD). En cambio, para la de video se emplea una portadora de banda lateral residual (BLR), modulada de tal manera que las frecuencias de vídeo bajas son próximas a la frecuencia portadora, mientras que las altas se alejan de ella. Se pueden enviar frecuencias de video que tienen hasta 4 Mhz.

En la práctica, una escena se divide en 525 líneas individuales y la exploración de cada línea se realiza en 1/15,750vo de segundo, por lo tanto, en un segundo la escena total es barrida 30 veces; si multiplicamos 525 líneas por 30 veces que aparece la imagen, esto en un segundo, tenemos que se explorarían 15,750 líneas en un segundo, De hecho cada segundo, la señal de vídeo de televisión produce 30 "instantáneas" o imágenes fijas enteras. Pero gracias a la persistencia de visión del ojo humano, las imágenes fijas proyectadas en rápida sucesión dan la impresión de que hay movimiento continuo. Además en realidad, las imágenes se proyectan a razón de 60 por segundo, por que cada imagen consta de dos cuadros los cuales contienen líneas alternadas de la imagen. Cuando estas se sobreponen en la pantalla, las líneas de un cuadro se combinan con las del otro, en lo que se llama entrelazado. Entonces, los 60 cuadros producen 30 imágenes completas por segundo

Ademas despues del barrido de la 525ava linea debe haber otro lapso para que el haz regrese a su punto inicial de arranque. Estos lapsos entre lineas se llaman tiempos de retorno horizontal y vertical y constituyen intervalos en los cuales no se transmite información de imagen



SEÑAL DE VIDEO COMPUESTA



(Se utiliza la señal completa para modular en amplitud la portadora de video)

En la descripción anterior de la señal de video sólo se trató de proporcionar algunos conceptos básicos. En una exposición más completa habría que incluir elementos y detalles que están fuera del alcance de este libro

Los pulsos de sincronismo vertical forman parte de un grupo de 18 pulsos especiales que se usan para sincronización tanto horizontal como vertical Esto se explica más adelante

IGURA 1.1

Los circuitos que producen este haz, deben sincronizarse con los que se usan para la exploración de la escena original en el estudio de televisiòn, esto se logra mediante los pulsos de sincronización que forman parte de una señal de vídeo

Sin embargo, para la operación apropiada del receptor de television se requiere que la señal de video ademas de llevar la informacion de imagen, también suministre los medios para cortar el haz electrico de los circuitos de exploración del receptor, durante los intervalos del retorno horizontal y vertical

El corte o supresion del haz, durante su retorno, se efectúa por medio de los pulsos de borrado que forman una de las partes de una señal de video. Dichos pulsos son de forma rectangular y tienen un nivel de voltaje suficientemente alto para suprimir el haz electrónico, de modo que no produzca luz en la pantalla.

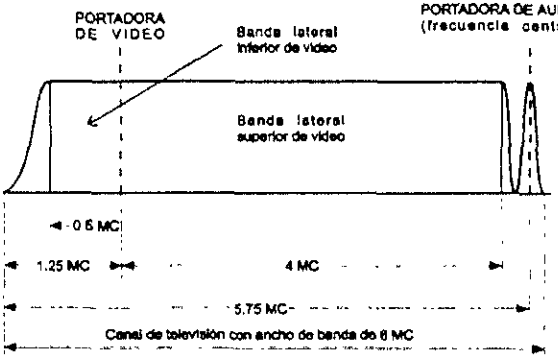
Al igual que hay pulsos de borrado, tanto horizontal como vertical existen también pulsos de sincronismo horizontal y vertical. Se les llama generalmente pulsos de sincronización, como se aprecia en la FIGURA 1.1, los pulsos de sincronización se transmiten encima de los pulsos de borrado durante el retorno, o sea en los instantes en que no se transmite información de la imagen.

En la señal de blanco y negro las partes de la señal que representan la información de imagen son simplemente variaciones de amplitud que corresponden a los efectos de luz y sombra en la imagen original. Pero las mismas partes en una señal a color, aunque siguen siendo variaciones en amplitud, constituyen una representación compleja de los colores y la brillantez de la escena. Además la señal de color tiene un tipo adicional de pulsos que constituyen la señal de sincronización de color, que sigue inmediatamente después de los pulsos de sincronización horizontal.
(Ver fig. 1.2)

En la señal de video a color, la parte correspondiente a la información de imagen esta compuesta de información de color así como de la brillantez o sombra. Para generarla, se requieren varias etapas. En la primera, se producen separadamente tres señales de imagen en color de la escena por transmitir

Una de dichas señales es para el rojo y consiste en un voltaje cuyas variaciones de amplitud corresponden a los diferentes tonos de rojo en la escena explorada. Las otras dos señales son para el verde y el azul y consiste de voltajes que varían en forma similar de acuerdo con los tonos de verde y azul.

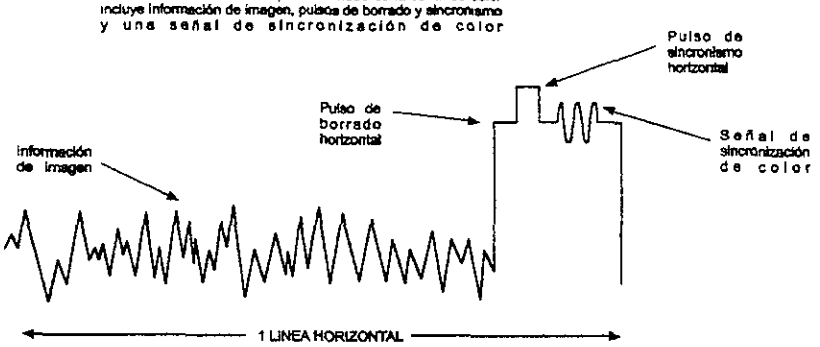
En la banda de 6 MC de un canal de televisión caben tanto la portadora de audio de FM como la portadora de video de AM



La información de audio se transmite por medio de una señal convencional de FM, en tanto que la de video está contenida en una señal de banda lateral residual

Las bandas de las partes de FM y AM de la señal completa son tales que no hay interferencia o interacción entre las dos

Cada línea horizontal de la parte de video de la señal de color incluye información de imagen, pulsos de borrado y sincronismo y una señal de sincronización de color



La información de imagen representa tanto el color como la luminosidad relativa del área particular de la escena explorada, en tanto que la señal de sincronización de color hace que el receptor reproduzca fielmente los colores de la imagen original

FIGURA 1.2.

Las señales de luminancia (Y) y crominancia (C) obtenidas a partir de las señales basicas de color de video , rojo, verde y azul, contiene toda la informacion de imagen que habrá de transmitirse. Estas se combinan en una sola señal, sumándose de tal manera que las variaciones de valor medio de la señal resultante representen las variaciones de luminancia, en tanto que las variaciones instantáneas representan la información y la señal de sincronización de color, forma lo que se llama señal de crominancia. La señal compuesta tiene la información de imagen de la señal moduladora de video y, junto con los pulsos de borrado, los de sincronismo y los de la señal de sincronización de color, forma lo que se llama señal de video colorplexada. (Fig. 1 4)

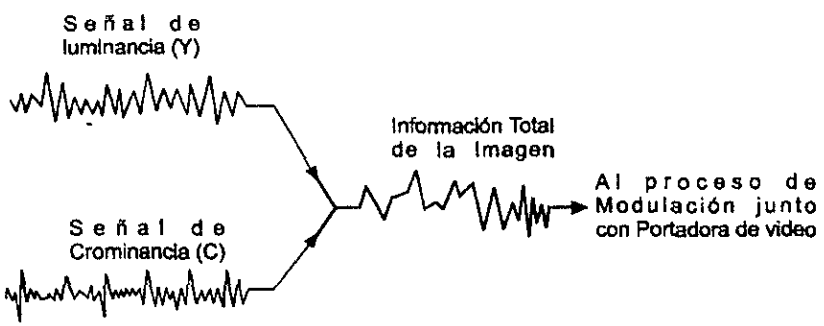


FIGURA 1.4

CAPITULO 2

MEDIOS DE TRANSMISION PARA VIDEO DIGITAL

2 1 MEDIOS DE TRANSMISION

Los medios de transmision son los medios fisicos para establecer la comunicación entre dos o más usuarios, y esto depende de las necesidades y las distancias que se manejen, y esta comunicación se puede dar entre personas o máquinas.

Cada medio de transmistón tiene ventajas y desventajas de acuerdo con:

- Caracteristicas de sus componentes
- Tipo de señal usado
- Costo
- Facilidad de instalación
- Capacidad
- Resistencia a la interferencia

2.2 CARACTERISTICAS DE UN MEDIO DE TRANSMISIÓN

Las caracteristicas de un medio de transmisión se puede delimitar en dos grupos principales:

- Medios fisicos. Lo más importante es el ancho de banda que puede manejar, lo cual se puede definir como la máxima cantidad de información que un determinado medio puede transportar

- Técnica de transmisión. Se refiere a la manera como se transmite la información y puede ser.

Banda base, la información se transmite tal como se encuentra, esto es, se transmite en forma digital

Banda ancha, la información se transmite en forma analógica y pueden ocurrir varias transmisiones dentro de un mismo canal, dependiendo de la técnica que se utilice

Los medios de transmisión pueden clasificarse de la siguiente manera·

Según su naturaleza física

- Medios materiales.
  - Sólidos (cables)
  - Líquidos (agua)
  - Gaseoso (atmósfera)

- Medios no materiales

Vacio

Si son creación o no del hombre

- Naturales

Atmósfera, vacio

Agua (mares, rios, lagos).

Tierra

- Artificiales.

Cables

Guías de onda.

Fibras ópticas.

En el proceso de la transmisión se deteriora la señal ya sea por fenómenos internos al sistema o por fenómenos externos denominándose genéricamente perturbación a esta degradación.

El efecto de la perturbación se traduce a la degradación de calidad de la información obtenida en la recepción manifestándose como ruido y errores en la información. Uno de los grandes objetivos del diseño de un sistema de comunicaciones es conseguir la transferencia de la información con una mínima degradación que permita obtener una calidad determinada.

2.3 CABLES DE COBRE

Los medios de transmisión por medio de líneas de cobre básicamente se pueden clasificar en dos· líneas aéreas de cobre y multipar subterráneo.

2 3 1 LINEAS AEREAS DE COBRE DESNUDO

Es un conjunto de conductores eléctricos convenientemente separados y soportados por aisladores en apoyos situados cada 50 metros aproximadamente, dispuestos de forma tal, que satisfagan las condiciones eléctricas determinadas y proporcionen la rigidez mecánica necesaria.

Este tipo de transmisión esta prácticamente en desuso.

2 3.2 CABLE MULTIPAR SUBTERRANEO

Son conjuntos de conductores aislados entre sí y colocados de tal forma que constituyen un bloque que se envuelve con una o varias cubiertas protectoras, instalándose ya sea sobre apoyos en canalización.

Elementos de un cable multipar

En las constituciones fisicas de un cable pueden distinguirse cuatro elementos

1 - Conductores
2 - Aislantes
3 - Cubierta protectora
4.- Revestimiento y armaduras

Los conductores son de cobre recocido puro y de diversos diámetros según el tipo de cable Cada conductor esta aislado de los demás por papel o por alguna materia plástica de bajas perdidas. Dentro del cable, los conductores se agrupan en pares y estos a su vez en capas anulares concéntricas.

Se les llama pares de cable concéntrico a aquellos cables que tienen sus dos hilos simétricos respecto a la tierra. Estos cables están constituidos por parejas de conductores trenzados independientemente y dispuestos en capas. Los cables de pares se utilizan tipicamente en aplicaciones de bajas frecuencias y de transmisión digital a nivel PCM 2.048 MBPS

2.4 CARACTERISTICAS DE PROPAGACION DE LOS CABLES

Las caracteristicas de propagación de los cables pueden establecerse bajo dos tipos de parámetros

1.- Parámetros primarios. Dependen de la construcción del cable, del tipo de calibre, etc

De acuerdo a la tabla 1.1

PARÁMETROS PRIMARIOS	DESCRIPCIÓN
Parámetros longitudinales	Resistencia R (ohms) e inducción L (henrios)
Parámetros transversales	Capacidad C (Farads) y la permitancia entre los hilos G (mhos)

2 - Parámetros secundarios Estos especifican las caracteristicas de la línea desde el punto de vista transmisión, de acuerdo a la tabla 1 2

PARAMETROS SECUNDARIOS	DESCRIPCION
Impedancia caracteristicas	Se denomina impedancia característica Z0 de una Linea homogénea, aquella impedancia tal que co-locada en un extremo cualquiera, se ve desde el otro la misma impedancia Z0
Constante de propagación	Depende de los parámetros primarios antes descritos Constante en la que no hay ondas estacionarias.
Constante de atenuación	Espera la atenuación o pérdida de la señal de Tx por Unidad de longitud
Constante de fase	Expresa la diferencia de fase en corriente o tensión

2.5 CARACTERISTICAS ELECTRICAS DE LOS CABLES

1.- Resistencia por unidad de longitud.
2.- Inductancia kilométrica.
3.- Capacidad kilométrica
4.- Permitancia.

2.6 CABLE DE PAR TRENZADO

Un par de alambres trenzados y aislados forman un par trenzado TP (Twisted -Pair). Uno o más pares trenzados forman un cable de par trenzado. Existen dos tipos:

- Cable UTP (Unshielded Twisted Pair)
- Cable STP (Shield Twisted Pair)

El trenzado de los pares de alambres reduce la interferencia. Se utilizan comúnmente conectores modulares telefónicos RJ-11 (para cable de dos pares) o RJ-45 (para cable de 4 pares).

Para los cables UTP existen las siguientes clasificaciones, en función de la naturaleza de la señal que transportarán y su velocidad.

- Categoría 1: Transporta voz pero no datos
- Categoría 2. Transporta datos hasta una velocidad de 4 Mbps.
- Categoría 3. Transporta datos hasta una velocidad de 10 Mbps.

- Categoria 4 Transporta datos hasta una velocidad de 16 Mbps
- Categoria 5 Transporta datos hasta una velocidad de 100 Mbps

2.6 1 VENTAJAS DE PAR TRENZADO

- Los sistemas telefónicos usan cable de par trenzado, estan presentes en la mayoria de los edificios; y los pares que no están en uso pueden utilizarse para las conexiones de red.
- Puede ser instalado con relativa facilidad.
- Es hasta cierto punto barato.

2.6.2 DESVENTAJAS

- Sensible a la interferencia electromagnética.
- En donde no existen pares libres en el sistema telefónico hay que hacer una nueva instalación

2.7 ESPECIFICACIONES PARA CABLE UTP (4 PARES).

Aplicaciones.- 100 Mbps TPDDI, 155 Mbps ATM, IEEE 802.3, IEEE 802.5, ISDN.

Estándares.- TIA/EIA-568-A, ISO/TEC - 11801, verificados por UL y ETL.

Longitudes estándares.- 500 ft (152 5 mts) y 1000 ft (305 mts.)

Materiales utilizados para resistencia a flama.- CMR

Descripción del cable : Cable sólido de calibre 24 AWG, aislante termoplástico, forro de aleación de polímeros

Caracteristicas fisicas del cable 4 pares.- forro gris, blanco, azul, rosa, rojo, amarillo, violeta ó naranja: diámetro externo en color gris 0.150" (3.81 mm) peso de 18 lb/kft (27 Kg/Km).

Desempeño:

Impedancia (+/- 15 % máx.)	100 ohms +/- 7 % típica 1-100 Mhz
Capacitancia Mutua	5.6 nF / 100 m
Resistencia DC	9.38 / 100 m
Velocidad Nom. de propagación	72 %

Frecuencia en MHz	Impedancia Caracteristica en ohms	SRL (dB) peor par	Atenuacion dB / 100m max.	NEXT peor par Min. (dB)
0 772	102+/-15 %	NA	1 8	64
1 0	100+/-15 %	23	2.0	62
4.0	100+/-15 %	23	4 1	53
8 0	100+/-15 %	23	5.8	48
10.0	100+/-15 %	23	6.5	47
16.0	100+/-15 %	23	8 2	44
20.0	100+/-15 %	23	9 3	42
25.0	100+/-15 %	22	10.4	41
31.25	100+/-15 %	21	11 7	39
62.5	100+/-15 %	18	17 0	35
100.0	100+/-15 %	16	22.0	32

ML 1C. 6P (F.O.)M.- (Cable de 12 fibras ópticas multimodo) Voz, Datos y Video
Uso rudo con armadura de acero para interiores y exteriores:

Beneficios:

- Esta fibra se puede utilizar en ambientes industriales y hostiles, internos y a la intemperie.
- Altamente protegida para áreas de alto riesgo
- Se puede enterrar directamente sin necesidad de un conduit.
- Extra protección para roedores.

Especificaciones ambientales:

- Temperatura de operación: -40 a 85 grados centígrados.
- Temperatura de almacenaje: -55 a 85 grados centígrados.

Longitudes estándares.- 1.0, 1.2, 2.0 Km.
Características físicas del cable de 6 fibras:

- Diámetro exterior del cable 0 583" / 14.8 mm)
- Peso del cable 235 lb/ft (350 Kg / Km)
- Mínimo radio de doblado al instalar 8.7" (22.2 cm)
- Carga máxima al instalar 645 lb (2.872 N)

Caracteristicas opticas (multimodo)

Atenuación máxima @ 850 nm/1300 nm	3 5/1 0 dB (62 5/ 125)
Ancho de banda mínimo @ 850 nm / 1300 nm	160 / 500 (62 5 / 125)

2 8 CABLE COAXIAL

El cable coaxial esta constituido por un conductor cilíndrico insertado concéntricamente en otro conductor de forma tubular.

En el cable coaxial se distinguen cuatro elementos o componentes:

1 - Conductores

2.- Dialécticos

3 - Aislamiento

4.- Armadura

2.8.1 CONDUCTORES

El cable coaxial está constituido por un conductor cilíndrico insertado concéntricamente en otro conductor separados por un material aislante.

2.8.2 DIALECTICO

Para líneas de transmisión de coaxial, el tubo se llena de un gas a presión, que junto con el material que los separa forma el dieléctrico. En algunos casos el conjunto separador dieléctrico es un material aislante de espuma sólida que rellena todo el espacio comprendido entre los conductores. El material utilizado es el polietileno.

2.8.3 AISLAMIENTO

Los tubos coaxiales se aíslan entre sí y el resto de los elementos del cable por medio de una cinta de papel enrollada al conductor exterior.

2.8.4 ARMADURA

Para aumentar la resistencia mecánica del cable y asegurar una protección complementaria contra la diafonía, se rodea cada tubo coaxial de una o más cintas de acero dulce, enrolladas helicoidalmente.

2 8 5 APLICACION DEL CABLE COAXIAL

Actualmente los cables coaxiales se utilizan en las interfaces entre los multiplexores digitales, en las interfaces de las centrales digitales con el equipo múltiplex y los terminales de línea, y en general en las interfaces eléctricas a 75 ohms

Varios tipos de cable coaxial son utilizados en redes comúnmente, dependiendo del tipo y de los requerimientos de servicio.

Tipos y estándares en los cuales se usa el cable coaxial:
-RG-8 y RG-11. - Para Ethernet en cable grueso (50 ohms).
-RG-58.- Para Ethernet en cable delgado (5 ohms).
-RG-59 - Usado en los sistemas de televisión por cable (75 ohms).

2.8 6 VENTAJAS

- Tecnología y standard maduros, lo cual indica que existe compatibilidad e interoperatibilidad entre diferentes marcas de equipos.
- En algunos de sus estándares maneja anchos de banda más amplios que el par trenzado.

2 8.7 DESVENTAJAS

- Susceptible a la interferencia electromagnética.
- Algunos tipos de cable son caros

2 9 FIBRA ÓPTICA

La fibra óptica, es actualmente el medio de transmisión más utilizado por su versatilidad, su aplicación va desde enlaces a alta velocidad en larga distancia, hasta enlaces de baja velocidad.

¿QUE ES LA FIBRA ÓPTICA?

Es un filamento hecho de fibras de material (vidrio o plástico) conductor de luz. Estas fibras se encuentran al centro de un tubo de revestimiento protector, a su vez rodeado de una gruesa cubierta exterior.

Los dispositivos de interfaz para fibra óptica convierten las señales en pulsos de luz y viceversa Loso pulsos de luz son generados por diodos emisores de luz (LED) o por diodos de inyeccion laser (ILD Injection Laser Diode), los pulsos de luz se convierten en señales electricas a través de fotodiodos.

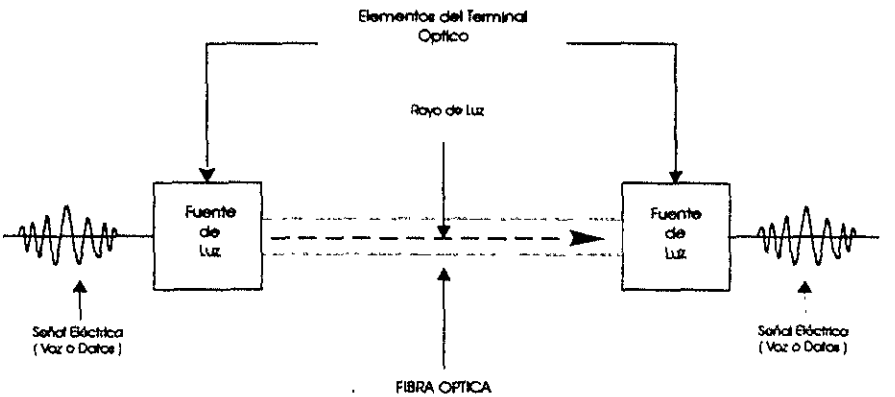


FIGURA 2.1.

Fibra óptica como medio de transmisión

La fibra óptica es un medio de transmisión de información analógica o digital, cuyos principios básicos de funcionamiento se ajustan de forma clara, aunque poca rigurosa aplicándole las leyes de la óptica geométrica. El mecanismo de propagación en el interior de la fibra, se puede explicar a través de la solución de las ecuaciones de campo electromagnético; es decir, las ecuaciones de Maxwell.

Básicamente la fibra óptica está compuesta de.

1.- Núcleo. Compuesto por una región cilíndrica, por la cual se efectúa la propagación de la luz.

2 - Revestimiento. La zona externa y coaxial con el núcleo, totalmente necesario para que se produzca el mecanismo de propagación, y que se denomina envoltura o revestimiento que sólo es de plástico

En cualquiera de las partes anteriores se deberá cumplir con la diferencia de los índices de refracción, como se ve en la siguiente figura 2.2.

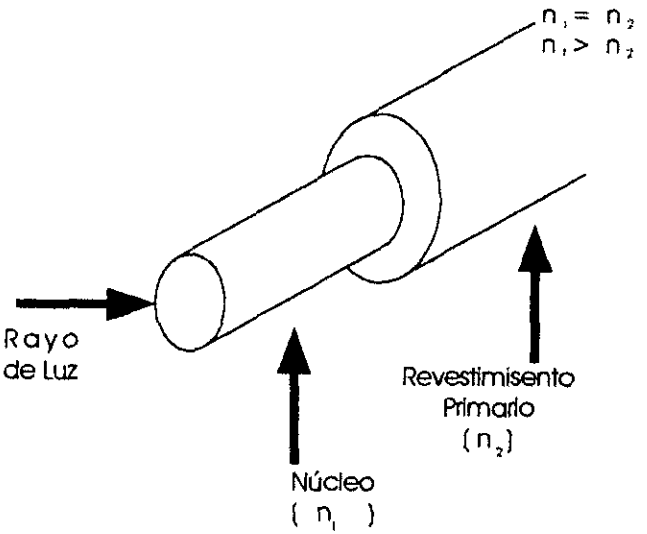


FIGURA 2.2.

Componentes de una fibra óptica

La capacidad de transmisión de la información que tiene la fibra óptica depende de tres características fundamentales:

a) Del diseño geométrico de la fibra

b) De las propiedades de los materiales empleados en su elaboración (Diseño óptico).

c) De la anchura espectral de la fuente de luz utilizada. Cuando mayor sea esa anchura, menor será la capacidad de transmisión de información de esa fibra.

2 9 1 PROPAGACION

Las ondas electromagnéticas viajan en el vacío a la velocidad de la luz,"C". En el aire es casi la misma velocidad, pero en otros medios, tales ondas viajan a menor velocidad (Vm). Para conocer la diferencia de las velocidades se introduce el índice de refracción como el cociente C/Vm.

El índice de refracción (designado por la letra "nu", η) es un número sin unidades y siempre mayor que uno ($\eta>1$)

Cada material tiene un valor específico del índice de refracción, leves variantes en la composición, con impurezas, afectan el valor del índice de refracción, alterándose también las propiedades ópticas del material.

En las fibras ópticas ocurre esto, la diferencia entre los núcleos y el revestimiento están en la segunda y terceras cifras decimales del índice de refracción

Cuando un rayo de luz choca con una superficie puede ocurrir una reflexión, una refracción o ambos fenómenos Esto es debido también, a los cambios del índice de refracción. En el caso de reflexión se deberán cumplir algunas condiciones.

a) Superficie altamente pulida o reflejante

b) Ángulo de incidencia adecuado

2.9.2 REFLEXION

En la siguiente figura se muestra la reflexión a la entrada de la fibra óptica donde θy (ángulo de incidencia) igual a θr (ángulo de reflejancia).

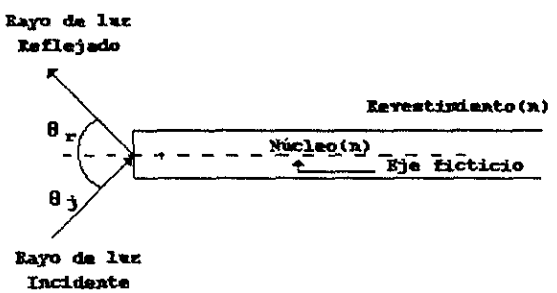


FIGURA 2.3

Reflexión en una fibra óptica

Como se puede observar, este fenómeno causa que la mayor cantidad de luz sea lanzada fuera del núcleo de la fibra óptica, el cual no es el objetivo.

Los ángulos que forman el rayo incidente y el reflejado con la normal a la superficie de separación de los dos medios son iguales.

2.9.3 REFRACCION

Este es otro fenómeno es el mas importante desde el punto de vista de la entrada de luz al núcleo de la fibra óptica.

En la siguiente figura podemos observar que la refracción ayuda a introducir la mayor cantidad del núcleo, con respecto al eje ficticio de la fibra

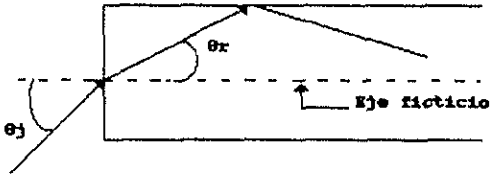


FIGURA 2.4

Refracción en una fibra óptica

¿Por que ángulos pequeños? Fundamentalmente es para cumplir con el aspecto geométrico de la luz (rayos de luz) y la condición de reflexión total en la frontera núcleo revestimiento.

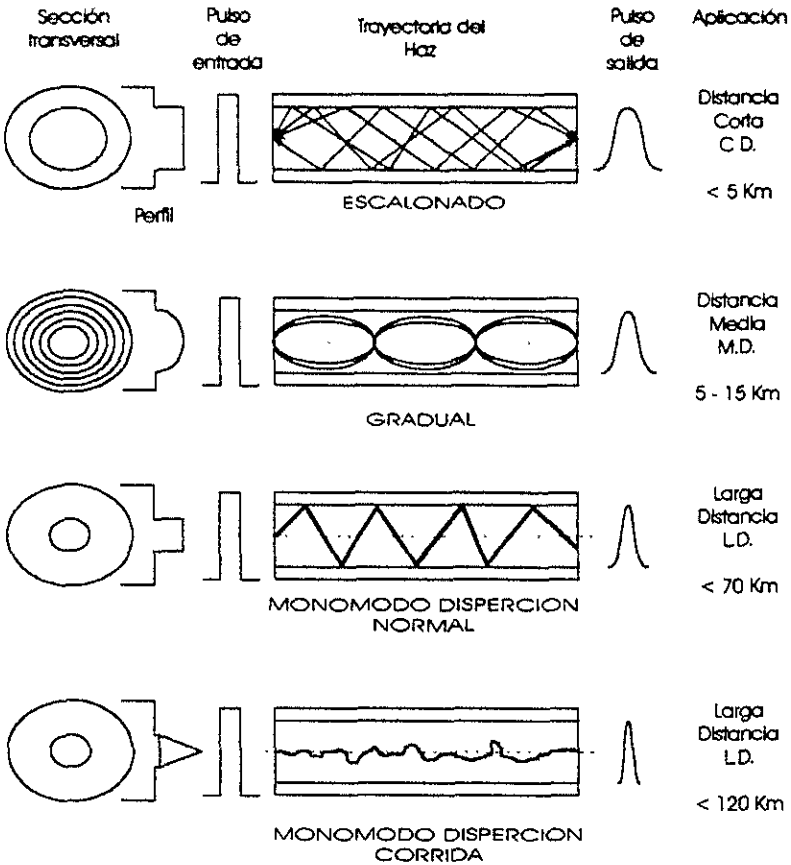
2.10 LEY DE SNELL

La ley de SNELL es una relación trigonométrica que nos permite evaluar el ángulo de entrada adecuado, en función de los índices de refracción (η_0, η_1, η_2) y la reflexión total interna del rayo de luz

Por otra parte, si existe un ángulo grande de incidencia, tendremos un rebote total del rayo de luz conocido como reflejancia (R), dado este por la siguiente expresión:

$$R = \frac{\eta 1 - \eta 0}{\eta 1 + \eta 0}$$

Existe una condición práctica a considerar, R deberá ser menor o igual al 4 %



Tipos de fibra óptica

FIGURA 2.5

TIPOS DE FIBRA ÓPTICA

2.11 VENTAJAS

- Inmunes a la interferencia que se genera afuera del cable. El cable de fibra es un medio de transmisión extremadamente confiable y seguro
- Maneja anchos de banda muy amplios
- No existe diafonia

- No puede ser interferida
- Capacidad de multiplexaje amplio
- Totalmente dieléctrica
- Tamaño pequeño, poco peso, soporta grandes tensiones y tiene mucha flexibilidad
- Inmune a la corrosion en comparacion con el cable de cobre

2 11.1 DESVENTAJAS

- Las pérdidas de acoplamiento y su dificultad en las aplicaciones de campo por el pequeño tamaño de cada una de las fibras
- Algunas fuentes luminosas tienen vida útil muy limitada, ejemplo el láser.
- Las interfaces de red y los cables son relativamente caros
- Las conexiones requieren de una fabricación muy precisa y de un manejo cuidadoso
- Relativamente complejas de configurar e instalar

2.12 MICROONDAS

Se encuentran generalmente en el intervalo de frecuencias de los Ghz. Para que pueda darse uno de estos enlaces debe existir línea de vista entre las antenas parabólicas de ambas estaciones, esto quiere decir que no debe de haber ningún obstáculo entre una y otra.

Susceptibilidades a la interferencia externa, la sobretransmisión (jamming) y la atenuación Las microondas de muy alta frecuencia son más atenuadas por la lluvia y la niebla en enlaces de larga distancia.

2 12 1 VENTAJAS

- Es mucho más barato que tender cable entre las estaciones
- Son posibles amplios anchos de banda
- Requieren autorización del canal por parte de la SCT

2.12 2 DESVENTAJAS

- Susceptibles a la interferencia y a la atenuación en grandes distancias

2 13 SATELITALES

Enteramente dependiente de la tecnologia espacial, pero proveen enlaces a las más remotas zonas del planeta

2 13 1 VENTAJAS

- El retardo de propagacion y el costo de la comunicación es independiente de la distancia entre el transmisor y el receptor.
- Son posibles amplios anchos de banda
- Las estaciones de tierra pueden ser fijas o móviles
- Pueden abarcar una amplia gama de cobertura
- Requiere de solicitar el servicio a la SCT

2.13 2 DESVENTAJAS

- Susceptibles a la interferencia externa, sobretransmisión e interferencia entre canales adyacentes
- La tecnología utilizada es cara
- Los enlaces de larga distancia tienen un notable retardo de propagación en comparación con la línea directa en transmisión de datos.

2 14 RDI: Red Digital Integrada

Entre los servicios que proporciona la RDI encontramos principalmente:

- Dataenlace
- Enlace digital DS-0
- Enlace privado E-0
- Enlace privado E-1
- Enlace privado E-1 Punto - Multipunto
- Enlace privado satelital de voz hasta 19.2 Kbps Nacional
- Enlace privado satelital de datos hasta 9.6 Kbps Nacional
- Enlace privado satelital de datos hasta 19 2 Kbps Nacional
- Enlace privado satelital de datos hasta 64 Kbps Nacional

2.15 ENLACE DIGITAL DS-0

Es un servicio para transmision de voz, datos o video, permitiendo integrar enlaces punto a punto, a una velocidad de 64 Kbps, por medio de un canal digital sincrono, brindado a traves de una interface V.35 y un conector M.34.

Los enlaces privados pueden ser establecidos a nivel:

Local. Se da cuando los extremos se encuentran dentro de la misma ciudad o area metropolitana.

Larga distancia. Se da cuando los extremos se encuentran en diferentes poblaciones.

Caracteristicas y aplicaciones.

El servicio se entrega en un par de hilos de cobre con terminación V.35 en el último tramo del o los sitios o vía radio digital.

Alta calidad en la transmisión de señales con un promedio minimo de errores.

En larga distancia internacional y de cruce fronterizo, el cliente deberá elegir el carrier con el que desea la conexión

Aplicación para: voz, datos y video.

2.16 DATAENLACE

Servicio digital para transmisión de voz, datos y video que permite integrar enlaces punto a punto, a una velocidad comprendida en el rango de 4.8 a 19.2 Kbps, por medio de un canal sincrono con una interface V.24 y conector DB.25

Caracteristicas y aplicaciones

El servicio se entrega en un par de hilos de cobre con terminación V24 en el último tramo del o los hilos o vía radio digital.

Alta calidad en la transmisión de señales con un promedio mínimo de errores.

Se puede manejar a velocidades hasta de 19.2 Kbps.

En larga distancia internacional y de cruce fronterizo, el cliente deberá elegir el carrier con el que se desea la conexión.

No requiere de acondicionamiento del local por parte del cliente.

Por ser una señal digital el cliente no requiere módem.

Aplicaciones para: voz, datos y video.

CAPITULO 3

OPTIMIZACION DE RECURSOS PARA TRANSMISION DE VIDEO

3 1 COMPRESION DE VIDEO

Las imágenes de televisión terrestres comerciales son transmitidas como señales analógicas y parecen permanecer así por algunos años, debido al costo y decisiones que se tendrían en los estándares internacionales Pero los servicios satelitales dejan atrás estas técnicas para convertirlas en transmisiones digitales que se encuentra libre de señales de ruido y dado la información se puede comprimir, puede dar televisión de alta definición y servicios de audio con una amplia variedad de canales a un costo razonable. Desafortunadamente así como todos los nuevos conceptos, las diferentes tecnologías compitiendo, tendrán que examinarse, probarlas exhaustivamente por ingenieros, agencias internacionales para elegir la mejor. Aunque la mayor parte del trabajo ya se realizó pasará algún tiempo antes de que los estándares internacionales sean adoptados

La compresión de video en concreto es la conversión de datos en una forma especifica que haga su manejo más eficiente para una mejor grabación en discos, comunicación más rápida con maquinas de fax a través de líneas telefónicas, transmisión de imágenes vía satélite, etc La compresión es usualmente hecha por la reducción de redundancia o por la eliminación de datos que no sea necesario tener presentes para un propósito especifico *Esto es, transportar la misma información pero de un modo más eficiente.*

El entendimiento de la compresión es difícil ya que existen diferentes algoritmos, aún más cada industria habla su propio lenguaje y tiene su propio conjunto de expectativas de acuerdo a las necesidades primordiales.

Un algoritmo es simplemente un conjunto de procedimientos, una serie de operaciones matemáticas que se utilizan para descartar grandes cantidades de información de vídeo digital mientras retiene información para construir una imagen. Existe un número de familias de algoritmos de compresión con nombres como· Transformación del coseno discreto (DCT), Ondas y Fractales.

Varios grupos de estudio trabajando bajo el control de ISO (Intertational Standar Organization), la CCITT y la CCIR están ya trabajando en la transmisión digital de imágenes y en particular en técnicas de reducción de rango de bit (bit-rate). El grupo experto de película en movimiento denominado MPEG (Motion Picture Expert Group), se le acredito como el primero en producir un algoritmo con el hardware necesario para procesamiento de imagen con tiempo real de movimiento

La television viene a ser un medio analogo, los cuadros de video son capturados, almacenados procesados y transmitidos usando tecnicas analogicas en la que la señal da forma al cuadro referido

Ahora la television une informacion tecnica y electronica de comunicacion y lo hace en forma digital, esto es, la informacion es muestreada en muchos puntos en espacio y tiempo, y estos valores muestreados son convertidos en códigos binarios digitales (ceros y unos)

La transmisión digital incluye un gran conjunto de datos, los cuales retan la capacidad de acarreamiento de información de canales de transmisión, para dicha transmisión se requiere el manejo de corriente de datos digitales La velocidad de esta corriente de datos es la llamada bit-rate, esta medida de cantidad de datos se da en bit/seg.

El reto es encontrar el camino en que las altas demandas de información puedan ser acomodadas por la capacidad de almacenamiento de la media existente y la capacidad de acarreamiento de información de las bandas de canales de transmisión existente y transmisión por cable. Hoy en dia, grandes conjuntos de datos digitales pueden ser empacados con una media analógica existente. Datos de compresión de audio/vídeo vienen a ser el corazón de la tecnologia después de numerosas aplicaciones en el mundo del entretenimiento, negocios e industria.

"La relación de compresión" se refiere a la cantidad de información necesaria para representar la imagen comprimida. Por lo tanto, una relación de compresión 20:1 significa que la imagen comprimida utiliza aproximadamente 1/20 de datos del original.

Para efectuar la compresión en tiempo real se requiere una gran cantidad de poder de cálculos para producir un vídeo de calidad. Por lo tanto, en algunos casos, particularmente para cuadros completos de vídeo con 30 fps (tramas por segundo), aún no es posible hacer la compresión en tiempo real y producir una mejor calidad Un usuario que necesite preservar la calidad debe comprimir más lentamente, permitiendo a la *computadora que tome su tiempo para hacer los cálculos complejos de compresión.*

Alguna compresión de vídeo está hecha dentro de cada cuadro de vídeo y se le conoce a está como "Compresión de Entrecuadro". Mientras que otros trabajan prediciendo el movimiento entre cuadros y se le conoce como "Compresión de Intercuadro".

La compresión de intercuadro puede ser muy eficiente y permite muy altas relaciones de compresión, pero graba un cuadro completo solamente cada 10 cuadros.

Actualmente dominan los algoritmos basados en DCT, especialmente en MPEG 1 y 2, un par de normas que surgen a nivel mundial que tienen aplicaciones en transmision por cable, satélite, inalambrico y computacion.

Los fractales están siendo utilizados en algunas aplicaciones que no requieren compresión en tiempo real. Permiten relaciones de compresión muy grandes, de hasta 500:1 aunque 100:1 es más típico También dan la habilidad para reconstruir una imagen en un rango excepcionalmente amplio de resoluciones, dependiendo de la potencia del hardware de descompresión Es problema con los fractales es que pueden ser altamente asimétricos. Frecuentemente se necesitan 60 veces el tiempo real para comprimir una imagen, pero puede requerir tanto como *100 veces.*

3 2 SEÑAL DE VÍDEO

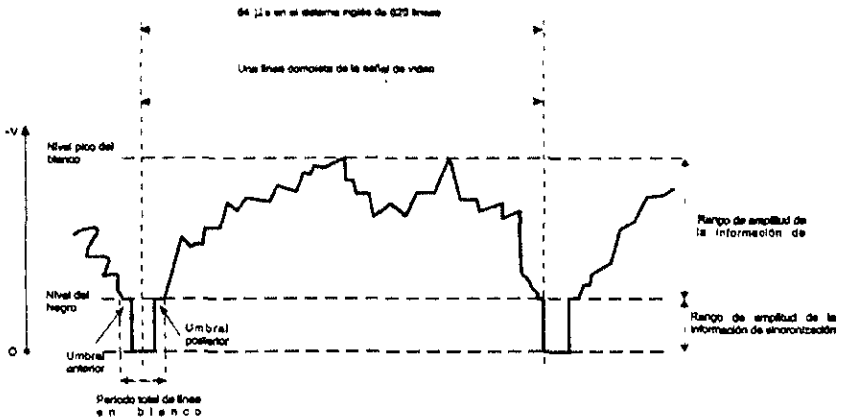
La combinación de una señal de visión (o imagen) y pulsos sincronizadores es llamada señal de video.

También se incluye un periodo en blanco o periodo de supresión de imagen a fin de darle tiempo al punto para que haga el retorno desde una línea hasta la próxima, y desde el final de un campo o cuadro al principio del próximo. Esto se ilustra de manera sencilla en la figura 3.1, donde puede verse que la imagen y la información de sincronización están separadas por tiempo y amplitud.

La figura 3.1 ilustra lo que es conocido como un envío positivo o modulación positiva de la señal de video. Aquí debe indicarse que algunos sistemas de televisión usan un envío negativo o modulación negativa de la señal de video que esta de cabeza comparada con la figura 3.1.

Los pulsos sincronizadores de línea y campo (o cuadro) se incluyen en la región de amplitud del nivel en blanco los pulsos sincronizadores de línea son simples pulsos cortos, mientras que los pulsos sincronizadores de campo son una serie de pulsos anchos. Esto se ilustra en forma simple en la figura 3.2.

Los pulsos sincronizadores de campo toman un tiempo equivalente a un cierto número de líneas de acuerdo con el sistema en uso, y son seguidos de un número de líneas suprimidas.



Principio simple de la señal de video

Figura 3.1

En el sistema de 405 líneas del Reino Unido los pulsos sincronizadores de campo ocupan el equivalente a cuatro líneas, seguidas por 10 líneas suprimidas, dando una supresión total equivalente a 14 líneas por campo. Así, por cada imagen completa consistente de dos campos entrelazados sucesivos, se usan 28 líneas para sincronización de campo lo que da (405-28) = 377 líneas que contienen la información de *video o imagen*

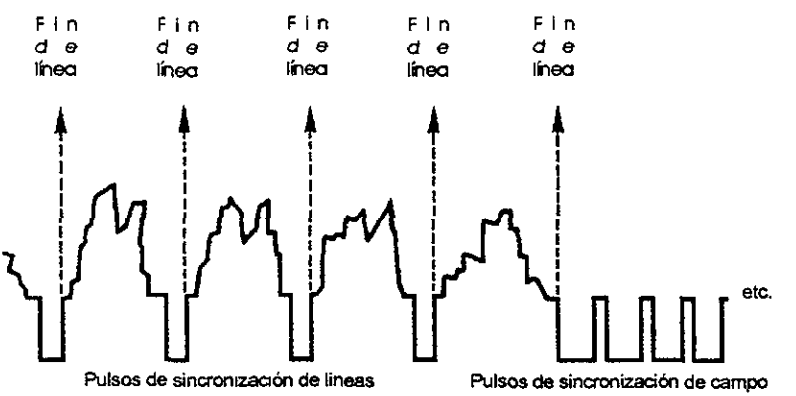


Ilustración simple de pulsos de sincronización de línea y campo

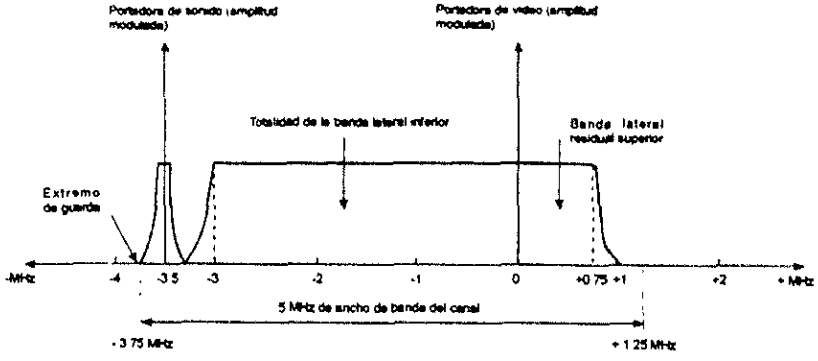
FIGURA 3 2

3 3 ANCHO DE BANDA DE LAS SEÑALES PORTADORAS MODULADAS EN VÍDEO

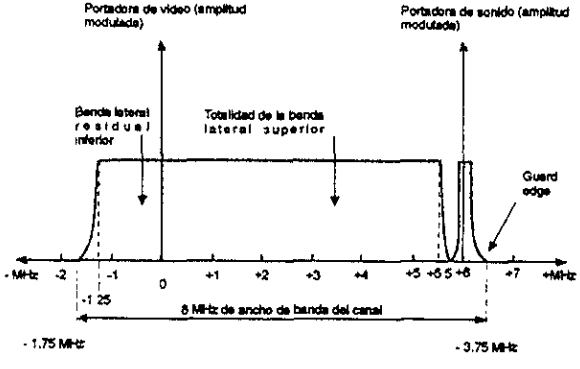
Cuando una portadora es modulada en su amplitud por una señal de información, el ancho de banda de la onda modulada es el doble de la frecuencia más alta de la señal modulada Se establece que una señal de visión tiene un amplio rango de frecuencias, cuya frecuencia más alta es de aproximadamente 3 Mhz para un sistema de 405 líneas y 5.5 Mhz para un sistema de 625 líneas. Si se usa amplitud modulada en doble banda lateral, se requerirá por tanto una amplitud de banda de aproximadamente de 6 Mhz para 405 líneas y 11 Mhz para 625 líneas, más un ancho de banda para la otra onda portadora modulada en sonido.

A fin de reducir el ancho de banda necesario para cada transmisión y así permitir más transmisiones en una banda de frecuencia dada, la onda modulada se pasa a través de un filtro de banda lateral residual que suprime parte de una de las bandas laterales como se ilustra en la figura 3.3.

En la figura 3 3 se muestran frecuencias relacionadas con las frecuencias portadoras de visión. Se verá que en un sistema de 405 líneas la portadora de sonido está 3.5 Mhz por debajo de la portadora de visión asociada, y la banda lateral superior esta restringida. Para comparar en un sistema de 625 líneas la portadora del sonido está 6 Mhz por arriba de la portadora de visión asociada, y la banda lateral baja esta restringida. Observe también en la misma figura que hay un "margen de seguridad" entre el ancho de banda de la información de sonido y el extremo de un canal en particular.



a) Sistema de 405 lineas



b) Sistema de 625 lineas

FIGURA 3.3

En el Reino Unido las frecuencias portadoras de visión y sonido están asignadas a los diferentes canales en las bandas de televisión, de manera que cada canal completo queda dentro de una sección particular de la banda, y así se evita la interferencia entre canales adyacentes

3.4 LO QUE VE EL OJO

Un cuadro de vídeo contiene una gran distribución de información, no toda visible para el ojo humano. En cada señal de vídeo existe redundancia en espacio y tiempo, dichas redundancias son las que las técnicas de vídeo compresión explotan para tener varios grados de reducción de bit-rate.

La redundancia en espacio se refiere a la información redundante en la información horizontal y vertical de un cuadro, datos similares o repeticiones del mismo en areas del cuadro que estan cerca una de otra

Redundancia en tiempo se refiere a las redundancias en diferente tiempo, el dato es similar o se repite a ratos, excepto si el área del cuadro cambia.

En el dominio de espacio, el grado de correlacion es usualmente encontrado en áreas adyacentes del cuadro. En todos los casos, el nivel de dependencia entre valores de pixeles es determinado por la capacidad de respuesta en frecuencia del sistema

En el dominio del tiempo, la mayoría de las señales de vídeo incluye grandes conjuntos de redundancia de datos. Si esta circunstancia no cambia en algunos segundos o en algunos minutos, puede consistir enteramente en datos de pixel redundantes. Conociendo la amplitud del pixel antes de que aparezca en la secuencia de video permite más eficiencia en los esquemas de reducción de bit-rate.

3.5 NECESIDADES DE LA COMPRESION DIGITAL

Las transmisiones de satélite comercial así como las transmisiones terrestres, deben permanecer económicamente viables para hacer uso eficiente de los canales disponibles y capacidad de almacenaje.
La selección recae entre pocas transmisiones de alta calidad, cada una ocupando un amplio ancho de banda, o un número mayor de transmisiones de aceptable calidad, cada una ocupando un ancho de banda mas angosto empleando técnicas basadas en el concepto de redundancia.

Para justificar las complicaciones adicionales de las técnicas de compresión útil estudiar la aritmética de las señales digitales. Una señal de vídeo normal sin comprimir tipo PAL-1 ocupa un ancho de banda de 5 5 Mhz, así que de acuerdo al teorema de Nyquist que dice que la señal debe de ser muestreada digitalmente a 11 Mhz. Para una resolución razonable, cada muestra requiere de al menos 8 bits binarios y el rango de transmisiones de 88 Mbps aún para blanco y negro. Una imagen de color tiene componentes rojo, verde y azul, entonces el rango de transmisión debe de ser tres veces mayor resultando una transmisión final de 264 Mbps.

Los problemas de transmisión en este tipo, podrían ser lo suficientemente malos, pero los problemas de almacenamiento podrían ser peor aún Por ejemplo, una película dura 90 minutos (5400 seg) un disco duro de 340 Mbyts de una computadora personal tiene una capacidad de 2.7 Gbit, esto tomaría 528 discos duros para almacenar tal película. Los ciclos o velocidades de transmisión entre la computadora y el disco duro raramente son mayores a 30 Mbps lo cual significa que son 8 veces más lentos El CD-ROM comúnmente

disponible trabaja a 2 4 Mbps (110 veces mas lento) Esta claro que la compresion de video digital no es solo ventajosa sino comercialmente necesaria

La compresion esta justificada económicamente. Si el costo de la comunicación y su almacenamiento es menor que el costo del equipo de compresión y descompresión del video y cuando reúne los requisitos mínimos de calidad.

La señal analógica de video más usada en los EU es la señal NTSC, con un ancho de banda de 4 2 Mhz Siguiendo el teorema de Nyquist, una señal NTSC requiere una frecuencia de muestreo de 8 4 Mhz, con 8 bits por muestra, esto conduce a una razón de bits de 67.2 Mbps. Multiplicando por 3 cada uno de los colores primarios (rojo, verde y azul), conduce una tasa de bits de 201 Mbps La dificultad de mover y almacenar información a tan alta razón de datos es difícil de ver

Otro ejemplo esta en la velocidad de los módems para canales de voz en la red de teléfono público que opera a menos de 20 Kbps; así necesariamente 10000 canales para llevar la señal. Muchas de las aplicaciones más interesantes del video podrían continuar siendo inconcebibles sin compresión.

Con el surgimiento de la compresión sus aplicaciones están ya mostrando el video desde el disco duro de la computadora y de los CD- ROOMS. Se ha desarrollado un video teléfono que permitirá la comunicación de vídeo y voz sobre una línea telefónica sencilla.

La fuente de una imagen digital puede ser una escena de tres dimensiones en el mundo real, o puede ser una imagen de dos dimensiones generadas previamente, por ejemplo, una fotografía. En otro caso, la información de la fuente generadora es analógica, es decir, es continua en espacio y en amplitud. Para generar una imagen digital, la fuente, primero es muestreada en locaciones discretas usando algún tipo de censor (o censores, si algunos datos a color o multiespectrales son requeridos). Estas muestras son los llamados pixeles o pels (picture elements). Los valores del pixel producidos por el sensor son continuos sobre algún rango finito, y usualmente están relacionados linealmente con la intensidad de energía radiante en cada localización de las muestras. El uso del término energía radiante (más que luz) es deliberado puesto que el sensor puede ser sensitivo a longitudes de onda fuera del rango de la visión humana. En el caso de una imagen generada previamente (tal como una fotografía o transparencia), la energía radiante es el resultado de una fuente de iluminación alumbrando a la imagen y llegando la energía a ser reflejada o transmitida al censor.

Hay diferentes estrategias para el muestreo de las locaciones, pero la forma más común es el uso de una rejilla rectangular igualmente espaciada. Idealmente cada muestra corresponde a una región infinitamente pequeña de la fuente, pero debido a la naturaleza física de los censores y a la óptica asociada, esto es un valor integrado sobre alguna área finita El número de locaciones de muestra por unidad de área

define la razon de muestreo del sistema, y esta razon de muestreo puede ser escogida basandose en el teorema de muestreo de Nyquist, es decir, la razon de muestreo podria ser por lo menos dos veces el componente de frecuencia mas alta de la fuente

En un sistema de digitalización de imagen, la razon de muestreo es continuamente dada en términos de la resolución de exploración, la cual es la inversa de la razon de muestreo En general la razón de la exploracion requerida depende de la aplicación.

Cada punto muestreado de valor continuo es cuantizado a un número discreto de niveles en orden para formar la imagen digital. Los cambios uniformes en los valores de intensidad no son percibidos igualmente por el SVH (sistema visual humano). Por ejemplo, la cuantización uniforme de los valores de intensidad (es decir, cuantización en el espacio lineal) puede resultar en errores de cuantización visualmente aparentes como áreas obscuras. Puesto que las imágenes son vistas por los humanos en el mayor número de aplicaciones, es importante desarrollar la cuantización en un dominio que este en acuerdo con la percepción del SVH. En el mayor número de los casos, los valores de pixel son sujetos a la no linealidad (tal como una función logarítmica o raíz cúbica), antes de la cuantización, que aproxima a la no linealidad el SVH. El número de niveles de cuantización requeridos para representar adecuadamente una imagen también es dependiente de la aplicación. Para documentos de texto binarios, únicamente dos niveles (1 bit/pixel) son requeridos puesto que cada punto muestreado puede ser blanco o negro. Para escenas naturales o fotografías de tono continuo, es común usar 8 bits/pixel (256 niveles). Sin embargo dependiendo del rango dinámico de la fuente y del tipo de salida del censor (lineal o logarítmica), puede ser necesario utilizar 10 o 12 bits/pixel. En realidad para sobrellevar la inexactitud asociada con la implementación analógica directa de la no linealidad, muchos de los digitalizadores de imagen sofisticados emplean 12-14 bits para cuantizar los valores de pixeles el espacio lineal, aplicando la no linealidad al dato digital, y después recuantizado a 8 bits usando tablas de mejoramiento.

La necesidad de la compresión de imagen llega a ser aparente cuando se computa el número de bits resultantes por imagen desde esquemas de cuantización y razones de muestreo típicas.

Una demanda simple de datos en términos de consumo de una banda digital para aplicarse en su transmisión y su almacenamiento son las secuencias de vídeo digital. En general, es necesaria ya que existe una considerable desigualdad técnica y económica entre los requerimientos para transmisión/almacenamiento de vídeo digital en tiempo real y lo que puede alcanzarse por las tecnologías.

Aplicaciones típicas de la transmisión de imágenes son

- La difusión de imágenes de televisión,
- el video teléfono,
- la video conferencia,
- la percepción remota, (imágenes multiespectrales y de radar),
- las comunicaciones entre computadoras,
- la transmisión de documentos, (facsímile),
- etc.

El almacenamiento de imágenes se requiere en áreas tales como

- La educación,
- la publicidad, (multimedia),
- la medicina, (tomografía computarizada y resonancia magnética),
- la percepción remota, (imágenes multiespectrales y de radar),
- la edición por computadora,
- los sistemas de información geográfica,
- el arte,
- etc

De acuerdo a la necesidad, existen diversas relaciones de bits en los canales de transmisión e interfaces digitales.

Ejemplos de volumen de información que representan las imágenes digitales son:

- Televisión digital. 216 Mbps
- Televisión de alta definición. 1.6 Gbps
- Vídeo conferencia: 384 Kbps a 2 Mbps
- Videoteléfono: 64 Kbps
- Tomografía computarizada: 1 Megabyte por corte
- Arte: 16 Megabytes por imagen.
- Bases de datos de multimedia· 100 imágenes de 512 x 512 pixeles.
- DS-1 (T1)· 1 544 Mbps
- Ethernet· 10 Mbps (Max.)
- Canal de RF 6 Mhz (mod. Digital) 20-25 Mbps

- SCSI 40 Mbps
- Wide SCSI II 160 Mbps (Max.)
- CD Rom 1 2 Mbps

Existe otro problema para tener necesidad de compresión de imagen, considerando la transmisión de imágenes de video de baja resolución de 512 x 512 x 8 bits/pixel x 3 colores sobre lineas telefónicas. Usando un módem con una velocidad de 9600 baud (bits/s), la transmisión podria tomar aproximadamente 11 minutos para una sola imagen, lo cual es inaceptable para el mayor número de aplicaciones.

3.6 CAPACIDAD DE ALMACENAMIENTO

- 4:2:2 Componentes digitales, requiere 97 Gb (216 Mbps)
- NTSC digital, requiere 58 Gb (128 Mbps)
- HDTV 1125/60 en estudio, requiere 540 Gb (1.2 Gbps)

3.7 EFECTOS DE LOS PARAMETROS DE DIGITALIZACION EN LA COMPRESION DE IMAGEN

La redundancia presente en una imagen digital es altamente dependiente del sistema usado para formar la imagen, tanto como, de los parámetros usados para representarlo. En particular, la razón de muestreo, el número de niveles de cuantización, y la presencia de la fuente y/o censor de ruido pueden afectar todo el desarrollo de compresión. Aunque las variaciones existieran de imagen a imagen, las tendencias siguientes son generalmente encontradas para algoritmos de compresión basados estadisticamente:

- Como la razón de muestreo se incrementa, la correlación (o dependencia) pixel a pixel también se incrementa, lo cual permite una razón de compresión más alta. La razón de compresión (RC) esta definida como:

  RC = Número de bits de la imagen original/ Numero de bits de la imagen comprimida

  Este incremento en correlación de pixel a pixel significa, por ejemplo, que si la razón de muestreo es incrementado por un factor de dos, el incremento en el número de bits requeridos para la imagen compresada será menor en un factor de dos (aunque el número total de bits aún aumentara).

- Aumentando el número de niveles de cuantización se reduce la correlación pixel a pixel, de esta manera se reduce la compresión llevada a cabo.

- La presencia de alguna fuente de ruido (por ejemplo, el ruido granular de película (film) en una impresion fotográfica) o ruido introducido por el censor decrementara la correlación pixel a pixel y reduce la cantidad de compresion llevada a cabo

3.8 ENTROPIA EL PARAMETRO QUE DEFINE LA COMPRESIÓN

Para que podamos o no hacer la compresión eficiente de una serie de datos, dependemos de las caracteristicas de los datos, que vamos a comprimir. No podemos esperar una codificación eficiente para una imagen en donde la aparición de sus caracteres ocurre con igual probabilidad.

Lo anterior explica que puede o no una serie de datos ser eficientemente codificada depende de la probabilidad de aparición de cada dato. En terminología técnica la palabra "entropía" es usada para expresar esto. Si las series de datos tienen una larga curva estadística de la probabilidad de aparición de cada dato, decimos que la entropía es baja. Esto hace que estas series puedan ser eficientemente codificadas. Por otro lado, si la serie de datos no tiene una larga curva estadistica de que cada dato ocurra, decimos que la entropia es alta, refiriéndonos al hecho de no poder codificar eficientemente estos datos.

3 9 CODIFICACION

Como se dijo anteriormente, los datos son comprimidos por una selección de una forma apropiada de codificación, lo que se refiere a asignar un código especifico para cada símbolo (dato) en una corriente de datos . Cada regla de codificación probablemente usada por la corriente de datos es larga pero el receptor (decodificador) conoce esta reglas y puede reproducir los simbolos originales de estos códigos.

Imaginemos una corriente de datos que toma solo dos valores y ese mismo valor continúa por un número de muestras como se observa en la figura (3.4) (a)

Si solo dos valores aparecen en la corriente de datos, A y B, un dato es expresado en forma de bit (= 21). Por instancia, al símbolo A se le asignará el valor 1 y al simbolo B el 0 (b).. El número de bits requeridos para transmitir esta corriente de datos es exactamente el mismo que el número de muestras (c). Esta es la manera más simple de codificar esta corriente de datos.

Por lo tanto, si consideramos que solo hay dos valores en la corriente de datos y que el mismo valor continua por el número de muestras, es fácil imaginar que transmitimos información de tantas muestras como continúe el valor (llamado "run") (d) en lugar de transmitir el valor que expresa cada símbolo por cada muestra. Y esta técnica es conocida como "run lengh encoding"(codificación de longitud corrida).

Si comparamos que requerimos 58 bits cuando transmitimos el valor que expresa el simbolo (c), solo 16 bits son requeridos cuando transmitimos la informacion de tantas muestras como el mismo valor *continúe(c)*.

En este ejemplo los datos son comprimidos por el cambio de la codificación a una más eficiente. Por lo tanto, podemos notar otra vez que la eficiencia de codificar no solo depende del código que usemos la probabilidad de aparición de cada simbolo (o entropia) determina la máxima eficiencia de codificación cuando el código elegido es el apropiado *En una corriente de datos se toman solo dos valores, esto es* determinado por la longitud de corriente de 1's (la longitud recorrida de unos) y la corriente de 0's continuos (esto es la probabilidad de que un 1 aparezca después de un 1 o un 0 aparezca después de un 0 será muy grande), lo más grande la compresión de la velocidad de transmisión.

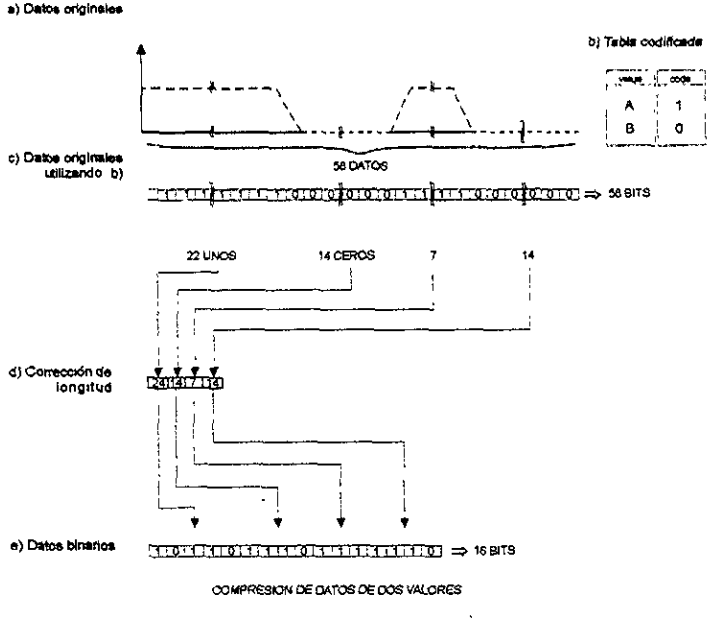


FIGURA 3 4

3.10 TIPOS DE COMPRESION EN SEÑALES DIGITALES

El numero de bits actualmente requerido para representar la informacion en una imagen puede ser substancialmente menos debido a la redundancia En general tres tipos de redundancia pueden ser identificados.

1 Redundancia espacial, la cual es debido a la correlación (o dependencia) entre pixeles vecinos (cercanos entres si).
2 Redundancia espectral, la cual es debido a la correlación entre los diferentes planos de color (por ejemplo, en una imagen de color RGB) o bandas espectrales (por ejemplo, fotografías aéreas en percepción remota).
3 Redundancia temporal, la cual es debida a la correlación entre diferentes tramas en una secuencia de imágenes.

El objetivo de la investigación de la compresión de imagen es reducir el número de bits requeridos para representar una imagen por medio del removimiento de las redundancias anteriores En suma se busca establecer limites fundamentales en el desempeño de algún esquema de compresión para una clase de imágenes dada. Esto es hecho, usando conceptos de la teoría de información. Hay muchos planteamientos para la compresión de imagen, pero pueden ser categorizados en dos grupos fundamentales· Sin pérdidas y con pérdidas.

3.11 TECNICAS DE COMPRESION

En la compresión sin pérdidas (también conocido como preservación del bit o compresión reversible), la imagen reconstruida después de la compresión es numéricamente idéntica a la imagen original sobre una base de pixel-por-pixel. Obviamente la compresión sin pérdidas es idealmente deseada. Sin embargo, solamente una pequeña cantidad de compresión es posible, ya que solo permite una pequeña reducción de bit-rate (velocidad de transmisión)

En la compresión con pérdidas (también conocida como compresión irreversible), la imagen reconstruida contiene degradaciones relativas a la original, Como resultado una compresión mucho más alta puede ser llevada a cabo comparada a la compresión sin pérdidas. En general, más compresión es obtenida a expensas de mas distorsión. Es importante notar que estas degradaciones pueden o no ser visibles aparentemente. La compresión con pérdidas permite alta reducción de bit -rate En realidad, el término visualmente sin pérdidas continuamente ha sido usado para caracterizar esquemas de compresión con pérdidas, que no resultan en pérdidas visibles bajo condiciones de visión normales Desafortunadamente, la

definición de visualmente sin pérdidas es subjetiva y una precaución extrema debe de ser necesariamente tomada en su interpretación

Sobre distancia en espacio, pequeñas diferencias en la amplitud de los pixeles pueden ser enmascaradas en una transición de cerca a lejos. En areas de intensa actividad en espacio la videocompresión puede remover pixeles sin introducir distorsión (o artefactos codificados) que el ojo humano pueda distinguir. Por otra parte, el ojo humano es muy sensible a distorsiones que aparezcan en áreas iguales de un cuadro. En estas areas la compresión de vídeo debe de tener una capacidad muy conservadora.

El ojo y el cerebro no responden a la distorsión de artefactos codificados en objetos móviles o en imágenes inmediatas después de un cambio de escena Usando técnicas para reducir la redundancia entre campos visuales y tramas en el tiempo la compresión de video puede ser terminada con una pérdida no visible en la calidad del cuadro.

Estas dos categorías pueden ser más divididas basándose en la naturaleza de la imagen de entrada original. La imagen puede ser binaria, por ejemplo, textos y documentos, o de tonos continuos, por ejemplo, video de 8-bits, imágenes médicas de 12-bits, etc Puede ser una imagen inmóvil, la cual contiene redundancia espacial (y redundancia espectral si es una imagen de color), o puede ser una secuencia de imágenes, por ejemplo, imágenes en movimiento que también contienen redundancia temporal

3.11.1 TECNICA DE COMPRESION SIN PERDIDAS

Características primordiales

A) Los datos a la salida son totalmente iguales a la entrada.
B) La pérdida de un dato es problemática.
C) El factor d compresión está limitado a un máximo de 2:1
D) El factor de compresión es variable en el tiempo.

Algunas aplicaciones de la compresión de imágenes requieren que la imagen reconstruida sea sin pérdidas, es decir, numéricamente idéntica a la original sobre una base de pixel-por-pixel. Un ejemplo es en la imagen médica donde al comprimir radiografías digitales con un esquema con pérdidas (y por lo tanto introducir error) puede comprometer la precisión del diagnostico médico. Como se debe de esperar, el precio a pagar por la reconstrucción libre de error es una razón de compresión mucho más baja comparada con la compresión con pérdidas

La eficiencia de la compresion varia para las diferentes tecnicas, pero la eleccion de un planteamiento particular no esta determinado estrictamente por la razon de bits desempeñada Esto es debido a que cada estrategia ofrece ciertas caracteristicas y pretenden la satisfaccion de ciertos requerimientos que deben existir en un ambiento particular, dos tecnicas de compresión sin perdidas para imagenes de tonos continuos son

- La codificacion del plano de bits
- La codificacion predictiva y sin pérdidas

3.11.1.a CODIFICACION DEL PLANO DE BITS

Considerando una imagen de N x N pixeles en la cual cada valor de pixel es representado por k bits. Seleccionando un solo bit desde la misma posición en la representación binaria de cada pixel, una imagen binaria de N x N pixel llamada "un plano de bit" puede ser formada. Por ejemplo, seleccionando el bit más significativo de cada valor de pixel para generar una imagen binaria de N x N, la cual representa el plano de bit *más significativo*. Repitiendo este proceso para otras posiciones de bits, la imagen original puede ser descompuesta dentro de un conjunto de K planos de bit (numerados desde 0 para el plano de bit menos significativo (LSB) hasta k=I para el plano de bit mas significativo (MBS), como se muestra en la figura. Por ejemplo, una imagen con 256 niveles de grises, puede ser considerado como un conjunto de 8 planos de 1- bit. La motivación para esta descomposición es que a cada plano de bit puede ser después codificada eficientemente usando una técnica de compresión sin pérdidas binaria. El método de codificación usado es el de codificación de longitud recorrida (run-lenght-encoding).

Este método de codificación de planos de bit es el mas simple para codificar datos binarios donde las agrupaciones de 0's y 1's ocurren frecuentemente.

Considerando una fuente de datos binarios de quien la salida es codificada como el número de 0's entre dos sucesivos 1's, es decir, la longitud de los dos corrimientos de 0's son codificados. Esto es llamado codificación de longitud recorrida, y es útil cuando grandes cantidades de corrimientos de 0's son esperados. *Una situación como la anterior ocurre en documentos impresos, gráficas, etc., donde la probabilidad de un* cero (representando a un pixel blanco) es cercana a la unidad.

Además, en ciertas aplicaciones el usuario puede desear una aproximación a una baja razón de bit para la imagen original antes de tomar la decisión de escoger un método de compresión sin pérdidas. Puesto que el plano de bit más significativo (correlación vertical) contiene mayor información estructural y son altamente comprensibles

3 11 1 b CODIFICACION PREDICTIVA SIN PERDIDAS

Para imagenes tipicas, los valores de los pixeles adyacentes son altamente correlacionados, es decir, una gran distribución de la información alrededor de un pixel puede ser obtenida por la inspeccion de sus pixeles vecinos. Esta propiedad es explotada en las tecnicas de codificacion predictivas donde se intenta hacer una predicción del valor de un pixel dado sobre los valores previos de los pixeles circundantes La forma de codificacion más común de éste tipo es la " modulación por código de pulsos diferencial (DPCM = diferencial pulse code modulation) y puede ser llevada a cabo en dos formas·

En lugar de considerar todas las estimaciones posibles del píxel dado (x_m) dentro de cada estado, únicamente la estimación más probable es almacenada Esta forma requiere tablas de mejoramiento para cada estado, con estas tablas se provee el valor del pixel previsto (x') que maximiza probabilidades condicionales. La diferencia entre el valor del pixel actual (x_m) y su predicción mas cercana (x'_m) es formada y es llamada la señal diferencial o señal de error e_m· es decir:

$$em = x_m - x'_m$$

Esta técnica requiere el conocimiento de las probabilidades condicionales y también requiere el almacenamiento de tablas de mejoramiento potencialmente grandes. Está técnica es una implementación muy compleja y de requerimientos grandes de almacenamiento

Para sobrellevar estas dificultades, la predicción puede ser formada como una combinación lineal de los valores de pixeles previos De esta manera no se requieren tablas de mejoramiento para estimar el valor mas probable del pixel y tampoco se requiere el conocimiento de las probabilidades condicionales. En general, la predicción lineal es sub-optima comparada con la predicción no lineal que maximiza la probabilidad condicional, pero el mayor número de los casos, esta pérdida pequeña en el desempeño es mas que compensada por la significativa reducción en complejidad y almacenamiento. Esta técnica por tener pérdidas es clasificada como una técnica de compresión con pérdidas.

3.11.2 TECNICAS DE COMPRESION CON PERDIDAS

3.11.2 a CARACTERISTICAS PRICIPALES

A) Los datos a la salida no son totalmente iguales a la entrada

B) Los codecs de este tipo no se usan en computación, solamente en vídeo y audio.

C) Las pérdidas se arreglan para hacerlos menos imperceptibles.

D) Los codecs se basan en la percepción psicoacústica y psicovisual

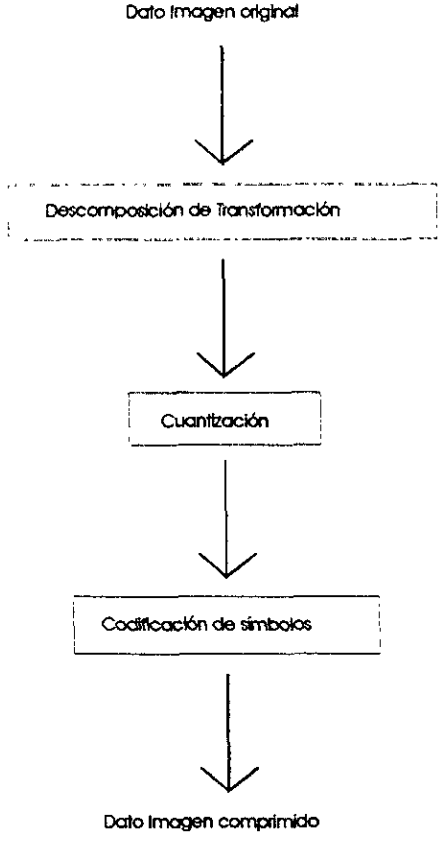
E) No pueden ser puestos en serie en forma indiscriminada sobre todo si son de diferente tipo

F) Operan con una compresión fija ya que deben estar modelados a los sentidos humanos

G) Son mas practicos para transmision y grabacion

H) La única regla es que los errores sean indistinguibles en la imagen final

En esquemas de compresión con perdidas las degradaciones son permitidas en la imagen reconstruida a cambio de una reducida razón de bits comparados con los esquemas sin pérdidas Estas degradaciones pueden o no ser visualmente aparentes y una compresión más grande puede ser llevada a cabo permitiendo más degradación. La trama de trabajo general para un esquema con pérdidas es mostrada en la siguiente figura 3 5



Trama de trabajo de la compresión con pérdidas

FIGURA 3.5

Esta trama de trabajo incluye 3 componentes Descomposicion o transformacion de la imagen, cuantizacion y codificacion simbolica La relativa importancia de cada componente varia de una tecnica a otra y no todos los componentes son necesariamente incluidos en una tecnica particular Como una regla general, lo mas sofisticado en un esquema es, la mejor calidad que puede ser llevada a cabo para una razón de bits dada

La descomposición o transformación de imagen es llevada a cabo para reducir el rango dinámico de la señal para eliminar la información redundante, o en general, proveer una representación que puede ser codificada más eficientemente La siguiente etapa es la de cuantización. El tipo y el grado de cuantización tiene un gran impacto sobre la razón de bits y la calidad del esquema. El proceso de codificación simbólica debe de incluir técnicas como la codificación Huffman, en está técnica, la secuencia generada por la fuente es generalmente dividida en bloques, y a cada bloque le es asignada una palabra clave de longitud variable dependiendo de la probabilidad que cada bloque tenga

En general, algunos de los componentes de un esquema con pérdidas puede ser implementado en un modo adaptivo Un esquema de compresión es adaptivo si la estructura de un componente o sus parámetros cambian localmente dentro de una imagen para tomar ventaja de las variaciones estadisticas. La adaptabilidad ofrece el potencial para mejorar el desempeño a cambio del incremento en complejidad. La adaptabilidad puede ser llevada a cabo en un modo casual o no casual. En sistemas con adaptabilidad causal los parámetros del codificador son basados en los valores de pixel reconstruidos previamente y el proceso de tomar una decisión en el codificador es duplicado en el decodificador. Hay dos desventajas asociadas con estos sistemas. La primera, el codificador puede fallar al adaptar cambios bruscos en las estadisticas de entrada. La segunda, la adaptabilidad causal incrementa la complejidad del codificador y del decodificador. En sistemas con adaptabilidad no causal, los parámetros del codificador son basados en el valor de pixel previo (actual o reconstruido) así como los valores de entrada futuros. Puesto que los últimos no están disponibles en el decodificador, el codificador debe de enviar bits adicionales al decodificador para informarle de las adaptaciones. En este tipo de compresión se hablará de tres técnicas.

- Codificación predictiva con pérdidas
- Codificación por transformación
- Codificación por bloques truncados

3.11 2.b CODIFICACION PREDICTIVA CON PERDIDAS

En un esquema general de codificación predictiva, la correlación entre los valores de pixel vecinos es usada para formar una predicción para cada pixel. La técnica de DPCM es la más común y la más simple de los sistemas de codificación predictivos. En estos sistemas se calcula, a cada instante, una predicción de la

señal de entrada a partir de su pasado y solo se transmite la diferencia entre la señal de entrada y su prediccion La alta correlacion espacial y temporal en las imagenes fisicas y en movimiento nos permite utilizar las muestras vecinas, en el espacio y en el tiempo, para calcular la prediccion de la señal de entrada Si la predicción es correcta la dinamica del error de predicción es inferior a la de la señal de entrada, de donde una reduccion del numero de bits a transmitir Un diagrama a bloques de un sistema básico transmisor y receptor DPCM es mostrado en la figura 3 6

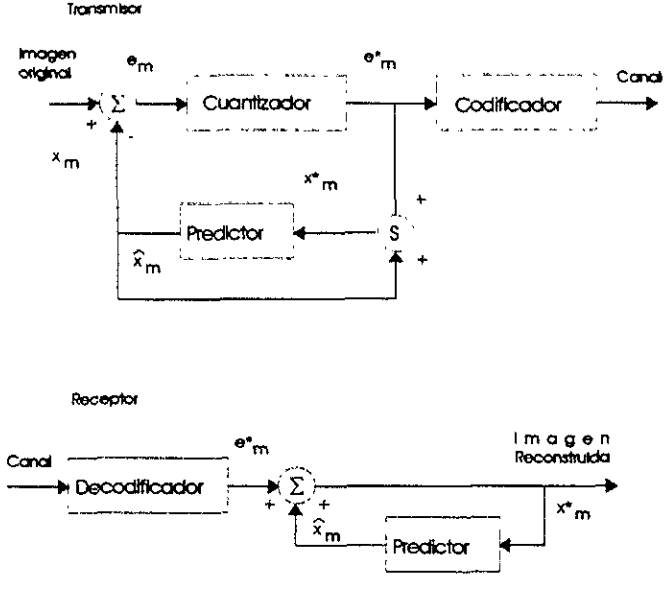


Diagrama a bloques de un DCPM

Figura 3.6.

En la fig. 3 6 Donde e_m es la diferencia obtenida de la ecuación, $e_m = x_m - x'_m$ donde em representa la imagen diferencial cuantizada. Es importante notar que al formar la predicción el receptor tiene únicamente acceso a los valores de pixel reconstruidos. Puesto que la cuantización de la imagen diferencial introduce error, los valores reconstruidos difieren de los valores originales. Para asegurar que predicciones idénticas son formadas en el receptor y el transmisor, el transmisor también basa su predicción en los valores reconstruidos. En esencia Cada transmisor DPCM incluye el receptor en su estructura. El diseño de un sistema DPCM consiste de la optimización del predictor y del cuantizador. Este sistema trabaja con

prediccion lineal, es decir, que para cada muestra de las señal de entrada x_m la prediccion lineal x'_m se construye con las n-1 muestras.

$$x_m = \sum_{i=1}^{n-1} a_i x_{n-1}$$

La predicción utiliza las muestras ya transmitidas (reconstruidas) de manera que el receptor es capas de construir la misma predicción que el emisor los coeficientes del predictor a_i se optimizan de tal manera que e_m tenga varianza mínima. El cuantificador puede ser optimizado con respecto al error de cuantificación o con respecto del SVH. El diseño de un cuntificador optimo, con respecto a un criterio objetivo es posible si se conoce la distribución de probabilidad de los diferentes valores que puede tomar la señal que se desea cuantificar. Los coeficientes ai son calculados utilizando una secuencia de imágenes de prueba al momento de diseñar el sistema de codificación (predicción fija) En general, la utilización de una sola predicción resulta en un sistema de codificación mediocre con respecto a la taza de compresión y a la calidad de las imágenes a causa de la no estacionaridad de las imágenes (contornos, texturas, etc.) para sobrellevar este problema a continuacion se habla del DPCM adaptivo.

Debido a la característica de no estacionaridad de las imágenes, una predicción fija tendrá un desempeño pobre en las regiones donde se producen cambios bruscos El esquema DPCM puede ser hecho adaptivo en términos del predictor o del cuantizador o ambos. La predicción adaptiva usualmente reduce el error de predicción antes de la cuantización, de esta manera para la misma razón de bits, el rango dinámico reducido de la señal de entrada del cuantizador resulta en menos errores de cuantización y una mejor calidad de imagen reconstruida. El la cuantización adaptiva se busca reducir el error de cuantización directamente por la variación de los niveles de decisión y de los niveles reconstruidos de acuerdo a las estadísticas de la imagen.

3 12 CODIFICACION POR TRANSFORMACION

Un esquema general de codificación por transformación envuelve la subdivisión de una imagen dentro de bloques pequeños y la transformación unitaria de cada sub imagen. Una transformada unitaria es una transformación lineal reversible de la cual su núcleo describe un conjunto de funciones básicas discretas ortogonales. El objetivo de la transformación es decorrelacionar la señal original y esta decorrelación generalmente resulta en la señal de energía siendo redistribuida entre un pequeño conjunto de coeficientes de transformación. De esta manera, muchos coeficientes pueden ser descartados después de la cuantización y antes de la codificación. También la compresión visualmente sin pérdida continuamente puede ser llevada a cabo por la incorporación de la función de la sensitividad de contraste del SVH en la cuantización de los coeficientes Un diagrama a bloques de un esquema básico de codificación por transformación es mostrado en

la figura 3 7 Una transformada se dice de una dimension (1-D), si es desarrollada a lo largo de una sola dimensión de una imagen, es decir, a lo largo de una columna de pixeles Una transformada de 1-D desarrollada sobre n pixeles es llamada como transformada de n-puntos Una transformada es de 2-D si es desarrollada sobre un bloque de 2-D de pixeles Todas las transformadas de imagen mencionadas en esta sección son separables, es decir, que el núcleo de la transformada puede ser descompuesto en dos nucleos de 1-D especificando separadamente las operaciones horizontal y vertical. De esta manera una transformada separable sobre un bloque de pixeles puede ser desarrollada en dos pasos, el primero, una transformada de 1-D de n- puntos es desarrollada a lo largo de cada renglón del bloque y después otra transformada de 1-D de n-puntos es desarrollada a lo largo de cada columna.

Hay varias caracteristicas que son deseables en una transformada cuando es usada para el propósito de compresión de imagen.

- Decorrelación de imagen: La transformada ideal decorrelaciona completamente los datos en un bloque; es decir, que empaqueta la mayor cantidad de energia en pocos coeficientes.
- Funciones base de imagen- independiente: Que se debe a las grandes variaciones estadísticas entre las imágenes, la transformada óptima usualmente depende de la imagen. Desafortunadamente la tarea computacional es muy intensiva para encontrar las funciones base. Esto es particularmente un problema si los bloques de imagen son altamente no estacionaria, lo cual necesita el uso de más de un conjunto de funciones base para llevar a cabo una alta decorrelación y por lo tanto una compresión más eficiente.

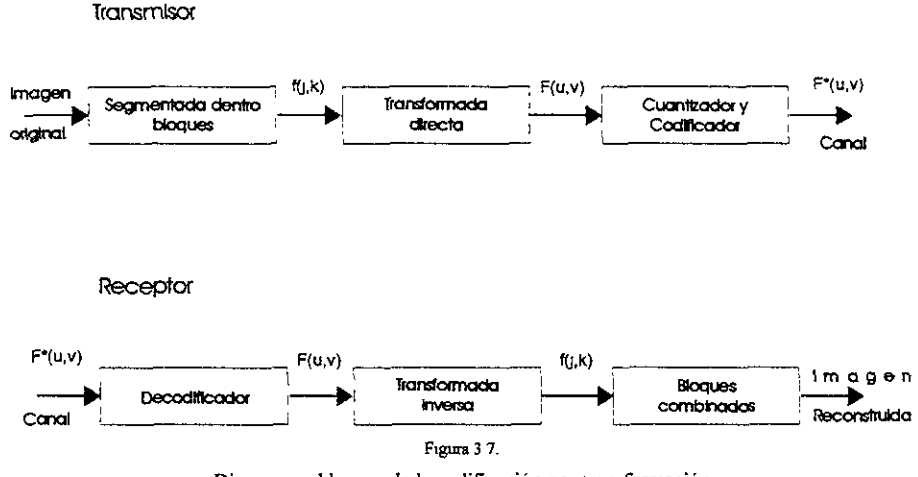


Figura 3 7.

Diagrama a bloques de la codificación por transformación

- Implementacion rapida El numero de operaciones requeridas para una transformada, generalmente es muy grande por lo que se requieren rápidas implementaciones Algunas transformadas tiene estas implementaciones rápidas, tal es el caso de la transformada discreta de Fourier que se puede llevar a cabo por la transformada rapida de Fourier (TRF), la cual reduce el número de operaciones requeridas.

Hay diferentes transformadas de imagen, entre las mas importantes: la transformada Karhunen-Loeve (TKL), la transformada discreta de Fourier (TDF), la transformada discreta de coseno (TDC) y la transformada de Walsh- Hadamard (TWH). A continuación se menciona la TDF por ser la más común de estas transformadas.

La TDF es comúnmente usada para análisis espectral y filtrado. Para un bloque de pixeles, f. La TDF de 2-D directa esta definida como:

$$F(u,v) = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} f(j,k) \exp \frac{2\pi \imath(uj + vk)}{n}$$

y la TDF de 2-D inversa esta definida como:

$$F(j,k) = \frac{1}{n} \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} f(u,v) \exp \frac{2\pi i(uj + vk)}{n}$$

donde y=(-1)1/2 . La TDF esencialmente descompone el bloque de imagen dentro de sus componentes espectrales, y los índices "u" y "v" son llamados las frecuencias espaciales de la transformada. El núcleo de 2-D es separable; es decir,

$$\exp \frac{2\pi i(uj + vk)}{n} = \exp \frac{2\pi iuj}{n} \exp \frac{2\pi ivk}{n}$$

lo cual permite que la transformada de 2-D sea implementada con dos transformadas de 1-D. Extensivos estudios han sido realizados sobre las implementaciones rápidas de la TDF, conocida como la transformada rápida de Fourier, la cual reduce el número de operaciones. En general, los coeficientes de transformación

generados por TDF son complejos, es decir, que estos coeficientes consisten de componentes reales e imaginarios, o componentes de magnitud y de fase, y la manipulación y almacenamiento de estas cantidades complejas pueden ser una desventaja.

3 13 CODIFICACION POR BLOQUES TRUNCADOS

Encodificación por bloques truncados (CBT), una imagen es segmentada dentro de bloques de n x n pixeles (tipicamente 4 x 4) no traslapados y un cuantizador de dos niveles (un bit) que es diseñado independientemente para cada bloque. El umbral del cuantizador y los dos niveles de reconstrucción son variados en respuesta a la estadistica de cada bloque. De está manera, la codificación es esencialmente un proceso de binarización local y la representación de un bloque consiste de un mapa de n x n bits indicando el nivel de reconstrucción asociado con cada pixel, especificando los dos niveles de reconstrucción. La decodificación es un proceso simple de localización de los valores apropiados de reconstrucción en cada locación de pixel y para el mapa de bit Un esquema básico de CBT es mostrado en la siguiente figura 3 8

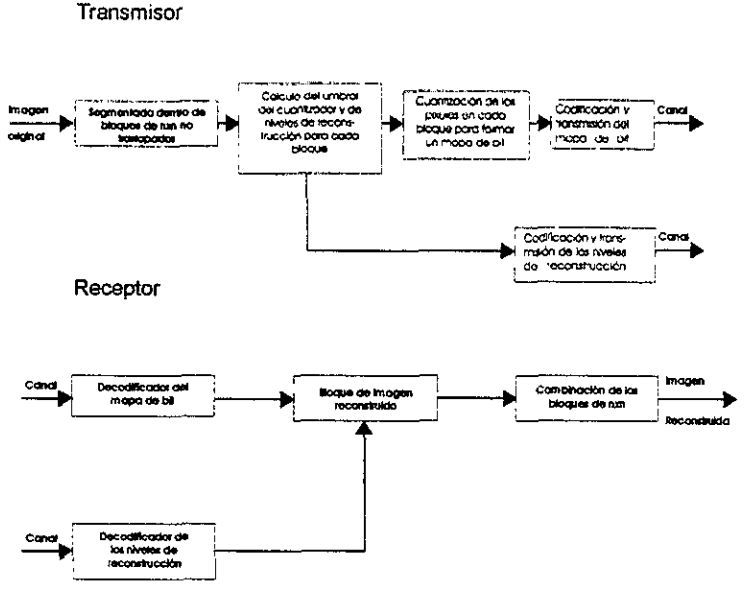


Diagrama a bloques del sistrema CBT

Figura 3.8.

Con un ejemplo de CBT, considere un bloque de 4 x 4 pixeles conteniendo un contorno de ruido diagonal

$$x = \begin{matrix} 146 & 149 & 152 & 156 \\ 97 & 122 & 144 & 147 \\ 89 & 90 & 135 & 145 \\ 85 & 92 & 99 & 120 \end{matrix} \quad \text{a} \qquad B = \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{matrix} \quad \text{b} \qquad x = \begin{matrix} 147 & 147 & 147 & 147 \\ 99 & 99 & 147 & 147 \\ 99 & 99 & 147 & 147 \\ 99 & 99 & 99 & 99 \end{matrix} \quad \text{c}$$

Este ejemplo, el cuantizador se diseña de tal manera que el umbral es la medida de x del bloque entero, y los dos niveles de reconstrucción a y b son las medidas de los segmentos determinados por el umbral. Para este bloque de pixeles x= 123 0, y usando esto como el umbral, el mapa de los bits será el mostrado por el nivel b donde el 1 indica que el valor del pixel actual es más grande que el umbral y el 0 indica que el valor es más bajo que el umbral. Calculando la medida de cada segmento y redondeándolo al número más cercano, encontramos que los dos valores de reconstrucción son: a= 99 y b= 147. Estos valores son transmitidos a lo largo junto con el mapa de bits, y el bloque reconstruido es el que se muestra en el nivel c.

3.14 DIMENSIONES APLICABLES A LA COMPRESION

A) Posición vertical
B) Posición horizontal
C) Magnitud de la muestra (8 bits-10 bits)
D) Tiempo

3 15 CATEGORIA DE LA COMPRESION

A) Codificación interna (intra - code); se hace una sola imagen, en este caso se excluye el tiempo, ya que no se hace referencia a otra imagen.

B) Codificación entre (inter - code); se hace entre imágenes, se pueden obtener grandes factores de compresión ya que una imagen existe solo como datos diferentes de una edición previa.

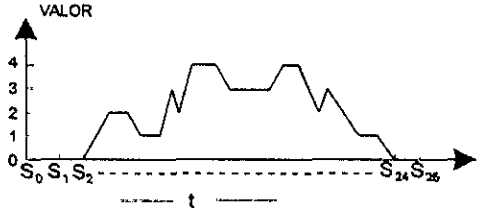
3.16 EL PROCESO DPCM (Modulación por diferencia de pulsos codificados)

Hemos notado que la máxima eficiencia de codificación es determinada por la entropía de la corriente de datos cuando la codificación adecuada es seleccionada.

¿Entonces, como podemos comprimir datos con alta entropía?

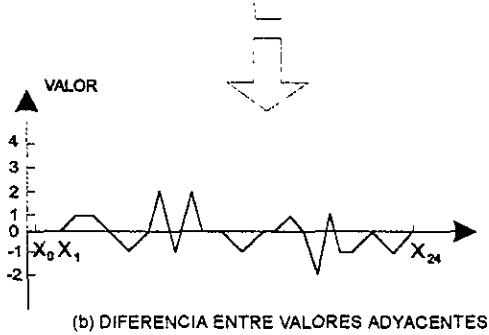
Esto es lo que origina el centro del problema, es paso mas importante de la compresion de datos Naturalmente, se llego a la conclusion de usar un proceso de baja entropia que en la corriente de compresión es llamada codificacion transformada Muchos esquemas de codificacion transformada, son utilizados para disminuir la entropia de la corriente de datos Por lo tanto, a manera de hacer una mejor idea de como hacer disminuir la entropia vale la pena ver las bases de DPCM, un ejemplo tipico de codificación de transformada.

Imaginemos una corriente de datos como la mostrada en la figura que toma 5 valores. En este caso, no podemos codificar la corriente de datos por el número de valores repetidos (el tamaño de la carrera) ya no es una corriente de datos de sus valores y no se repiten los mismos valores para un largo corrimiento. La probabilidad de aparición de cada valor es el mismo como muestra la figura. Esto es que la entropia de estos cinco valores es muy alta.



Valor	Probabilidad
4	5/25
3	5/25
2	5/25
1	5/25
0	5/25

(a) CORRIENTE DE DATOS (S_N)



Valor	Probabilidad
4	11/24
3	6/24
2	4/24
1	2/24
0	1/24

(b) DIFERENCIA ENTRE VALORES ADYACENTES ($X_N = S_N S_{N-1}$)

Reducción de Entropia usando DPCM
(Diferencia Pulse Code Modulation)

Figura 3 9

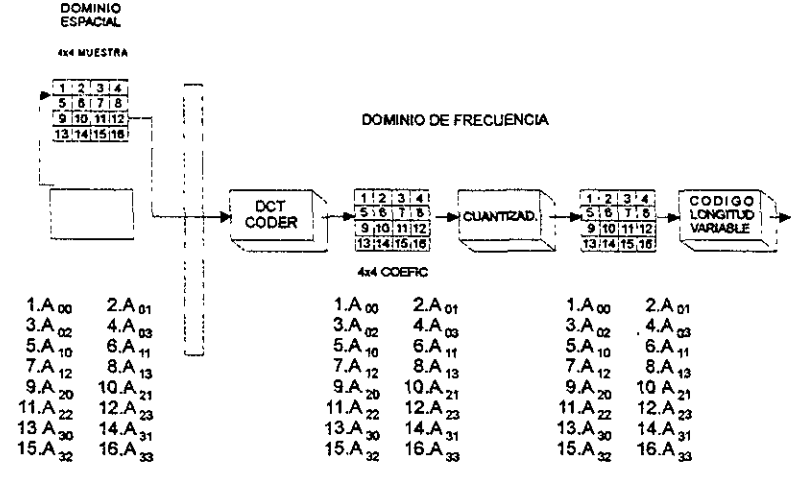
Ahora, regresemos a nuestro objetivo principal, la reduccion de la entropia sabemos que el largo de las curvas estadisticas de la probabilidad de que cada valor ocurra disminuye la entropia En la figura 3 9 (a), podemos ver que no tiene largos cambios entre cada transicion (por simplicidad, asumimos que todas las transiciones están en el rango de -2 a 2), esto nos propone que si substraemos los dos valores adyacentes, el resultado de cada substraccion sera un valor pequeño. Esto esta graficado en la figura 3 9. (b).

Comparado con la corriente de datos original, los 5 valores (-2,-1,0,1,2) ocurren 11 veces el "0", 6 veces el "-1" 4 veces el "1" 2 veces el "2" y 1 vez l "-2". Es obvio que esto es ahora una curva estadistica de la probabilidad de que ocurra cada valor y de que la entropia de la corriente de datos sea reducida. Ahora podemos usar un esquema de codificación eficiente.

GRAFICA REDUCCION DE ENTROPIA

3 17 PROCESO DE CODIFICACION DCT Y REDUCCION DE ENTROPIA

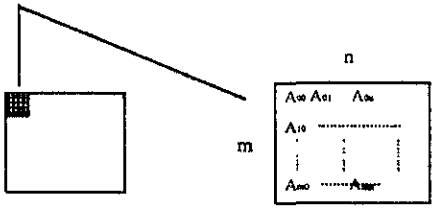
La figura 3.10. muestra los tres procesos más importantes que son usados en el sistema DCT para comprimir datos de video digital.



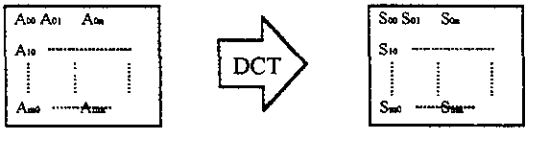
Procesos más importantes utilizados en DCT (Discrete Cosine Transform), para datos de compresión de video

Figura 3 10

La imagen original primero es dividida en una muestra de mx n (horizontal por vertical) bloques como se ve en la fig 3 11 Cada tamaño de bloque de m x n puede ser seleccionado 4 x 4, 4 x 8, 8 x 8, 8 x 16, etc , dependiendo de la aplicacion del sistema que se va a usar Cada muestra de estos bloques, claro son valores digitales, representa la amplitud de la señal de video del pixel correspondiente en el campo El proceso de compresión de datos en el metodo DCT es aplicado a cada uno de estos bloques individualmente. Los bloques de 4 x 4 muestras son transmitidos al codificador DCT, bloque a bloque. Un codigo DCT de dos dimensiones es usado aqui DCT es un proceso de transformacion del dominio del tiempo al dominio de la frecuencia Aplicando este proceso a señales de video digital resulta en agrupar mas de la información en el bloque de muestras original en un coeficiente en el bloque de salida del codificador DCT. Naturalmente, esto es que el nivel de los otros coeficientes pueden ser usualmente pequeños y pueden ser una larga curva estadistica de la probabilidad de aparición de cada nivel para estos coeficientes, resultando una baja entropia para ellos, y en consecuencia, el bloque entero de 4 x 4.



La imagen original es dividida primero en bloques de mxn muestras



Un bloque de mxn muestras es transformando en un bloque de mxn coeficientes

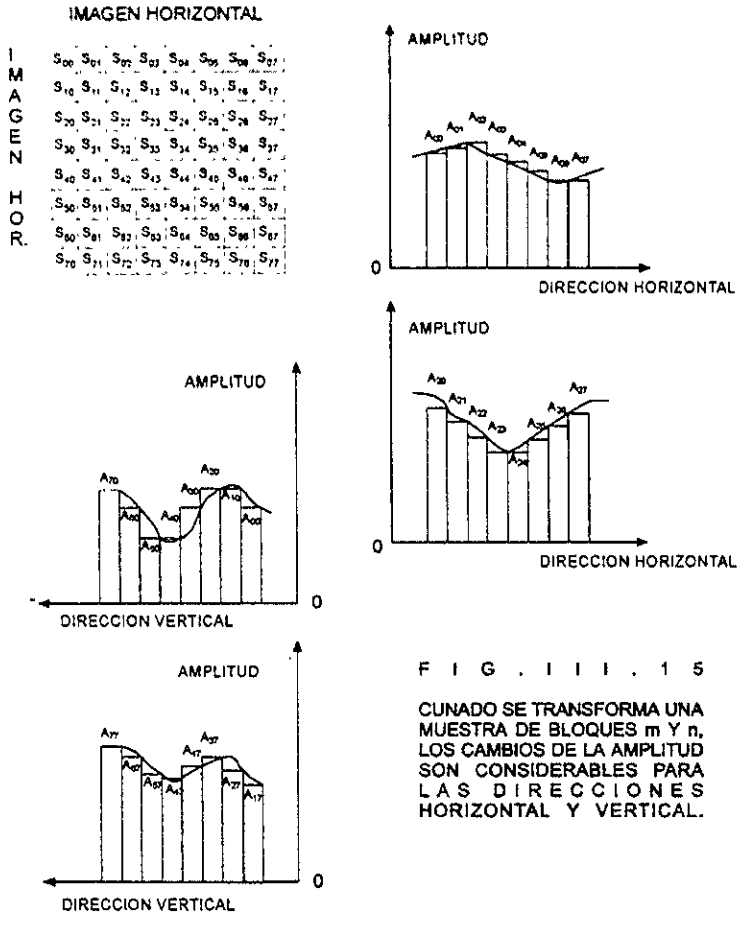
Figura 3.11

Los espectros de baja frecuencia de una señal de video tomen valores desde cero hasta el maximo nivel con casi la misma probabilidad mientras que los espectros de alta frecuencia usualmente toman bajos niveles unicamente, por lo tanto se llego a la conclusion de manejar espectros de baja y alta frecuencia separadamente. Ahora, ¿Cómo podemos hacerlo?

Primero, debemos entender lo que los coeficientes del bloque m x n obtenidos a la salida codificada del DCT representan. En resumen en lugar de representar las muestras m x n por cada una de las amplitudes (A_{mn} en fig. 3 11 a) del bloque original de muestras introducido en el codificador DCT, los coeficientes (S_{mn} fig 3.11.b) en el bloque m x n de coeficientes a la salida del codificador DCT representa como las amplitudes del bloque m x n original cambian a lo largo de las muestras ya sea que cambien gradualmente o abruptamente. Este cambio de amplitudes entre muestras es representado por una expresión de frecuencia y la razón por la que nos referimos a este proceso de transformar el dominio del tiempo al dominio de la frecuencia.

Arreglar para transformar el dominio del tiempo de un bloque m x n al dominio de la frecuencia, dos códigos DCT dimensionales lo cual hace que sea un proceso un poco complejo el usado.

En el actual proceso de compresión, el bloque de muestras (de m x n) puede darnos un valor mayor a 1 a manera de obtener una compresión de la velocidad de transmisión práctica. Esto es que el cambio de amplitud entre muestras debe ser considerado en ambas direcciones (horizontal y vertical) de la imagen (fig. 3.12). En otras palabras, el proceso de DCT debe ser aplicado a ambos espectros representando el cambio de amplitudes a través de las muestras horizontales y a través de las muestras verticales es decir, DCT de dos dimensiones.



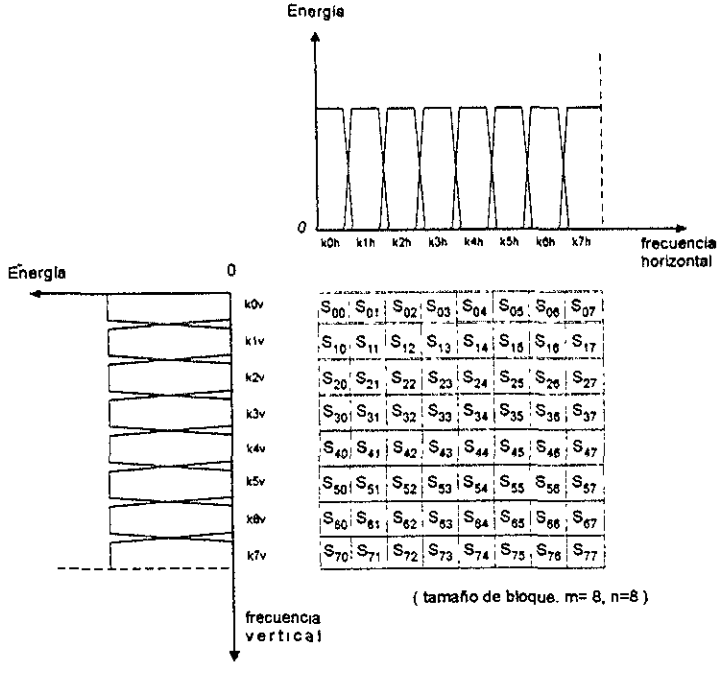
F I G . I I I . 1 5

CUNADO SE TRANSFORMA UNA MUESTRA DE BLOQUES m Y n, LOS CAMBIOS DE LA AMPLITUD SON CONSIDERABLES PARA LAS DIRECCIONES HORIZONTAL Y VERTICAL.

Figura 3.12.

El bloque de coeficientes obtenido a la salida del codificador DCT de dos dimensiones es el mismo tamaño de bloque que el del bloque de muestras a ala entrada del decodificador DCT (fig. 3 12). Si consideramos un bloque de muestras de 8 x 8, el cambio de amplitudes a lo largo de las 8 x 8 muestras en cada dirección horizontal y vertical, es presentado por 8 x 8 coeficientes a la salida del codificador. El codificador DCT bidimencional de 8 x 8 separa el espectro que representa el cambio de amplitud a lo largo de las muestras horizontales en 8 bandas de frecuencia así como también separa el espectro que representa el cambio de amplitud a lo largo de las muestras verticales en 8 bandas de frecuencia. Esto es que el bloque original de muestras es separado en 64 diferentes patrones de frecuencia, es decir, un bloque de 8 x 8 coeficientes.

La fig 3 13 muestras las 8 bandas de frecuencia horizontales y las 8 bandas de frecuencia verticales con respecto a los 8 x 8 coeficientes. ¿Ahora que relacion tiene cada coeficiente S_{mn} con estas bandas de frecuencia? Si consideramos un bloque de muestras bidimencionales es fácil imaginar que cada coeficiente incluyendo S_{00} incluye informacion de como la amplitud de las muestras cambia en la dirección vertical Como la fig 3.13. muestra, el coeficiente S_{00} representa la energia de los espectros de baja frecuencia (esto incluye la banda-de frecuencia k0v) de los cambios de amplitud de las muestras verticales S_{00} representa los cambios de amplitud a lo largo de las 64 muestras entre la banda de frecuencia horizontal k0h y la banda de frecuencia vertical k0v



El codificador DCT bidimensional separa el espectro de dos dimensiones que representa el cambio de amplitud a lo largo de las muestras horizontales y verticales en 64 patrones de frecuancia.

Figura 3.13

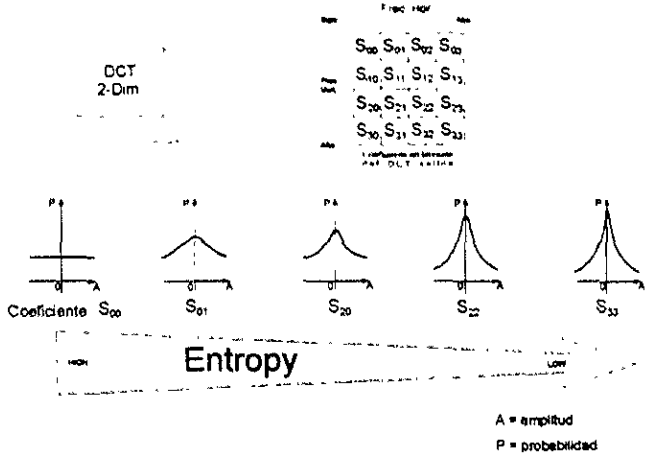
El coeficiente S_{00} es llamado DC. Los demás son llamados AC De la misma manera, el coeficiente a la derecha de AC (S_{01}),por ejemplo, representa la energía de el cambio de amplitud a lo largo de 64 muestras en la banda de frecuencia horizontal k1h y la banda de frecuencia k0v. El coeficiente S_{53} representará la banda de frecuencia horizontal k3h y la banda de frecuencia vertical k5v y así respectivamente.

Asi, como opuesto al coeficiente S_{00}, que representa el espectro de frecuencia horizontal y vertical más bajo, el coeficiente S_{77} representa el espectro mas alto de frecuencia horizontal y vertical de los cambios de amplitud de las 64 muestras

Regresando al objetivo principal, la reduccion de entropia usando codificación DCT El coeficiente DC S_{00} representa el contenido de la imagen que contenga un espectro de frecuencia horizontal y vertical bajo. Moviéndose en y hacia el coeficiente de la esquina inferior derecha del bloque de coeficientes, el coeficiente representa el contenido de imagen que tenga el espectro de frecuencia horizontal y vertical mas alto Aquí es donde la entropia entra en discusión

La fig.3.14. muestra de la entropia de los coeficientes de un bloque de 4 x 4 coeficientes. Como se describe el coeficiente DC tiene alta entropia. Esto es porque el espectro de video de las áreas de baja frecuencia toma valores desde 0 hasta el valor máximo con la misma probabilidad y esto será el coeficiente que represente la energia de estos espectros de baja frecuencia Por otro lado, mientras más nos movamos hacia la esquina inferior derecha del bloque, lo bajo de la entropia viene con el coeficiente de la esquina inferior derecha (S_{33} EN ESTE CASO) que tiene el más bajo. Esto es que puede una curva estadística en la probabilidad de aparición de los niveles que estos coeficientes tomen. Aquí, no debemos olvidar que en DCT bidimensional estamos considerando ambos espectros de frecuencia horizontal y vertical, no el espectro de frecuencia en una dimensión.

Ahora entendemos que el coeficiente más alto es el coeficiente DC, lo pequeño de la entropia del coeficiente. La entropia referida a esto es expresada como la entropia de la probabilidad de que cada valor del coeficiente ocurra fuera de un cierto tiempo. De cualquier modo, en el sistema DCT, más que considerar la entropia de cada coeficiente, es más práctico considerar la entropia del bloque entero no en términos de probabilidad de una función de tiempo pero si por el número de veces que aparece cada valor en la corriente de datos.



Decremento de la entropia respecto a coeficientes de distancia desde el coeficiente de DC (S00), utilizando los coeficientes de entropia S01, S20, S22, S33, (el tamaño de bloque de coeficientes es descrito por m = 4, n = 4)

Figura 3.14.

A manera de hacer esto más fácil de entender abreviamos el proceso de cuantización aquí
Si la entropía del coeficiente DCT es muy grande comparada con la de los coeficientes y procesado separadamente (en la actualidad esto es hecho después de cuantizar) entonces podemos esperar una compresión altamente eficiente para los coeficientes AC.

3 18 COMPRESION MPEG (MOTION PICTURE EXPERT GROUP)

La técnica de compresión de vídeo desarrollada por (MPEG, Grupo de Expertos de Vídeo en Movimiento) proporciona algunas aplicaciones de los sistemas interactivos en CD-ROOM para facilitar la información de vídeo sobre las redes de telecomunicaciones. El algoritmo de compresión de vídeo de MPEG se realiza básicamente en dos técnicas. La primera se refiere a la compensación del movimiento por medio de la reducción de información temporalmente redundante, y la transformación en el dominio de la compresión por medio de la reducción del espacio redundante. En los procesos de la compensación del movimiento son aplicadas dos técnicas básicas, la de predicción y la de interpolación La predicción del error en una señal de vídeo comprimida es más eficaz mediante la reducción de la redundancia espacial (DCT) . La calidad del vídeo comprimido con el algoritmo de MPEG está alrededor de 1.5 Mbps.

El algoritmo del MPEG se realizo tomando en cuenta los estandar a nivel mundial de otros organismos dedicados a la compresion de video Estas consideraciones son de interes, por que pretenden unificar los criterios de compresión de video mediante el comite MPEG.

El formato tipico de video MPEG 352 pix * 240 lineas, 30 cuadros/seg. y es comprimido cerca de 1 2 Mbps , lo que implica que no se puede ser usado en redes menores a esta velocidad y a la capacidad de almacenamiento de datos como ejemplo el protocolo X.25, que requenria de un frame adicional

3.19 ESTANDAR DEL JPEG

Las actividades del Joint Photografic Expert Group, JPEG (Grupo de expertos en video fijo) desempeñan una función importante en los inicios del MPEG, y ambos comités fueron originalmente creados en el mismo grupo de International Standar Organization, ISO (Organización de Estándar Internacionales) y han tenido una considerable participación con miembros de esté grupo Las actividades a las que el JPEG está enfocado son el mejoramiento de las técnicas para el desarrollo de la compresión de las imágenes sin movimiento.

La relación entre las imágenes en movimiento y las imágenes inmóviles es muy estrecha, ya que una imagen activa se forma mediante la secuencia de imágenes fijas, para dar un efecto de movimiento. Sin embargo, hacer una secuencia de imágenes fijas tiene sus desventajas, ya que se tiene demasiada información redundante de un cuadro a otro durante toda la secuencia.

3 20 REQUERIMIENTOS DE MPEG PARA EL VIDEO

El estándar de MPEG es genérico; un medio genérico en el que el estándar es independiente de una aplicación particular.

Las características del algoritmo de la compresión de video se han derivado de lo que se percibe como las aplicaciones de los estándares. Estás caracteristicas son identificadas por orden de importancia para conocer las necesidades de las aplicaciones de MPEG

- Acceso aleatorio
- Búsqueda rápida en adelanto/regreso
- Lector de regreso.
- Sincronización de audio y video
- Retraso en la codificación y decodificación.

3 20 1 ACCESO ALEATORIO

El acceso aleatorio es una caracteristica esencial del medio para el almacenaje de video, en todo caso, el medio es un acceso aleatorio, tal como el disco compacto o un disco magnetico, o un medio secuencial de cintas de memoria. Este acceso aleatorio requiere de una trama de bits de video que sea decifrable en un tiempo limite. Un acceso aleatorio implica la existencia de puntos de acceso, es decir, los segmentos de informacion de codigos únicamente son referencias para ellos mismos. Un acceso aleatorio de uno a dos segundos no debe ser significativo para degradar considerablemente la calidad.

3.20.2 BUSQUEDA RAPIDA EN ADELANTO/REGRESO

Si el medio de almacenaje lo permite, se podria revisar una trama de bits (posiblemente con ayuda de una aplicación especifica de directorio); y usando los puntos especificos de acceso, muestra el video seleccionado para obtener el efecto de un adelanto o regreso rápido. Está es una caracteristica mas que demanda esencialmente una forma de acceso aleatorio.

Sin embargo, una cinta como medio de almacenaje puede proveer un mecanismo para una búsqueda ràpida, mientras que este almacenaje no es apropiado para un acceso aleatorio

3 20.3 LECTOR DE REGRESO

Las posibles aplicaciones interactivas requieren reproducir una señal de vídeo en regreso; mientras que esto no es necesario para todas las aplicaciones para mantener la calidad en el modo en regreso, o tener un modo de regreso constante.

Esta caracteristica está contemplada para que el costo de la memoria no se eleve considerablemente.

3.20.4 SINCRONIZACION DE AUDIO Y VIDEO

La señal de vídeo debe ser exactamente sincronizada con audio asociado. Este proceso debe resincronizarse periódicamente. Estas caracteristicas son adoptadas por el sistema del grupo MPEG, que tiene la tarea de definir las herramientas para la sincronización e integración de múltiples señales de audio y vídeo.

3 20 5 RETRASO EN LA CODIFICACION/DECODIFICACION

En las aplicaciones tales como en videoconferencia , en el sistema debe mantenerse un retraso por debajo de 150 ms, de manera que pueda mantenerse la comunicación.

Por otra parte, se pretende mantener un nivel bajo en el retraso en largas codificaciones; esto es, mantenerlo en el umbral de 1 seg.; y se pretende también que la calidad y el retraso puedan ser cambiados.

El algoritmo deberá ejecutarse por encima del rango aceptable de retraso y será considerado un parámetro

3 21 ALGORITMO DE COMPRESIÓN DE MPEG

El algoritmo de compresión de MPEG logra la compresión en tres etapas, reducción de ancho de banda, una adaptación subjetiva de las pérdidas de compresión y una etapa final de pérdidas de compresión (corrección).

La primera etapa consiste en empalmar primeramente la resolución de la fuente con el rango de disparo de pulsos, y reducir la resolución de la crominancia a una razón subjetiva. La segunda etapa es el algoritmo de compresión por si mismo; retira la redundancia temporal y espacial por medio del análisis de forma de onda y una cuantificación adaptada subjetivamente. La tercera etapa resulta la pérdida de información dentro de una cadena de bits por una forma larga de combinaciones fijas y códigos largos variables

El algoritmo de compresión se realiza básicamente con dos técnicas una, basada en el movimiento compensado de la redundancia temporal; y la otra basada en la DCT (transformada discreta del coseno), basada a su vez en la compresión para la reducción de la redundancia espacial. Las técnicas para la reducción de la redundancia espacial son usadas directamente sobre la fuente de vídeo con tanto éxito como sobre una señal residual después de una predicción temporal.

Las técnicas de predicción temporal con una compensación de movimiento son usadas para explotar la fuerte correlación temporal de las señales de vídeo. La predicción temporal esta dirigida con dos causas: predicción de código y predicción no casual (interpolación de códigos). La permanencia de la señal (predicción de error) está, además, comprimida con la reducción espacial (8 x 8 DCT).

La información relativa para el movimiento está basada sobre 16 x 16 bloques y se transmite junto con la información espacial.

3 21 1 REDUCCION DE LA INFORMACION ESPACIAL

Similarmente, una imagen fija y las señales con prediccion de error tienen una muy alta redundancia espacial. Las técnicas para la reducción de la redundancia usadas para este efecto son muchas, solamente por causa de los bloques basados en la naturaleza del proceso de compensacion del movimiento, las técnicas basadas en bloques son las adecuadas

Las técnicas para ejecutar la compresión del intercuadro con la DCT tienen bases similares en MPEG, JPEG y CCITT H.261 (p x 64) y consiste en tres etapas:

1 Computación de la transformada de coeficientes.

2 Cuantización de la transformada de coeficientes.

3 Conversión de la transformada de coeficientes.

Después, da una reorganización por pares con un rastreo ordenado de datos en zig zag, como se muestra en la siguiente figura. 3 15.

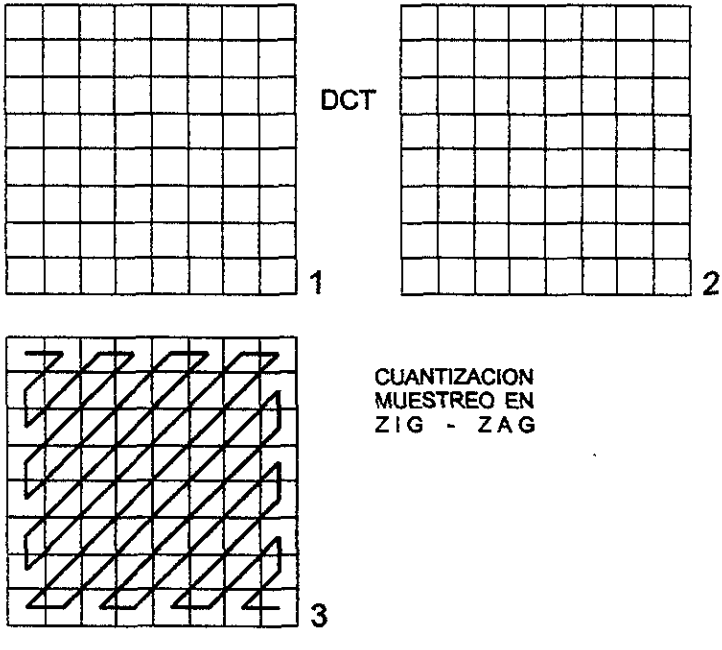


Figura 3 15. TDC

La transformada discreta del coseno (DCT) tiene un umbral de entrada en el rango -225 a 225 porque las señales son usadas con predicción de error y el rendimiento de las señales está en el rango -2048 a 2047 a condicion de que la exactitud sea lo suficientemente buena para fines de cuantizacion

Para efecto de errores redundantes, donde diferentes implementaciones de la transformada inversa están en uso, la exactitud de la transformada inversa es determinada de acuerdo con el estándar especificado por el CCITT H.261.

3 21 2 REDUCCION DE REDUNDANCIA TEMPORAL

La importancia del acceso aleatorio para almacenar vídeo y el significado de la reducción de las tasas de bit consisten en soportar la interpolación del movimiento compensado, donde se consideran tres tipos de cuadro, según MPEG:

1 Entre cuadro (I)

2 Predicción de cuadro (P)

3 Interpolación de cuadro (B para una predicción bidireccional).

El intercuadro provee puntos para un acceso aleatorio, pero solamente con una compensación moderada El código de cuadros con predicción está referido a un cuadro anterior (inter o predecido) y generalmente será usado como una referencia para la futura predicción de cuadros. Los cuadros bidireccionales proporcionan un desarrollo eficiente de la compresión , pero esto requiere de sus referencias: una pasada y una futura para predecir. Los cuadros bidireccionales nunca son usados como referencia. En todos los casos, cuando un cuadro es codificado con respecto a una referencia, el movimiento de compensación es usado para mejorar la eficiencia de codificación. La relación entre los tres cuadros se ilustra a continuación.

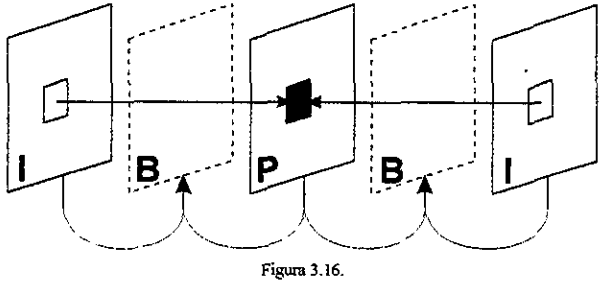


Figura 3.16.

La organizacion de los cuadros en MPEG es discreta y flexible, y dependera de la aplicacion especifica de los parámetros tales como la accesibilidad aleatoria y la codificacion retardada, en la figura se observa que el cuadro es insertado cada 8 cuadros, y el radio de cuadros interpolados para inter o prediccion de cuadros está entre tres y cuatro

3 22 DESEMPEÑO DE LA COMPRESION EN EL MUNDO REAL

La compresión simple es solo codificada y decodificada una sola vez. Para producción y post-produccion, las señales de video pueden ser codificadas, decodificadas y procesadas muchas veces

En aplicaciones de producción y post-producción en el mundo real, los sistemas de compresión usando técnicas de compresión inter-campo/cuadro pueden dar como resultado un aumento al número de problemas.

Cada producción se enfrenta con problemas

Primero, hay una carencia de flexibilidad para encontrar los puntos exactos de entrada y salida de una secuencia de edición. Esta inflexibilidad se eleva debido al uso de la predicción de inter-cuadro, tal es el caso de imágenes P e imágenes B ene sistemas de compresión MPEG. Solamente las imágenes I que son las de más alta calidad son idóneas tanto los puntos de entrada como los de salida, y las imágenes I solo ocurren a intervalos en las secuencias de vídeo que llega.

Una solución posible a este problema sería descomprimir el flujo de bits y realizar operaciones de edición o procesamiento en el dominio incomprimido. Esto, sin embargo, sería como introducir degradaciones en la calidad de la imagen después de compresiones sucesivas y etapas de compresión

Para producción de vídeo, los sistemas de compresión MPEG también crean un nuevo problema. Como definir, en cualquier etapa dada de compresión, que es lo que se espera como imágenes I, pero pudiera ser de hecho imágenes P o imágenes B de generaciones previas. Esto da un aumento a la degradación rápida de la calidad de imagen mientras se incrementan las generaciones de imagen.

3 23 ESCOGIENDO UNA TECNICA DE COMPRESION DE IMAGENES

La pregunta ¿Cual es mejor algoritmo para la compresión? es continuamente hecha en el campo del procesamiento digital de imagen, pero desafortunadamente no hay una respuesta absoluta. La elección de un algoritmo particular para una aplicación dada depende de varios factores Por ejemplo, cundo la compresión es usada en una aplicación de transmisión de imagen, la operación de codificación y de decodificación continuamente necesitan ser desempeñados en tiempo real y la distribución de las implementaciones de

complejidad sensibilidad a errores de canal y requerimientos de areas de almacenamiento para acoplar el rango de salida del codificador al rango del canal llegan a ser importantes En contraste, en las aplicaciones en donde la compresión es usada para reducir los requerimientos de almacenamiento, la operación de codificación continuamente no necesita ser desarrollada en tiempo real. El codificador puede ser completamente complejo puesto que será usado únicamente una sola vez para una imagen dada, mientras que un decodificador simple es deseado puesto que será usado repetidamente. También, las razones de error encontradas en el almacenamiento y aplicaciones de recuperación son tipicamente menores en magnitud que el rango de un canal de comunicaciones

Lo siguiente es una lista de factores que pueden influir en la elección de un algoritmo. En general, el peso de cada factor al tomar una decision es altamente dependiente de la aplicación.

- Sensitividad a tipos de imágenes de entrada: dentro de la clase general imágenes de tonos continuos, las caracteristicas de la imagen de entrada tales como el rango dinámico, ruido de imagen, contenido de frecuencia, correlación de pixel-a-pixel, y la resolución de imagen pueden afectar todo el desempeño y de esta manera la elección de un algoritmo. También algunos esquemas de compresión pueden requerir refinamiento de los parámetros para obtener un buen desempeño con una clase dada de imágenes y este mismo desempeño puede degradarse si otros tipos de imágenes de entrada son permitidos

- Razón de bit operacional: en algunas aplicaciones, la prioridad es llevar a cabo un muy alto grado de compresión nivelado con la baja calidad de imagen. En contraste, otras aplicaciones pueden requerir un alto grado de calidad de imagen que puede ser llevada a cabo por modestas razones de compresión. Tales requerimientos pueden limitar severamente la elección del algoritmo de compresión. En general, para la mayoría de los esquemas de compresión, hay un cierto rango para la razón de bits de salida para el cual el algoritmo es más eficiente. Más allá de este principio hay otros dos aspectos que deben ser considerados

Primero, por su naturaleza, algunos algoritmos no pueden ser operados debajo de una cierta razón de bits, mientras que otros algoritmos son libres de operar a altas razones de bits.

Segundo, algunas aplicaciones requieren un solo algoritmo de compresión para operar a razones de bits variantes o con diferentes grados de calidad. El tales casos es deseable tener la habilidad de optimizar y facilitar la razón de bit para la calidad de imagen reconstruida, por medio del ajuste de los parámetros de compresión.

- Implementación: Esto se refiere a la naturaleza y complejidad de el algoritmo en el ambiento del hardware o software en particular en la cual será implementado. Tres aspectos de un algoritmo necesitan ser considerados. (1) complejidad computacional es decir, el número de adiciones, multiplicaciones,

commientos, comparaciones por pixel y otras aplicaciones requeridas, (2) requerimientos de memoria, y (3) disponibilidad de procesamiento en paralelo u otras estructuras de procesamiento Ambientes con implementaciones tipicas con tecnologia en general incluyendo sistemas basados en PC's, basados en chips DSP (Digital Signal Procesor = Procesador de Señal Digital) y sistemas basados en ASIC (Aplicatton Especific Integrated Circuit = Circuitos Integrados de Aplicacion Especifica). Las caracteristicas de cada tipo de ambiente determinan la compatibilidad de un algoritmo y la velocidad a ala cual podrá operar en su ambiente

- Asimetria del codificador/decodificador Algunas aproximaciones para la compresión resultan en codificadores complejos y codificadores simples, mientras que otras requieren de codificadores de igual complejidad. Mientras que codificadores y decodificadores de igual complejidad pueden ser aceptables en muchas aplicaciones de transmisión, un decodificador simple es más deseable en aplicaciones donde será usado repetidamente tales como en sistemas de almacenamiento de imagen.

- Tolerancia a errores de canal. Desafortunadamente, uno de los preciso pagados por la compresión de datos es el aumento en la sensibilidad de los datos codificados a los errores del canal y el grado de aumento varia entre los diferentes esquemas de compresión.

- Capacidad de transmisión progresiva: La transmisión de imagen progresiva permite a una imagen ser enviada a una razón de bits baja para el rápido reconocimiento y después los detalles restantes de la imagen son transmitidos si es deseado por el usuario.

- Compatibilidad del sistema: Si el sistema requiere compatibilidad con otros productos fabricados, entonces la elección de algún esquema de compresión puede ser dictado por la existencia de estándares que han sido propuestos y/o adoptados. Por ejemplo, los estándares del facsímil del CCITT o el algoritmo de compresión de imagen al color de tonos continuos propuesto por el JPEG.

3.24 APLICACIONES

a) VÍDEO CONFERENCIA

El más completo y avanzado servicio de transmisión de punto a punto o multipunto de voz, datos e imágenes en vivo, para intercomunicar e interactuar a dos o más grupos de personas que se encuentran a grandes distancias entre sí ya sea en el mismo país o en el extranjero.

Gracias a la introduccion en Mexico de la RDSI, nos colocamos a la altura tecnológica de los paises mas avanzados Existen cerca de mil salas en 30 paises distintos, cuentan con la posibilidad de tratar una situacion frente a frente a pesar da las grandes distancias.

Dicho sistema de transmision posee la caracteristica de ser 100 % confidente, lo cual se asegura por medio de un código digital que hace accesible su recepción únicamente en el o los lugares programados.

Beneficios:

- Eleva productividad
- Agiliza la toma de decisiones
- Mejora notablemente la comunicación corporativa
- Reduce costos de viaje y tiempo
- Optimiza el uso de la red digital integrada

Aplicaciones

Las video conferencias son útiles para toda empresa con necesidades de comunicación audiovisual interactiva como

- Instituciones financieras
- Dependencias de gobierno
- Universidades y escuelas
- Cadenas hoteleras
- Consorcios
- Empresas privadas
- Hospitales
- Compañías aseguradoras
- Etc.

Y sus posibilidades no tienen límite:

- Investigación y desarrollo
- Promoción y publicidad
- Actualización
- Manufacturas
- Reclutamiento y selección de personal

- Transferencia de información
- Negociaciones diversas
- Transmisión de operaciones quirúrgicas, seminarios médicos
- Capacitación y entrenamiento
- Juntas regionales
- Revisión de presupuestos
- Conferencias de prensa
- Etc.

El servicio de videoconferencia utiliza un medio de transmisión digital que puede ser fibra óptica, satelite o radio digital y salas debidamente acondicionadas con equipos " CODECS" que codifican y decodifican imágenes; y accesorios tales como cámaras de documentos, videograbadoras, proyectores de transparencias, pizarrones electrónicos, computadoras personales, etc.

b) VIDEO CODEC's

Comparado con la transmisión de voz la transmisión de video requiere de 4 Mhz de BW, o sea 1000 veces más grande que el BW de la señal de telefonía y resulta mucho más costoso. Además de que se requiere un estricto control para minimizar la distorsión de fase y así tener una alta calidad. Por lo tanto, el avance en la tecnología digital hace posible tener circuitos de video de alta calidad y económicos basados en las siguientes razones:

- Para transmisión digital la calidad depende solo del proceso de codificación y decodificación por lo que es independiente del medio y de la longitud de la línea de transmisión. Así, a través
del uso de tecnología digital, es posible tener una buena calidad de transmisión lo cual robustece el canal en contra de distorsión y ruido.
- Una señal de televisión tiene mucha redundancia, entonces, es posible comprimir la información usando ciertos tipos de técnicas de compresión que utilizan procesamiento digital de señales. Esto da lugar a una gran reducción en los costos de transmisión.

Sobre estas bases, se hacen los primeros descubrimientos para equipo de codificación intra-trama e inter-trama y se inicia su comercialización, todo esto para obtener alta calidad aunado a una transmisión económica de la señal de vídeo digital.

Desarrollo

En 1970 se inicio el desarrollo de los CODEC's para la transmision de video digital Desde entonces, se han provisto algunos sistemas de codificacion para reducir los costos de transmision en la industria de la televisión y para sistemas de video conferencias

Se comercializó el VC-2F CODEC en 1978 tambien es conocido como TRIDEC (Tri Parameter Codec or Transmision Rate Reduction Interframe Codec) el cual empieza un metodo de codificacion de diferencia combinacional intertrama para convertir una señal de TV, que involucra pequeños movimientos, una señal digital de segundo orden cuyo valor es de 6 312 Mbps El CODEC VC-2F es el primero en el mundo para la aplicación comercial. Fue usado en una video conferencia entre Tokio y Osaka. Desde entonces, se han hecho considerables desarrollos tanto en la tecnologia como en los algoritmos de codificación; estos desarrollos tienen resultados en la implementación del CODEC VC-6M inter- trama. Recientemente fue desarrollado un CODEC más eficiente, este CODEC inter- trama utiliza técnicas tales como· Reducción de ruido, submuestreo, compensación de movimiento y predicción de fondo; todo esto lo hace capaz de convertir señales de televisión que tengan pequeños movimientos, en una señal digital de primer orden (1.544 Mbps). El CODEC es llamado VC-1.5M.

Para codificar una imagen con movimientos rápidos, tal como TV, el CODEC VC-32M se usa por vez primera entre Tokio y Osaka en el año de 1981. Este convierte la señal de TV a color en una señal digital de 32 064 Mbps que es de tercer orden se uso un simple chip LSI para los convertidores A-D y D-A, un método de muestreo asincrono y una codificación predictiva en una dimensión, y con esto viene a ser más económico que el sistema análogo VSB- 12M. Hablando de ventajas en recientes descubrimientos para tecnologia LSI, el CODEC VC-32M fue también rediseñado para dar mejor funcionamiento y ser más económico.

NUEVA LÍNEA DE CODEC's

VC-32M CODEC

A) Métodos de predicción

Los métodos de codificación para una señal de televisión NTSC son divididos en dos grupos: codificación de componente y codificación compuesta. Con el método antiguo la señal compuesta NTSC es separada en una componente de luminancia y en dos de crominancia antes de la codificación predictiva. En casos mas adelante, no será necesario separar la señal NTSC, por que la codificación se aplicará directamente. Con el método inicial; se puede esperar una buena calidad en una imagen, pero se necesitarían una gran cantidad de circuitos. En el nuevo método, la exactitud de la predicción es mucho menor pero el CODEC es más compacto y más económico Hasta ahora en VC-32M emplea la codificación por componente.

En el metodo de codificacion por componente, las señales compuestas de luminancia y crominancia son previstas por separado y en las cuales se tiene una buena exactitud de la prediccion NTT desarrolló un diseño LSI para la separacion de color por medio de procesamiento digital de señales, el cual proporciona una buena separación de las componentes y estabilidad

B) Selección de velocidad de muestreo

Ya que la banda de frecuencia para una señal NTSC es de 4 Mhz, la velocidad de muestreo fs debe de ser 6 4 Mhz. También , si fs es muy alto el promedio de la longitud de la palabra asignada por muestra tiene que ser como para mantener la velocidad de transmisión por debajo de cierto valor. Esto significa que el número de niveles de cuantización, seria reducido y por lo tanto la longitud de palabra es pequeña, es entonces cuando hace dificil obtener una buena calidad en la imagen.

Como 32 Mbps fue seleccionado como la velocidad de transmisión en una codificación compuesta, 3 fsc (fsc es la frecuencia de la subportadora de color) puede ser considerado como el valor superior de velocidad de muestreo En contraste, en la codificación por componente, se puede usar una alta frecuencia de muestreo, por que es posible ejecutar predicciones más exactas. Por lo tanto, la sincronización de frecuencia entre fs y fsc es requerida para usar procesamiento digital de señales en la separación de color. Por esta razón, una velocidad de muestreo de 4 fsc puede ser seleccionada.

En la entrada, la señal compuesta de TV es muestreada a una razón de 4 fsc dentro de un código de 8 bits PCM. Desde esté código PCM las componentes de luminancia y crominancia son separadas. El circuito de separación de color está compuesto de filtros digitales pasabanda y un filtro combinador usando una línea de memoria como retardo de línea La componente de la señal entra al circuito predictor, el valor de predicción es substraído al valor actual, y entonces la diferencia es transmitida.

C) Cuantificación y funcionamiento del codificador de longitud variable

Tomando en consideración las características del SVH, es posible reducir el número de niveles de cuantificación usando un método no lineal. Esto también es posible al reducir la longitud promedio de la palabra de código para cada muestra utilizando una codificación de longitud variable auxiliándonos de la desviación de la función de distribución de diferencia combinacional (estadística). Debido a la naturaleza variable de la salida de información, es posible que el buffer de memoria tenga desbordamientos o este vacío. Por lo tanto, varios tipos de cuantización y tablas de código que tengan diferentes longitudes de código son separadas y remplazadas de acuerdo a la ocupación del buffer de memoria.

D) Proteccion contra error de canal

En este metodo de codificación predictiva, si la información de control de la codificacion desaparece durante la transmisión, ocurre una propagación de error y se afecta mucho la calidad de imagen Para esto se ha adoptado una protección contra el error de canal y así evitar la destruccion de informacion.

1) Linea de reposición (RESET)

Al recetear un valor integrado dentro de un loop de codificación/decodificacion predictiva sobre una base línea por linea, y usando una integración filtrada como la función de predicción, el efecto del error de canal esta grandemente decrementado y limitado a unas cuantas lineas.

2) Transmitiendo datos, reportando el número de muestras y modos de cuantización

El efecto de decodificación falsa es disminuido al transmitir el número de muestras para la línea previa y así como el modo de cuantización de la linea, además se está asegurando que existe una correspondencia entre estos parámetros tanto para el Tx como para el Rx.

E) Transmisión de voz

El VC-32M CODEC puede transmitir no solo una señal de video sino también una señal de voz, para dos canales, con BW máximo de 15 Khz. La señal de voz es muestreada a una velocidad de 32 Khz y codificada en 14 bits de PCM no -lineal, este código es convertido a 11 bits de PCM lineal más un bit de paridad Es entonces cuando la señal codificada se transmite.

F) Interfaz digital para conexión D/D

El un caso donde el VC-32M este conectado a otro sistema de transmisión de vídeo digital, una interfaz digital puede ser provista para remplazar un panel. Esto hará posible que se puedan conseguir redes para vídeo conferencia a bajo precio.

CODEC VC-1.5M

A) Método de predicción

El método de codificación diferencial combinacional fue seleccionado para poner en uso comercial; este método transmite una sela de TV, que tenga pocos movimientos (por ejemplo una vídeo conferencia), como una señal digital de segundo orden, es decir, 6 312 Mbps.

Sin embargo, fue necesario promover un sistema mas economico para el uso practico de los servicios de video conferencia. Asi entonces se desarrollo un nuevo CODEC el cual puede transmitir señales de video a 1 544 *Mbps Este CODEC tiene tecnicas adicionales para la reduccion de informacion, compensacion* de movimiento y prediccion de fondo ademas de las funciones tradicionales del CODEC intertrama Estas técnicas incrementan eficientemente la predicción y decrementan el volumen de la información que tiene que ser transmitida.

B) Selección de la velocidad de muestreo.

La velocidad del muestreo puede ser seleccionado considerando los siguiente factores:

1) Con el fin de reducir la información generada por la codificación es preferible escoger la más baja velocidad de muestreo posible.

2) La predicción intertrama directa no puede predecir exactamente la amplitud de la señal de crominancia, esto por que la señal de la subportadora de color en la señal NTSC invierte la fase para cada trama de video.

Desde el punto de vista estabilidad y realización, así como para diseño y producción sencilla el esquema de filtro digital es superior al de un analógico. Para el esquema del filtro digital es necesario seleccionar una velocidad de muestreo muy particular, la cual esta asociada con fsc en una relación como 4 fsc, 3 fsc ó 12/5 fsc.

C) Codificación por submuestra

En la codificación intertrama dos técnicas adicionales son introducidas para la reducción de información sin causar ninguna degradación de la calidad de la imagen. La primera es un método de *codificación por submuestra y la segunda es una repetición del campo o método de submuestreo.*

En el método de submuestreo, las muestras son codificadas en forma alterna y ya teniendo estas se ordena en forma de hileras Por el lado del receptor, el código es interpolado y las señales son reproducidas con exactitud

D) Codificación de longitud variable

Tal como la distribución de la señal de predicción de error tiene una clara desviación, es posible reducir la longitud promedio de la palabra de código y así disminuir el número de niveles de cuantización por medio de codificación de longitud variable y cuantificación no lineal.

E) Protección contra error de canal

En codificación intertrama, los errores de canal causan una degradacion muy alta, ya que son decodificados errores que se propagan a traves de las tramas Por lo tanto, los siguientes dos metodos son *empleados para prevenir errores de canal*

1) Códigos de corrección de error

El código BCH se presenta como detector y corrector de errores. Aún, si la taza de error está arriba de 10^{-6}, el código BCH puede mejorarlo a 10^{-10}.

2) Refrescar (Refreshing)

Cuando la taza del error de canal excede un cierto valor de umbral, el código de corrección de error no funciona entonces ocurre una degradación. Al demandar una restauración en la parte del receptor se detectan errores de canal por medio de los bits de paridad (b bits/trama) esto sucede entre la memoria de trama enviada y la memoria de trama recibida. Cuando los errores son detectados, una señal de detección de error es enviada desde el decodificador hasta el codificador a través del canal de regreso, y las señales que se están enviando se recetean, además la señal de confirmación se envía de regreso al codificador.

F) *Método de codificación de voz*

Esté sistema de codificación intertrama fue diseñado para una transmisión simultánea de señales de TV a color NTSC y su correspondiente señal de audio de 7 Khz de BW.

La señal de audio de una vídeo conferencia son codificadas por sub-banda de ADPCM y transmitida a una razón de 64 Kbps.

LSI's para los CODEC's

Una forma efectiva de hacer más económico un CODEC para vídeo es introducir tecnologia LSI (Large Escale Integration). De hecho, si el CODEC esta en un solo integrado su efectividad es muy alta Sin embargo, esto puede no ser posible desde el punto de vista de la escala del circuito Hasta este momento se han desarrollado LSI's para cada bloque funcional, todo esto como primer paso para fabricar un solo circuito integrado.

1) Convertidores A/D y D/A en LSI

Como la señal de TV tiene mas de 4 Mhz de BW es necesario tener una velocidad de muestreo de 10 Mhz para el convertidor A/D, si se quiere implementar este convertidor con componentes discretos el costo seria muy alto y los acoplamientos no serian tan perfectos como un solo CI

c) SCIENTIFIC ATLANTA

El sistema compresor de video puede ser compatible con los sistemas en uso de una red de estaciones terrenas; puede ser utilizado tanto en comunicaciones via satélite, en fibra óptica o en cable coaxial. Una caracteristica propia del equipo, es la de multiplexar señales de video, audio y datos, además de reservar un canal para el envio de señales de protocolos de contról Nuestro sistema compresor permite, por tanto, la transmisión de datos, audio, video y teletexto via terrestre o por medio de un enlace satelital para obtener una cadena de múltiples puntos receptores/ transmisores (dependiendo de las necesidades de la cadena de transmisión). Con base en lo anterior, podemos definir a este sistema como una opcion para bajar costos e incrementar la eficiencia de transmisión de señales de un mismo transpondedor (canal satelital).

Scientific Atlanta tiene designado su propio sistema de compresión digital con una multiplexión básica de 25.5 Mbps como envolvente de video, audio, sincronización, acceso condicional, adelanto de corrección de error, otras herramientas y utileria en la cadena de datos. Este multiplexor será portador de HDTV, varios niveles de video NTSC y numerosos canales de video NTSC y audio con calidad de disco compacto.

Este equipo de compresión reúne las normas estandarizadas PAL - M (525 líneas), PAL - B, PAL - G, PAL - H, PAL - Y (625 líneas) y NTSC y ofrece aspectos tales como una calidad disco compacto en audio y un acceso controlado y seguro.

Por varios años, las técnicas de compresión de vídeo han sido objeto de interés, tanto de EU como de otros países. Hasta hace dos años, sin embargo, el desarrollo se concretaba a dos canales de transmisión de video en una muy baja transmisión de datos con un rango de 56 / 64 Kbps a 1.544 / 2.048 Mbps. Esta tecnología fue aceptada para radio - transmisores y producción de videos que requieran de poco movimiento.

Hoy día la tecnología de Scientific Atlanta para la compresión de vídeo hace una transmisión digital full motion.

La compresión de vídeo está generando una enorme cantidad de programas y negocios de televisión profesional en EU Esto realmente se da en el mercado internacional, donde la competencia de la tecnología

ha llegado a ser crítica En algunas partes del mundo el uso adicional del transpondedor no es posible, por que no existen canales disponibles

Alternativas para el uso del sistema.

Con la tecnología del equipo de compresión digital de video que posee Scientific Atlanta, es posible trabajar con 10 señales por BW de 36 Mhz en un transpondedor satelital, con lo que es posible ahorrar en espacio y costos al momento de rentar los servicios de un satelite

También se tiene capacidad de enviar diferentes señales de diferentes puntos geográficos a un mismo satélite y transpondedor, lo cual reduce la necesidad de solicitar los servicios de un espacio satelital, y es posible enviar alguna señal desde otro punto distinto al de la estación terrena fija.

La FDM (Multiplexaje por División de Frecuencia) es la técnica satelital que hace posible la transmisión desde diferente puntos por canales separados, aun en el mismo satélite y transpondedor. La TDM, sin embargo, hace posible que la transmisión de las señales sea desde un mismo punto geográfico y dirigido hacia un mismo satélite y transpondedor, haciendo más efectiva la transmisión, y dando más capacidad al sistema; en otras palabras, hace mas controlable la transmisión

d) EL SISTEMA CODIFICADOR

Este sistema codificador, desarrollado por la empresa Scientific Atlanta incluye un codificador de audio / video y un multiplexor, así como la parte referente al programa de codificación y digitalización de las señales Este sistema compresor se puede implementar en un sistema ya establecido de las normas NTSC o PAL.

Posee un sistema interno de autoajuste de la trama o tramas de datos, lo que permite que la señal a transmitir sea de una alta calidad en video y audio

El sistema de multiplexión recibe una señal digital de audio y video proveniente del codificador, esta señal tiene una calidad de disco compacto en audio y en video de alta resolución.

De la salida del sistema de multiplexión se envía la señal a un sistema modulador digital que se encarga de enviar la señal al satélite. Este equipo ofrece dos formas para la transmisión satelital·

- La multiplexión por división de tiempo (TDM), por medio del cual se pueden incorporar hasta 10 señales de video y 40 señales de audio con calidad de disco compacto.

- La multiplexion por división de frecuencia (FDM), por medio de la cual se puede incorporar una señal de vídeo y 4 señales de audio

CARACTERÍSTICAS GENERALES

- Compatible para los sistemas con normas NTSC o PAL - M (525 líneas) o PAL - B/G/H/I/N (625 líneas).
- Modulador RF con entrada y salida de señal de TV.
- Vídeo y audio (canal estéreo) en banda base.

Especificaciones de algunos modelos:

- *Modelo D9101 (con norma de MPEG)*
- Señal insertada en la línea 21 con un campo y una sola entrada por canal
- Señal de salida normalizada con MPEG
- Modelo D9170 (modulador QPSK)
- *Dos entradas multiplexadas (A y B) con 21.5 Mbps cada una.*
- Velocidad de transmisión de 49.2 Mbps
- Aplicación de la modulación QPSK con un factor de corrección de error de 7/8

e) VÍDEO CODEC VT34A3 DE
ABL ENGINEERING, INC.

El ABL es un codificador integrado de 109 bits de resolución para servicios de transmisión de vídeo, audio y corrientes de datos. Opera a una razón de 34 Mbps (34.368 Mbps) y tiene la capacidad de transmitir simultáneamente señales de vídeo en formato NTSC (525 líneas a 4.5 Mhz) o señales en formato PAL - B (625 líneas a 5.5 Mhz), además de un canal de datos de 2,048 Mbps.

La corriente de datos de 2,048 Mbps puede acarrear señales de audio digitales (dos audios) o datos digitales, contiene interfaces para vídeo programas y señales de teletexto independientes.

En su estructura, el equipo se compone de:

- Detector de fase y cuadratura
- Sincronizador de base de tiempo
- Convertidor A/D de vídeo
- Modulador diferencial de pulso codificado
- Codificador de palabra variable
- Transmisor multiplexor de corrección de error FEC

- Convertidor A/ D de audio

Este equipo emplea la tecnica de compresion digital de longitud de palabra variable

La señal de video analógico (PAL - B o NTSC) primero se digitaliza a una resolucion de 10 bits La señal se filtra analógica y digitalmente, antes y después de la conversión A / D , en pasabajo, con el propósito de suprimir las componentes mayores a 4.3 Mhz. La selección entre las señales PAL o NTSC se realiza por medio de un interruptor en el codificador, el cual se pondrá en el formato de la señal apropiada

El segundo estado del video codificador es la modulación diferencial de pulso codificado y la selección de la cuantización estadística. El sistema emplea diferentes coeficientes de predicción tanto para el formato NTSC como para el PAL, pero ambos usan muestras de campos previos y campos presentes, con el fin de soportar cambios bruscos en la información del video; por ejemplo, movimientos rápidos de escena

Las cuantizaciones estadísticas usadas son de 3, 5 y 7 bits de salida (longitud de palabra)

La selección de cuantización es el tercer estado del codificador, y depende de la cantidad de información contenida en la memoria de 2.048 Mbytes. Cuando la memoria tiene en 1 Kbyte y 255 Kbytes libres, la palabra y cuantización es de 5 bits; si la memoria tiene por arriba de 255 Kbytes libres, la palabra y cuantización cambia ahora a 3 bits y, por último si la capacidad de memoria es menor de 1 Kbyte, la palabra y cuantización es ahora de 7 bits; esto depende del tamaño de la información generada por la DPCM comparada con PCM.

En la figura 3 17 se puede observar el diagrama a bloques del decodificador ABL VT34A3

La señal de video codificada es entonces suministrada al circuito de corrección de error (FEC) y al multiplexor. La FEC es sincronizada por el sistema multiplexor a una razón de 34 Mbps; el multiplexor multiplexa la información de video, el canal auxiliar de datos y el teletexto. El canal auxiliar de datos puede ser reemplazado por dos módulos conversores de audio de 15 Khz, para tener un sonido estéreo para un canal de TV transmitidos simultáneamente con el vídeo.

Especificaciones.

Vídeo

- Impedancia de entrada: 75 ohms
- nivel de entrada: 1 Vpp
- Relación S / N: >60 dB
- Diferencia de fase < 3 grados

- Ganancia diferencial < 3 %
- Retraso croma / luminancia < 20 nS

Respuesta en frecuencia +/- 0 5 dB de 20 hz a 4 5 Mhz

Audio

- Respuesta en frecuencia: 20 Hz a 15 Khz
- Nivel de entrada: + 0 dBm nominal a +21 dB máximo
- Distorsión: 0.2 %; 1 Khz a 0 dBm

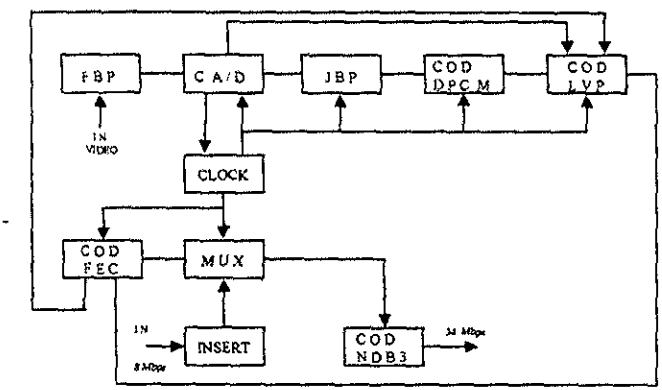


Figura 3.17

Interfase de datos 2.048 Mbps

- Razón de bits: 2 048 Mbps
- Impedancia: 75 Ohms
- Formato: HDB3

Modulación

- Razón de bits. 34 368 Mbps +/- 20 ppm
- Formato: HDB3
- Impedancia: 75 ohms
- Eb/No: $1x10^{-5}$

CAPITULO 4

SEGURIDAD EN LA TRANSMISION DE VIDEO

4.1 MODELOS, OBJETIVOS Y SISTEMAS DE CODIFICACIÓN

Modelo del proceso de encriptamiento y decriptamiento

El deseo de comunicarse de una manera privada a sido la intención del hombre desde tiempos remotos.

Por tanto, el estudio de técnicas para distinguir mensajes así como para advertir de intercepciones no autorizadas es llamado criptografia. Los términos encipher (encodificación) y encriptación se refiere a la transformación del mensaje llevada a cabo en el transmisor y en términos de decipher (decodificación) y decrypt (decriptamiento) se refiere a la transformación inversa llevada a cabo en el receptor.

Las dos razones primarias para el uso de criptosistemas en comunicaciones son: privacidad, para prevenir de personas no autorizadas de la extracción de información del canal; y autenticación, para evitar a personas no autorizadas de la inserción de información dentro del canal. Algunas veces como en el caso de la transferencia electrónica de fondos o contratos y negociaciones es importante prevenir la equivalencia electrónica de una firma escrita en orden de evitar o aclarar alguna disputa entre el transmisor y el receptor, así como el mensaje si es que alguno fue enviado

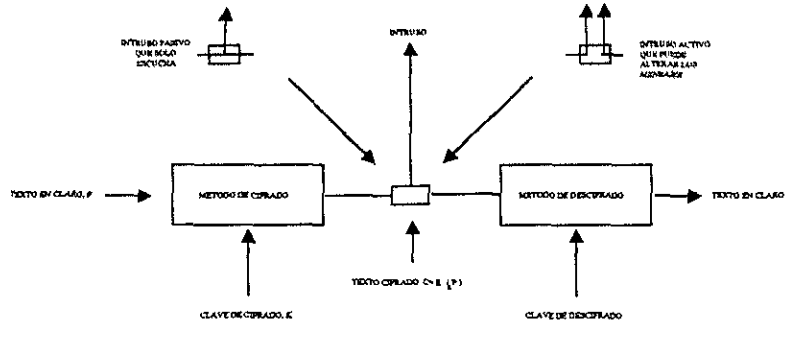
Históricamente cuatro clases de individuos han utilizado y han contribuido, de una manera importante, en el arte de la criptografia: los militares, los cuerpos diplomáticos, las personas que llevan un diario etc. De todos estos el grupo de los militares es el que ha tenido el papel más importante y el que ha limpiado el camino Dentro de las organizaciones militares, los mensajes que se ha necesitado poner en clave, han sido asignados tradicionalmente a empleados, encargados de efectuar dicho trabajo y de transmitir los mensajes. El escaso volumen de mensajes a transmitir ha impedido que este tipo de trabajo se le haya encargado a una élite de especialistas.

Hasta el advenimiento de los ordenadores una de las principales restricciones de la criptografia era la falta de habilidad de los codificadores para efectuar las transformaciones necesarias, con frecuencia en el campo de batalla y contando con poco equipo. Una restricción adicional, ha sido la dificultad para conmutar rápidamente de un método criptográfico a otro, dado que esto obligaría a reciclar a un gran número de personas. Sin embargo, el peligro que existe de que un codificador sea secuestrado por el enemigo, ha hecho

esencial tener la capacidad de cambiar instantaneamente de metodo criptografico, cuando sea necesario Estos requisitos conflictivos han propiciado la generación del modelo que se representa en la figura 4 1

Los mensajes que se tienen que poner en clave, conocidos como texto claro, se transforman mediante una función que esta parametrizada mediante una clave La salida del proceso de puesta en clave, conocido como texto cifrado o criptograma, es entonces transmitida, muy frecuentemente por medio de un mensajero o por radio.

Se supone que el enemigo, o sea el intruso, escucha y copia cuidadosamente el texto cifrado completo. Sin embargo, a diferencia del receptor asignado, el intruso no conoce la clave y , por lo tanto, no puede descifrar con facilidad dicho texto. En algunas ocasiones el intruso no solo escucha la comunicación que se hace a través del canal (intruso pasivo), sino también puede registrar los mensajes y repetirlos posteriormente, incluir sus propios mensajes, o bien, modificar los mensajes originales antes de que lleguen al receptor (caso de un intruso activo). El arte de quebrar el cifrado se le conoce como criptoanálisis. El arte de inventar cifras (criptografia) y desbaratarlas (criptoanálisis) se le conoce colectivamente, como criptologia.



EL MODELO DE PUESTA EN CLAVE

Figura 4.1.

Una regla fundamental en criptografia es que, uno debe suponer que el criptoanalista conoce el método general utilizado para el cifrado. En otras palabras, que el criptoanalista conoce la forma como trabaja el método de cifrado de la figura 4.1. La cantidad de esfuerzo necesario para inventar, probar e instalar un nuevo método cada vez que el antiguo método está, o se piensa que puede estar comprometido, ha hecho siempre impractico el tratar de mantenerlo en secreto y, pensar que es un secreto cundo realmente ya no lo es, causa más daño que beneficio.

Aquí es, precisamente, el lugar en el cual aparece el papel relevante de la clave, la cual consiste (por lo general) en una cadena corta de caracteres que selecciona uno de los tantos cifrados potenciales A diferencia del método general que solamente puede cambiarse cada cierto número de años, la clave se puede cambiar tan a menudo como sea necesario Así, el modelo básico es un método general estable y públicamente conocido, parametrizado mediante una clave secreta que puede cambiarse fácilmente.

Desde el punto de vista de los criptoanalistas el problema del criptoanálisis tiene tres variantes. Cuando tiene una cantidad de texto cifrado y nada de texto en claro, el criptoanalista se ve confrontado con el problema de tener solo texto cifrado Los criptogramas que aparecen en la sección de acertijos de los periódicos, plantean precisamente este tipo de problemas. Cuando se tiene un texto cifrado y un texto en claro confrontados, al problema se le conoce como el problema de texto en claro conocido. Por último, cuando el criptoanalista tiene la habilidad para poner en clave las partes de texto en claro que se desee, se tiene el problema de texto en claro seleccionado. Los criptogramas de los periódicos podrían desbaratarse trivialmente si al los criptoanalistas se les permitiera hacer preguntas como la siguiente:

¿Cuál es el cifrado de ABCDE ?

Los principiantes en el medio criptográfico suponen frecuentemente que si un cifrado puede resistir a un ataque basado sólo en texto cifrado entonces es seguro.

Esta suposición es bastante ingenua. Los criptoanalistas, en muchas ocasiones, pueden adivinar algunas partes de texto en claro. Por ejemplo, lo primero que muchos sistemas de tiempo compartido pueden contestar cuando se les llama es "PLEASE LOGIN" El trabajo de los criptoanalistas llega a ser mucho más sencillo cuando están equipados con algunos juegos de texto en claro y texto cifrado confrontados Para lograr toda la seguridad el criptógrafo deberá ser conservador y estar seguro de que el sistema no se puede desbaratar incluso cuando su oponente sea capaz de poner en clave cantidades arbitrarias de texto en claro seleccionado.

Históricamente, los métodos de cifrado han sido divididos en dos categorías:
Cifradores de substitución (incluyendo los códigos) y cifradores de transposición

Cifradores de substitución.

En un cifrador de substitución, cada letra o grupo de letras se substituye por otra letra o grupo de letras para descifrarlas. El cifrado más antiguo que se conoce es el cifrado de Cesar, atribuido a Julio Cesar. En este método, *a* se representa por D, *b* se representa por E , *c* se representa por F, ..., y *z* se representa por

C Por ejemplo, ataque se representa por DWDTXHQ En los ejemplos, los textos claro se representaran con letras minúsculas, mientras que los textos cifrados utilizaran letras mayusculas En el texto, los dos tipos se representaran por medio de letras italicas

Una sencilla generalizacion del cifrador de Cesar permite que el alfabeto cifrado se pueda desplazar k letras, en lugar de que siempre sean tres. En este caso, k se convierte en una clave para el método general de *alfabetos desplazados circularmente. El cifrador de Cesar pudo haber engañado a los cartagineses, pero desde* entonces no lo ha hecho con nadie más

La siguiente mejora consiste en tener cada uno de los símbolos de texto en claro, digamos las 26 letras por simplicidad correlacionadas con alguna otra letra por ejemplo,

Texto en claro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Texto cifrado : Q W E R T Y U Y O P A S D F G H J K L Z X C V B N M

A este sistema general se le conoce como substitución monoalfabética, en donde la clave está constituida por la cadena de 26 letras correspondiente al alfabeto completo. Para está clave en particular, la *palabra ataque apareceria como: QZQJXTF.*

A primera vista esto podria parecer un sistema seguro por que, aún cuando el criptoanalista conozca el sistema general (es decir la substitución letra por letra), no conoce cual de las 26! = 4 * 10^{26} posibles claves esta empleándose A diferencia del cifrador de Cesar, probar todas las claves no representa una solución prometedora. Aún con el empleo de un ordenador pudiera probar una clave en 1 micro segundo, el procedimiento para probar todas las claves se llevaría 10^{13} años aproximadamente a pesar de esto dada una cantidad sorprendentemente pequeña de texto cifrado, el cifrador puede desbaratarse fácilmente. El ataque básico aprovecha las propiedades estadísticas de los lenguajes naturales En ingles por ejemplo, la letra mas común es la *e* seguida por las letras *t,o,a,n,i,* etc. Las combinaciones más comunes de dos letras, o diagramas, son las siguientes: *th,in,er,re y an.* Las combinaciones más comunes de tres letras o triagramas son: *the,ing,and y ion.*

Si un criptoanalista intentara desbaratar un cifrado monoalfabético, comenzaría contando las frecuencias relativas de todas las letras que aparecieran en el texto cifrado después, podría asignar, tentativamente, la letra e a la que apareciera con mayor frecuencia, la letra t, a la siguiente que aparezca con mayor frecuencia Después, observaría los triagramas para encontrar el más común de la forma tXe, que sugeriría fuertemente que la X es una h, de la misma manera, si el patrón thYt se presenta con frecuencia es muy probable que la Y represente a una letra a con esta información, él puede buscar un triagrama de la forma

ZW que se represente frecuentemente, que es muy probable que sea la palabra and Por medio de suposiciones con las letras, diagramas y tnagramas mas comunes, el criptoanalista genera un texto ordinario tentativo, letra por letra

Para hacer mas difícil el trabajo del criptoanalista es necesario uniformar las frecuencias del texto cifrado de tal forma que las letras representando ae, t, etc., no sobresalgan tan claramente Una manera de alcanzar este objetivo consiste en introducir múltiples alfabetos de cifrado para utilizarlos en rotación, dando así un resultado, que se conoce como cifrado polialfabético. Como un ejemplo, considérese el cifrado vigenére, el cual consiste de una matriz cuadrada que contienen 26 alfabetos de Cesar El primer renglón, llamado renglon A, es ABCDEFGH .. XYZ. El siguiente renglón, llamado renglón B es BCDEFGHI. YZA. Finalmente, el último renglón llamado renglón Z, es ZABCDEFG. WXY.

Al igual que el cifrado monoalfabético este cifrado tambien tiene una clave, pero en lugar de ser una cadena de 26 caracteres diferentes, la clave es generalmente una palabra o frase corta y fácil de recordar, como por ejemplo, COOKIEMONSTER. Para poner en clave un mensaje, la clave se escribe en forma repetida en la parte superior del texto en claro, por ejemplo:

COOKIEMONSTER COOKIEMONSTER COOKIEMONSTERCOOKIEMO
f o u r s c o r e a n d s e v e n y e a r s a g o o u r m o t h e r s b r o u g h t f o r t h

La letra clave que esta arriba de cada letra del texto en claro indica el renglón que se debe utilizar para la puesta en claro. La f se pone en clave utilizando el alfabeto de Cesar del renglón C, la o y la u se ponen en clave por medio del alfabeto de Cesar del renglón O, etc. Queda claro que una letra de texto se representará mediante diferentes letras en el texto cifrado, dependiendo de la posición en el texto claro. De la misma manera, los triagramas como la palabra the se correlacionarán con diferentes trigramas en el texto cifrado dependiendo de su posición

Utilizando cifrados monoalfabéticos arbitrarios para los renglones en lugar de restringirlos al cifrado de Cesar, se puede construir un cifrado polialfabético más poderoso. El único problema que se presenta con este esquema es que la matriz cuadrada de 26 por 26 entonces se convierte en parte de la clave y, también, deberá memorizarse o escribirse.

Aunque indudablemente los cifradores polialfabéticos son mucho mejores que los monoalfabéticos también pueden desbaratarse fácilmente mediante un ataque basado sólo en texto cifrado, a condición de que el criptoanalista tenga una cantidad suficiente de texto cifrado El ardid aquí, consiste en suponer la longitud de la clave Primeramente, el criptoanalista, en forma tentativa, supone una clave de longitud k. Después,

ordena en renglones el texto cifrado, tomando k letras por renglon Si su suposicion es correcta, todas las letras del texto cifrado en cada columna habran sido puestas en clave mediante el mismo cifrador monoalfabético, en cuyo caso deberan exhibir la misma distribucion de frecuencia que un texto normal en ingles. la letra mas común con un 13 %, la siguiente letra mas común con en 9 %, etc Si obviamente este no es el caso, el valor tentativo de k se considera incorrecto y se deberá probar con otro Una vez que se haya obtenido una buena correspondencia, cada columna podrá atacarse como si fuera un cifrado monoalfabetico separado

El siguiente paso de mayor complejidad para el criptógrafo consiste en utilizar una clave que sea de mayor longitud que la del texto en claro, provocando asi que el ataque anterior sea inútil. De hecho, la construcción de un cifrado indestructible es muy sencilla. Primeramente, se escoge como clave una cadena de bits aleatoria, se convierte el texto en claro en una cadena de bits por ejemplo, por medio de una representación en ASCII. Por último, se aplica un OR EXCLUSIVO, bit por bit, con estas dos cadenas. El texto cifrado resultante, no podrá desbaratarse, debido a que todos los posibles textos en claro son candidatos igualmente probables. El texto cifrado no le proporciona en absoluto ninguna información al criptoanalista. En una muestra suficientemente grande de texto cifrado, cada letra aparecerá con la misma frecuencia, como lo harán todos los digramas y trigramas.

Desafortunadamente este método, conocido como clave de una sola vez, tiene numerosas desventajas en la práctica. Para comenzar, la clave no se puede memorizar, por lo cual tanto el receptor como el transmisor deben llevar consigo una copia escrita. Si alguno de ellos es capturado, se ve claramente la desventaja de cargar consigo la clave escrita. Adicionalmente, la cantidad total de datos que pueden transmitirse queda limitada por la cantidad de clave disponible La sensibilidad del método ante la pérdida de mensajes, o de mensajes que llegan en un orden incorrecto, viene a ser otro problema importante. Si el transmisor y el receptor se desincronizan, en cuanto a la parte de la clave en la que se encuentren, se encontrarán sumidos en una situación problemática.

Todos estos problemas pueden resolverse si se hace que el transmisor y el receptor, sencillamente, lleguen a un acuerdo para iniciar cada mensaje de nuevo desde el comienzo de la clave, y para partir los mensajes muy largos en múltiples mensajes.

Ahora la clave ya no será una clave de una sola vez, y podrá desbaratarse, aunque con dificultad. Para romper el sistema, el criptoanalista deberá adquirir varios mensajes puestos en clave y ponerlos uno encima de otro, como una serie de renglones. El primer carácter de cada renglón puede verse como una columna puesta en clave por medio de un cifrado monoalfabético, y puede atacarse de una manera normal De hecho, la clave

de una sola vez es ahora, conceptualmente equivalente a un cifrador polialfabetico, solo que con una clave mas larga, y podra descifrarse de la misma manera

Es importante hacer una observación con respecto a la generación de claves de una sola vez, estas deben de ser aleatorias para ser seguras. La peor manera de generar una clave es la de utilizar un generador de números pseudoaleatorios, basado en una cadena de Markov Cuando se utilizan estos números aleatorios, no solo el resto de la clave deja de ser independiente de lo que existio antes, sino que está determinado únicamente por lo que apareció originalmente. Asi, si el criptoanalista logra adquirir alguna vez parejas correlacionadas de texto en claro y texto cifrado, será capaz de producir la clave utilizada para dichas parejas. A partir de esta clave podrá tener la posibilidad de deducir el algoritmo que la produjo y, a partir de éste, podrá generar el resto de la clave. Para generar una clave en verdad aleatoria, el ruido cuántico en un resistor eléctrico deberá ser amplificado y digitalizado. Las leyes de la mecánica cuántico garantizan que el resultado no será reproducible

Los cifradores de sustitución no siempre necesitan trabajar con una letra (o bit) a la vez. Por ejemplo, el cifrador de Porta utiliza una matriz de 26 X 26, al igual que el cifrador vigénere. El texto en claro se codifica con dos caracteres al mismo tiempo; el primer carácter indica un renglón , y el segundo una columna. La pareja de números o letras que se encuentra en una intersección representa el valor puesto en clave. Si se preparan 26 matrices diferentes, los triagramas pueden ponerse en clave como si fueran unidades, utilizando la primera letra de cada triagrama para seleccionar una matriz

4.2 CODIGOS

A medida que las unidades que se ponen en clave llegan a ser más largas, el cifrado comienza a parecerse a un código. La principal diferencia entre un cifrado y un código es que el primero pone en clave una unidad de tamaño fijo de texto en claro con cada operación efectuada, en tanto que el segundo pone en clave una sola unidad lingüística de longitud variable, que típicamente viene a ser una palabra o frase. Antes de la llegada de los ordenadores, los códigos se representaban en dos tipos diferentes: código de una parte y código de dos partes. En los códigos de una parte, tanto la palabra de texto en claro como el símbolo de código están dispuestos en el mismo orden. Por ejemplo los, los símbolos de código para las palabras amnesia, amoeba, amok, among, amorous, amorphous, amortize y ampere podrían ser 16142, 16144, 16149, 16155, 16160, 16189, 16201, y 16209 En un código de dos partes, estas mismas palabras podrían ser codificadas como 15202, 16902, 40420, 30012, 80032, 76290, 39320 y 10344. Con un código de una parte, tanto la codificación como la decodificación puede utilizar el mismo logro de código, mientras que en el caso de un código de dos partes se necesitan libros dispuestos en forma diferente para codificar y decodificar. Un código de una parte es mucho más fácil de descifrar que uno de dos partes, dado que el mismo código del símbolo

contiene una información aproximada sobre el lugar del libro en que se encuentra el símbolo en texto en claro Sin embargo, un codigo de dos partes necesita, que tanto el transmisor como el receptor transporten cerca del doble de equipaje

El desciframiento de un código es igual al desciframiento de un gigantesco cifrador monoalfabético El símbolo mas común en código es, generalmente, el símbolo para stop, que se utiliza para terminar un enunciado Después, vienen los símbolos para the, of, and, to, a, in y that. El conocimiento de la estructura de los enunciados en inglés es también muy útil; por ejemplo, la mayoría de los enunciados comienzan con un sujeto, y los sujetos normalmente son de la forma artículos adjetivos sustantivo.

Los códigos tienen la desventaja de que requieren de grandes libros, los cuales no pueden sustituirse tan fácilmente como la clave de un cifrador Sin embargo, tienen la ventaja de ser generalmente más fáciles de desbaratar que los cifradores. Los códigos y los cifradores pueden combinarse para hacer todavía menos agradable la vida de los criptoanalistas. Por ejemplo, la codificación de un mensaje podría producir una lista de números de cinco dígitos. Estos números podrían concentrarse para formar una secuencia de dígitos que, entonces, se podrían poner en clave utilizando un cifrador polialfabético. El cifrado de un mensaje codificado se denomina supercifrado.

4 3 CIFRADORES DE TRANSPOSICION

Los cifradores de substitución y los códigos preservan un orden de los símbolos del texto en claro, pero los disfrazan. A diferencia de éstos, los cifradores de transposición, reordenan las letras pero no las disfrazan. La clave del cifrador es una palabra o frase que no contiene ninguna letra repetida. El propósito de la clave es enumerar las columnas, comenzando con la columna cuya letra clave tiene el valor inferior

Para desbaratar un cifrador de transposición, el criptoanalista deberá primero estar enterado de que se esta enfrentando a un cifrador de transposición, el siguiente paso, sería suponer cual es el número de columnas, en muchos casos una palabra o frase probablemente puede llegar a adivinarse a partir del contexto del mensaje. Mediante la búsqueda de las diferentes posibilidades, los criptoanalistas pueden frecuentemente determinar la longitud de la clave fácilmente.

El siguiente paso consiste en ordenar las columnas Cuando el número de columnas, k, es pequeño, cada una de los k (k - 1) pares de columnas pueden examinar para ver si sus frecuencias de diagramas corresponden a las de un texto cifrado en inglés. Se supone que el par de mayor correspondencia es el que está colocado en la posición correcta Ahora, cada una de las columnas restantes se prueba tentativamente como la sucesora de este par La columna cuyas frecuencias de diagramas y triagramas producen la mayor

correspondencia, se considera tentativamente como correcta La columna predecesora se encuentra en un orden probable Existe la posibilidad de que el texto en claro se reconozca en este momento (por ejemplo, si apareciera mifloin, se veria con claridad cual es el error)

Algunos cifradores de transposición aceptan un bloque de entrada de longitud fija, y producen un bloque de salida de longitud fija Estos cifradores pueden describirse completamente al dar solamente una lista indicando el orden en que deberán salir los caracteres. Por ejemplo, el cifrador de la figura 4.3 puede verse como un cifrador con un bloque de 64 caracteres. Su salida es 4,12,20,28,36,44,52,60,5,13,. .,62. En otras palabras, el cuarto caracter de entrada, a, es el primero en salir, seguido por el doceavo, f, y asi sucesivamente.

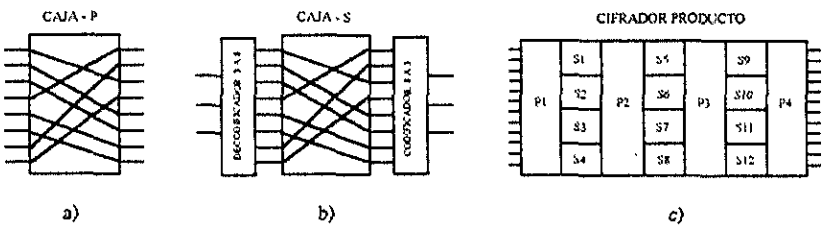
4.4 LA NORMA DE CIFRADO DE DATOS

Mientras se han estado describiendo varios esquemas criptográficos clásicos, también se ha tratado de poner en claro el hecho de que los ordenadores puedan utilizarse como una poderosa herramienta para los criptoanalistas, tanto como para recoger datos estadisticos de frecuencias como para someter a prueba un número considerable de soluciones tentativas. Ahora desde el punto de vista de un criptógrafo: es decir, *pensar en la manera de diseñar un proceso de cifrado tan complicado que, incluso por medio de un ordenador,* no se puede descifrar o desbaratar.

Aunque la criptografia moderna utiliza las mismas ideas básicas de la criptografia tradicional, es decir, los conceptos de transposición y sustitución, su énfasis es diferente. Los criptógrafos, tradicionalmente, han utilizado algoritmos muy sencillos y han confiado en claves muy largas para su seguridad. En la actualidad, lo contrario resulta cierto: el objetivo es el de hacer un algoritmo de cifrado tan complicado que, incluso el criptoanalista adquiere grandes cantidades de texto cifrado de su propia elección, no tenga ninguna posibilidad de obtener de él nada con sentido.

Las transposiciones y sustituciones pueden instrumentarse con circuitos muy sencillos En la figura 4.2a, se muestra un dispositivo, conocido como caja-P (la P quiere decir permutación), que se utiliza para efectuar una transposición a una entrada de 8 bits. Si los 8 bits se designan, de arriba hacia abajo, como 01234567, la salida de esta caja-P particular sería 36071245 Mediante un cableado interno apropiado, se puede hacer que la caja-P efectúe cualquier transposición.

La sustitucion se lleva a cabo por medio de las cajas- S, como se muestra en la figura 4 2b En este ejemplo, se tiene como entrada un texto en claro de 3 bits, y como salida un texto cifrado de 3 bits La entrada de 3 bits, selecciona una de las ocho lineas que salen de la primera etapa, y la fija con un valor de 1, todas las demas lineas tienen un valor de 0 La segunda etapa es una caja-P La tercera etapa codifica la linea de entrada seleccionada, de nuevo en binario. Con el cableado mostrado, si los ocho números octales 01234567 se introdujeran uno después de otro, la secuencia de salida seria 24506713. En otras palabras, el 0 se ha substituido por el 2, el 1 por el 4, etc Aqui, nuevamente, mediante un cableado apropiado de la caja-P, cualquier substitucion se puede llegar a efectuar.



Elementos basicos de cifradores producto

Figura 4 2

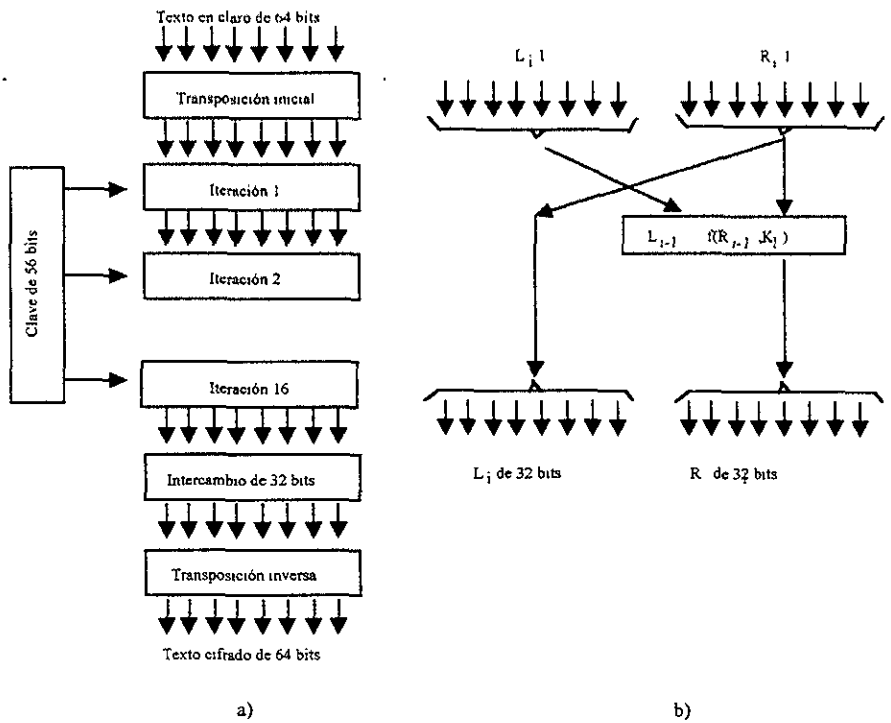
La potencia real de estos elementos básicos sólo aparece cuando se pone en cascada una serie completa de cifradores, como se muestra en la figura 4.2c. En este ejemplo, la primera etapa transpone 12 líneas de entrada. Teóricamente, sería posible tener en la segunda etapa una caja- S que correlacionara un número de 12 bits, con otro número de 12 bits Sin embargo, semejante dispositivo necesitaría, $2^{12} = 4096$ cruzamientos de cables en su etapa intermedia. En lugar de esto, la entrada se divide en 4 grupos de 3 bits, cada uno de los cuales se substituye en forma independiente de los demás. Aunque este método es menos general, todavía resulta poderoso. Al incluir un número suficientemente grande de etapas en el cifrador resultante, la salida puede representarse como una función no lineal de la entrada

En enero de 1977, el gobierno de EU, adoptó un cifrador producto desarrollado por IBM, como su norma oficial para información no clasificada. Esta adopción, ha su vez, ha llegado a estimular a numerosos fabricantes para que realicen en hardware el algoritmo de cifrado, conocido como "norma de cifrado de datos", haciéndolo por consiguiente más rápido y económico.

4 5 TECNICAS DE ENCRIPTAMIENTO

4 5 1 ALGORITMO DES

El cifrado del texto en claro se realiza en bloques de 64 bits, produciendo asi 64 bits de texto cifrado. El algoritmo, que se parametriza por medio de una clave de 56 bits, tiene 19 etapas diferentes La primera etapa es una transposición independiente de la clave, sobre el texto en claro de 64 bits La última etapa es exactamente la inversa de esta transposición La etapa, anterior a la última, intercambia los 32 bits de la parte izquierda, con los 32 bits de la parte derecha. Las 16 etapas restantes son funcionalmente idénticas, pero están parametrizadas por diferentes funciones de clave El algoritmo se ha diseñado para permitir que el proceso inverso del cifrado se realice con la misma clave de cifrado. Los pasos a seguir, por lo tanto, son exactamente los mismos, pero se realizan en orden contrario. En el diagrama de la figura 4.3.a, se muestra el esquema general del cifrado de datos.



La norma de cifrado de datos.
a) Esquema general b) Detalle de una iteración

Figura 4 3

En la figura 4 3b, se ilustra el funcionamiento de una de estas etapas intermedias, cada una de ellas toma dos entradas de 32 bits y produce dos salidas de 32 bits La salida de la izquierda es simplemente una copia de la entrada de la derecha La salida de la derecha es un OR EXCLUSIVO bit a bit de la entrada de la *izquierda, y una función de la entrada de la derecha y la clave de la etapa, ki Toda la complejidad descansa* en esta función.

La función consta de cuatro pasos, que se llevan a cabo en secuencia Primero, se construye un número E de 48 bits, mediante la expansión de los 32 bits R_{i-1} deacuerdo con la regla fija de transposición y duplicación. Segundo, E y K_i se someten conjuntamente a una función OR EXCLUSIVO. Esta salida, después, se divide en ocho grupos de 6 bits, cada uno de los cuales alimenta a una caja- S diferente. Las cajas - S producen salidas de 4, en lugar de 6 bits, cada una de las 64 posibles entradas a una caja - S se corresponde con salidas de 4 bits. Por último, estos 32 bits se pasan por una caja - P

En cada una de las 16 iteraciones, se utiliza una clave diferente. Antes de que comience el algoritmo se aplica una transposición de 56 bits a la clave Justo antes de cada iteración, se divide la clave en dos unidades de 28 bits, cada una de las cuales es rotada a la izquierda según un número de bits que depende del número de iteración. El valor de K_i se deriva de esta clave rotada, mediante la aplicación de otra transposición de 56 bits sobre ella. A pesar de toda esta complejidad, la DES es básicamente un cifrador de substitución monoalfabética que utiliza un carácter de 64 bits.

Una manera de fortalecer la DES (o cualquier cifrador para este efecto), consiste en incluir caracteres aleatorios en el texto en claro, deacuerdo con una regla bien definida (por ejemplo, todos los n-ésimos caracteres son reales, y el resto son solo ruido). Además, mensajes de relleno pueden insertarse a los que son reales, a este principio se le conoce como cifrador nulo, el cual es obviamente, un desperdicio de ancho de banda, pero que llega a ser muy difícil de descifrar, por que la posición de los caracteres reales y de los mensajes se conserva en secreto, y se cambia cuando se modifica la clave. En líneas privadas alquiladas, vale la pena la importancia de transmitir basura, cuando de otra manera la línea quedaría inactiva.

4.5.2 CIFRADOR DE FLUJO

Otra manera de lograr que el criptoanálista de la DES sea más difícil, es la de hacerla funcionar como si fuera un cifrador de flujo como se muestra en la figura 4.5, en lugar de que opere como un cifrador de bloque Cuando se utiliza como un cifrador de bloque, tanto el receptor como el transmisor operan sus circuitos integrados DES en modo de cifrado (es decir, opuesto al descifrado). Cada uno de los circuitos integrados DES cuenta con un registro de entrada de 64 bits, el cual opera como un registro de desplazamiento, y un registro de salida de 64 bits, que no lo hace así. En el momento en que llega un carácter de texto en claro, se realiza un OR EXCLUSIVO con los ocho bits del registro de salida, O_1. (Los

correspondientes a O_2 hasta O_8, nunca se utilizan) De esta manera, el caracter así creado se transmite al receptor y se introduce en el registro de desplazamiento de entrada, sacando a Y8 del registro Despues, el circuito integrado es activado, y la salida se calcula para la nueva entrada

En el extremo receptor, al caracter que llega se aplica primero una OR EXCLUSIVA con un O1 (produciendose el texto en claro), y despúes se introduce en I1. Si el receptor y el transmisor arrancan con registros de entrada idénticos, éstos permanecerán iguales para siempre, lo cual significa que O1en el extremo transmisor será siempre el mismo que O1 en el extremo receptor Dado que aí carácter de texto en claro, que llega al transmisor, se le hace un OR EXCLUSIVO con el mismo carácter, que se usara con el de entrada del texto cifrado en el receptor, la salida en el receptor será el texto en claro original. La propiedad de los cifradores de flujo, que los hace muy valiosos, es que O1 depende de la historia completa del texto en claro, por lo que la repetición de un patrón en el texto en claro no generará un patrón repetido en el texto cifrado. Los cifradores de flujo, también son muy apropiados para utilizarse en terminales, por que no tienen que colectar ocho caracteres antes de emitir un texto cifrado.

Problema en la distribución de clave.

Otro problema con la DES es que, para que el receptor descifre los mensajes, necesita utilizar la misma clave que el transmisor empleó para ponerlos en clave.

Como consecuencia de esto, surge el problema sobre la manera segura de distribuir las claves secretas. Tradicionalmente se han estado inventando pares de claves idénticas, en un servicio central generador de claves, y se transmitían a sus destinos respectivos por correo personal.

Una posible solución al problema de inseguridad es utilizar una clave jerárquica, cada organización selecciona una clave maestra aleatoriamente, y la distribuye mediante correo personal a cada una de sus oficinas; las cuales están agrupadas en regiones, y la oficina central de cada región se encarga de seleccionar una clave regional. Las claves regionales se cifran por medio de una clave maestra y se distribuyen a través de la red Cuando cualquier par de oficinas, dentro de una misma región, deseen comunicarse, una de ellas deberá seleccionar una clave de sesión y enviársela a otra, cifrándola mediante la clave regional. Alternativamente, un proceso administrador de claves selecciona la clave de sesión y la transmite a los dos interlocutores, cifrada mediante la clave regional.

La filosofía detrás de este diseño es que tanto las claves maestras como las regionales se utilizan tan rara vez que ningún intruso será capaz de recolectar suficiente texto cifrado como para tener la posibilidad de descifrarlas. Además, el testo en claro de estos mensajes consta de números aleatorios, de 56 bits, haciendo virtualmente imposible realizar una operación de criptoanálisis con ellos Los mensajes en la práctica,

deberán empezar con una cabecera " " con el objeto de impedir que el criptoanalista pueda adquirir un par correlacionado de texto en claro y texto cifrado, la cabecera debera transmitirse sin estar cifrada.

Sin embargo, se ve claramente que para hacer funcionar el sistema se sigue necesitando realizar un transporte fisico de las claves maestras, por medios externos a la red Cada vez que se piense que la clave maestra pueda estar comprometida o que, un empleado que la conozca, o que podria haberla conocido, esté a punto de dejar la organización (por ejemplo, los mensajeros de correo personal), se deberá generar una nueva clave y transportarla fisicamente a todas la oficinas.

Lo peor de todo es que no existe un medio sencillo para que dos personas totalmente extrañas, que pertenezcan a organizaciones diferentes, se puedan comunicar de manera segura, excepto si se reúnen fisicamente y acuerdan emplear una clave escogida en ese lugar y momento. Esto es equivalente a pensar que alguien no tuviese la posibilidad de hacer una llamada telefónica a otra persona, hasta que esta haya entregado su tarjeta de presentación. Obviamente, es necesario desarrollar un método mejor

Por fortuna ya se conocen varios métodos ingeniosos para resolver el método de la distribución de claves. El método de Merkle, supone que dos interlocutores, el A y el B, nunca antes se habían comunicado, pero ahora desean hacerlo de una manera segura Deberán utilizar el canal que los une para fijar la clave, aún cuando algún intruso pudiese llegar a copiar todo lo que se transmite por ese canal

El método se basa en lo que Merkle llama acertijos. Un acertijo, es un criptograma que se pretende descifrar. Supóngase que A inicia la conversación.

4 5 3 PROTECCION DE CLAVE

Aunque el hecho de esconder la clave para que no esté al alcance de los intrusos es importante, también lo es hacerlo para uno mismo. Para ser más precisos, una compañía podria no querer delegar una autoridad ilimitada (bajo forma de una clave) a cualquier empleado. Shamir ha ideado una técnica muy inteligente para compartir claves criptográficas entre múltiples empleados, de una manera muy flexible.

4 6 MODELO MATEMATICO

Se considera un emisor que quiere enviar un mensaje a un receptor mediante un canal inseguro, existen dos situaciones en las que el receptor puede ser engañado. Puede que el canal sea ruidoso y por ello el mensaje se reciba con perturbaciones o bien puede que el canal este bajo el control de un enemigo que modifique los mensajes transmitidos por el receptor e inyecte mensajes fraudulentos.

Se hacen algunas suposiciones previas En primer lugar, se supone que el emisor y el receptor confían uno en el otro y ninguno se trata de engañar En ese caso, es innecesaria la presencia de un arbitro

En cualquier protocolo de autenticación se supone que el receptor sólo acepta como auténticos los mensajes pertenecientes a una parte del conjunto total de mensajes posibles y que el emisor usa solo un subconjunto de esa parte para comunicares con el receptor autorizado. La criptografía se utiliza para *suministrar a emisor y a receptor una forma fácil de definir el subconjunto de mensajes que usan y captan* respectivamente según la clave secreta conocida solo por ellos.

Todo esquema de autenticación depende de la presencia de información redundante que haya sido introducida deliberadamente o bien que estuviera presente en la estructura del mensaje

La información redundante debe ser reconocible por el receptor. Se utiliza el término autenticador para denotar la información redundante añadida por el emisor para permitir al receptor verificar que el mensaje es autentico

Al igual que en los códigos detectores y correctores de error, en los esquemas de autenticacion para una regla de codificación fija existe también un subconjunto de secuencias aceptables (autenticas) que contienen la información redundante y una colección no vacía de secuencias que no contienen la información redundante, por lo que son rechazadas (no autenticas) La diferencia estriba en la teoría de la codificación, solo existe una regla de codificación cerrespondiente al código fijado, mientras que en los esquemas de autenticación existen muchas reglas de codificación entre las que el receptor debe escoger la regla particular secreta que fue usada para enviar el código.

Se distinguen aquellos esquemas de autenticación en los que el enemigo conoce la información que se transmite (llamados con secreto) de los esquemas en los que el enemigo ignora la información que se *transmite (llamados sin secreto). En el primero el mensaje se codifica según una regla de codificación* acordada por ambos comunicantes, mientras que en el segundo el mensaje se cifra utilizando una clave también acordada por ambos usuarios.

En la práctica lo habitual es destinar una parte de la clave a autenticación y el resto a proporcionar secreto.

Se supone que el enemigo conoce completamente el sistema, incluyendo la regla de codificación o el espacio de claves, según el tipo de esquema del que se trate. Lo único que no conoce es la regla particular de codificación o clave acordada por ambos comunicantes.

Por tanto, el modelo matemático esta formado por las tres partes ya mencionadas emisor, receptor y enemigo

Sean S el conjunto de m estados de la fuente, M el conjunto de v mensajes y E en cada caso (con secreto y sin secreto) el conjunto de b reglas de codificación o claves posibles. La informacion que se desea transmitir es un estado de la fuente $s \in S$.

Se habla de un modelo con división (splitting) cuando para cada estado de la fuente el emisor puede escoger entre varios mensajes determinados por dicho estado. Sin embargo, obsérvese que para que el receptor sea capaz de determinar unicidad el estado de la fuente que corresponde a un mensaje recibido debe existir como mucho un estado de la fuente que se codifique mediante un mensaje $\alpha \in M$, $\forall\ e \neq E$; o sea, si $s \neq s'$, entonces $e(s) \neq e(s')$.

En un modelo sin división (non splitting), una vez que emisor ha seleccionado el elemento particular $e \in E$, el mensaje asociado a cada estado de la fuente queda determinado con unicidad. *Es decir*, dado $e \in E$, $\forall\ s \in S$, entonces $\exists\ \alpha = e(s)$. Esta condición en un esquema sin secreto implica que, efectivamente, no hay secreto en el sentido de que si un enemigo observa un mensaje codificado sabe exactamente que estado de la fuente se esta transmitiendo. Un esquema con esta ultima propiedad se denomina esquema cartesiano

Por otro lado, una clasificación natural de los esquemas de autenticación se desprende, al igual que en los sistemas de cifrado de la seguridad computacional así se distinguen los esquemas llamados respectivamente, computacionalmente, probablemente e incondicionalmente seguros.

Un esquema se dice que es computacionalemte seguro si la seguridad depende de que un enemigo *pueda o no realizar algún cálculo que en principio, aunque posible es tal que requiere una cantidad de cálculo* irrealizable. Un esquema de autenticación se dice que es probablemente seguro si puede demostrarse que romperlo implica resolver algún problema supuestamente irresoluble, como la factorización del producto de dos grandes números primos o la obtención de logaritmos discretos.

Un esquema de autenticación se dice que es incondicionalmente seguro si la seguridad no depende de la potencia de cálculo ni de el tiempo de que dispone un enemigo.

Estos esquemas de autenticación incondicionalmente seguros constituyen un dual matemático de los códigos detectores y correctores de error , en ambos casos la información redundante se introduce en la secuencia de símbolos a transmitir, resultando que sólo una fracción del conjunto de posibles secuencias son *utilizadas por el emisor En el último caso, si el receptor recibe una secuencia que no pudo haber sido*

enviada por el emisor utiliza una regla fija para decidir cual de las secuencias validas es con mayor probabilidad la que fue transmitida, en el otro caso la recepcion de una secuencia que no pudo haber sido enviada por el emisor es interpretada por el receptor como que no fue el autentico emisor quien la envió o que si lo fue, algún enemigo altero el mensaje por el trayecto, y rechaza el mensaje declarándolo no autentico

Según sus condiciones, el enemigo puede elegir entre dos tipos de ataque:

- Puede construir un mensaje fraudulento sin haber conseguido previamente ninguno autentico
- Puede valerse de un mensaje autentico interceptado para realizar el fraude.

4 6 1 METODOS

La actividad del adversario puede constituir en:

- Bloquear el flujo de información grabar información y repetirla luego en una transmisión falsa.
- Cambiar la información borrando, insertando y/o reordenándola

Tal y cómo se definierón los esquemas de autenticación con y sin secreto, se tiene que en el primero, un autenticador conocido por emisor y receptor se añade al texto que se desea autenticar y luego se cifra. De esta manera, el texto resultante se le proporciona al mismo tiempo secreto y autenticación Si en alguno de estos dos casos se usa un sistema simétrico, entonces emisor y receptor han de confiar plenamente el uno en el otro, por que ambos comparten la misma clave.

Por tanto se puede clasificar claramente los métodos de autenticación, según si se utiliza criptografia simétrico o asimétrica, en·

Métodos basados en criptosistemas simétricos y
Métodos basados en criptosistemas asimétricos.

En primer lugar analizamos la autenticación mediante criptosistemas simétricos. Se supone que se cumple el esquema de la ilustración 19, donde T es un subconjunto del conjunto de mensajes M. El subconjunto T de los mensajes validos debe ser conocido por ambos comunicantes, de tal forma que tras descifrar el criptograma, el receptor comprueba si el mensaje resultante pertenece o no a él Ambos comunicantes, además fijan a priori un mensaje Ms que corresponde a cierta información redundante que permite autenticar cualquier mensaje M El mensaje Ms debe mantenerse en secreto. El remitente cifra el mensaje cuya autenticidad quiere salvaguardar según C = Ek (M, Ms), con lo que el receptor solo tiene que comprobar tras descifrar que Ms coincide con el fijado a priori.

Suponiendo que no hay acuerdo previo y que los mensajes estan escritos en un mensaje natural En este caso se consideran como autenticos solo aquellos mensajes que tras descifrarlos sean legibles y tengan significado

Por otro lado en los sistemas de clave secreta, la percepción del receptor sobre que todo texto que al ser descifrado sea legible debe provenir del emisor legitimo puede ser una falsa impresión ya que el enemigo puede estar aprovechando algún texto previamente calculado.

Cuando un sistema simétrico se utiliza para proporcionar secreto es recomendable cambiar a menudo la clave; sin embargo, con propósito de autenticación es mejor no arriesgar demasiado su captura. Ahora se considera el caso de autenticación mediante sistemas asimétricos, considerando en particular el algoritmo RSA. Cada usuario i genera una clave secreta di a partir de dos números primos (pi, qi) y publica ni = pi qi y ei = di - 1 (mod ϕ (ni)). Recordemos que el cifrado del mensaje consiste en Ei (α) = α^e, (mod ni) y el descifrado en Di (m) = m^e; (mod ni). Para usar este sistema como esquema de autenticación el usuario i obtiene Di (m) y lo envía al receptor Este, para verificar su autenticidad le aplica Ei con la clave publica de y, obteniendo Ei (Di (m)) = m (mod ni), demostrando así que es autentico.

Secreto y autenticidad son atributos independientes de los criptosistemas.
En general, uno se maximiza a costa del otro.

Uno de los principales problemas que se presentan en la autenticación es la posibilidad de que el enemigo utilice mensajes anteriores. Para intentar resolverlo, es conveniente añadir al texto alguna señal que impida al engaño, por ejemplo la fecha.

Aunque un esquema de autenticación permite al usuario A confiar en que el mensaje que ha recibido viene de quien dice venir eso no le permite convencer a un tercero de ello. Por eso, los esquemas de autenticación resultan débiles ante el engaño de uno de los dos interlocutores legítimos.

4 7 IDENTIFICACION DE USUARIO

Cuando un usuario quiere acceder a un servicio de un computador (por ejemplo, cuando un cliente quiere usar un cajero automático o cuando el cajero quiere acceder al computador central del banco) siempre surge la siguiente cuestión: ¿ Como puede estar seguro el servidor de que el cliente no esté utilizando una identidad falsa ? La solución clásica a este problema pasa por el empleo de passwords. Esto se basa en que el usuario y el computador comparten cierta información confidencial, por lo que el último puede comprobar la identidad del primero simplemente requiriéndole dicha información. Claramente la seguridad de tal esquema depende completamente de la habilidad para mantener en secreto los passwords.

Los principales puntos debiles del esquema de password son

La existencia de un listado en el computador,

La amenaza de escucha

El solo hecho de que los password esten almacenados en el computador ya resulta muy peligroso No importa que estén protegidas o escondidas, un enemigo inteligente siempre puede encontrarlas; en la mayoría de los sistemas informáticos siempre existe almenos una persona, el administrador del sistema o superusuario, que tiene acceso legal al directorio de passwords, por lo que los demás usuarios se ven forzados a confiar en esta persona Como mínimo, todo usuario prudente debería usar distintos password en distintos sistemas.

La amenaza que representa el administrador puede resolverse fácilmente en la práctica. Para ello la idea clave que hay que utilizar es que el computador en realidad no necesita conocer exactamente los passwords. Sólo debe de ser capaz de validarlas y esto puede hacerse mediante una función trampa, basta con que el computador tenga almacenadas las imágenes de los passwords de los usuarios según una función trampa fija. Ni siquiera hace falta que esta función se mantenga en secreto. Siempre que un usuario deba mostrar su identidad, solo tiene que transmitir su password. El computador inmediatamente aplica la función trampa y coteja el resultado con el listado, por la imposibilidad de invertir la función trampa.

Este esquema resulta bastante débil si los usuarios usan passwords fáciles de deducir, por que en ese caso que un enemigo que tenga acceso al listado y conozca la función trampa puede conseguir sus fines. Escoge los passwords más comunes y compara los resultados con el listado cifrado, cada existo corresponde a un password descubierto

Aunque en este caso no se pueden proteger individualmente los password, existe otra técnica, llamada salting, que elimina la amenaza colectiva anterior. Está consiste en que cada usuario escoge una secuencia aleatoria y la añade a su password, de manera que en el listado se asocia a cada usuario el valor que toma la función trampa aplicado al bloque formado por el password del usuario y la secuencia aleatoria. Como resultado, aunque dos usuarios distintos escojan el mismo password, producen distintos datos en el listado

A pesar de estas mejoras, queda un punto más de debilidad en la técnica de password Cada vez que el usuario tiene que establecer su identidad, debe transmitir su password al computador. En ese momento, la transmisión es vulnerable a la intercepción, tanto a través de los cables de comunicación del computador como por la memoria en la que el computador guarda ese password antes de aplicarle la función trampa

Para liberarse de esta amenaza, no basta con que el computador no almacene nunca el password en claro, sino que incluso no se le debe transmitir así Esta aparente paradoja puede realizarse siempre que los usuarios utilicen terminales inteligentes, o bien tarjetas inteligentes.

En este caso se puede resolver el problema de la identificación de usuario utilizando un sistema de clave pública. Cada usuario escoge una clave secreta aleatoria y la usa para generar la correspondiente clave pública, revela la clave de cifrado al computador y programa el algoritmo descifrado en su terminal. Siempre que el computador desee conocer su identidad, genera un mensaje aleatorio, calcula el cifrado de ese mensaje con la clave pública del usuario y envía el resultado a la terminal del usuario Este descifra dicho mensaje y se lo devuelve al computador, el cual por fin comprueba su validez

Realmente no es totalmente necesario el uso de funciones trampa para el último esquema de identificación de usuario planteado, ya que basta con utilizar funciones tales que el cálculo de su inversa sea posible, pero menos eficiente siempre que no se tenga la información que lo facilite. Por ejemplo, el cifrado puede hacerce el cifrado en menos de un segundo, pero el criptoanálisis, por el contrario, requiere varias horas. Desde luego, ese sistema no se consideraría válido para cifrados habituales de textos cuyo secreto se desea preservar. Sin embargo, si lo es como esquema de identificación de usuario porque el computador puede controlar cuánto tarda la terminal del usuario en responder, de manera que una respuesta correcta calculada muy tarde será tan útil como ninguna

En general, el problema de identificación también puede resolverse mediante una técnica llamada demostración nulo.

4.8 SEGURIDAD EN REDES

Una red es una configuración de computadoras conectadas entre sí mediante las llamadas aristas, que permiten el intercambio de datos e información, estas terminales están conectados a nodos que a su vez se interconectan formando una subred.

En una red de computadoras, los nodos suelen tener tres funciones básicas:
El control de errores
El almacenamiento temporal de información y
Su direccionamiento.

La subred es una parte especialmente suceptible a la acción de usuarios mal intencionados

Con el objeto de unificar criterios para el desarrollo de implantacion de redes, algunas organizaciones internacionales definieron un modelo de arquitectura de interconexion conocido como OSI (Open System Interconection)

NIVEL 7	APLICACION
NIVEL 6	PRESENTACION
NIVEL 5	SESION
NIVEL 4	TRANSPORTE
NIVEL 3	RED
NIVEL 2	ENLACE
NIVEL 1	FISICO

Debido a las grandes dimensiones fisicas que suelen tener las redes, es imposible el control por medios fisicos, luego es necesario el empleo de criptografia.

Hay tres formas de incorporar la criptografia para salvaguardar la seguridad de las redes, (figura 4 4):

Cifrado de aristas, protege los datos entre nodos adyacentes en la red Los servicios criptograficos se sitúan en los respectivos nodos, donde se utiliza exactamente la misma clave. Se realiza en los niveles uno o dos del modelo OSI Para cada nueva comunicación a través de una arista se genera una nueva clave en cada extremo El punto débil en este caso está en que los nodos intermedios los datos están descifrados

Cifrado nodo a nodo, es similar al anterior, pero en este caso cualquier par de nodos, no necesariamente adyacentes, comparte una clave para sus intercomunicaciones. D esta forma, los datos que pasan por nodos intermedios son completamente ininteligibles en ellos Al contrario de lo que ocurria en el caso anterior, en esté los datos no tienen que ser descifrados en los nodos intermedios

Cifrado extremo a extremo, los datos están protegidos durante la transmisión a través de toda la red por que las operaciones de cifrado y descifrado se realizan en los terminales. Cada usuario debe disponer de tantas claves como interlocutores en otros terminales, y los datos son inteligibles en todos los nodos intermedios, el problema en este caso esta en el coste debido al número y distribución de claves.

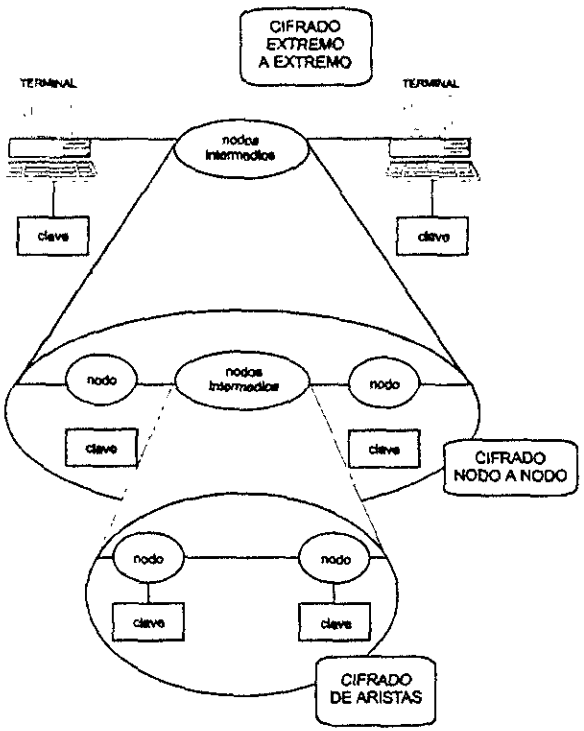


Figura 4.4

Las dos primeras soluciones planteadas, el cifrado de aristas y el cifrado nodo a nodo, implican que el usuario que esté en un terminal debe generar una clave para la comunicación con cada nodo. Sin embargo, en el caso del cifrado extremo a extremo, la mejor solución al problema de la gestión de claves consiste en que cada usuario comparta una clave, llamada clave maestra, con un centro distribuidor de claves, de forma que cuando un usuario quiera comunicarse con otro, debe contactar previamente con dicho centro. Este genera una clave y se le envía a ambos usuarios cifrada mediante la clave maestra de cada uno Las claves del usuario del terminal en el cifrado de aristas se llaman claves transacción, mientras que en el caso de cifrado extremo a extremo se llaman claves de sesión.

Los principales problemas que surgen al utilizar la criptografía para la protección de una red son:

La gestión de claves

los protocolos a usar

El problema de la gestion de claves en un sistema criptografico incluye la generacion, almacenamiento, distribucion y mantenimiento de las claves necesarias para que el sistema tenga garantizada la seguridad. Representa uno de los mayores problemas en un sistema de clave secreta, por que los cuatro son procesos que se tienen que realizar constantemente. El problema de la distribucion existe como tal solo en los criptosistemas simetricos.

Un generador de claves ideal es aquel que las genera de forma equiprobable, por tanto es muy recomendable utilizar para ese fin generadores de secuencias seudoaleatorias .

CAPITULO 5

APLICACION PRACTICA DE COMPRESION Y ENCRIPTAMIENTO

5 1 S-HTTP.

S-HTTP (Secure Hypertext Transfer Protocol) es una extensión para HTTP (Hypertext Transfer Protocol) que proporciona servicio de seguridad. Fue originalmente desarrollado por Enterprise Integration Tecnologies, y posteriormente desarrollado por Tensa System HTTP es el protocolo que forma la base del World Wide Web, conteniendo el intercambio de documentos multimedia en la Web. S-HTTP esta diseñado para proveer confidencialidad, autenticidad, Integridad y no repudiabilidad mientras soporta multiples mecanismos de manejos de claves y algoritmos criptograficos via opción negociación entre las partes involucradas en cada transacción Este es un servicio proporcionado por INTERNET.

5 2 SSL

El SSL (Secure Socket Layer) Handshake Protocol fue desarrollado por Net Scape comunication Corporation para proporcionar seguridad y privasidad sobre el Internet El protocolo soporta servidores y autenticación a clientes El protocolo SSL es una aplicación independiente, contiene protocolos como HTTP, FTP (File Transfer Protocol), y Telnet para ser llevado a su maxima transparencia. El protocolo SSL es capaz de negociar con claves de encriptación así como autenticación de servidores antes del intercambio de información por la aplicación de alto nivel. El protocolo SSL mantiene la seguridad e integridad del canal de transmisión por medio del uso de un canal de encriptación, autenticsacion y códigos de autenticación de mensajes.

El protocolo SSL Handshake, consiste en dos fases, autenticación de servidor y autenticación de cliente, con la segunda fase siendo opcional. En la primera fase, el servidor, en respuesta a la petición del cliente envia la información cifrada y certificada. El cliente entonces genera una clave maestra, la cual es encriptada con la clave pública en el servisor, y transmite la clave maestra ya encriptada hacia el servidor El servidor recupera la clave maestra y la autentifica el mismo para el cliente, para regresar el mensaje encriptado con la clave maestra. Susecuentemente la informacion encriptada con la clave derivada de la clave maestra. En la segunda fase opcional, el servidor envia una contraseña para el cliente. El cliente autenfifica por el mismo para que el servidor le regrese su firma digital en la contraseña así como su certificado de clave pública.

5 3 UNIDAD MOVIL DE PRODUCCION REMOTA

5 3 1 DESCRIPCION

Empecemos por explicar la constitución de una unidad móvil de producción remota
Una unidad de producción movil está constituida por el equipo que se menciona a continuación.

* 5 Cámaras de video con su respectiva uúmidad de control de camara
* 5 VTR de formato profesional (BETACAM) Play
* 5 VTR de formato profesional (BETACAM) Rec
* De uno a dos generadores de patrones de video
* Mixer de 20 entradas como mínimo.
* 2 Vectorscopios
* 2 Monitores de forma de onda.
* De uno a dos sincronizadores.
* Microfonos de ambiente.
* Distribuidores de audio.
* 7 Monitores de video
* Titulador.
* Planta generadora de energía eléctrica.
* Equipos de microondas
* Modulador.
* Amplificador de R.F.
* Antena.
* Un canal de microondas.

De lo anterior para transmitir un partido de fútbol por ejemplo.

Las camaras de vídeo son el transductor o la puerta de entrada a los sistemas de televisión, la cámara genera la señal de vídeo que es la copia de una escena viva.

La señal de video, es una señal eléctrica de amplitud variable con el tiempo y que es de 1 Vpp cuando es compuesto. Pero las cámaras de tipo industrial requieren de una unidad de control de cámara, la cual proporciona a la cámara comunicación con el operador, fuentes de poder, la señal de vídeo, está dada por componentes RGB y también sirve para sincronizar la cámara con el swither y el tiempo de video adicional.

Las VTR son equipos reproductores y grabadores profesionales para editar formas y repetir secuencias de alguna escena

Los generadores de patrones de video, nos generan un patron de sincronia con el cual nos referira a todo nuestro equipo

El mixer conmutará entre las cámaras y las señales de salida editadas por las VTR los tituladores y otros accesorios de video.

El vectorscopio nos indica el nivel de croma y la fase de la misma

El monitor de forma de onda nos indica el nivel de video, el nivel de Burst, el nivel de sincronia y la posición del SCH (Subcarrier Horizontal) para revisar la señal que se transmitirá en los sincronizadores nos restauran los niveles y protegen contra la ausencia de video

Los microfonos de ambiente nos proporcionan el sonido ambiente hacia los distribuidores de audio y el mixer. El titulador nos proporciona un croll sobre una escena definida

Donde se requieren almenos:

* 5 Camarográfos.
* 5 Operadores de video tape
* 1 Operador de titulador.
* 2 Operadores de mixer.
* 1 Productor
* 1 Auxiliar de productor
* 2 Ingenieros de video tape
* 2 Ingenieros de transmisiones
* De 4 a 10 auxiliares.
* 1 Electricista
* 1 Auxiliar de electricista.

A los cuales se les pagan viáticos y alimentos, así como un salario por su jornada.

Además que en el centro productor se requiere de un estudio donde se recibe la señal maestra (Audio Video) donde se encuentra otro director, los comentaristas, un operador master, un coordinador de master, de ahí la señal maestra sale hacia la antena para su difusión máxima.

Como se puede observar los elementos y personas que intervienen son mayores si el evento es en vivo

En un sistema de transmisión, podemos observar que existen demasiados costos de operacion, costos de depresiación de equipo, y que se tiene un canal de microondas o medio de transmisión, del que se trate con un ancho de banda limitado para una sola señal maestra

Nosotros proponemos el uso de la tecnologia de compresion de ancho de banda para video, empleando el equipo DigiCipher, el cual maneja hasta diez servicios (canales) de tv de formato NTSM, comprimidos, multiplexados y modulados en una portadora de tipo QPSK donde se pueden suprimir algunos elementos del sistema anterior y elevar la calidad de transmisión.

El modelo que se propone es el siguiente:

El empleo de un equipo DigiCipher de la fase 1 de General Instruments nos resume de la lista anterior de equipo para una unidad móvil siguiente:

* Hasta diez cámaras de video con su unidad de control de cámara
* 1 Generador de patrones de video.
* Hasta diez microfonos de ambiente.
* 10 monitores de video de 4 pulgadas.
* 1 Equipo DigiCipher.
* 1 Equipo de transmisión 1+1
* 1 Unidad de energía eléctrica

Con un mínimo de personal como se muestra a continuación.

* 10 Camarográfos
* 2 Ingenieros
* 2 Auxiliares
* 1 Electricista.

5.4 VIDEOCONFERENCIA SOBRE REDES LAN

La aplicacion de la videoconferencia a traves de redes IP es una opcion muy atractiva, pero hasta hace algún tiempo muy poco accesible. Si se esta utilizando internet o la intranet corporativa, la videoconferencia significa poder usar el lenguaje corporal y expresiones faciales para que la gente con la que se habla pueda entender mejor sin levantarse de su propio lugar, pero esto debe ser en tiempo real.

Los dos programas de videoconferencia para Windows 95 demostraron que es posible tener una comunicación multimedia instantanea y más conveniente, sobre internet o sobre la intranet corporativa, sin embargo es necesario vencer dos obstáculos: la barrera del ancho de banda y la barrera de la facilidad de uso. Además del rendimiento poco adecuado, sobre enlaces de 28.8 Kbps, la videoconferencia necesita mucho ancho de banda y también que los sistemas esten bien configurados. Debido a que se basa en una gran variedad de hardware, software y tecnologías de red aún se esta lejos de conseguir que sea tan simple como levantar la bocina de un teléfono y entablar una conversación.

La especificación H.323 de la Unión Internacional de Telecomunicaciones, es un estándar independiente del fabricante, el cual define como debe de ser la transmisión de datos desde una aplicación de conferencia audiovisual, sobre una red abierta utilizando protocolos de transporte estándares como TCP/IP.

Dos de los productos que se apegan o están por apegarse a este estándar de conferencia audiovisual son el CU-SeeMe versión 3.0 de White Pine software y el NetMeeting versión 2.0 de Microsoft. Dentro de la herramientas colaborativas que hacen que la videoconferencia con estos nuevos clientes sea aún más útil se incluyen los anteriormente mencionados pizarrones electrónicos, que ofrecen un espacio limpio en el cual todos los participantes pueden utilizar aplicaciones compartidas que permiten a los participantes ver la misma ventana de la aplicación mientras que uno de ellos la manipula, transferencia de archivos y diálogo.

El software colaborativo de IP basado en estándares, todavía es una tecnología muy nueva y requiere de una plataforma con una PC muy bien equipada y configurada con conectividad de IP.

La interoperabilidad es el principal objetivo, no importa que tan buena sea una solución propietaria de videoconferencia, si puede interactuar con otras soluciones de videoconferencia, no le será nada útil. A pesar de que los primeros en implementar afirmaron estar apegados al H.323, nunca puede interoperar CU-SeeMe con NetMeeting, ya que la capacidad de ineroperatibilidad H.323 cliente a cliente del CU-SeeMe no estuvo disponible sino hasta mucho después. Esta capacidad de habilita a través del producto Meeting Point de videoconferencia de White Pine para el servidor. NetMeeting no tuvo problema en interactuar con otros productos, pero CU-SeeMe necesita del Meeting Point para soportar videoconferencias multipunto,

multiventanas con otros clientes basados en H 323 La configuracion es un problema muy grande, es necesario que todo este junto, las entradas de video, las entradas y salidas de audio, el software de red de IP adecuado, así como el propio software de la videoconferencia, sin embargo después de la instalacion es necesario afinar algunos detalles, en particular cuando se tiene que trabajar con firewalls y manipular el consumo de ancho de banda en conexiones de LAN internas

Los aspectos de interoperatibilidad van más allá de la compatibilidad entre los clientes. la videoconferencia es una aplicación compleja que además tiene que interoperar con otras piezas de la red El *estándar H.323 para comunicación audiovisual multipunto, complica las cosas para los firewalls, ya que utiliza* dos conexiones del protocolo para control de transmision TCP, asi como datagramas del protocolo de Datagrama de Usuario (UDP por User Datagram Protocol) para establecer y mantener una sola conexión (TCP es un protocolo de transporte que crea un circuito virtual; UDP es un protocolo de transporte no *orientado a conexión) T.120, es el estándar para conferencias de documentos multipunto y para compartir* datos, requiere un sólo circuito TCP, a diferencia del H 323, por lo tanto las conferencias de datos no tienen los mismos problemas con el firewall como lo tienen las comunicaciones de audio y video. A menos de que firewall explícitamente permita videoconferencias H.323, el administrador tiene que abrir la manera manual de los puertos TCP y UDP que se usaran para conferencias.

Problemas de rendimiento

La latencia, el retraso en la recepción de la señal después de que fue enviada, puede verdaderamente acabar con a aplicaciones hambrientas de ancho de banda como las de video en tiempo real: Un retraso de más de una fracción de segundo puede distorsionar seriamente la recepción. El NetMeeting de Microsoft tiene un mecanismo de tono automático para compensar las variaciones del ancho de banda CU-SeeMe utiliza la corrección de errores hacia adelante para compensar la pérdida de paquetes en internet y utiliza el método del intercalar para reducir la pérdida real de datos cuando se tiran paquetes.

Debido a que los flujos de audio y video demandan mucho ancho de banda, los productos de videoconferencia deben de comprimir los datos en un extremo final. Este proceso de compresión y descompresión reduce la calidad del original y esto se manifiesta de varias maneras como sonido estático y discontinuo y el video aparece como pixeles en desorden.

Los codecs son el software que comprime y descomprime estos datos y la selección de un codec en vez de otro involucra puntos en los cuales se tiene que escoger entre calidad o rendimiento, la calidad de ancho de banda que tenemos disponible y la necesidad de interoperatibilidad.

Estos productos tambien utilizan codecs distintos para asignar determinada cantidad de flujo de datos a la transmision del audio lo mejor posible sin afectarla calidad del video Cualquiera que haya utilizado un telefono de altavoz barato, sabe que solo una persona puede hablar al mismo tiempo y cuando la persona de un extremo esta hablando, los del otro extremo solo pueden escuchar, lo que en otros terminos es comunicación half-duplex. La conferencia a manos libres, full-duplex que ofrecen CU-SeeMe y NetMeeting, permite a varios participantes escuchar y hablar al mismo tiempo, pero con el costo de ancho de banda adicional.

Una manera de manejar el ancho de banda es utilizar productos conocidos como "guardianes" o "gatekeepers", los cuales permiten a los administradores del sistema monitorear los flujos de audio y video. A diferencia de los gateways que rutean trafico de H.323, los gatekeepers monitorean y limitan el ancho de banda de la red y permiten a los administradores restringir el BW utilizado por las aplicaciones de audio y video, existen otras variantes que afectan el rendimiento, como, conectar la cámara a un pizarrón de captura de vídeo es mucho más eficiente con los recursos del sistema, que enlazarse a través de un puerto paralelo y que la mezcla de redes LAN y líneas telefónicas en la misma conferencia hicieron el sistema de pruebas más lento.

Los usuarios pueden restringir información de sus contactos en un servidor de localidades, como el de Four11 y el Microsoft el ILS (por Internet Locator Server). Eventualmente ILS estará integrado a los servicios de directorio de Microsoft, Active Directory Services.

El software del cliente le notifica al servidor cosas como el cambio de una dirección IP cada vez que el usuario se conecta. El uso de un servidor de directorio no es siempre necesario y puede quitar mucho tiempo Algunos de los directorios tienen que entregar su base de datos completa cada ves que se hace una consulta

Estándares de conferencia

Los estándares de la ITU, mantienen las siguientes 4 importantes familias de especificaciones para las tecnologías de conferencia.

ITU H.320 fue adoptado en 1990 y se refiere a un conjunto de estándares para establecer conferencias multipunto con audio y vídeo, sobre redes digitales conmutadas. H.320 establece estándares para conferencias sobre enlace ISDN, estableciendo un fundamento para los sistemas de conferencias basados en un salón, los cuales serán muy utliles para organizaciones que puedan pagar los altos costos. ITU T.120 es parte de este conjunto.

ITU T 120 especifica protocolos para usarse en conferencias multipunto de documentos y de compartición de datos Incluye funciones como compartición e intercambio de imagenes, conferencia con pizarrón electronico y transferencia de archivos Algunos de estos protocolos, sobre todo los que definen como deben de interactuar aplicaciones en la videoconferencia y lo que deben de hacer, ya fueron ratificados. *Otros protocolos de este grupo, en particular aquellos que definen el control de la conferencia y los servicios* de reservación, no se han terminado

El estándar ITU H.323 se refiere a comunicaciones audiovisuales multipunto Como una extensión de H.320, especifica servicios sobre ISDN y enlaces directos con servicios telefónicos viejos (POST por Plain Old Telephone Services) así como sobre redes IP LAN's Ethernet.

El estándar IUT H 324 se refiere a compartir audio, video y datos utilizando conexiones punto a punto con modems analógicos sobre POTS; esta especificacion es análoga al grupo H.320 para conferencias sobre ISDN y circuitos de datos conmutados.

Es el más completo y avanzado servicio de transmisión de punto a punto o multipunto de voz, datos e imágenes en vivo, para intercomunicar o interactuar a dos o más grupos de personas que se encuentran a grandes distacias entre si, ya sea en el mismo pais o en el extranjero.

Gracias a la introducción en México de la Red Digital Integrada, nos colocamos a la altura tecnológica de los apises más avanzados. Existen ya cerca de 1000 salas en 30 paises distintos, cuentan con la posibilidad de tratar una situación frente a frente, a pesar de las grnades distancias.

Dicho sistema de transmisión posee la caracteristica de ser 100 % confidente, lo cúal se asegura por medio del encriptamiento de imágen que hace accesible su recepción únicamente en el o los lugares programados.

5.4 1 BENEFICIOS

- Eleva productividad
- Agiliza la toma de decisiones
- Mejora notablemente la comunicación corporativa
- Reduce costos de viaje y tiempo
- Optimiza el uso de la red digital integrada

5.4.2 APLICACIONES

Las videoconferencias son útiles para toda empresa con necesidades de comunicacion audiovisual interactiva como

- Instituciones financieras
- Dependencias de gobierno
- Universidades y escuelas
- Cadenas hoteleras
- Consorcios
- Empresas privadas
- Hospitales
- Compañías aseguradoras
- Etc

Y sus posibilidades no tienen limite:

- *Investigación y desarrollo*
- Promoción y publicidad
- Actualización
- Manofacturas
- Reclutamiento y selección de personal
- Transferencia de información
- Negociaciones diversas
- *Transmisión de operaciones quirurgicas, seminarios médicos*
- Capacitación y entrenamiento
- Juntas regionales
- Revision de presupuestos
- Conferencias de prensa
- Etc.

El servicio de videoconferencia utiliza como medio de transmisión digital recursos como fibra óptica, satélite o radio digital y salas debidamente acondicionadas con equipos CODECS que codifican y decodifican imágenes; y accesorios tales como camaras de documentos, videograbadoras, proyectores de transparencias, pizarrones eléctronicos, computadoras personales, etc.

La introduccion de este servicio tiene como objetivo mostrar los alcances y beneficios del uso de la videoconferencia, así como establecer una operación comercial

TELMEX a traves de la red de Sprint International introduce el sistema videoconferencia en mas de 1200 salas distribuidas en la union Americana y el resto de l mundo

5.4.3 TARIFAS VIDEO ENLACE DIGITAL (DIGITAL LINK)

No incluye IVA sujetas a cambio sin previo aviso

Tarifas por servicio nacional·

Velocidad distancia (km)	748kbps	2048kbps
000-300	$110.00	$215.00
301-600	$150.00	$300.00
601.... .	$200.00	$400.00

Tarifa multipunto por media hora

Velocidad	748Kbps	2048Kbps
	$550 00	$1100.00

Tarifa México - USA (*)

Tarifa punto punto por hora.

384Kbps	748Kbps	2048Kbps
$1280.00	$1430.00	$1650 00

(*) Incluye tarifa de USA

Tarifa para servicio mundial

Tarifa punto a punto por hora (**)

384Kbps	748Kbps	2048Kbps
$780 00	$780 00	$900 00

(**) A estas tarifas hay que añadir el pago correspondiente al enlace del pais o los paises con los que se va a llevar a cabo la videoconferencia más el pago por el transito en USA

Tarifa por uso de sala:

$175.00 USD por hora

CONCLUSIONES

El presente trabajo trata de reunir dos temas que actualmente son fundamentales dentro del procesamiento de la información dentro de las telecomunicaciones El avance de la tecnologia ha significado para el ser humano, la facilidad sobre todo, de alcanzar una de las metas primordiales que es la comunicacion.

El alcance de las telecomunicaciones, ha llegado a tal magnitud, que surgen nuevas necesidades continuamente dentro del mismo contexto; al incrementarse la velocidad de comunicación tambien aumenta el volumen de los datos a transmitir y esto conlleva a la creación de técnicas para que la información a transmitir sea confidencial y confiable.

Dentro de estas técnicas, se encuentra la compresión, que como ya se trato en el desarrollo de este material, nos permite optimizar el vehículo de transporte de la información. La compresión sin lugar a dudas, ha convertido los grandes volúmenes de información en paquetes fáciles de transportar sin afectar la velocidad a la que viaja la información; la gran ventaja de la compresión, hace que se pueda manejar información tan compleja como la que contiene imágenes fijas, o en movimiento.

El vídeo en movimiento, como se mostró en este trabajo, requiere de grandes volúmenes de información, por lo que la compresión se vuelve imprescindible. Dentro de la compresión, existen diferentes técnicas, y esto facilita el trabajo por que nos da la oportunidad de escogerla adecuadamente de acuerdo a cada necesidad que pueden ser sin lugar a dudas muy diversas ya que dependen de cada usuario. Por tanto, es necesario explicar de alguna manera alguna de las opciones que existen para la transmisión de información digital, así como dar a conocer las grandes posibilidades y el gran ahorro económico que aporta la compresión.

Pero para que toda la información sea confiable y llegue a su destinatario sin problemas, se tienen que enfrentar algunas dificultades en la transmisión de la información, como es la seguridad de la misma, esto es; el que exista la posibilidad de enviar información vital y enteramente confidencial con la completa convicción de que únicamente el destinatario tendrá acceso a tal información. Deacuerdo a estas necesidades es por lo que se plentean en este trabajo algunas de las técnicas de encriptamiento de la información para lograr un alto grado de confidencialidad.

El encriptamiento, ofrece la facilidad de transportar grandes cantidades de información sin temor de que pueda ser interferida por alguien o algo. Esta necesidad hace del encriptamiento una herramienta de gran importancia, en este trabajo se trata de dar un enfoque más importante sobre la transmisión de vídeo digital.

En resumen, las necesidades a nivel macro, es decir, de grandes volumenes de informacion, que como ya se a ha mencionado, el video es uno de los que cumple con estas caracteristicas, ha llevado a la creación de técnicas que nos garantizan tanto que la información llegara completa como segura al destinatario final

El video en movimiento, es actualmente un medio a través del cual se unen paises o naciones, que a pesar de las grandes distancias que lo separa pueden estar unidos e interactuar entre si para diferentes fines, buscando la mayor rapidez y confiabilidad en la informacion que se transmite, para que esta llegue segura y sin contratiempos.

El campo de las comunicaciones, es muy extenso, y en la actualidad se ha vuelto indispensable el manejo de información, através de nuevas tecnologías; es por eso, que al adentrarnos en este tema, logramos comprender la importancia, tanto de la seguridad como la capacidad de información que se maneja, la aplicación de nuevas tecnologias dentro de este campo, se ha vuelto cotidiano, y el conocer uno de tantos avances que hay en la actualidad significa un paso hacia el inmenso mundo de la ciencia y tecnología actual.

Con el presente trabajo nos pudimos dar cuenta del manejo de una técnica importante, tanto para compresión como para encriptamiento de video que hoy por hoy significa desarrollo industrial y tecnológico, y por consecuencia un mayor beneficio económico.

El lograr encontrar información de éste tipo y conjuntarla dentro de un mismo contexto nos permite hacer uso de una herramienta más concisa y fidedigna en cuanto a la forma de transmitir información, en este caso imagen de una forma mas digerible y concreta.

GLOSARIO

CCIR	Consejo Consultivo Internacional de Radio
CCITT	Consejo Consultivo Internacional de Telecomunicaciones y Telegrafia
DCT	Codificación por transformacion
DPCM	Modulación Diferencial de Pulsos Codificados
PIXEL	Unidad Minima de una imagen.
RDI	Red Digital Integrada.
SCT	Secretaria de Comunicaciones y Transportes.
SVH	Sistema Visual Humano
TKL	Transformada Karhumen-Loeve
TRF	Transformada Rápida de Fourier.
TDC	Transformada Directa de Coseno.
TWH	Transformada de Walsh-Hadamard.
CBT	Codificación por Bloques Truncados.
ENTROPIA	Capacidad para comprimir datos con una alta probabilidad de aparición de cada dato
BW	Ancho de Banda.
LSI	Integración de Escala Extendida.
FSC	Frecuencia Subportadora de Color.
BCH	Técnica de Correción de Errores.
RF	Radio Frecuencia.
DTE	Equipo Terminal de Datos.
DCE	Equipo de Comunicación de Datos.
INTERNET	Red entre Computadoras de Diferente Tecnología.
TDM	Multiplexaje por División de Tiempo.
OSI	Interconexión de Sistema Abierto.
ANSI	Instituto Nacional Americano de Normalización.
MTU	Unidad Máxima de Transferencia.
HOST	Unidad Anfitriona de Procesamiento de Datos.

BIT	Unidad Mínima de Información
LAN	Red de Area Local.
WAN	Red de Area Extendida.
BLD	Banda Lateral Derecha.
BLR	Banda Lateral Residual.
UTP	Unshielded Twisted Pair (Par de Cable Trenzado Blindado).
STP	Shield Twisted Pair (Par de Cable Trenzado sin Blindar).
RJ-11	Conector Modular Telefónico para Cable de Dos Pares.
RJ-45	Conector Modular Telefónico para Cable de 4 Pares.
NTSC	Señal de Vídeo Analógica usada en E.E.U U.
TRF	Transformada Rapida de Fourier.
TDF	Transformada Discreta de Fourier.
MPEG	Grupo Experto de Vídeo en Movimiento.
JPEG	Grupo Experto de Vídeo Fijo
DCT	Transformada Discreta de Coseno
ASIC	Aplicación Específica de Circuitos Integrados
DSP	Procesador de Señal Digital.
CODEC	Reducción del Rango de Transmisión de Intertrama.
TRIDEC	Reducción del Rango de Transmisión de Intertrama para 3 parámetros.
PAL	Norma de Compresión para Señales de Vídeo
FDM	Multiplexaje por división de Frecuencia.
HTTP	Protocolo de Transferencia de Hipertextos.
FTP	Protocolo de Transferencia de Archivos.
SSL	Protocolo de Seguridad de Transferencia de Hipertextos.
SCH	Subportadora Horizontal
ILS	Servidor Ubicado de Internet

BIBLIOGRAFIA

Lathi B P., ***Introducción a la teoría de sistemas de comunicación***, Ed. Limusa, Mexico 1993

Don L. Cannon y Gerald Luecke, ***A fondo: Sistemas de Comunicaciones***, Ed., Anaya Multimedia, Madrid 1988.

Ferrel G. Stremler, ***Sistemas de comunicación***., Ed., Alfa-omega , México ,1989

P.H. Smale, ***Sistemas de telecomunicaciones***, Ed., Trillas, México 1993.

Mischa Shwartz, ***Transmisión modulación y ruido*** Ed. Ra-ma México 1998

Kahn, D., ***The Codebrakers,Macmillan Publishing Company***, New York, 1967.

Diffie, W., and Hellman, M. E., "**Privacy and Authentication: An Introduction to Cryptography**," Proc. IEEE, vol. 67 no. 3, Marzo 1979

Denning, D. E. R., ***Cryptography and Data Security***, Addison-Wesley Publishing Company, Reading, Mass , 1982

Tom Lookabaugh , **Data, *Speech,Image and Video Compression:Principles,Applications and standars***.., Lecture notes. 19990

Netravali and Haskel,***Digital Pictures:Representation and Compresion***, Plenum Press,1988.

Lee and Messerchmitt, ***Digital Comunication***, Kluwer Academic Press, 1988

LSI for Audio and Video Mpeg standars, Nec Research and Develop., Vol, 35 No , 4 Octubre 1994

Feistel, H. "***Cryptography and Computer Privacy***"., Sci. Am., vol. 228 no. 5, Mayo 19773, PP 15-23

Shannon,C.E.,"**Communication Theory of Secrecy Systems**," Bell Syst. Tech. J., vol. 28 Oct. 1949, pp. 656-715