ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

ESTUDIO DEL PROTOCOLO DE STREAMING SMPTE 2110 Y DE LOS MECANISMOS DE SEGURIDAD PARA TRANSMISIÓN DE MULTIMEDIA

MECANISMOS DE SEGURIDAD PARA TRANSMISIÓN DE MULTIMEDIA

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

JOSÉ DARWIN PUPIALES TIPÁN

jose.pupiales@epn.edu.ec

DIRECTOR: MSc. WILLIAMS FERNANDO FLORES CIFUENTES

fernando.flores@epn.edu.ec

Quito, agosto 2023

CERTIFICACIONES

Yo, José Darwin Pupiales Tipán declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

_____

JOSÉ DARWIN PUPIALES TIPÁN

Certifico que el presente trabajo de integración curricular fue desarrollado por José Darwin Pupiales Tipán, bajo mi supervisión.

_____

MSc. WILLIAMS FERNANDO FLORES CIFUENTES
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JOSÉ DARWIN PUPIALES TIPÁN

MSc. WILLIAMS FERNANDO FLORES CIFUENTES

DEDICATORIA

A mi familia, quienes han sido de gran apoyo a lo largo de este viaje académico.

A mis padres, María Tipán y José Pupiales por su paciencia, sacrificio, y por alentarme a conseguir mis metas.

AGRADECIMIENTO

A mis padres por confiar en mí y brindarme los recursos necesarios durante mi vida universitaria.

A todas las personas que contribuyeron de manera significativa en el desarrollo y éxito de este trabajo de integración curricular.

A mi director del presente trabajo de integración, su experiencia y conocimientos han sido fundamentales para la realización de esta investigación.

ÍNDICE DE CONTENIDO

RESUMEN

La transmisión de contenido multimedia es esencial en una sociedad digital cada vez más interconectada, Desde compartir fotos y videos hasta realizar videoconferencias, dependemos cada vez más de la transferencia de datos multimedia. Sin embargo, esta creciente dependencia también plantea preocupaciones en términos de seguridad y protección de la información transmitida.

El presente trabajo consiste en describir algunos de los mecanismos de seguridad para la transmisión de multimedia. En el primer capítulo se presentará una breve reseña sobre multimedia y su evolución en la transmisión. Posteriormente, se abordará las diferentes categorías de servicio de Video-on-Demand tales como per-per-view, broadcast, casi video-on-demand, entre otros. La gestión de derechos digitales también es un tema expuesto en esta sección junto con la importancia de los derechos de autor y las soluciones técnicas para proteger el contenido multimedia. Finalmente, se explorará las industrias con interés en la protección de contenido digital.

En el capítulo 2 se presentará los mecanismos de protección ampliamente utilizados en la transmisión de contenido multimedia. Se examinará el empleo de técnicas como el cifrado y la codificación, las cuales desempeñan un papel fundamental en la preservación de la confidencialidad y la integridad de los datos transmitidos. Asimismo, se abordarán las soluciones CAS, que ofrecen una capa adicional de protección al controlar el acceso y la autenticación de los usuarios autorizados al contenido multimedia.

En el tercer capítulo se muestra la retroalimentación y el escenario de aplicación de los mecanismos de seguridad presentados para la transmisión de contenido multimedia.

PALABRAS CLAVE: multimedia, compresión, gestión de derechos digitales, marca de agua, cifrado, codificación, seguridad, privacidad, confidencialidad, control de acceso.

ABSTRACT

Multimedia content transmission is essential in an increasingly interconnected digital society. From sharing photos and videos to video conferencing, we are increasingly dependent on the transfer of multimedia data. However, this growing dependency also raises concerns in terms of security and protection of the information transmitted.

The present work consists of describing some of the security mechanisms for the transmission of multimedia. In the first chapter, a brief review of multimedia and its evolution in transmission will be presented. Subsequently, the different categories of Video-on-Demand service such as per-per-view, broadcast, almost video-on-demand, among others, will be addressed. Digital rights management is also a topic discussed in this section along with the importance of copyright and technical solutions to protect multimedia content. Finally, industries with an interest in digital content protection will be explored.

In chapter 2, the protection mechanisms widely used in the transmission of multimedia content will be presented. The use of techniques such as encryption and coding, which play a critical role in preserving the confidentiality and integrity of transmitted data, will be examined. Likewise, CAS solutions will be addressed, which offer an additional layer of protection by controlling access and authentication of authorized users to multimedia content.

Third chapter shows the feedback and the application scenario of the security mechanisms presented for the transmission of multimedia content.

KEYWORDS: multimedia, compression, digital rights management, watermark, encryption, coding, security, privacy, confidentiality, access control.

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

La integración de las tecnologías de la información y la comunicación ha generado la aparición de diversas plataformas de medios que ofrecen una amplia gama de servicios a una comunidad de usuarios. Estas plataformas se caracterizan por ser medios que permiten la transferencia de información o cualquier otro objeto como bienes y servicios. Los medios pueden ser considerados como espacios de información y comunicación que, gracias a los avances tecnológicos e innovaciones en las TIC, facilitan la creación, gestión e intercambio de contenido entre una comunidad de agentes, que pueden ser organizaciones, seres humanos o incluso agentes artificiales (como agentes de software). [1]

En la década de 1990, se consideraba que las telecomunicaciones, los equipos de oficina, los productos electrónicos de consumo, los medios y las computadoras eran industrias independientes y diferentes, cada una con su propia oferta de servicios y formas de entrega. Sin embargo, a medida que la computadora se convirtió en una herramienta fundamental para el manejo de información, las empresas empezaron a utilizar tecnologías digitales emergentes, realidad virtual y otras tecnologías para expandir sus ofertas de servicios y los límites entre las diferentes industrias comenzaron a desaparecer.

La convergencia tecnológica ha resultado en la fusión de distintas industrias y sectores, como las telecomunicaciones, la televisión digital y la informática, en un solo mercado que ofrece una amplia gama de servicios y tecnologías a diferentes usuarios. Este proceso ha llevado a la creación de un gran mercado TIC, donde las diferentes tecnologías, servicios y categorías de usuarios se combinan.

Los servicios digitales han cambiado la forma en que las personas consumen y comparten contenido multimedia. Las imágenes y videos digitales se han vuelto cada vez más populares en nuestra sociedad, muchas aplicaciones y servicios dependen de la seguridad y privacidad con gran confiabilidad en el almacenamiento y transmisión de estos datos. En particular, los servicios de TV de paga, videoconferencias confidenciales y sistemas de imágenes militares son solo algunos ejemplos de aplicaciones que requieren una seguridad confiable para sus datos multimedia

El rápido progreso de Internet ha aumentado la importancia de la seguridad en el contenido multimedia. En los últimos años, cada vez más dispositivos electrónicos de consumo, como teléfonos móviles, han comenzado a proporcionar funciones adicionales para guardar e intercambiar mensajes multimedia, lo que ha hecho que este tipo de contenido cobre mayor importancia que los textos convencionales. Como resultado, se requiere una protección de privacidad sólida y confiable para garantizar la seguridad de los usuarios.

El uso de técnicas de protección como el cifrado de contenido multimedia se ha vuelto cada vez más importante ya que esto ayuda a frustrar los ataques maliciosos de terceros no autorizados y garantiza que la información se mantenga confidencial durante el almacenamiento y la transmisión. En este sentido, el propósito de la presente investigación es mostrar los distintos mecanismos que contribuyen a la protección del contenido multimedia. [2]

1.1 Objetivo general

Presentar una descripción general de los mecanismos de seguridad y las técnicas de cifrado usadas en la transmisión de multimedia para proteger la confidencialidad y la integridad de la información.

1.2 Objetivos específicos

1. Analizar la seguridad en la transmisión de multimedia en el contexto de la privacidad y el control de acceso de los usuarios.
2. Elaborar un estudio bibliográfico de los distintos mecanismos nuevos y existentes que se usan en la protección para la transmisión de multimedia.
3. Identificar los mecanismos de seguridad apropiados para las aplicaciones de multimedia en función de su contenido.

1.3 Alcance

El trabajo de integración curricular se enfocará en presentar los mecanismos de seguridad para transmisión de multimedia. Se realizará una descripción de las técnicas y soluciones utilizadas en la protección de contenido multimedia con el objetivo de entender cómo se protege el contenido digital durante su transmisión.

La seguridad en la transmisión de multimedia es fundamental para garantizar la privacidad de la información y evitar posibles ataques de terceros. Por esta razón, se abordarán diferentes tecnologías y algoritmos utilizados en la protección de contenido, como los sistemas de gestión de derechos digitales (DRM), el cifrado, la marca de agua, los sistemas de autorización de acceso condicional (CAS) y los sistemas de codificación de video.

El presente trabajo no cuenta con una implementación práctica ya que se centrará en proporcionar una visión sobre la importancia de la seguridad en la transmisión de multimedia y las herramientas utilizadas para proteger el contenido multimedia. La investigación a presentar utilizará la información disponible sobre algoritmos, protocolos,

soluciones y técnicas para la protección de contenido multimedia. Para facilitar la comprensión de los conceptos, se emplean las mismas notaciones y definiciones que se encuentran en la fuente original. De esta manera, se busca establecer un lenguaje común en el tratamiento de los temas abordados.

1.4 Marco teórico

1.4.1 Fundamentos de multimedia

Definición de multimedia

Frecuentemente, la palabra "multimedia" es utilizada por diversas personas con enfoques y perspectivas muy diferentes, llegando incluso a ser opuestos. En el caso de un proveedor de computadoras personales, el concepto de multimedia se referirá a una PC con capacidad de sonido, una unidad de DVD-ROM y, posiblemente, una mejora en los microprocesadores de tal forma que permita procesar instrucciones multimedia adicionales. Por otra parte, un proveedor de entretenimiento podría entender como multimedia a un servicio de televisión por cable interactiva que cuente con cientos de canales digitales, o un servicio similar a la televisión por cable que se entregue a través de una conexión a Internet de alta velocidad.

Multimedia es una plataforma informática, herramienta de software o inclusive una red de comunicaciones que combina múltiples elementos, entre los que se incluyen texto, imágenes, dibujos, animación, video, sonido y muy probablemente interactividad de algún tipo. Los sistemas multimedia representan una innovadora forma de comunicación que aprovecha dichos elementos, en un entorno único. En este enfoque se unen las diversas aportaciones de cada medio con el único fin de transmitir un concepto al usuario. [3] [4]

1.4.2 Compresión de datos

La compresión de datos es uno de los desafíos más importantes y evidentes al utilizar multimedia. Es esencial que la compresión de datos sea eficiente y rápida para evitar tasas de datos tan altas que generen problemas en la red y en el almacenamiento, especialmente si se busca compartir estos datos. Asimismo, la velocidad de entrada y salida del dispositivo de almacenamiento también se ve afectada por la cantidad de datos que se debe transferir. La compresión depende de la aplicación, de la capacidad de visualización de la computadora y la pantalla, y el ancho de banda disponible para la transmisión. Por lo general los datos de audio y video deben ser comprimidos antes de que sean almacenados o previo a su transmisión. [5]

JPEG

Es considerado como uno de los estándares más populares para la compresión de imágenes. JPEG utiliza una técnica de compresión con pérdida que elimina detalles redundantes e información visualmente menos importante de la imagen original para reducir su tamaño de archivo, lo que permite ahorrar espacio de almacenamiento o reducir el tiempo de descarga en línea.

JPEG2000

Es una evolución de JPEG que ha sido mejorado con la finalidad de proporcionar una calidad superior en compresión con perdida y sin perdida en un solo flujo de bits. Este formato ha sido utilizado en diversas aplicaciones, como internet, escaneo, fotografía digital imágenes médicas, biblioteca digital, etc.

MPEG

Es un estándar de compresión de audio y video. Es utilizado para permitir la transmisión de audio y video de alta calidad a través de canales limitados como ancho de banda internet y televisión digital. MPEG ha sido actualizado varias veces.

MPEG-1: Se lo utilizó principalmente para la transmisión de video en CD. De los 1.5 Mbps, 1,2 Mbps están destinados a video codificado y 256 kbps se pueden usar para audio estéreo.

MPEG-2: Es un formato de compresión para video de mayor calidad a una tasa de más de 4 Mbps, se utiliza en una amplia variedad de aplicaciones de vídeo, como la televisión digital, DVD, discos Blu-ray y transmisiones de televisión por satélite y cable.

MPEG-4: En este formato además de la compresión, se presta gran atención a la interactividad del usuario, su tasa de bits cubre un amplio rango, entre 5 kbps y 10 Mbps. Es ampliamente utilizado en la transmisión de video por internet, videoconferencias, videojuegos y aplicaciones de realidad virtual, entre otros.

MPEG-7: El objetivo principal de este formato es satisfacer la necesidad de recuperación basada en contenido audiovisual en aplicaciones como bibliotecas digitales. MPEG-7 no se enfoca en la compresión de los datos en sí mismos, sino en la creación de una descripción precisa y completa del contenido multimedia. [6]

1.4.3 Evolución de las aplicaciones multimedia

En los inicios de los años 2000, se inició una revolución en los medios digitales con tecnologías básicas como los videojuegos, las enciclopedias electrónicas y los discos láser,

lo que convirtió a la multimedia en un dominio de estudio emergente y un campo novedoso. Las tecnologías actuales, como la televisión interactiva, las bibliotecas digitales y las videoconferencias, han sentado las bases para nuevos desarrollos tecnológicos.

En la actualidad, varias industrias, incluyendo empresas de televisión por satélite, telefonía, comunicación, estudios de cine, software, compañías discográficas, canales de cable, proveedores de servicios de internet e informática, están involucradas en el sector de multimedia. [7]

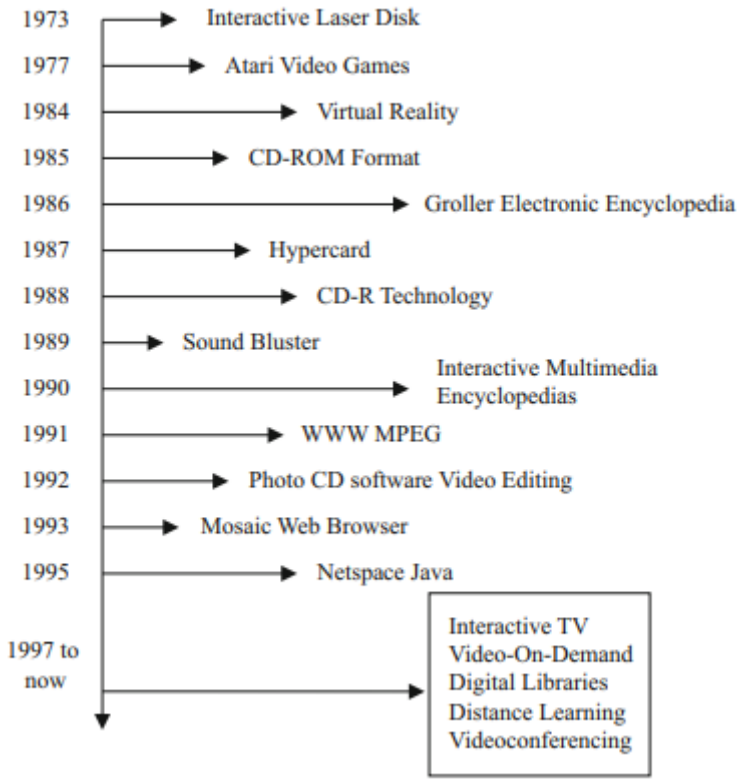


Figura 1.1 Línea de tiempo de las aplicaciones multimedia. (Fuente: [7])

1.4.4 Transmisión de multimedia

En la transmisión multimedia, los datos multimedia se envían desde el remitente al receptor después de que se cifran o se descifran en línea o fuera de línea, la eficacia del cifrado puede ser alta o baja. Sin embargo, el ancho de banda de transmisión suele ser limitado, lo que requiere que el cifrado multimedia no cambie la compresión. [3]

1.4.5 Categorías en el servicio de Video-on-Demand

Con el fin de satisfacer las diversas necesidades de un sistema de video-on-demand (VOD) a gran escala, se han propuesto varios diseños que se adaptan a la naturaleza de los distintos servicios de video. Estos servicios pueden clasificarse en diferentes categorías en

función del grado de interactividad permitido y de las políticas de programación de entrega de datos aplicadas.

1. Broadcast (No-VoD): Este servicio sigue el modelo tradicional de televisión donde el usuario es pasivo y no tiene control, solo puede seleccionar un programa específico del sistema.

2. Pay-per-view (PPV): Este servicio es similar al modelo de televisión por cable, donde el usuario se registra y paga por programas específicos en horarios determinados. El usuario no tiene control sobre la sesión de video.

3. Casi video-on-demand (N-VoD): Cuando varios usuarios solicitan el mismo video, se ofrece una transmisión de video. Los usuarios pueden seleccionar cualquier video en cualquier momento, pero el servidor central determina la hora de inicio del servicio, Dado que varios canales pueden desviar el mismo programa en diferentes momentos los usuarios pueden cambiar entre estos canales para realizar funciones básicas como avance y retroceso del contenido.

4. Quasi video-on-demand (Q-VoD): Este sistema es similar al N-VoD, pero se agrupa a los usuarios en función de umbrales de interés, lo que les permite realizar actividades básicas de control temporal cambiando a un grupo diferente.

5. Verdadero video-on-demand (T-VoD): Es un servicio en el que el usuario tiene el control total sobre la sesión de video, lo que significa que puede solicitar y ver cualquier video en cualquier momento y utilizar funciones completas de VCR. Para proporcionar este servicio, se asigna una transmisión dedicada a cada usuario. [8]

1.4.6 Protección de datos multimedia en la transmisión y el almacenamiento

Antes de la llegada de la tecnología digital, los contenidos se almacenaban y distribuían en formatos analógicos, como las cintas de video. Con la popularización de las videocaseteras, los usuarios pudieron disfrutar de los contenidos en sus hogares, pero también se incrementó el riesgo de copia no autorizada. En la actualidad, se han implementado medidas de protección en los dispositivos electrónicos de consumo para prevenir la piratería de contenido analógico.

La llegada de las tecnologías digitales ha permitido la creación de herramientas para realizar copias exactas de contenido original a través de la representación digital de datos. Con el alcance de la distribución digital a través de Internet, se ha creado un problema crucial de protección de contenido multimedia digital que requiere soluciones inmediatas.

La evolución de las tecnologías de almacenamiento y comunicación digital ha transformado la manera en que se distribuye el contenido multimedia al público. La implementación de estándares de video digital, la disminución significativa de los precios de almacenamiento y el aumento en la capacidad de la red desde 1990 hasta la actualidad han permitido que los sistemas multimedia sean procesados, indexados y compartidos de maneras nuevas y más allá de la representación de solo texto. [2] [9]

1.4.7 Gestión de derechos digitales (DRM)

En el mundo digital en línea, las restricciones legales y tecnológicas pueden ser complementarias en la propiedad del contenido. Los creadores de contenido deben enfrentar decisiones difíciles en cuanto a la apertura o restricción del contenido, ya que cada restricción adicional puede alejar a los consumidores hacia opciones más simples.

La distribución ilegal ha afectado la música y la industria del entretenimiento en general ya que sus creadores no pueden recaudar ingresos o rastrear los diferentes lugares en los que se distribuye su contenido. Para abordar este problema, la industria ha trabajado con matemáticos emprendedores, piratas informáticos y organizaciones de piratas informáticos para proteger el contenido. Las organizaciones también están implementando sistemas de gestión de derechos de autor para controlar la propiedad de su contenido. [10]

1.4.8 Principios fundamentales de DRM

Para implementar una estrategia de DRM efectiva, los propietarios de contenido deben examinar una serie de principios y técnicas. Los tres principios fundamentales de cualquier implementación de DRM son:

1) Proteger la propiedad intelectual, no solo de los medios digitalizados.
2) Desarrollar, proteger y automatizar una cadena de confianza que proteja los medios de principio a fin.
3) Establecer y rastrear la identidad de todos los que acceden al contenido.

1.4.9 Propiedad intelectual en el mundo digital

En el mundo digital, la distribución ilegal de la propiedad intelectual es un problema mayor que en el mundo físico. Los medios digitales son fáciles de duplicar y distribuir en todo el mundo, lo que preocupa a los propietarios de contenido. Además, la sociedad actual tiene actitudes informales hacia la propiedad intelectual, lo que agrava el problema. Para abordar estos problemas, se necesita tanto tecnología como educación social, y la efectividad de

cualquier sistema DRM depende de la capacidad del propietario para detectar y hacer cumplir sus derechos.

Los principios fundamentales de seguridad en el tratamiento de datos son la confidencialidad, integridad, disponibilidad, resiliencia y trazabilidad. Los primeros tres principios son la base de la gestión de riesgos de ciberseguridad, han sido y siguen siendo de gran importancia. Los últimos dos principios, resiliencia y trazabilidad, son implícitos en la práctica de la ciberseguridad por expertos en el área. La implementación de medidas de seguridad adecuadas en cada uno de estos principios permite crear un entorno seguro y confiable para los usuarios y las empresas involucradas en la transmisión de multimedia. [11]

1.4.10 Aspectos éticos y legales en la transmisión de multimedia

La informatización de la sociedad ha aportado mejoras significativas en términos de eficiencia, productividad y acceso a la información, pero también ha generado una serie de nuevos problemas relacionados con la seguridad. La informatización ha permitido la transmisión y el intercambio de grandes cantidades de información multimedia a través de internet, lo que ha hecho que los contenidos estén disponibles para un público más amplio. Sin embargo, esta mayor accesibilidad también ha generado preocupaciones de seguridad, como la piratería de contenido y la violación de derechos de autor.

La piratería de contenido multimedia es un delito que viola los derechos de propiedad intelectual y puede dar lugar a sanciones civiles y penales. Para evitar la utilización no autorizada de una obra, la ley establece el derecho de propiedad exclusivo del autor, conocido como copyright o derecho de autor. Sin embargo, es importante destacar que este derecho no es ilimitado, por lo que tiene un plazo temporal. De esta manera, cuando el plazo de protección del derecho del autor ha transcurrido, la obra deja de ser considerada como propiedad privada y pasa a formar parte del dominio público. El objetivo de esta medida es encontrar un equilibrio entre los derechos del autor y el derecho de acceso a la cultura del público. [12] [13]

1.4.11 Soluciones Técnicas

Ante el incremento de dispositivos de almacenamiento y los canales de comunicación, el contenido multimedia se ha convertido en parte del día a día, sin embargo, en muchas aplicaciones es necesario proteger el contenido multimedia por diversas razones.

Los proveedores de contenido han identificado el cifrado y la marca de agua como dos grupos de tecnologías complementarias para proteger los datos multimedia. Aunque la

incrustación y detección de marcas de agua se consideran en ocasiones análogas al cifrado y descifrado, su propósito es diferente: la marca de agua se utiliza para identificar y rastrear el contenido multimedia, mientras que el cifrado se utiliza para proteger los datos multimedia mediante el cifrado y descifrado de los mismos. [2]

Cifrado

El cifrado es un proceso que transforma el contenido en un formato ilegible mediante una operación matemática reversible, que se realiza utilizando una clave secreta. En la distribución segura de contenido multimedia, se realiza la compresión, empaquetamiento y cifrado del flujo de datos audio/visual. [8]

Figura 1.2 *Medios* de distribución de contenido digital. (Fuente: [2])

En la figura 1.2 se presenta un conjunto de sistemas de distribución de contenido digital que consta de cinco medios principales para llegar a los consumidores: satélite, cable, terrestre, internet y medios pregrabados, como los ópticos y magnéticos.

Los requisitos más importantes para lograr seguridad de extremo a extremo desde el origen hasta el destino final son:

- **Distribución segura de contenidos y claves de acceso:** La información se convierte en datos que no pueden ser entendidos por partes no autorizadas, se usan 2 tipos de cifrado: de clave simétrica y de clave asimétrica.
- **Autenticación de los dispositivos involucrados (transmisor y receptor):** Antes de que pueda tener la transferencia de contenido, el transmisor y receptor deben autenticarse mutuamente para proporcionar evidencia de que están fabricados con la tecnología de protección autorizada.
- **Asociación de derechos digitales con contenido:** Cuenta con dos enfoques que son la utilización de metadatos o marcas de agua.

- **Renovabilidad de los sistemas de protección de contenidos:** Cuando la información secreta de un dispositivo con licencia se ve comprometida, el proveedor de tecnología agrega su identificación a una lista de revocación. Al llegar a los dispositivos autorizados, esta lista hace que los dispositivos pirateados fallen en el proceso de autenticación y sean incapaces de procesar el contenido protegido.

Marca de agua

Una marca de agua digital es un patrón de bits que se inserta en un elemento multimedia, como una imagen digital, un archivo de audio o video. Su presencia debe pasar inadvertida para la percepción humana, pero debe ser detectable con facilidad por medio de un algoritmo específico de extracción. [14]

Las propiedades más importantes de un sistema de marca de agua en aplicaciones como la identificación del propietario, control de copias y control de dispositivos son:

- **Transparencia perceptiva:** La degradación que pueda producir la inserción de una marca de agua en la imagen no debería ser perceptible a simple vista.
- **Robustez:** Se refiere a la capacidad de detectar la marca de agua en un archivo audio/visual después de que se hayan aplicado algunas operaciones comunes de procesamiento de señales.
- **Seguridad:** Es la capacidad de resistir la remoción incrustación o extracción no autorizada
- **Capacidad:** Se refiere a la cantidad de datos que un sistema puede incrustar en un archivo multimedia sin afectar perceptiblemente su transparencia.

1.4.12 Industrias con interés en la protección de contenido digital

Existen tres industrias con intereses particulares en el ámbito de la protección de contenido digital: la industria cinematográfica, la electrónica de consumo y la tecnología de la información. En los últimos tiempos se han desarrollado y aplicado diversos sistemas de protección en las redes de distribución digital que son ampliamente utilizados. Éstos incluyen:

- Sistemas de acceso condicional (CA), utilizados en la distribución satelital, por cable y sistemas terrestres.
- Sistemas de gestión de derechos digitales (DRM) (basados en unidifusión y multidifusión), se los usa para la distribución a través de Internet.

- Sistemas de protección contra copias (CP), enfocados en la distribución dentro de las redes domesticas digitales.

En sistemas de protección de extremo a extremo, el problema principal es determinar si el usuario está autorizado para acceder al contenido deseado. La analogía de controlar el acceso físico a lugares se ha aplicado al mundo digital donde los distribuidores de contenido digital a más de ofrecer servicios confiables a largo plazo deben controlar el uso de los contenidos después del acceso.

1.4.13 Seguridad en sistemas de acceso condicional para satélite cable y distribución terrestre

Un sistema de acceso condicional permite el acceso a servicios basados en el pago y otros requisitos. Los proveedores de servicios entregan diferentes tipos de contenido multimedia utilizando transmisiones satelitales, terrestres o por cable, desde programas de acceso gratuito hasta servicios de pago como PayTV, Pay-Per-View y Video-On-Demand.

Las actividades comunes para este modelo general son:

1. El contenido digital se comprime con el propósito de minimizar los requisitos de ancho de banda.
2. El programa es enviado hacia la cabecera de acceso condicional para ser protegido y empaquetado con permisos acorde a las condiciones de acceso.

3. El flujo de datos audiovisuales se codifica y multiplexa con los mensajes de autorización, que incluyen mensajes de control de autorización (ECMs) y mensajes de administración de derechos (EMMs). Los mensajes de control de autorización contienen claves de descifrado y detalles del programa, mientras que los mensajes de administración de derechos especifican los niveles de autorización. Los servicios se cifran utilizando un cifrado simétrico como DES o algún otro algoritmo que puede ser de dominio público o privado, y la protección de los mensajes de control de autorización es privada para los proveedores de CA por motivos de seguridad.

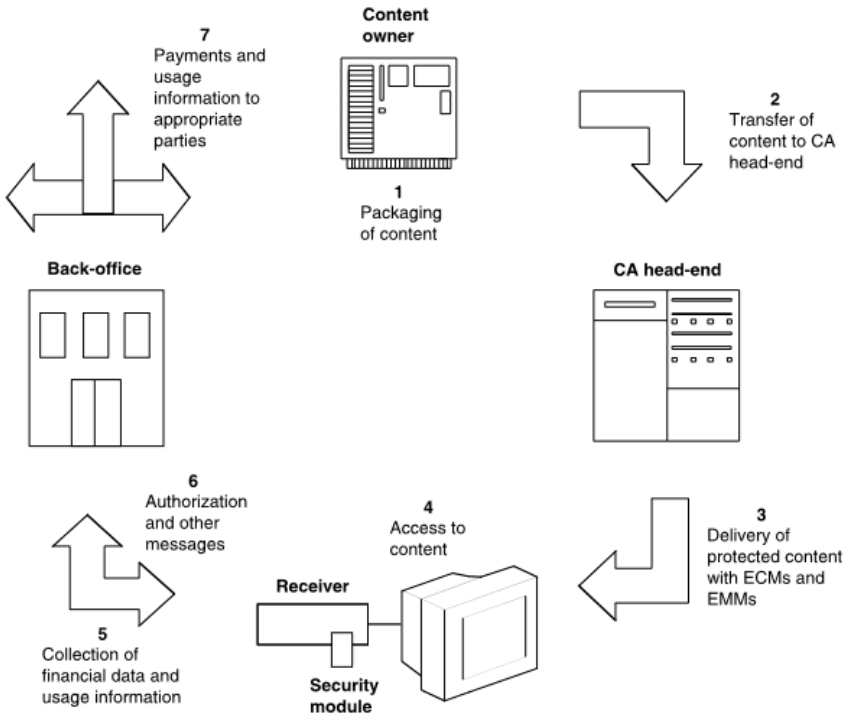


Figura 1.3 Arquitectura del sistema CA. (Fuente: [2])

4. Si Después de que el cliente recibe autorización para ver el programa protegido, el flujo de datos audiovisual se descifra y se envía a la unidad de visualización para ser visto. Un módulo de seguridad extraíble, como una tarjeta inteligente, proporciona un entorno seguro para el procesamiento de mensajes de autorización y otras funciones confidenciales, como la autorización de usuarios y el almacenamiento temporal de registros de compras.

5. El back office es un componente crucial en los sistemas de acceso condicional, ya que se encarga de la facturación, pagos, transmisión de EMMs y aplicaciones de TV interactiva. Se establece un enlace uno a uno con el decodificador a través de un canal de retorno, similar a una conexión telefónica mediante un modem. La seguridad de este canal puede ser definida de forma privada por los proveedores de CA.

6. Las autorizaciones como EMMs y otros mensajes que pueden ser actualizaciones del sistema y de seguridad, se envían al receptor del cliente.
7. La información de pagos y uso es enviada a las entidades correspondientes como proveedores de contenido, operadores de servicios y proveedores de CA.

1.4.14 Seguridad en sistemas DRM para distribución en internet

Un sistema DRM se encarga de la protección, distribución, modificación y aplicación de los derechos relacionados con el uso de contenido digital. En resumen, las funciones principales de un sistema de DRM son:

- Empaquetado de contenido
- Entrega y almacenamiento seguros de contenido
- Prevención de acceso no autorizado
- Cumplimiento de las reglas de uso
- Seguimiento del uso de contenidos

La criptografía es el elemento central en la seguridad de un sistema DRM. Los sistemas utilizan cifrado simétrico, cifrado de clave pública y firmas digitales para funciones relacionadas con la seguridad, incluyendo la entrega segura de contenido, la entrega segura de la clave de contenido y los derechos de uso, y la autenticación del cliente. Aunque los procedimientos pueden diferir en los sistemas DRM, a continuación, se resumen las actividades comunes en un sistema de comercio electrónico compatible con DRM.:

1. El proveedor de contenido encapsula el archivo multimedia, y lo protege mediante un cifrado simétrico. Dentro del paquete puede incluir información sobre el proveedor de contenido, el minorista o la dirección web para adquirir los derechos de uso.
2. El contenido multimedia cifrado se aloja en un servidor para su descarga o transmisión, y puede ser encontrado a través de un motor de búsqueda utilizando el índice de contenido correspondiente.
3. El cliente solicita el archivo multimedia del servidor.
4. Una vez autenticado el dispositivo cliente, el archivo es enviado y en algunos casos se solicita al cliente que complete una transacción de compra. En la autenticación se utilizan comúnmente certificados de clave pública.

5. El cliente adquiere y utiliza el contenido según las condiciones y reglas establecidas.
6. En ciertos momentos, el sistema de pagos puede recopilar registros financieros y de uso de los clientes en ciertos momentos.
7. La confirmación de pago y otros mensajes como información del sistema y seguridad, actualizaciones, entre otros parámetros son entregados al cliente.
8. La información de pagos y uso es compartida con las partes correspondientes, como proveedores de contenido, editores, distribuidores, autores y artistas.

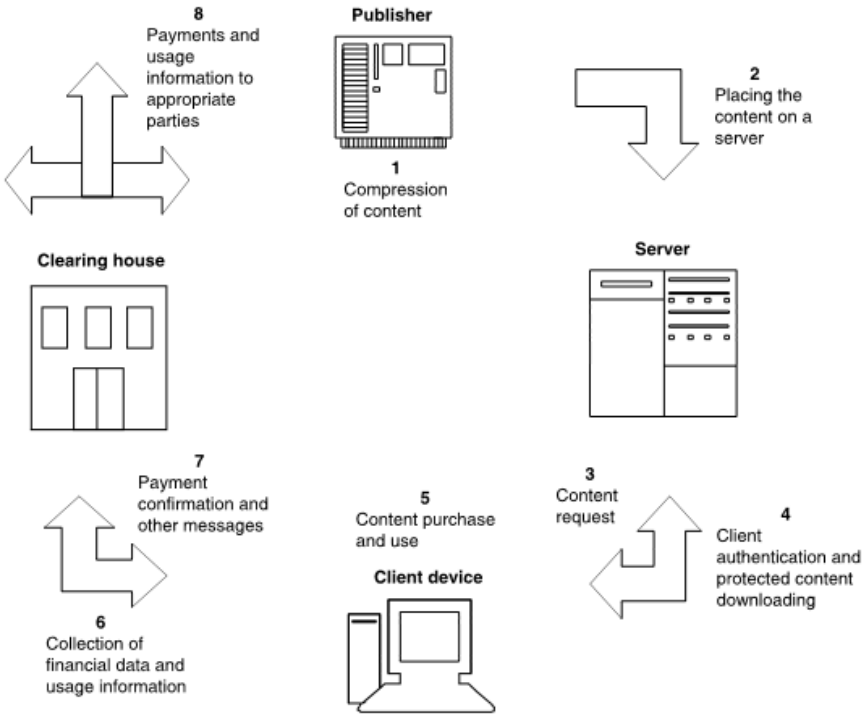


Figura 1.4 Arquitectura del sistema DRM. (Fuente: [2])

Los propietarios de contenido pueden especificar sus modelos de negocio para gestionar el uso del contenido mediante un DRM. Hay una variedad de modelos de venta posibles, como suscripción, pago por uso y superdistribución (reenvío de un contenido que ha sido adquirido previamente hacia otros consumidores). También hay varios escenarios posibles, como la lectura por tiempo limitado de un libro electrónico, la visualización múltiple de una película y la transferencia de una canción a un reproductor de música portátil.

1.4.15 Seguridad en Sistemas Multicast para Distribución por internet

El mecanismo tradicional de comunicaciones multidifusión es IP multicast, donde los miembros son identificados por una dirección de grupo y se utiliza un protocolo de

enrutamiento multicast para optimizar, replicar el mensaje y reenviar copias a los miembros del grupo ubicados en toda la red.

La transmisión multimedia mediante multidifusión IP se ha vuelto popular debido a su eficiencia y ahorro de ancho de banda en la red IP. Cada flujo de video se asigna a una dirección única de Clase D para permitir que varios usuarios vean el mismo contenido al mismo tiempo. Cuando un host solicita unirse al grupo de multidifusión, el enrutador envía el mismo flujo de datos a todos los hosts que han hecho la misma solicitud, lo que permite que todos los miembros del grupo vean el mismo contenido en tiempo real. Cuando un host abandona el grupo, el enrutador deja de enviar la transmisión solo a ese host y continúa transmitiendo a los demás miembros del grupo.[15]

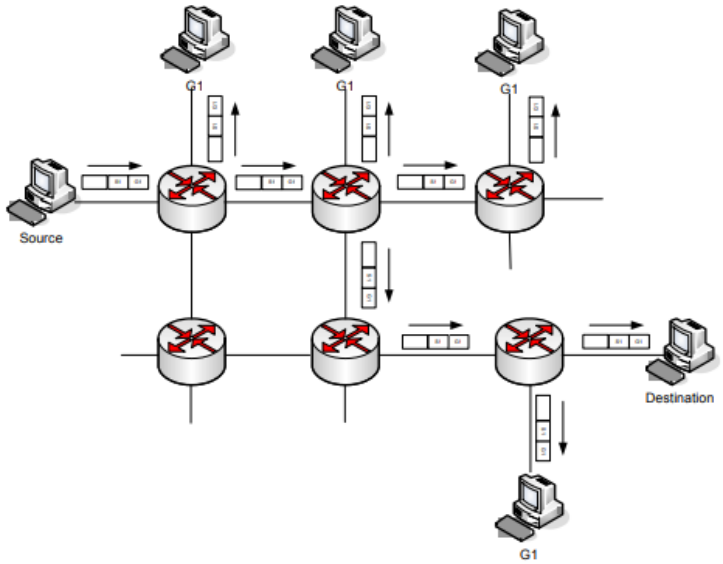


Figura 1.5 Sistema multicast. (Fuente: [15])

1.4.16 Seguridad en Redes Domésticas Digitales

La protección de contenidos en las redes domésticas implica la seguridad y la privacidad de los datos que se intercambian entre los dispositivos digitales, como decodificadores, televisores, reproductores de DVD y computadoras personales. Este problema se enfoca en la protección de los derechos de autor, evitando que el contenido sea pirateado o compartido ilegalmente. Las dimensiones que se deben considerar incluyen la autenticación, la autorización, el cifrado, marcas de agua y la gestión de derechos digitales (DRM). [2]

2 METODOLOGÍA

El presente componente es un trabajo de investigación que se basa en una revisión bibliográfica para recopilar información sobre las diferentes técnicas y soluciones de protección existentes en la transmisión de contenido multimedia. Se consultaron diversas

fuentes confiables y relevantes para identificar las tecnologías y estrategias de seguridad más eficaces para proteger el contenido multimedia durante su transmisión.

El trabajo comienza con una revisión general sobre la seguridad multimedia, que incluye una descripción sobre el nivel de seguridad que debería tener un determinado tipo de contenido multimedia. Posteriormente, se aborda el tema de los cifrados de bloque y de flujo, los cuales son considerados las técnicas más utilizadas para garantizar la privacidad y seguridad de los datos multimedia durante su transmisión. Además, se explican los algoritmos de cifrado simétricos y asimétricos, así como su aplicación en la protección de datos multimedia. Finalmente, se presentan las soluciones propuestas para la protección de contenidos de audio y video,

El enfoque es cualitativo debido a que se fundamenta en la revisión y análisis de información de diversas fuentes documentales. A través de esta metodología, se busca comprender y explicar los diferentes mecanismos de seguridad utilizados en la transmisión de contenido multimedia

Como técnica de recolección de información se examinó diversas fuentes relevantes y confiables, tales como revistas especializadas, artículos científicos y técnicos, informes de investigación, estudios de casos y documentos gubernamentales, entre otros.

2.1 Seguridad multimedia

La seguridad multimedia en general proporciona los métodos utilizados para proteger el contenido multimedia, los cuales se basan principalmente en la criptografía. Estos métodos permiten garantizar la seguridad de las comunicaciones y proteger el contenido contra la piratería mediante la administración de derechos digitales y marcas de agua. Para proteger la comunicación de los datos multimedia, se utiliza la criptografía de clave simétrica estándar, que convierte los datos multimedia en una secuencia binaria y los encripta utilizando un sistema criptográfico como AES o DES. En el caso de los datos multimedia estáticos, es decir que no se encuentren en una transmisión en tiempo real, se pueden utilizar técnicas de encriptación convencionales tratándolos como datos binarios normales.

Mantener la transmisión segura de contenido multimedia de audio y video es un desafío debido a la variedad de restricciones como la velocidad casi en tiempo real. No es suficiente aplicar algoritmos de cifrado como DES o AES a la secuencia binaria de los datos. Se requiere un análisis cuidadoso para determinar el método de cifrado más adecuado para los datos de audio y video.

Para datos de texto y algunas transmisiones multimedia de baja calidad, se puede utilizar el cifrado de paquetes en tiempo real mediante el Protocolo de Transporte Seguro en

Tiempo Real (SRTP), que se basa en AES y cifra todo el flujo de bits multimedia. SRTP es comúnmente utilizado para proteger la privacidad e integridad de las comunicaciones de voz y video en tiempo real a través de redes IP. En el caso de imágenes fijas, también es posible aplicar el cifrado de paquetes utilizando SRTP, lo que permite proteger los datos y evitar que sean interceptados por terceros no autorizados.

Determinar el nivel de seguridad adecuado puede ser más complejo de lo que parece. Es esencial comparar detenidamente el costo de proteger la información multimedia con el valor de la información misma. Si el contenido multimedia no es muy valioso, se puede elegir un nivel de encriptación más bajo, pero si la información es confidencial o de gran valor, como secretos gubernamentales o militares, se debe seleccionar el nivel de seguridad criptográfica más alto posible. Es fundamental evaluar cuidadosamente el riesgo y la importancia de la información multimedia a proteger antes de decidir el nivel de seguridad necesario.

En muchas situaciones, el contenido multimedia puede tener una tasa de datos muy alta, pero su valor monetario no es significativo. En estos casos, los ataques costosos no son atractivos para los adversarios y un cifrado más ligero puede ser suficiente para proteger el contenido, especialmente para aplicaciones como pay-per-view. Sin embargo, en otras aplicaciones como la videoconferencia o el videoteléfono, donde se tratan secretos importantes, se requiere un mayor nivel de confidencialidad, lo que hace necesario un cifrado más fuerte. [2]

2.2 Cifrado multimedia

El cifrado multimedia es una tecnología utilizada para proteger la confidencialidad de los contenidos multimedia, evitando el acceso no autorizado y permitiendo un control persistente de acceso y gestión de derechos. Aunque comparte algunos elementos con el cifrado general, en contenido multimedia presenta desafíos únicos que no se ven en el cifrado de texto y se convierte en una herramienta fundamental en la actualidad para los servicios y aplicaciones digitales.

Al igual que en el cifrado general, su principal objetivo es garantizar la privacidad y confidencialidad en la transmisión de servicios multimedia. Para ello, el cifrado multimedia codifica la representación de los contenidos multimedia de tal manera que el contenido no pueda ser entendido de manera inteligible o con una calidad perceptible aceptable. [16] [17]

2.3 Criptografía moderna

La tecnología del cifrado multimedia se deriva del cifrado convencional, que es una de las áreas más importantes estudiadas en el campo de la criptografía moderna. El cifrado multimedia se enfoca principalmente en garantizar la privacidad del contenido multimedia y, por lo tanto, se centra en el uso de tecnologías criptográficas específicas que proporcionan confidencialidad. [16]

2.3.1 Criptosistemas

En la criptografía moderna, los mensajes se consideran como elementos algebraicos o números en un espacio. El proceso de cifrado implica una transformación matemática o algoritmo que toma el mensaje original como entrada y lo convierte en otro mensaje diferente que oculta su significado original. El mensaje original se llama texto claro o sin formato, mientras que el mensaje cifrado se conoce como texto cifrado. En la práctica, el mensaje cifrado debe ser descifrado para recuperar el mensaje original. Por lo tanto, la transformación de cifrado debe ser reversible, y la transformación inversa se llama descifrado. Juntos, un algoritmo de cifrado y su correspondiente algoritmo de descifrado forman un cifrado. Los algoritmos de cifrado y descifrado se definen mediante claves criptográficas que pueden tener un gran número de valores posibles. El espacio de claves es el conjunto de valores que una clave puede tomar.[16]

Existen dos tipos principales de criptosistemas: simétricos y de clave pública. En un criptosistema simétrico, también conocido como criptosistema de clave secreta, la clave de cifrado y la clave de descifrado son iguales o se pueden calcular una a partir de la otra. El emisor y el receptor deben compartir la clave de cifrado para poder cifrar y descifrar los mensajes. En cambio, en un criptosistema de clave pública o asimétrico, la clave de cifrado y la clave de descifrado son diferentes y no se pueden calcular una a partir de la otra. La clave de cifrado puede ser pública, mientras que la clave de descifrado debe mantenerse en secreto. Este tipo de criptosistema es generalmente más lento que un criptosistema simétrico, aunque ambos pueden tener el mismo nivel de seguridad. Debido a esta diferencia de velocidad, los criptosistemas simétricos se usan comúnmente en el cifrado de contenido multimedia. Sin embargo, en algunos casos, la clave de cifrado del contenido se cifra con un criptosistema de clave pública para garantizar que solo los usuarios

autorizados puedan recuperar la clave de descifrado y acceder al contenido cifrado. Un criptosistema se muestra en la siguiente figura:

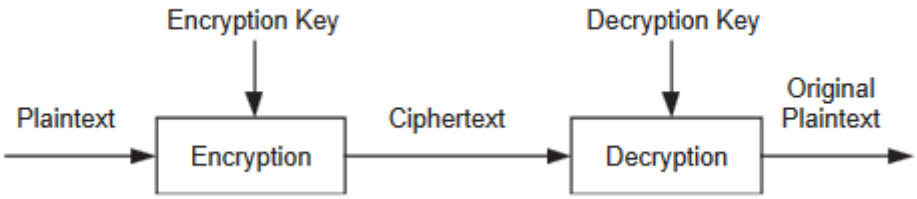


Figura 2.1 Criptosistema. (Fuente: [16])

Dentro de los cifrados simétricos está Blowfish que se utiliza para el cifrado de bloques de datos, y se ha convertido en uno de los algoritmos más populares para la protección de datos. Blowfish se caracteriza por tener una longitud de clave variable, lo que lo hace extremadamente versátil. Un cifrado simétrico más simple es XOR donde cada bit de un mensaje es operado con otro bit de una clave secreta para producir un mensaje cifrado. generalmente se lo utiliza en combinación con otros algoritmos más complejos para proporcionar una mayor seguridad. En cuanto a un ejemplo de cifrado asimétrico está RSA, el cual es utilizado comúnmente en la seguridad de la información y se basa en el problema matemático conocido como factorización de enteros. La seguridad del cifrado radica en la complejidad de este problema matemático, que es difícil de resolver en un tiempo razonable para números extremadamente grandes.

2.3.2 Cifrados de bloque y flujo

Existen dos tipos de cifrados simétricos, denominados bloque y flujo, que se clasifican según la forma en que se realiza la transformación de cifrado. Los cifrados de bloque operan en bloques de texto sin formato y texto cifrado mediante una transformación de cifrado fija. Para ello, el texto sin formato se divide en bloques de un tamaño fijo y se aplica un cifrado de bloque que cifra cada bloque por separado, tras ser rellenado si es necesario. De esta manera, con la misma clave, un bloque de texto sin formato siempre se cifrará en el mismo bloque de texto cifrado. Entre los cifrados de bloque más populares, destacan el estándar de cifrado de datos (DES) y su sucesor, el estándar de cifrado avanzado (AES).

Los cifrados de flujo funcionan de manera diferente a los cifrados de bloque, ya que operan en flujos de texto sin formato y texto cifrado de forma continua, en lugar de dividir el texto en bloques. La transformación de cifrado utilizada en un cifrado de flujo es variable en el tiempo, lo que significa que cada bit de texto sin formato se cifrará en un bit diferente cada vez. Para generar el flujo de claves necesario, se puede utilizar un generador de flujo de claves o una semilla. Los cifrados de flujo, como el RC4, ofrecen varias ventajas, como mayor velocidad y menor almacenamiento en búfer de datos en comparación con los

cifrados de bloque. Además, los cifrados de flujo síncrono no propagan errores, lo que los hace ideales para redes propensas a errores, como las comunicaciones inalámbricas. [16]

Modo ECB

El modo de libro de código electrónico cifra y descifra cada bloque de datos de manera independiente, sin tener en cuenta los datos anteriores o posteriores. Una ventaja de esto es que se pueden cifrar múltiples bloques en paralelo y los errores de transmisión se limitan al bloque actual. Sin embargo, este modo es vulnerable a ataques de reproducción o análisis de tráfico, ya que un bloque que contiene datos constantes se cifrará con el mismo bloque de cifrado cada vez que se utilice la misma clave. [18]

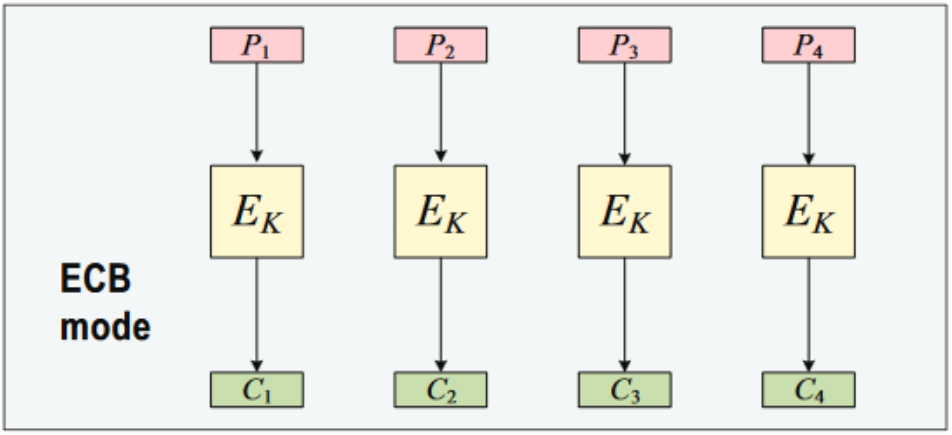


Figura 2.2 Modo ECB. (Fuente: [18])

Modo CBC

En el modo de encadenamiento de bloques de cifrado, se busca proteger contra los ataques de repetición que pueden presentarse en el modo ECB. En este modo, se realiza una operación XOR entre la salida del bloque anterior y el bloque actual de texto sin formato, posteriormente se cifra y se transmite o almacena. Luego, la salida del bloque actual se utiliza para la operación XOR con el siguiente bloque de texto sin formato. En el proceso de descifrado se hace lo contrario: se descifra el bloque actual, se realiza una operación XOR con el bloque de texto cifrado anterior y se obtiene el bloque de texto sin formato original. Para solucionar un problema que se presenta al inicio de la cadena, se debe transmitir primero un bloque ficticio llamado "vector de inicialización" (IV). Los errores de transmisión tienen un mayor impacto que en ECB, ya que un solo bit invertido en el

bloque actual puede cambiar completamente la versión del texto sin formato y afectar a un solo bit en el siguiente bloque.

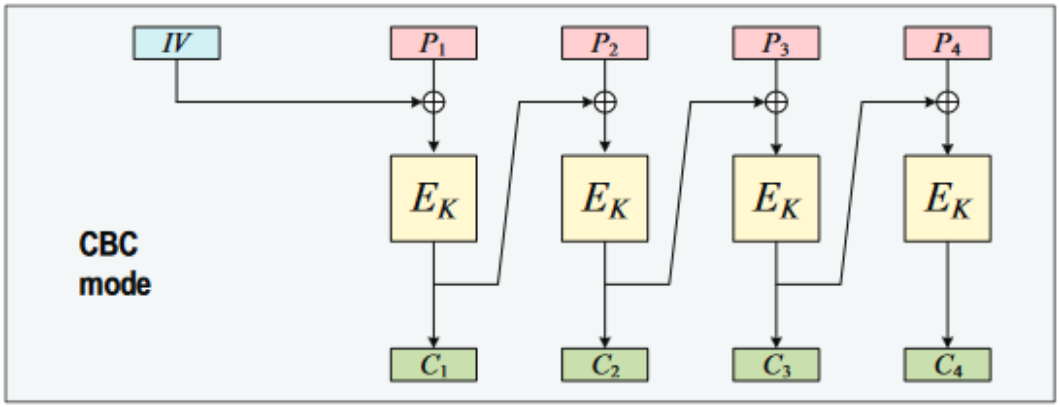


Figura 2.3 Modo CBC. (Fuente: [18])

Modo CFB

El modo de retroalimentación de cifrado permite transformar un cifrado de bloque en un cifrado de flujo. Este modo es útil cuando se necesita cifrar datos con un tamaño menor que la longitud del bloque. Para empezar, se utiliza un vector de inicialización (IV) y se almacena en un registro de desplazamiento. Luego, el contenido del registro se cifra y los n bits más a la izquierda se utilizan para realizar una operación XOR con los datos de entrada sin cifrar de tamaño n. Los datos cifrados resultantes (también de tamaño n) se envían o almacenan, y se vuelven a colocar en el registro de desplazamiento en el lado derecho. La operación de descifrado es similar al cifrado, utilizando el mismo IV. Los datos cifrados de tamaño n recibidos se colocan en el registro de desplazamiento, se cifran y se someten a una operación XOR con los datos cifrados recibidos. Es importante usar un IV único para cada mensaje, pero no es necesario mantenerlo en secreto.

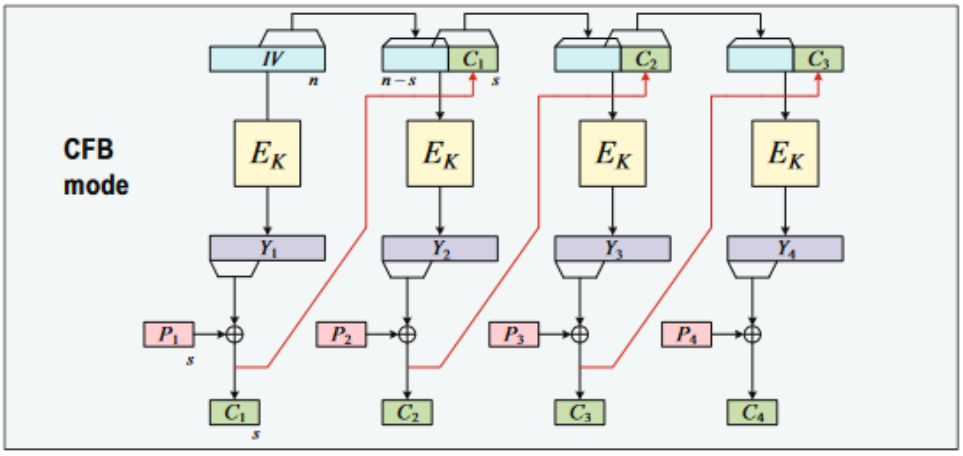


Figura 2.4 Modo CFB. (Fuente: [18])

Modo OFB

El modo de retroalimentación de salida es parecido al modo CFB, la principal diferencia es que en el modo OFB, la retroalimentación no implica los datos del usuario. En cambio, la retroalimentación se realiza solo entre la función de cifrado y el registro de desplazamiento. El resultado de la función de cifrado se retroalimenta directamente en el registro de desplazamiento, lo que significa que el flujo de claves se puede calcular de manera independiente a los datos que se van a cifrar.

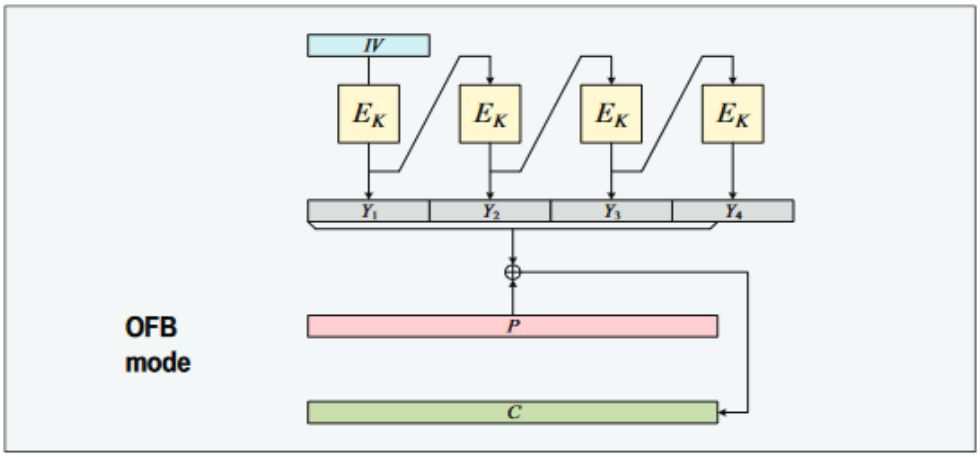


Figura 2.5 Modo OFB. (Fuente: [18])

Modo CTR

El modo de contador es una variante del modo OFB, pero en lugar de utilizar un registro de desplazamiento, se usa un valor de contador como entrada para la función de cifrado. Después de cada cifrado, el contador se cambia, generalmente se incrementa en uno. Este modo tiene la ventaja de permitir el acceso aleatorio a algunos datos sin los problemas que presenta el modo ECB. [19]

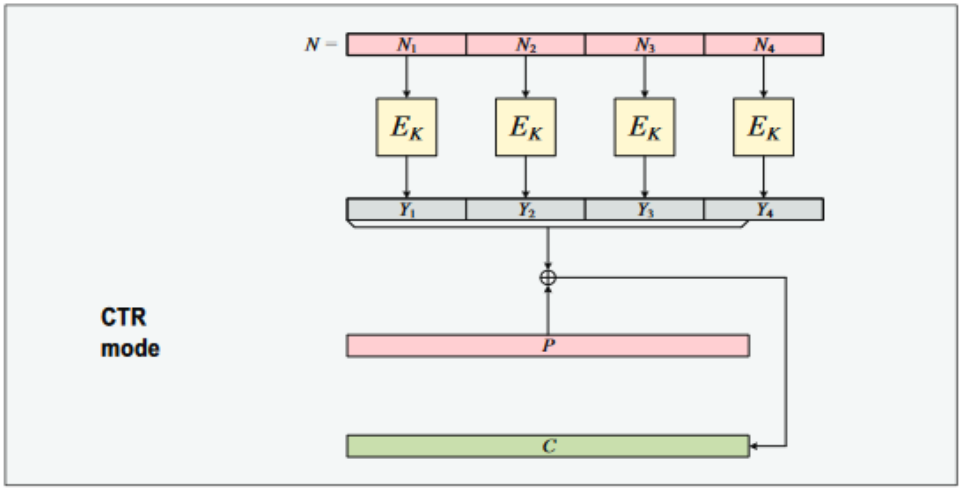


Figura 2.6 Modo CTR. (Fuente: [18])

2.1 Descripción general del algoritmo DES y triple DES

El algoritmo de cifrado DES utiliza una clave de 56 bits para cifrar bloques de datos de 64 bits de longitud.

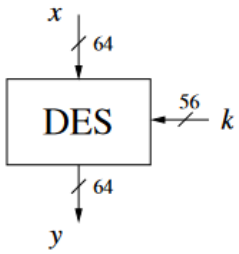


Figura 2.7 Cifrado de bloque DES. (Fuente: [20])

DES es un tipo de cifrado simétrico que emplea la misma clave para cifrar y descifrar los datos. Este algoritmo es iterativo y utiliza 16 rondas para cifrar cada bloque de texto sin formato. Todas las rondas ejecutan la misma operación y en cada una de ellas se utiliza una subclave distinta. Todas las subclaves son derivadas de la clave principal k. Se puede observar la estructura de DES en la figura 2.7.

Cuando se publicó DES en 1975, el uso de bloques de 64 bits y claves de 56 bits proporcionaba una seguridad suficiente para la época y los años siguientes. A pesar de que el NIST ha extendido su validez varias veces, se ha demostrado que es susceptible a ataques de fuerza bruta. En 1998, la EFF realizó un intento público de fuerza bruta y demostró que con una inversión de solo 200 000 USD era posible descifrar un cifrado. La ley de Moore sugiere que cada 18 meses, la duración esperada del ataque se reduce a la mitad, lo que hace que la fuerza bruta sea más asequible. Debido a que muchas organizaciones confiaban en DES, esto se convirtió en un problema importante.

Una solución para abordar la vulnerabilidad de DES ante los ataques por fuerza bruta fue extender su uso a triple-DES, donde cada bloque de texto es cifrado tres veces. Esto crea claves con una longitud de 2*56 o 3*56 bits. Aunque es seguro para la mayoría de las aplicaciones, triple-DES es lento en comparación con otros cifrados de fuerza similar, ya que fue diseñado para procesadores de 4 bits en los años 70 y no funciona bien en las CPU actuales. [19] [20]

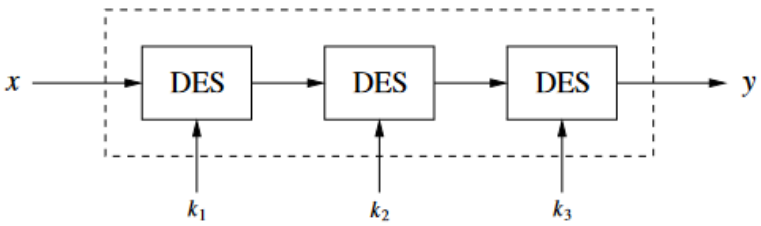


Figura 2.8 Cifrado de bloque triple-DES. (Fuente: [20])

2.2 Descripción general del algoritmo AES

El cifrado AES y el cifrado en bloque Rijndael son casi idénticos, con la única diferencia de que el tamaño del bloque y la clave pueden variar en Rijndael (128, 192 o 256 bits). En cambio, el estándar AES solo permite un tamaño de bloque de 128 bits, por lo que solo Rijndael con un tamaño de bloque de 128 bits se conoce como el algoritmo AES.

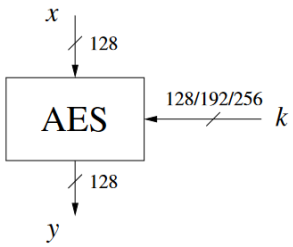


Figura 2.9 Cifrado de bloque AES. (Fuente: [20])

Antes de que AES sea publicado como estándar el Instituto Nacional de Estándares y Tecnología (NIST) creó una serie de normas y directrices de seguridad para los algoritmos de cifrado, entre las que se encuentra la necesidad de que estos funcionen correctamente en diversos tipos de hardware, desde CPU de 8 bits en tarjetas inteligentes hasta CPU de servidores modernas de 64 bits. Dependiendo del tamaño de la clave, el algoritmo AES utiliza 10, 12 o 14 rondas, y en cada ronda se aplican cuatro funciones para alterar los datos de entrada: SubBytes(), ShiftRows(), MixColumns() y AddRoundKey().

Debido a que se ha establecido un algoritmo de reemplazo en AES para DES, NIST propuso retirar DES como un estándar y solo mantener su variante triple-DES. [20]

2.3 Paradigma del cifrado multimedia

El cifrado multimedia es una variante especial del cifrado general que consiste en transformar la representación de los archivos multimedia en una forma diferente para que no puedan ser percibidos de manera inteligible. Es posible preguntarse por qué es necesario este tipo de cifrado, y si es posible tratar los datos multimedia como un mensaje general y cifrarlos de esa forma. La respuesta es que sí, este método se conoce como cifrado ingenuo y es el más directo y general. Sin embargo, una variante de este método implica cifrar los datos de cada paquete que se transmite a través de una red como si fuera un texto cifrado, lo cual puede ser efectivo para proteger la confidencialidad de los multimedia, pero puede sacrificar muchas características deseables de las aplicaciones multimedia. Por ejemplo, es necesario aplicar el descifrado para extraer información básica, como la tasa de bits del archivo multimedia cifrado mediante este método.

2.6.1 Características y requerimientos deseables en el cifrado multimedia

El cifrado multimedia es una aplicación especial del cifrado general, que tiene requisitos y características únicas. A diferencia del cifrado general, el cifrado multimedia necesita que cierta información, como el formato, la tasa de bits y el artista, esté disponible públicamente para que el flujo de código multimedia cifrado sea útil. Existen varios requisitos y características deseables que se deben tener en cuenta en el diseño de un criptosistema multimedia práctico, pero algunos de estos requisitos están relacionados entre sí y otros son mutuamente competitivos. Por lo tanto, es esencial equilibrar cuidadosamente estos requisitos conflictivos para lograr un diseño efectivo del criptosistema multimedia para cada aplicación específica. Los requisitos principales y las características deseables se enumeran a continuación.

- **Complejidad.** El cifrado y descifrado de datos multimedia puede ser complejo debido a la gran cantidad de información que se debe transmitir o procesar, especialmente en el caso del video. Para reducir el espacio de almacenamiento y el ancho de banda de transmisión, los datos multimedia se comprimen, pero aun así se requiere una gran cantidad de potencia y recursos informáticos para cifrar y descifrarlos. Esto puede generar una sobrecarga significativa de procesamiento, especialmente cuando se procesa una gran cantidad de datos multimedia. La complejidad del cifrado y descifrado multimedia es una consideración importante en el diseño de un sistema criptográfico multimedia, especialmente si se trata de una aplicación que requiere reproducción en tiempo real en dispositivos portátiles con recursos informáticos y energía limitados. Por lo tanto, es esencial asegurarse de que el cifrado y descifrado de datos multimedia tengan una baja complejidad para cumplir con los requisitos de aplicaciones específicas.

- **Fuga de contenido (o perceptibilidad).** El cifrado multimedia tiene una característica única en la que parte del contenido cifrado puede ser perceptible sin la clave de descifrado. Diferentes aplicaciones tienen diferentes requisitos para el nivel de perceptibilidad del contenido protegido. Para aplicaciones de entretenimiento en el hogar, como las de pago por evento, el cifrado que distorsiona el contenido visual puede ser suficiente. Sin embargo, las aplicaciones militares y financieras pueden requerir la máxima protección para evitar que el adversario extraiga información del contenido. Por lo tanto, el cifrado multimedia debe ser diseñado para cumplir con el nivel deseado de perceptibilidad para la aplicación específica con la menor complejidad posible. El objetivo del cifrado en las

aplicaciones de entretenimiento es degradar el contenido en lugar de mantenerlo en secreto, mientras que, en aplicaciones militares y financieras, el objetivo es mantener la confidencialidad del contenido. El nivel de perceptibilidad necesario varía según la aplicación y debe tenerse en cuenta en el diseño del criptosistema multimedia.

- **Sobrecarga de eficiencia de compresión.** El cifrado multimedia puede tener un impacto negativo en la eficiencia de compresión, lo que puede manifestarse de varias formas. Por ejemplo, el cifrado puede alterar los parámetros o procedimientos de compresión óptimos, o puede cambiar las propiedades estadísticas de los datos que se comprimirán. Además, se pueden agregar encabezados adicionales al flujo de datos para indicar parámetros de descifrado y límites de segmentos encriptados. Es importante minimizar la sobrecarga de eficiencia de compresión causada por el cifrado para garantizar una buena calidad de compresión.

- **Resiliencia al error.** Las aplicaciones multimedia suelen requerir la transmisión de datos a través de redes, que pueden presentar errores y pérdidas de paquetes, especialmente en redes inalámbricas. El cifrado de los datos puede empeorar la situación al propagar los errores y afectar la percepción de los datos. Es importante diseñar un criptosistema multimedia que limite la propagación de errores durante el cifrado y permita una recuperación rápida de errores de bits y resincronización de paquetes perdidos. Desafortunadamente, muchos criptosistemas propuestos no han tenido en cuenta la resiliencia a errores, lo que puede provocar una degradación significativa de la percepción durante la transmisión multimedia. Por lo tanto, es esencial tener en cuenta la resiliencia a errores en el diseño de cualquier criptosistema multimedia.

- **Adaptabilidad y escalabilidad.** Una de las ventajas del contenido multimedia cifrado es que puede ser reproducido en dispositivos con diferentes características y capacidades de procesamiento. Sin embargo, en ocasiones se requiere adaptar el cifrado a un dispositivo específico o ajustar la velocidad de transmisión para adaptarse al ancho de banda disponible. Por lo tanto, es importante que el cifrado multimedia sea fácilmente adaptable sin afectar su calidad o seguridad. Esto es especialmente relevante para el cifrado de formatos multimedia escalables, que permite codificar el contenido en un flujo de bits estructurado jerárquicamente y escalable, lo que permite ajustar la cantidad de datos transmitidos para adaptarse a las necesidades de cada aplicación.

- **Cifrado multinivel.** El cifrado multimedia presenta una característica única la cual es permitir el acceso a múltiples niveles de calidad desde un solo flujo de código cifrado. Los datos multimedia pueden agruparse y cifrarse para ofrecer diferentes opciones de calidad para los usuarios. En los formatos FGS, el contenido multimedia se puede cifrar en un solo flujo de código para permitir el acceso simultáneo a diferentes tipos de calidad, resolución, tamaño de cuadro y velocidad, así como a múltiples capas para cada tipo de acceso. Este cifrado multinivel permite que los usuarios accedan a diferentes versiones del mismo contenido desde un solo flujo de código cifrado que se adapte mejor a sus redes y dispositivos de reproducción con diferentes características y capacidades. El cifrado multinivel también garantiza que los usuarios solo puedan acceder a los niveles para los que están autorizados y no a los datos que requieren privilegios más altos. En resumen, el cifrado multinivel es una tecnología que respalda el modelo comercial de "lo que ves es lo que pagas" con un único flujo de código cifrado.

- **Cumplimiento de la sintaxis.** La tecnología de codificación popular, como MPEG-1/2, cuenta con una amplia base de usuarios. Sin embargo, muchos sistemas multimedia se diseñaron sin tener en cuenta el cifrado, lo que puede resultar en la falta de compatibilidad de la infraestructura existente y los dispositivos instalados con una tecnología de cifrado adicional posterior. Para superar este problema de retrocompatibilidad, es necesario que el flujo codificado encriptado sea compatible con la sintaxis específica del formato multimedia, lo que permite su reproducción (decodificación) sin descifrarlo, como si el flujo codificado no estuviera encriptado, aunque el resultado final puede no ser comprensible. A este tipo de cifrado multimedia se le conoce como cifrado compatible con la sintaxis (o compatible con el formato). Este tipo de cifrado es transparente y presenta ventajas como la adaptabilidad, la escalabilidad y la resistencia a errores.

- **Independiente del contenido.** Existen tres tipos principales de datos en archivos multimedia: audio, imagen y video, y cada tipo puede utilizar diferentes tecnologías de compresión, generando flujos de bits únicos. Para poder agrupar estos flujos en un formato multimedia común, es importante que el cifrado aplicado sea independiente del contenido y de la tecnología de codificación específica utilizada. De esta manera, se puede reducir la complejidad del cifrado y se puede utilizar un único módulo de cifrado o descifrado para procesar una gran variedad de tipos de multimedia y flujos de bits codificados. [16]

2.6.2 Seguridad de los criptosistemas multimedia

La seguridad de un criptosistema multimedia depende de su complejidad para descifrarlo, al igual que con cualquier otro criptosistema. Cada criptosistema ofrece diferentes niveles de seguridad basados en lo difícil que sea romperlos. Si el costo para descifrar un criptosistema multimedia es mayor que el valor del contenido multimedia encriptado, entonces se puede considerar que el criptosistema es seguro. El valor del contenido multimedia disminuye rápidamente después de su lanzamiento, por lo que el tiempo necesario para descifrar un criptosistema debe ser más largo que el tiempo en que los datos multimedia permanecen encriptados para considerar el criptosistema seguro.

Es importante destacar que la seguridad de un criptosistema multimedia varía según la aplicación específica. Por ejemplo, algunas aplicaciones que requieren alta seguridad, como las militares, no permitirían ninguna clase de ataque en el contenido, mientras que otras aplicaciones, como el entretenimiento en el hogar, pueden tolerar ataques siempre y cuando el contenido resultante tenga una calidad significativamente inferior. La complejidad de descifrar un criptosistema multimedia y el valor del contenido encriptado también deben ser considerados en la evaluación de seguridad. Aunque los datos multimedia, especialmente los videos, tienen una alta tasa de datos, el valor monetario por unidad de datos puede ser bajo en muchas aplicaciones, por lo que un criptosistema ligero y económico puede proporcionar suficiente seguridad a un costo razonable. Al diseñar un sistema multimedia, es fundamental identificar el nivel adecuado de seguridad para la aplicación específica. La falta de protección es inaceptable, pero una protección excesiva puede resultar en una complejidad y costo computacional innecesarios y no deseables. [16]

2.4 Técnicas de protección para audio y voz

En diferentes escenarios, es necesario mantener la confidencialidad de las secuencias de audio mientras se transmiten. En algunas situaciones un enfoque ingenuo puede ser suficiente, en muchos casos, puede resultar demasiado costoso en términos de recursos computacionales, especialmente en dispositivos móviles. En cuanto a la seguridad, el habla es quizás el tipo de datos de audio más importante. A diferencia de los archivos de música y otras secuencias de audio de entretenimiento, el habla se considera crítica en muchas aplicaciones y requiere un alto nivel de seguridad.

El uso de un enfoque ingenuo puede resultar costoso en la protección de los datos de audio, lo que hace que su viabilidad sea cuestionable. Por esta razón, se han llevado a cabo iniciativas de investigación para desarrollar enfoques más selectivos y eficientes de encriptación para flujos de audio comprimido. [2] [21]

2.7.1 Cifrado de voz por Wu y Kuo

La recomendación G.723.1 de la UIT es uno de los códecs de voz digital más utilizados debido a su capacidad de compresión. Este estándar tiene una tasa de bits muy baja, lo que lo hace adecuado para la comunicación de voz a través de redes basadas en conmutación de paquetes. Además, forma parte del estándar ITU H.324, que se utiliza para la videoconferencia y la telefonía a través de líneas telefónicas públicas regulares.

El códec de voz G.723.1 de la UIT utiliza el método de análisis por síntesis para comprimir audio. El codificador sintetiza voz a partir de coeficientes de entrada, ajustando estos coeficientes hasta que la diferencia entre el habla original y el habla sintetizada esté dentro de un rango aceptable. La decodificación se realiza mediante tres decodificadores diferentes y los coeficientes se clasifican según el decodificador al que se alimentan. Este códec también tiene dos modos de funcionamiento diferentes con tasas de bits de 6.3 Kbps y 5.3 Kbps.

Wu y Kuo proponen aplicar cifrado selectivo a los bits más importantes de los coeficientes G.723.1. Identificaron cinco coeficientes críticos: los índices del libro de códigos LSP, el retraso del predictor de tono, los vectores de ganancia de tono, las ganancias del libro de códigos fijo y la bandera de modo VAD. El cifrado cubre un total de 37 bits en cada cuadro, lo que es menos del 20% de la transmisión de voz completa a 6.3 Kbps y menos del 25% a 5.3 Kbps. [21]

2.7.2 Cifrado de voz por Servetti y De Martin

Servetti y De Martin desarrollaron un algoritmo basado en la percepción para cifrar el habla de ancho de banda telefónico utilizando el códec ITU-T G.729 a una tasa de 8 Kbps. Propusieron dos métodos de cifrado: uno con baja seguridad, pero alta tasa de bits y otro que encripta una mayor parte del flujo de bits para proporcionar mayor seguridad. Aunque el segundo método encripta solo alrededor de la mitad del flujo de bits, el nivel de seguridad es comparable al del algoritmo ingenuo según sus desarrolladores. En la siguiente figura

se presenta el cifrado selectivo para el códec de voz G.729 donde los bits grises se seleccionan para el cifrado.

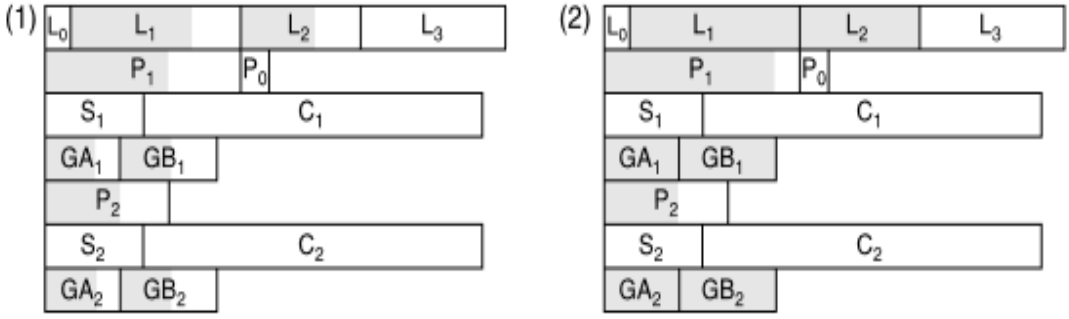


Figura 2.10 Cifrado parcial para el códec de voz G.729: (1) algoritmo de baja seguridad y (2) algoritmo de alta seguridad. (Fuente: [21])

De acuerdo a los experimentos realizados, el uso del algoritmo de cifrado selectivo de alta seguridad resultó en una codificación significativa del habla que no puede ser reconstruida a partir de los bits conocidos, y a la vez se obtuvo un ahorro computacional superior al 50%. [21]

2.7.3 Cifrado de audio por Thorwirth, Horvatic, Weis y Zhao

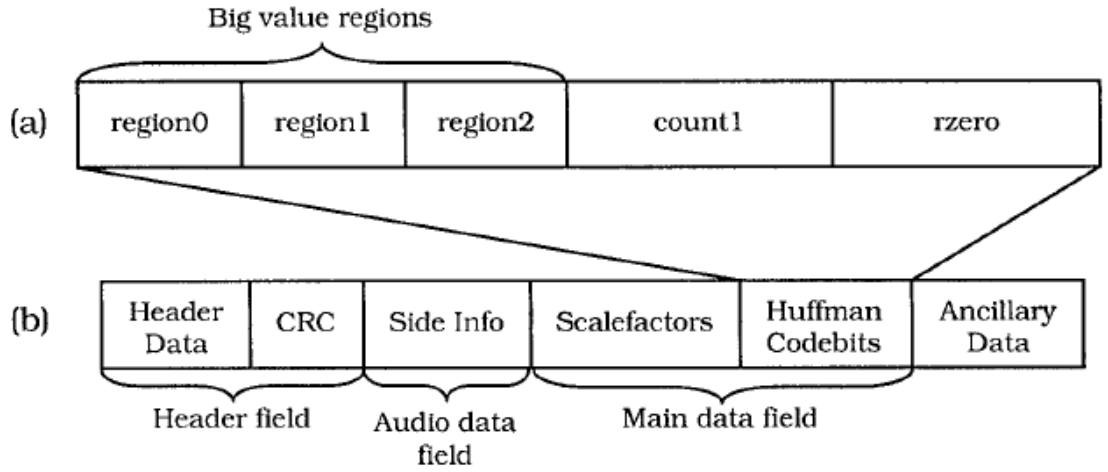
Thorwirth, Horvatic, Wels y Zhao presentaron un algoritmo de cifrado selectivo para archivos de audio en formato MP3 y otros estándares de compresión basados en codificación de audio perceptual (PAC). MP3 es un códec de audio de percepción que utiliza los algoritmos de enmascaramiento de percepción para eliminar la redundancia de la señal digital de audio. La propuesta consiste en cifrar las capas de calidad de audio asociadas con los datos de audio comprimidos, identificando los límites del espectro de frecuencias para determinar estas capas. El cifrado de bloque se aplica a cada capa conocida antes de volver a conectar los datos cifrados al flujo de bits MP3. La velocidad de bits es casi constante, aunque puede haber un ligero aumento debido al uso del cifrado de bloque. Este enfoque es compatible con el formato y las secuencias de MP3 encriptadas son decodificables y reproducibles por cualquier reproductor de MP3 válido. [21]

2.7.4 Cifrado de audio por Servetti, Testa y De Martin

Servetti, Testa y De Martin propusieron un método de cifrado selectivo para archivos de audio MP3 que degrada la calidad del sonido, pero mantiene la información perceptiva. Este algoritmo produce una música en modo de muestra que se puede actualizar a alta calidad con el descifrado adecuado. Durante la compresión de MP3 cada canal de salida se subdivide en 18 bandas utilizando una transformada de coseno discreta modificada con

ventana (MDCT), los coeficientes de MDCT se codifican utilizando una tabla de Huffman y luego se dividen en cinco regiones: region0, region1, region2, count1 y rzero (figura 2.11a).

Figura 2.11 Estructura del flujo de bits de MP3: (a) las 5 regiones de los bits de código de



Huffman, y (b) trama MP3. (Fuente: [21])

La estructura lógica del MP3 se compone de regiones llamadas codebits de Huffman, siendo la trama MP3 el componente más alto del flujo de bits. Cada trama consta de un encabezado que contiene los parámetros de decodificación y datos como la tasa de bits, frecuencia de muestreo, número de canales, bits de sincronización, información del sistema y un código de verificación de redundancia cíclica (CRC). El campo de datos de audio especifica los parámetros de control de decodificación, en la información adicional se encuentra la asignación de bits y factores de escala., seguido de un campo de datos principal con factores de escala y bits de código de Huffman, por último, se tiene un segmento de datos auxiliares al final de cada cuadro. La estructura de un cuadro MP3 se puede ver en la figura 2.11-b. [21]

El modelo de cuantificación psicoacústica aplicado a los coeficientes de MDCT produce valores altos en frecuencias bajas y valores bajos o ceros en frecuencias altas. A continuación, se divide un total de 576 coeficientes en las cinco regiones antes mencionadas. Las últimas tres regiones tienen una tabla de Huffman diferente para mejorar la compresión y la resistencia a errores, mientras que la región count1 tiene dos opciones de tabla Huffman y la región rzero no tiene codificación Huffman. La señal se asigna a cada región según su frecuencia y se elige la tabla de Huffman que mejor se ajuste a las estadísticas de la región. El índice de tabla de Huffman se almacena para cada región.

Es posible hacer que un decodificador de MP3 ignore los valores espectrales de una región utilizando un índice de tabla de Huffman privado. El estándar MP3 reserva el uso de dos tablas Huffman adicionales para codificar las regiones de gran valor y los índices 4 o 14

podrían indexar estas dos tablas, mientras que los otros índices se utilizan para indexar las 30 tablas estándar de Huffman para regiones de gran valor. La mayoría de los decodificadores llenan la parte correspondiente con coeficientes de valor cero cuando se encuentra un índice reservado. En el algoritmo de cifrado selectivo de MP3 propuesto por Servetti, Testa y De Martin, los índices de la tabla de Huffman de todas las regiones después de la region0 se establecen en uno de los valores no utilizados, ya sea 4 o 14. De esta manera, el decodificador omitirá el proceso de decodificación de las cuatro regiones que siguen a la region0.

Para preservar el cumplimiento del formato MP3, se debe establecer en 288 todos los pares de valores grandes para que el decodificador descarte los bits restantes de forma segura. La información de mejora, incluyendo los índices de tabla y el número de pares de gran valor para los fotogramas MP3, se cifra y se adjunta al comienzo del flujo de bits MP3. Aunque este prefijo no es parte del formato de archivo MP3, la mayoría de los reproductores de MP3 estándar lo ignoran y procesan el resto del flujo de bits. Esto se utiliza para mejorar la calidad del sonido, pero puede afectar negativamente la calidad si solo se decodifica una región. El aumento en el flujo de bits debido a la información cifrada es mínimo y, por lo general, representa menos del 5%.

Se podría realizar un ataque criptoanalítico para mejorar la calidad del sonido en un archivo MP3 reemplazando valores de la tabla de Huffman. Por lo tanto, se sugiere cifrar datos adicionales para proteger contra posibles ataques. Esto incluye un bit de veinte en la region1 y entre 70 y 100 bits en la region2. El esquema es en gran parte compatible con el formato y la cantidad de información cifrada es solo del 10%. Aunque es un cifrado de baja seguridad, en la mayoría de los casos, el control de calidad es suficiente en lugar de una seguridad absoluta en los datos MP3. [21]

2.5 Técnicas de protección de video

Como se mencionó previamente, es posible aplicar un enfoque simple para encriptar contenido multimedia. Este método utiliza un sistema de cifrado de clave simétrica para cifrar todo el flujo multimedia. Sin embargo, incluso los esquemas simétricos modernos más rápidos, como DES o AES, pueden resultar computacionalmente muy costosos para procesar grandes cantidades de datos como el audio y video en tiempo real. [2]

2.8.1 Codificación de video

La codificación de señal de video es un método comúnmente utilizado para introducir una distorsión rápida y básica con el objetivo de dificultar la visualización gratuita de canales de cable pagados. Este método fue desarrollado rápidamente por las compañías de cable

para ofrecer una solución inmediata y efectiva ante el problema de la piratería de señales de televisión. [2]

La Fig. 2.12 muestra un ejemplo con cuadros de video codificados. Es evidente que el contenido de video cifrado es demasiado confuso para ser entendido. Esto hace que el programa de televisión sea ilegible para los usuarios no autorizados que no poseen claves legales.

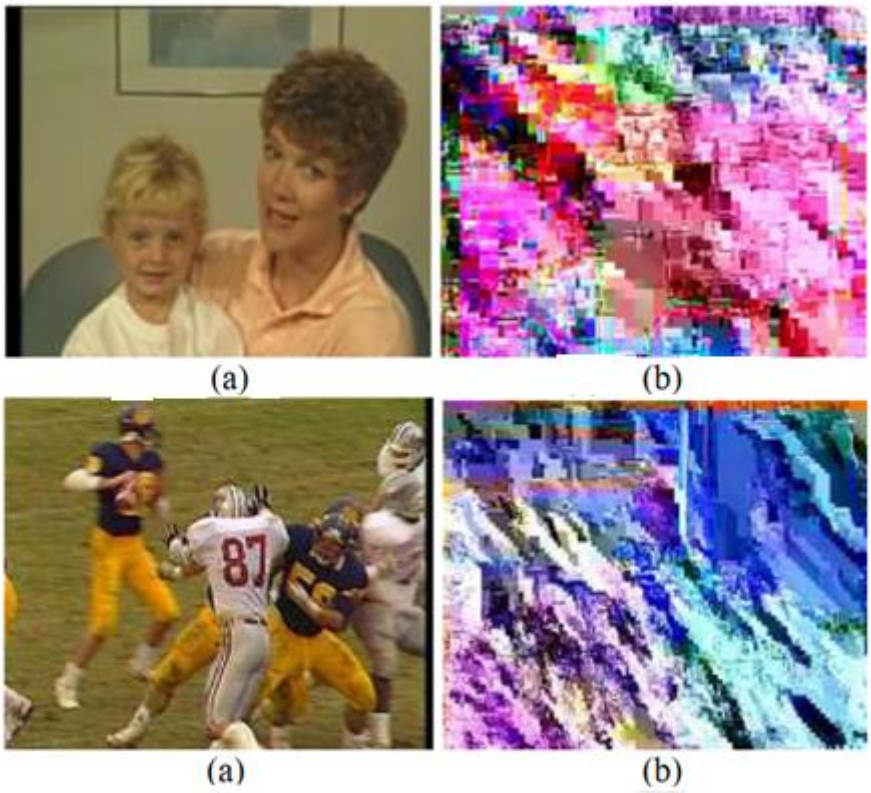


Figura 2.12 Ejemplos de codificación de contenido de video. (a) video original; (b) video codificado (Fuente: [22])

La codificación hace referencia a los métodos de cifrado más simples, como la sustitución y transposición simples, cuya seguridad es muy baja en el mundo actual. Los primeros trabajos de codificación de señales se basaron en la permutación de la señal en el dominio del tiempo o la distorsión de la señal en el dominio de la frecuencia mediante filtros o convertidores de frecuencia analógicos. Sin embargo, estos esquemas no son seguros y son fáciles de descifrar con la ayuda de computadoras modernas. Los métodos de codificación son solo una forma temporal de dificultar que un atacante obtenga la señal original de audio o video.

A menudo, la codificación sigue siendo una solución utilizada por muchas compañías de cable en todo el mundo, ya que la mayoría de las personas carecen de los conocimientos y habilidades técnicas para descifrar la señal de video codificada. Aunque esta solución

puede funcionar efectivamente, la facilidad de fabricación de cajas de cable modificadas capaces de descifrar el contenido codificado aumenta la posibilidad de piratería y compromete la seguridad de la transmisión. Debido a estas debilidades, la codificación se considera inadecuada para aplicaciones que requieren un nivel de seguridad más alto. [2]

2.8.2 Cifrado de video selectivo

Las técnicas de encriptación selectiva han sido desarrolladas para garantizar la reproducción en tiempo real de contenido multimedia de audio y video. La idea principal de esta técnica es encriptar solo una parte del flujo de bits comprimido, lo cual es comúnmente realizado a través de la integración de la compresión y el cifrado. Esta integración se puede observar en la Figura 2.13.

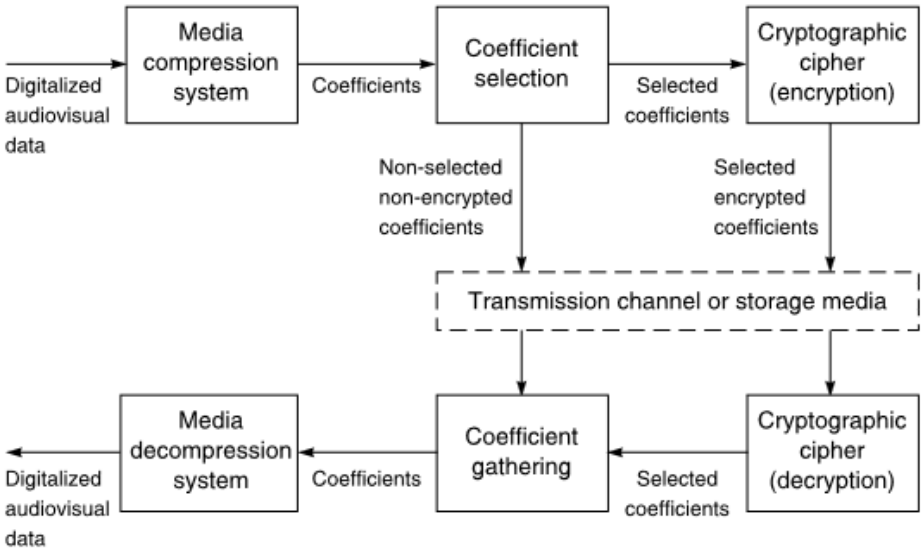


Figura 2.13 Esquema de cifrado selectivo común. (Fuente: [2])

Una técnica común en el cifrado selectivo consiste en seleccionar solo los coeficientes más importantes de los procesos de compresión y cifrar solo esos coeficientes. Los coeficientes menos importantes se dejan sin cifrar, aunque algunos esquemas prefieren cifrarlos ligeramente. En ocasiones incluso los coeficientes menos importantes son cifrados de manera "ligera", lo que significa que se utiliza un esquema de cifrado simple con una velocidad alta y un nivel de seguridad bajo. [2]

2.8.3 Tecnologías y plataformas de distribución

Los proveedores utilizan sistemas de protección de contenido como CAS y DRM para asegurar la entrega segura de contenido comercial y servicios de múltiples canales. Estos sistemas controlan las autorizaciones para habilitar o deshabilitar el video. Sin embargo,

existen múltiples amenazas a la seguridad que los distribuidores de programación de video multicanal (MVPD) deben abordar.

Los sistemas de protección de contenido, incluidas las soluciones CAS y DRM, se basan en una combinación de hardware y software para garantizar la entrega segura de servicios de video, la mayoría de las soluciones incluyen componentes de software descargables. Una forma de mejorar la seguridad es mediante el uso adecuado del hardware, como, por ejemplo, la ejecución de partes de la solución de software en una zona segura del hardware conocida como "Entorno de Ejecución Confiable" (TEE), en lugar de utilizar la unidad central de procesamiento (CPU) general, que es menos segura.

La entrega de servicios de video a dispositivos clientes se ha vuelto cada vez más común a través del uso de “aplicaciones” en los proveedores de servicios. Las aplicaciones son utilizadas como un medio para hacer frente a las diferencias y cambios constantes entre los servicios y plataformas de electrónica de consumo. Estas aplicaciones se distribuyen a través de IP y pueden incluir software descargable y/o DRM compatible con la plataforma. Los distribuidores de video "over the top" (OTT), como Netflix y Amazon, tienen que crear versiones personalizadas de sus aplicaciones para cada plataforma que admiten, mientras que algunos fabricantes de dispositivos adaptan y prueban estas aplicaciones. Los proveedores multicanal siguen el mismo modelo, brindando sus servicios de video a través de aplicaciones en millones de dispositivos habilitados para IP propiedad del cliente, como iOS, Android, Mac OS X, PC/Windows, Xbox, Roku, Kindle y una variedad de televisores inteligentes. [23]

2.8.4 Software, hardware y seguridad descargable

Las soluciones de protección de contenido, como CAS y DRM, utilizan tanto hardware como software para garantizar la entrega segura de servicios de video. La fortaleza de estas soluciones depende en gran medida de la capacidad del hardware para complementar y reforzar la seguridad del software. La mayoría de estas soluciones ofrecen la posibilidad de descargar componentes de software. Por ejemplo, una solución CAS descargable puede incluir una combinación de componentes de software y hardware, un entorno de ejecución confiable proporcionado por el hardware, un modelo de descarga segura para el componente de software y una raíz de confianza segura que autentique el hardware para que el software pueda confiar en él.

La forma en que se instala el sistema de protección de contenido puede variar entre diferentes sistemas como se describe a continuación:

- **Integrado:** El sistema de protección de contenido es instalado en el dispositivo durante su fabricación y no puede ser modificado, aunque puede contener algunos componentes actualizables mediante software.
- **Hardware instalable:** El sistema de protección de contenido se puede instalar mediante hardware que se conecta a un dispositivo a través de un conector externo, lo cual permite que el operador o el consumidor realicen la instalación. Aunque estos sistemas pueden incluir componentes de software actualizables, requieren la instalación de hardware adicional a través de un conector externo.
- **Software descargable:** El sistema de protección de contenido utiliza un módulo que se instala únicamente mediante descarga de software. Por ejemplo, la protección de contenido en navegadores web de PC utiliza el DRM descargable de software. El software DRM descargable se ejecuta en la unidad central de procesamiento (CPU) del dispositivo, sin necesidad de hardware externo que se conecte a través de un conector.

Para muchas soluciones en dispositivos de consumo, como DRM solo de software que se usa en tablets y PC, la CPU de propósito general no se usa como un elemento de seguridad de hardware y el componente de software puede tratar de ocultar elementos críticos (código de objeto, nombres de variables, elementos criptográficos, etc.) debido a la falta de componentes de hardware seguros. [23]

2.8.5 Tecnologías de distribución de los proveedores de video

Los proveedores de video utilizan diversas tecnologías de distribución para entregar contenido a los consumidores, incluyendo la transmisión en vivo, la descarga de archivos y la entrega por cable. También pueden utilizar diferentes formatos de archivo, códecs y protocolos de transmisión para optimizar la calidad de la experiencia de visualización y la eficiencia de la entrega. En la siguiente tabla se presenta un resumen de los distintos sistemas CAS implementados, cada uno con su propia infraestructura de licencias, adicionalmente se muestran los cifrados centrales, los transportes, los canales de control y los códecs de video que se utilizan en cada sistema.

Tabla 2.1 Tecnologías de distribución. (Fuente: [23])

MVPD	CAS	Cifrado	Transporte	Canales	Códec
Cable	DigiCipher 2	DES-CBC	QAM/ MPEG- 2 TS	SCTE-55-1	MPEG-2/ AVC
	MediaCipher	DES-CBC	QAM/ MPEG- 2 TS	CTE-55-1/ DOCSIS	MPEG-2/ AVC
	Powerkey	DES-ECB	QAM/	CTE-55-2/	MPEG-2/

			MPEG- 2 TS	DOCSIS	AVC
	NDS VideoGuard	CSA	QAM/ MPEG- 2 TS	Generic IP	MPEG-2/ AVC
	Conax	CSA	QAM/ MPEG- 2 TS	Generic IP	MPEG-2/ AVC
	Nagravision	CSA	QAM/ MPEG- 2 TS	CTE-55-2/ DOCSIS	MPEG-2/ AVC
	DTA	DES-CBC/ DES-ECB	QAM/ MPEG- 2 TS	In-Band	MPEG-2/ AVC
	OMS	CSA/DES/ AES	QAM/ MPEG- 2 TS	DOCSIS	MPEG-2/ AVC
	BBT	AES	QAM/ MPEG- 2 TS	Generic IP	MPEG-2/ AVC
	Verimatrix VCAS for Broadcast-Hybrid	AES/DES/ CSA	QAM/IP/ MPEG- 2 TS	Generic IP	MPEG-2, MPEG-4/ H.264
Satelite	NDS VideoGuard	DES/AES	QPSK/DSS TS DVB - S2/ MPEG - 2 TS	In-Band	MPEG-2/ AVC
	Nagravision	CSA/DES/ AES	PSK, 8- PSK Turbo/ MPEG - 2 TS	In-Band	MPEG-2/ AVC
	Terrestrial free to air	N/A	8 -VSB/ MPEG - 2 TS	N/A	MPEG-2
Telco	Mediaroom DRM	AES	Multicast/ Unicast-IP/ VDSL/FTTP	IP/ VDSL/ FTTP	AVC
	MediaCipher/ Powerkey	CSA	QAM/ MPEG - 2 TS & IP/BPON or IP/GPON	SCTE-55-1/ SCTE-55-2	MPEG-2/ AVC
	Verimatrix VCAS for IPTV	AES/DES/ CSA	IP Multicast/ MPEG- 2 TS	Generic IP	MPEG-4/ H.264
Googe Fiber TV	Widevine	AES	IP/GPON	IP/GPON	AVC

2.6 Cifrado multimedia en aplicaciones típicas

Dado que la seguridad es un tema critico debido a que el contenido puede ser vulnerable a ataques malintencionados, el cifrado multimedia se ha convertido en una solución clave para garantizar la seguridad del contenido multimedia en las siguientes aplicaciones:

Reproductor multimedia seguro: Los reproductores multimedia pueden incorporar técnicas de cifrado para descifrar datos multimedia, además de reproducir y descomprimir. Esto permite a los proveedores de servicios desarrollar reproductores con características de seguridad integradas, donde los datos cifrados y la clave de descifrado son los datos de entrada. La operación de descifrado y la operación de descompresión deben encajar

correctamente. El orden de estas operaciones puede variar según el método de cifrado utilizado.

Para un reproductor multimedia seguro, es importante que la operación de descifrado sea lo suficientemente rápida para no afectar el rendimiento de la descompresión de datos multimedia en tiempo real. Como se utiliza principalmente cifrado simétrico, el método de cifrado debe tener una alta eficiencia de encriptación para asegurar una reproducción de calidad sin demoras.

Streaming multimedia seguro: El streaming se ha convertido en una herramienta popular para entretenimiento en tiempo real, como el video a pedido, y se utiliza una técnica de encriptación para garantizar la privacidad del contenido, permitiendo solo que los usuarios autorizados lo visualicen. La seguridad y la eficiencia son consideradas propiedades fundamentales en el streaming. Se han propuesto varios métodos para proteger el streaming, pero no todos son adecuados para datos multimedia. A continuación, se presenta tres métodos comunes:

- ISMACryp define ciertos métodos para cifrar y autenticar flujos de datos que utilizan la codificación MPEG-4. Ya que el códec MPEG-4 se usa para comprimir contenido de video, ISMACryp opera en la capa de aplicación.

- SRTP proporciona una forma de encriptar y autenticar paquetes RTP. A diferencia de ISMACryp, que funciona en la capa de aplicación, RTP opera en la capa de transporte, por lo tanto, SRTP funciona en la capa de transporte.

- IPSec proporciona métodos para cifrar y autenticar paquetes IP, así como también ofrece técnicas seguras para el intercambio de información. Ya que la capa de red es responsable de la transferencia de paquetes IP, IPSec funciona en esta capa.

En general, Los métodos que operan en capas superiores ofrecen una mayor seguridad en comparación con los que funcionan en capas inferiores. ISMACryp proporciona seguridad de extremo a extremo, mientras que IPSec solo ofrece seguridad de igual a igual. Además, SRTP e IPSec están diseñados para la transmisión general de datos, mientras que ISMACryp es adecuado para la transmisión de multimedia.

Transcodificación multimedia segura: Actualmente, es posible ver programas de televisión en cualquier lugar gracias a la convergencia de múltiples redes y la codificación escalable. En este proceso, el programa de TV se comprime y se transmite por Internet, se cambia la tasa de bits en el transcodificador y luego se envía a las redes móviles. Para realizar una transcodificación segura, se utiliza un algoritmo de cifrado escalable que

admita la conversión directa de la tasa de bits. Además, se puede utilizar el modo de encriptación parcial para reducir el costo de energía en el terminal móvil.

Distribución multimedia segura: El contenido se transmite del remitente al usuario de manera segura mediante técnicas de cifrado para asegurar la confidencialidad y técnicas de marcas de agua o huellas dactilares para proteger los derechos de autor. En el escenario que se muestra en la figura solo el usuario autorizado puede recibir y descifrar el contenido. Si el usuario A pretende redistribuir una copia al usuario B, se puede detectar la distribución. Por otro lado, si intenta grabar el contenido y luego enviarlo por ejemplo a través de internet, el usuario puede ser rastreado. Para realizar esta funcionalidad, durante el proceso de descifrado en el receptor, se incrusta un código único del usuario, como una ID del decodificador o un código de registro, en el programa de TV de manera imperceptible. De esta manera, el programa descifrado contiene el código único que puede ser extraído y utilizado para identificar a los usuarios ilegales. [24]

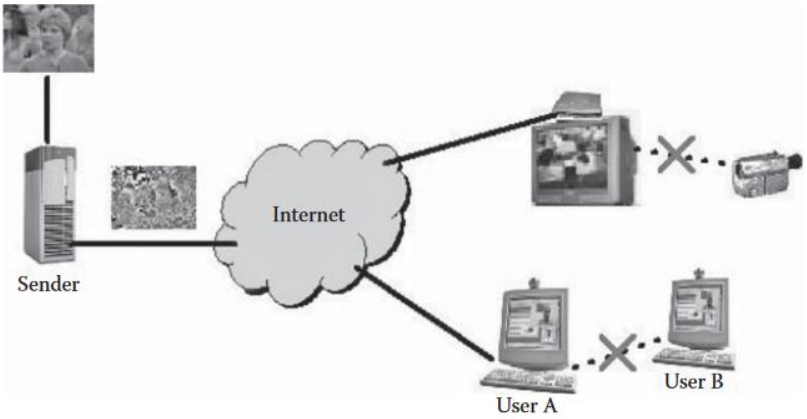


Figura 2.14 Arquitectura de la distribución multimedia. (Fuente: [24])

2.7 Soluciones de protección de contenidos

Las soluciones de protección de contenido son herramientas que permiten a los proveedores de contenido proteger su propiedad intelectual y evitar su uso no autorizado. Algunas soluciones se integran en el hardware de los dispositivos, mientras que otras se basan únicamente en software. Los proveedores de contenido deben evaluar cuidadosamente las diferentes soluciones de protección de contenido disponibles para seleccionar la que mejor se adapte a sus necesidades de seguridad y compatibilidad con los dispositivos de los usuarios. En la siguiente tabla se presenta brevemente las soluciones técnicas de protección para las diferentes arquitecturas en el mercado multimedia.

Tabla 2.2 Técnicas de protección de diferentes arquitecturas. (Fuente: [2])

Medios protegidos	Sistema	Descripción de la protección
Medios Pregrabados	Video en DVD-ROM	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre la unidad de DVD y la PC. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** CSS. • **Renovabilidad del sistema:** Revocación del dispositivo.
	Audio en DVD-ROM	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre la unidad de DVD y la PC. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** CPPM. • **Renovabilidad del sistema:** Revocación del dispositivo
		• **Tipo de protección:** Marca de agua • **Dispositivo de autenticación:** N/A. • **Asociación de derechos digitales:** Watermark. • **Licencia de la tecnología:** 4C/Verance Watermark. • **Renovabilidad del sistema:** N/A
	Video o audio en DVD-R/RW/RAM	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre la unidad de DVD y la PC. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** CPRM. • **Renovabilidad del sistema:** Revocación del dispositivo
		• **Tipo de protección:** Marca de agua. • **Dispositivo de autenticación:** N/A • **Asociación de derechos digitales:** Watermark. • **Licencia de la tecnología:** tbd. • **Renovabilidad del sistema:** N/A.
	Video en cinta digital	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** N/A. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** Protección de copia de alta definición (HDCP). • **Renovabilidad del sistema:** Revocación del dispositivo.
Interfaz Digital	IEEE 1394	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre el transmisor y receptor.

		• **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** DTCP. • **Renovabilidad del sistema:** Revocación del dispositivo.
	Interfaz visual digital (DVI) e Interfaz Multimedia de Alta Definición (HDMI).	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre el transmisor y receptor. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** HDCP. • **Renovabilidad del sistema:** Revocación del dispositivo.
	Interfaz NRSS	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Mutuo entre el transmisor y receptor. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** Estándares abiertos. • **Renovabilidad del sistema:** Revocación del dispositivo.
Broadcasting	Transmisión Satelital (Definido en privado por proveedores de servicios y proveedores CA.	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Ninguno. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** Sistemas de acceso condicional, definido en privado por los proveedores del servicio. • **Renovabilidad del sistema:** Revocación de la tarjeta electrónica.
	Transmisión Terrestre	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Ninguno. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** Sistemas de acceso condicional, marco definido por ATSC. • **Renovabilidad del sistema:** Revocación de la tarjeta electrónica.
Trasmisión por cable		• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Ninguno. • **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** Sistemas de acceso condicional, definido en privado por OpenCable. • **Renovabilidad del sistema:** Revocación de la tarjeta electrónica.
Internet	Sistemas DRM basados en unicast definidos de forma	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Receptor.

	privada y sin interoperabilidad	• **Asociación de derechos digitales:** Metadata. • **Licencia de la tecnología:** DRM. • **Renovabilidad del sistema:** Actualización del software.
	Sistemas DRM basados en multicast	• **Tipo de protección:** Cifrado • **Dispositivo de autenticación:** Transmisor y receptor, dependiendo del tipo de autenticación. • **Asociación de derechos digitales:** Gestión de claves de grupo; Propuestas de marca de agua. • **Licencia de la tecnología:** DRM. • **Renovabilidad del sistema:** tbd.

2.8 Inteligencia artificial en la protección de multimedia.

La Inteligencia Artificial (IA) es una disciplina en constante evolución dentro de la informática. Los sistemas de IA utilizan técnicas de aprendizaje automático para reconocer patrones y aprender a partir de ellos. Estos sistemas pueden procesar grandes cantidades de datos y mejorar su capacidad de realizar tareas específicas a medida que se les proporciona más información.

La IA es una integración de ciencias computacionales que incluye áreas del conocimiento, como la filosofía, las matemáticas, la economía, la neurociencia, la psicología, la ingeniería informática, la cibernética y la lingüística. La IA tiene aplicaciones en una amplia variedad de campos, como la medicina, la educación, la industria manufacturera, la ingeniería, la seguridad y muchos otros.

La tecnología de inteligencia artificial (IA) está avanzando rápidamente y no tardará mucho en estar presente en la mayoría de soluciones para la protección del contenido multimedia. A continuación, se presentan algunas de las formas en que la IA puede ayudar a proteger el contenido multimedia. [25] [26]

Identificación de infracciones de derechos de autor: Los sistemas de detección de infracciones de derechos de autor basados en IA pueden analizar grandes cantidades de contenido multimedia y compararlos con una base de datos de contenido protegido. Si se encuentra que un contenido coincide con un contenido protegido, el sistema puede bloquearlo automáticamente.

Verificación de la autenticidad: La IA puede ser utilizada para verificar la autenticidad de contenido multimedia, como fotos o videos, para determinar si han sido alterados o manipulados de alguna manera.

Análisis de comportamiento: La IA puede ser utilizada para analizar el comportamiento del usuario durante la transmisión para detectar patrones sospechosos, como descarga ilegal o uso indebido del contenido multimedia. Esto puede ayudar a prevenir la piratería y el uso no autorizado del contenido.

Control de acceso: La IA puede ser utilizada para controlar el acceso al contenido multimedia durante la transmisión. Esto puede incluir la asignación de roles y permisos, lo que garantiza que solo los usuarios autorizados tengan acceso al contenido multimedia.

Marcas de agua y huellas digitales: La IA puede ser empleada para proteger el contenido multimedia por medio de la utilización de tecnologías como las marcas de agua y las huellas dactilares digitales. La IA puede generar y analizar estas marcas y huellas para detectar cualquier contenido infractor o para prevenir el uso no autorizado del material multimedia.

Cifrado: La inteligencia artificial puede ser capacitada para generar claves de cifrado altamente seguras. Esto se puede lograr aplicando algoritmos de aprendizaje automáticos para analizar patrones en los datos de cifrado y generar claves más sólidas y difíciles de descifrar. La IA puede examinar grandes cantidades de datos y patrones, lo que puede aumentar la complejidad de las claves de cifrado y hacer que sean más difíciles de adivinar o de ser vulneradas por atacantes. Al utilizar la IA para generar claves de cifrado, también se puede reducir la necesidad de que los humanos diseñen manualmente claves de cifrado complejas, lo que puede ser una tarea tediosa y propensa a errores. La combinación de la IA y la criptografía puede ser un paso importante en la mejora de la seguridad de la información en la era digital.

Ventajas del uso de la inteligencia artificial

- Las tareas son realizadas con mayor rapidez.
- Proporciona mayor escalabilidad en la protección del contenido multimedia al permitir el tratamiento de grandes volúmenes de contenido de manera automatizada.
- Puede detectar ataques que aún no han sido identificados en el contenido multimedia mediante el análisis de patrones y comportamientos sospechosos en el

tráfico de red y la identificación de posibles amenazas antes de que puedan causar daño al contenido multimedia.

- Puede aprender de los ataques anteriores y adaptarse para mejorar la protección contra amenazas futuras.

Desventajas del uso de la inteligencia artificial

- La implementación puede ser costosa, especialmente para las empresas más pequeñas.
- Algunos métodos como el análisis de datos personales, pueden plantear preocupaciones de privacidad.
- La IA no es infalible y puede cometer errores o puede ser mal utilizado, lo que puede resultar en una falsa sensación de seguridad.
- La implementación de sistemas de protección de contenido multimedia con IA puede requerir una cierta cantidad de tiempo y recursos para capacitar y configurar el sistema.

2.9 Blockchain en la protección multimedia

Blockchain es una tecnología de base de datos distribuida que mantiene una lista continua y creciente de registros, llamados bloques, que están vinculados y asegurados criptográficamente. Esta característica hace que los datos almacenados en blockchain sean inmutables, ya que cualquier alteración o eliminación de alguno de los bloques anteriores alteraría la integridad de toda la cadena. Además, la tecnología blockchain se utiliza para establecer registros digitales seguros y transparentes de transacciones

multimedia, incluyendo la gestión de derechos digitales, la autenticación y el seguimiento de los datos transmitidos.

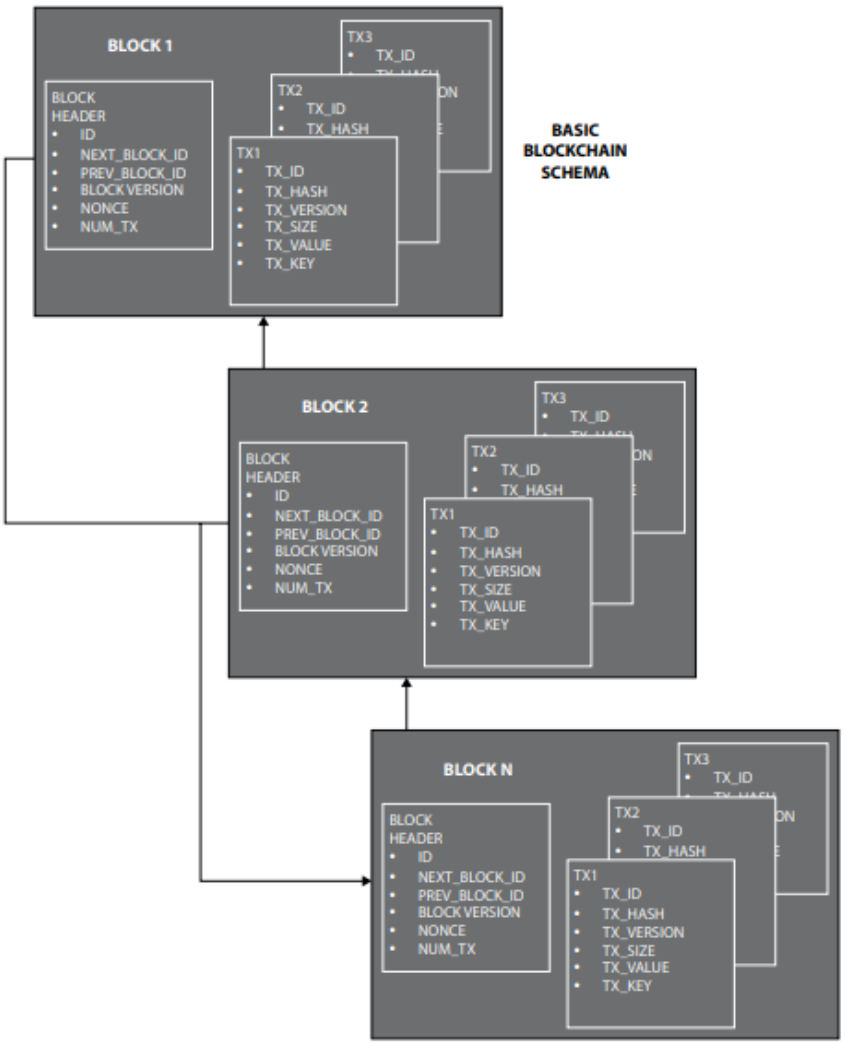


Figura 2.15 Esquema básico de una estructura blockchain. (Fuente: [28])

En cada bloque de la estructura blockchain se tiene un promedio de 1 megabyte que contiene datos de control de aproximadamente 200 bytes tales como una marca de tiempo, un identificador único un enlace a un bloque anterior la versión del bloque, y otros campos que se puede observar en la figura 2.15. El resto del espacio en el bloque está reservado para transacciones, por lo que los archivos multimedia deben ser adaptados y segmentados en fragmentos más pequeños para ser almacenados en la cadena de bloques.

La seguridad multimedia con blockchain se está convirtiendo en una de las principales áreas de investigación en la actualidad, ya que esta tecnología promete garantizar la integridad y seguridad de datos multimedia en un entorno cada vez más vulnerable. Al utilizar blockchain para proteger archivos multimedia, se asegura que estos sean

almacenados en una base de datos distribuida y segura, lo que impide su manipulación o alteración. [27] [29]

Ventajas del uso de blockchain

- La Integridad del contenido multimedia: Blockchain proporciona una forma segura de almacenar y verificar la integridad de los datos multimedia. Cada bloque de datos está vinculado criptográficamente al bloque anterior, lo que dificulta la manipulación o alteración de los archivos multimedia.
- Descentralización: Al estar basado en una red distribuida de nodos, blockchain elimina la necesidad de una autoridad centralizada en la seguridad multimedia. Esto reduce los riesgos de ataques malintencionados y asegura que los datos multimedia estén protegidos incluso en ausencia de una entidad central.
- Transparencia y auditoría: La tecnología blockchain permite un registro transparente y auditable de todas las transacciones relacionadas con el contenido multimedia. Esto facilita la verificación de la autenticidad y el seguimiento de la procedencia del contenido, lo que es especialmente útil en casos de plagio o violaciones de derechos de autor.

desventajas del uso de blockchain

- Dependencia de la tecnología: Al utilizar blockchain para la seguridad multimedia, las organizaciones deben depender de la disponibilidad y confiabilidad de la tecnología blockchain. Cualquier falla o brecha en la red puede tener un impacto en la seguridad y accesibilidad de los datos multimedia.
- Escalabilidad: A medida que la cantidad de contenido multimedia y usuarios aumenta, pueden surgir desafíos de escalabilidad en blockchain. La capacidad de la red para manejar un alto volumen de transacciones puede verse limitada, lo que podría afectar la experiencia del usuario y la capacidad de respuesta en la seguridad multimedia.
- Complejidad técnica: Implementar y operar una red blockchain requiere conocimientos técnicos especializados. La complejidad de la tecnología puede dificultar su adopción y limitar su uso en entornos donde no se disponga de personal capacitado.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En esta sección, se describe los resultados, las conclusiones y las recomendaciones derivadas de la investigación documental sobre los mecanismos de seguridad utilizados en la transmisión de multimedia.

3.1 Resultados

En lo que respecta a proporcionar mecanismos de protección en la transmisión de contenido multimedia y garantizar su seguridad, existen diversas herramientas y técnicas disponibles. Entre las opciones más comunes se encuentran la marca de agua, el cifrado y DRM. Cada una de estas herramientas ofrece enfoques distintos para proteger los archivos. En la siguiente tabla se muestra un resumen y el escenario de aplicación para estas técnicas.

Tabla 3.1 Técnicas usadas en la protección de contenido multimedia.

Medida de protección	Descripción	Escenario de uso
Cifrado	Utiliza algoritmos de cifrado para proteger la confidencialidad de los datos multimedia durante su transmisión y almacenamiento.	Transmisión de contenido multimedia sensible, como archivos de vídeo o audio confidenciales.
Marca de agua	Incrusta información única y oculta en el contenido multimedia para identificar su origen y autenticidad.	Protección de derechos de autor y prevención de la piratería en imágenes, vídeos o audio de propiedad intelectual.
DRM (Digital Rights Management)	Implementa un sistema de gestión de derechos digitales para controlar y proteger el acceso, copia y distribución del contenido multimedia.	Distribución de contenido multimedia con restricciones de acceso y licencias, como películas, música o libros electrónicos.

Cada una de estas técnicas tienen características de seguridad muy importantes que se utilizan en los diferentes escenarios para salvaguardar y proteger contenido transmitido. A continuación, se presentan algunas de las principales características de seguridad de la marca de agua, el cifrado y DRM:

Tabla 3.2 Comparación de características.

Características de seguridad	Cifrado	Marca de agua	DRM
Confidencialidad	✓		
Integridad	✓		
Autenticidad		✓	✓
Protección de derechos de autor		✓	✓
Control de acceso			✓

Prevención de copias no autorizadas			✓
Protección contra transmisión no autorizada	✓		✓
Detección de uso no autorizado			✓
Rastreo de distribución			✓
Verificación de autenticidad de origen	✓		
Protección contra ataques de intermediarios	✓		
Protección contra manipulación de contenido	✓		
Protección de datos personales			✓
Protección contra descarga	✓	✓	✓
Restricciones de reproducción			✓
Protección contra copia de pantalla	✓		✓

Dentro del ámbito del cifrado, se pueden identificar dos tipos principales de criptosistemas: los simétricos y los asimétricos. A continuación, se presenta una tabla que muestra las características principales de cada uno de estos criptosistemas.

Tabla 3.3 Características de los criptosistemas.

Aspecto	Cifrado Simétrico	Cifrado Asimétrico
Clave(s)	Utiliza una única clave compartida	Utiliza un par de claves: pública y privada.
Eficiencia	Más eficiente en términos de rendimiento y velocidad de cifrado/descifrado	Menos eficiente debido a la complejidad computacional requerida.
Seguridad	Menos seguro, ya que la misma clave se utiliza tanto para cifrar como para descifrar	Más seguro, ya que la clave privada se mantiene en secreto y la clave pública se comparte.
Administración de claves	Requiere una gestión y distribución segura de la clave compartida	Requiere una gestión y almacenamiento seguro de la clave privada.
Uso en transmisión de contenido multimedia	Adecuado para transmisiones en tiempo real o cuando se requiere un cifrado y descifrado eficiente	Adecuado cuando se necesita una mayor seguridad y autenticidad, aunque puede ser menos eficiente para transmisiones en tiempo real.
Ejemplos de algoritmos	AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES	RSA, DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography).

Del análisis experimental realizado en [30], se extrae una detallada comparación entre cuatro técnicas de cifrado: Blowfish, AES, XOR y RSA. Este estudio proporciona resultados significativos que permiten evaluar el rendimiento y la efectividad de cada uno de estos métodos criptográficos. En la siguiente tabla se muestra los tiempos de cifrado para archivos de audio de diferente tamaño.

Tabla 3.4 Tiempos de cifrado para distintos archivos de audio. (Fuente: *[30]*).

Time (ms)	100 KB	200 KB	400 KB	800 KB	1600 KB	2000 KB	2400 KB	3200 KB	4000 KB	4800 KB
Blowfish	3	9	16	26	34	64	72	84	88	90
AES	1	1	2	3	3	4	9	12	15	16
XOR	1	2	3	5	6	9	12	15	16	18
RSA	84	195	498	1629	6707	11070	16787	31972	52236	88469

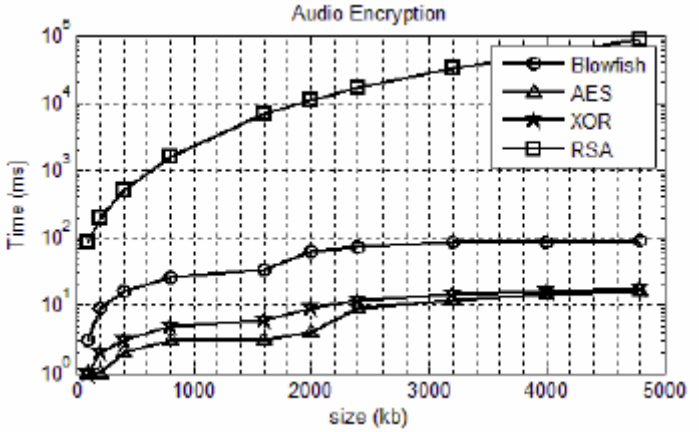


Figura 3.1 Tamaño de archivo vs tiempo de cifrado. (Fuente: [30]).

De acuerdo a los datos de la tabla 3.4 se obtiene una gráfica en la que se observa que RSA tiene los tiempos más elevados para cifrar un archivo de audio, mientras que AES y XOR tienen los tiempos más bajos para el cifrado.

Tabla 3.5 Tiempos de cifrado para distintos archivos de audio. (Fuente: [30]).

Time (ms)	100 KB	300 KB	500 KB	1000 KB	2000 KB	3000 KB	4000 KB	5000 KB	6000 KB	7000 KB
Blowfish	3	5	9	18	39	56	78	94	108	144
AES	1	2	2	3	5	5	7	8	14	19
XOR	1	2	2	4	7	13	14	20	22	26
RSA	83	335	789	2527	11653	39703	54328	88396	129695	187856

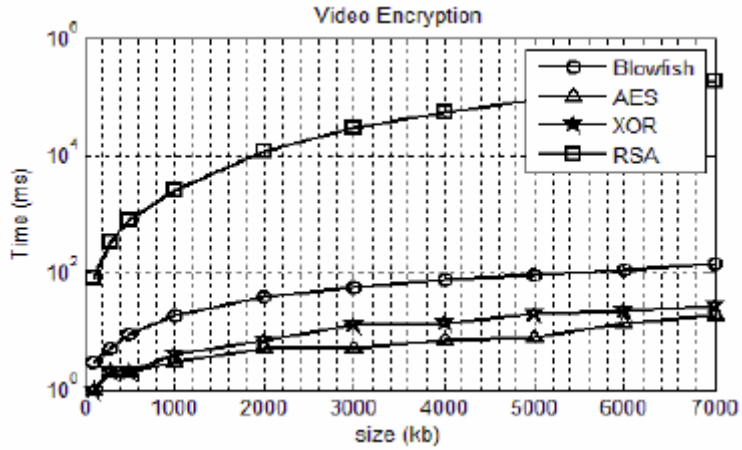


Figura 3.2 Tamaño de archivo vs tiempo de cifrado. (Fuente: [30]).

En el cifrado de archivos de video, RSA sigue siendo el algoritmo que presenta mayores tiempos de cifrado, mientras que XOR y AES ofrecen tiempos más bajos, lo que se traduce en una mayor eficiencia en términos de rendimiento y velocidad para los cifrados de tipo simétricos.

Las soluciones de protección de contenido multimedia se basan en una combinación de cifrado, marca de agua, protección DRM, o codificación. La selección de la protección adecuada dependerá del valor potencial del contenido y del nivel de amenaza que pueda representar un atacante. En la tabla 3.6 se presenta el nivel de riesgo de algunos tipos de contenido multimedia.

Tabla 3.6 Nivel de riesgo y mecanismo de protección.

Nivel de riesgo	Contenido Multimedia	Mecanismos de Protección
Bajo	Videos personales	Encriptación básica, protección con contraseña.
	Música no comercial	Protección DRM básica.
	Fotos personales	Acceso restringido, encriptación básica.
	Presentaciones no confidenciales	Protección con contraseña, control de acceso
Medio	Transmisión de video en línea	Codificación de video, protección DRM.
	Archivos de audio comerciales	Protección DRM avanzada.
	Archivos de imágenes comerciales	Marcas de agua invisibles, protección DRM.
Alto	Contenido confidencial empresarial	Encriptación avanzada, autenticación fuerte.
	Aplicaciones militares	Cifrado de grado militar, autenticación biométrica.
	Transmisión de videoconferencia segura	Cifrado de extremo a extremo, autenticación de usuarios
	Transmisión en vivo de eventos	Protección DRM avanzada, autenticación de usuarios.
	Contenido de investigación científica	Encriptación de extremo a extremo, control de acceso.

3.2 Conclusiones

- La seguridad en la transmisión de contenido multimedia desempeña un papel fundamental en el entorno digital actual. A medida que la tecnología avanza y la accesibilidad a los medios de comunicación se expande, también aumentan los riesgos asociados con la piratería, la manipulación y el uso no autorizado de la información. La implementación de medidas de seguridad adecuadas es esencial para salvaguardar la confidencialidad, integridad y disponibilidad de los datos

multimedia. Además, los mecanismos usados en la transmisión de multimedia contribuyen a preservar la privacidad de los usuarios al proteger sus datos personales y evitar la exposición no deseada de información sensible.

- La privacidad y el control de acceso son elementos fundamentales en la transmisión de contenido multimedia. La protección de la privacidad asegura que la información personal y sensible esté protegida durante la transmisión, esto se logra con técnicas de cifrado para proteger los datos durante la transmisión, asegurando que solo los destinatarios autorizados puedan acceder y decodificar la información. El control de acceso garantiza que solo los usuarios autorizados puedan acceder al contenido y realizar acciones permitidas, para ello se implementan políticas de gestión de derechos digitales (DRM).

- Una técnica inmediata y efectiva ante la piratería es la codificación ya que permite comprimir y convertir los datos multimedia en formatos más eficientes para su almacenamiento y transmisión, al tiempo que puede proporcionar cierto nivel de protección contra accesos no autorizados. Sin embargo, es importante tener en cuenta que la codificación por sí sola no es suficiente para garantizar una seguridad completa, pero es una solución rápida para ciertos proveedores de contenido multimedia.

- Tanto el cifrado simétrico como el cifrado asimétrico son elementos esenciales para garantizar la protección del contenido multimedia. El cifrado simétrico se destaca por su eficiencia y velocidad en el cifrado y descifrado de datos, lo que lo hace adecuado para aplicaciones que requieren un procesamiento rápido de grandes volúmenes de contenido multimedia. Por otro lado, el cifrado asimétrico ofrece ventajas en términos de seguridad y autenticación, ya que utiliza un par de claves pública y privada para cifrar y descifrar los datos. La elección entre el cifrado simétrico y asimétrico depende de las necesidades y requisitos específicos de seguridad de la transmisión de contenido multimedia. Ambos métodos pueden complementarse entre sí para brindar una protección más sólida.

- Las soluciones de Sistema de Acceso Condicional (CAS) brindan mecanismos efectivos para controlar el acceso y prevenir el uso no autorizado. Ofrecen una combinación de tecnologías de cifrado, autenticación y gestión de derechos para garantizar que solo los usuarios autorizados puedan acceder y disfrutar del contenido. Esto ayuda a proteger los intereses de los creadores y distribuidores de contenido, así como a garantizar una experiencia de visualización segura y satisfactoria para los usuarios. Además, las soluciones CAS proporcionan un nivel

adicional de seguridad al implementar controles robustos y monitoreo continuo para detectar y prevenir cualquier intento de piratería o violación de derechos de autor.

- La protección de contenido multimedia depende directamente del valor que se le atribuye a dicho contenido. Es importante encontrar un equilibrio entre el costo de implementar medidas de protección y el valor del contenido en sí. En el caso de aplicaciones de entretenimiento, donde el contenido no involucra información crítica o confidencial, a menudo es suficiente utilizar mecanismos básicos de protección. Si el contenido multimedia tiene un alto valor comercial, contiene información confidencial o está sujeto a regulaciones específicas, entonces se requerirán medidas de protección más sólidas y personalizadas para mitigar los riesgos y preservar la integridad del contenido.

- Los nuevos mecanismos como la inteligencia artificial (IA) o la tecnología blockchain, han revolucionado la protección de contenido multimedia. La IA ofrece capacidades avanzadas para detectar y prevenir ataques, generando claves de cifrado más seguras y proporcionando un análisis exhaustivo de los datos. Por su parte, la tecnología blockchain ofrece una solución descentralizada, transparente e inmutable para asegurar la integridad y autenticidad de los datos multimedia. Es importante tener en cuenta que ninguna solución es completamente infalible, y se debe realizar un análisis cuidadoso de las necesidades y requerimientos específicos de cada caso. Al combinar y utilizar adecuadamente estos nuevos mecanismos, se puede lograr un nivel más alto de seguridad y privacidad en la transmisión y protección del contenido multimedia.

3.3 Recomendaciones

- Para garantizar una protección apropiada de contenido multimedia, es necesario evaluar y determinar previamente la importancia y el nivel de confidencialidad del mismo. No todos los contenidos requieren el mismo nivel de seguridad, por lo que las medidas de protección deben ajustarse en función de sus características. Esto garantiza que se apliquen las medidas de seguridad necesarias de manera proporcional a la sensibilidad y relevancia del contenido.

- Es aconsejable utilizar una combinación de distintas técnicas de seguridad, como el cifrado, las marcas de agua, políticas DRM y la autenticación de usuarios, para proteger el contenido multimedia de manera efectiva, puesto que, cada uno de estos mecanismos aporta una capa adicional de seguridad y juntos crean una barrera sólida contra accesos no autorizados. Al implementar esta variedad de

medidas, se incrementa la protección del contenido multimedia y se reduce significativamente el riesgo de manipulación, robo o uso no autorizado.

- Para garantizar la seguridad en la transmisión de contenido multimedia, es esencial llevar a cabo evaluaciones periódicas de seguridad. Estas evaluaciones permiten identificar posibles vulnerabilidades en los sistemas de transmisión, lo que a su vez brinda la oportunidad de corregir cualquier debilidad y fortalecer la seguridad. Al conocer las posibles amenazas, se pueden implementar medidas preventivas y correctivas adecuadas para proteger la integridad y confidencialidad de los datos transmitidos. De esta manera, se logra establecer un entorno de transmisión seguro y confiable para el contenido multimedia, generando confianza tanto en los proveedores como en los usuarios finales.
- El uso del cifrado simétrico es recomendado en situaciones que requieren un procesamiento rápido y eficiente de datos, especialmente cuando se trata de comunicaciones entre partes confiables. Por otro lado, el cifrado asimétrico resulta más apropiado cuando se busca un nivel más elevado de seguridad. La elección del tipo de cifrado a utilizar dependerá de las necesidades específicas de seguridad y rendimiento de la aplicación multimedia. En algunos casos, puede ser beneficioso combinar ambos tipos de cifrado para aprovechar sus fortalezas en diferentes aspectos de la protección de datos.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] M. Pagani, Cur., *Encyclopedia of Multimedia Technology and Networking, Second Edition:* IGI Global, 2009. doi: 10.4018/978-1-60566-014-1.

[2] B. Furht et D. Kirovski, *Multimedia security handbook*. in Internet and communications. Boca Raton, Fla: CRC Press, 2005.

[3] H. Purchase, 'Defining multimedia', *IEEE Multimed.*, t. 5, n. 1, pp. 8–15, mar. 1998, doi: 10.1109/93.664737.

[4] S. Banerjee, *Elements of Multimedia*, 1º ed. Boca Raton : Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc, 2019.: Chapman and Hall/CRC, 2019. doi: 10.1201/9780429433207.

[5] K. R. Rao, D. N. Kim, et J. J. Hwang, *Video coding standards: AVS China, H.264/MPEG-4 PART 10, HEVC, VP6, DIRAC and VC-1*. in Signals and Communication Technology. Dordrecht: Springer Netherlands, 2014. doi: 10.1007/978-94-007-6742-3.

[6] Z.-N. Li, M. S. Drew, et J. Liu, *Fundamentals of Multimedia*. in Texts in Computer Science. Cham: Springer International Publishing, 2014. doi: 10.1007/978-3-319-05290-8.

[7] A. K. Singh et A. Mohan, Curs., *Handbook of Multimedia Information Security: Techniques and Applications*. Cham: Springer International Publishing, 2019. doi: 10.1007/978-3-030-15887-3.

[8] B. Furht, Cur., *Encyclopedia of multimedia*, 2nd ed. New York: Springer, 2008.

[9] M. G. Christel, *Automated Metadata in Multimedia Information Systems: Creation, Refinement, Use in Surrogates, and Evaluation*. in Synthesis Lectures on Information Concepts, Retrieval, and Services. Cham: Springer International Publishing, 2009. doi: 10.1007/978-3-031-02258-6.

[10] C. Poole et J. Bradley, *Developer's Digital Media Reference: New Tools, New Methods*. Taylor & Francis Group, 2017.

[11] L. E. Álvarez, ‘La Visión de América Latina sobre el Reglamento General de Protección de Datos’, *Coment. Int. Rev. Cent. Andino Estud. Int.*, n. 19, Art. n. 19, 2019, doi: 10.32719/26312549.2019.19.4.

[12] J. J. R. Fonseca, J. González-Argote, et C. L. Vázquez, ‘Multimedia “Seguridad y Protección” para los directivos y personal de seguridad y protección de la salud’, *Infodir Rev. Inf. Para Dir. En Salud*, t. 12, n. 22, pp. 9–15, feb. 2016.

[13] A. M. Porcelli, ‘LOS BIENES DIGITALES Y EL DERECHO DE AUTOR EN INTERNET. LA DENOMINADA “PIRATERÍA INFORMÁTICA”’, t. 2.

[14] Á. G. Vieites, *MF0489_3 Sistemas Seguros de Acceso y Trans. de Datos*. Ra-Ma Editorial, 2011.

[15] N. Molavi et X. Zhao, ‘A Security Study of Digital TV Distribution Systems’.

[16] *Multimedia Security Technologies for Digital Rights Management*. Elsevier, 2006. doi: 10.1016/B978-0-12-369476-8.X5000-3.

[17] Department of Computer Science and Engineering, Lovely Professional University, Jalandhar (Punjab), India. *et al.*, ‘A Novel Encryption RAAM Algorithm in Different Multimedia Applications’, *Int. J. Soft Comput. Eng.*, t. 10, n. 5, pp. 9–13, mai. 2021, doi: 10.35940/ijsce.F3492.0510521.

[18] P. Rogaway, ‘Evaluation of Some Blockcipher Modes of Operation’.

[19] A. Uhl et A. Pommer, *Image and video encrytion: from digital rights management to secured personal communication*. in Advances in information security, no. 15. New York, NY, USA: Springer, 2005.

[20] C. Paar et J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. doi: 10.1007/978-3-642-04101-3.

[21] B. Furht, Cur., *Multimedia Technologies and Applications for the 21st Century*. Boston, MA: Springer US, 1998. doi: 10.1007/978-0-585-28767-6.

[22] S. Lian et Y. Zhang, ‘Protecting Mobile TV Multimedia Content in DVB/GPRS Heterogeneous Wireless Networks’.

[23] U. S. F. C. Commission, *FCC Record: A Comprehensive Compilation of Decisions, Reports, Public Notices, and Other Documents of the Federal Communications Commission of the United States*. The Commission, 2015.

[24] S. Lian, *Multimedia content encryption: techniques and applications*. Boca Raton: CRC Press, 2009.

[25] J.-S. Pan, J. Li, O.-E. Namsrai, Z. Meng, et M. Savić, Curs., *Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the 16th International Conference on IIHMSP in conjunction with the 13th international conference on FITAT, November 5-7, 2020, Ho Chi Minh City, Vietnam, Volume 1*, t. 211. in Smart Innovation, Systems and Technologies, vol. 211. Singapore: Springer Singapore, 2021. doi: 10.1007/978-981-33-6420-2.

[26] K. C. A. Khanzode, 'ADVANTAGES AND DISADVANTAGES OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING: A LITERATURE REVIEW'.

[27] A. Qureshi et D. Megías Jiménez, 'Blockchain-Based Multimedia Content Protection: Review and Open Challenges', *Appl. Sci.*, t. 11, n. 1, p. 1, dec. 2020, doi: 10.3390/app11010001.

[28] J. J. Bambara, P. R. Allen, K. Iyer, R. Madsen, S. Lederer, et M. Wuehler, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw Hill Professional, 2018.

[29] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, et S. Rajput, 'Secure Data Transmission of Electronic Health Records Using Blockchain Technology', *Electronics*, t. 12, n. 4, Art. n. 4, ian. 2023, doi: 10.3390/electronics12041015.

[30] Md. M. Ahamad et Md. I. Abdullah, 'Comparison of Encryption Algorithms for Multimedia', *Rajshahi Univ. J. Sci. Eng.*, t. 44, pp. 131–139, nou. 2016, doi: 10.3329/rujse.v44i0.30398.