Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

T.807

(05/2006)

SERIE T: TERMINALES PARA SERVICIOS DE TELEMÁTICA

Tecnología de la información – Sistema de codificación de imágenes JPEG 2000: Sistema JPEG 2000 seguro

Recomendación UIT-T T.807

UIT-T

Unión Internacional de Telecomunicaciones

NORMA INTERNACIONAL ISO/CEI 15444-8
RECOMENDACIÓN UIT-T T.807

Tecnología de la información – Sistema de codificación de imágenes JPEG 2000: Sistema JPEG 2000 seguro

Resumen

El objetivo de la presente Recomendación | Norma Internacional es establecer una sintaxis que permita la aplicación de servicios de seguridad a los datos de imágenes codificadas JPEG 2000. Estos servicios de seguridad incluyen la confidencialidad, la verificación de la integridad, la autenticación de fuente, el acceso condicional, la difusión progresiva segura y la transcodificación segura. La sintaxis permite la aplicación total o parcial de estos servicios de seguridad a datos de imágenes codificadas y no codificadas. Se mantienen las características inherentes de JPEG 2000, como la escabilidad y el acceso a distintas zonas espaciales, niveles de resolución, componentes de color y capas de calidad, otorgando al mismo tiempo servicios de seguridad a estos elementos.

Orígenes

La Recomendación UIT-T T.807 fue aprobada el 29 de mayo de 2006 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. Se publica también un texto idéntico como Norma Internacional ISO/CEI 15444-8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

En la "Era digital", Internet ofrece múltiples nuevas oportunidades a los detentores de derechos en cuanto a la distribución electrónica de sus obras (libros, vídeos, música, imágenes, etc.).

Al mismo tiempo, las nuevas tecnologías de la información simplifican en gran medida el acceso al contenido por parte del usuario, lo que va a la par con todo el problema que suponen las copias digitales pirateadas, con la misma calidad que los originales, y la "compartición de ficheros" en las redes par a par, que la industria de contenido sigue considerando responsables de grandes pérdidas.

La Organización Mundial de la Propiedad Intelectual (OMPI) y sus Estados Miembros (170) tiene un importante papel que desempeñar a la hora de garantizar la correcta protección de los derechos de autor, y la expresión cultural e intelectual que representan, en el siglo XXI. La nueva economía digital y los creadores de todos los países dependen de ello. Además, en diciembre de 1996 se promulgó el Tratado de la OMPI sobre derechos de autor, que contiene dos importantes artículos (11 y 12) sobre medidas tecnológicas y obligaciones relativas a la información sobre la gestión de derechos:

Artículo 11
Obligaciones relativas a las
medidas tecnológicas

Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley.

Artículo 12
Obligaciones relativas a la información
sobre la gestión de derechos

(1) Las Partes Contratantes proporcionarán recursos jurídicos efectivos contra cualquier persona que, con conocimiento de causa, realice cualquiera de los siguientes actos sabiendo o, con respecto a recursos civiles, teniendo motivos razonables para saber que induce, permite, facilita u oculta una infracción de cualquiera de los derechos previstos en el presente Tratado o en el Convenio de Berna:

(i) suprima o altere sin autorización cualquier información electrónica sobre la gestión de derechos;

(ii) distribuya, importe para su distribución, emita, o comunique al público, sin autorización, ejemplares de obras sabiendo que la información electrónica sobre la gestión de derechos ha sido suprimida o alterada sin autorización.

(2) A los fines del presente Artículo, se entenderá por "información sobre la gestión de derechos" la información que identifica a la obra, al autor de la obra, al titular de cualquier derecho sobre la obra, o información sobre los términos y condiciones de utilización de las obras, y todo número o código que represente tal información cuando cualquiera de estos elementos de información estén adjuntos a un ejemplar de una obra o figuren en relación con la comunicación al público de una obra.

Este Tratado representa una sólida base para la protección de la propiedad intelectual. En 2004 cerca de 50 países ratificaron este importante Tratado. Por consiguiente, se espera que las herramientas y métodos de protección recomendados en JPEG 2000 garanticen la seguridad en las transacciones, protejan el contenido (IPR) y las tecnologías.

Las cuestiones relativas a la seguridad, como la autenticación, la integridad de los datos, la protección del derecho de autor y la propiedad intelectual, la privacidad, el acceso condicional, la confidencialidad, el rastreo de transacciones, por sólo mencionar algunas, son características importantes de muchas aplicaciones de imagen que utilizan JPEG 2000.

Los medios tecnológicos para la protección de contenido digital se describen y pueden lograrse de distintas maneras, como la marca de agua digital, la firma digital, la criptación, los metadatos, la autenticación y la comprobación de la integridad.

La Parte 8 de la norma JPEG 2000 pretende proporcionar herramientas y soluciones en forma de especificaciones que permitan a las aplicaciones generar, consumir e intercambiar trenes codificados JPEG 2000 seguros. A esto se le denomina **JPSEC**.

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Sistema de codificación de imágenes JPEG 2000: Sistema JPEG 2000 seguro

1 Alcance

En la presente Recomendación | Norma Internacional se especifica el marco general, los conceptos y la metodología para la aplicación de sistemas de seguridad a los trenes codificados JPEG 2000. El alcance de esta Recomendación | Norma Internacional se reduce a la definición de:

1) Una sintaxis de tren codificado normativa que contiene información para interpretar los datos de imágenes seguros.
2) Un proceso normativo para el registro de herramientas JPSEC ante una autoridad de registro que otorga un identificador único.
3) Ejemplos informativos de herramientas JPSEC en casos prácticos típicos.
4) Directrices informativas sobre la implementación de servicios de seguridad y los metadatos correspondientes.

La presente Recomendación | Norma Internacional no pretende describir aplicaciones de imágenes seguras específicas ni limitar la seguridad de imágenes a técnicas específicas, sino crear un marco que permita ampliaciones posteriores a medida que evolucionen las técnicas de imagen seguras.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

– Recomendación UIT-T T.800 (2002) | ISO/CEI 15444-1:2004, *Tecnología de la información – Sistema de codificación de imágenes JPEG2 2000: Sistema de codificación básico*.

– Recomendación UIT-T T.801 (2002) | ISO/CEI 15444-2:2004, *Tecnología de la información – Sistema de codificación de imágenes JPEG2 2000: Extensiones*.

3 Términos y definiciones

A los efectos de la presente Recomendación | Norma Internacional, se utilizan las siguientes definiciones. Las definiciones contenidas en la Rec. UIT-T T.800 | ISO/CEI 15444-1, cláusula 3, se aplican a la presente Recomendación | Norma Internacional.

3.1 **control de acceso**: Prevención de utilización no autorizada de un recurso, incluida la utilización de un recurso de manera no autorizada.

3.2 **autenticación**: Proceso de verificación de la identidad reclamada por o para una entidad de sistema.

3.2.1 **autenticación de fuente**: Verificación de que una entidad fuente (por ejemplo, usuario/parte) es efectivamente la entidad fuente que se reclama.

3.2.2 autenticación de imagen frágil/semifrágil: Proceso tanto de autenticación de la fuente de la imagen como de verificación de la integridad de datos/contenido de imagen que debería poder detectar cualquier modificación de la señal e identificar dónde se ha producido y, posiblemente, como era la señal antes de ser modificada.

NOTA – Sirve para demostrar la autenticidad de un documento. La diferencia entre la autenticación de imagen frágil y semifrágil es que la primera verifica la integridad de los datos de imagen y la segunda verifica la integridad del contenido de imagen.

3.3 confidencialidad: Característica de la información cuando no se pone a disposición de personas, entidades o procesos no autorizados, ni se les divulga.

3.4 división de datos: Método para proteger datos sensibles de acceso no autorizado mediante criptación de los datos y almacenamiento de distintas partes del fichero en distintos servidores.

NOTA – Cuando se accede a datos divididos, cada una de las partes se extrae, combina y descripta. Una persona no autorizada habría de conocer la ubicación de los servidores que contienen las partes, poder acceder a cada uno de ellos, saber qué datos es necesario combinar y, descriptarlos.

3.5 descriptación, desciframiento: Transformación inversa a la criptación.

3.6 firma digital: Datos anexos a una unidad de datos que permite al receptor de la unidad de datos demostrar la fuente y la integridad de los datos y protegerlos contra la falsificación, por ejemplo, por parte del receptor, o transformación criptográfica de la unidad de datos.

3.7 criptación: Transformación reversible de los datos mediante un algoritmo criptográfico para producir un texto cifrado, es decir, esconder el contenido de la información de los datos.

NOTA – Un término alternativo para algoritmo de criptación es cifrado.

3.8 huellas digitales: Características de un objeto que tienden a distinguirlo de otros objetos similares para permitir a su propietario seguir la pista de los usuarios autorizados que los distribuyen de manera ilegal.

NOTA – A este respecto, se suele hablar de huellas digitales en el contexto del seguimiento de traidores.

3.9 función generadora: Función que establece la correspondencia entre cadenas de bits y cadenas de bits de longitud fija, satisfaciendo las dos siguientes condiciones:

NOTA – Para un determinado producto, es computacionalmente imposible encontrar un producto origen que se corresponde con el resultado. Para un determinado producto origen es computacionalmente imposible encontrar un segundo producto origen que corresponda al mismo resultado. Esta imposibilidad computacional depende de los requisitos de seguridad específicos del usuario y del entorno.

3.10 integridad: Propiedad de las cosas para poder salvaguardar su exactitud y entereza.

3.10.1 integridad de los datos de imagen: Propiedad de los datos que no han sido alterados o destruidos de manera no autorizada.

3.10.2 integridad del contenido de imagen: Garantía de que el contenido de imagen no ha sido modificado por partes no autorizadas de manera que se modifique su significado perceptual.

NOTA – Permite la realización de operaciones de preservación del contenido en la imagen sin desencadenar una alarma de integridad.

3.11 aplicación de JPSEC: Proceso de software o hardware capaz de consumir trenes codificados JPSEC interpretando la sintaxis JPSEC para proporcionar los servicios de seguridad especificados.

NOTA – Una aplicación JPSEC utiliza una o varias herramientas JPSEC.

EJEMPLO – Una aplicación JPSEC puede leer trenes codificados JPSEC criptados, descriptarlos cuando se le otorgue la clave adecuada y proporcionar los datos de imagen sin codificar originales JPEG 2000.

3.12 tren codificado JPSEC: Secuencia de bits resultantes de la codificación y aplicación de mecanismos de seguridad a una imagen utilizando la codificación JPEG 2000 y las herramientas de seguridad JPSEC.

3.12.1 creador JPSEC: Entidad que crea un tren codificado JPSEC a partir de una imagen, un tren codificado JPEG 2000 u otro tipo de tren codificado JPSEC para proporcionar servicios JPSEC.

3.12.2 consumidor JPSEC: Entidad que recibe un tren codificado JPSEC y aplica un servicio JPSEC de acuerdo con ese tren codificado.

3.13 servicio JPSEC: Servicio que proporciona seguridad para el consumo de imágenes JPEG 2000. El servicio contrarresta los ataques a la seguridad y utiliza cualquiera de las diversas herramientas JPSEC.

3.14 autoridad de registro JPSEC: Entidad encargada de otorgar un identificador único para denominar una herramienta y almacenar la lista de parámetros de la descripción de las herramientas JPSEC.

3.15 herramienta JPSEC: Proceso de hardware o software que utiliza técnicas de seguridad para aplicar un servicio de seguridad.

3.15.1 herramienta JPSEC normativa: Herramienta JPSEC que utiliza modelos predefinidos para la descriptación, autenticación o función generadora especificados por la parte normativa de esta Recomendación | Norma Internacional.

3.15.2 herramienta JPSEC no normativa: Herramienta JPSEC especificada por un número de identificación que le otorga la autoridad registro JPSEC o por una aplicación definida por el usuario.

3.15.3 herramienta JPSEC definida por el usuario: Herramienta JPSEC no normativa definida por una aplicación definida por el usuario.

3.15.4 herramienta de la autoridad de registro JPSEC: Herramienta JPSEC no normativa definida por la autoridad de registro JPSEC.

3.16 descripción de la herramienta JPSEC: Descripción de los parámetros utilizados por una herramienta JPSEC.

NOTA – Sin embargo, la descripción de la herramienta JPSEC no describe el algoritmo o método utilizados. La descripción de la herramienta JPSEC está formada por dos partes: la lista de parámetros y sus valores. En el caso de las herramientas JPSEC normativas, la lista de parámetros está definida por la norma. En el caso de las herramientas JPSEC no normativas, la lista de parámetros puede estar definida por la autoridad de registro. En ambos casos, los valores de parámetros son los especificados en los segmentos marcadores SEC e INSEC.

3.17 clave: Secuencia de símbolos que controla las operaciones de cifrado y descifrado

3.17.1 claves simétricas: Par de claves para cuya utilización el creador y el receptor utilizan la misma clave secreta o dos claves que pueden fácilmente derivarse mutuamente en un sistema criptográfico.

3.17.2 par de claves asimétricas: Par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.

3.17.2.1 clave privada: Clave de un par de claves asimétricas de una entidad que no debe divulgarse.

3.17.2.2 clave pública: Clave de un par de claves asimétricas de una entidad que puede divulgarse.

3.18 generación de claves, función generadora de claves: Función que, a partir de una serie de parámetros, de los cuales al menos uno de ellos debe ser secreto, elabora claves adecuadas al algoritmo o aplicación de que se trate.

NOTA – La función debe garantizar que sea computacionalmente imposible deducir el resultado sin conocer previamente el material original secreto.

3.19 gestión de claves: Generación, almacenamiento, distribución, eliminación, archivo y aplicación de claves de acuerdo con una política de seguridad.

3.20 emulación de marcador: Texto cifrado resultante de un proceso de criptación que contiene un código inicial JPEG.

3.21 algoritmo codificado de autenticación de mensaje, función de verificación criptográfica, función de verificación global criptográfica: Algoritmo para el cómputo de una función que establece la correspondencia entre cadenas de bits y una clave secreta y cadenas de bits de longitud fija, satisfaciendo las dos siguientes condiciones:

- para cualquier clave y cualquier cadena de origen la función ha de aplicarse eficientemente;
- para cualquier clave fija, sin conocimiento previo de la clave, debe ser computacionalmente imposible deducir el valor de la función de cualquier cadena nueva, incluso conociendo las cadenas de origen y los correspondientes valores de función, cuando el valor de la enésima cadena origen se ha elegido tras observar el valor de los primeros i-1 valores de la función.

NOTA – La posibilidad computacional depende de los requisitos de seguridad específicos del usuario y del entorno.

3.21.1 código de autenticación del mensaje, (MAC, *message authentication code*): Cadena de bits resultado de la aplicación de un algoritmo MAC.

3.22 no repudio: Vinculación de una entidad a la transacción en que participa, de manera que esta transacción no pueda repudiarse (denegarse) más tarde.

NOTA – Es decir, el receptor de la transacción puede demostrar a un tercero neutro que el remitente de la transacción es efectivamente el que se supone.

3.23 paquete: Parte de un tren de bits JPEG 2000 Parte 1 que comprende el encabezamiento de paquete y los datos de imagen comprimidos de una capa del precinto de una resolución de un componente losa.

NOTA – Esto difiere del término "paquete" utilizado en la transmisión de datos a través de una red.

3.24 protección: Proceso para asegurar el contenido.

3.24.1 modelo de protección: Modelo o lista de campos de parámetros necesarios para la aplicación de un método de protección.

3.24.2 método de protección: Método utilizado para crear o consumir contenido protegido, como la criptación, la descriptación, la autenticación y la verificación de integridad.

3.25 seguridad: Todos los aspectos relacionados con la definición, consecución y mantenimiento de la confidencialidad, la integridad, la disponibilidad, la responsabilidad, la autenticidad y la fiabilidad.

NOTA – Un producto, sistema o servicio se considera seguro en la medida en que sus usuarios pueden confiar en que funciona (o funcionará) de la manera prevista. Se utiliza generalmente en el contexto de la evaluación de amenazas reales o supuestas.

3.26 sintaxis de señalización: Especificación del formato de trenes codificados JPSEC que contienen toda la información requerida para el consumo de imágenes JPEG 2000 seguras.

3.27 transcodificación: Operación que consiste en tomar un tren codificado comprimido y adaptarlo o convertirlo para producir otro tren codificado comprimido que tiene las características deseadas.

EJEMPLO – El tren codificado comprimido resultante puede representar una imagen con una resolución espacial inferior o una velocidad binaria inferior que el tren codificado comprimido original.

3.27.1 transcodificación segura: Operación que consiste en la transcodificación o adaptación de contenido comprimido original sin desproteger el contenido.

NOTA – El término transcodificación segura se utiliza por oposición a transcodificación para subrayar que la transcodificación se realiza sin poner en peligro la seguridad. La transcodificación segura también puede denominarse transcodificación de calidad en el dominio de la criptación.

3.28 marca de agua: Señal añadida imperceptiblemente a la cobertura de la señal para transportar datos ocultos.

3.28.1 marcado de agua: Proceso que inserta imperceptiblemente datos de información en los datos multimedia de alguna de las dos siguientes maneras:

- Con pérdidas, lo que significa que no podrá recuperarse la cobertura de señal exacta una vez incorporada la marca de agua.
- Sin pérdidas, que significa que podrá recuperarse la cobertura de señal exacta una vez extraída la marca de agua.

4 Símbolos y abreviaturas

A los efectos de la presente Recomendación | Norma Internacional, se utilizan las siguientes abreviaturas.

BAS	Segmento con alineación de bytes (*byte aligned segment*)
FBAS	Segmento con alineación de bytes por campos (*field byte aligned segment*)
G	Granularidad (*granularity*)
GL	Nivel de granularidad (*granularity level*)
INSEC	Marcador de seguridad en el tren codificado (*in-codestream security marker*)
IP	Propiedad intelectual con respecto a la tecnología *(intellectual property related to technology*)
IPR	Derechos de propiedad intelectual relacionados con el contenido (*intellectual property rights related to content*)
JPSEC	JPEG 2000 seguro (*secure JPEG 2000*)
KT	Modelo de clave (*key template*)
LSB	Bit menos significativo (*least significant bit*)
MAC	Código de autenticación de mensaje (*message authentication code*)
MSB	Bit más significativo (*most significant bit*)
PD	Dominio de procesamiento (*processing domain*)
PKI	Infraestructura de clave pública (*public key infrastructure*)
PO	Orden de procesamiento (*processing order*)
RA	Autoridad de registro (*registration authority*)
RBAS	Segmento con alineación de bytes por gamas (*range byte aligned segment*)
SEC	Marcador de seguridad (*security marker*)
T	Modelo (*template*)
V	Valores (*values*)

VL Lista de valores (*value list*)

ZOI Zona de influencia (*zone of influence*)

5 Sintaxis JPSEC (normativa)

5.1 Generalidades de JPSEC

JPSEC define un marco para la aplicación de medidas de seguridad a los datos codificados JPEG 2000. El núcleo de la presente Recomendación | Norma Internacional es la Especificación de la sintaxis de las imágenes JPEG 2000 seguras, el *tren codificado JPSEC*. La sintaxis se dirige a los datos codificados JPEG 2000 y permite la protección de todo el tren codificado o de partes de éste. En cualquier caso, los datos protegidos (es decir, el tren codificado JPSEC) debe ajustarse a la sintaxis normativa definida por la presente Recomendación | Norma Internacional.

Al tren codificado JPSEC se asocian una serie de *servicios de seguridad JPSEC*, incluida la confidencialidad y la autenticación del origen y el contenido.

La *sintaxis de señalización* especifica:

- qué servicios de seguridad están asociados con los datos de imagen;
- qué *herramientas JPSEC* se necesitan para proporcionar los servicios correspondientes;
- cómo se aplican las herramientas JPSEC;
- qué parte de los datos de imagen se protegen.

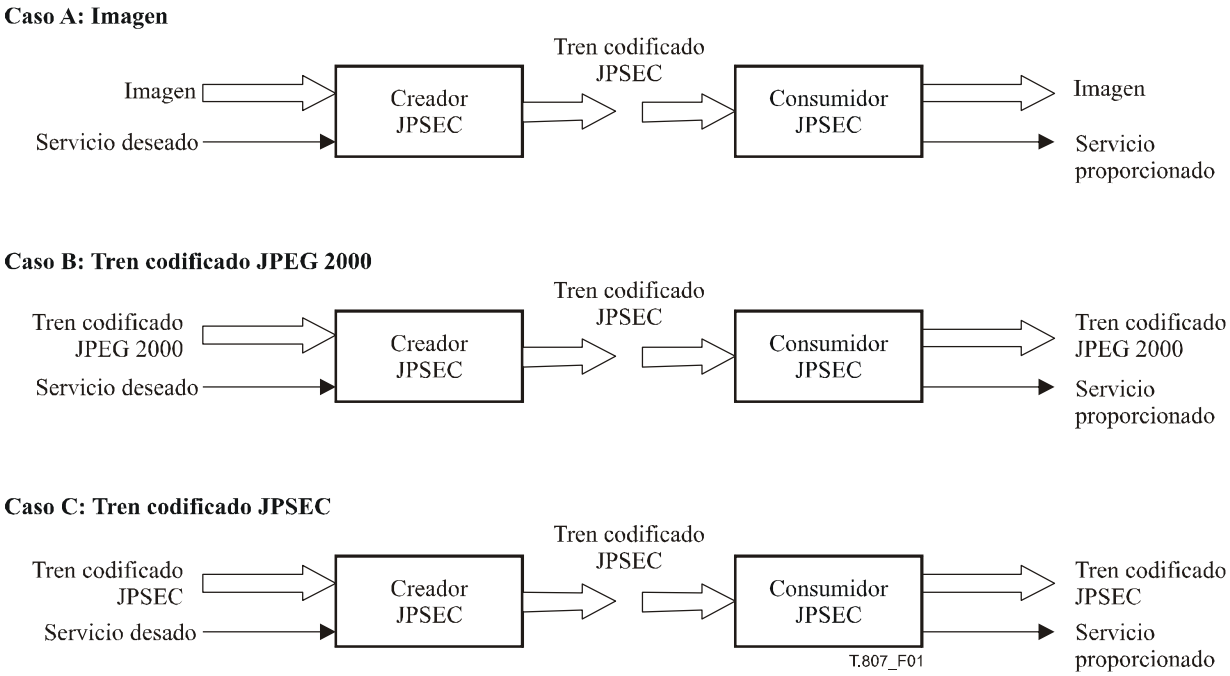


Figura 1 – Conceptos generales del marco general JPSEC

La sintaxis del tren codificado JPSEC es normativa y su propósito es permitir a las aplicaciones JPSEC el consumo de trenes codificados JPSEC de manera compatible (véase la figura 1). La aplicación consumidora JPSEC que interpreta el tren codificado JPSEC, lo identifica y aplica las herramientas JPSEC señaladas, proporciona los servicios de seguridad correspondientes y produce un tren codificado JPEG 2000 resultante o una imagen para su procesamiento posterior, por ejemplo, por parte del usuario.

Como se muestra en el caso C de la figura 1, el tren codificado JPSEC puede ser creado a partir de otro tren codificado JPSEC, lo que puede ocurrir cuando se aplican al mismo contenido diversas herramientas JPSEC, pero en distintos momentos por parte de distintas entidades. En este caso, puede revestir importancia el orden en que se aplican las herramientas JPSEC durante la creación y consumo de las operaciones.

La sintaxis de señalización identifica las herramientas que utiliza el consumidor JPSEC. Las herramientas están definidas por la parte normativa de la norma o por la autoridad de registro o por herramientas privadas. Las

herramientas definidas normativamente soportan la confidencialidad (gracias a herramientas de criptación) y la autenticación de la fuente y del contenido. Proporcionan un grado más alto de compatibilidad, pues las implementaciones del proceso de consumo independientes pueden procesar el mismo tren codificado JPSEC y proporcionar los servicios correspondientes con el mismo comportamiento.

La manera en que se crea el tren codificado JPSEC queda fuera del alcance de la presente Recomendación | Norma Internacional. Para ajustarse a su cumplimiento, los creadores JPSEC deben generar trenes codificados JPSEC que incluyan la señalización JPSEC adecuada. Los trenes codificados JPSEC pueden crearse de distintas maneras, por ejemplo, una herramienta JPSEC puede aplicarse a píxeles de imagen o a coeficientes de ondícula o a coeficientes cuantizados o a paquetes.

Un consumidor puede implementar una o más herramientas JPSEC. Por ejemplo, debe poder realizar una descriptación utilizando el cifrado de bloque AES en modo ECB y la verificación de firma utilizando una función generadora SHA-128 y una clave pública RSA. Con estas capacidades, debería poder garantizar servicios de seguridad de confidencialidad y autenticación.

En el marco de la JPSEC, las herramientas JPSEC están especificadas por modelos, definidos a nivel privado o registrados por la *Autoridad de Registro JPSEC*. Las herramientas JPSEC especificadas por los modelos tienen un único comportamiento de procesamiento y no requieren una identificación exclusiva. Las especificadas por la autoridad de registro están asociadas con un número de identificación exclusivo proporcionado por el registro.

5.2 Servicios de seguridad JPSEC

El objetivo de esta subcláusula es exponer y explicar las funcionalidades que entran dentro del alcance de la presente Recomendación | Norma Internacional.

Las herramientas JPSEC se utilizan para implementar funciones de seguridad. JPSEC es un marco abierto, es decir, ampliable en el futuro, que en la actualidad se centra en los siguientes aspectos:

– *Confidencialidad mediante criptación y criptación selectiva*

  Un fichero JPSEC puede soportar una transformación de los datos (imagen y/o metadatos) (texto simple) en otra forma (texto cifrado) que oculta el significado original de los datos. Por criptación selectiva se entiende que no se cripta toda la imagen y/o los metadatos sino solamente parte de ellos.

– *Verificación de la integridad*

  Un fichero JPSEC puede soportar métodos de detectar las manipulaciones de la imagen y/o metadatos, verificando así su integridad. Hay dos clases de verificación de la integridad:

  1) Verificación de la integridad datos de imagen, donde un solo bit de datos de imagen erróneo da como resultado un fallo de la verificación (es decir, la verificación devuelve un resultado "no integridad"). Esta verificación suele denominarse verificación de la imagen (integridad) frágil.

  2) La verificación de la integridad del contenido de imagen en la que un determinado grado de alteración de los datos de imagen da como resultado una verificación satisfactoria, siempre y cuando esta alteración no modifique el contenido de la imagen desde el punto de vista del sistema visual humano, es decir, no se modifica la percepción de la imagen, se denomina verificación de la imagen (integridad) semifrágil.

  La verificación de la integridad de la imagen frágil o semifrágil puede identificar la ubicación de los datos de imagen/la imagen cuya integridad está en peligro. Las soluciones que pueden aplicarse son:

  1) Métodos criptográficos, como los códigos de autenticación de mensaje (MAC, *message authentication codes*), firmas digitales, verificaciones criptográficas globales o funciones generadoras con clave.

  2) Métodos basados en la marca de agua. Esta Recomendación | Norma Internacional no define un modelo normativo para la tecnología de marcado de agua, aunque soporta las herramientas no normativas que utilizan esta tecnología.

  3) Una combinación de los dos métodos anteriores.

– *Autenticación de la fuente*

  Un fichero JPSEC puede soportar la verificación de la identidad del usuario/parte que ha generado el fichero JPSEC. Para ello pueden utilizarse métodos tales como las firmas digitales o los códigos de autenticación de mensaje (MAC).

– *Acceso condicional*

  Un fichero JPSEC puede soportar un mecanismo y una política que otorgue o restrinja el acceso a los datos de imagen o porciones de los mismos. Puede, por ejemplo, permitir una visualización de baja resolución (vista previa) de una imagen sin permitir la visualización con una resolución superior.

– *Identificación del contenido registrado*

  Un fichero JPSEC puede registrarse ante la autoridad de registro de contenido. Puede soportar un método que establezca la correspondencia entre los datos de imagen/contenido de imagen (supuestos) y los datos de imagen/contenidos de imagen registrados. Un ejemplo de este método podría ser la lectura de un identificador de fichero (matrícula) ubicado dentro de los metadatos, que comprueba la coherencia entre esta matrícula y la información que se ha actualizado durante el proceso de registro. La matrícula puede contener suficiente información para solicitar información de la autoridad de registro de contenido donde se haya registrado el fichero y verificar que ésta corresponda con el identificador.

– *Difusión progresiva segura y transcodificación segura*

  Un fichero JPSEC o una secuencia de paquetes pueden soportar métodos que supongan que el mismo nodo, o uno distinto, puedan realizar la difusión y transcodificación sin requerir la descriptación ni desproteger el contenido. Un ejemplo de ello es cuando el contenido JPEG 2000 protegido se difunde a un nodo intermedio de la red o un intermediario que, a su vez, transcodifica el contenido JPEG 2000 protegido de manera que se preserva la seguridad de extremo a extremo.

5.3 Comentario sobre el diseño e implementación de sistemas JPSEC seguro

Esta Recomendación | Norma Internacional soporta un conjunto rico y flexible de servicios de seguridad. Por ejemplo, las primitivas de criptación pueden utilizarse de diversas maneras para lograr distintos objetivos, desde la criptación de todo el tren codificado JPEG 2000 a una criptación selectiva de sólo una pequeña parte del tren codificado. No obstante, es importante subrayar que debe tenerse mucho cuidado al implementar cualquier sistema de seguridad, incluidos los basados en JPSEC.

Se recomienda vivamente a los diseñadores de sistemas de seguridad que tengan cuidadosamente en cuenta las directrices recomendadas para las primitivas de seguridad que se emplean. Para la mayoría de las primitivas de seguridad señaladas utilizando JPSEC, las normas ISO/CEI correspondientes proporcionan importantes directrices para su uso correcto. Por ejemplo, para realizar una criptación utilizando un cifrado de bloque y el modo de cifrado de bloque asociado (cuadro 29), pueden encontrarse las directrices para la elección y funcionamiento del modo de cifrado de bloque en ISO/CEI 10116.

Además, en muchas aplicaciones de seguridad, la autenticación es el servicio más importante. Incluso cuando el objetivo del servicio de seguridad es la confidencialidad, debe sumarse también la autenticación para evitar diversas formas de ataques. En concreto, en las aplicaciones de imagen, donde el objetivo principal es la confidencialidad, se recomienda que se aplique también la autenticación.

La gestión de claves queda fuera del alcance de JPSEC, aunque hay que subrayar su importancia. En cualquier sistema criptográfico es de vital importancia la gestión de las claves criptográficas que controlan las operaciones. Si estas claves se ven comprometidas, la seguridad de todo el sistema queda en entredicho de tal manera que no puede detectarse el peligro. Es por tanto imperativo que las claves se generen, distribuyan, almacenen y destruyan con un nivel de seguridad como mínimo igual al de los datos que se protegen. Además, puesto que las posibilidades de que una clave se vea comprometida aumentan con el tiempo, también es imperativo que las claves se utilicen durante un periodo determinado de tiempo. Para más información sobre la utilización y gestión de claves criptográficas, véase ISO/CEI 11770.

Al igual que ocurre con todos los sistemas de seguridad, la utilización de métodos criptográficos deben ser completamente opaca al usuario. Es decir, el usuario no debe poder descubrir información alguna sobre las operaciones criptográficas, excepto para el resultado. Por ejemplo, el usuario no debe poder acceder a la información sobre por qué una operación criptográfica no ha logrado producir el resultado deseado. Del mismo modo, el usuario no debe poder obtener ninguna información adicional, incluso aunque pueda medir "canales paralelos" como la temporización y/o el análisis de potencia. En resumen, el usuario no debe poder notar la diferencia en las aplicaciones que consume, independientemente de cuáles sean, ya que, de no ser así, la fuga de información puede poner en compromiso la seguridad del sistema.

En conclusión, se recomienda vivamente que los diseñadores de sistemas de seguridad, incluidos los basados en JPSEC, presten una atención especial a los detalles de diseño del sistema para garantizar su seguridad.

5.4 Segmento con alineación de bytes (BAS, *byte-aligned segment*)

5.4.1 Segmento con alineación de bytes

Para ampliar la señalización de clases y modos, la presente Recomendación | Norma Internacional utiliza una estructura de datos de longitud variable denominada "segmento con alineación de bytes" (BAS). Los campos de parámetros con un número extensible de campos se representan gracias a la estructura BAS por campos (FBAS, *field BAS*). Los valores de parámetro con gamas más grandes se representan gracias a la estructura BAS por gamas (RBAS, *range BAS*).

Como se muestra en la figura 2, el BAS está compuesto por una secuencia de uno o más bytes BAS. El bit más significativo (MSB) de cada byte BAS indica la existencia de otro byte BAS a continuación. Concretamente, si MSB = 1, hay un byte BAS a continuación, mientras que si MSB = 0, no hay ningún byte BAS a continuación y la estructura BAS se da por terminada. Los bits menos significativos restantes de cada byte BAS están concatenados para formar una lista de bits que se utilizan de distintas maneras para distintos parámetros BAS. A menudo, se utilizan junto con una lista de parámetros que tiene un número de elementos, y cada bit BAS se pone a 1 ó 0 para proporcionar información sobre su elemento correspondiente. Se ha elegido esta estructura flexible porque podrá ampliarse para adaptarse a la evolución de la norma, pues se extiende para permitir la señalización de nuevos parámetros.

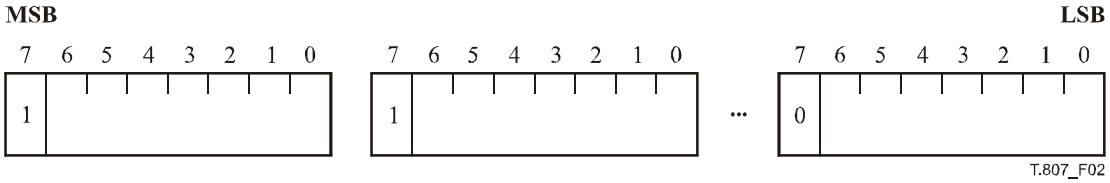


Figura 2 – Estructura del segmento con alineación de bytes (BAS)

5.4.2 BAS por campos (FBAS)

El BAS por campos (FBAS) es un tipo de BAS donde los bits restantes de los bytes BAS se utilizan para poner los campos a 1 ó 0. El FBAS se utiliza, por ejemplo, en la clase de descripción de la zona de influencia (DCzoi), donde pueden especificarse múltiples descripciones de imagen como el índice de losa, el nivel de resolución y el componente de color. En este caso, se ponen a 1 los tres bits BAS correspondientes a la losa, la resolución y el color.

Por ejemplo, si se quiere representar un BAS por campos con 9 campos, f1 a f9, habrá que utilizar, como mucho, dos bytes BAS. Si los dos bytes fuesen "a" y "b", el bit más significativo de cada byte sería a0 y b0, por lo que el FBAS sería:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

a0 y b0 son los bits indicadores. Los campos f1 a f7 se representan en los bits a1 a a7 y el campo f8 está en el bit b1 y el campo f9 en el bit b2. Los bits restantes, b3 a b7 se reservan y se ponen a 0.

a0 f1 f2 f3 f4 f5 f6 f7 | b0 f8 f9 0 0 0 0 0

Cuando se utiliza en un tren JPSEC, el FBAS de este ejemplo puede representarse con uno o dos bytes, dependiendo de los valores reales del campo, porque el valor por defecto de los campos es 0. Por consiguiente, si los campos f8 y f9 no están configurados (es decir, el valor es 0), el segundo byte del BAS no es necesario, y a0 se pone a 0. Por otra parte, si el campo 8 o el campo 9 están configurados, son necesarios los dos bytes. En este caso, a0 se pone a 1 y b0 se pone a 0.

Cabe señalar que los bits de campo están alineados a la izquierda, lo que permitirá en el futuro añadir más campos de manera compatible.

5.4.3 BAS por gamas (RBAS)

El BAS por gamas (RBAS) se utiliza para ampliar la gama o el número de bits utilizados para representar un valor. Hay dos tipos de RBAS, RBAS-8 y RBAS-16.

RBAS-8 contiene uno o más bytes RBAS que contienen los bits del valor. Al igual que ocurre en FBAS, el primer bit de cada byte indica si hay otro byte RBAS a continuación.

Por oposición al FBAS, el RBAS está alineado a la derecha, por lo que, si un valor tiene 9 bits significativos, v1 a v9, siendo v1 el bit más significativo, se representaría con dos bytes BAS:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

de la siguiente manera:

1 0 0 0 0 0 v1 v2 | 0 v3 v4 v5 v6 v7 v8 v9

Si el valor es pequeño, de tal manera que v1 y v2 son cero, la representación de dos bytes anterior puede utilizarse con v1 y v2 puestos a cero, o puede utilizarse un RBAS de un byte como se muestra a continuación:

0 v3 v4 v5 v6 v7 v8 v9

El RBAS-16 puede utilizarse para representar valores que, generalmente, tienen más de 7 bits, pero menos de 15. En este caso, el primer tramo del RBAS tiene dos bytes, siendo el primer bit el indicador, y los siguientes 15 bits, bits de valor, y los bytes restantes se amplían de uno en uno utilizando la estructura BAS típica, siendo el primer bit de cada byte el indicador de los bits BAS siguientes.

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7 | c0 c1 c2 c3 c4 c5 c6 c7

Si un valor de un parámetro tiene 22 bits, puede representarse con una estructura RBAS-16 de tres bytes como se muestra a continuación, donde a0 y c0 son bits indicadores para especificar si a continuación hay otro byte BAS. Cualquier byte BAS restante es un segmento BAS de un byte tradicional.

a0 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | c0 v16 v17 v18 v19 v20 v21 v22

Así, los bits indicadores se configuran de la siguiente manera:

1 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | 0 v16 v17 v18 v19 v20 v21 v22

Tanto para RBAS-8 como para RBAS-16 los bits de valor también se "alinean a la derecha".

Hay que señalar que es importante que los creadores y consumidores de JPSEC presten atención a las presentaciones en orden creciente y decreciente.

5.5 Marcador de seguridad principal (SEC, *security marker*)

5.5.1 Segmento marcador de seguridad

En esta subcláusula se presenta una sintaxis simple y flexible, aunque sólida, para señalización JPSEC. Los segmentos marcadores SEC están definidos con este propósito y se ubican en el encabezamiento principal. La sintaxis del segmento marcador SEC permite la descripción de toda la información necesaria para garantizar la seguridad de las imágenes JPEG 2000. Para ello, se hace referencia a herramientas normativas JPSEC especificadas por los modelos que se describen en 5.8 o a herramientas JPSEC no normativas que pueden haberse registrado *a priori* ante la autoridad de registro JPSEC, o haberse definido a nivel privado, y se prevé el tratamiento de los parámetros relacionados con estas herramientas.

Un tren codificado JPSEC puede protegerse con una o más herramientas JPSEC. Cada una de ellas es una herramienta JPSEC normativa o una herramienta JPSEC no normativa. Los parámetros de estas herramientas se incluyen en uno o más segmentos marcadores SEC ubicados en el encabezamiento principal del tren codificado después del segmento marcador SIZ. Cuando se utilizan múltiples segmentos marcadores SEC, éstos van concatenados y deben aparecer consecutivamente en el encabezamiento principal. En la mayoría de los casos, todos los parámetros JPSEC pueden ir en un único segmento marcador SEC. No obstante, en algunos casos, la longitud de la señalización puede superar el tamaño máximo del segmento marcador. En este caso, pueden utilizarse segmentos marcadores SEC adicionales.

En la figura 3 se muestra la sintaxis del segmento marcador SEC. El segmento va señalado por el marcador SEC 0xFF65. L_{SEC} es la longitud del segmento marcador SEC, que incluye los dos bytes L_{SEC}, pero no los dos bytes del marcador SEC mismo. Z_{SEC} es el índice del segmento marcador SEC. Z_{SEC} debe ponerse a 0 en el primer segmento marcador que aparece en el tren codificado. P_{SEC} es un campo de parámetros que describe los parámetros de seguridad pertinentes a todo el tren codificado y sólo está presente en el primer segmento marcador SEC, es decir, si $Z_{SEC} = 0$. La sintaxis soporta la utilización de diversas herramientas JPSEC que se señalan en uno o más segmentos marcadores. Si se utiliza más de una herramienta JPSEC, el consumidor deberá procesar las herramientas en el orden en que aparecen en el tren codificado.

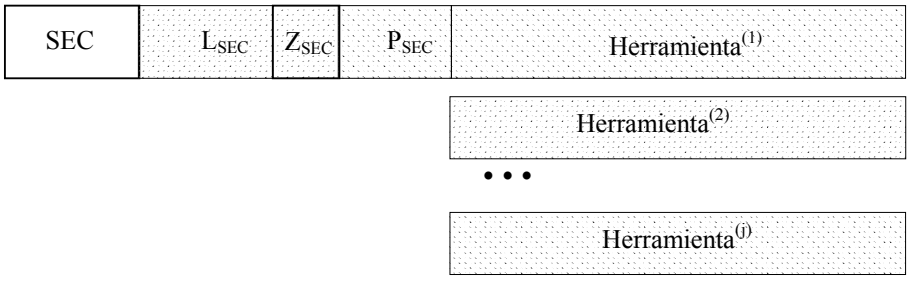


Figura 3 – Sintaxis del segmento marcador de seguridad principal

SEC: Código marcador. En el cuadro 1 se muestran los tamaños y valores de los símbolos y parámetros del segmento marcador de seguridad principal.

L_{SEC}: Longitud del segmento marcador en bytes (incluido L_{SEC}, pero excluido el marcador).

Z_{SEC}: Índice del segmento marcador con respecto a los demás segmentos marcadores SEC presentes en el encabezamiento. Ese campo utiliza la estructura RBAS.

P_{SEC}: Campo de parámetros para los parámetros de seguridad del tren codificado. Este campo sólo está presente en el primer segmento marcador SEC, es decir, cuando Z_{SEC} es 0.

Herramienta$^{(i)}$: Parámetros para la herramienta JPSEC i. Si se señalan múltiples herramientas JPSEC, el consumidor deberá procesarlas en el orden en que aparecen en el tren codificado JPSEC.

Cuadro 1 – Valores del parámetro de seguridad principal

Parámetro	Tamaño (bits)	Valores
SEC	16	0xFF65
L_{SEC}	16	2 ... $(2^{16} – 1)$
Z_{SEC}	8 + 8 * n (RBAS)	0 ... 2^{7+7*n}
P_{SEC}	0, si $Z_{SEC} > 0$ En cualquier otro caso, variable	Si $Z_{SEC} = 0$, véase el cuadro 2
Herramienta$^{(i)}$	Variable	Véanse 5.6.2 y 5.6.3

En la figura 4 se muestra la sintaxis de los parámetros de seguridad del encabezamiento principal cuando se utilizan múltiples segmentos marcadores SEC. En este caso, los parámetros de la herramienta JPSEC se encuentran en distintos segmentos marcadores SEC. Cada segmento marcador empieza con un marcador SEC, 0xFF65, y va seguido de la longitud y el índice de segmentos marcadores. El índice del primer segmento marcador deberá ponerse a 0 e incrementarse en uno para cada segmento marcador en el orden en que aparezca. Sólo el primer segmento marcador contiene los parámetros de seguridad del tren codificado, P_{SEC}. Todos los segmentos marcadores contienen los parámetros de una o más herramientas JPSEC.

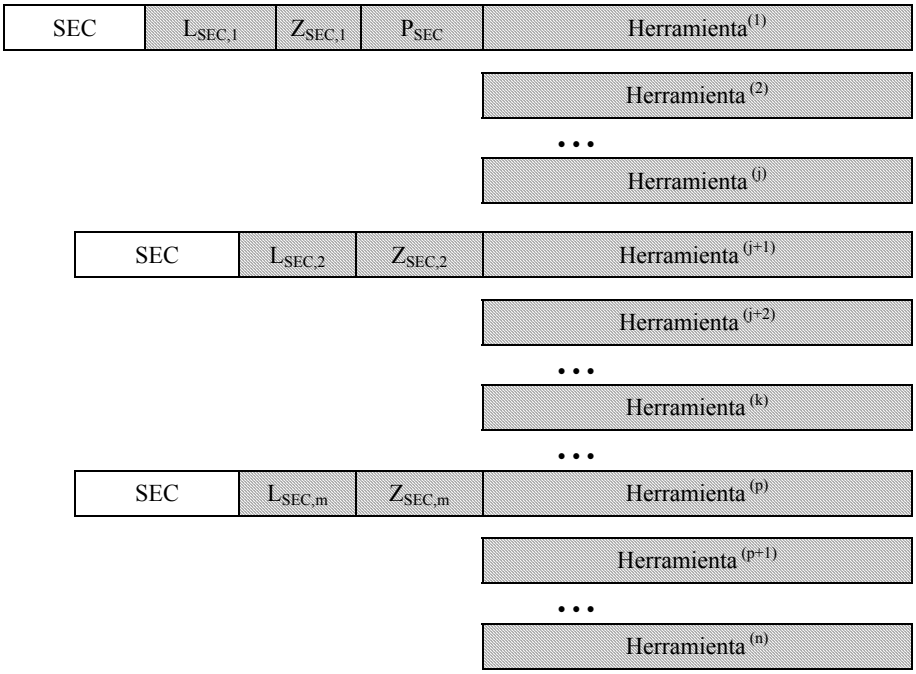


Figura 4 – Sintaxis del marcador de seguridad principal cuando se utilizan múltiples segmentos marcadores

De ser necesario, la descripción de una herramienta JPSEC puede ocupar varios segmentos marcadores SEC, por ejemplo, si se requiere una longitud que supera el tamaño máximo del marcador SEC. Dado que la longitud de la descripción de la herramienta está completamente especificada, el creador de JPSEC simplemente divide las herramientas en varios segmentos marcadores SEC. El decodificador debe entonces concatenar todos los segmentos, excepto el marcador SEC y los valores L_{SEC} y Z_{SEC}, e interpretar las herramientas convenientemente.

P_{SEC} es un campo de parámetros que describe los parámetros de seguridad de todo el tren codificado, por oposición a una herramienta en concreto. Se utiliza para indicar eventos tales como el cumplimiento con JPEG 2000 Parte 1 o la utilización de marcadores INSEC. En la figura 5 se muestran los parámetros P_{SEC}.

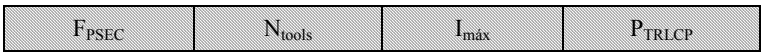


Figura 5 – Sintaxis de los parámetros de seguridad del tren codificado (PSEC)

F_{PSEC}: Bandera que indica si se utiliza un segmento marcador INSEC, si se utilizan múltiples segmentos marcadores SEC, si se han modificado los datos del tren codificado JPEG 2000 Parte 1 original, y si se ha definido la utilización de la etiqueta TRLCP. Este campo utiliza la estructura FBAS.

N_{tools}: Número de herramientas JPSEC utilizadas en el tren codificado. Este campo utiliza la estructura RBAS.

$I_{máx}$: Valor del índice de máximos ejemplares de herramienta utilizadas en el tren codificado. Este campo utiliza la estructura RBAS.

P_{TRLCP}: Campo de parámetros para definir el formato de la etiqueta TRLCP. Este campo existe si $F_{TRLCP} = 1$.

Cuadro 2 – Parámetros de seguridad del tren codificado (P_{SEC}) en el primer segmento marcador SEC

Parámetro	Tamaño (bits)	Valores
F_{PSEC}	Variable (FBAS)	Véase el cuadro 3
N_{tools}	8 + n * 8 (RBAS)	1 ... 2^{7+7*n}
$I_{máx}$	8 + n * 8 (RBAS)	0 ... 2^{7+7*n}
P_{TRLCP}	0, si $F_{TRLCP} = 0$ 32, si $F_{TRLCP} = 1$	Véase el cuadro 4

F_{PSEC} es una estructura FBAS que se utiliza para indicar el número de banderas de parámetro del tren codificado JPSEC. Los campos representados por F_{PSEC} se muestran en el cuadro 3. F_{INSEC} se pondrá a 1 si se utilizan marcadores INSEC en el tren codificado JPSEC. $F_{multiSEC}$ se podrá a 1 si se utilizan múltiples segmentos marcadores SEC en el tren codificado JPSEC. F_{mod} se pondrá a 1 si se han modificado los datos JPEG 2000 originales en el tren codificado JPSEC. Cabe señalar que, si se utilizan marcadores INSEC, se modifican los datos JPEG 2000 originales y, por consiguiente, F_{INSEC} y F_{mod} deben ponerse a 1. F_{TRLCP} debe ponerse a 1 si se define en P_{SEC} la utilización de la etiqueta TRLCP. Si esta etiqueta está definida, el descriptor de etiqueta P_{TRLCP} se especifica en el campo de parámetros P_{SEC}. Debe especificarse la utilización de la etiqueta TRLCP si cualquiera de las herramientas del tren codificado JPSEC utiliza etiquetas TRLCP.

Cuadro 3 – Semántica de los valores F_{PSEC} (FBAS)

Campo BAS	Número de bit BAS	Valor (bits)	Semántica
F_{INSEC}	1	0	no se utiliza INSEC
		1	se utiliza INSEC
$F_{multiSEC}$	2	0	se utiliza un segmento marcador SEC
		1	se utilizan múltiples segmentos marcadores SEC
F_{mod}	3	1	se han modificado los datos JPEG 2000 originales
		0	cualquier otro caso
F_{TRLCP}	4	0	no se define en P_{SEC} la utilización de la etiqueta TRLCP
		1	se define en P_{SEC} la utilización de la etiqueta TRLCP

JPSEC define la estructura denominada etiqueta TRLCP, que puede utilizarse para identificar de manera exclusiva un paquete JPEG 2000. El paquete JPEG 2000 puede estar especificado exclusivamente por su índice de nivel de resolución, su índice de capa, su índice de componente y su índice de precinto. La etiqueta TRLCP se define como una unidad de datos con un número fijo de bits utilizados para especificar cada uno de estos valores de índice. El número de bits para cada índice se determina en P_{SEC}. P_{TRLCP} es un campo de parámetros que describe el formato de la etiqueta TRLCP como debe utilizarse en las herramientas JPSEC. Este campo sólo existe si $F_{TRLCP} = 1$. P_{TRLCP} está formado por las siguientes variables, que se muestran en la figura 6.

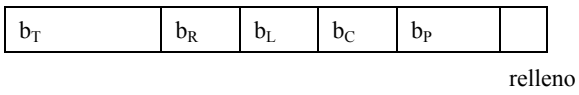


Figura 6 – Sintaxis del descriptor de etiqueta TRLCP (P_{TRLCP})

b_T: El número de bits que representa el índice de losa es $b_T + 1$ en la etiqueta TRLCP.

b_R: El número de bits que representa el índice de nivel de resolución es $b_R + 1$ en la etiqueta TRLCP.

b_L: El número de bits que representa el índice de capa es $b_L + 1$ en la etiqueta TRLCP.

b_C: El número de bits que representa el índice componente es $b_C + 1$ en la etiqueta TRLCP.

b_P: El número de bits que representa el índice de precinto es $b_P + 1$ en la etiqueta TRLCP.

Cuadro 4 – Campo de parámetros para el descriptor de etiqueta TRLCP (P_{TRLCP})

Parámetro	Tamaño (bits)	Valores
b_T	8	$0 \ldots (2^8 - 1)$
b_R	4	0 ... 15
b_L	5	0 ... 31
b_C	5	0 ... 31
b_P	8	$0 \ldots (2^8 - 1)$
Relleno	2	0

El tamaño de cada etiqueta TRLCP resultante es el byte entero más pequeño que contiene todos los bits. El formato de la etiqueta TRLCP contiene los bits del índice de losa, el índice de nivel de resolución, el índice de capa, el índice de componente y el índice de precinto, por ese orden. De ser necesarios bits adicionales para llenar todo el byte, la etiqueta TRLCP se situará en los bits menos significativos, y los demás bits se pondrán a 0. Cabe señalar que estos bits adicionales serán los MSB de la etiqueta TRLCP, de haberlos.

5.5.2 Aplicación de múltiples herramientas JPSEC

Muchas aplicaciones necesitan la utilización de múltiples herramientas JPSEC en un único tren codificado JPEG 2000. Por ejemplo, puede utilizarse tanto la criptación como la autenticación para proteger una imagen JPEG 2000. En las figuras 3, 4 y 7, donde se utilizan N herramientas, muestran la hipótesis general de aplicación de múltiples herramientas JPSEC. El consumidor JPSEC leerá las N herramientas en el orden en que se sitúan en el segmento marcador SEC que se muestra en las figuras 3 ó 4, y las aplicará en ese mismo orden para consumir el tren codificado JPSEC. Hay que señalar que, mientras el consumidor JPSEC aplica las herramientas JPSEC en el orden 1, 2, … , N, tal y como los lee del segmento marcador SEC, durante la creación del tren codificado JPSEC estas herramientas se aplican en orden inverso, es decir, N, N – 1, …2, 1, como se muestra en la figura 7. La numeración de las herramientas en la figura se ha elegido para subrayar que el consumidor JPSEC aplica las herramientas JPSEC en el orden inverso de como las ha introducido el creador. No obstante, cualquier numeración de las herramientas JPSEC es aceptable, siempre y cuando en el tren codificado JPSEC cada una de ellas disponga de un número exclusivo para su identificación.

En términos generales, las herramientas JPSEC se crean y consumen en orden inverso dependiendo del proceso. Por ejemplo, si el creador JPSEC aplica N herramientas JPSEC, el consumidor generalmente aplicará esas mismas N herramientas pero en orden inverso. El consumo correcto de múltiples herramientas JPSEC puede garantizarse mediante una utilización secuencial de las N herramientas en orden correcto y exigiendo que el consumidor y el creador coincidan en estado en una etapa intermedia. Por ejemplo, en la figura 7, el estado del consumidor tras la utilización de la herramienta 1 debe ser igual al estado del creador después de que haya aplicado la herramienta 2. Como ejemplo concreto de este estado, las gamas de bytes deben ser coherentes, es decir, que cualquier byte añadido al aplicar la herramienta 1 ha de eliminarse cuando el consumidor JPSEC haya terminado con esta herramienta.

En determinadas aplicaciones puede ser preferible para el consumidor utilizar múltiples herramientas JPSEC de manera distinta a como se describe anteriormente. Por ejemplo, el consumidor puede elegir utilizar múltiples herramientas en orden distinto para no utilizar algunas de ellas. Además, el consumidor puede preferir la aplicación de determinadas herramientas JPSEC, pero no eliminarlas, es decir, por ejemplo, verificar la firma digital, pero no eliminarla. Ha de prestarse una atención especial a estos casos para garantizar que el procesamiento desordenado o salteado no tiene a consecuencias incorrectas o inesperadas. Este tipo de utilización no se recomienda a menos que la aplicación JPSEC sea plenamente consciente de las posibles consecuencias.

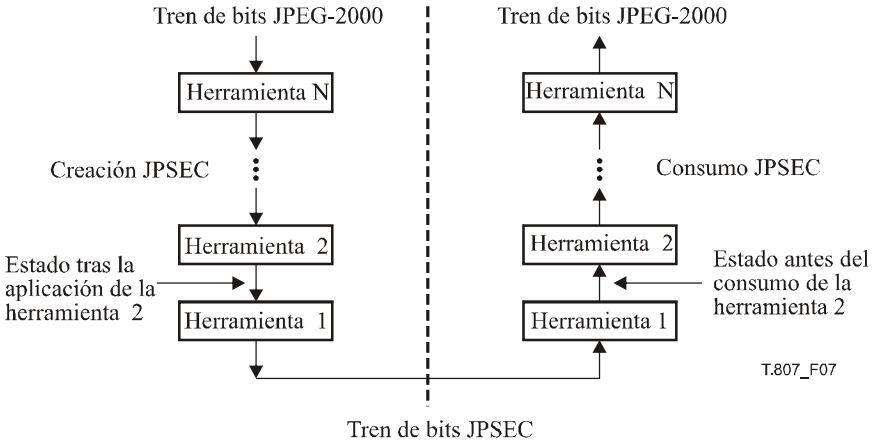


Figura 7 – Utilización de múltiples herramientas JPSEC

5.6 Herramientas JPSEC

5.6.1 Sintaxis de las herramientas JPSEC

Como se ha dicho anteriormente, hay dos tipos de herramientas JPSEC. Las herramientas JPSEC normativas están especificadas por los modelos de métodos de protección que se describen en 5.8, y que también se denominan herramientas JPSEC normativas. Las herramientas JPSEC no normativas están especificadas por una autoridad de registro JPSEC o por una aplicación JPSEC privada de acuerdo con un número identificador y se denominan, respectivamente, herramientas de la autoridad de registro JPSEC o herramientas JPSEC definidas por el usuario. La sintaxis de las herramientas JPSEC normativas puede encontrarse en 5.6.2. La sintaxis de las herramientas JPSEC no normativas se encuentra en 5.6.3.

En la figura 8 se muestra la sintaxis de las herramientas JPSEC. Esta sintaxis se divide en tres partes principales que describen:

1) qué herramienta se aplica y su identificación;
2) dónde se aplica la herramienta y cuál es la estructura de la zona de influencia; y,
3) cómo se aplica la herramienta y un campo de parámetros más detallado.

Por ejemplo, con esta sintaxis, una sintaxis de herramienta JPSEC puede especificar que debe utilizarse una herramienta de descriptación (qué) en el componente de resolución más baja ubicado en una gama de bytes concreta (dónde) utilizando la descriptación AES en modo CBC con un conjunto específico de vectores de inicialización y claves (cómo).

Figura 8 – Sintaxis de herramienta JPSEC (herramienta$^{(i)}$)

t: Tipo de herramienta. El valor 0 en el primer bit BAS indica que se trata de una herramienta JPSEC normativa. El valor 1 en el primer bit BAS indica que se trata de una herramienta JPSEC no normativa. Este campo utiliza la estructura FBAS.

i: Índice de ejemplares de herramienta (puede utilizarse como identificador exclusivo). Este campo utiliza la estructura RBAS.

ID: Valor de identificación para la herramienta JPSEC *i*. Para las herramientas JPSEC normativas, el ID = ID_T es de 8 bits y especifica el tipo de modelo. Para las herramientas JPSEC no normativas, el ID = ID_{RA} se define en la figura 10 y en el cuadro 8.

L_{ZOI}: Longitud de la ZOI en bytes (excluido el L_{ZOI}). Este campo utiliza la estructura RBAS.

ZOI: Zona de influencia de la herramienta JPSEC *i*.

L_{PID}: Longitud del P_{ID} en bytes (excluido el L_{PID}). Este campo utiliza la estructura RBAS.

P_{ID}: Parámetros para la herramienta JPSEC *i*.

Cuadro 5 – Valores de parámetro de las herramientas JPSEC

Parámetro	Tamaño (bits)	Valores
t	8 + 8 * n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} – 2)$ $(2^{7+7*n} – 1)$, reservado
ID	8, si t = 0 Variable, si t = 1	Véase el cuadro 6 Véanse la figura 10 y el cuadro 8
L_{ZOI}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
ZOI	Variable	Véase 5.7
L_{PID}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
P_{ID}	Variable	Cuadro 7, si t = 0. Gestionado por la autoridad de registro JPSEC, si t = 1.

Todas las herramientas JPSEC tienen la siguiente sintaxis. El primer byte identifica si la herramienta es una herramienta JPSEC normativa o no normativa y le asigna un identificador de ejemplar. A continuación va el **ID** identificador de la herramienta, seguido por L_{ZOI}, que indica la longitud del siguiente campo zona de influencia ZOI y la zona de influencia misma, que describe dónde se aplica la herramienta JPSEC en el tren de datos. A continuación se encuentra el L_{PID}, que indica la longitud del siguiente campo de parámetros P_{ID}, que es un campo utilizado para transmitir uno o más parámetros de la herramienta JPSEC.

El primer byte de la herramienta utiliza una estructura FBAS de un byte cuyo primer bit BAS representa el tipo de herramienta, t, donde 0 especifica que se trata de una herramienta JPSEC normativa y 1 especifica que es una herramienta JPSEC no normativa. A continuación se encuentra el índice de ejemplar, i, que se representa mediante una estructura RBAS. El índice de ejemplar debe ser un identificador exclusivo de la herramienta dentro del tren codificado y, por consiguiente, no debe repetirse en ninguna otra herramienta del tren codificado, incluso en otro segmento marcador SEC. El índice de ejemplar es especialmente importante (y necesario) cuando se utilizan marcadores INSEC, porque el segmento marcador INSEC contiene el índice de ejemplar de la herramienta a que corresponde. Se

recomienda que la primera herramienta aplicada por el creador JPSEC tenga un índice de ejemplar de 1, y que las siguientes herramientas adicionales se enumeren secuencialmente, como se hace en el protector.

Además, todas las herramientas JPSEC tienen un número identificador de 8 bits para las herramientas JPSEC normativas y de 32 bits para las herramientas JPSEC no normativas. En el caso de las herramientas JPSEC normativas, el número de identificador describe qué modelo de método de protección se utiliza, por ejemplo, describe el modelo de descriptación, el modelo de autenticación o el modelo generador. En el caso de las herramientas JPSEC no normativas, el primer bit indica si es una herramienta dependiente de la autoridad de registro o definida por el usuario. En cualquier caso, el número ID denomina una herramienta en concreto. Una autoridad de registro JPSEC puede garantizar que los números ID válidos son exclusivos. No obstante, una aplicación JPSEC con un número ID definido por el usuario correrá el riesgo de escoger un número ID que también está siendo utilizado por otra aplicación JPSEC, por lo que debe utilizarse este método con mucha precaución.

Cuando el creador JPSEC ha aplicado todas las herramientas JPSEC, se actualizará el campo de parámetros P_{SEC} del cuadro 2. Por ejemplo, el campo de parámetros P_{SEC} contiene el parámetro $I_{máx}$ que especifica el índice de ejemplares máximos utilizado por las herramientas en el tren codificado JPSEC. Cuando se aplica una nueva herramienta, se le debe asignar un índice de ejemplar exclusivo. El protector JPSEC puede remitirse al parámetro $I_{máx}$ dado en el campo de parámetros P_{SEC} para determinar el índice de ejemplares que ha de asignar a la herramienta. Por ejemplo, puede elegir un valor superior en uno al valor I_{max} actual e incrementar a su vez el valor de $I_{máx}$ en uno convenientemente.

5.6.2 Herramientas JPSEC normativas

Las herramientas JPSEC normativas utilizan las sintaxis de herramientas JPSEC que se describe en 5.6.1 y se muestra en la figura 8, donde el tipo de herramienta es t = 0 y el tamaño del ID es 8 bits. Las herramientas JPSEC normativas se basan en modelos de métodos de protección descritos en 5.8. Hay tres tipos de modelos de método de protección; el tipo utilizado por la herramienta va especificado por identificador de herramienta ID = ID_T, que utiliza los valores que se muestran en el cuadro 6.

Cuadro 6 – Valores ID del modelo de herramienta JPSEC normativa (ID_T)

Valores	Modelo de método de protección
0	Reservado
1	Modelo de descriptación
2	Modelo de autenticación
3	Modelo de función generadora
4	Herramienta NULA
	Todos los valores están reservados para utilización por parte de la ISO

En el caso de las herramientas JPSEC normativas, el campo de parámetros P_{ID} tiene la estructura que se muestra en la figura 9. P_{ID} está formado por cuatro campos principales: el modelo de método de protección, T, su dominio de procesamiento, PD, su granularidad, G, y su lista de valores, V. La sintaxis de cada uno de estos campos puede encontrarse en 5.8, 5.9, 5.10 y 5.11, respectivamente. En conjunto, estos campos describen cómo se aplica la herramienta. El modelo de método de protección, T, describe el método de protección concreto para el modelo de descriptación, el modelo de autenticación o el modelo de función generadora identificado por el ID de herramienta normativa. También puede especificar que es una herramienta NULA en caso de que no se utilice ningún modelo, pero sigan utilizándose otras funcionalidades. Por ejemplo, la zona de influencia puede estar especificada para representar regiones de la imagen y sus correspondientes gamas de bytes. El dominio de procesamiento, PD, describe el dominio donde se aplica el método de protección. La granularidad, G, indica la granularidad con que se aplica el método de protección. La lista de valores, V, contiene una lista de los valores que pueden necesitar cada uno de los métodos de protección con granularidad más fina. Para el modelo de descriptación, la lista de valores puede utilizarse para especificar un conjunto de valores de inicialización de granularidad más fina que han de utilizarse. En el caso del modelo de autenticación, la lista de valores contiene el conjunto de valores MAC o firmas digitales. En el caso del modelo de función generadora, la lista de valores contiene el conjunto de valores generadores. En todos los casos, la lista de valores contiene una granularidad de valores especificada por el campo granularidad, G.

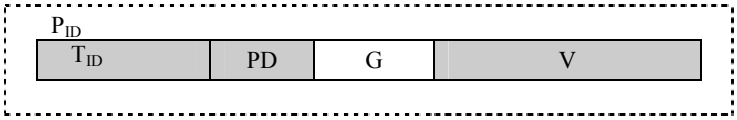


Figura 9 – Sintaxis de parámetros (P_{ID}) para las herramientas JPSEC normativas (t = 0)

T_{ID}: Parámetros del modelo para la herramienta JPSEC normativa con identificador de modelo ID_T.

PD: Dominio de procesamiento de la herramienta JPSEC normativa.

G: Granularidad de la herramienta JPSEC normativa.

V: Lista de valores de la herramienta JPSEC normativa, por ejemplo, vectores de inicialización, valores MAC, firmas digitales o valores generadores, dependiendo del ID del modelo.

Cabe señalar que los parámetros del modelo dependen del ID del modelo. No obstante, el dominio de procesamiento, la granularidad y la lista de valores son independientes del ID del modelo.

Cuadro 7 – Valores de parámetros de la herramienta JPSEC normativa

Parámetro	Tamaño (bits)	Valores
T_{ID}	0, si $ID_T = 4$ Variable, en cualquier otro caso	N/A Véase 5.8.
PD	Variable	Véase 5.9.
G	24	Véase 5.10.
V	Variable	Véase 5.11.

5.6.3 Herramientas JPSEC no normativas

En determinados casos, puede resultar útil que una aplicación JPSEC tenga la posibilidad de aplicar una herramienta que amplía las funcionalidades de las herramientas JPSEC normativas. Esta capacidad se soporta utilizando una herramienta JPSEC no normativa, lo que permite utilizar muchos elementos de las herramientas JPSEC normativas, incluyendo la ZOI y los modelos JPSEC, pero añade la flexibilidad de utilizar parámetros de manera distinta asociados a un valor ID de herramienta.

Las herramientas JPSEC no normativas utilizan la sintaxis de las herramientas JPSEC que se describe en 5.6.1 y se muestra en la figura 8, donde el tipo de herramienta t = 1 y el identificador ID_{RA} está formado por un espacio de nombre y un número ID, como se define en la figura 10 y en el cuadro 8.

Hay dos clases de herramientas JPSEC no normativas:

1) Herramientas de la autoridad de registro JPSEC: herramientas JPSEC no normativas cuya señalización se especifica mediante una autoridad de registro.
2) Herramientas JPSEC definidas por el usuario: herramientas JPSEC no normativas cuya señalización está especificada por una aplicación JPSEC.

Estas dos clases de herramientas JPSEC no normativas se señalan utilizando el identificador $ID_{RA,\ id}$ de 32 bits que se muestra en el cuadro 9, estando los identificadores cuyo primer bit es un 0 definidos por la autoridad de registro, y aquéllos cuyo primer bit es 1 definidos por una aplicación JPSEC particular.

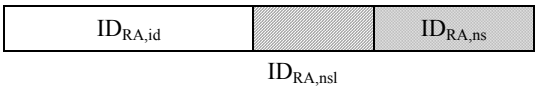


Figura 10 – Sintaxis de ID_{RA}

$ID_{RA,id}$: Identificador de la herramienta para una herramienta de la autoridad de registro y una herramienta definida por el usuario.

$ID_{RA,nsl}$: Longitud del campo $ID_{RA,ns}$ en bytes. Este campo utiliza la estructura RBAS.

$ID_{RA,ns}$: Cadena que contiene el espacio de nombre de la herramienta de la autoridad de registro especificada o de la herramienta definida por el usuario.

Cuadro 8 – Valores de parámetros en la sintaxis de ID_{RA}

Parámetro	Tamaño (bits)	Valores
$ID_{RA,id}$	32	Véase el cuadro 9
$ID_{RA,nsl}$	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
$ID_{RA,ns}$	Variable	Una cadena que contiene el espacio de nombre

Cuadro 9 – Valores ID para las herramientas JPSEC no normativas ($ID_{RA,id}$)

$ID_{RA,id}$	Significado
0x00 00 00 00 ... 0x7F FF FF FF	Herramienta JPSEC de la autoridad de registro. Los valores están gestionados por la autoridad de registro JPSEC.
0x80 00 00 00 ... 0xEF FF FF FF	Herramienta JPSEC definida por el usuario. Los valores pueden estar definidos por una aplicación JPSEC particular.
0xF0 00 00 00 ... 0xFF FF FF FF	Reservado para utilización por parte de la ISO.

En el caso de las herramientas de la autoridad de registro, el campo $ID_{RA,ns}$ es el espacio de nombre de la autoridad de registro (RA, *registration authority*) donde está registrada la herramienta. Como cada RA tiene un espacio de nombre exclusivo, se utilizan $ID_{RA,id}$ y $ID_{RA,ns}$ juntos para identificar una herramienta RA. En el caso de las herramientas definidas por el usuario, el campo $ID_{RA,ns}$ lo eligen sus propios creadores. Para limitar el riesgo de coincidencia de ID, se recomienda que los creadores busquen la exclusividad al elegir el espacio de nombre, por ejemplo, escogiendo el nombre de dominio de su organización o empresa. No obstante, hay que decir que, en el caso de las herramientas definidas por el usuario, no hay manera posible de garantizar la exclusividad del espacio de nombre, por lo que puede haber coincidencias de ID, y este aspecto ha de tenerse en cuidadosamente en cuenta al utilizar herramientas definidas por el usuario.

El campo P_{ID} se utiliza para transmitir uno o más parámetros de la herramienta JPSEC no normativa *i*. El formato del campo P_{ID} no entra plenamente en el alcance de JPSEC. Si se recurre a una autoridad de registro, el formato se registra ante ella junto con el ID. Si no se recurre a una autoridad de registro, la herramienta está definida por el usuario y sólo se especifica la longitud de este campo, y corresponde a los usuarios utilizarla adecuadamente.

No obstante, JPSEC permite que se utilicen en el campo P_{ID} de herramientas JPSEC no normativas estructuras sintácticas definidas para las herramientas JPSEC normativas. Por ejemplo, una herramienta JPSEC no normativa puede utilizar los modelos de método de protección, el dominio de procesamiento, la granularidad y la lista de valores que se describen en 5.8, 5.9, 5.10 y 5.11, respectivamente.

Esta sintaxis es muy flexible y puede acomodarse a una amplia gama de técnicas de seguridad, como la integridad de datos de imagen, el control de acceso y los métodos de protección de derechos. Por consiguiente, ofrece un amplio conjunto de funcionalidades siendo al mismo tiempo simple y concisa.

5.7 Sintaxis de la zona de influencia (ZOI, *zone of influence*)

5.7.1 Introducción

La zona de influencia (ZOI) puede utilizarse para describir la zona de cobertura de una herramienta JPSEC. Los datos dentro de esa zona de cobertura (especificada por la ZOI) se denominan datos influidos. Las herramientas JPSEC normativas utilizan a la ZOI para describir su zona de cobertura. Las herramientas JPSEC no normativas pueden utilizar la ZOI para describir su zona de cobertura o pueden utilizar un método alternativo. En caso de utilizarse un método alternativo, la longitud de ZOI es 0, es decir, no existe.

La zona de influencia (ZOI) describe la zona de cobertura de todas las herramientas JPSEC. Esta zona de cobertura puede describirse mediante parámetros relacionados con la imagen, por ejemplo, según la zona de resolución o imagen; o por parámetros no relacionados con la imagen, por ejemplo, segmentos del tren codificado o índices de paquetes. En los casos en que se utilizan al mismo tiempo parámetros relacionados con la imagen y parámetros no relacionados con la imagen, la ZOI describe la correspondencia entre estas zonas. Por ejemplo, la ZOI puede utilizarse para indicar que las resoluciones y la zona de imagen especificadas por los parámetros relacionados con la imagen corresponden a los segmentos del tren codificado especificados por parámetros no relacionados con la imagen. Esto permite que la ZOI se utilice como metadatos que indican la ubicación de ciertas partes de la imagen en el tren codificado JPSEC.

En la figura 11 se muestra la estructura conceptual de la ZOI. La ZOI está formada por una o más zonas. Cuando se utilizan varias zonas dentro de una única ZOI, ésta está definida por su unión, lo que indica que la herramienta JPSEC debe aplicarse a todas las zonas. Todas las zonas de una ZOI se describen gracias a tres unidades fundamentales: clase de descripción, modo de parámetro y elementos (valores) de parámetro. En la presente Recomendación | Norma Internacional se definen dos tipos de clase de descripción: clase de descripción relacionada con la imagen y clase de descripción no relacionada con la imagen. Estos parámetros pueden especificarse utilizando un número de modos, por ejemplo, mediante un valor único, múltiples valores enumerados o una gama. Los valores o elementos de parámetros se enumeran a su vez de acuerdo con el modo.

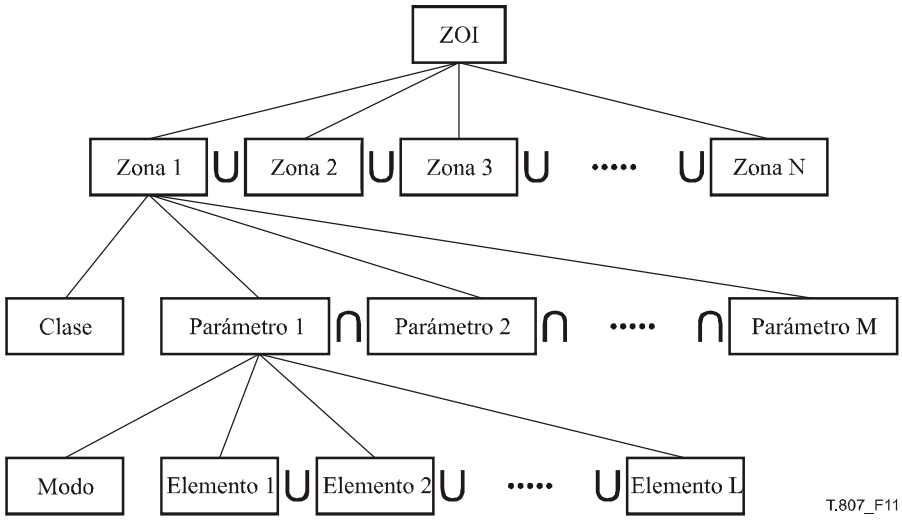


Figura 11 – Estructura conceptual de la zona de influencia

5.7.2 Sintaxis de la ZOI

En la figura 12 se muestra la sintaxis de la ZOI. La ZOI puede contener una o más zonas. También puede estar vacía, en ese caso NZzoi será 0. En este caso, la influencia de la herramienta se especifica por otros medios, como el marcador INSEC o los parámetros definidos por una herramienta de protección JPSEC no normativa.

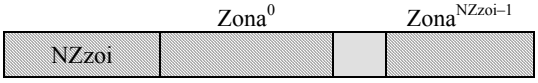


Figura 12 – Sintaxis de la ZOI

NZzoi: Número de zonas. Este campo utiliza la estructura RBAS.

Zona^{k}: Zona. La estructura se especifica en 5.7.3.

Cuadro 10 – Valores de parámetros del campo zona de influencia (ZOI)

Parámetro	Tamaño (bits)	Valores
NZzoi	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} – 2)$ $(2^{7+7*n} – 2)$, reservado
Zona^{k}	Variable	Véase 5.7.3

5.7.3 Sintaxis de la zona

La zona contiene un indicador de campo clase de descripción de zona seguido por los parámetros de esta clase. La clase de descripción de zona utiliza la estructura FBAS. Como se muestra en la figura 13, el segundo byte más significativo de cada byte, denominado "x", indica la utilización de una clase de descripción específica. En la presente Recomendación | Norma Internacional se definen dos clases de descripción: clase de descripción relacionada con la imagen y clase de descripción no relacionada con la imagen (véase el cuadro 12). En los cuadros 13 y 14 se definen los números del indicador de campo para la clase de descripción relacionada con la imagen y la clase de descripción no relacionada con la imagen, respectivamente. Mediante la concatenación de 6 bits en cada byte, denominado "y", que siguen a la bandera de clase de descripción, se indica la utilización de una descripción específica dentro de la clase de descripción determinada. Un bit con el valor "1" en cada clase indica que existe el correspondiente campo de

parámetros. El número de parámetros será idéntico al número de indicadores de campo clase de descripción de zona puesto a '1', y aparecerá en el orden en que se señale el indicador de campo de clase. La clase de descripción de zona tiene un número variable de bytes y, cuando el MSB es 1, quiere decir que a continuación hay otro byte de clase de descripción de zona. El MSB del último byte de clase de descripción es 0. Si se utilizan tanto clases de descripción relacionadas con la imagen como no relacionadas con la imagen, los bytes de la clase de descripción relacionada con la imagen precederán a los bytes de la clase de descripción no relacionada con la imagen. Cuando se utiliza esta estructura para representar una serie de elementos, el primer elemento de la lista corresponderá al bit más significativo disponible en el primer byte.

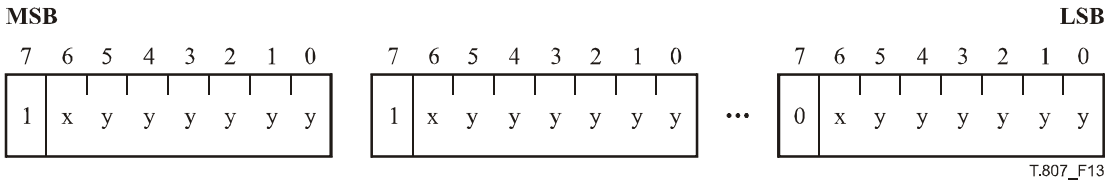


Figura 13 – Estructura de la clase descripción de zona (DCzoi)

En la figura 14 se muestra la sintaxis de la zona.

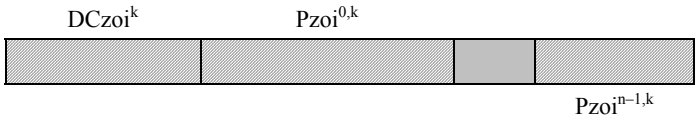


Figura 14 – La sintaxis de la zona está formada por una clase de descripción y uno o más conjuntos de parámetros

DCzoi^{k}: Clase de descripción de zona kº. Este campo utiliza la estructura FBAS.

Pzoi^{i,k}: Parámetros de la zona de acuerdo con la clase de descripción de zonas especificadas (DCzoi^{k}). Véase 5.7.6.

DCzoi^{k} especifica el número *n* de los campos clase de descripción de zona que existen, de acuerdo con el número de bits que están puestos a 1. Para cada campo clase de descripción de zona, hay un campo de parámetro de zona Pzoi^{i,k}. Estos campos aparecen secuencialmente en el mismo orden en que aparecen las banderas en DCzoi^{k}.

Cuadro 11 – Valores de parámetros de zona

Parámetro	Tamaño (bits)	Valores
DCzoi^{k}	Variable (FBAS)	Varía de acuerdo con el conjunto de valores del cuadro 12.
Pzoi^{i,k}	Variable	Véase en 5.7.6 la sintaxis de este campo.

Cuadro 12 – Valor indicador clase de descripción

Valor	Clase de descripción
0	Clase de descripción relacionada con la imagen. Los números de bit siguientes se definen en el cuadro 13.
1	Clase de descripción no relacionada con la imagen. Los números de bit siguientes se definen en el cuadro 14.

Cuadro 13 – Clases de descripción relacionada con la imagen

Número de bit	Semántica
1	Región de imagen
2	Losa(s), como se define en JPEG 2000 Parte 1
3	Nivel(es) de resolución, como se define en JPEG 2000 Parte 1
4	Capa(s), como se define en JPEG 2000 Parte 1
5	Componente(s), como se define en JPEG 2000 Parte 1
6	Precinto(s), como se define en JPEG 2000 Parte 1
7	Etiqueta(s) TRLCP (losa-resolución-capa-componente-precinto)
8	Paquete(s), como se define en JPEG 2000 Parte 1
9	Subbanda(s) como se define en JPEG 2000 Parte 1
10	Bloque(s) de código, como se define en JPEG 2000 Parte 1
11	ROI(s)
12	Velocidad binaria
13	Definido por el usuario. Los detalles pueden especificarse por cualquier otro medio (por ejemplo, ID de JPSEC)
	Todos los demás valores están reservados.

Cuadro 14 – Clase de descripción no relacionada con la imagen

Número de bit	Semántica
1	Paquete(s), como se define en JPEG 2000 Parte 1
2	Gama(s) de bytes (de relleno) (empezando en el primer byte después del primer marcador SOD)
3	Gama(s) de bytes (de relleno) (empezando en el primer byte después del primer marcador SEC)
4	Gama(s) de bytes sin relleno cuando se utiliza el relleno
5	Etiqueta(s) TRLCP (losa-resolución-capa-componente-precinto)
6	Valor(es) de distorsión
7	Importancia(s) relativa(s)
8	Definido por el usuario. Los detalles pueden especificarse por cualquier otro medio (por ejemplo, ID de JPSEC)
	Todos los demás valores están reservados

Los índices de paquetes se numeran secuencialmente dentro de una losa, por lo que es posible que no sean exclusivos en cada losa. Además, los índices de paquetes dentro de una losa pueden desbordarse cuando se supera el máximo valor de 65535. Por este motivo, se describe más detalladamente la indexación de paquetes. Cuando los índices de paquetes dentro de una losa no exceden los 65535 paquetes, el índice de paquetes descrito en el cuadro 13 se define por el índice de paquetes que se encuentra en el parámetro Nsop SOP, como se define en el cuadro A.40 de la norma JPEG 2000 Parte 1. Es necesario tener en cuenta que cuando el valor máximo no supera los 65536, un paquete JPEG 2000 puede especificarse únicamente con un índice de losa y un índice de paquetes. Cuando el índice de paquete supera los 65535 paquetes, el índice de paquetes de JPEG 2000 Parte 1 se define para pasar a 0. En este caso, el índice de paquetes no identifica exclusivamente un paquete y no puede utilizarse. En este caso, se recomienda utilizar en su lugar la etiqueta TRLCP. Es necesario tener en cuenta que los servicios de seguridad que requieren índices de paquetes exclusivos son vulnerables si el índice se desborda y se repite.

Cuando se utilizan etiquetas de TRLCP, su formato debe estar definido por el campo de parámetros P_{SEC} del cuadro 2. En concreto, el formato de la etiqueta TRLCP se especifica en el campo de parámetros P_{TRLCP} del cuadro 4, que define el tamaño de las etiquetas TRLCP en la ZOI.

La clase de descripción no relacionada con la imagen puede también contar con múltiples campos configurados simultáneamente. En este caso, los modos para los distintos campos de parámetros tendrán el mismo número de elementos (a continuación se describe la única excepción a esta regla), y estos elementos se corresponderán mutuamente uno a uno y en el mismo orden. Por ejemplo, si la zona utiliza gamas de bytes y gamas de paquetes cada una de ellas deberá tener el mismo número de elementos por gama y la primera gama de bytes se corresponderá con la primera gama de paquetes, etc.

Hay una excepción a la anterior regla que exige que cada campo tenga el mismo número de elementos, y esto ocurre cuando uno de los campos f1 contiene un elemento que especifica una gama de elementos (como se describe en el modo de gama de 5.7.6), cuando esta gama contiene N elementos y otro campo f2 está especificado por una lista de N elementos. En este caso, el campo f1, que sólo contiene un elemento (la gama) se interpreta como una lista de N elementos. Estos N elementos especificados por la gama f1 se corresponderán uno a uno con los N elementos enumerados en f2. Por consiguiente, una gama de elementos puede asociarse a un único elemento o a múltiples elementos (uno para cada elemento de la gama).

El índice de bytes se ordena a partir del primer byte después del primer marcador SOD o a partir del primer byte después del primer marcador SEC. En cualquiera de los casos, el byte se etiqueta como byte 0.

Los campos distorsión (tanto el campo distorsión como el campo importancia relativa) proporcionan la capacidad de indicar la importancia de las áreas especificadas en la ZOI. El parámetro de distorsión especifica la contribución de reducción de distorsión del segmento de datos especificado, ya sea para un conjunto de paquetes o una gama de bytes o la zona relacionada con la imagen especificada. La distorsión se expresa en términos de error cuadrático total, utilizando una descripción de un byte o de dos bytes dentro de Mzoi. El parámetro de distorsión relativa puede utilizarse para especificar la importancia relativa de los segmentos de datos especificados utilizando valores de uno, dos o cuatro bytes dentro de Mzoi. Pueden encontrase en 5.7.3.2 más detalles sobre los formatos de estos campos.

La etiqueta TRLCP especifica la losa, la resolución, la capa, el componente y el precinto del paquete protegido en el tren codificado. Esta etiqueta se utiliza dentro de la ZOI para especificar estos parámetros, ya que la información puede resultar difícil de inferir a partir de un tren codificado protegido.

Cabe señalar que cuando se utilizan únicamente descripciones relacionadas con la imagen, este campo puede darse por terminado, por lo que no es necesario representar descripciones no relacionadas con la imagen si no se utilizan.

5.7.3.1 Campo gama de bytes

La clase de descripción no relacionada con la imagen permite que la ZOI se describa en gamas de bytes. En general, el segundo y tercer elementos del cuadro 14 se utilizarán para representar las gamas de bytes de la mayoría de las herramientas, como la autenticación y la criptación/descriptación sin relleno. No obstante, algunos métodos de protección, como la criptación/descriptación con relleno, modifican la longitud de los datos. En estos casos, es necesario especificar tanto la gama de bytes de relleno como la gama de bytes original o sin relleno. Así, la gama de bytes de relleno está especificada por el 2º y 3º elementos del cuadro 14, de conformidad con las necesidades de la herramienta de protección. (Hay que indicar que estos dos elementos no pueden utilizarse al mismo tiempo.) Además, la gama de bytes sin relleno se especifica gracias al cuarto elemento del cuadro 14. La gama de bytes sin relleno ha de definirse con el mismo modo de descripción que la gama de bytes con relleno y tener el mismo número de elementos. Estos elementos deben corresponderse mutuamente uno a uno y en el mismo orden.

5.7.3.2 Campo distorsión y campo importancia relativa

Los campos distorsión e importancia relativa proporcionan la capacidad de indicar la importancia de la zona especificada por la ZOI.

El campo distorsión se utiliza para asociar una distorsión a una zona especificada por la ZOI. El valor de distorsión especifica la distorsión por error cuadrático total (o suma de errores cuadráticos) que resultaría si la zona correspondiente no estuviese disponible para la decodificación. La distorsión por error cuadrático total es la medida de distorsión básica que se utiliza en el procesamiento de imagen y vídeo, y se utiliza para derivar la distorsión por error cuadrático medio (MSE, *mean-squared-error*) común y la relación señal/ruido de cresta (PSNR, *peak-signal-to-noise ratio*). El campo distorsión se expresa utilizando una descripción de uno o dos bytes, que se explican más abajo, y la elección de una descripción de uno o dos bytes indicada por el valor de parámetro Mzoi, que especifica la longitud de este campo. El campo importancia relativa puede utilizarse para describir la importancia relativa entre distintas áreas especificadas por las correspondientes ZOI, sin necesariamente estar ligado a una medición de la distorsión específica. La longitud del campo importancia relativa también figura en Mzoi. Estos campos se exponen más detalladamente a continuación.

5.7.3.2.1 Campo distorsión de un byte

La distorsión por error cuadrático total se expresa utilizando un campo distorsión de un byte con una representación de tipo seudo punto-flotante. Los 8 bits disponibles del campo distorsión se asignan como se muestra en la figura 15 y en el cuadro 15 para obtener un equilibrio adecuado entre la exactitud y la gama dinámica. Cabe señalar que no se necesita un bit de signo ya que la distorsión no es negativa. Para abarcar una gama dinámica suficiente, se utiliza una base 16 y se emplean 4 bits para el exponente (exp). La mantisa (m) se expresa con 4 bits. Por consiguiente, el valor distorsión total, D, viene dado por:

$$D = m \times 16^{exp}$$

donde m tiene un valor dentro de la gama $0 \leq m \leq 15$ y exp tiene un valor comprendido en la gama $0 \leq exp \leq 15$. Un valor de distorsión cero se representa por m = 0 y exp = 0, lo que supone que el campo distorsión es cero. Al asignar 4 bits para la mantisa, m, la exactitud es de $½ \times (1/2^4) = 1/32$ o cerca del 3%. Con 4 bits para el exponente y la utilización de una base 16, la gama dinámica va de 0 a máx, estando máx determinado por m = 15 y exp = 15, lo que corresponde a una distorsión de $15 \times 16^{15} = 1{,}7 \times 10^{19}$.

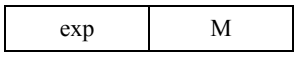


Figura 15 – Sintaxis del campo distorsión

exp: Exponente del valor del campo distorsión (base 16).

m: Mantisa del valor del campo distorsión.

Cuadro 15 – Valores de parámetros del campo distorsión

Parámetro	Tamaño (bits)	Valores
exp	4	0 ... 15
m	4	0 ... 15

Cabe señalar que con este formato de distorsión, puede realizarse fácilmente una comparación entre dos distorsiones para determinar cuál de ellas es mayor comparando los dos valores de distorsión como un carácter si signo. Específicamente, para realizar esta comparación no es necesario convertir el formato de seudo punto-flotante a la distorsión total real para determinar cuál de los dos valores de distorsión es mayor. Esta propiedad puede simplificar el procesamiento de varias aplicaciones.

5.7.3.2.2 Campo distorsión de dos bytes

En el formato de dos bytes, los valores de distorsión se expresarán como un número de dos bytes con un formato de seudo punto-flotante. El formato de seudo punto-flotante para la distorsión se define a continuación. Este formato se utiliza en E.1.1.1 (ecuación E.3) de la Rec. UIT-T T.800 | ISO/CEI 15444-1 para expresar el tamaño del escalón de cuantización para JPEG 2000. Cada número de 16 bits contiene el exponente (5 bits) y la mantisa (11 bits) del valor métrico. En concreto, el valor *V* de punto flotante de la medición se obtiene mediante la siguiente fórmula:

$$V = 2^{\varepsilon - 15}\left(1 + \frac{\mu}{2^{11}}\right) \quad \text{si } \varepsilon \neq 0$$

$$V = 0 \quad \text{si } \varepsilon = 0$$

donde ε es el entero sin signo obtenido a partir de los cinco bits más significativos del parámetro, y μ el entero sin signo que se obtiene a partir de los 11 bits restantes. El caso especial de $V = \infty$ corresponde a μ = 0 y ε = 31. Cabe señalar que los valores por debajo de esta representación se ponen a cero.

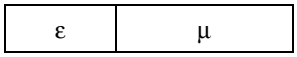


Figura 16 – Sintaxis del campo distorsión

ε: Exponente del valor del campo distorsión de dos bytes

μ: Mantisa del valor del campo distorsión de dos bytes

Cuadro 16 – Valores de parámetros del campo distorsión

Parámetro	Tamaño (bits)	Valores
ε	5	0 ... 31
μ	11	0 ... $(2^{11} - 1)$

El algoritmo para calcular ε y μ no se define como parte obligatoria de esta Recomendación | Norma Internacional. Puede utilizarse una técnica que aplica los siguientes pasos (se presenta un ejemplo de conversión del número 12,25). Si $V = 0$, $\varepsilon = \mu = 0$. Es decir:

- convertir V en número binario ($12{,}25_{10} = 1100{,}01_2$);
- normalizar el número. Esto significa que debería haber un 1 a la izquierda de la coma y que la multiplicación al cuadrado representa el valor original. La forma normalizada de 1100,01 es $1{,}10001 \times 2^3$;
- el exponente es 2, presentado en notación de exceso. La desviación exponencial es 15. En este ejemplo, el exponente se representa como 18_{10} (10010_2);
- la mantisa representa los bits significativos, *excepto el bit a la izquierda de la coma*, que siempre es uno y por consiguiente no ha de almacenarse. Pueden añadirse ceros hasta obtener 11 bits. En este ejemplo, la mantisa es 10001000000.

5.7.3.2.3 Campo importancia relativa

El campo importancia relativa, *r*, puede utilizarse para describir la importancia relativa entre distintas unidades de codificación sin necesariamente remitirse a una medida específica de la distorsión. Esto permite describir la importancia relativa o la prioridad entre unidades de codificación sin explícitamente indicar cuánto más importante es una con respecto a la otra. Esta importancia relativa de los datos asociados se especifica gracias a un campo de *n* bytes que soporta 2^{8n} clasificaciones posibles, como se muestra en la figura 17 y en el cuadro 17, y el número de bytes *n* de este campo está indicado en Mzoi. Por ejemplo, utilizando un campo importancia relativa de un byte, pueden obtenerse hasta 256 clasificaciones posibles. Cuanto mayor es el valor, mayor es la importancia, como ocurre en el campo distorsión.

Figura 17 – Sintaxis del campo importancia relativa

r: Valores de importancia relativa

Cuadro 17 – Valores de parámetros del campo importancia relativa

Parámetro	Tamaño (bits)	Valores
r	8 * n	0 ... ($2^{8n} - 1$)

5.7.3.2.4 Comentarios adicionales sobre el campo distorsión y el campo importancia relativa

Tanto en el campo distorsión de un byte como en el campo importancia relativa de un byte los valores más grandes corresponden a una mayor importancia, por lo que es posible establecer una comparación entre estas dos unidades de datos, independientemente de si el campo distorsión especifica la distorsión real o la importancia relativa. Se pueden así simplificar las aplicaciones.

Los encabezamientos pueden especificarse utilizando los campos distorsión o importancia relativa. La pérdida de varios tipos de datos, como el encabezamiento principal y el encabezamiento de parte losa o el encabezamiento SEC impiden la decodificación de los datos de imagen correspondientes. El creador JPSEC puede querer asignar una distorsión a los datos utilizando:

1) el mayor valor de distorsión (que se especifica a continuación) para señalar el encabezamiento o los datos más importantes; o
2) para describir la distorsión total que se puede crear si la imagen o la porción de la imagen no pueden decodificarse.

El creador dispone de un cierto grado de flexibilidad a la hora de señalar los encabezamientos.

El mayor valor de distorsión para los campos de un byte es un byte de todo unos (0xFF). Cabe señalar que este valor representa el mayor valor de distorsión posible tanto para el campo distorsión por error cuadrático total de un byte, como para el campo importancia relativa de un byte. El mayor valor de distorsión en un campo distorsión de dos bytes son dos bytes puestos a todo unos (0xFFFF). La mayor importancia en el campo importancia relativa de una longitud de n bytes es un valor de n bytes puestos a todo unos.

5.7.3.2.5 Uso conjunto del campo distorsión y el campo importancia relativa

El campo distorsión y el campo importancia relativa pueden utilizarse simultáneamente para describir la zona especificada por la ZOI. En este caso, ambos campos especifican la distorsión por error cuadrático, aunque el campo distorsión especifica la reducción incremental de la distorsión, mientras que el campo importancia relativa indica la distorsión total. En concreto, el campo distorsión especifica la reducción incremental de la distorsión que se produciría en la ZOI decodificada. Esto supone que toda la información necesaria para decodificar la ZOI está disponible y se centra en la reducción incremental de la distorsión producida por la ZOI. El campo importancia relativa específica la distorsión total que se obtendría de no estar disponible la ZOI, es decir, especifica la distorsión total que se obtendría si no pudiese decodificarse la ZOI teniendo en cuenta no sólo el valor de la ZOI (como se expresa en el campo distorsión) sino también la distorsión producida por la imposibilidad de decodificar otras partes del tren de bits comprimido que dependen de la ZOI. La distorsión total asociada con distintas ZOI sirve para medir la importancia relativa de las distintas ZOI. Cuando ambos campos se utilizan, se utilizará la misma expresión matemática para la distorsión, como se indica en el campo distorsión.

5.7.3.3 Campo velocidad binaria

El campo velocidad binaria se utiliza para especificar la zona protegida en un dominio de coeficiente ondícula. Identifica los planes de bits más significativos cuya velocidad binaria comprimida está especificada en este campo. Los MSB se seleccionan utilizando un proceso de optimización de distorsión de velocidad como se especifica en la Parte 1. Por ejemplo, si la velocidad binaria es 2,5, las zonas protegidas incluyen los MSB de todos los coeficientes ondícula cuya velocidad binaria comprimida es 2,5 bit por píxel. La sintaxis del campo velocidad binaria se encuentra en la figura 18 y en el cuadro 18. La velocidad binaria especificada se obtiene con la fórmula:

$$R = I_R + F_R/16$$

Por ejemplo, la velocidad binaria de cero se representa por $I_R = 0$ y $F_R = 0$; y la velocidad binaria de 2,5 se representa por $I_R = 2$ y $F_R = 8$.

Figura 18 – Sintaxis del campo velocidad binaria

I_R: Parte entera de la velocidad binaria especificada.

F_R: Parte fraccionaria de la velocidad binaria especificada.

Cuadro 18 – Valores de parámetros del campo velocidad binaria

Parámetro	Tamaño (bits)	Valores
I_R	4	0 ... 15
F_R	4	0 ... 15

5.7.4 Relación entre múltiples parámetros

5.7.4.1 Generalidades

Cuando la clase de descripción relacionada con la imagen tiene múltiples campos configurados simultáneamente, la zona resultante será la intersección de estos campos. Por ejemplo, una zona puede especificar el nivel de resolución más bajo en la 2ª losa. La unión de los campos puede determinarse utilizando múltiples zonas en la ZOI.

La clase de descripción no relacionada con la imagen también puede tener múltiples campos configurados simultáneamente. En este caso, los modos para los distintos campos de parámetros tendrán el mismo número de elementos (la excepción a esta regla se expone a continuación), y estos elementos se corresponderán mutuamente uno a uno. Por ejemplo, si la zona utiliza gamas de bits y gamas de paquetes, cada una de ellas tendrá el mismo número de elementos en cada gama, y la primera gama de bits se corresponderá con la primera gama de paquetes, etc.

Hay una excepción a la regla expuesta que requiere el mismo número de elementos en cada campo. Esto ocurre cuando uno de los campos f1 contiene un elemento que especifica una gama de elementos (como se describe en el modo de gama de 5.7.6) y esta gama contiene N elementos, y otro campo f2 está especificado por una lista de N elementos. En este caso, el campo f1, que sólo contiene un elemento (la gama) se interpreta como una lista de N elementos. Estos N elementos especificados por la gama de f1 se corresponderán uno a uno con los N elementos enumerados en f2. Por consiguiente, una gama de elementos puede asociarse a un único elemento o a múltiples elementos (uno para cada elemento de la gama).

5.7.4.2 Ejemplos

Como se muestra en la figura 11, la estructura de la clase de descripción de zona puede tener múltiples campos configurados simultáneamente, donde los campos N son las descripciones relacionadas con la imagen (D_i^1, D_i^2, ... , D_i^N) y los campos M son las descripciones no relacionadas con la imagen (D_n^1, D_n^2, ... , D_n^M). La semántica puede entenderse como $\{D_i^1 \cap D_i^2 \cap \ldots \cap D_i^N\} = D_n^1 = D_n^2 = \ldots = D_n^M$, es decir, la intersección de las descripciones relacionadas con la imagen N se corresponden con cada descripción no relacionada con la imagen M y, además, las descripciones no relacionadas con la imagen M se corresponden mutuamente. Esta relación se ilustra en los tres siguientes ejemplos.

En el primer ejemplo, la descripción de zona tiene dos descripciones relacionadas con la imagen: una para la resolución 2 y la otra para la capa 3. En este caso, los datos incluidos son la intersección de la resolución 2 y la capa 3, como se muestra en la figura 19.

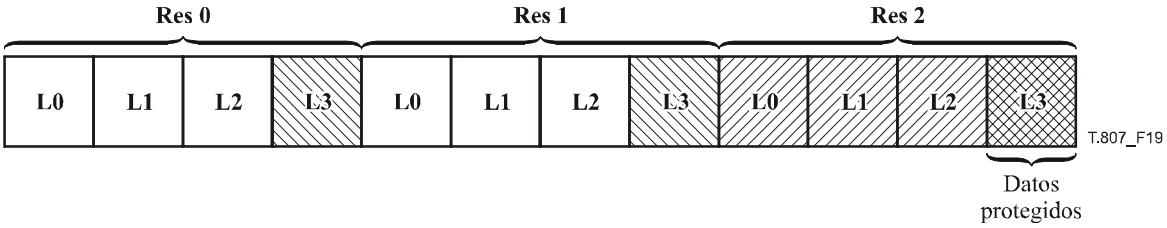


Figura 19 – Ejemplo de ZOI utilizando descripciones relacionadas con la imagen

En el segundo ejemplo la descripción de zona tiene dos descripciones relacionadas con la imagen (que son la resolución 2 y la capa 3) y una descripción no relacionada con la imagen (que es la gama de paquetes 80-100 paquetes). En este caso, los datos influidos son la intersección de la resolución 2 y la capa 3. Además, se indica que los datos influidos están en la gama de paquetes 80 a 100.

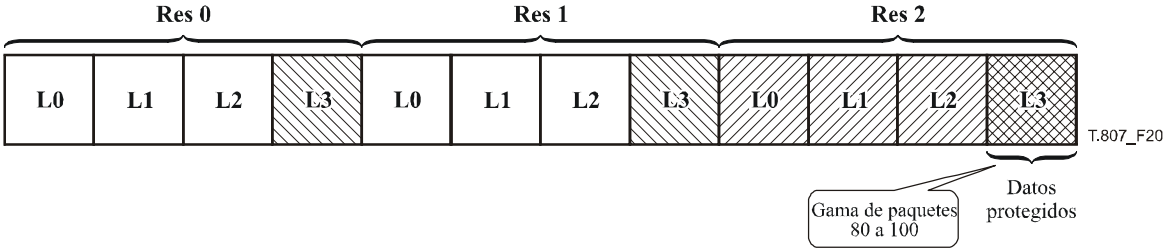


Figura 20 – Ejemplo de ZOI utilizando descripciones relacionadas con la imagen y no relacionadas con la imagen

En el tercer ejemplo, la descripción de zona tiene dos descripciones relacionadas con la imagen (resolución 2 y capa 3) y dos descripciones no relacionadas con la imagen (gama de paquetes 80-100 y gama de byte 856-1250). Una vez más, los datos influidos son la intersección de la resolución 2 y la capa 3 y están contenidos en los paquetes de la gama 80 a 100. Además, estos paquetes y la zona influida están ubicados en la gama de bytes 856-1250.

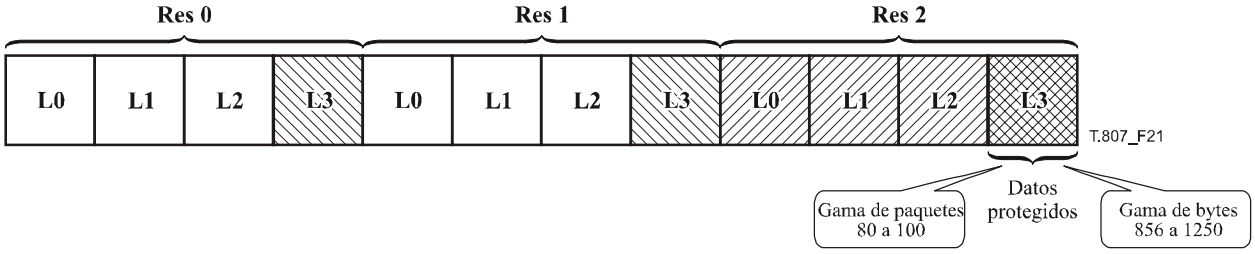


Figura 21 – Segundo ejemplo de ZOI utilizando descripciones relacionadas con la imagen y no relacionadas con la imagen

5.7.5 Protección de datos después del marcador SEC

Todo lo antes expuesto se ha centrado principalmente en el soporte de servicios de protección para el tren codificado JPEG 2000. No obstante, muchos elementos del encabezamiento principal, incluida la señalización JPSEC, también pueden protegerse y pueden asimismo utilizarse la ZOI y los métodos de protección para ello.

En concreto, el modo de gama de bytes de la clase de descripción no relacionada con la imagen puede utilizarse para especificar que ha de aplicarse una herramienta JPSEC a cualquier dato que vaya detrás del marcador SEC. Como se ha indicado antes, el primer byte del encabezamiento SEC es el byte 1 para la indexación de la gama de bytes. Los datos que siguen al marcador SEC y pueden protegerse incluyen el segmento SEC y la mayor parte del encabezamiento principal. Cabe señalar que todo el encabezamiento principal JPEG 2000, excepto el segmento marcador SIZ, puede trasladarse después del marcador SEC y, por consiguiente, protegerse utilizando este método. Si ha de protegerse el segmento marcador SIZ JPEG 2000, esto se hará a un nivel superior, es decir, en la capa de formato de fichero.

Las herramientas JPSEC para la protección del segmento SEC serán generalmente las primeras herramientas del segmento SEC, lo que permite al consumidor obtener en primer lugar los datos del segmento SEC que, posteriormente, utilizará para procesar el resto del tren codificado.

5.7.6 Sintaxis de parámetros de la descripción de zona (Pzoi)

En la figura 22 se muestra la sintaxis de parámetros de la descripción de ZOI.

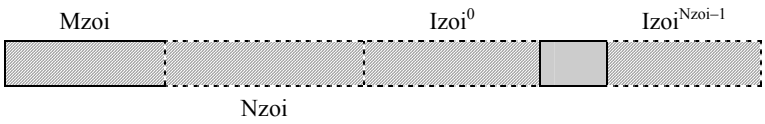


Figura 22 – Sintaxis de parámetros de descripción de ZOI

Mzoi: Modo de descripción de ZOI. Este campo utiliza la estructura FBAS.

Nzoi: Número de Izoi. Este campo utiliza la estructura RBAS.

Izoi^{i}: Elemento.

Cuadro 19 – Valores de parámetros de Pzoi^{i}

Parámetro	Tamaño (bits)	Valores
Mzoi	Variable (FBAS)	Véase el cuadro 20
Nzoi	0 8 + 8 * n (RBAS)	Si el bit número 2 de Mzoi es 0. 2 ... (2^{7+7*n} – 1)
Izoi^{i}	Variable	Depende del modo especificado en Mzoi

Cuadro 20 – Valores de parámetro de Mzoi

Número de bit FBAS	Valores (bits)	Semántica
1	0	Las zonas especificadas están influidas por la herramienta JPSEC
	1	El complemento de las zonas especificadas influidas
2	0	Se especifica un solo elemento
	1	Se especifican múltiples elementos
3, 4	00	Modo rectángulo. Una región rectangular donde el primer par de valores especifica la esquina superior izquierda y el segundo par la esquina inferior derecha, inclusive. Para cada esquina, el primer valor será la posición horizontal y el segundo la posición vertical. La indexación empezará en 0 y utilizará la cuadrícula de referencia definida en JPEG 2000 Parte 1.
	01	Modo gama. Una gama de valores donde el primero especifica el índice inicial y el segundo el índice final, inclusive
	10	Modo índice. Especifica un único valor
	11	Mod máx. Especifica el valor máximo
5, 6	00	$Izoi^i$ utiliza enteros de 8 bits
	01	$Izoi^i$ utiliza enteros de 16 bits
	10	$Izoi^i$ utiliza enteros de 32 bits
	11	$Izoi^i$ utiliza enteros de 64 bits
7, 8	00	$Izoi^i$ se describe en una dimensión
	10	$Izoi^i$ se describe en dos dimensiones
	01	$Izoi^i$ se describe en tres dimensiones
9	0	No se utiliza el modo de desplazamiento con longitudes
	1	Se utiliza el modo de desplazamiento con longitudes: se especifica el desplazamiento inicial con las longitudes de los bytes contiguos que siguen. La existencia de esta bandera anula los modos especificados en los bits 3 y 4.
		Todos los demás valores están reservados

Cuando se utilizan las etiquetas TRLCP, su tamaño está definido por P_{TRLCP}, como se indica en el cuadro 4. En este caso, se anulan los bits 5 y 6 del parámetro M_{ZOI}.

El modo de desplazamiento con longitudes puede utilizarse para representar convenientemente una serie de segmentos consecutivos, por ejemplo, una serie de gamas de bytes consecutivas. El primer valor especifica el desplazamiento inicial y los siguientes valores las longitudes de cada segmento consecutivo. Si se utiliza este campo para representar n segmentos, Nzoi se podrá a n + 1.

5.8 Sintaxis del modelo de método de protección (T)

5.8.1 Generalidades

Los modelos de método de protección contienen parámetros para cada herramienta JPSEC descrita en 5.6.1. Por ejemplo, se utilizan en las herramientas JPSEC normativas de 5.6.2. Asimismo, pueden utilizarse en las herramientas JPSEC no normativas de 5.6.3. Hay tres tipos de modelos de métodos de protección: modelo de descriptación, modelo de autenticación y modelo de función generadora. El modelo utilizado por una herramienta JPSEC normativa se especifica por su ID, como se muestra en el cuadro 6, y nuevamente en el cuadro 21 con referencia a las subcláusulas donde están definidas.

Como se indica en 5.6.2, el modelo de método de protección, T, junto con el dominio de procesamiento de la herramienta JPSEC, PD, la granularidad, G, y la lista de valores, V, describen la aplicación de la herramienta JPSEC.

Cuadro 21 – Valores ID de modelo (ID_T)

Valores	Modelo de método de protección
0	Reservado
1	Modelo de descriptación, véase 5.8.2
2	Modelo de autenticación, véase 5.8.3
3	Modelo de función generadora, véase 5.8.4
4	Herramienta NULA
	Todos los demás valores están reservados para utilización por parte de la ISO

5.8.2 Modelo de descriptación ($T = T_{decry}$, si $t = 0$ e $ID = 1$)

El modelo de descriptación, T_{decry}, se utiliza para indicar al descriptador cómo descriptar el tren codificado recibido. En la figura 23 se muestra la sintaxis del modelo de descriptación. En el cuadro 22 se muestran los tamaños y valores de los símbolos y parámetros del modelo de descriptación.

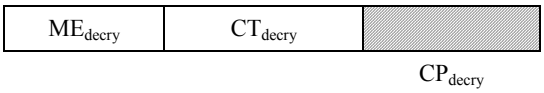


Figura 23 – Sintaxis del modelo de descriptación

ME_{decry}: Bandera de emulación de marcador falsa que indica si se ha realizado una emulación de marcador falsa en los datos criptados. La emulación de marcador falsa puede afectar negativamente el funcionamiento de los decodificadores JPEG 2000 Parte 1. Este campo utiliza la estructura FBAS.

CT_{decry}: Identificación del tipo de cifrado.

CP_{decry}: Parámetro de cifrado.

Cuadro 22 – Valores de parámetros del modelo de descriptación

Parámetro	Tamaño (bits)	Valores
ME_{decry}	8 + 8 * n (FBAS)	Cuadro 23
CT_{decry}	16	Cuadro 24
CP_{decry}	Variable	Si $CT_{decry} < 0x6000$, véase 5.8.2.1. Si $0x6000 \leq CT_{decry} < 0xC000$, véase 5.8.2.2. Si $CT_{decry} \geq 0xC000$, véase 5.8.2.3.

Cuadro 23 – Valores de la bandera de emulación de marcador (ME_{decry})

Valores	Tipo de método
01xx xxxx	Los datos criptados no contienen una emulación de marcador falsa
00xx xxxx	Otro
	Todos los demás valores están reservados para utilización por parte de la ISO

El valor por defecto de la bandera de emulación de marcador es 0. Esta bandera puede ponerse a 1 para indicar que los datos criptados JPSEC no contienen una emulación de marcador falsa. El creador JPSEC puede optar por dejar esta bandera en su valor por defecto de 0.

Cuadro 24 – Valores de identificador cifrado (CT_{decry})

Valores	Tipo de cifrado
0 ... 0x5FFF	Cifrado de bloque (véase el cuadro 25)
0x6000 ... 0xBFFF	Cifrado de tren (véase el cuadro 26)
0xC000 ... 0xFFFF	Cifrado asimétrico (véase el cuadro 27)

Cuadro 25 – Valores de identificador del cifrado de bloque (CT_{decry})

Valores	Tipo de cifrado
0x0000	NULO (no hay criptación)
0x0001	AES (ISO/CEI 18033-3)
0x0002	TDEA (ISO/CEI 18033-3)
0x0003	MISTY1 (ISO/CEI 18033-3)
0x0004	Camellia (ISO/CEI 18033-3)
0x0005	CAST-128 (ISO/CEI 18033-3)
0x0006	SEED (ISO/CEI 18033-3)
	Todos los demás valores se reservan para utilización por parte de la ISO

Cuadro 26 – Valores de identificador de cifrado de tren (CT_{decry})

Valores	Tipo de cifrado
0x6000	SNOW 2 (ISO/CEI 18033-4)
	Todos los demás valores están reservados para utilización por parte de la ISO

Cuadro 27 – Valores de identificador del cifrado asimétrico (CT_{decry})

Valores	Tipo de cifrado
0xC000	RSA-OAEP (ISO/CEI 18033-2)
	Todos los demás valores están reservados para utilización por parte de la ISO

5.8.2.1 Modelo de cifrado de bloque (CP_{decry} para cifrado de bloque)

El modelo de cifrado de bloque se utiliza para indicar al descriptador de bloque cómo descriptar el tren codificado recibido. En la figura 24 se muestra el modo cifrado de bloque, el modo relleno, el tamaño del bloque y la información de clave.

Algunos modos de cifrado de bloque utilizan vectores de inicialización. En estos casos, los vectores de inicialización de las herramientas se especifican utilizando el campo granularidad de herramienta (G) descrito en 5.10 y el campo lista de valores (V) de 5.11. Concretamente, los vectores de inicialización se utilizan únicamente para los modos con ID $M_{bc} > 0x80$, por ejemplo CBC, CFB, OFB y CTR. En el caso de CTR, no se trata en realidad de un IV, sino de un *contador*. El tamaño del vector de inicialización especificado por la lista de valores, V, se pondrá al tamaño de bloque, SIZ_{bc}.

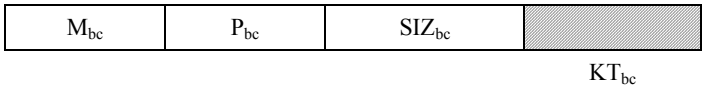


Figura 24 – Sintaxis del modelo de cifrado de bloque

M_{bc}: Modo cifrado de bloque. El primer bit indica la utilización de vectores de inicialización con esta herramienta. Si $M_{bc} < 0x8$, no se utilizan IV, en cualquier otro caso, se requieren uno o más valores IV para este modo.

P_{bc}: Modo relleno.

SIZ_{bc}: Tamaño del bloque en bytes.

KT_{bc}: Modelo de clave (véase 5.8.5). Contiene información sobre las claves utilizadas por el cifrado de bloque.

Cuadro 28 – Valores del modelo de cifrado de bloque

Parámetro	Tamaño (bits)	Valores
M_{bc}	6	Cuadro 29
P_{bc}	2	Cuadro 30
SIZ_{bc}	8	1 ... 256
KT_{bc}	Variable	Véase 5.8.5

Cuadro 29 – Valores del modo cifrado de bloque (M_{bc})

Valores	Tipo de modo
0	Reservado
0x xxxx	Modos utilizados sin IV
1x xxxx	Modos utilizados con un IV
x0 xxxx	Los bits no se rellenan
x1 xxxx	Los bits se rellenan
0x 0001	ECB (ISO/CEI 10116)
1x 0010	CBC (ISO/CEI 10116)
1x 0011	CFB (ISO/CEI 10116)
1x 0100	OFB (ISO/CEI 10116)
1x 0101	CTR (ISO/CEI 18033-2)
	Todos los demás valores están reservados para utilización por parte de la ISO

NOTA 1 – Se requiere una implementación cuidadosa en todos los modos, porque una aplicación indebida puede crear vulnerabilidades. Cabe señalar que incluso una implementación correcta de ECB crea una fuga de información cuando aparecen bloques idénticos. Las directrices al respecto pueden encontrarse en ISO/CEI 10116.

NOTA 2 – Los valores del cuadro 30 sólo son aplicables cuando M_{bc} del cuadro 29 especifica que los bits llevan relleno. Cuando los bits no llevan relleno, P_{bc} se pondrá a 00.

Cuadro 30 – Modo relleno para el cifrado de bloque (P_{bc})

Valores	Tipo de relleno
00	Robo de texto cifrado (RFC 2040)
01	Relleno PKCS#7 (PKCS#7)
	Todos los demás valores están reservados para la utilización por parte de la ISO

NOTA 3 – Cuando se utiliza el relleno, debe diseñarse cuidadosamente el sistema para evitar posibles fallos de seguridad, como ataques cifrados.

5.8.2.2 Modelo de cifrado de tren (CP_{decry} para cifrado de tren)

El modelo de cifrado de tren se utiliza para indicar al descriptador de tren cómo descriptar el tren codificado recibido. En la figura 25 se muestra la sintaxis del modelo de cifrado de tren. En el cuadro 31 se muestran los valores del modelo de cifrado de tren.

Los vectores de inicialización del cifrado de tren se especifican utilizando el campo granularidad de la herramienta (G) descrito en 5.10 y el campo lista de valores (V) de 5.11. El tamaño del vector de inicialización especificado en la lista de valores V se pondrá al tamaño de clave definido en el modelo de información de clave, KT_{sc}.

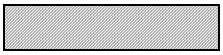


Figura 25 – Sintaxis del modelo de cifrado de tren

KT_{sc}: Modelo de información de clave (véase 5.8.5). Contiene información sobre las claves utilizadas para cifrar el tren.

Cuadro 31 – Valores del modelo de cifrado de tren

Parámetro	Tamaño (bits)	Valores
KT_{sc}	Variable	Véase 5.8.5

5.8.2.3 Modelo de cifrado asimétrico (CP_{decry} para el cifrado asimétrico)

El modelo de cifrado asimétrico se utiliza para indicar al descriptador de cifrado asimétrico cómo descriptar el tren codificado recibido. En la figura 26 se muestra la sintaxis del modelo cifrado asimétrico. El cuadro 32 muestra los valores del modelo de cifrado asimétrico.

En el caso de las herramientas que utilizan el modelo de cifrado asimétrico, el campo granularidad de la herramienta (G) especifica la granularidad con que se aplica el cifrado. No obstante, el campo lista de valores (V) no se utiliza para representar valor alguno, por lo que el número de elementos (N_v) del campo lista de valores se pondrá a 0.

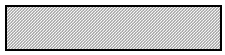


Figura 26 – Sintaxis del modelo de cifrado asimétrico

KT_{sy}: Modelo información de clave (véase 5.8.5). Contiene información sobre las claves que se utilizan para el cifrado asimétrico.

Cuadro 32 – Valores del modelo de cifrado asimétrico

Parámetro	Tamaño (bits)	Valores
KT_{sy}	Variable	Véase 5.8.5

5.8.3 Modelo de autenticación (T = T_{auth}, si t = 0 e ID = 2)

El modelo de autenticación, T_{auth}, se utiliza para indicar al verificador cómo verificar la autenticidad del tren codificado recibido. Hay tres clases generales de métodos de autenticación: autenticación por número generador, autenticación por cifrado y firmas digitales. Los métodos de autenticación por número generador y por cifrado también suelen denominarse códigos de autenticación de mensaje (MAC) y a sus valores, que se utilizan para la autenticación, se les suele denominar valores MAC. En la figura 27 se muestra la sintaxis del modelo de autenticación y en el cuadro 33 los tamaños y valores de los símbolos y parámetros para el modelo de autenticación.

En numerosas aplicaciones de seguridad, la autenticación es el servicio de seguridad más importante. Incluso cuando la confidencialidad es el servicio de seguridad deseado, éste debe complementarse con la autenticación para evitar cualquier tipo de ataque. En concreto, se recomienda autenticar partes del segmento marcador SEC. Además, la autenticación se realizará tanto en los parámetros del modelo de autenticación (T_{auth}) como en el mensaje que hay que autenticar. Específicamente, la zona de influencia indicará que tanto el contenido como los parámetros del modelo de autenticación (T_{auth}) deben autenticarse.

Figura 27 – Sintaxis del modelo de autenticación

M_{auth}: Método de autenticación.

P_{auth}: Parámetros de autenticación.

Cuadro 33 – Valores de parámetros del modelo de autenticación

Parámetro	Tamaño (bits)	Valores
M_{auth}	8	Cuadro 34
P_{auth}	Variable	Si M_{auth} = 0, véase 5.8.3.1, Si M_{auth} = 1, véase 5.8.3.2, Si M_{auth} = 2, véase 5.8.3.3.

Cuadro 34 – Método de autenticación (M_{auth})

Valores	Método
0	MAC por número generador
1	MAC por cifrado
2	Firma digital
	Todos los demás valores están reservados para utilización por parte de la ISO

5.8.3.1 Autenticación por número generador (P_{auth} para MAC por número generador)

La autenticación MAC por número generador se utiliza para indicar al verificador cómo verificar la autenticidad del tren codificado recibido. En la figura 28 se muestra la sintaxis del modelo de autenticación por número generador y en el cuadro 35 los valores de los parámetros.

Los valores MAC se especifican utilizando el campo granularidad de la herramienta (G) de 5.10 y el campo lista de valores (V) de 5.11. El tamaño del valor MAC especificado en la lista de valores V se pondrá al tamaño MAC definido por SIZ_{HMAC}.

Figura 28 – Modelo de autenticación por número generador

M_{HMAC}: Identificador del método de autenticación por número generador.

H_{HMAC}: Identificador del número generador.

KT_{HMAC}: Modelo de clave.

SIZ_{HMAC}: Tamaño de MAC (bits).

Cuadro 35 – Valores de parámetros del modelo de autenticación por número generador

Parámetro	Tamaño (bits)	Valores
M_{HMAC}	8	Cuadro 36
H_{HMAC}	8	Cuadro 37
KT_{HMAC}	Variable	Véase 5.8.5
SIZ_{HMAC}	16	0 ... 65535

Cuadro 36 – Identificador del método de autenticación por número generador (M_{HMAC})

Valores	Método de autenticación por número generador
0	Reservado
1	HMAC (ISO/CEI 9797-2)
	Todos los demás valores están reservados para su utilización por parte de la ISO

Cuadro 37 – Identificador de la función generadora (H_{HMAC})

Valores	Función generadora
0	Reservado
1	SHA-1 (ISO/CEI 10118-3)
2	RIPEMD-128 (ISO/CEI 10118-3)
3	RIPEMD-160 (ISO/CEI 10118-3)
4	MASH-1 (ISO/CEI 10118-4)
5	MASH-2 (ISO/CEI 10118-4)
6	SHA-224 (ISO/CEI 10118-3)
7	SHA-256 (ISO/CEI 10118-3)
8	SHA-384 (ISO/CEI 10118-3)
9	SHA-512 (ISO/CEI 10118-3)
10	WHIRLPOOL (ISO/CEI 10118-3)
	Todos los demás valores están reservados para uso por parte de la ISO

Cabe señalar que si SIZ_{HMAC} es inferior al tamaño nominal del número generador, se trata de la versión truncada correspondiente a los primeros bits SIZ_{HMAC} del número generador.

5.8.3.2 Modelo de autenticación por cifrado (P_{auth} para MAC por cifrado)

La autenticación MAC por cifrado se utiliza para indicar al verificador cómo verificar la autenticidad del tren codificado recibido. En la figura 29 se muestra el modelo y en el cuadro 38 el tamaño de claves de número generador. Un ejemplo de autenticación por cifrado es CBC-MAC. En estas técnicas de cifrado de bloque para autenticación, el vector de inicialización tiene una longitud de un bloque y un valor de 0. Para el cifrado de bloque se utiliza una longitud por defecto de un bloque. Hay que tener en cuenta que, si SIZ_{CMAC} es inferior al tamaño nominal del MAC autenticación por cifrado, se trata de la versión truncada correspondiente a los primeros bits SIZ_{CMAC} de MAC.

Cabe señalar que, si el número de bits de datos no es un múltiplo del tamaño de bloque de cifrado, el bloque original final será un bloque parcial de datos, con alineación a la izquierda y ceros anexados para formar un bloque de cifrado completo. Hay que tener en cuenta también que CBC-MAC sólo se aplicará a los datos con una longitud fija y conocida.

Los valores MAC se especifican utilizando el campo granularidad de la herramienta (G) de 5.10 y el campo lista de valores (V) de 5.11. El tamaño del valor MAC especificado en la lista de valores V, se pondrá al tamaño MAC definido por SIZ_{CMAC}.

Figura 29 – Sintaxis del modelo de autenticación por cifrado

CA_{CMAC}: Método de autenticación por cifrado.

C_{CMAC}: Valor identificador de cifrado de bloque.

KT_{CMAC}: Modelo de clave.

SIZ_{CMAC}: Tamaño del MAC (bits).

Cuadro 38 – Valores del modelo MAC

Parámetro	Tamaño (bits)	Valores
CA_{CMAC}	8	Cuadro 39
C_{CMAC}	8	Cuadro 25
KT_{CMAC}	Variable	Véase 5.8.5
SIZ_{CMAC}	16	0 ... 65535

Cuadro 39 – Método de autenticación por cifrado (C_{CMAC})

Valores	Método
0	CBC-MAC MAC Algoritmo 1 (ISO/CEI 9797-1)
1	CBC-MAC MAC Algoritmo 2 (ISO/CEI 9797-1)
2	CBC-MAC MAC Algoritmo 3 (ISO/CEI 9797-1)
3	CBC-MAC MAC Algoritmo 4 (ISO/CEI 9797-1)
	Todos los valores están reservados para su utilización por parte de la ISO

5.8.3.3 Modelo de firma digital (P_{auth} para firmas digitales)

La firma digital se utiliza para indicar al verificador cómo verificar la autenticidad del tren codificado recibido, así como para verificar la identidad del emisor con objetivos de identificación y no de repudiación. En la figura 30 se define el modelo y en el cuadro 40 se enumeran los valores.

La firma digital se especifica utilizando el campo granularidad de la herramienta (G) de 5.10 y el campo lista de valores (V) de 5.11. El tamaño del valor de firma digital especificado en la lista de valores V se configurará para adaptarse al tamaño definido por SIZ_{DS}. Dado que el tamaño de la lista de valores está representado por bytes y no por bits, este tamaño debe ser el número mínimo de bytes que puedan ajustarse a SIZ_{DS}. Cada valor se representará con los bits menos significativos, y los bits MSB restantes se pondrán a 0.

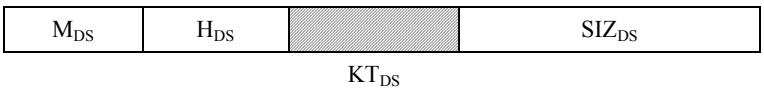


Figura 30 – Sintaxis del modelo de firma digital

M_{DS}: Método de firma digital.

H_{DS}: Función generadora.

KT_{DS}: Modelo de claves (véase 5.8.5). Contiene toda la información relacionada con la clave pública o el certificado necesario para verificar la firma digital.

SIZ_{DS}: Tamaño de la firma digital (bits).

Cuadro 40 – Valores del modelo de firma digital

Parámetros	Tamaño (bits)	Valores
M_{DS}	8	Cuadro 41
H_{DS}	8	Cuadro 37
KT_{DS}	Variable	Véase 5.8.5
SIZ_{DS}	16	0 ... 65535

Cuadro 41 – Métodos de firma digital (M_{DS})

Valores	Método
1	RSA (ISO/CEI 14888-2)
2	Rabin (ISO/CEI 14888-2)
3	DSA (ISO/CEI 14888-3)
4	ECDSA (ISO/CEI 14888-3)
	Todos los demás valores están reservados para utilizarse por parte de la ISO

5.8.4 Modelo de función generadora ($T = T_{hash}$, si t = 0 e ID = 3)

El modelo de función generadora, T_{hash}, se utiliza para indicar los parámetros utilizados para calcular la función generadora. El cuadro 42 muestra los tamaños y valores de los símbolos y parámetros del modelo de función generadora.

Hay que señalar que, por oposición al modelo de autenticación por número generador de 5.8.3.1, que supone la utilización de una función generadora y una clave secreta, este modelo de función generadora no utiliza claves. Si bien este modelo de función generadora puede utilizarse para detectar cualquier error accidental o modificación accidental de los datos, no puede evitar una alteración malintencionada de los datos. Para evitar alteraciones malintencionadas de los datos, debe utilizarse un modelo de autenticación, puesto que la clave secreta utilizada por los modelos de autenticación evita que los datos sean alterados de manera oculta.

Los valores generadores se especifican utilizando el campo granularidad de la herramienta (G) de 5.10 y el campo de lista de valores (V) de 5.11. El tamaño del valor generador especificado en la lista de valores V, se configurará como el tamaño del valor definido por SIZ_{hash}.

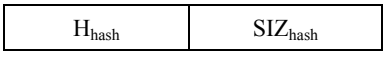


Figura 31 – Sintaxis del modelo de función generadora

H_{hash}: Identificador de la función generadora.

SIZ_{hash}: Tamaño del valor generador (bytes).

Cuadro 42 – Valores de parámetros del modelo de función generadora

Parámetro	Tamaño (bits)	Valores
H_{hash}	8	Cuadro 37
SIZ_{hash}	8	0 ... 255

5.8.5 Modelo de información de claves (KT)

El modelo información de claves se utiliza para comunicar la información de claves. En la figura 32 se define el modelo y en el cuadro 40 se enumeran los valores.

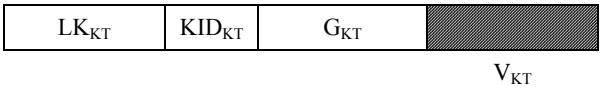


Figura 32 – Sintaxis del modelo de información de claves

LK_{KT}: Longitud de la clave en bits.

KID_{KT}: Identificador información de clave. Indica el significado de los valores en la lista de valores V_{KT}. En el modelo de descriptación este valor debe ponerse a 2 (la URI extrae la clave secreta). En el caso de una firma digital, el valor de este campo puede elegirse libremente.

G_{KT}: Campo granularidad que representa la granularidad con que se modifica la información de claves.

V_{KT}: Campo lista de valores que representa la lista de información de claves en continuo cambio.

Cabe señalar que, en el caso de una clave secreta (modelo de descriptación), la clave pública del certificado no tiene significado: el modelo de claves debe contener alguna información sobre la ubicación de la clave (por ejemplo URI).

La información de claves puede representarse con uno o más valores utilizando el campo granularidad de la herramienta (G_{KT}) de 5.10 y el campo lista de valores (V_{KT}) de 5.11. Los dos campos (G_{KT} y V_{KT}) juntos determinan cómo los valores de clave de la lista de valores (V_{KT}) se aplican a los datos de imagen protegida, como se indica en 5.10 y 5.11.

La información de claves de la lista de valores puede adoptar las formas especificadas en el cuadro 44. Si $KID_{KT} = 1$, cada valor se especifica con un modelo de certificado X.509, como se indica en 5.8.5.1. Si $KID_{KT} = 2$, los valores se especifican mediante una URI para el certificado de la clave secreta.

Cuadro 43 – Valores del modelo de claves

Parámetros	Tamaño (bits)	Valores
LK_{KT}	16	1 ... 65535
KID_{KT}	8	Cuadro 44
G_{KT}	24	Véase 5.10
V_{KT}	Variable	Véase 5.11

Cuadro 44 – Valores del identificador de información de claves (KID_{KT})

Valores	Identificador de información de clave
0	Reservado
1	Certificado X.509 (ISO/CEI 9594-8)
2	URI para certificado o clave secreta
	Todos los demás valores se reservan para uso por parte de la ISO

5.8.5.1 Modelo de certificado X.509

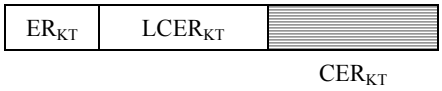


Figura 33 – Sintaxis de certificado X.509

ER_{KT}: Regla de codificación para el certificado X.509.

$LCER_{KT}$: Longitud del certificado X.509 (CER_{KT}) en bytes.

CER_{KT}: Certificado X.509.

Cuadro 45 – Valores de certificado X.509 (KI_{KT} si KID_{KT} = 2)

Parámetros	Tamaño (bits)	Valores
ER_{KT}	8	0 ... 255 (véase el cuadro 46)
$LCER_{KT}$	16	1 ... 65535
CER_{KT}	Variable	–

Cuadro 46 – Valores de la regla de codificación (ER_{KT})

Valores	Identificador de la regla de codificación
0	Reservado
1	DER (RFC 3217)
2	BER (RFC 3394)
	Todos los demás valores están reservados para uso de la ISO

5.9 Sintaxis del dominio de procesamiento (PD)

La sintaxis del dominio de procesamiento se utiliza para indicar en qué dominio se aplica la herramienta JPSEC. Los dominios posibles son el dominio de píxel, el dominio de coeficiente de ondícula, el dominio de coeficiente de ondícula cuantizado y el dominio de tren codificado.

Figura 34 – Sintaxis del dominio de procesamiento

PD: Dominio de procesamiento. Este campo utiliza la estructura FBAS.

F_{PD}: Campo dominio de procesamiento, donde se da información detallada sobre el dominio de procesamiento. Este campo utiliza la estructura FBAS.

Cuadro 47 – Parámetros del dominio de procesamiento

Parámetro	Tamaño (bits)	Valores
PD	Variable (FBAS)	Véase el cuadro 48
F_{PD}	Variable (FBAS)	Para el dominio de coeficiente de ondícula y el dominio de coeficiente cuantizado, véase el cuadro 49 Para el dominio de tren codificado, véase el cuadro 50

Cuadro 48 – Valores de parámetros del dominio de procesamiento (PD)

Número de bit FBAS	Valores	Semántica
1	1	Dominio de píxel. El método de protección se aplica a los píxeles de imagen.
	0	Otro
2	1	Dominio de coeficiente de ondícula. El método de protección se aplica a los coeficientes de ondícula.
	0	Otro
3	1	Dominio de coeficiente cuantizado: El método de protección se aplica al coeficiente de ondícula cuantizado.
	0	Otro
4	1	Dominio de tren codificado: El método de protección se aplica al tren codificado generado por un codificador aritmético.
	0	Otro

Hay que indicar que el campo PD tendrá única y exclusivamente un bit puesto a 1, puesto que las herramientas JPSEC sólo pueden aplicarse a un dominio.

En el dominio de píxel de imagen, el dominio de coeficiente de ondícula y el dominio de coeficiente de ondícula cuantizado, los datos en dos dimensiones han de transformarse a una dimensión para poder aplicar las herramientas de seguridad. Esta transformación se realizará barriendo los datos de imagen en dos dimensiones por filas.

Cuadro 49 – Valores de parámetros del campo dominio de procesamiento (F_{PD}) en el dominio de coeficiente de ondícula y el dominio de coeficiente de ondícula cuantizado

Número de bit FBAS	Valor	Semántica
1	0	El método de protección se aplica al bit con signo
	1	El método de protección se aplica al bit más significativo

Cuadro 50 – Valores de parámetros del campo dominio de procesamiento (F_{PD}) en el dominio de tren codificado

Número de bit FBAS	Valor	Semántica
1	0	El método de protección se aplica tanto al encabezamiento de paquetes como al cuerpo del paquete
	1	El método de protección se aplica únicamente al cuerpo del paquete

El campo (F_{PD}) se utiliza para proporcionar más información relativa al dominio de procesamiento. Con un valor diferente de PD, este campo (F_{PD}) tiene varias semánticas. Por ejemplo, en el dominio de coeficiente de ondícula y el dominio de coeficiente de ondícula cuantizado, el primer bit de F_{PD} se utiliza para indicar si la herramienta JPSEC se aplica al bit más significativo. En el dominio de tren codificado, el primer bit de F_{PD} se utiliza para indicar si la herramienta JPSEC se aplica únicamente al cuerpo del paquete o al cuerpo y al encabezamiento del paquete. En el dominio de píxel, este campo (F_{PD}) está reservado.

5.10 Sintaxis de granularidad (G)

La granularidad se utiliza para indicar la unidad de protección de cada uno de los métodos de protección. En el cuadro 53 se definen las granularidades posibles. En la figura 35 se muestra la sintaxis de la granularidad.

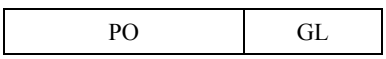


Figura 35 – Sintaxis de granularidad

PO: Orden de procesamiento

GL: Nivel de granularidad

Cuadro 51 – Valores del parámetro granularidad (G)

Parámetro	Tamaño (bits)	Valores
PO	16	Véase el cuadro 52
GL	8	Véase el cuadro 53

Cuadro 52 – Valores de orden de procesamiento (PO)

Valores MSB LSB	Orden de procesamiento
0 000 000 000 000 000	Orden especificado por los parámetros relacionados con la imagen de la zona de influencia
1 000 000 000 000 000	Orden especificado por los parámetros del tren de bits no relacionados con la imagen de la zona de influencia
1 000 000 000 000 001	Orden especificado por los parámetros de paquete no relacionado con la imagen de la zona de influencia
0 000 001 010 011 100	Losa-resolución-capa-componente-precinto
0 000 011 100 001 010	Losa-componente-precinto-resolución-capa
0 000 010 001 011 100	Losa-capa-resolución-componente-precinto
0 000 100 011 001 010	Losa-precinto-componente-resolución-capa
0 000 001 100 011 100	Losa-resolución-precinto-componente-capa
	Todos los demás valores están reservados

Cuadro 53 – Valores del nivel de granularidad (GL)

Valores MSB LSB	Granularidad
0000 0000	Losa
0000 0001	Parte losa
0000 0010	Componente
0000 0011	Nivel de resolución
0000 0100	Capa
0000 0101	Precinto
0000 0110	Paquete
0000 0111	Subbanda
0000 1000	Bloque de código
0000 1001	Zona total identificada por la ZOI
1000 0000	Elemento identificado en una ZOI no relacionada con la imagen
1000 0001	Zona identificada en una ZOI no relacionada con la imagen
	Todos los demás valores están reservados

Para procesar toda la zona especificada por la ZOI, el nivel de granularidad debe ser "zona identificada por la ZOI".

5.11 Sintaxis de la lista de valores (V)

El campo lista de valores se utiliza para especificar valores que cambian a medida que la herramienta se aplica, así como la granularidad con la que se modifica. Esto se utiliza para indicar valores cambiantes, como pueden ser claves, vectores de inicialización, valores MAC, firmas digitales y valores generadores. El campo lista de valores especifica en primer lugar el número de valores en la lista y el tamaño de cada uno de ellos. A continuación los enumera.

Como ya se indicó en 5.6.2, en el caso de las herramientas JPSEC normativas, el campo lista de valores representa un parámetro distinto para cada modelo. Para el modelo de descriptación representa los vectores de inicialización, IV_{bc} o IV_{sc}, dependiendo de si se utiliza un cifrado de bloque o un cifrado de tren. Para el modelo de autenticación, representa el valor MAC, VAL_{MAC}, para la autenticación por número generador o por cifrado. Para el modelo de firma digital, representa la firma digital, SIG_{DS}. Para el modelo de función generadora, representa el modelo generador, HV_{hash}. Algunas utilizaciones de los modelos no requieren la especificación de valores, por ejemplo, no todos los modos de descriptación utilizan vectores de inicialización. En estos casos, el campo lista de valores debe poner N_v y S_v igual a 0, de manera que la lista de valores, VL, no tenga ningún elemento. Si sólo ha de especificarse un único valor, por ejemplo, si se utiliza una única clave para toda la imagen, N_v se pondrá a 1 de manera que la lista de valores sólo contenga un valor.

Figura 36 – Sintaxis del campo lista de valores

N_V: Número de valores en la lista de valores, VL. Si $N_V = 0$, el campo termina. Este campo utiliza la estructura RBAS.

S_V: Tamaño de cada valor en la lista de valores, VL, en bytes. Este campo utiliza la estructura de RBAS.

VL: Lista de valores

Cuadro 54 – Valores de marcador de parámetros del campo lista de valores (V)

Parámetro	Tamaño (bits)	Valores
N_V	16 + 8 * n (RBAS)	0 ... $(2^{15+7*n} - 1)$
S_V	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
VL	0, si $N_V = 0$ $N_V * S_V$, en cualquier otro caso	N/A Determinado por el modelo

5.12 Relaciones entre la ZOI, la granularidad (G) y la lista de valores (VL)

La ZOI, el PO y la GL se utilizan para garantizar el comportamiento exclusivo de las herramientas JPSEC aplicadas, independientemente del orden de progresión del tren codificado JPEG 2000. En otras palabras, la firma resultante, los valores MAC y el tren codificado criptado son independientes del orden progresivo del tren codificado JPEG 2000. La zona de influencia (ZOI) especifica, en su integridad, la parte del tren codificado JPEG 2000 que debe ser protegida por la herramienta JPSEC. El orden de procesamiento (PO, *processing order*), por otra parte, especifica el orden en que la herramienta JPSEC procesa el tren codificado. El nivel de granularidad (GL, *granularity level*) especifica las unidades de protección que contienen secuencias de bytes contiguas en el tren codificado reordenado. Por último, cada unidad de protección corresponde a un valor de la lista de valores (VL, *value list*) en el orden en que aparecen en el tren codificado reordenado. Esta relación puede ilustrarse gracias a un ejemplo en que un tren codificado JPEG 2000 tiene una losa, 3 niveles de resolución y 3 capas, sin importar el número de componentes y precintos. El orden de progresión es RLCP en el tren codificado JPEG 2000 original, la zona de influencia es resolución 0 y 1, y el orden de procesamiento (PO) es TLRCP. En las figuras 37 y 38 se muestra el reordenamiento del tren codificado y la correspondencia entre cada unidad de protección y la lista de valores (VL), cuando el nivel de granularidad (GL) es resolución y capa, respectivamente.

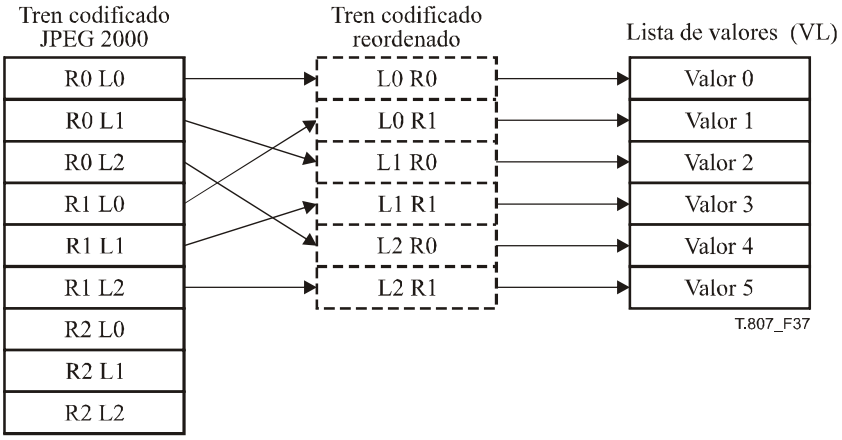


Figura 37 – El nivel de granularidad (GL) es resolución

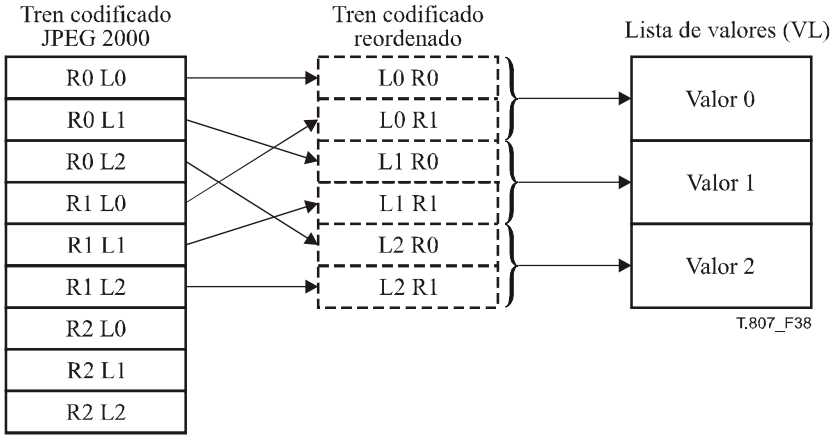


Figura 38 – El nivel de granularidad (GL) es capa

NOTA – El tren codificado reordenado sólo se utiliza para generar valores en la lista de valores (VL). El tren codificado JPSEC final tendrá el mismo orden de progresión que el tren codificado JPEG 2000 original.

5.13 Marcador de seguridad en el tren codificado (INSEC, *in-codestream security marker*)

El marcador de seguridad en el tren codificado (INSEC) es un medio adicional de transmitir información seguridad. Su utilización es facultativa y puede hacerse junto con los marcadores de seguridad SEC. En concreto, se utiliza con herramientas JPSEC no normativas.

Más exactamente, el marcador SEC está presente en el encabezamiento principal y ofrece la información general sobre las herramientas JPSEC que se aplican para proteger la imagen. El marcador INSEC figura en los datos del tren de bits mismo y ofrece parámetros adicionales o alternativos para las herramientas JPSEC no normativas identificadas por el parámetro índice de ejemplar de herramientas. Por consiguiente, el índice de ejemplar de herramientas del marcador INSEC corresponderá a un índice de ejemplar de herramientas del encabezamiento principal.

El segmento marcador INSEC puede situarse en los datos del tren de bits y se aprovecha de que el descodificador aritmético de JPEG 2000 deja de leer bytes del tren de bits cuando encuentra un marcador de terminación (es decir, dos bytes con un valor superior a 0xFF8F).

La información transportada por el segmento marcador INSEC atañe a los bloques de código seguros anteriores y siguientes hasta que se encuentra otro marcador INSEC.

Cabe señalar que la inclusión de un marcador INSEC da como resultado un fichero que puede no ser compatible con JPEG 2000 Parte 1. Hay que tener en cuenta que algunos decodificadores pueden experimentar dificultades a la hora de tratar el marcador en medio de un paquete. La inserción en cualquier punto dentro de un paquete invalida la longitud del paquete como se indica en el encabezamiento del paquete. Asimismo, puede haber problemas con la criptación y los marcadores INSEC debido a:

a) la falta de restricciones de emulación de marcadores en la criptación; y/o

b) la incapacidad de ubicar el marcador en caso de utilizarse la criptación.

La sintaxis del marcador INSEC es la que se muestra en la figura 39.

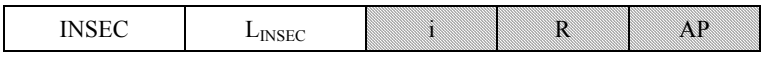


Figura 39 – Sintaxis de marcador de seguridad en el tren codificado

INSEC: Código de marcador. En el cuadro 55 se muestran los tamaños y valores de los símbolos y parámetros del segmento marcador de seguridad en el tren codificado.

L_{INSEC}: Longitud del segmento marcador en bytes (excluido el marcador). Cabe señalar que el segmento marcador INSEC debe estar alineado por bytes.

i: Índice de ejemplar de herramientas correspondiente a uno de los parámetros del índice de ejemplar de herramientas del segmento marcador SEC y, por tanto, que identifica el ejemplar de la herramienta JPSEC a que se refiere este marcador INSEC. Este campo utiliza la estructura RBAS.

R: Zona de relevancia para la información INSEC. Este campo utiliza la estructura FBAS.

AP: Parámetros adicionales alternativos del método de protección. El codificador deberá siempre asegurarse de que el codificador no emula un marcador en este parámetro.

Cuadro 55 – Valores de parámetros de seguridad en el tren codificado (INSEC)

Parámetro	Tamaño (bits)	Valores
INSEC	16	0xFF94
L_{INSEC}	16	2 ... $(2^{16} – 1)$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} – 1)$
R	Variable (FBAS)	Véase cuadro 56
AP	Variable	Definido por la autoridad de registro o la aplicación

Cuadro 56 – Valores de la zona de relevancia (R)

Número de bit FBAS	Valores	Zona de relevancia
0	0	bloques de códigos precedentes
	1	Bloques de códigos siguientes

Dado que INSEC se utiliza con herramientas JPSEC no normativas, el formato de los parámetros adicionales o alternativos está definido por la herramienta misma, identificada por el ID de herramienta. En concreto, las herramientas JPSEC no normativas están definidas por una autoridad de registro o por aplicaciones JPSEC privadas, por lo que la definición de estas herramientas deberá incluir si se permite o no la utilización de INSEC.

6 Ejemplos de utilización de la sintaxis normativa (informativo)

6.1 Ejemplos de ZOI

Esta subcláusula contiene ejemplos que muestran cómo puede utilizarse la sintaxis de la zona de influencia.

En los ejemplos siguientes, los superíndices utilizados con Pzoi, Mzoi, e Izoi corresponden al índice de los elementos relacionados con la imagen y no relacionados con la imagen que se señalan en la estructura BAS de DCzoi en el orden en que aparecen dentro de DCzoi.

6.1.1 Ejemplo 1

En esta subcláusula se muestra un ejemplo en que se ven influidos más de tres niveles de resolución en la región de la imagen cuya esquina superior izquierda es (100, 120) y la esquina inferior derecha es (180, 210). En este ejemplo son necesarios 9 bytes.

Cuadro 57 – ZOI en el ejemplo 1

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es uno
$Zone^0$	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	101000_b	Las regiones de la imagen y los niveles de resolución se especifican en orden
	$Pzoi^1$	$Mzoi^1$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	00_b	Modo rectángulo
			2	00_b	Izoi utiliza un entero de 8 bytes
			1	1_b	Izoi se describe en dos dimensiones
		$Izoi^1$	8	$0110\ 0100_b$	Xul es 100
			8	$0111\ 1000_b$	Yul es 120
			8	$1011\ 0100_b$	Xlr es 180
			8	$1101\ 0010_b$	Ylr es 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	No sigue un segmento alineado por bytes
			1	1_b	El complemento de las zonas especificadas está influido por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	11_b	Modo máx
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^3$	8	$0000\ 0010_b$	Se especifican ≤ 2 niveles de resolución (es decir, > 3 niveles de resolución se especifican en el modo Máx y el cambio de complemento)

6.1.2 Ejemplo 2

En esta subcláusula se muestra un ejemplo en que se ven influidos códigos de bloque cuyo índice de esquina superior izquierda es 5 y el índice de la esquina inferior derecha es 10 en la subbanda 1 con un nivel de resolución 0. En este ejemplo, se necesitan 10 bytes.

Cuadro 58 – ZOI en el ejemplo 2

Parámetro			Tamaño (bits)	Valores (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es uno
$Zone^0$	$DCzoi^1$		1	1_b	Sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001000_b	Se especifican niveles de resolución
	$DCzoi^2$		1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001100_b	Se especifican subbandas y bloques de código
	$Pzoi^3$	$Mzoi^3$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	La zona especificada está influida por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	10_b	Modo índice
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^3$	8	$0000\ 0000_b$	El índice de nivel de resolución es 0
	$Pzoi^9$	$Mzoi^8$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	10_b	Modo índice
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^8$	8	$0000\ 0001_b$	Se especifica de subbanda 1
	$Pzoi^{10}$	$Mzoi^9$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	00_b	Modo rectángulo
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^9$	8	$0000\ 0101_b$	El índice de código para la esquina superior izquierda es 5
			8	$0000\ 1010_b$	El índice de bloque código para la esquina inferior derecha es 10

6.1.3 Ejemplo 3

En esta subcláusula se muestra un ejemplo en que están influidos segmentos de datos de los bytes 10 a 100 y de los bytes 10000 a 12000. En este ejemplo se necesitan 12 bytes.

Cuadro 59 – ZOI en el ejemplo 3

Parámetro			Tamaño (bits)	Valores (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es uno
$Zone^0$	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010000_b	Se especifican las gamas de bytes después del marcador SOD
	$Pzoi^2$	$Mzoi^2$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	1_b	Se especifican múltiples elementos
			2	01_b	Modo gama
			2	01_b	Izoi utiliza un entero de 16 bits
			1	0_b	Izoi se describe en una dimensión
		$Nzoi^2$	8	$0000\ 0010_b$	El número de segmentos de datos es 2
		$Izoi^{21}$	16	$0000\ 0000_b$ $0000\ 1010_b$	El byte de inicio es el 10º (bytes)
			16	$0000\ 0000_b$ $0110\ 0100_b$	El último byte es el 100º (bytes)
		$Izoi^{21}$	16	$0010\ 0111_b$ $0001\ 0000_b$	El byte de inicio es el 10000º (bytes)
			16	$0010\ 1110_b$ $1110\ 0000_b$	El último byte es el 12000º(bytes)

6.1.4 Ejemplo 4

En esta subcláusula se muestra un ejemplo en que está influido un nivel de resolución 0 y el segmento de bytes 10 a 100 corresponde a los datos para el nivel de resolución 0. En este ejemplo se necesitan 10 bytes.

Cuadro 60 – ZOI en el ejemplo 4

Parámetro			Tamaño (bits)	Valores (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es uno
$Zone^0$	DC_{zoi}^1		1	1_b	Sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001000_b	Los niveles de resolución se especifican en orden
	DC_{zoi}^2		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010000_b	Se especifican gamas de bytes
	$Pzoi^1$	$Mzoi^1$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	10_b	Modo índice
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^1$	8	$0000\ 0000_b$	El nivel de resolución es 0
	$Pzoi^2$	$Mzoi^2$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	01_b	Modo gama
			2	01_b	Izoi usa enteros de 16 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^1$	16	$0000\ 0000$ $0000\ 1010_b$	El primer byte es el 10º (bytes)
			16	$0000\ 0000$ $0110\ 0100_b$	El último byte es el 100º(bytes)

6.1.5 Ejemplo 5

En esta subcláusula se muestra un ejemplo en que se influyen más de 3 niveles de resolución en losas cuyo índice de losa superior izquierdo es 0 y el índice de losa inferior derecha es 5, con capas en un número inferior o igual a 5 en losas cuyo índice de losa superior izquierdo es 10 y el índice de losa inferior derecha es 15. En este ejemplo se necesitan 13 bytes.

Cuadro 61 – ZOI en el ejemplo 5

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	2	El número de zonas es 2
Zone[0]	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	01 1000_b	Las losas y los niveles de resolución se especifican en orden
	Pzoi[2]	Mzoi[2]	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	00_b	Modo rectángulo
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		Izoi[2]	8	0000 0000_b	El índice de losa superior izquierda es 0
			8	0000 0101_b	El índice de losa inferior derecha es 5
	Pzoi[3]	Mzoi[3]	1	0_b	No sigue un segmento alineado por bytes
			1	1_b	El complemento de las zonas especificadas está influido por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	11_b	Modo máx
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		Izoi[3]	8	0000 0010_b	Se especifican ≤ 2 niveles de resolución (es decir se especifican > 3 niveles de resolución en modo máx y cambio de complemento)
Zone[1]	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Clases de descripción relacionada con la imagen
			6	010100_b	Las losas y capas se especifican en orden
	Pzoi[2]	Mzoi[2]	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	00_b	Modo rectángulo
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		Izoi[2]	8	0000 1010_b	El índice de losa superior izquierda es 10
			8	0000 1111_b	El índice de losa inferior derecha es 15
	Pzoi[4]	Mzoi[4]	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	11_b	Modo máx
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		Izoi[4]	8	0000 0101_b	Se especifican ≤ 5 capas en modo máx

6.1.6 Ejemplo 6

En esta subcláusula se muestra un ejemplo en que la parte influida es un segmento del encabezamiento del byte 10 a 100. En este ejemplo hacen falta 8 bytes.

Cuadro 62 – ZOI en el ejemplo 6

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es 1
$Zone^0$	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	001000_b	Se especifican gamas de bytes después del marcador SEC
	$Pzoi^3$	$Mzoi^3$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	01_b	Modo gama
			2	01_b	Izoi utiliza un entero de 16 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^3$	16	0000 0000 $0000\ 1010_b$	El primer byte es el 10º (bytes)
			16	0000 0000 $0110\ 0100_b$	El último byte es el 100º (bytes)

6.2 Ejemplos de modelo información de claves

6.2.1 Ejemplo 1

En el cuadro 63 se muestra un ejemplo en que se utiliza una única clave secreta (128 bits) para descriptar un tren codificado. La clave secreta está identificada utilizando una URI y se extrae del servidor de claves a partir de la URI en la fase de descriptación.

Cuadro 63 – Información de claves en el ejemplo 1

Parámetro		Tamaño (bits)	Valor	Significado derivado
LK_{KT}		16	128	La longitud de la clave es 128 bits
KID_{KT}		8	2	Se identifica la URI de clave secreta
G_{KT}	PO	16	$000\ 001\ 010\ 011\ 100\ 0_b$	El orden de procesamiento es losa-resolución-capa-componente-precinto
	GL	8	$0000\ 1001_b$	La unidad de protección es la zona total identificada por la ZOI
V_{KT}	N_V	16 (RBAS)	1	El número de valores en la lista valores, V es 1
	S_V	8 (RBAS)	19	La longitud de la información de claves es 19 bytes
	V1	152	https://server/file	La clave secreta puede extraerse de https://server/file

6.2.2 Ejemplo 2

El cuadro 64 muestra un ejemplo en que se utiliza un certificado X.509 para autenticar un tren codificado, estando el certificado X.509 incorporado en KI_{KT} con un método de codificación DER.

Cuadro 64 – Información de clave en el ejemplo 2

Parámetro			Tamaño (bits)	Valor	Significado derivado
LK_{KT}			16	1024	La longitud de la clave es 1024 bits
KID_{KT}			8	2	Se identifica el certificado X.509
G_{KT}	PO		16	000 001 010 011 100 0_b	El orden de procesamiento es losa-resolución-capa-componente-precinto
	GL		8	0000 1001_b	La unidad de protección es la zona total identificada por la ZOI
V_{KT}	N_V		16 (RBAS)	1	El número de valores de la lista de valores, V es 1
	S_V		8 (RBAS)	Variable	Longitud del certificado X.509
	V1	ER_{KT}	8	1	El certificado X.509 está codificado con el método DER
		$LCER_{KT}$	16	Variable	Longitud de CER_{KT}
		CER_{KT}	Variable	Valor certificado	Está incorporado un certificado con una clave pública de 1024 bits

6.2.3 Ejemplo 3

En el cuadro 65 se muestra una única clave pública utilizada para autenticar un tren codificado, estando la clave pública incorporada en KI_{KT}.

Cuadro 65 – Información de clave en el ejemplo 3

Parámetro		Tamaño (bits)	Valor	Significado derivado
LK_{KT}		16	1024	La longitud de la clave es 1024 bits
KID_{KT}		8	1	Se identifica la clave pública
G_{KT}	PO	16	000 001 010 011 100 0_b	El orden del procesamiento es losa-resolución-capa-componente-precinto
	GL	8	0000 1001_b	La unidad de protección es la zona total identificada por la ZOI
V_{KT}	N_V	16 (RBAS)	1	Número de valores en la lista de valores, V es 1
	S_V	8 (RBAS)	256	La longitud de la clave pública es 256 bytes
	V1	2048	Valor clave pública	La clave pública está incorporada

6.2.4 Ejemplo 4

En el cuadro 66 se muestra la utilización de múltiples claves secretas para descriptar un tren codificado, utilizándose cada una de las claves en capas distintas.

Cuadro 66 – Información de claves en el ejemplo 4

Parámetro		Tamaño (bits)	Valor	Significado derivado
LK_{KT}		16	128	La longitud de la clave es 128 bits
KID_{KT}		8	3	Se identifica la URI de la clave secreta
G_{KT}	PO	16	000 001 010 011 1000_b	El orden de procesamiento es losa-resolución-capa-componente-precinto
	GL	8	0000 0100_b	La unidad de protección es la capa
V_{KT}	N_V	16 (RBAS)	3	El número de valores en la lista de valores, V es 3
	S_V	8 (RBAS)	16	La longitud de cada Vn es 16 bytes
	V1	128	https://server/1	La clave secreta para la primera capa puede extraerse de https://server/1
	V2	128	https://server/2	La clave secreta para la segunda capa puede extraerse de https://server/2
	V3	128	https://server/3	La clave secreta para la tercera capa puede extraerse de https://server/3
	V4	128	https://server/4	La clave secreta para la cuarta capa puede extraerse de https://server/4

6.3 Ejemplos de herramientas JPSEC normativas

En los siguientes ejemplos se indica cómo pueden utilizarse la ZOI y los modelos de claves para proporcionar servicios básicos de seguridad como la criptación y la autenticación en una imagen codificada JPEG 2000.

6.3.1 Ejemplo 1

Una imagen se codifica con JPEG 2000 y tiene tres resoluciones. En este ejemplo, la primera resolución no se cripta para proporcionar la capacidad de vista previa, y la segunda y la tercera resoluciones se criptan con las claves k1 y k2, respectivamente. La imagen original en este caso está codificada con un orden de progresión RLCP, tiene 1 losa, 3 resoluciones, 3 capas, Nc componentes, y Np precintos (el número de componentes y precintos no es importante en este ejemplo específico). La criptación se realiza utilizando una AES en modo CBC sin relleno (utilizando el robo de texto cifrado), utilizando la clave k0 para criptar la resolución 1 y la clave k2 para criptar la resolución 2, y dejando sin criptar la resolución 0.

JPSEC indica al consumidor cómo debe descriptar el tren codificado JPSEC. En primer lugar, se indica el ID de modelo de herramienta del modelo descriptación. Se especifican dos ZOI para la resolución 1 y su correspondiente gama de bytes B0-B1, y para la resolución 2 y su correspondiente gama de bytes, B2-B3. Los parámetros del modelo de descriptación indican que se ha aplicado una criptación AES sin relleno (utilizando el robo de texto cifrado). La información de claves y el hecho de que claves distintas se apliquen a resoluciones distintas se indican gracias a los parámetros de información de claves. En concreto, la granularidad de la clave se especifica como una resolución, de manera que cada resolución tenga una clave distinta, siendo el orden de procesamiento TRLCP. La información de claves de cada resolución figura en la lista de valores de claves. La criptación se realiza en el tren codificado, criptando tanto los encabezamientos de paquetes como los cuerpos de paquetes. La granularidad de la criptación es la resolución, mientras que el procesamiento se realiza en el orden TRLCP, que es el mismo que el del tren codificado original. Puesto que las dos resoluciones se criptan separadamente, es necesario contar con dos vectores de de inicialización (IV) y que éstos estén incluidos en la lista de valores.

Cabe señalar que el texto cifrado del paquete resultante está especificado por el orden de procesamiento y, por consiguiente, es independiente del orden de progresión del tren codificado original, aunque la ubicación de los paquetes criptados en el tren codificado resultante sigue el mismo orden de los paquetes del tren codificado original.

Cuadro 67 – Segmento marcador SEC para el ejemplo 1

Parámetro			Tamaño (bits)	Valores	Significado
SEC			16	0xFF65	Marcador SEC
L_{SEC}			16 (RBAS)	0x82	La longitud del segmento marcador SEC es 130 bytes
Z_{SEC}			8 (RBAS)	0	Índice de este segmento marcador SEC
P_{SEC}	F_{PSEC}		1	0_b	No sigue una estructura FBAS
		F_{INSEC}	1	0_b	No se utiliza INSEC
		$F_{multiSEC}$	1	0_b	Se utiliza un segmento marcador SEC
		F_{mod}	2	00_b	Se han modificado los datos JPEG 2000 originales
		F_{TRLCP}	1	0_b	No se define en P_{SEC} la utilización de la etiqueta TRLCP
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	El número de la herramienta de seguridad es uno
	I_{max}		8 (RBAS)	0000000_b	El índice de ejemplar de herramienta máximo es cero
t			8 (FBAS)	0	Herramienta JPSEC normativa
i			8 (RBAS)	0	Índice de ejemplar de herramienta
ID_T			8	1	Modelo de descriptación
L_{zoi}			16 (RBAS)	0x17	La longitud de la ZOI es 23 bytes
ZOI			184	Véase el cuadro 68	Zona de influencia de esta herramienta
L_{PID}			16 (RBAS)	0x5e	La longitud de P_{ID} es 94 bytes
P_{ID}			752	Véase el cuadro 69	Parámetros para esta tecnología

Cuadro 68 – Ejemplo de ZOI

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	2	El número de zonas es 1
$Zone^0$	DC_{ZOI}^1		1	1_b	Sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001000_b	Se especifica la resolución
	$DCzoi^2$		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010000_b	Se especifican las gamas de bytes después del marcador SOD
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	10_b	Modo índice
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		I_{ZOI}	8	$0000\ 0001_b$	Se especifica la resolución 1
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	01_b	Modo gama
			2	01_b	Izoi utiliza enteros de 16 bits
			1	0_b	Izoi se describe en una dimensión

Cuadro 68 – Ejemplo de ZOI

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
		$Izoi^{21}$	16	0x31CC	El primer byte es el 12 748 (bytes). (B0)
			16	0xA3E8	El último byte es el 41 960 (bytes). (B1)
$Zone^{1}$	$DC_{ZOI}{}^{1}$		1	1_b	Sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001000_b	Se especifica la resolución
	$DCzoi^{2}$		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010000_b	Se especifican gamas de bytes después del marcador SOD
	$Pzoi^{0,1}$	$Mzoi^{1}$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	10_b	Modo índice
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$I_{ZOI}{}^{1}$	8	$0000\ 0010_b$	Se especifica la resolución 2
	$Pzoi^{0,2}$	$Mzoi^{2}$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_{b2}	Se especifica un único elemento
			2	01_b	Modo gama
			2	10_b	Izoi utiliza un entero de 32 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^{2}$	32	0xA3EE	El primer byte es el 41 966 (bytes). (B2)
			32	0x21101	El último byte es el 135 425 (bytes). (B3)

Cuadro 69 – Ejemplo de P_{ID}

Parámetro		Tamaño (bits)	Valores	Significado
T_{ID}		432	Véase el cuadro 70	Modelo de descriptación
PD		8 (FBAS)	0_b	No sigue un segmento alineado por bytes
			0_b	No se utiliza el dominio de píxel
			0_b	No se utiliza el dominio de coeficiente de ondícula
			0_b	No se utiliza el dominio de coeficiente de ondícula cuantizado
			1_b	Se utiliza el dominio de tren codificado
			000_b	Reservado para utilización por parte de la ISO
F_{PD}		8 (FBAS)	0_b	No sigue un byte FBAS
			1_b	Sólo se cripta el cuerpo del paquete
			000000_b	Reservado para utilización por parte de la ISO
G	PO	16	$000\ 001\ 010\ 011\ 100\ 0_b$	El orden de procesamiento es losa-resolución-capa-componente-precinto
	GL	8	$0000\ 0011_b$	La unidad de protección es el nivel de resolución
V	N_V	16 (RBAS)	2	El número de valores en la lista de valores, V, es 2
	S_V	8 (RBAS)	16	La longitud de cada Vn es 16 bytes
	V1	128	IV0	Valor del vector de inicialización para R1
	V2	128	IV1	Valor del vector de inicialización para R2

Cuadro 70 – Ejemplo de modelo de descriptación

Parámetro		Tamaño (bits)	Valor (en orden)	Significado derivado
ME_{decry}		8	0	Ha ocurrido una emulación de marcador
CT_{decry}		16	0001_b	Cifrado de bloque (AES)
CP_{decry}	M_{bc}	6	100000_b	Modo CBC. Los bits no tienen relleno
	P_{bc}	2	00_b	Robo de texto cifrado
	SIZ_{bc}	8	16	Tamaño de bloque (16 bytes, 128 bits)
	KT_{bc}	392	Véase el cuadro 71	Modelo de claves

Cuadro 71 – Ejemplo de modelo de claves

Parámetro		Tamaño (bits)	Valores	Significado derivado
LK_{KT}		16	128	La longitud de la clave es 128 bits
KID_{KT}		8	2	URI para la clave secreta
G_{KT}	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	El orden de procesamiento es losa-resolución-capa-componente-precinto
	GL	8	$0000\ 0011_b$	La unidad de protección es el nivel de resolución
V_{KT}	N_V	32 (RBAS)	2	El número de valores en la lista de valores, V, es 2
	S_V	8 (RBAS)	19	La longitud de cada Vn es 19 bytes
	V1	152	https://server/key1	La clave secreta para el nivel de resolución 1 puede extraerse de https://server/key1
	V2	152	https://server/key2	La clave secreta para el nivel de resolución 2 puede extraerse de https://server/key2

6.3.2 Ejemplo 2

En este caso, la autenticación se aplica a la misma imagen codificada JPEG 2000 que anteriormente. En este ejemplo, se autentican las tres resoluciones y tres capas por resolución, utilizando para la autenticación de cada resolución una clave distinta. Puesto que hay tres resoluciones, hay tres claves, y al haber tres capas por resolución, habrá tres valores MAC por resolución. Así, habrá un total de nueve valores MAC para toda la imagen JPSEC. En concreto:

- la resolución 0 tendrá los valores MAC M0, M1, M2 (uno para cada capa) utilizando la clave0;
- la resolución 1 tendrá los valores MAC M3, M4, M5 (uno para cada capa) utilizando la clave1;
- La resolución 2 tiene los valores MAC M6, M7, M8 (uno para cada capa) utilizando la clave2.

Este ejemplo muestra cómo puede señalarse la autenticación, así como la flexibilidad que proporciona la ZOI y las herramientas de granularidad. Como en el ejemplo anterior, la imagen original está codificada en el orden de progresión de RLCP, tiene una losa, tres resoluciones, tres capas, Nc componentes y Np precintos (el número de componentes y precintos no es importante en este ejemplo concreto). La autenticación se realiza utilizando HMAC con SHA-1.

JPSEC indica cómo el consumidor puede verificar o autenticar el contenido protegido JPSEC. En primer lugar, se indica el ID de modelo de herramienta del modelo de autenticación. A continuación se utiliza la ZOI para indicar que hay tres resoluciones y las gamas de bytes correspondientes a cada resolución. Los parámetros del modelo de autenticación muestran que se utiliza HMAC con SHA-1. El modelo de información de claves ofrece información sobre las claves, incluido el hecho de que la granularidad de claves es la resolución y proporciona información sobre cada una de las tres claves en la lista de valores de clave. El dominio de procesamiento para la autenticación está especificado en el tren codificado, incluidos los encabezamientos de paquetes. La granularidad de herramienta para la autenticación se especifica como la capa, por lo que hay tres MAC para cada resolución, lo que suma un total de nueve valores MAC. La lista de valores contiene los nueve valores MAC. El orden de procesamiento de todo lo anterior se identifica como TRLCP, que es el mismo orden del tren codificado original.

Cabe señalar que la utilización de orden de procesamiento en el campo de granularidad garantiza que los mismos valores MAC darán resultado independientemente del orden de progresión del tren codificado.

Es necesario indicar que, si este ejemplo demuestra la utilización de las MAC, el mismo ejemplo puede utilizarse para mostrar cómo se utilizan múltiples firmas digitales.

Cuadro 72 – Segmento marcador SEC

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
SEC			16	0xFF65	Marcador SEC
L_{SEC}			16	0x0099	Longitud del segmento marcador SEC
Z_{SEC}			8 (RBAS)	0	Índice de este segmento marcador SEC
P_{SEC}	F_{PSEC}		1	0_b	No sigue una estructura FBAS
		F_{INSEC}	1	0_b	No hay un segmento marcador INSEC
		$F_{multiSEC}$	1	0_b	Sólo hay un segmento marcador SEC en este tren codificado
		F_{mod}	1	0_b	No se han modificado los datos JPEG 2000 originales
		F_{TRLCP}	1	0_b	No se utiliza la etiqueta TRLCP
		Padding	3	000_b	No se utiliza la etiqueta TRLCP
	N_{tools}		7	1	Sólo se utiliza una herramienta en este tren codificado
	I_{max}		7	0	El índice de ejemplar de herramienta máximo es 0
$Tool^0$	t		8 (FBAS)	0	Herramienta JPSEC normativa
	i		8 (RBAS)	0	Índice de ejemplar de herramienta
	ID_T		8	2	Esta herramienta normativa utiliza un modelo de autenticación
	L_{ZOI}		16 (RBAS)	0x20	La longitud de ZOI es 32 bytes
	ZOI		256	Cuadro 73	Zona cubierta de la imagen
	L_{PID}		16 (RBAS)	0x6c	La longitud de P_{ID} es 108 bytes
	P_{ID}		928	Cuadro 74	Parámetros de la herramienta JPSEC

Cuadro 73 – Significado de la ZOI

Parámetro			Tamaño(bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es 1
$Zone^0$	DC_{zoi}^1		1	1_b	Sigue un segmento alineado por bytes
			1	0_b	Clase de descripción relacionada con la imagen
			6	001000_b	Se especifican los niveles de resolución en orden
	DC_{zoi}^2		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010000_b	Se especifica la gama de bytes
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	La zona especificada está influida por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	01_b	Modo gama
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^1$	8	0	El comienzo de la gama es 0
			8	2	El final de la gama es 2
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	No sigue un elemento alineado por bytes
			1	0_b	La zona especificada está influida por la herramienta JPSEC
			1	1_b	Se especifican múltiples elementos
			2	01_b	Modo gama
			2	10_b	Izoi utiliza enteros de 32 bits
			1	0_b	Izoi se describe en una dimensión

Cuadro 73 – Significado de la ZOI

Parámetro			Tamaño(bits)	Valor (en orden)	Significado derivado
		N_{ZOI}	8 (RBAS)	3	El número de I_{ZOI} es 3
		$Izoi^1$	32	104	El primer byte es el 104 (bytes)
			32	12762	El último byte es el 12762 (bytes)
		I_{ZOI}^2	32	12768	El primer byte es el 12768 (bytes)
			32	41980	El último byte es el 41980 (bytes)
		I_{ZOI}^3	32	41986	El primer byte es el 41986 (bytes)
			32	135445	El último byte es el 135445 (bytes)

Cuadro 74 – Parámetros de señalización de P_{ID}

Parámetro					Tamaño (bits)	Valor (en orden)	Significado derivado
T_{auth}	M_{auth}				8	0	Método de autenticación: autenticación por número generador
	P_{auth}	M_{HMAC}			8	1	Se utiliza HMAC para la autenticación
		H_{HMAC}			8	1	Se utiliza SHA-1 como función generadora
		KT_{HMAC}	LK_{KT}		16	128	Longitud de la clave en bits
			KID_{KT}		8	3	KI_{KT} contiene la URI de la clave privada
			G_{KT}	PO	16	0 000 001 010 011 100_b	El orden es losa-resolución-capa-componente-precinto
				GL	8	00000011_b	La granularidad de la clave es la resolución
			V_{KT}	N_V	16 (RBAS)	3	Hay tres claves en la lista
				S_V	8 (RBAS)	8	El tamaño de cada clave es 8 bytes
				VL	64	*Key0*	La primera clave es *clave0* para la resolución 0
					64	*Key1*	La segunda clave es *clave1* para la resolución 1
					64	*Key2*	La tercera claves es *clave2* para la resolución 2
		SIZ_{HMAC}			16	20	El tamaño de MAC es 20
PD					8 (FBAS)	0_b	No sigue un segmento alineado por bytes
						0_b	No se utiliza el dominio de píxel
						0_b	No se utiliza el dominio de coeficiente de ondícula
						0_b	No se utiliza el dominio de coeficiente de ondícula cuantizado
						1_b	Se utiliza el dominio de tren codificado
						000_b	Reservado para utilización por parte de la ISO
F_{PD}					8 (FBAS)	0_b	No sigue un byte FBAS
						0_b	Se cripta el encabezamiento de paquete y el cuerpo de paquete
						000000_b	Reservado para la utilización por parte de la ISO
G	PO				16	00000101001 11000_b	El orden es losa-resolución-capa-componente-precinto
	GL				8	00000100_b	La granularidad de la herramienta es la capa

Cuadro 74 – Parámetros de señalización de P_{ID}

Parámetro		Tamaño (bits)	Valor (en orden)	Significado derivado
V	N_V	32 (RBAS)	9	Hay 9 MAC (3 MAC por resolución)
	S_V	8 (RBAS)	20	El tamaño de cada MAC es 20 bytes
	VL	160	*M0*	El primer MAC es *M0*
		160	*M1*	El segundo MAC es *M1*
		160	*M2*	El tercer MAC es *M2*
		160	*M3*	El cuarto MAC es *M3*
		160	*M4*	El quinto MAC es *M4*
		160	*M5*	El sexto MAC es *M5*
		160	*M6*	El séptimo MAC es *M6*
		160	*M7*	El octavo MAC es *M7*
		160	*M8*	El noveno MAC es *M8*

6.4 Ejemplos del campo distorsión

En esta subcláusula se presentan algunos ejemplos sobre la utilización del campo distorsión.

6.4.1 Ejemplo 1

Este ejemplo se basa en el ejemplo 3 de ZOI de 6.1.3 para mostrar cómo pueden asociarse los valores de distorsión con dos segmentos de datos indicados por la ZOI en este ejemplo. Para resumir, el ejemplo 3 de 6.1.3 muestra dos segmentos de datos: (1) bytes 10 a 100, y (2) bytes 10000 a 12000. La asociación de los campos distorsión con estos dos elementos de datos se hace en dos fases. En primer lugar, se indica el campo distorsión DCzoi. En segundo lugar, los valores de distorsión se indican utilizando $Pzoi^2$. Por consiguiente, los únicos cambios que se aportan al ejemplo 3 de ZOI de 6.1.3 es la configuración de los bits del campo distorsión en DCzoi, y la adición de $Pzoi^2$ (las nueve últimas filas del cuadro 75).

Cuadro 75 – Asociación del campo distorsión con dos segmentos de datos (ampliación del ejemplo 3 de ZOI de la subcláusula 6.1.3)

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es 1
$Zone^0$	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	010001_b	Se especifican las gamas de bytes después del marcador SOD y se especifican los campos distorsión
	$Pzoi^2$	$Mzoi^2$	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	1_b	Se especifican múltiples elementos
			2	01_b	Modo gama
			2	01_b	Izoi utiliza un entero de 16 bits
			1	0_b	Izoi se describe en una dimensión
		$Nzoi^2$	8 (RBAS)	2	El número de segmentos de datos es 2
		$Izoi^{2,1}$	16	0000 0000 $0000\ 1010_b$	El primer byte es el 10º (bytes)
			16	0000 0000 $0110\ 0100_b$	El último byte es el 100º (bytes)

Cuadro 75 – Asociación del campo distorsión con dos segmentos de datos (ampliación del ejemplo 3 de ZOI de la subcláusula 6.1.3)

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
		Izoi[2,2]	16	0010 0111 0001 0000_b	El primer byte es el 10 000º (bytes)
			16	0010 1110 1110 0000_b	El último byte es el 12 000º (bytes)
	Pzoi[6]	Mzoi[6]	1	0_b	No sigue un elemento asignado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	1_b	Se especifican múltiples elementos
			2	10_b	Modo índice
			2	00_b	Izoi utiliza 8 bits para representar cada valor de distorsión
			1	0_b	Izoi se describe en una dimensión
		Nzoi[6]	8 (RBAS)	2	El número de segmentos de datos es 2
		Izoi[6,1]	*8*	Valor D1	Valor de distorsión para el primer segmento
		Izoi[6,2]	*8*	Valor D2	Valor de distorsión para el segundo segmento

6.4.2 Ejemplo 2

En este ejemplo se muestra cómo pueden asociarse los valores de distorsión con los paquetes JPEG 2000. DCzoi especifica una gama de cuatro paquetes así como el campo distorsión. Pzoi[1] da la gama de paquetes y Pzoi[2] la distorsión asociada con cada uno de estos paquetes. Cabe indicar que, puesto que Pzoi[1] especifica una gama de longitud 4, y Pzoi[2] especifica cuatro valores, cada elemento de la gama está asociado con un valor, por ejemplo, cada paquete está asociado con una distorsión.

Cuadro 76 – Señalización de una gama de paquetes y distorsión asociada con cada paquete

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8 (RBAS)	1	El número de zonas es 1
Zone[0]	DCzoi		1	0_b	No sigue un segmento alineado por bytes
			1	1_b	Clase de descripción no relacionada con la imagen
			6	100001_b	Se especifican los paquetes y los campos distorsión asociados
	Pzoi[1]	Mzoi[1]	1	0_b	No sigue un segmento alineado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	0_b	Se especifica un único elemento
			2	01_b	Modo gama
			2	00_b	Izoi utiliza enteros de 8 bits
			1	0_b	Izoi se describe en una dimensión
		Nzoi[1]	8 (RBAS)	1	El número de segmentos de datos es 1
		Izoi[11]	8	$0000\ 0000_b$	El primer paquete es el 0
			8	$0000\ 0011_b$	El último paquete es el 3
	Pzoi[6]	Mzoi[6]	1	0_b	No sigue un segmento asignado por bytes
			1	0_b	Las zonas especificadas están influidas por la herramienta JPSEC
			1	1_b	Se especifican múltiples elementos
			2	10_b	Modo índice
			2	00_b	Izoi utiliza 8 bits para representar cada valor de distorsión
			1	0_b	Izoi se describe en una dimensión

Cuadro 76 – Señalización de una gama de paquetes y distorsión asociada con cada paquete

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
		Nzoi[6]	8 (RBAS)	4	El número de segmentos de datos es 4
		Izoi[6,1]	8	Valor D1	Valor de distorsión para el primer paquete
		Izoi[6,2]	8	Valor D2	Valor de distorsión para el segundo paquete
		Izoi[6,3]	8	Valor D3	Valor de distorsión para el tercer paquete
		Izoi[6,4]	8	Valor D4	Valor de distorsión para el cuarto paquete

7 Autoridad de registro JPSEC

7.1 Introducción

El mecanismo de registro JPSEC proporciona una identificación inequívoca de las herramientas de seguridad no normativas que siguen la norma JPSEC y que pueden posteriormente presentarse como herramientas no normativas JPSEC, o convertirse en tales, sumándose a las enumeradas en el anexo B. Este registro lo realiza la autoridad de registro JPSEC, y debe ser conforme a las directivas JTC 1. El registro de estas nuevas herramientas JPSEC está controlado por el proceso que se define en esta subcláusula.

Los solicitantes pueden presentar tecnologías que quieran incluir en la lista de referencia JPSEC. Cabe señalar que la utilización de herramientas JPSEC se especifica con un marcador JPSEC presente en el tren codificado. Cuando una aplicación encuentra un ID JPSEC desconocido, puede recurrir a la autoridad de registro JPSEC y obtener la información allí registrada sobre la herramienta.

7.2 Criterios para poder solicitar el registro

Los solicitantes deberán ser organizaciones reconocidas por los organismos nacionales.

7.3 Solicitud de registro

Las solicitudes para registrar nuevas herramientas JPSEC se publicarán en el sitio web de la autoridad de registro JPSEC.

Este sitio web contendrá los formularios de solicitud de registro, solicitud de actualización, notificación de asignación o actualización, y rechazo de la solicitud.

Todos los formularios deberán incluir:

- el nombre de la organización solicitante;
- la dirección de la organización solicitante;
- el nombre, título, dirección postal/de correo electrónico, número de teléfono/facsímil de la persona de contacto dentro de la organización.

Los formularios de solicitud de registro y solicitud de actualización contarán también con los siguientes datos:

- Nombre de la herramienta JPSEC (obligatorio).
- Tipo de herramienta JPSEC, por ejemplo, firma digital, marca de agua, criptación, aleatorización, generación y gestión de claves, autenticación (facultativo).
- Resumen técnico descriptivo (obligatorio).
- Descripción general de la herramienta (obligatorio).
- Descripción de un ejemplo práctico (facultativo).
- Especificación de la sintaxis de los parámetros, incluidos los valores posibles (facultativo).
- Directrices de utilización óptima (facultativo).
- Información relativa a los derechos de propiedad intelectual, por ejemplo, propietario, detentor de los derechos (facultativo).
- Condiciones de IPR para su utilización (obligatorio).

- Restricciones de utilización, por ejemplo, condiciones de exportación (facultativo).
- Información sobre descarga de las implementaciones (facultativo).
- Comentarios adicionales, motivación, referencias, etc. (facultativo).
- Requisitos de confidencialidad de las entradas de la aplicación seleccionada (facultativo).
- Plazo solicitado para el registro de la herramienta (facultativo).

La autoridad de registro JPSEC proporcionará asimismo material formativo para asistir a los solicitantes en la preparación de las solicitudes.

7.4 Examen de las solicitudes y respuesta

En esta subcláusula se define el proceso que realiza la autoridad de registro JPSEC al examinar las solicitudes para garantizar su exactitud y responder a las mismas.

Se crea un comité técnico de examen que se encarga de las solicitudes. Este comité está compuesto por miembros de la ISO/CEI JTC 1/SC 29/GT 1 y miembros de la autoridad de registro JPSEC. El comité examina las solicitudes en una reunión del GT 1 a más tardar nueve meses después de la presentación de la solicitud.

El comité de examen acepta o rechaza la solicitud de acuerdo con los criterios de rechazo de 7.5.

De ser aceptada, se asigna a la nueva herramienta JPSEC un identificador (ID) durante un periodo determinado de tiempo. La sintaxis de ID será conforme a 5.6.3. El comité de examen aprueba la información de descripción de la herramienta JPSEC de 7.3. Entonces, el ID deberá utilizarse para su señalización en el tren codificado JPSEC.

Una vez examinada y aceptada la solicitud, la autoridad de registro JPSEC notifica al solicitante la respuesta positiva o negativa a su petición de registro. En esta respuesta se incluirá una breve explicación de los resultados del examen técnico y se enviará a los solicitantes a más tardar nueve meses después de la fecha de solicitud.

Puede presentarse apelación a una respuesta negativa si el solicitante cree que se ha cometido un error, o cuando se requiere más información para aclarar problemas o dudas. Si el solicitante pide un examen adicional aparte del proceso que sigue esta autoridad, puede someter su caso a examen al Comité del GT 1 en la siguiente reunión del GT 1. Se le podrá entonces pedir que presente información adicional, según lo determinen expertos que, bajo la autoridad del GT 1, proporcionarán una respuesta definitiva de aceptación o rechazo. Para que el GT 1 examine una solicitud rechazada, los solicitantes deberán volver a presentar la propuesta a través de su organismo nacional, especificando por qué solicitan el examen por parte del GT 1.

7.5 Rechazo de las solicitudes

Los criterios de rechazo en la solicitud son los siguientes:

- el solicitante no está capacitado para presentar la solicitud;
- no se han abonado las tasas correspondientes (de haberlas);
- ya existe un elemento aprobado y registrado con contenido idéntico al de la solicitud;
- la información de la solicitud está incompleta o es incomprensible;
- la justificación para inclusión en el registro no es adecuada; la herramienta JPSEC candidata debe demostrar que proporciona un servicio de seguridad útil y proporcionar ejemplos prácticos, cuando proceda;
- la autoridad considera que la herramienta propuesta no es suficientemente original para poder ser aplicada a un elemento existente aprobado;
- la solicitud contiene errores o no se ajusta a las especificaciones JPSEC normativas o a la norma;
- la descripción técnica no es suficiente;
- las condiciones de confidencialidad no son adecuadas.

7.6 Asignación de identificadores y registro de las definiciones de objeto

El proceso de examen y la sintaxis anterior garantizan que los ID asignados son exclusivos dentro del registro y que no se asigna el mismo ID a otro objeto.

Una vez realizada la asignación, el ID y la información asociada se incluirán en el registro y la autoridad de registro JPSEC informará al solicitante de la asignación en el plazo de nueve meses.

La definición de la herramienta JPSEC se incluirá en el registro en el momento en que se le asigne un ID.

7.6.1 Reutilización de ID

La autoridad de registro podrá reutilizar los identificadores. Por ejemplo, los identificadores que queden disponibles para reutilización una vez hayan expirado o cuando se reclamen o abandonen voluntariamente.

Los propietarios de los ID podrán abandonar voluntariamente su ID mediante una solicitud de actualización.

7.6.2 Reclamación

La autoridad de registro JPSEC podrá reclamar un identificador por motivos técnicos o por utilización incorrecta de la herramienta. En este caso, el propietario del identificador recibirá una notificación de actualización.

7.7 Mantenimiento

A efectos de mantenimiento del registro, la autoridad de registro JPSEC aplicará mecanismos de mantenimiento de la integridad del registro, incluida una copia de seguridad de los archivos.

El propietario de un ID podrá actualizar la información de la herramienta JPSEC que le corresponde mediante una solicitud de actualización.

La autoridad de registro JPSEC dispondrá de mecanismos para mantener la confidencialidad de las entradas, como se hayan presentado en la solicitud.

7.8 Publicación del registro

En términos generales, los intereses de la comunidad de los usuarios de las tecnologías de la información están mejor preservados si la información de registro es pública. En determinados casos, no obstante, puede ser necesaria la confidencialidad de la integridad o parte de los datos atinentes a un registro en concreto, de manera permanente o durante una parte del proceso de registro.

La autoridad de registro JPSEC publicará la información de registro de manera compatible con los requisitos de confidencialidad de las herramientas JPSEC.

En los casos en que sea necesaria la publicación, ésta será obligatoriamente de manera electrónica y en papel. Si la autoridad de registro JPSEC debe ser responsable de la publicación, mantendrá un archivo de distribución preciso de sus publicaciones.

7.9 Requisitos de información de registro

La autoridad de registro JPSEC publicará electrónicamente la lista de herramientas JPSEC no normativas en su registro, así como toda la información asociada con ellas, de manera compatible con los requisitos de confidencialidad de las herramientas JPSEC.

En el registro de cada herramienta JPSEC se incluirá la siguiente información:

- el ID asignado;
- el nombre del solicitante inicial;
- la dirección del solicitante inicial;
- la fecha de la asignación original;
- la fecha de la última transferencia de asignación, de ser posible (actualizable);
- el nombre del propietario actual (actualizable);
- la dirección del propietario actual (actualizable);
- el nombre, título, dirección postal/correo electrónico, número de teléfono/facsímil de la persona de contacto dentro de la organización (actualizable);
- la fecha de la última actualización (actualizable).

También contendrá información presentada por el solicitante en la herramienta JPSEC, como se especifica en 7.3, así como información sobre la aprobación.

Anexo A

Directrices y casos prácticos

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

A.1 Una clase de solicitudes JPSEC

A.1.1 Introducción

En esta subcláusula se obtiene una descripción conceptual de cómo puede implementarse una clase de aplicaciones JPSEC. Esta clase de aplicación ejemplifica casos de distribución de imagen JPEG 2000 seguras. En las siguientes subcláusulas se ofrece un panorama general de una aplicación JPSEC conceptual que incluye a las entidades JPSEC y la información que se comunica entre ellas. Esta descripción es conceptual y no pretende definir una implementación concreta ni especificar requisitos para su implementación. Las aplicaciones específicas podrán incluir entidades identificadas por la siguiente descripción.

A.1.2 Exposición de una distribución de imagen JPEG 2000 segura

En la figura A.1 se muestra el esquema de una clase de aplicación JPSEC de distribución de imagen JPEG 2000 segura. En este caso, la aplicación JPSEC deberá proporcionar diversos servicios de seguridad para JPEG 2000, por ejemplo, confidencialidad en el intercambio de imágenes, autenticación del origen y el contenido de la imagen.

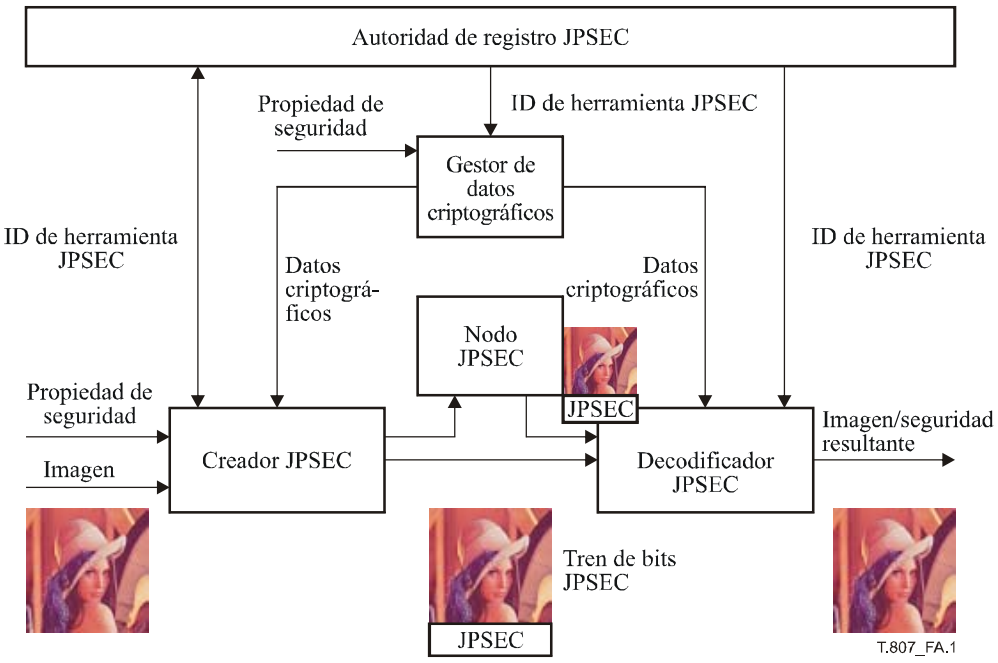


Figura A.1 – Esquema de una aplicación de distribución de imagen segura JPEG 2000

En la aplicación de distribución de imagen JPEG 2000 segura se pueden identificar los siguientes pasos:

Paso 1: El creador JPSEC crea un tren codificado JPSEC.

Paso 2: El tren codificado JPSEC se distribuye a través de un nodo o varios nodos JPSEC.

Paso 3: El consumidor recibe y consume el tren codificado JPSEC.

Paso 1: Creación de un tren codificado JPSEC

El creador es responsable de la creación de un tren codificado JPEG 2000 seguro. Este tren codificado puede crearse a partir de datos de un mapa de bits o a partir de datos comprimidos JPEG 2000. El creador JPSEC aplica diversas técnicas de seguridad, como la criptación, la generación de firmas y la generación ICV (valor de verificación de integridad) a unos datos de imagen determinados.

Para asegurar los datos de imagen, el creador define qué propiedad de parámetros de seguridad se asocian con la imagen. La "propiedad parámetros de seguridad" tiene los siguientes atributos:

- Zona de influencia (zona de cobertura de cada método de protección).
- Dominio de procesamiento (dominio que ha de ser procesado por cada método de protección).
- Granularidad (unidad de cada método de protección).
- Identificación de la herramienta JPSEC (algoritmo criptográfico aplicado y parámetros correspondientes).

Paso 2: Entrega del tren codificado JPSEC

Un tren codificado JPSEC puede transferirse a un consumidor JPSEC directamente o a través de una red o un medio (como un CD-ROM). También puede transferirse a través de un nodo JPSEC que puede aplicar varios tipos de procesamiento adicional, como la transcodificación, al tren codificado JPSEC.

Cuando así lo requieran los métodos de la herramienta de seguridad JPSEC del parámetro de propiedad de seguridad del tren codificado JPSEC (por ejemplo, para la criptación o la autenticación), el creador JPSEC distribuirá al consumidor JPSEC los datos criptográficos correspondientes a través de un canal independiente (secreto). Estos datos, como pueden ser las claves o la firma digital, pueden estar gestionados manual o automáticamente por un gestor de datos criptográficos.

Paso 3: Consumo del tren codificado JPSEC

El tren codificado JPSEC se somete a un proceso de consumo de acuerdo con la aplicación de la propiedad parámetros de seguridad. Esto implica la aplicación de técnicas de seguridad adecuadas, como la descriptación, la autenticación y la verificación de la integridad. Además, para cada método de seguridad de la herramienta JPSEC, el creador y el consumidor JPSEC podrán utilizar diversos tipos de datos criptográficos.

El consumidor JPSEC recibe como resultado unos datos de imagen descriptada y/o un servicio de seguridad, como la verificación.

El creador JPSEC, el consumidor JPSEC y el gestor de datos criptográficos pueden recurrir a la autoridad de registro JPSEC para obtener las instrucciones de procesamiento necesarias para un ID de herramienta JPSEC específica.

En las siguientes subcláusulas pueden encontrarse más detalles sobre las entidades JPSEC conceptuales correspondientes a un servicio JPSEC. En la figura A.2 se muestra la leyenda que se utiliza.

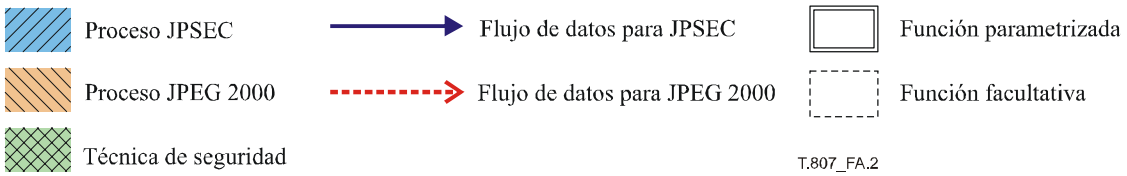


Figura A.2 – Descripción de la leyenda

- **Proceso JPSEC**: Proceso que utiliza las herramientas definidas en la presente Recomendación | Norma Internacional.
- **Proceso JPEG 2000**: Proceso definido por la Rec. UIT-T T.800 | ISO/CEI 15444-1 (JPEG 2000 Parte 1).
- **Técnica de seguridad**: Técnica de seguridad conocida definida por la presente Recomendación | Norma Internacional o por otra norma o documento.
- **Flujo de datos JPSEC**: Flujo de datos que comunica información definida en la presente Recomendación | Norma Internacional. La línea punteada indica que es opcional.
- **Flujo de datos JPEG 2000**: Flujo de datos definido en la Rec. UIT-T T.800 | ISO/CEI 15444-1 (JPEG 2000 Parte 1).
- **Función parametrizada**: Función que tiene diversas funciones alternativas que puede seleccionar una aplicación.
- **Función facultativa**: Función que puede aplicarse facultativamente a una aplicación JPSEC.

A.1.3 Procedimiento de criptación y descriptación

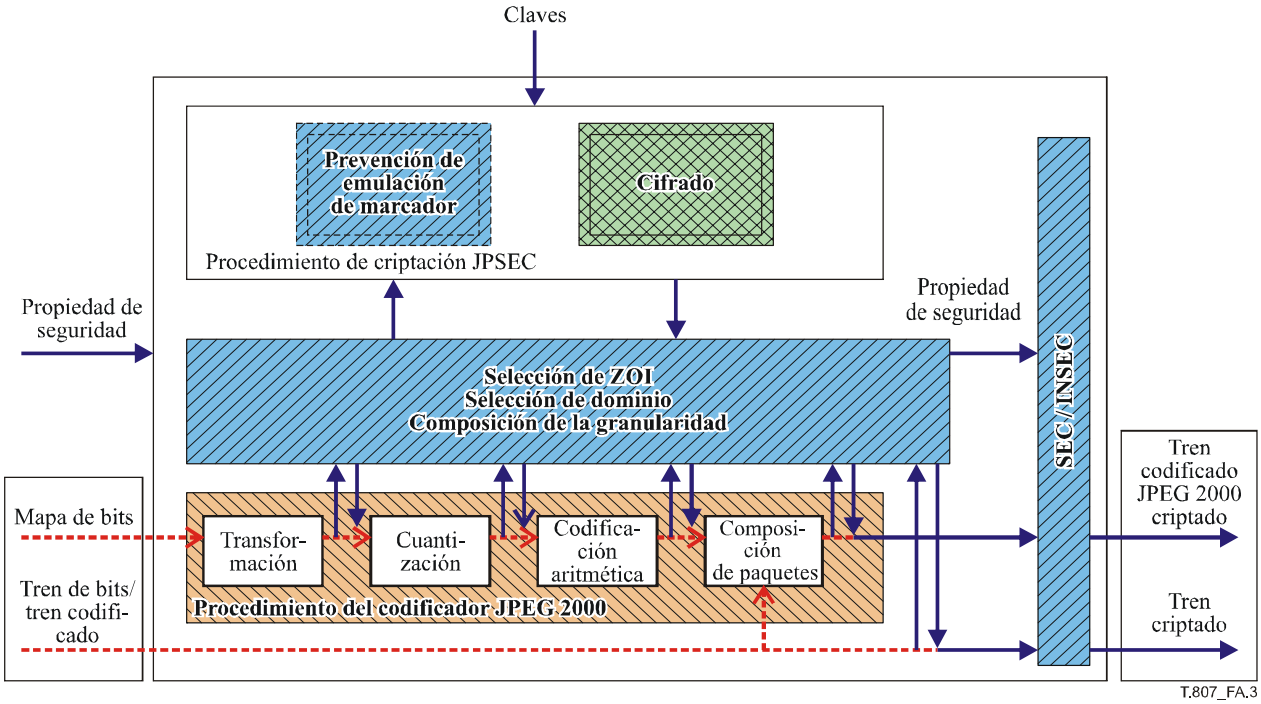


Figura A.3 – Procedimiento de criptación

En la figura A.3 se muestra un esquema de procedimiento de criptación para un creador JPSEC. Este procedimiento incluye los siguientes procesos:

- extracción de datos de acuerdo con el dominio de procesamiento especificado;
- selección de una porción de los datos extraídos de acuerdo con la zona de influencia especificada (es decir, criptación parcial);
- criptación de los datos seleccionados utilizando una técnica de seguridad especificada. Además, es posible criptar datos en una unidad basada en la granularidad. En este caso, pueden utilizarse claves distintas para unidades diferentes;
- sustitución de los datos de texto simple por datos criptados;
- (facultativo) aplicación de un mecanismo de prevención de emulador de marcador;
- composición de la propiedad de parámetro de seguridad en el segmento marcador SEC y/o INSEC.

Cabe señalar que, en general, el procedimiento de criptación JPSEC genera un tren codificado JPSEC que no es compatible con versiones anteriores de JPEG 2000 Parte 1. Los datos de imagen habrán de pasar a un decodificador compatible con la Parte 1 una vez adecuadamente descriptados. Es posible aplicar un mecanismo de prevención de emulación de marcador para evitar la emulación del segmento marcador dentro del tren codificado criptado.

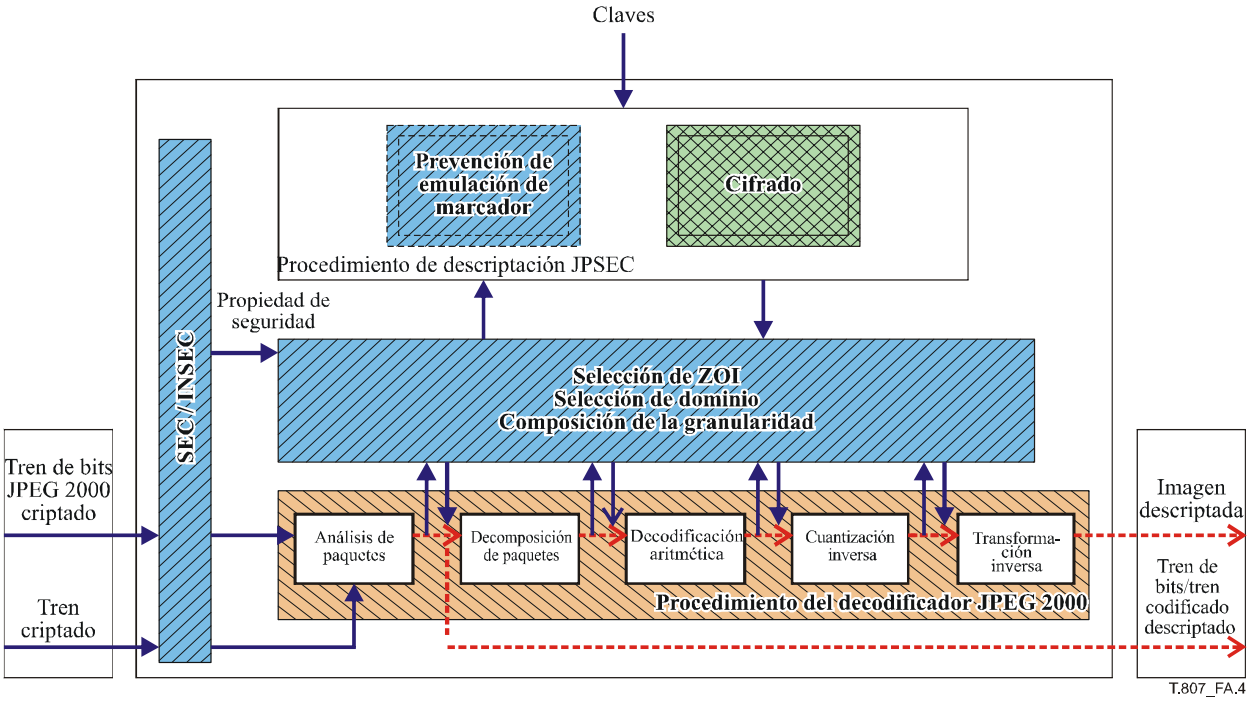


Figura A.4 – Procedimiento de descriptación

En la figura A.4 se muestra un esquema de procedimiento de descriptación para el consumidor JPSEC. Este procedimiento incluye los siguientes procesos:

- análisis sintáctico de la propiedad de parámetros de seguridad en el segmento marcador SEC y/o INSEC;
- extracción de datos de acuerdo con el dominio de procesamiento indicado;
- selección de una porción de los datos extraídos de acuerdo con las claves que han de mantenerse (es decir, descriptación parcial);
- descriptación de los datos seleccionados utilizando la técnica de seguridad indicada. Además, es posible descriptar datos en una unidad de acuerdo con la granularidad;
- sustitución de los datos criptados por datos descriptados;
- aplicación de un mecanismo de prevención de emulación de marcador, si se ha aplicado en el proceso de criptación.

A.1.4 Procedimiento de generación y autenticación de firmas

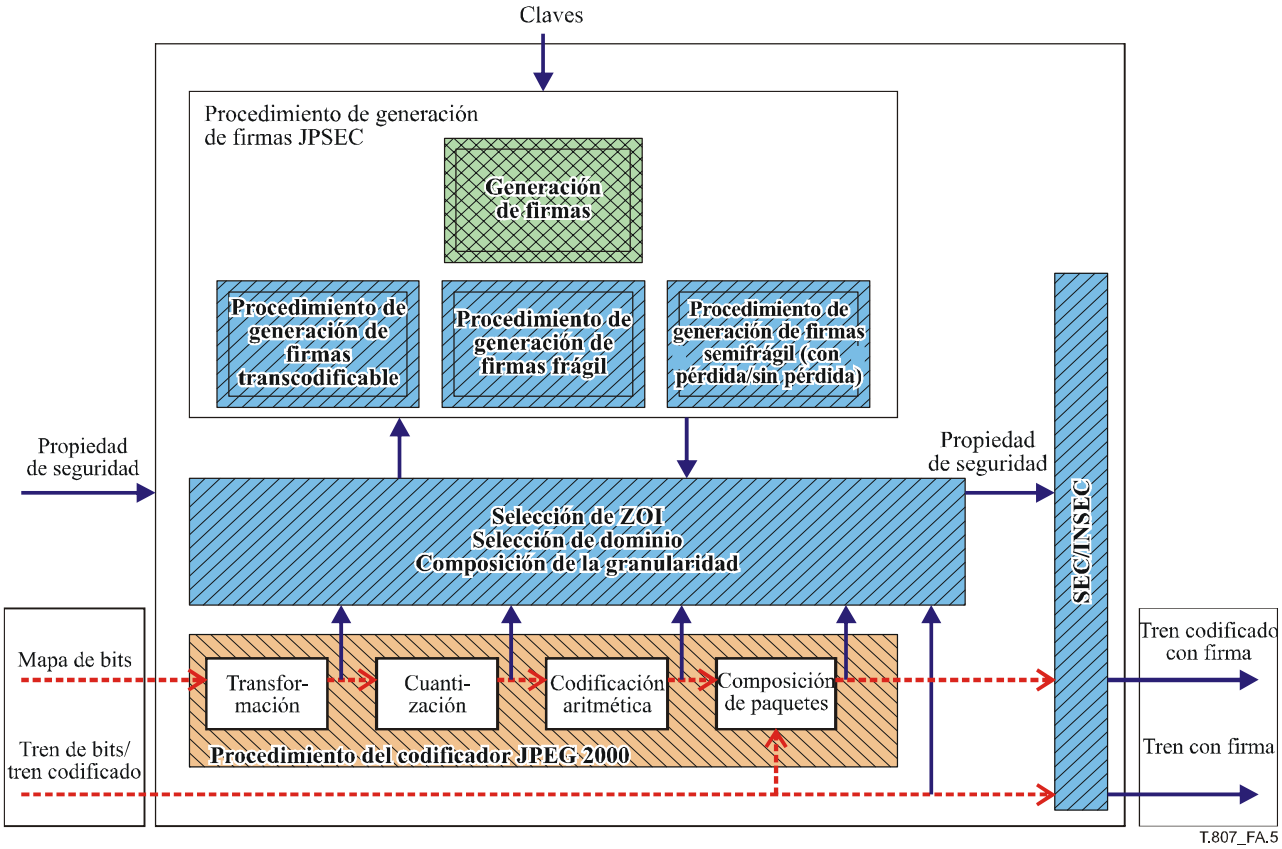


Figura A.5 – Procedimiento de generación de firmas

En la figura A.5 se muestra un esquema de procedimiento de generación de firmas para el creador JPSEC. Este procedimiento incluye los siguientes procesos:

- extracción de datos de acuerdo con el dominio de procesamiento especificado;
- selección de una porción de datos extraídos de acuerdo con la zona de influencia especificada (es decir, firma parcial);
- cálculo de firmas digitales correspondientes a los datos seleccionados utilizando la técnica de seguridad especificada. Además, es posible generar firmas digitales en una unidad basada en la granularidad;
- composición de la propiedad de parámetro de seguridad, incluidas las firmas digitales calculadas, en el segmento marcador SEC y/o INSEC.

Cabe señalar que, en JPSEC, se definen tres modos de autenticación: "frágil", "semifrágil (con perdida/sin pérdida)" y "transcodificable". El modo de autenticación "frágil" puede detectar cualquier modificación de un bit en un tren codificado, mientras que el modo de autenticación "semifrágil" puede detectar cualquier modificación intencional, pero soportar una distorsión incidental hasta determinado punto. Además, el modo de autenticación "transcodificable" puede verificar la parte fuente del tren codificado.

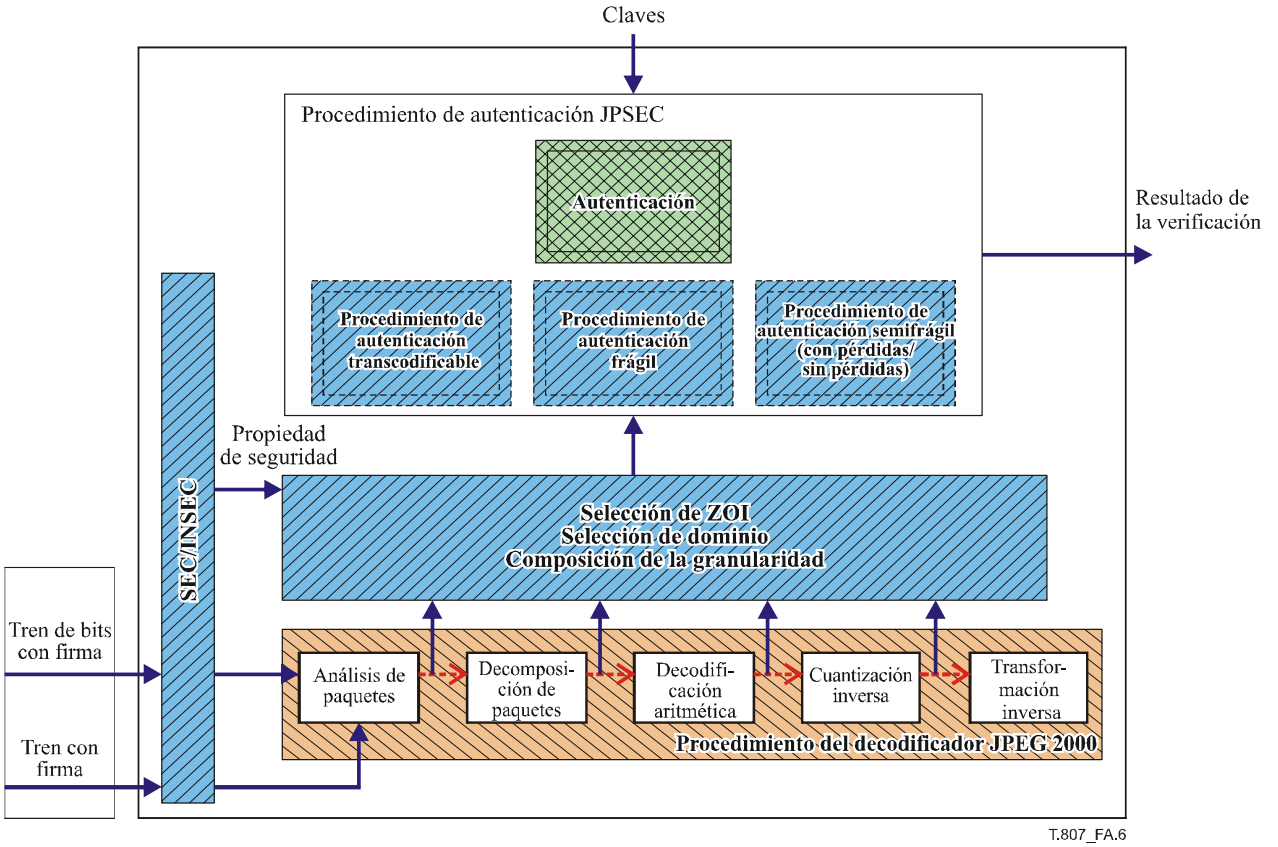


Figura A.6 – Procedimiento de autenticación

En la figura A.6 se muestra un ejemplo de procedimiento de autenticación para el consumidor JPSEC. Este procedimiento incluye los siguientes procesos:

– extracción de datos en el dominio de procesamiento indicado;

– selección de una porción de los datos extraídos de acuerdo con la zona de influencia indicada;

– verificación de los datos seleccionados utilizando la técnica de seguridad indicada. Además, es posible verificar los datos seleccionados en una unidad basada en la granularidad.

A.1.5 Generación de ICV (valor de verificación de integridad) y procedimiento de verificación de integridad

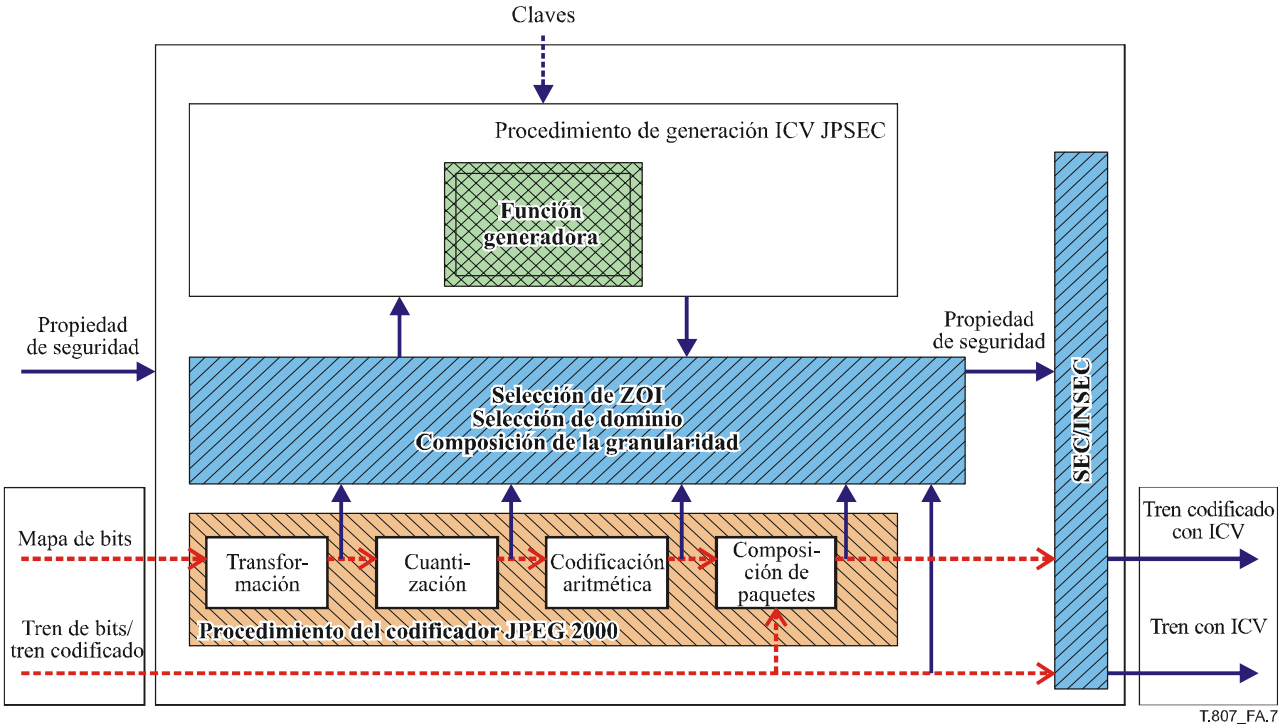


Figura A.7 – Procedimiento de generación ICV (valor de verificación de integridad)

En la figura A.7 se muestra un ejemplo de procedimiento de generación ICV para un creador JPSEC. Este procedimiento incluye los siguientes procesos:

- extracción de datos en el dominio de procesamiento especificado;
- selección de una porción de los datos extraídos de acuerdo con la zona de influencia especificada;
- cálculo de ICV correspondientes a los datos seleccionados utilizando la técnica de seguridad especificada. Además, es posible generar ICV en una unidad basada en la granularidad;
- composición de la propiedad de parámetro de seguridad, incluido los ICV, calculados en el segmento marcador SEC y/o INSEC.

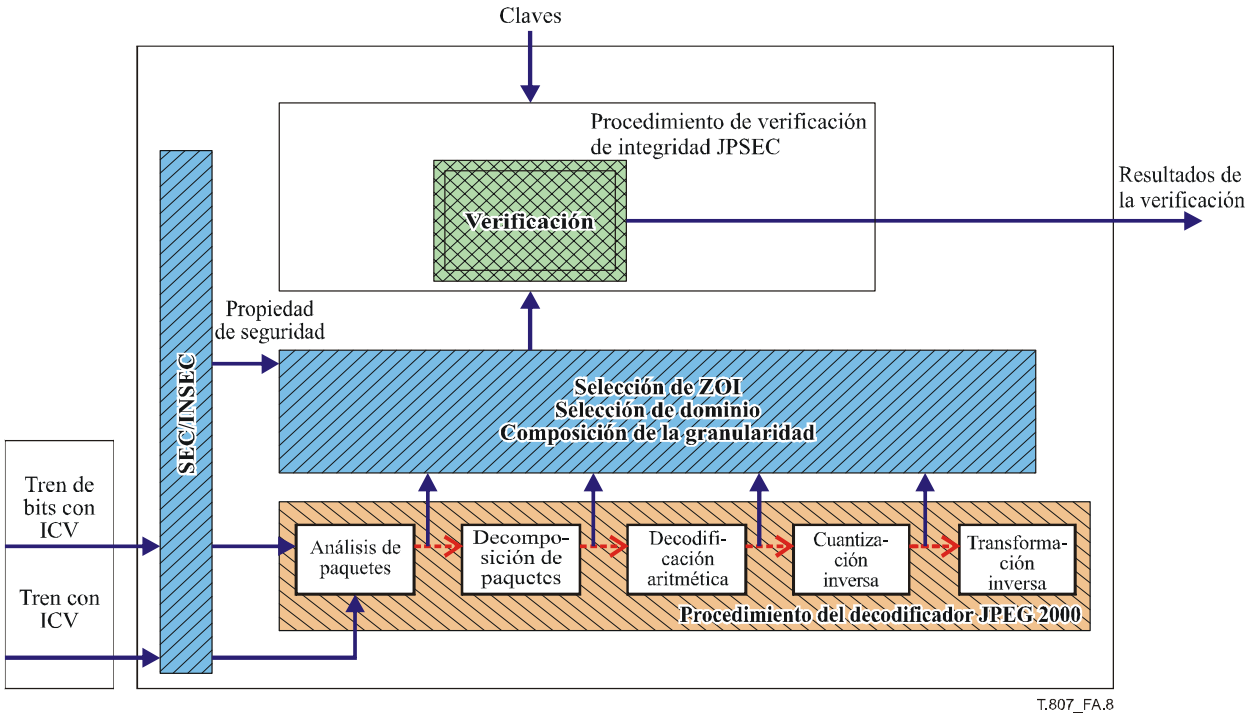


Figura A.8 – Procedimiento de verificación de integridad

En la figura A.8 se muestra un ejemplo de procedimiento de verificación de la integridad para un consumidor JPSEC. Este procedimiento incluye los siguientes procesos:

- extracción de datos de acuerdo con el dominio de procesamiento indicado;
- selección de una porción de los datos extraídos de acuerdo con la zona de influencia indicada;
- verificación de los datos seleccionados utilizando una técnica de seguridad indicada. Además, es posible verificar los datos seleccionados en una unidad basada en la granularidad.

Anexo B

Ejemplos de tecnología

(El presente anexo es parte integrante de esta Recomendación | Norma Internacional)

B.1 Introducción

La sintaxis JPSEC permite aplicar a las imágenes JPEG 2000 herramientas de seguridad normativas y no normativas. En la presente subcláusula se describen 10 ejemplos de tecnología mediante los que se presentan diferentes usos de JPSEC. Estos ejemplos son estrictamente ilustrativos y no forman parte de la norma JPSEC, aunque no obstante dan una idea de la flexibilidad de la norma.

Los ejemplos de tecnología son los siguientes:

- Plan de control de acceso flexible a JPEG 2000.
- Marco de autenticación unificada para imágenes JPEG 2000.
- Método sencillo de criptación basado en paquetes para trenes codificados JPEG 2000.
- Herramienta de criptación para el control de acceso al JPEG 2000.
- Herramienta de generación de claves para el control de acceso al JPEG 2000.
- Aleatorización en los dominios de ondícula y de tren de bits para el control de acceso condicional.
- Acceso progresivo al tren codificado JPEG 2000.
- Autenticación con capacidad evolutiva de trenes codificados JPEG 2000.
- Sistema de control de acceso y confidencialidad de los datos JPEG 2000 basado en la división y compactación de datos.
- Transmisión en secuencias con capacidad evolutiva y transcodificación protegida.

B.2 Plan de control de acceso flexible a trenes codificados JPEG 2000

B.2.1 Servicio de seguridad

El plan de control de acceso permite reconstruir trenes codificados JPEG 2000 conforme a una combinación de resoluciones, capas de calidad, losas y precintos.

B.2.2 Aplicación típica

Sirve para proteger el contenido distribuido por diversos medios, por ejemplo Internet, televisión digital por cable, radiodifusión por satélite y CD-ROM. Por regla general, la tecnología puede aplicarse a las aplicaciones en las que el tren codificado se cripta una sola vez en el lado del editor y en el lado usuario se descripta el tren codificado protegido de diversas maneras según los privilegios de que goce el usuario.

B.2.3 Motivos

En el modelo superdistribución, el editor distribuye libremente el contenido protegido y protege las claves de seguridad de contenido. El usuario que desee acceder a partes del tren codificado debe solicitarlo al servidor de claves. Por su parte, el servidor de clave responde con las correspondientes claves de descriptación en función de los derechos de usuario. En definitiva, el usuario accede a las subimágenes autorizadas.

B.2.4 Descripción técnica

El editor genera el tren codificado JPEG 2000 protegido mediante la criptación de cada paquete. El núcleo de la tecnología consiste en gestionar el árbol de claves que se construye en cualquier orden de losas, componentes, resoluciones, capas, prerecintos e incluso bloques de código. Para describir fácilmente la tecnología, se toma como hipótesis que el orden del árbol de claves es RLCP (resolución-capa-componente-precinto) y que cada resolución tiene el mismo número de prerecintos. A continuación, dada una función generadora unidireccional h(.), se supone que el tren codificado de una imagen JPEG 2000 consta de n_T losas, n_C componentes, n_L capas, n_R niveles de resolución por componente losa, n_P prerecintos por resolución. Sea K la clave maestra del tren codificado JPEG 2000, el árbol de claves se construye del modo siguiente:

1) Se genera la clave $k^t = h(K\,|"T"|t)$, para cada losa $t = 0, 1, ..., n_T - 1$, siendo "|" el símbolo de concatenación y *"T"* el código ASCII de la letra *T*.

2) Se genera la clave $k^r = h(k^{r+1})$, para cada $r = n_R - 2, ..., 1, 0$, siendo $k^{n_R-1} = h(k^t\,|"R")$ y "*R*" el código ASCII de la letra *R*.

3) Se calcula la clave $k^{rl} = h(k^{r(l+1)})$, para cada $r = n_R - 1, ..., 1, 0$, $l = n_L - 2, ..., 1, 0$, siendo $k^{r(n_L-1)} = h(k^r|"L")$ y siendo "*L*" el código ASCII de la letra *L*.

4) Se calcula la clave $k^{rlc} = h(k^{rl}\,|"C"|c)$, para cada $r = n_R - 1, ..., 1, 0$, $l = n_L - 1, ..., 1, 0$, $c = 0, 1, ..., n_C - 1$, siendo "*C*" el código ASCII de la letra *C* y *c* el índice de este componente.

5) Se generan las claves $k^{rlcp} = h(k^{rlc}\,|"P"|p)$, para cada $r = n_R - 1, ..., 1, 0$, $l = n_L - 1, ..., 1, 0$, $c = 0, 1, ..., n_C - 1$, $p = 0, 1, ..., n_R - 1$, siendo "*P*" el código ASCII de la letra *P* y *p* el índice de este precinto.

El tren codificado protegido se genera mediante la criptación del cuerpo de cada paquete con su correspondiente clave (una rama del árbol de claves).

Para reconstruir una subimagen a partir del tren codificado protegido, el usuario obtiene las correspondientes claves de acceso (por ejemplo, a partir de un servidor de claves). Mediante estas claves de acceso se puede extraer exactamente las ramas del árbol de claves correspondientes a los paquetes de la subimagen del caso. El proceso de reconstrucción de claves es similar al de generación del árbol de claves. Se utilizan las ramas para descriptar los paquetes correspondientes.

B.2.5 Sintaxis del tren codificado

En el cuadro B.1 se ilustra la estructura de un segmento SEC. El campo *ZOI* indica los parámetros concedidos, el campo P_{ID} indica los parámetros del método de protección para este plan de control de acceso. El campo PM_{ID} está siempre puesto a 1 para notificar que se utiliza la plantilla de descriptación. El campo TP_{ID} indica los parámetros adicionales para este plan de control de acceso. *KTO* corresponde al orden de generación del árbol de claves. El campo L_{aki} indica la longitud de la información de la clave de acceso.

Cuadro B.1 – Ejemplo de parámetros para este plan

t	i	ID_{RA}	L_{ZOI}	ZOI	L_{PID}	P_{ID}

Parámetro		Tamaño (bits)	Valores	Descripción
t		8 (FBAS)	1	Mecanismo de protección de la autoridad de registro
i		8 (RBAS)	*Valor del ejemplar*	Identificador del ejemplar de mecanismo
ID_{RA}	$ID_{RA,id}$	32	*Valor ID de la herramienta*	ID registrado
	$ID_{RA,nsl}$	8 (RBAS)	21	Longitud del $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$	168	*Namespace*	Espacio de nombres del RA en el que se registró este mecanismo
L_{ZOI}		16 (RBAS)	$[2 ... 2^{16} - 1]$	Longitud de ZOI
ZOI		Variable	Véase 5.7	Zona de influencia de este plan
L_{PID}		16 (RBAS)	$[2 ... 2^{16} - 1]$	Longitud de $L_{PID} + P_{ID}$
P_{ID}		Variable	Véase el cuadro B.2	Parámetros de este plan

Cuadro B.2 – P_{ID}

$PM_{ID} = 1$	T_{decry}	TP_{ID}

Parámetro	Tamaño (bits)	Valores	Descripción
$ID_T = 1$	8	Siempre puesto a 1	Etiqueta de la plantilla de descriptación
T_{decry}	Variable	Valores de la plantilla de descriptación	Plantilla de descriptación
TP_{ID}	Variable	Véase el cuadro B.3	Información adicional de este plan

Cuadro B.3 – TP_{ID}

KTO	L_{aki}	AK_{Info}

Parámetro	Tamaño (bits)	Valores	Descripción
KTO	8	0 ... (2^8 – 1)	Orden del tren de claves, puede ser diferente del orden de progresión del tren codificado, por ejemplo, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL otros: Reservado
L_{aki}	16	0 ... (2^{16} – 1)	Longitud de la información de la clave de acceso, si L_{aki} = 0, el campo AK_{Info} no estará presente
AK_{Info}	Variable	Véase el cuadro B.4	Información sobre la clave de acceso (por ejemplo longitud de la clave, número de claves)

Cuadro B.4 – AK_{info}

L_{uk}	UK	E_{ak}	N_{ak}	AK

Parámetro	Tamaño (bits)	Valores	Descripción
L_{uk}	16	0 ... (2^{16} – 1)	Longitud de la clave de usuario
UK	L_{uk}	NaN	Información de la clave de usuario
E_{ak}	16	Véase el cuadro 24	Clave descifrada utilizada para criptar las claves de acceso
N_{ak}	16	0 ... (2^{16} – 1)	Número de claves de acceso
AK	N_{ak} * K_{bc}	NaN	Claves de acceso

B.2.6 Conclusión

Esta tecnología permite al editor proteger el tren codificado JPEG 2000 mediante una clave maestra. El tren codificado protegido puede distribuirse a varios usuarios, pero las claves de los paquetes se mantienen secretas. El servidor de claves genera diferentes claves de acceso para los usuarios en función de sus prioridades. El usuario genera las claves de paquetes concedidas a partir de claves de acceso y obtiene diferentes imágenes autorizadas. Es decir, la tecnología se conoce con el muy apropiado nombre "*se cripta una sola vez, se accede de diversas maneras*".

B.3 Marco de autenticación unificado para imágenes JPEG 2000

B.3.1 Descripción de procedimiento

Esta herramienta JPSEC proporciona los siguientes servicios JPSEC: verificación de la integridad de los datos/contenido de la imagen y autenticación del origen, es decir, autenticación frágil/semifrágil para imágenes JPEG 2000 basadas en planes con firma digital.

Dado que esta herramienta soporta la autenticación frágil y semifrágil, puede utilizarse en diversas aplicaciones, en particular la distribución de imágenes, la transmisión en secuencias de imágenes, en imágenes médicas y militares, la aplicación de la ley, el comercio electrónico y el cibergobierno.

En entornos ubicuos, las imágenes pueden experimentar diversos tipos de distorsiones imprevistas como la transcodificación y la conversión de formato. Las técnicas de autenticación tradicionales basadas en la criptografía protegen las imágenes JPEG 2000 a nivel de integridad de datos, por lo que no pueden aplicarse estos tipos de distorsiones que preservan el contenido. Por consiguiente, para proteger las imágenes JPEG 2000 a nivel de contenido de la imagen es necesario utilizar técnicas de autenticación semifrágil. Esta herramienta unifica la autenticación del contenido y datos de la imagen y presenta un nuevo concepto denominado velocidad binaria mínima de autenticación (LABR). Es decir, si la imagen está transcodificada a una velocidad binaria no inferior a la LABR, se considera auténtica, de lo contrario no se considera auténtica. La autenticación puede ser frágil o semifrágil. En esta última, la herramienta es capaz de identificar el lugar en el que se ha producido la alteración cuando la imagen se considera no auténtica.

B.3.2 Descripción técnica

Para ofrecer la autenticación frágil y semifrágil, en esta herramienta informativa de JPSEC se han aplicado un conjunto de técnicas, a saber, la selección de funciones, la firma digital, la ocultación de datos con pérdidas y sin pérdidas, y ECC (códigos de corrección de errores). En función de la LABR identificada por los usuarios, se seleccionan las correspondientes funciones de acuerdo con el análisis aplicado a la estructura JPEG 2000 y luego se genera la firma digital. En el caso de la autenticación semifrágil, se utiliza ECC para mejorar la robustez. Los bits de verificación de paridad (PCB) se incorporan en los mensajes en la forma de una filigrana de modo que puedan identificarse las posiciones que han sido atacadas. La integración de los datos puede llevarse a cabo de dos maneras diferentes, esto es, con pérdidas y sin pérdidas. En el caso de la ocultación de datos con pérdidas la imagen original no puede reconstruirse después de haber ocultado los datos. En cambio, en el caso de ocultación de datos sin pérdida la imagen se modifica de manera reversible, es decir puede reconstruirse la imagen original si la imagen marcada no se ha alterado. La autenticación semifrágil sin pérdidas resulta muy útil para JPEG 2000 dado que la norma soporta la compresión con pérdidas a sin pérdidas. Resulta particularmente útil para aplicaciones de imágenes médicas e imágenes distantes, en las que el requisito sin pérdidas es esencial.

Así como la velocidad binaria de compresión de imágenes se utiliza para controlar y caracterizar el grado de compresión, el parámetro LABR (velocidad binaria mínima de autenticación) se utiliza para controlar cuantitativamente el grado de protección. Por ejemplo, cuando una imagen JPEG 2000 se protege con una LABR de 2 bpp (bits per píxel), el sistema propuesto considera auténtica toda versión transcodificada de la imagen siempre que la velocidad binaria después de la transcodificación sea mayor o igual a 2 bpp.

La figura B.1 ilustra cómo utilizar la herramienta para proteger imágenes.

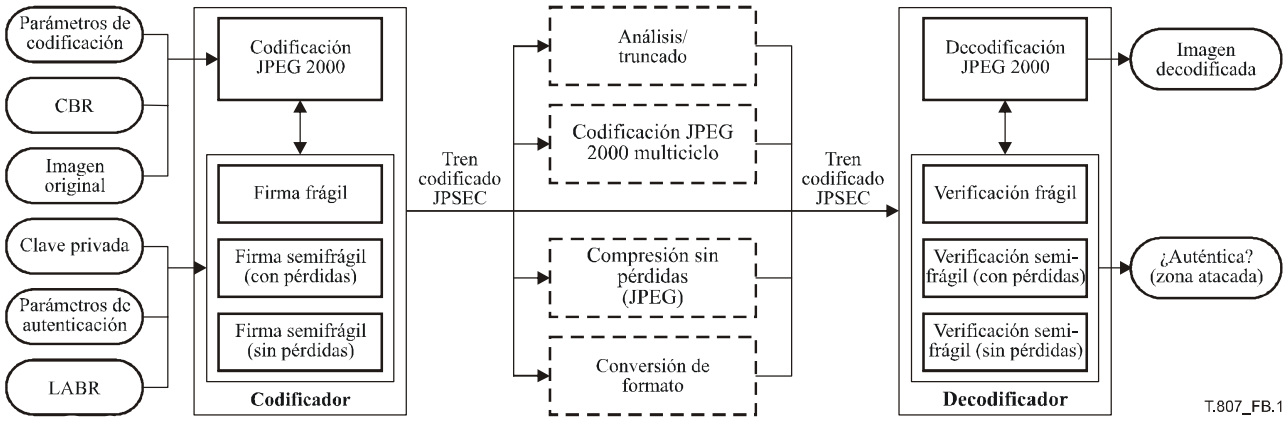


Figura B.1 – Protección de la imagen utilizando el marco de autenticación unificado de JPEG 2000

La sintaxis de señalización que se utiliza en esta herramienta depende del método de autenticación seleccionado. En el caso de autenticación frágil se utiliza la sintaxis de herramienta normativa JPSEC, definida en 5.8.3. Para la autenticación semifrágil se utiliza la sintaxis de herramienta normativa JPSEC, que se muestra en el cuadro B5. Además, F_{INSEC} debe ponerse a 0 dado que esta herramienta no utiliza el marcador ISENC, y F_{mod} debe ponerse a 1 puesto que el tren codificado resultante de esta herramienta JPSEC sigue siendo coherente con la JPEG 2000 Parte 1.

Cuadro B.5 – Sintaxis para la autenticación semifrágil

Parámetro				Tamaño (bits)	Valor	Significado derivado
t				8 (FBAS)	1	Se utiliza una sintaxis no normativa para la herramienta
i				8 (RBAS)	0 ... (2^7 – 1)	Índice del ejemplar de herramienta
ID_{RA}	$ID_{RA,id}$			32	0 ... (2^{32} – 1)	Número de ID que asignará la RA
	$ID_{RA,nsl}$			8 (RBAS)	21	Longitud de $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$			168	*namespace*	Espacio de nombres de la RA en la que se registra la herramienta
L_{ZOI}				16 (RBAS)	0 ... (2^{16} – 1)	Longitud de ZOI
ZOI				Variable	*Valores ZOI*	Zona abarcada en la imagen protegida mediante la herramienta
L_{PID}				16 (RBAS)	0 ... (2^{16} – 1)	Longitud de P_{ID} y L_{PID} en bytes
P_{ID}	ID_T			8	2	Se utiliza una plantilla de autenticación, definida en el cuadro 21
	T_{auth}	M_{auth}		8	2	Se utilizan métodos de firma digital, definidos en el cuadro 34
		P_{auth}	M_{DS}	8	Véase el cuadro 41	Se utiliza un algoritmo de firma digital, por ejemplo DSA o RSA
			H_{DS}	8	Véase el cuadro 37	Se utiliza la función generadora
			KT_{DS}	Variable	*Valores de la plantilla de clave*	La clave pública se almacena en KT_{DS}. Esa herramienta utiliza sólo una clave pública
			SIZ_{DS}	16	0 ... (2^{16} – 1)	Tamaño de la firma digital en bytes
	PD			1	0_b	La estructura FBAS está terminada
				1	0_b	No se utiliza el dominio de píxels
				1	0_b	No se utiliza el dominio de coeficientes de ondícula
				1	1_b	Se utiliza el dominio de coeficientes de ondícula cuantificados
				1	0_b	No se utiliza el dominio del tren codificado
				3	000_b	Reservado para uso ISO
	G	PO		16	*Valores de la orden de procesamiento*	Orden de procesamiento
		GL		8	0000 1001	Nivel de granularidad: la unidad de protección es la zona total identificada en la ZOI
	V	N_V		16	1	El número de firmas digitales en la lista es 1
		S_V		8 (RBAS)	1 ... (2^8 – 1)	Tamaño de la firma digital en bytes
		VL		8* S_V	*Valor de la firma digital*	Las firmas digitales generadas por la herramienta
	LABR	$LABR_{int}$		8	0 ... (2^8 – 1)	La parte entera de LABR
		$LABR_{fra}$		8	0 ... (2^8 – 1)	La parte decimal de LABR
	Threshold			8	[0,2^8 – 1]	El valor umbral (válido únicamente para la autenticación sin pérdidas)
	Shuffle			8	[0,2^8 – 1]	El número de permutaciones en el orden para integrar bits de filigrana (válido únicamente en el caso de autenticación sin pérdidas)

El ID único de esta herramienta ha de asignarlo la autoridad de registro. La descripción de la herramienta puede descargarse de la autoridad de registro (RA) utilizando el ID asignado.

B.3.3 Conclusiones

En resumen, esta herramienta dispone de las siguientes características especiales:

- Autenticación de imágenes JPEG 2000 a nivel de datos o de contenido de la imagen mediante la integración de autenticación frágil y semifrágil en un marco. Además, la autenticación semifrágil incluye los modos con pérdidas y sin pérdidas.
- Robustez con respecto a diversas distorsiones indeseadas, tales como las que introduce la transcodificación, la conversión de formatos, la compresión con pérdidas y multiciclo de codificación JPEG 2000. Por consiguiente, esta herramienta puede utilizarse para proteger imágenes JPEG 2000 en entornos ubicuos.
- Protección con capacidad evolutiva de imágenes JPEG 2000. Concretamente, esta herramienta permite proteger cualquier losa, componente, resolución, capa, prerecinto o bloque de código.
- Compatibilidad con el marco de seguridad de la información más reciente denominado infraestructura de clave pública, que es la base de las normas internacionales existentes tales como la X.509.
- Intensidad de protección cuantitativa controlada por un solo parámetro denominado LABR, que resulta muy conveniente para los usuarios.
- Capacidad para localizar las zonas de la imagen posiblemente atacadas si la imagen se considera que no es auténtica. Esto puede resultar útil para los usuarios a efectos de visualización.
- Permite la protección con pérdidas a sin pérdidas, que corresponde a la compresión con pérdidas a sin pérdidas de las normas de codificación JPEG 2000. Por consiguiente, la herramienta dispone de aplicaciones más amplias, en particular aplicaciones de imágenes médicas y de imágenes distantes.

B.4 Método sencillo de criptación basada en paquetes para trenes codificados JPEG 2000

B.4.1 Descripción del funcionamiento

En la presente subcláusula se describe una técnica de criptación selectiva para imágenes JPEG 2000, basada en la criptación a nivel de paquetes y algoritmos de cifrado robustos normativos.

Esta técnica emplea como servicio de seguridad la confidencialidad de imágenes JPEG 2000, que se obtiene mediante el cifrado del tren codificado. Por consiguiente, mediante esta técnica se logra tanto la protección de DPI como la protección de la privacidad.

El método soporta la transcodificación, la capacidad evolutiva y otras funciones de procesamiento de contenido sin tener que acceder a la clave criptográfica o descriptar y volver a criptar. Además, no interfiere en los procesos de codificación y de decodificación, los efectos negativos sobre la eficacia de la compresión son muy limitados y no repercute perjudicialmente en la recuperación de errores. Este método permite la máxima flexibilidad a la hora de implementar configuraciones y aplicaciones con diversos niveles de seguridad.

Los productores de contenido pueden utilizar esa técnica para limitar el acceso al contenido de la imagen, y los proveedores de contenido pueden utilizarla para la transmisión confidencial de contenido a los usuarios.

B.4.2 Descripción técnica

La técnica consiste en criptar el tren codificado después de comprimir la imagen, como se muestra en la figura B.2.

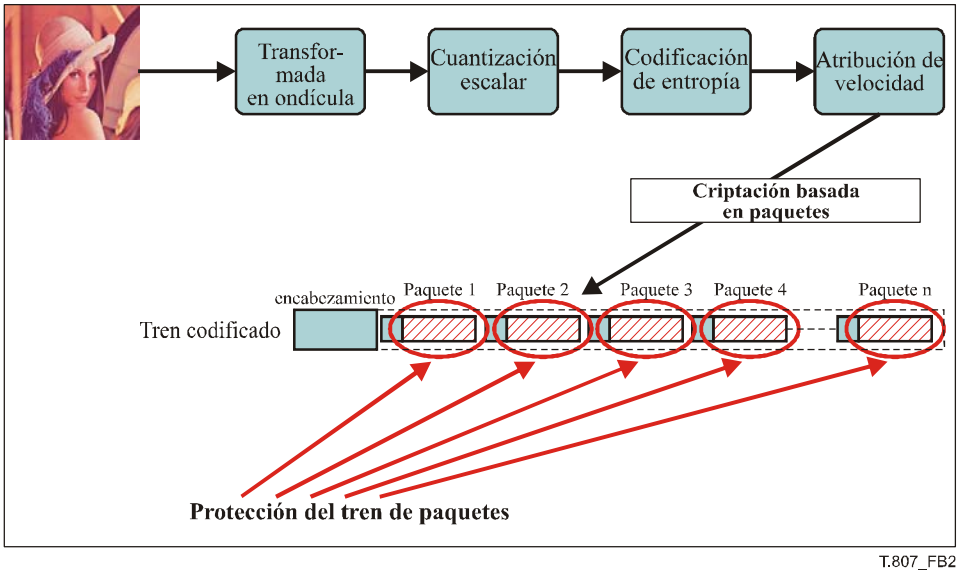


Figura B.2 – Principios de criptación basada en paquetes

Esta herramienta JPSEC puede aceptar como argumento diversos parámetros de la imagen, a saber, niveles de resolución, capas de calidad, componentes, prerecintos o losas. Sólo se procesan las cabidas útiles del paquete correspondiente a estos parámetros de entrada. Así pues, el tren codificado protegido mantiene la estructura normal de JPEG 2000. Una vez cifrado el tren codificado, se añade el segmento marcador SEC al encabezamiento principal para permitir que el consumidor JPSEC pueda más tarde descriptar correctamente la imagen.

Este método utiliza algoritmos subyacentes normalizados sobradamente conocidos para criptar selectivamente los paquetes, a saber, métodos de DES o AES, relacionados con los modos normalizados descritos en [22] tales como ECB, CBC, CFB, OFB y CTR. Obviamente, pueden utilizarse otros algoritmos de cifrado en bloque; DES y AES se presentan como ejemplos de cifrados normalizados.

B.4.2.1 Ejemplo de señalización

Para la señalización de esta técnica puede emplearse la sintaxis basada en plantillas de la cláusula normativa. A continuación figura un ejemplo de señalización para esta técnica (veáse el cuadro B.6), en la que se especifica una zona para la ZOI, aunque evidentemente podría haber más, seguido de la misma sintaxis que la zona^{0}.

Cuadro B.6 – Ejemplo de la zona de influencia, en coordenadas espaciales, resoluciones y capas

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NZzoi			8	1 (RBAS)	El número de zonas es uno
$Zone^0$	DCzoi		1	0	El segmento alineado por bytes no figura a continuación
			1	0	Clase de descripción relacionado con la imagen
			6	101100	Regiones de la imagen, niveles de resolución, capas de calidad y componentes se especifican en orden
	$Pzoi^1$	$Mzoi^1$	1	0	El segmento alineado por bytes no figura a continuación
			1	0	Las zonas especificadas se ven afectadas por el método de protección
			1	0	Se especifica un solo elemento
			2	00	Modo rectángulo
			2	00	Izoi utiliza un entero de 8 bits
			1	1	Izoi se describe en dos dimensiones
		$Izoi^1$	8	0110 0100	Xul es 100
			8	0111 1000	Yul es 120
			8	1011 0100	Xlr es 180
			8	1101 0010	Ylr es 210
	$Pzoi^3$	$Mzoi^3$	1	0	El segmento alineado por bytes no figura a continuación
			1	1	Las zonas especificadas no se ven afectadas por el método de protección
			1	0	Se especifica un solo elemento
			2	11	Modo Máx
			2	00	Izoi utiliza un entero de 8 bits
			1	0	Izoi se describe utilizando una sola dimensión
		$Izoi^3$	8	0000 0010	Se especifican niveles de resolución ≤ 2. (es decir, niveles de resolución > 3 se especifican en el modo Máx y un conmutador complementario)
	$Pzoi^4$	$Mzoi^4$	1	0	El segmento alineado por bytes no figura a continuación
			1	0	Las zonas especificadas se ven afectadas por el método de protección
			1	0	Se especifica un solo elemento
			2	11	Modo Máx
			2	00	Izoi utiliza un entero de 8 bits
			1	0	Izoi se describe en una dimensión
		$Izoi^4$	8	0000 0101	Las capas ≤ 5 se especifican en modo Máx

Cuadro B.7 – Descripción de la plantilla de descriptación, en el caso de AES-192/CBC

Parámetro					Tamaño (bits)	Valor	Significado derivado
P_{PM}	ME_{decry}				8	0000 0000	NULL: no se utilizan métodos de prevención de emulación del marcador
	CT_{decry}				16	0x0003	Identificador de cifrado: AES (cifrado en bloque)
	CP_{decry}	M_{bc}			6	10 0000	Modo de cifrado: CBC
		P_{bc}			2	01	Modo de relleno (relleno PKCS#7)
		SIZ_{bs}			8	0001 0000	Tamaño del bloque: 16 bytes (128 bits)
		KT_{bc}	LK_{KT}		16	0x00C0	Tamaño de la clave: 192 bits
			KID_{KT}		8	0000 0011	Información de clave es una URI
			LKI_{KT}		16	0x0021 (=33)	Longitud de la URI: 33 bytes
			KI_{KT}		264	https://server/ path/secretkey .pem	Esta URI es un https URL, que ha de entender la aplicación que utilice JPSEC. La técnica de extracción eficaz de la clave no se describe en la norma
			G_{KT}	PO	16	0 000 001 010 011 100	El orden de procesamiento es TRLCP
				GV	8	0000 1001	La granularidad de la clave es zona total en ZOI
			V_{KT}	Nv	16	0x0001	Valor de una sola clave en KI_{KT}; los valores no se especifican en el V_{KT}
				Sv	16	0010 0001	Longitud de la URI: 33 bytes
				VL	264	https://server/ path/secretkey .pem	Esta URI es un https URL, que ha de entender la aplicación que utilice JPSEC. La técnica de extracción eficaz de la clave no se describe en la norma

Cuadro B.8 – Sintaxis del dominio de procesamiento

Parámetro	Tamaño (bits)	Valor	Significado derivado
PD	1	0_b	El segmento alineado por bytes no figura a continuación
	1	0_b	No en el dominio de píxel
	1	0_b	No en el dominio de coeficientes de ondícula
	1	0_b	No en el dominio de coeficientes de ondícula cuantificado
	1	1_b	Procesado en el dominio del tren codificado
	3	000_b	No utilizado

Cuadro B.9 – Granularidad y sintaxis de la lista de valores

Parámetro		Tamaño (bits)	Valor	Significado derivado
G	PO	16	0 000 001 010 011 100	El orden de procesamiento es TRLCP
	GV	8	0000 0110	La unidad de protección es el paquete
V	N_V	16	1	Número de valores IV especificado
	Sv	8	16	Tamaño de IV en bytes
	VL	128	*Valor*	Valor IV

B.4.3 Conclusión

La técnica descrita en la presente subcláusula sirve para la criptación selectiva de imágenes JPEG 2000. Esta técnica se basa en la criptación a nivel de paquetes y en algoritmos de cifrado robustos normalizados. Para su señalización pueden utilizarse las plantillas definidas en 5.8 y soporta la utilización de diversos niveles de complejidad.

B.5 Herramienta de criptación para el control de acceso a JPEG 2000

B.5.1 Servicios de seguridad a los que pueden aplicarse

Esta tecnología sirve de herramienta de criptación para impedir la emulación del marcador en un tren codificado criptado.

B.5.2 Aplicaciones típicas

Esta tecnología permite la criptación selectiva e íntegra de trenes codificados JPEC 2000. Estos métodos de criptación selectiva pueden utilizarse para visualizar únicamente una imagen aprobada, por ejemplo un icono, una imagen de baja calidad y una imagen parcialmente aleatorizada.

B.5.3 Posibles usuarios, modelo de implementación y motivos

Esta tecnología consiste básicamente en la criptación basada en paquetes de trenes codificados JPEG 2000 mediante un algoritmo de cifrado sobradamente conocido. Concretamente, esta tecnología impide la emulación del marcador en el tren codificado criptado. Por consiguiente, aun cuando el tren codificado criptado resultante se haga pasar por un decodificador compatible JPEG 2000 Parte 1, es improbable que el decodificador colapse y que pueda reproducir correctamente las imágenes protegidas.

B.5.4 Descripción técnica

(1) Criptación

Paso 1 El código de 2 (bytes) se cripta temporalmente utilizando un algoritmo de cifrado conocido.

Paso 2 Si el código criptado temporalmente o su código relacionado es mayor que 0xFF8F, el código de 2 (bytes) no se cripta.

De lo contrario, el código criptado temporalmente se considera como el código criptado resultante.

Paso 3 Se aplica este procedimiento al siguiente código de 2 (bytes), y se repiten los pasos 1 y 2.

Todos los códigos de 2 (bytes) en el texto llano deberán ser inferiores a 0xFF90 conforme a la especificación de Parte 1. Además, si el código criptado temporalmente o su código relacionado es mayor que 0xFF8F, este código de 2 (bytes) no se cripta. En definitiva, todos los códigos de 2 (bytes) en el texto cifrado son inferiores a 0xFF90.

Si la longitud del texto llano es impar, el procesamiento tiene una excepción, a saber, el último byte no se cripta o se rellena con un byte adicional.

(2) Descriptación

Paso 1 Se descripta el código 2 (bytes) temporalmente utilizando los mismos algoritmos de cifrado que se utilizó en la criptación.

Paso 2 Si el código descriptado temporalmente o su código relacionado es mayor que 0xFF8F, no se descripta el código de 2 (bytes). De lo contrario, el código descriptado temporalmente se considera como el código descriptado.

Paso 3 Se procede al siguiente código 2 (bytes), y se repiten los pasos 1 y 2.

Todos los códigos de 2 (bytes) en el texto llano original antes de la criptación deben ser inferiores a 0xFF90. Así pues, es posible saber si el código de 2 (bytes) no está criptado comprobando simplemente que el código descriptado temporalmente o su código relacionado es mayor que 0xFF8F.

B.5.5 Método de señalización

En el cuadro B.10 se muestran los parámetros de ejemplo de esta tecnología. Todos los parámetros de esta tecnología se deberán señalar conforme a la sintaxis especificada en JPSEC. Concretamente, esta tecnología debe utilizar la plantilla "descriptación", granularidad de "paquete" y dominio de procesamiento "tren de bits" con la correspondiente ZOI.

Cuadro B.10 – Parámetros de ejemplo para esta tecnología

Parámetro		Tamaño (bits)	Valor	Significado
SEC		16	0xFF65	Marcador SEC
L_{SEC}		16	Variable	Longitud del segmento marcador SEC
Z_{SEC}		8	1 (ejemplo)	Índice de este segmento marcador SEC
P_{SEC}		1	0	El byte FBAS no figura a continuación
	F_{INSEC}	1	1 (ejemplo)	Se utiliza INSEC
	$F_{multiSEC}$	1	0_b	Se utiliza un segmento marcador SEC
	F_{mod}	1	1_b	Los datos JPEG 2000 originales fueron modificados
	F_{TRLCP}	1	0_b	La utilización de la etiqueta TRLCP no está definida
	Padding	3	000_b	No utilizado
	N_{tools}	8 (RBAS)	1	El número de la herramienta de seguridad es uno
	I_{max}	8 (RBAS)	0	El índice máximo del ejemplar de herramienta es cero
t		8 (FBAS)	1	Herramienta normativa JPSEC de protección de la RA
i		8 (RBAS)	0000000_b	Índice del ejemplar de herramienta
ID_{RA}	$ID_{RA,id}$	32	0	ID registrado
	$ID_{RA,nsl}$	8 (RBAS)	21	La longitud de $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$	168	*namespace*	El espacio en nombres de la RA en la que se registró la herramienta
L_{zoi}		16	9	Longitud de la ZOI es de 9 bytes
ZOI		Variable	Véase el cuadro B.11 (ejemplo)	La zona de influencia para esta herramienta
L_{PID}		16	Variable	Longitud de L + T + PD + G
P_{ID}		Variable	Véase el cuadro B.12 (ejemplo)	Parámetros de esta tecnología

Cuadro B.11 – Ejemplo de ZOI de esta herramienta de generación de claves

Parámetro			Tamaño (bits)	Valor (en orden)	Significado derivado
NDzoi			8	1	El número de zona es uno
$Zone^0$	Dczoi		1	0_b	El segmento alineado por byte no figura a continuación
			1	0_b	Clase de descripción relacionada con la imagen
			6	101000_b	Regiones de la imagen y niveles de resolución se especifican en orden
	$Pzoi^1$	$Mzoi^1$	1	0_b	El segmento alineado por bytes no figura a continuación
			1	0_b	Las zonas especificadas se ven afectadas por el método de protección
			1	0_b	Se especifica un solo elemento
			2	00_b	Modo rectangular
			2	00_b	Izoi utiliza un entero de 8 bits
			1	1_b	Izoi se describe en dos dimensiones
		$Izoi^1$	8	$0110\ 0100_b$	Xul es 100
			8	$0111\ 1000_b$	Yul es 120
			8	$1011\ 0100_b$	Xlr es 180
			8	$1101\ 0010_b$	Ylr es 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	El segmento alineado por bytes no figura a continuación
			1	1_b	Las zonas especificadas se ven afectadas por el método de protección
			1	0_b	Se especifica un solo elemento
			2	11_b	Modo máx
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^3$	8	$0000\ 0010_b$	Se especifican un número de niveles de resolución > 3

Cuadro B.12 – P_{ID} para esta tecnología

Parámetro		Tamaño (bits)	Valor	Significado
T		Variable	Véase el cuadro B.13	Plantillas de descriptación
PD		8	$0000\ 1000_b$	El byte FBAS no figura a continuación. Procesado en el dominio del tren codificado
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100\ 0_b$	El orden de procesamiento es losa-resolución-capa-componente-prerecinto
	GL	8	$0000\ 0110_b$	La unidad de protección es el paquete
Skip		8	0	El parámetro *Skip* para esta herramienta

Cuadro B.13 – Ejemplo de plantilla de descriptado de esta tecnología

Parámetro		Tamaño (bits)	Valor (en orden)	Significado derivado
ME_{decry}		8	1	No se ha producido emulación del marcador
CT_{decry}		16	1	Cifrado en bloque (AES)
CP_{decry}	M_{bc}	6	$10\ 0010_b$	Se utiliza el modo OFB. (No hay relleno de bits.)
	SIZ_{bc}	16	128	Tamaño de bloque (128 bits)
	KT_{bc}	Variable	*Valores de la plantilla de clave*	Plantilla de clave
	IVsc	128	*Valores del vector inicial*	Valor del vector inicial

B.5.6 Conclusión

En esta subcláusula se describe una tecnología de criptación para los trenes codificados JPEG 2000. La ventaja más importante de esta tecnología es que impide la emulación del marcador en el tren codificado criptado.

B.6 Herramienta de generación de claves para el control de acceso a JPEG 2000

B.6.1 Servicios de seguridad a los que se aplica

Esta tecnología proporciona el control de acceso a la imagen para JPEG 2000 conforme a una estructura jerárquica en JPEG 2000.

B.6.2 Aplicaciones típicas

La aplicación típica de esta tecnología es la distribución de imágenes con seguridad, de modo que sólo los usuarios autorizados puedan reproducir la imagen aceptada. Por ejemplo, sirve para que pueda verse libremente una imagen en miniatura, pero que la imagen de mayor resolución sólo pueda decodificarla el usuario que dispone de la clave.

B.6.3 Posibles usuarios, modelo de implementación y motivos

Esta tecnología permite generar claves que se utilizarán en la distribución de imágenes JPEG 2000 con seguridad. Se basa en el control de acceso a la imagen, por ejemplo a una región de la misma, o bien con una determinada resolución o calidad. El principio de esta tecnología radica en generar jerárquicamente claves de criptación y descriptación utilizando para ello una función unidireccional criptográfica, por ejemplo la función generadora.

B.6.4 Descripción técnica

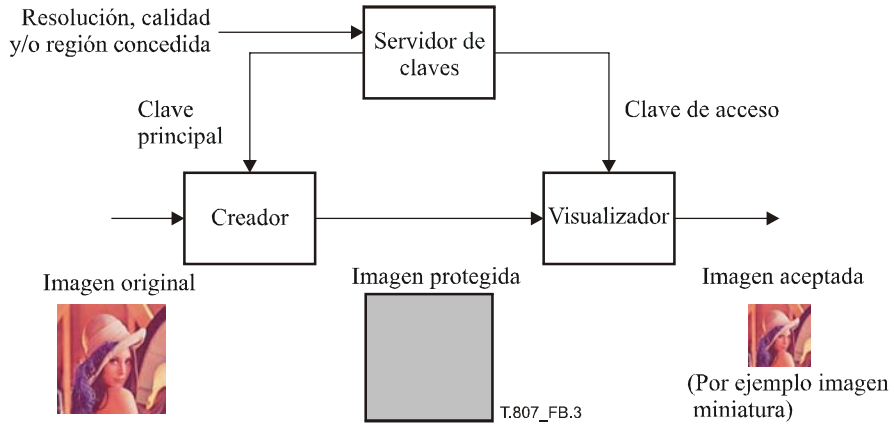


Figura B.3 – Descripción general de esta tecnología

En la fase de la criptación, el servidor de claves genera una clave principal. Seguidamente, el creador cripta la imagen utilizando las claves de paquetes que se generan a partir de la clave principal. En la fase de descriptación, el servidor de clave genera una clave de acceso en función de la resolución, calidad y/o región concebidas. Posteriormente, el visualizador decripta la imagen criptada mediante las claves de paquete que se generaron a partir de la clave de acceso. Obsérvese que estas claves se generan de manera secuencial conforme a una cadena generada protegida.

Esta tecnología utiliza concretamente la siguiente política de control de acceso: "si un usuario puede acceder a un nivel de resolución/capa, ese mismo usuario puede acceder también a niveles de resolución/capas inferiores". En cambio, el acceso a una losa no significa que el usuario tenga acceso a las demás losas.

La ventaja más importante de esta tecnología es que el número de claves que es necesario pasar desde un servidor de claves a un visualizador es mucho menor que en el caso convencional. Esto significa que esta tecnología utiliza menos recursos en cuanto a capacidad de almacenamiento.

B.6.5 Método de señalización

En el cuadro B.14 se muestran los parámetros recomendados en esta tecnología. Todos los parámetros deben señalarse conforme a la sintaxis definida en JPSEC. Esta herramienta debería utilizar especialmente la plantilla "descriptación", la granularidad "paquete" y el dominio de procesamiento "tren de bits" con la correspondiente ZOI.

Cuadro B.14 – Parámetros recomendados en esta tecnología

Parámetro		Tamaño (bits)	Valores	Significado
SEC		16	0xFF65	Marcadores SEC
L_{SEC}		16	0 ... 255	Longitud de marcadores SEC
Z_{SEC}		8	0	Índice de este segmento marcador SEC
P_{SEC}		1	0	El byte FBAS no figura a continuación
	F_{INSEC}	1	1	Se utiliza INSEC
	$F_{multiSEC}$	1	0_b	Se utiliza un segmento marcador SEC
	F_{mod}	1	1_b	Los datos JPEG 2000 originales fueron modificados
	F_{TRLCP}	1	0_b	La utilización de la etiqueta TRLCP no está definida
	Padding	3	000_b	No utilizado
	N_{tools}	8 (RBAS)	1	El número de la herramienta de seguridad es uno
	I_{max}	8 (RBAS)	0	El índice máximo del ejemplar de herramienta es cero
t		8 (RBAS)	1	Herramienta no normativa JPSEC

Cuadro B.14 – Parámetros recomendados en esta tecnología

Parámetro		Tamaño (bits)	Valores	Significado
i		8 (RBAS)	0	Índice del ejemplar para esta herramienta
ID_{RA}	$ID_{RA,id}$	32	5	ID registrado para esta herramienta
	$ID_{RA,nsl}$	8 (RBAS)	21	La longitud de $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$	168	*namespace*	El espacio de nombres de la RA en la que se registró la herramienta
L_{zoi}		16	Variable	Longitud de ZOI para esta herramienta
ZOI		Variable	*Valor ZOI*	Zona de influencia para esta herramienta
L_{PID}		16	Variable	Longitud de L + T + PD + G
P_{ID}		Variable	Véase el cuadro B.16	Parámetros de esta tecnología

Cuadro B.15 – Ejemplo de ZOI de esta herramienta de generación de claves

Parámetro			Tamaño (bits)	Valor (en orden)	Significado
NDzoi			8	1	El número de zona es uno
$Zone^0$	Dczoi		1	0_b	El segmento alineado por byte no figura a continuación
			1	0_b	Clase de descripción relacionado con la imagen
			6	101000_b	Regiones y niveles de resolución de la imagen se especifican en orden
	$Pzoi^1$	$Mzoi^1$	1	0_b	El segmento alineado por bytes no figura a continuación
			1	0_b	Las zonas especificadas se ven afectadas por el método de protección
			1	0_b	Se especifica un solo elemento
			2	00_b	Modo rectángulo
			2	00_b	Izoi utiliza un entero de 8 bits
			1	1_b	Izoi se describe en dos dimensiones
		$Izoi^1$	8	$0110\ 0100_b$	Xul es 100
			8	$0111\ 1000_b$	Yul es 120
			8	$1011\ 0100_b$	Xlr es 180
			8	$1101\ 0010_b$	Ylr es 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	El segmento alineado por bytes no figura a continuación
			1	1_b	Las zonas especificadas no se ven afectadas por el método de protección
			1	0_b	Se especifica un solo elemento
			2	11_b	Modo Máx
			2	00_b	Izoi utiliza un entero de 8 bits
			1	0_b	Izoi se describe en una dimensión
		$Izoi^3$	8	$0000\ 0010_b$	Se especifica un número de niveles de resolución > 3

Cuadro B.16 – P_{ID} para esta tecnología

Parámetro		Tamaño (bits)	Valores	Significado
T		Variable	Véase el cuadro B.17	Plantillas de descriptación
PD		8	$0000\ 1000_b$	El byte FBAS no figura a continuación. Procesado en el dominio de tren codificado
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	El orden de procesamiento es losa-resolución-capa-componente-prerecinto
	GL	8	$0000\ 0110_b$	La unidad de protección es el paquete
H		16	Véase el cuadro 38 de 5.5.3.1	Función generadora para esta herramienta de generación de claves
L_k		8	0 ... 255	Longitud de la información de clave de acceso
AK_{info}		Variable	*Valor de la clave de acceso*	Información de clave de acceso (esta información se cripta utilizando KT_{bc} en T)

Cuadro B.17 – Ejemplo de plantilla de descriptación de esta tecnología

Parámetro		Tamaño (bits)	Valor (en orden)	Significado derivado
ME_{decry}		8	1	No se ha producido emulación de marcador
CT_{decry}		16	3	Cifrado en bloque (AES)
CP_{decry}	M_{bc}	6	10 0010	Se utiliza el modo OFB (no hay bits de relleno)
	SIZ_{bc}	16	128	Tamaño de bloque (128 bits)
	KT_{bc}	Variable	Véase 5.8.5	Plantilla de claves
	IVsc	128	*Valor del vector inicial*	Valor del vector inicial

B.6.6 Conclusión

En esta subcláusula se describe una tecnología de control de acceso relacionado con la imagen para trenes codificados JPEG 2000. La ventaja más importante de esta tecnología es que el número de claves que se ha de gestionar y a la que se ha de acceder es muy inferior al del caso convencional.

B.7 Aleatorización en los dominios de ondícula de tren de bits y para el control de acceso condicional

B.7.1 Resumen

El control de acceso a una imagen es una función importante en los sistemas de imágenes con seguridad. A menudo se desea dar acceso a una imagen en miniatura de pequeña resolución o a una imagen de menor calidad, mientras que para acceder con mayor resolución o calidad se necesite una autorización. En esta subcláusula se describe una técnica para controlar el acceso condicional. El método se presentó originalmente en [23]. Consiste básicamente en añadir ruidos seudoaleatorios a la imagen. Los usuarios autorizados conocen la secuencia seudoaleatoria y, por consiguiente, pueden suprimir este ruido. Por el contrario, los usuarios no autorizados sólo tienen acceso a las imágenes altamente distorsionadas. El sistema consta de tres componentes principales, a saber, aleatorización, generador de números seudoaleatorios y algoritmo de criptación. A fin de explotar y mantener íntegra las propiedades de la JPEG 2000, la aleatorización se aplica selectivamente a los bloques de código que constituyen el tren codificado. Por consiguiente, el nivel de distorsión introducido en determinadas partes de la imagen puede controlarse. Esto permite controlar el acceso según la resolución, la calidad o las regiones de interés de la imagen.

B.7.2 Descripción técnica

El sistema consta de tres componentes principales:

- Aleatorización: Puede aplicarse de dos maneras, bien a los coeficientes de ondícula cuantizados o directamente a los bits en el tren codificado. En el primer caso los signos de los coeficientes en cada bloque de código se invierten de manera seudoaleatoria. En el segundo caso, se invierten también seudoaleatoriamente los bits del tren codificado.
- Generador de números seudoaleatorio (PRNG): Se utiliza para controlar la aleatorización. Se basa en un valor germen. Una de las formas de integración preferidas de esta técnica se basa en el algoritmo SHA1PRNG [24] con un germen de 64 bits para el generador de números seudoaleatorio (PRNG). Obsérvese que también pueden utilizarse otros algoritmos PRNG.
- Algoritmo de criptación: Para comunicar los valores germen a los usuarios autorizados, éstos se criptan y se insertan en el tren codificado. Una de las formas más utilizadas de integrar esta técnica consiste en utilizar el algoritmo RSA para la criptación [25]. No obstante, pueden utilizarse otros algoritmos de criptación. La longitud de la clave puede seleccionarse cuando se proteja la misma.

Las figuras B.4 y B.5 corresponden a los dos casos de aleatorización, a saber, en el dominio de ondícula y en el dominio de tren de bits.

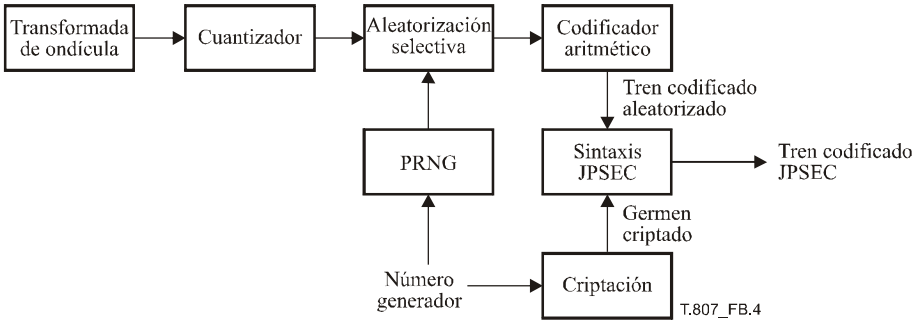


Figura B.4 – Diagrama de bloques de la aleatorización en el dominio de ondícula

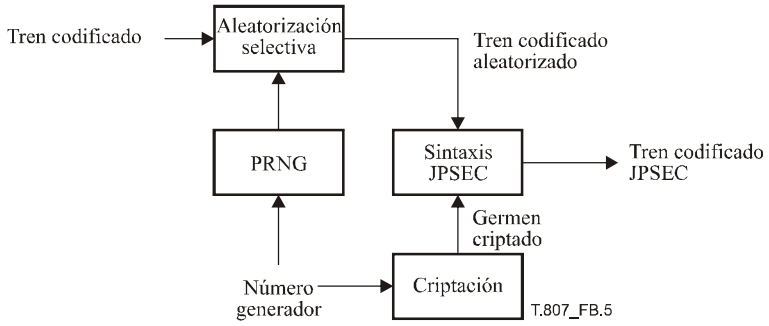


Figura B.5 – Diagrama de bloques de la aleatorización en el dominio del tren de bits

Para aumentar la seguridad del sistema, puede utilizarse un germen distinto en cada bloque de código. Además, pueden definirse diversos niveles de acceso utilizando para ello diferentes claves de criptación. La sintaxis que se describe a continuación es muy flexible y permite utilizar múltiples valores germen y múltiples claves.

B.7.3 Sintaxis del tren codificado

En este ejemplo, se utilizan segmentos marcadores SEC e INSEC. La sintaxis del tren codificado se define más abajo. El segmento marcador SEC utiliza la sintaxis de la herramienta para herramientas no normativas. El segmento marcador INSEC se utiliza para señalar qué bloques de código se aleatorizan y cuál es el germen que se utiliza.

B.7.3.1 Sintaxis del segmento marcador SEC

Se utiliza la sintaxis de herramienta para herramientas no normativas. En el caso de múltiples claves, se emplean varios ejemplares de la herramienta en el segmento marcador SEC. Concretamente, varios ejemplares i = 0, 1, 2, … con el mismo ID, cada una correspondiente a un identificador de clave distinto $KeyID^{(i)}$, como se ilustra a continuación. Véase la figura B.6

t	i = 0	ID	$L_{ZOI}^{(0)}$	$ZOI^{(0)}$	$L_{PID}^{(0)}$	$N_S^{(0)}$	$KeyID^{(0)}$	Data
t	i = 1	ID	$L_{ZOI}^{(1)}$	$ZOI^{(1)}$	$L_{PID}^{(1)}$	$N_S^{(1)}$	$KeyID^{(1)}$	Data
t	i = 2	ID	$L_{ZOI}^{(2)}$	$ZOI^{(2)}$	$L_{PID}^{(2)}$	$N_S^{(2)}$	$KeyID^{(2)}$	Data

Figura B.6 – Sintaxis de la herramienta de protección no normativa en el caso de múltiples claves

La semántica de P_{ID} es la siguiente:

Cuadro B.18 – Sintaxis y semántica de P_{ID}

Parámetros	Tamaño (en bits)	Significado
N_s	16	El número de gérmenes utilizado por este ejemplar
KeyID	32	Identificación de la clave que habrá de utilizarse al descriptar
Data	Variable	Los gérmenes criptados

B.7.3.2 Sintaxis del segmento marcador INSEC

Para incluir la información que se utiliza como germen para proteger cada bloque de código, se utiliza también el segmento marcador de seguridad dentro del tren codificado (INSEC). En este ejemplo, este segmento se añade antes de los bloques codificados protegidos para indicar qué germen se ha utilizado para protegerlos. En lugar de especificar el germen propiamente dicho, el marcador contiene un índice que apunta al germen contenido en el segmento marcador SEC del encabezamiento principal. Como en este ejemplo la información INSEC se aplica a los siguientes bloques codificados, R es siempre igual a 1. La sintaxis de AP es diferente en el caso de la aleatorización en el dominio de ondícula y de aleatorización en el dominio del tren de bits:

S_{idx}

Off	S_{idx}

Figura B.7 – Sintaxis de AP: Aleatorización en el dominio de ondícula (izquierda), aleatorización en el dominio tren de bits (derecha)

La semántica es la siguiente:

Cuadro B.19 – Sintaxis semántica de AP

Parámetro	Tamaño (en bits)	Significado
Off	16	La traslación en el tren de bits del bloque de código del primer byte aleatorizado
S_{idx}	16	El índice del germen para el bloque de código

En el caso de que existan múltiples claves, la combinación del ejemplar de herramienta i y del índice de gérmenes S_{idx} identifica únicamente a qué germen/clave se refiere este segmento marcador INSEC.

B.7.4 Conclusiones

En esta subcláusula se describe una herramienta de seguridad para el control de acceso condicional a las imágenes JPEG 2000. La técnica introduce ruido seudoaleatorio a determinadas partes del tren codificado. Por consiguiente, los decodificadores no autorizados que no saben cómo eliminar este ruido verán una imagen decodificada muy distorsionada.

El grado de seguridad de esta técnica depende de la seguridad de los algoritmos especificados para el generador de número seudoaleatorio y criptación del germen, que en el caso recomendado son, respectivamente, SHA1PRNG y RSA. SHA1PRNG es un PRNG protegido, dado que no puede deducirse información de la secuencia aunque se conozcan algunos de los números de la misma. En este ejemplo, el germen PRNG es de 64 bits por lo que cualquier ataque exhaustivo resultaría inofensivo. Los gérmenes se criptan con RSA utilizando una longitud de clave definida por el usuario. RSA se considera un algoritmo seguro, siempre que se utilice una clave lo suficientemente larga.

B.8 Acceso progresivo al tren codificado JPEG 2000

B.8.1 Servicios de seguridad a los que se aplica

Este método ofrece un control de acceso no relacionado con la imagen para JPEG 2000 conforme a un orden de progresión en el tren codificado.

B.8.2 Aplicaciones típicas

Una aplicación típica de esta tecnología es la distribución segura de imágenes en las que sólo los usuarios autorizados pueden reproducir la imagen aceptada. Concretamente, esta tecnología es adecuada para el control de acceso según un orden de progresión en el tren codificado.

B.8.3 Posibles usuarios, modelo de implementación y motivos

El problema que presenta el diseño del mecanismo de control de acceso es llegar a una solución de compromiso entre la seguridad, la eficiencia y la flexibilidad. Esta técnica de control de acceso para el tren codificado JPEG 2000 crea una cadena generadora de claves para cada paquete a fin de criptar paquetes en el tren codificado. Por consiguiente, sólo los usuarios que dispongan de la autorización de seguridad adecuada pueden descriptar los paquetes correspondientes a las imágenes concedidas en el tren codificado.

B.8.4 Descripción técnica

En la etapa de criptación, el servidor genera una clave maestra. Seguidamente, el creador cripta el tren codificado utilizando claves de paquetes que se generan a partir de la clave maestra. En la fase de descriptación, el servidor de claves genera una clave de acceso según el paquete concedido. Posteriormente, el visualizador descripta los trenes codificados criptados utilizando las claves de paquetes que fueron generadas a partir de la clave de acceso.

Esta tecnología se basa concretamente en la siguiente política de control de acceso: "si un usuario puede acceder a un paquete, también podrá acceder a los paquetes precedentes del tren codificado". Por consiguiente, este control de acceso se denomina "Acceso progresivo".

La ventaja más importante de esta tecnología es que el número de claves necesarias que han de transmitirse entre el servidor de claves y el visualizador es muy inferior al caso convencional. Esto significa que la tecnología permite utilizar menos recursos en cuanto a capacidad de almacenamiento.

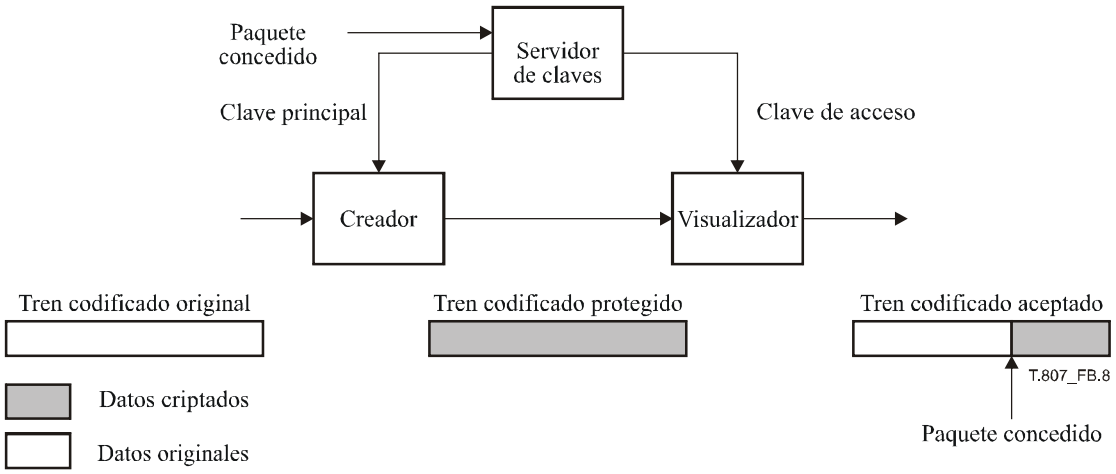


Figura B.8 – Descripción técnica de esta tecnología

B.8.5 Método de señalización

En el cuadro B.20 se muestran los parámetros recomendados en esta tecnología. Todos los parámetros deben señalarse conforme a la sintaxis definida en JPSEC. Concretamente, esta tecnología debe utilizar la plantilla "descriptación", la granularidad "paquete" y el dominio de procesamiento "tren de bits" dentro de la ZOI considerada.

Cuadro B.20 – Parámetros de ejemplo de esta herramienta

Parámetro		Tamaño (bits)	Valores	Significado
SEC		16	0xFF65	Marcador SEC
L_{SEC}		16	Variable 0 ... 255	Longitud del segmento marcador SEC
Z_{SEC}		8	0	Índice de este segmento marcador SEC
P_{SEC}		1	0	El byte FBAS no figura a continuación
	F_{INSEC}	1	1_b	Se utiliza INSEC
	$F_{multiSEC}$	1	0_b	Se utiliza un segmento marcador SEC
	F_{mod}	1	1_b	Los datos JPEG 2000 originales fueron modificados
	F_{TRLCP}	1	0_b	No está definida la utilización de la etiqueta TRLCP
	Padding	3	000_b	No utilizado
	N_{tools}	8 (RBAS)	1	El número de herramienta de seguridad es uno
	I_{max}	8 (RBAS)	0	El índice máximo del ejemplar de herramienta es cero
t		8 (RBAS)	1	Herramienta de protección RA
i		8 (RBAS)	0	Índice del ejemplar
ID_{RA}	$ID_{RA,id}$	32	7	ID registrado
	$ID_{RA,nsl}$	8 (RBAS)	21	La longitud de $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$	168	*namespace*	El espacio de nombres de la RA en la que se registró la herramienta
L_{zoi}		16 (RBAS)	Variable	Longitud de la ZOI
ZOI		Variable	Véase el cuadro B.21 (ejemplo)	Zona de influencia de esta herramienta
L_{PID}		16 (RBAS)	Variable	Longitud de L + T + PD + G
P_{ID}		Variable	Véase el cuadro B.22 (ejemplo)	Parámetros de esta herramienta

Cuadro B.21 – Ejemplo de ZOI de esta tecnología

Parámetro			Tamaño (bits)	Valor (en orden)	Significado
NDzoi			8	1	El número de zona es uno
$Zone^0$	DCzoi		1	0	El segmento alineado por bytes no figura a continuación
			1	1	Clase de descripción no relacionada con la imagen
			6	000100	Se especifican paquetes
	$Pzoi^4$	$Mzoi^4$	0	1	El segmento alineado por byte no figura a continuación
			1	1	Las zonas especificadas no se ven afectadas por el método de protección
			1	1	Se especifican múltiples elementos
			11	2	Modo Máx
			00	2	Izoi utiliza un entero de 8 bits
			00	2	Izoi se describe en una dimensión
		$Izoi^{11}$	8	0000 1010	Se ha detectado un índice de paquetes > 10

Cuadro B.22 – P_{ID} para esta tecnología

Parámetro		Tamaño (bits)	Valores	Significado
T		Variable	Véase el cuadro B.23	Plantillas de descriptación
PD		8	$0000\ 1000_b$	Rl byte BAS subsiguiente no existe Dominio de tren codificado
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	El orden de procesamiento es losa-resolución-capa-componente-prerecinto
	GL	8	$0000\ 0110_b$	La unidad de protección es el paquete.
H		16	Véase el cuadro 38 en 5.5.3.1	Función generadora para esta herramienta de generación de claves
L_k		8	0 – 255	Longitud de la información relativa a la clave de acceso
AK_{info}		Variable	*Valor de la clave de acceso*	Información relativa a la clave de acceso (esta información está encriptada utilizando KT_{bc} en T

Cuadro B.23 – Ejemplo de plantilla de descriptación de esta tecnología

Parámetro		Tamaño (bits)	Valor (en orden)	Significado
ME_{decry}		8	1	No se ha producido emulación de marcador
CT_{decry}		16	3	Cifrado de bloque (AES)
CP_{decry}	M_{bc}	6	10 0010	Se utiliza el modo OFB (sin relleno de bits)
	SIZ_{bc}	16	128	Tamaño del bloque (128 bits)
	KT_{bc}	Variable	*Valores de la plantilla de claves*	Plantilla de clave
	IV_{sc}	128	*Valor del vector inicial*	Valor del vector inicial

B.8.6 Conclusión

En esta subcláusula se describe una tecnología de control de acceso para el tren codificado JPEG 2000. La ventaja considerable de esta tecnología es que el número de claves que han de gestionarse y a las que se debe acceder es inferior al caso convencional. Esta tecnología ofrece un control de acceso JPEG 2000 flexible y eficaz conforme a un orden de progresión del tren codificado.

B.9 Autenticación con capacidad evolutiva de trenes codificados JPEG 2000

B.9.1 Servicio de seguridad

En esta subcláusula se describe un mecanismo de autenticación flexible para trenes codificados JPEG 2000. Permite a los usuarios verificar la autenticidad e integridad de diferentes subimágenes utilizando para ello una sola firma digital.

B.9.2 Aplicación típica

En los ámbitos de aplicación delicados, tales como gobierno, finanzas, atención sanitaria y legislación, los clientes exigen por regla general la autenticidad del contenido recibido. Por consiguiente, se necesita un mecanismo de seguridad evolutivo para autenticación del documento en la distribución del contenido.

B.9.3 Motivos

En las aplicaciones publicadas por terceras partes, el producto de imágenes genera un tren codificado y su firma, que luego los distribuye a una tercera parte para su publicación. Los usuarios pueden solicitar al editor que transcodifique el tren codificado debido a la limitación de recursos (por ejemplo, anchura de banda, capacidad de cálculo). El editor suministrará al usuario los datos de su imagen así como una prueba de su autenticidad.

B.9.4 Descripción técnica

El sistema ofrece un mecanismo de autenticación flexible de tren decodificado JPEG 2000. Consta de tres módulos: firma, transcodificación y verificación. La tecnología básica es el árbol Merkle que organiza los paquetes JPEG 2000.

B.9.4.1 Módulo firma

El módulo firma genera una firma en un tren codificado JPEG 2000 de entrada conforme al plan de firmas digitales preferido. El tren codificado protegido se genera insertando un segmento marcador SEC en el tren codificado original. Concretamente, el productor:

- lee un tren codificado JPEG 2000;
- crea un árbol generador para producir el valor *raíz*. El valor de cada rama es el valor generador de un paquete. El valor de cada nodo interno es el valor generador de sus nodos vástagos. La estructura en árbol es similar al orden de progresión del tren codificado;
- firma el valor *raíz* del árbol generador con una clave privada basada en el algoritmo de firma;
- crea los parámetros SEC y los inserta en el segmento SEC para producir un tren codificado auténtico.

B.9.4.2 Módulo de transcodificación

Genera testigos de integridad subsidiarios (SIT, *subsidiary integrity tokens*) y un tren codificado transcodificado basado en la resolución, capa, componente y región solicitados. El SEC del nuevo tren codificado incluye los SIT y otros parámetros. Concretamente, el editor y/o servidor intermediario:

- lee los paquetes descartados que no están incluidos en el tren codificado transcodificado;
- crea los subárboles generadores con los paquetes descartados;
- inserta los valores raíz de los subárboles en el segmento SEC.

Una vez transcodificado, el nuevo tren codificado incluye el segmento SEC actualizado y el anterior tren codificado salvo los paquetes descartados.

B.9.4.3 Módulo de verificación

El módulo de verificación comprueba la autenticidad del tren codificado protegido. En función de la técnica de firma digital preferida, el verificador obtiene la clave pública y luego:

- lee el tren codificado recibido;
- construye el árbol generador a partir de los paquetes recibidos y los encabezamientos del tren codificado de abajo a arriba. En caso de que se descarten algunos paquetes, sustituye el subárbol con el correspondiente SIT. De este modo se construye el valor *raíz'*;
- compara el valor *raíz'* con la firma del segmento SEC basado en el sistema de firmas específico. Si son iguales, se acepta el tren codificado, de lo contrario se rechaza el paquete recibido.

B.9.5 Sintaxis de tren codificado

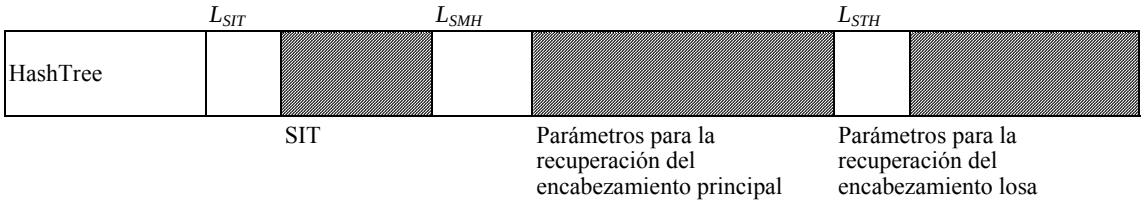
En el cuadro B.24 se muestra la estructura del SEC. Consta del marcador SEC, el ID de la herramienta y la ZOI, la plantilla de autenticación y los parámetros de seguridad para la verificación. Los parámetros de seguridad incluyen los datos para la recuperación de los encabezamientos de tren codificado.

Cuadro B.24 – Sintaxis de la herramienta normativa

t	i	ID	L_{ZOI}	ZoI_{ID}	L_{ID}	PM_{ID}	T	TP_{ID}

Parámetro		Tamaño (bits)	Valores	Semántica
t		8 (RBAS)	1	Herramienta de protección de la autoridad de registro
i		8 (RBAS)	*Valor del ejemplar*	Identificador del ejemplar de herramienta
ID_{RA}	$ID_{RA,id}$	32	*Valor de ID*	ID registrado
	$ID_{RA,nsl}$	8 (RBAS)	21	Longitud de $ID_{RA,ns}$ en bytes
	$ID_{RA,ns}$	168	*namespace*	Espacio de nombres de la RA en la que se registrará esta herramienta
L_{ZOI}		16	$[0 \ldots 2^{16} - 1]$	Longitud de los parámetros de ZOI
ZOI_{ID}		Variable	Valores ZOI	Parámetros de la zona
L_{ID}		16	$[19 \ldots 2^{16} - 1]$	Longitud de los parámetros
ID_T		8	2	id de la clase de plantilla de autenticación
T		Variable	*Valores de la plantilla de autenticación*	Plantilla de autenticación/MAC
TP_{ID}		Variable	Véase el cuadro B.25	Parámetros de seguridad

Cuadro B.25 – Parámetros de seguridad



Parámetro	Tamaño (bits)	Valores	Significado
HashTree	8	$0 \ldots (2^8 - 1)$	Orden del árbol generador. Puede ser diferente del orden de progresión del tren codificado. Por ejemplo, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL otros: Reservado
L_{SIT}	16	$0 \ldots (2^{16} - 1)$	Número de SIT
SIT	Variable: L_{hash}*L_{SIT}	NaN	Testigo de integridad subsidiario
L_{SMH}	16	$0 \ldots (2^{16} - 1)$	Longitud de SMH
SMH	Variable		Parámetros para la recuperación del encabezamiento principal
L_{STH}	16	$0 \ldots (2^{16} - 1)$	longitud del STH
STH	Variable		Parámetros para la recuperación del encabezamiento losa

a) Para la autenticación MAC basada en claves, la clave (verificación) deberá comunicarse por separado.

b) NaN: No es un número.

c) L_{hash} es el tamaño del valor generador, por ejemplo 160 para SHA-1.

B.9.6 Conclusión

Esta tecnología ofrece un mecanismo de autenticación flexible para trenes codificados JPEG 2000. Tienen la propiedad de que se "firma una sola vez, y puede verificarse de muchas maneras". Concretamente, después de que se haya firmado una vez el tren codificado JPEG 2000 original, podrán verificarse varios trenes codificados que han sido transcodificados a partir del tren codificado original confiando únicamente en el productor. Esta propiedad cumple a la perfección la característica de "comprimir una vez, descomprimir de muchas maneras". Obsérvese la diferencia con el método tradicional de autenticación de imágenes en el que una firma sirve únicamente para autenticar una sola imagen.

B.10 Sistema de control de acceso y confidencialidad de los datos JPEG 2000 basado en la división y compactación de datos

En esta cláusula se describe un sistema basado en la división mediante un proceso denominado *división y compactación de datos*, en el que el fichero JPEG 2000 original se divide en dos nuevos ficheros denominados, respectivamente, *Lured_jp2file*, que contiene el contenido protegido y el *Control_File*, en el que figura información necesaria para acceder al contenido protegido. La reconstrucción del fichero JPEG 2000 original sólo puede hacerse en tiempo real utilizando esos dos ficheros mediante el proceso *Live_Composing*. El proceso Live_Composing se gestiona mediante las reglas de control de acceso y la gestión de derechos. El sistema descrito ofrece un gran nivel de robustez y flexibilidad para el control de acceso y confidencialidad de los datos JPEG 2000 y se basa en operaciones de cálculo que consumen poco tiempo y pocos recursos de cálculo.

B.10.1 Descripción del funcionamiento

B.10.1.1 Servicios de seguridad a los que se aplica

- Confidencialidad: En el fichero Lured_jp2file figura el contenido protegido. Si se decodifica únicamente el fichero Lured_jp2file, el contenido que se obtiene está aleatorizado, lo que impide acceder al contenido original. El acceso al contenido original sólo puede realizarse en tiempo real mediante los datos almacenados en el fichero Control_File y utilizando el proceso Live_Composing.
- Control de acceso: Este sistema puede utilizarse para realizar el control de acceso al contenido de la imagen: varios usuarios comparten el mismo fichero Lured_jp2file, pero como tienen diferentes derechos de acceso no podrán acceder a las mismas partes del contenido.

Nota sobre la protección de derechos de propiedad intelectual (IPR): Para garantizar el control eficaz y el rastreo de la radiodifusión y utilización de contenido protegido puede establecerse una relación entre el acceso al contenido con autenticación y la gestión de derechos conforme a la voluntad y prerrogativas del propietario del contenido, utilizando para ello este sistema con la adición de filigranas y sellos.

B.10.1.2 Aplicaciones típicas

Una de las características principales del sistema descrito es la división del fichero JPEG 2000 original en dos ficheros, el primero (Lured_jp2file) contiene únicamente el 99% de los datos originales y 1% de datos falsos, denominados señuelos, fichero que puede distribuirse libremente, radiodifundirse o intercambiarse o copiarse a través de cualquier red o medio de transmisión clásico, y el segundo (Control_File) que transporta el 1% de datos originales más cierta información absolutamente indispensable para acceder al contenido protegido transportado en el Lured_jp2file.

La otra característica fundamental es vincular el acceso al contenido protegido incluido en el fichero Lured_jp2file con una identificación y gestión de derechos que son determinantes para la transmisión de secuencias de la información necesaria para recuperar en tiempo real únicamente el contenido aleatorizado.

Por último, se aplica eficazmente el seguimiento y la notificación mediante las estadísticas de los ficheros registro de los control_files protegidos que se encuentran en el servidor.

B.10.1.3 Posibles usuarios, modelo de implementación y motivos

Los usuarios potenciales del sistema descrito son los creadores, propietarios y proveedores de contenido, puesto que el sistema garantiza que una vez el contenido está protegido y transmitido en un fichero Lured_jp2file, sólo los usuarios autenticados y autorizados tendrán acceso al contenido original. Cabe destacar que únicamente el 99% del contenido original se facilita libremente, mientras que el 1% necesario para acceder al contenido original se distribuye únicamente después de haber aplicado los protocolos de autenticación y gestión de derechos.

B.10.2 Descripción técnica

En la figura B.9 se muestra un diagrama del sistema.

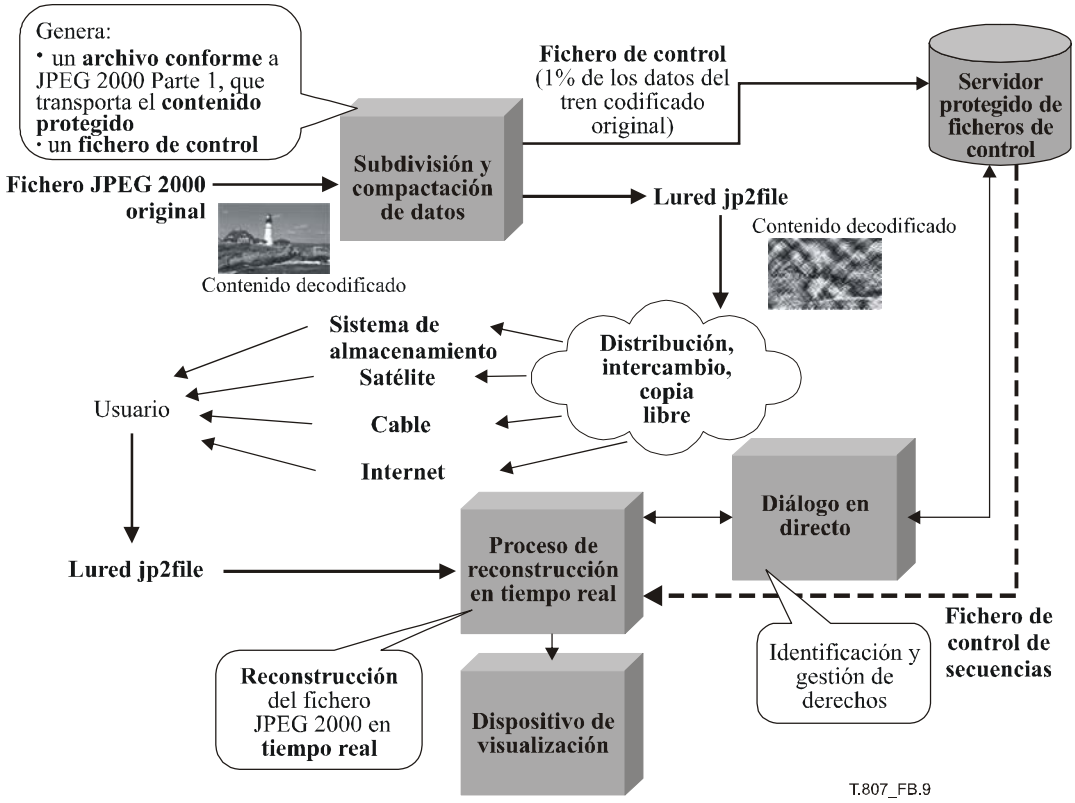


Figura B.9 – Descripción del sistema

El fichero JPEG 2000 original se divide en dos ficheros mediante una operación denominada *división y compactación de datos*, con el que se generan dos ficheros, a saber, *Lured_jp2file*, que transporta el contenido protegido (contenido JPSEC) y un *Control_File*.

Durante el proceso de división y compactación de datos, algunas partes del fichero JPEG 2000 original se extraen y se sustituyen por *señuelos*. El fichero Lured_jp2file transporta el 99% del contenido original mientras que el último 1% son datos falsos denominados señuelos, es decir datos que en principio no guardan relación alguna con los datos originales. A diferencia de la criptación clásica, el proceso de adición de señuelos no se basa en claves. El fichero Lured_jp2file puede distribuirse, intercambiarse o copiarse libremente por cualquier usuario. El fichero de control (Control_File) contiene el 1% de datos originales extraídos del fichero original, y se almacena en un *servidor protegido de ficheros de control*.

Cuando un decodificador conforme a JPEG 2000 Parte 1 decodifica el fichero Lured_jp2file, el contenido aparece aleatorizado. La única manera de acceder al contenido original es recuperar los datos originales extraídos utilizando para ello el fichero de control (Control_File). El dispositivo *Live_Composing* se conecta al servidor protegido de Control_Files mediante el protocolo *Live_Dialog* y se aplica el protocolo de identificación y gestión de derechos:

- si el usuario tiene derechos o acepta las condiciones de acceso al contenido (por ejemplo pago o abono), los datos se recuperan del fichero de control y el fichero JPEG 2000 original se recupera en tiempo real. Ahora bien, en función de los derechos del usuario, la reconstrucción de la imagen JPEG 2000 original puede ser parcial (por ejemplo permitir únicamente el acceso a una determinada losa y/o componente de color y/o resolución y/o prerecinto y/o capas de calidad) o íntegra;
- si el usuario no tiene derechos o no acepta las condiciones, sólo visualizará el contenido aleatorizado.

Las principales características de este sistema son las siguientes:

- *Separación del fichero original* JPEG 2000 en dos ficheros, el primero incluye el contenido JPEG 2000 protegido con el 99% de los datos originales más 1% de datos falsos denominados señuelos (Lured_jp2file), y el segundo almacena unos cuantos datos de información original (1%) necesario para reconstruir el contenido JPEG 2000 original;
- la *aleatorización visual* del contenido;
- la conformidad con JPEG 2000 Parte 1 y *se preserva el tamaño del fichero*;
- Sistema de proyección de costos *a baja velocidad de bits y con poca carga computacional*.

El sistema descrito puede utilizarse en cualquier entorno y/o sistema operativo. Tampoco son necesarios equipos o soporte lógico específicos.

En el proceso de adición de señuelos se añade el siguiente marcador SEC al fichero Lured_jp2file:

Cuadro B.26 – Valores de los parámetros de esta herramienta

Parámetro					Tamaño (bits)	Valor (en orden)	Significado
SEC					16	0xFF65	Marcador SEC
L_{SEC}					16	0xXXXX	Longitud del segmento marcador SEC
Z_{SEC}					8	1 ... 5	Índice del segmento marcador
P_{SEC} (si $Z_{SEC} = 1$)	F_{INSEC}				1	0	No se utiliza INSEC
	$F_{multiSEC}$				1	0	Se utiliza un solo segmento marcador SEC
	F_{J2K}				2	1	Tren JPSEC conforme con la JPEG 2000 Parte 1
	F_{TRLCP}				1	0	La utilización de la etiqueta TRLCP no se define en este campo
	N_{tools}				7	1	Se utiliza una herramienta de seguridad en el tren codificado
	I_{max}				7	1	Valor máximo utilizado del índice del ejemplar de herramienta
	Padding				5	0	Relleno
$Tool^{(0)}$	t				8 (RBAS)	1	Herramienta de protección no normativa
	i				8 (RBAS)	0	Índice del ejemplar de herramienta
	ID_{RA}		$ID_{RA,id}$		32	ID	Se utiliza la RA para obtener el número ID
			$ID_{RA,nsl}$		8 (RBAS)	21	Longitud de $ID_{RA,ns}$ es 21 bytes
			$ID_{RA,ns}$		168	*namespace*	Espacio en nombres de la RA en la que se registró la herramienta
	L_{ZOI}				16	*Valor longitud*	Longitud de L_{ZOI} + ZOI
	ZOI	NZ_{ZOI}			8	0 ... 254	Número de zonas
		$Zone^0$	DC_{ZOI}		1	0	El segmento alineado por bytes no figura a continuación
					1	1	No existe una clase de descripción relacionada con la imagen
					6	000010	Se especifican índices de paquetes
			$Pzoi^{0,0}$	Mzoi	1	0	El segmento alineado por bytes no figura a continuación
					1	0	Las zonas especificadas se ven afectadas por el método de protección
					1	1	Se especifican múltiples elementos
					2	10	Modo índice
					2	xx	Izoi utiliza un entero de 8, 16 ó 32 bits
					1	0	Izoi se describe en una dimensión
				Nzoi	8	Variable	2-255 (número de índices de paquete)
				$lzoi^i$	xxx Nzoi	variable	Índice de paquetes
	L_{PID}				16	0 ... $(2^{16} – 1)$	Longitud de L_{PID} + P_{ID} en bytes
	P_{ID}				Variable	Variable	ID del fichero de control, URL del servidor de fichero de control, etc.; la sintaxis la facilita la RA

Las herramientas necesarias para realizar la división y composición de datos y/o los procesos de composición en directo podrían obtenerse por medio de una conexión a la autoridad de registro para descargarlas.

B.11 Transmisión segura en secuencias y transcodificación con seguridad con capacidad evolutiva

B.11.1 Resumen y motivos

En esta subcláusula se describe el método para proporcionar servicios de protección de confidencialidad y autenticación de trenes codificado JPEG 2000 de manera que:

1) permita a una entidad (potencialmente no fiable) transcodificar con protección o adaptar trenes protegidos JPSEC sin que dicha entidad tenga que desproteger o descriptar el contenido; y
2) permitir al cliente validar que la operación y transcodificación fue realizada de manera válida y permitida.

Con frecuencia se necesita realizar la transcodificación para adaptar el contenido codificado JPEG 2000 a las diversas capacidades de los dispositivos del cliente (por ejemplo, para tamaños de pantalla pequeños o conexiones a la red a baja velocidad binaria) y en el caso de que las condiciones de la red varíen con el tiempo. La JPEG 2000 es especialmente adecuada para aplicaciones de transcodificación, dadas sus propiedades inherentes de capacidad evolutiva. Ahora bien, si no se toman ciertas preocupaciones al proteger los trenes codificados JPEG 2000, puede menoscabarse la propiedad de capacidad evolutiva. Esto puede suceder, por ejemplo, cuando el tren codificado está criptado en un solo fichero. En este caso, la única manera de transcodificar el tren codificado protegido es descriptarlo primero y luego transcodificarlo o adaptarlo al tren descriptado. Dado que el transcodificador debe descriptar el contenido, se rompe la seguridad de extremo a extremo del sistema.

JPSEC fue concebido para permitir la transcodificación segura de contenido protegido JPSEC, entendiéndose por transcodificación segura la *transcodificación sin desproteger (descriptar) el contenido*. Para ello se emplea la transmisión segura en secuencias con capacidad evolutiva, que combina la codificación evolutiva, la criptación y la señalización de manera que un servidor, un nodo de red intermedio o un servidor intermediario (potencialmente no fiable) pueda llevar a cabo la transcodificación segura de manera no muy compleja. Ello permite a JPSEC tener propiedades aparentemente conflictivas como son la transcodificación en la red intermedia y la seguridad de extremo a extremo. Por ejemplo, en la figura B.10 los medios se criptan en el transmisor y se descriptan únicamente en el receptor, por lo que permanecen criptados en todos los puntos intermedios: (izquierda) el nodo de red intermedio transcodifica de modo seguro el contenido protegido para cada cliente JPSEC, (derecha) un servidor no fiable transcodifica de modo seguro y emite en secuencias el contenido JPSEC sin desprotegerlo.

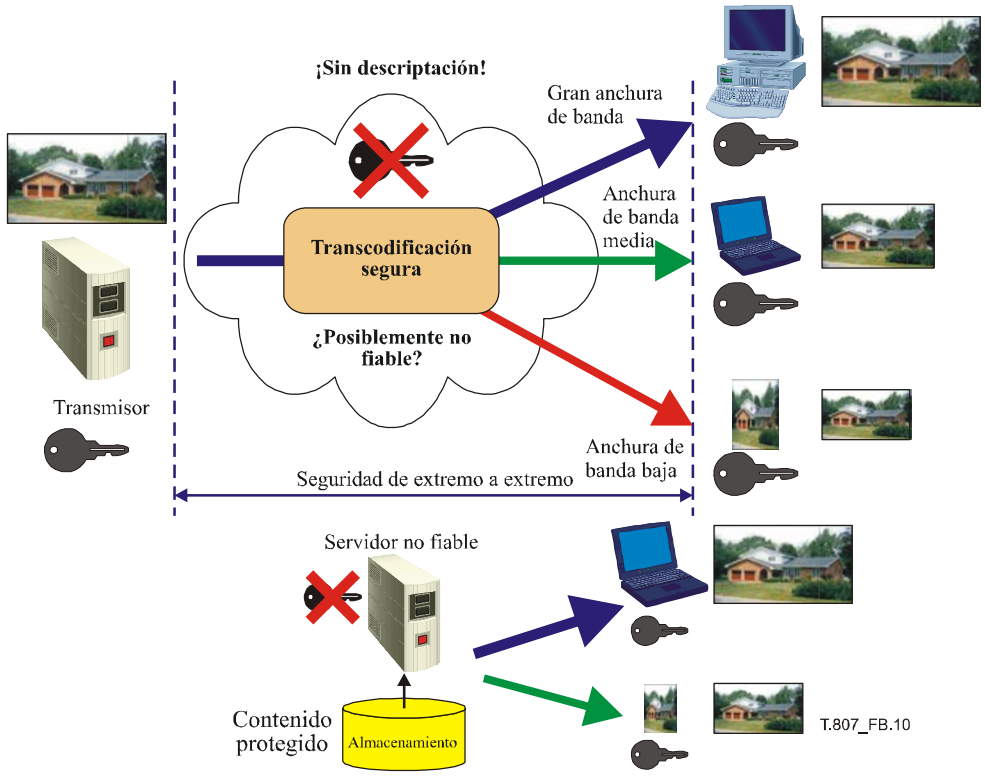


Figura B.10 – JPSEC permite la seguridad de extremo a extremo y la transcodificación segura en un punto intermedio de la red

B.11.2 Descripción del funcionamiento y dos ejemplos de utilización

En el primer ejemplo, el tren codificado JPEG 2000 original está en el orden RLCP y el objetivo es proteger este tren mediante la criptación y autenticación permitiendo a su vez la transcodificación segura del tren codificado protegido según la resolución. Dado que el tren codificado JPEG 2000 original utiliza el orden RLCP, cada componente de resolución está representada mediante un segmento de datos contiguo. La criptación puede realizarse en cada uno de los tres segmentos de datos contiguo. El encabezamiento JPSEC especifica tres zonas de influencia que describe el componente de resolución, el segmento de tren codificado y la plantilla de criptación utilizada para cada segmento. También se realiza la autenticación en cada uno de los tres segmentos de datos, antes o después de la criptación dependiendo de la funcionalidad deseada. Esto se especifica también en el encabezamiento SEC utilizando la plantilla de autenticación.

Para realizar la transcodificación segura del tren codificado JPSEC, el transcodificador sencillamente lee y analiza sintácticamente el encabezamiento SEC, identifica las posiciones de los segmentos de resolución y luego mantiene o suprime los primeros segmentos/resoluciones de datos adecuados. Obsérvese que esta operación de transcodificación consiste simplemente en un análisis sintáctico y que por lo tanto no se requiere desproteger los datos. La autenticación se realiza en los datos transcodificados recibidos con los valores MAC que se incluyeron en el encabezamiento SEC durante el proceso de protección JPSEC.

En el segundo ejemplo, el objetivo es de nuevo proteger en tren codificado permitiendo a su vez la transcodificación según la resolución. No obstante, este ejemplo es un poco más complejo que el anterior dado que el tren codificado JPEG 2000 original está en el orden PCRL en lugar de RLCP, de modo que los segmentos datos correspondientes a los tres componentes de resolución no están contiguos en el tren codificado original. JPSEC permite llevar a cabo de diversas maneras la transcodificación segura o el cambio de escala por resolución deseados. Un método consiste en criptar cada paquete salvo los encabezamientos. De este modo se obtiene el nivel más alto de capacidad evolutiva en el tren, aunque ello implica que la operación en transcodificación segura sea más compleja, dado que en este caso la transcodificación debe analizar el tren JPSEC a nivel de paquete. El otro extremo, que corresponde a la operación de transcodificación segura más sencilla, consiste en reordenar los datos de modo que los componentes de la resolución estén nuevamente en segmentos contiguos cuyas posiciones se indican en el encabezamiento SEC. Esto puede lograrse de manera conforme a la JPEG 2000 reordenando los paquetes JPEG 2000 de PCRL a RLCP e indicando el nuevo orden de progresión en el segmento marcador COD o en el segmento marcador de cambio de orden de progresión (POC). La reordenación de los datos y la transformación de protección se muestran en la figura B.11. Una vez más, el encabezamiento SEC principal contiene los parámetros ZOI que describen los correspondientes parámetros relacionados con la imagen y con el tren de bits para cada segmento de datos, pero en esta ocasión se refieren al tren codificado JPEG 2000 reordenado.

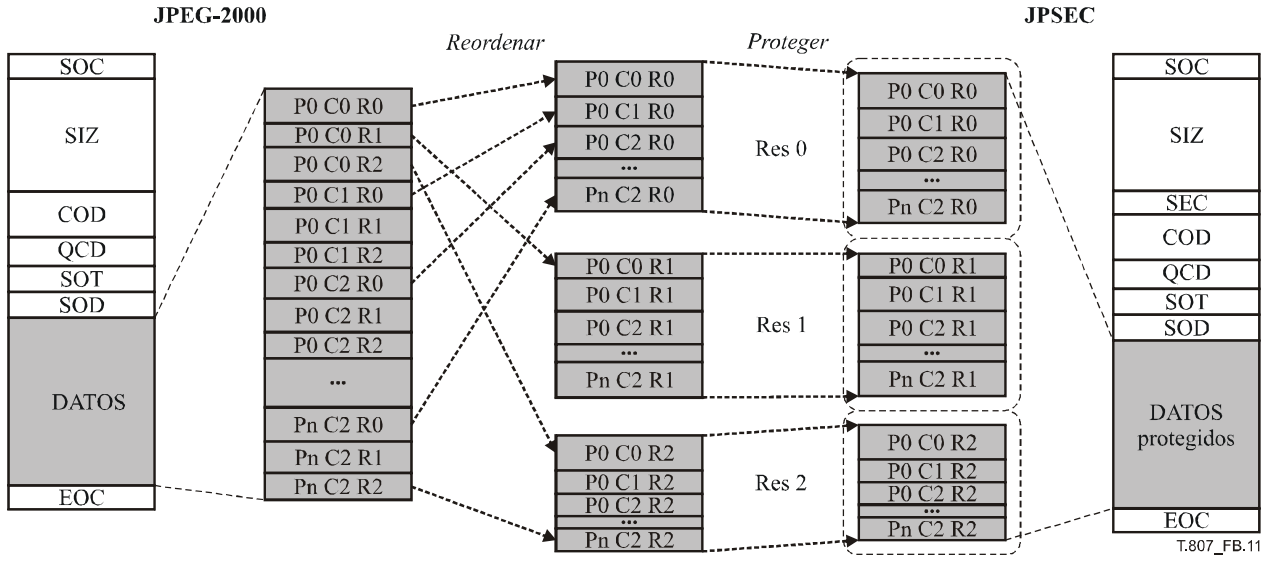


Figura B.11 – Ejemplo de construcción de un tren codificado JPSEC

B.11.3 Sintaxis del tren codificado

La sintaxis JPSEC puede utilizarse para crear un sistema de transcodificación seguro y de transmisión segura en secuencias con capacidad evolutiva utilizando para ello la herramienta de protección de plantilla. Concretamente, puede utilizarse la zona de influencia (ZOI, *zone of influence*) junto con la plantilla de descriptación, el dominio de procesamiento y la granularidad para definir completamente el proceso de descriptación que debe utilizar un cliente JPSEC autorizado para descriptar el tren. Por otra parte, los parámetros ZOI contienen la información que pueden utilizar los nodos de transcodificación para realizar la transcodificación segura.

La ZOI especifica tres zonas, una para cada resolución, y las gamas de bytes relacionadas con los bits criptados para cada zona. La sintaxis de señalización para la plantilla de protección de descriptación, el dominio de procesamiento y la granularidad se muestran en el cuadro B.27. El método de descriptación se indica en la plantilla de protección de descriptación. En este caso, se especifica criptación AES en modo CTR, así como el tamaño del bloque y la longitud de la clave. El dominio de procesamiento y la granularidad especifican con mayor detalle cómo se debe realizar la descriptación. Indica que el dominio de procesamiento es el propio tren de bits y que los encabezamientos de paquetes y el cuerpo de los paquetes están criptados. Pueden especificarse diferentes métodos de descriptación variando el dominio de procesamiento y la granularidad. Por ejemplo, la granularidad de la criptación puede aplicarse a cada uno de los paquetes por separado o sólo a los cuerpos de los paquetes. Por otra parte, el método de autenticación se especifica mediante la misma ZOI anterior, pero con la siguiente plantilla de autenticación. La sintaxis de la plantilla de autenticación se muestra en el cuadro B.28 para el caso de HMAC con SHA-1. Evidentemente, puede utilizarse también otros cifrados JPSEC y MAC. Además, la solución propuesta puede utilizarse con otras herramientas de firmas digitales, control de acceso y gestión de claves. Asimismo, puede asociarse una distorsión a cada paquete (u otra zona de datos) utilizando el campo distorsión (véase 5.7.3.2) con miras a lograr una tasa velocidad-distorsión (R-D) óptima para la transcodificación segura y la transmisión segura en secuencias [26], [27] y [28].

Cuadro B.27 – Valores de los parámetros para la herramienta de protección de plantillas, dominio de procesamiento y granularidad

Parámetro			Tamaño (bits)	Valor (en orden)	Significado
T_{decry}	ME_{decry}		8	0	El bit de emulación de marcadores NULL
	CT_{decry}		16	1	Criptación AES
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	CTR y sin relleno
		P_{bc}	2	0	No se utiliza el relleno en el modo CTR
		SIZ_{bc}	8	128	El tamaño del bloque es 128 bits
		KT_{bc}	Variable	*Plantilla de claves*	Plantilla de información sobre claves
PD			1	0_b	El segmento alineado por bytes (BAS) no figura a continuación
			1	0_b	No en el dominio de píxel
			1	0_b	No en el dominio de coeficiente de ondícula
			1	0_b	No en el dominio de coeficientes de ondícula cuantizados
			1	1_b	Procesado en el dominio de tren codificado
			3	000_b	No utilizado
G	PO		16	$0\ 0000\ 0101\ 0011\ 100_b$	El orden de procesamiento es TRLCP
	GL		8	$0000\ 1001_b$	La granularidad es la zona total identificada mediante la ZOI
V	N_V		16	1	Se especifica un solo valor
	Sv		8	16	El tamaño es de 16 bytes
	VL		128	*Valor provisional*	El valor de contador para el modo CTR

Cuadro B.28 – Valores de los parámetros para la herramienta de protección de la plantilla de autenticación

Parámetro			Tamaño (bits)	Valor (en orden)	Significado
T_{auth}	M_{auth}		8	0	MAC basado en función generadora
	P_{auth}	M_{HMAC}	8	1	HMAC
		H_{HMAC}	8	1	ID de la generación numérica es SHA-1
		KT_{HMAC}	variable	*Valor de la clave*	Véase la plantilla de claves
		SIZ_{HMAC}	16	80	El tamaño MAC es de 80 bits (truncados de los 160)

B.11.4 Conclusiones

En esta cláusula se describe la transmisión segura en secuencias y la transcodificación segura con capacidad evolutiva mediante JPSEC, lo que permite obtener las dos propiedades aparentemente conflictivas, a saber seguridad de extremo a extremo y transcodificación segura en nodos intermedios de la red. De este modo se permite la transcodificación de trenes codificados JPSEC *sin realizar la descriptación*. Además, este método permite autenticar que la transcodificación se realizó únicamente de manera válida y autorizada, y que no se produjo una modificación indeseada o voluntaria debido a un error o un ataque. Por todo lo anterior, el servidor o nodo intermediario de la red, por ejemplo un servidor intermediario (potencialmente no fiable), pueden realizar la transcodificación segura de tal manera que el consumidor JPSEC pueda autentificar que el contenido recibido se transcodificó de manera válida y autorizada.

Anexo C

Compatibilidad

(El presente anexo es parte integrante de esta Recomendación | Norma Internacional)

C.1 Parte 1

Pueden aplicarse varios métodos de protección a los trenes codificados JPEG 2000 para crear trenes codificados JPSEC que sigan siendo totalmente compatibles con la JPEG 2000 Parte 1. Utilizamos el término "conforme a la Parte 1" para referirse a los trenes codificados JPSEC para los cuales los decodificadores JPEG 2000 Parte 1, incluidos aquellos que no reconocen JPSEC tienen un comportamiento totalmente predecible.

El decodificador JPEG 2000 Parte 1 hará caso omiso de los segmentos marcadores que no reconozca. Las herramientas JPSEC, por ejemplo la herramienta normativa JPSEC para la autenticación, insertan valores de códigos de autenticación del mensaje, que se calculan a partir de los datos de JPEG 2000, en el segmento marcador SEC junto con los parámetros que describen los métodos concretos de autenticación que puede utilizar el consumidor JPSEC. Estos parámetros y valores informan al consumidor JPSEC sobre cómo verificar que el tren codificador JPSEC recibido es auténtico. Obsérvese que la herramienta de autenticación JPSEC no manipula los datos JPEG 2000. Por consiguiente, el decodificador JPEG 2000 Parte 1 que recibe este tren codificado JPSEC comenzará a decodificar el tren JPSEC, haciendo caso omiso del segmento marcador SEC, y seguirá decodificando el tren JPSEC como si se tratara de un tren JPEG 2000 Parte 1. La herramienta normativa JPSEC para la autenticación tiene estas mismas características y por consiguiente resulta en un tren codificado conforme a la Parte 1.

JPSEC permite la criptación y descriptación de trenes codificados JPEG 2000 y JPSEC. Cuando se utiliza la criptación, los datos JPEG 2000 se modifican. En sentido estricto, la conformidad con la Parte 1 no es posible con los trenes criptados dado que lo más probable es que el decodificador JPEG 2000 Parte 1 observará valores ilícitos. Una posible manera de resolver o al menos mitigar este problema es utilizar las capacidades de recuperación de errores de JPEG 2000. Gracias a la recuperación de errores se podrá disponer de trenes codificados JPSEC criptados para los que los decodificadores JPEG 2000 de Parte 1 tendrán un comportamiento predecible.

JPESC dispone de un campo paramétrico P_{sec} que contiene parámetros de seguridad para todo el tren codificado. En particular, el bit F_{J2K} que puede ponerse a 1 para indicar que el tren codificado JPSEC es decodificable por decodificadores JPEG 2000 Parte 1. El creador JPSEC puede configurar este parámetro al aplicar las herramientas JPSEC al tren codificado JPEG 2000. Como se dijo anteriormente, el creador JPSEC puede aceptar como entrada un tren codificado JPSEC protegido. Si el creador JPSEC recibe un tren codificado JPSEC de entrada cuyo bit F_{J2K} está configurado para indicar la conformidad con la Parte 1 y luego aplica una herramienta JPSEC que causa la pérdida de la conformidad con la Parte 1, deberá poner a 0 el bit F_{J2K}.

Para los trenes JPSEC que no son conformes con la Parte 1, se recomienda utilizar la extensión de fichero .jp2s para indicar que el decodificador JPEG 2000 Parte 1 quizá no pueda decodificar el tren codificado protegido.

C.2 Parte 2

Puede utilizarse la enmienda 2 de la Parte 2 de JPEG 2000 relativa al segmento marcador de capacidades ampliadas (CAP) para indicar que se utiliza JPSEC. Concretamente, la Parte 2 utiliza el parámetro R_{siz} para indicar la presencia del segmento marcador CAP que contiene el parámetro C_{cap} el cual puede utilizarse para indicar qué partes de JPEG 2000 se utilizan en el tren codificado. Es posible verificar que se utiliza JPEG 2000 Parte 8 (JPSEC) poniendo a 1 el bit adecuado de C_{cap}.

Por consiguiente, el creador JPSEC puede configurar el parámetro R_{siz} para indicar la presencia del segmento marcador CAP. Asimismo, puede insertar o editar el segmento marcador CAP para indicar en el parámetro C_{cap} que se utiliza la Parte 8.

C.3 JPIP

C.3.1 Relación general entre JPIP y JPSEC

JPIP especifica un protocolo que consiste en una serie estructurada de interacciones entre un cliente y un servidor mediante las cuales se intercambian a través de una comunicación eficiente metadatos y la estructura del fichero de imágenes y la totalidad o una parte de los trenes codificados de imágenes.

JPIP puede adaptarse mediante diversas ampliaciones del formato de fichero JPEG 2000, como se define en la Rec. UIT-T T.801 | ISO/CEI 15444-2, Rec. UIT-T T.802 | ISO/CEI 15444-3 y Rec. UIT-T T.805 | ISO/CEI 15444-6. Ahora bien, para lograr un grado de interactividad sencillo que permita transferir partes de un fichero o tren codificado JPEG 2000, esas otras capacidades no son obligatorias.

Se han incluido disposiciones para la ampliación de protocolos JPIP a fin de dar soporte a las normas JPEG 2000 actuales, Rec. UIT-T T.802 | ISO/CEI 15444-3, JPEG 2000 para imágenes de movimiento y Rec. UIT-T T.805 | ISO/CEI 15444-6, documentos compuestos, y las futuras partes JPEG 2000 (actualmente JP3D, JPSEC y JPWL).

JPSEC ofrece servicios de seguridad para imágenes JPEG 2000. La sintaxis JPSEC soporta dos tipos de marcadores, a saber, SEC e INSEC. El encabezamiento principal del tren de bits JPSEC puede contener uno o varios marcadores SEC. Es decir, JPSEC se basa en un tren codificado JPEG 2000, en el que se modifica el encabezamiento principal JPEG 2000 para crear un nuevo "encabezamiento principal" JPSEC y se modifican también los correspondientes trenes de datos JPEG 2000 para crear, en su caso, un nuevo tren de datos protegido. Los marcadores INSEC pueden aparecer como opción en la parte "datos" del tren de datos. Estos marcadores especifican parámetros "de menor tamaño" o "de zona local" comparados con el marcador SEC y pueden utilizarse para complementar el marcador SEC.

Cabe observar que JPIP se encuentra justo después de la capa de transporte, mientras que JPSEC está en la capa de aplicación. Visto de este modo, JPIP ofrece un servicio de transporte a JPSEC. Es decir, JPIP ofrece herramientas eficaces para la transmisión de información de imágenes, incluido el encabezamiento principal (todos los marcadores) y los trenes codificados, entre servidores y clientes. En esta cláusula se describe cómo puede utilizarse JPIP para transportar contenido JPSEC.

C.3.2 Aspectos específicos de la interactividad entre JPIP y JPSEC

En esta subcláusula se describen los aspectos que deben tener en cuenta el transmisor y el receptor JPIP para transportar contenido JPSEC.

En A.3.5 "Bin de datos del encabezamiento principal" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, los dos tipos de medios de trenes JPP y JPT utilizan los bines de datos del encabezamiento principal. Estos bins de datos consisten en una lista consecutiva de todos los marcadores y segmentos marcadores en el encabezamiento principal, comenzando por el marcador SOC. No contiene los marcadores SOT, SOD o EOC. Ahora bien, el encabezamiento principal de JPEG 2000 tampoco contiene el marcador SEC y su segmento. Por esa razón, en A.3.5 de JPIP FCD 2.0 no se especifica cómo utilizar el segmento marcador SEC especificado en JPSEC. Así pues, es necesario modificar el transmisor y receptor JPIP para que reconozcan los segmentos marcadores SEC que figuran en el encabezamiento principal de un tren codificado JPSEC.

En A.3.2 "Bins de datos de prerecinto" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, se describe cómo utilizar datos de precinto. Ahora bien, en A.3.2 de JPIP FCD 2.0 no se especifica que pueda utilizarse el marcador INSEC y su segmento especificado en JPSEC. Por consiguiente, es necesario modificar el transmisor y receptor JPIP para que reconozcan el segmento marcador INSEC que pudiera aparecer en la parte de datos de un tren codificado JPSEC.

En A.3.3 "Bins de datos del encabezamiento losa" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, los bins de datos del encabezamiento losa figuran únicamente dentro del tipo de medios de tren JPP. Para los bins de datos que pertenezcan a esta clase, el identificador dentro de la clase contiene el índice (comenzando desde 0) de la losa a la que se refieren los bins de datos. Estos bins de datos consisten en marcadores y segmentos marcadores de la losa n. No deben contener segmento marcador SOT alguno. La inclusión de segmentos marcadores SOD es opcional. Los bins de datos pueden crearse a partir del tren codificado legal, mediante la concatenación de todos los segmentos marcadores, excepto SOT y POC, en todos los encabezamientos de parte losa para la losa n.

En A.3.4 "Bins de datos de losa" de la Rec. UIT-T T.808 | ISO/CEI 15444-9, se indica que los bins de datos deben utilizarse únicamente en medios de tipo tren JPT. Para los bins de datos que pertenecen a esta clase, el identificador dentro de la clase es el índice (comenzando desde 0) de la losa a la cual pertenece el bin de datos. Cada bin de datos de losa corresponde a la cadena de bits formada por la concatenación de todas las partes losa que pertenecen a la losa, en orden, además de su SOT, SOD y todos los segmentos marcadores pertinentes.

Como se indicó anteriormente, en A.3.4 y A.3.5 de la Rec. UIT-T T.808 | ISO/CEI 15444-9 se describe la utilización del encabezamiento de parte losa y los datos de parte losa. Ahora bien, en estas cláusulas no se especifica si se soportan segmentos marcadores SEC y segmentos marcadores INSEC. Por consiguiente, debe modificarse el transmisor y receptor JPIP para reconocer y transportar estos segmentos marcadores junto con los datos protegidos.

C.3.3 Resumen

En términos generales, JPSEC resulta adecuado para el transporte mediante JPIP. El marcador INSEC se utiliza en el tren codificado para describir algunas partes "pequeñas" de datos específicas que están protegidas mediante herramientas de seguridad. De este modo se consigue que JPSEC sea más flexible. Para mejorar la robustez de INSEC, la capa de servicio (en este caso JPIP) debe facilitar una buena calidad de servicio o protección en el marcador INSEC y sus segmentos. Para lograr este objetivo, es necesario resolver ciertos problemas de JPIP y JPSEC y garantizar la interactividad entre ambos.

C.4 JPWL

La norma JPEG 2000 inalámbrica o JPWL (Rec. UIT-T T.810 | ISO/CEI 15444-11) amplía la especificación básica de JPEG 2000 para lograr la transmisión eficaz de imágenes JPEG 2000 por un entorno de transmisión propenso a errores. Concretamente, la JPWL define un conjunto de herramientas y métodos para proteger el tren codificado contra errores de transmisión. Asimismo, define mecanismos para describir la sensibilidad del tren codificado a errores de transmisión y las posiciones en el tren codificado que contienen errores de transmisión residuales.

JPWL versa particularmente sobre la protección del encabezamiento de la imagen, los códigos de corrección de errores en recepción (FEC, *forward error correcting*), la protección desigual contra errores (UEP, *unequal error protection*), la codificación conjunto de origen y canal, la partición y entrelazado de datos y la codificación aritmética robusta. JPWL no está vinculada a una red o protocolo de transporte específicos, sino que ofrece una solución genérica para la transmisión robusta de imágenes JPEG 2000 por redes propensas a errores.

Las principales funciones de JPWL son:

- proteger el tren codificado contra errores de transmisión,
- indicar el grado de sensibilidad de las diferentes partes del codificado a errores de transmisión, y
- especificar las posiciones de los errores residuales en el tren codificado.

El JPWL define cuatro segmentos marcadores, a saber, la capacidad de protección contra errores (EPC, *error protection capability*), el bloque de protección contra errores (EPB, *error protection block*), el descriptor de sensibilidad a errores (ESD, *error sensitivity descriptor*) y el descriptor de errores residuales (RED, *residual error descriptor*).

El segmento marcador EPC indica qué herramientas normativas e informativas de JPWL se utilizan en el tren codificado. Concretamente, el EPC indica si el tren codificado contiene los otros tres segmentos marcadores normativos definidos por JPWL, a saber, el descriptor de sensibilidad a errores (ESD), el descriptor de errores residuales (RED) y el bloque de protección contra errores (EPB). Por otra parte, el EPC indica la utilización de herramientas informativas que se habían registrado previamente en la RA JPWL. El EPC debe figurar obligatoriamente en el tren codificado JPWL.

La función primordial del EPB es proteger el encabezamiento principal y de parte losa. No obstante, también puede utilizarse para proteger el resto del tren codificado. El segmento marcador EPB contiene información sobre los parámetros de protección contra errores y los datos sobre redundancia utilizados para proteger el tren codificado contra errores.

El segmento marcador ESD contiene información sobre la sensibilidad a errores del tren codificado. Esta información puede emplearse al aplicar la técnica de protección desigual contra errores (UEP). Es decir, se utilizan códigos más potentes para proteger las partes más sensibles del tren codificado. Esta información también puede utilizarse para la retransmisión selectiva. Por último, la información contenida en el ESD también podría utilizarse en otras aplicaciones no JPWL, tales como la transcodificación a velocidad eficaz o la prebúsqueda inteligente.

El segmento marcador RED indica la presencia de errores residuales en el tren codificado. En realidad, puede suceder que el decodificador JPWL no sea capaz de corregir todos los errores del tren codificado. El RED permite indicar la posición de esos errores residuales. Esta información puede utilizarse después en el decodificador JPEG 2000 para tener en cuenta estos errores. Por ejemplo, el decodificador podría solicitar la retransmisión, ocultar los errores o descartar la información corrupta.

C.4.1 Relación en general entre JPWL y JPSEC

La combinación de JPWL y JPSEC es necesaria siempre que las imágenes JPEG 2000 tengan que protegerse y transmitirse por un canal inalámbrico propenso a errores.

En el lado transmisor, la sensibilidad a errores JPWL se genera normalmente durante la codificación JPEG 2000. Posteriormente se aplica en las herramientas JPSEC al tren codificado para protegerlo. Por último, las herramientas de codificación JPWL se utilizan para mejorar la robustez del tren codificado en cuanto a errores de transmisión.

En el lado receptor, se aplican en primer lugar las herramientas de decodificación JPWL para corregir los posibles errores de transmisión. En esta fase, la JPWL también puede generar información relativa a errores residuales. Por último, se aplican las herramientas JPSEC para satisfacer la necesidad de los servicios de seguridad seleccionados.

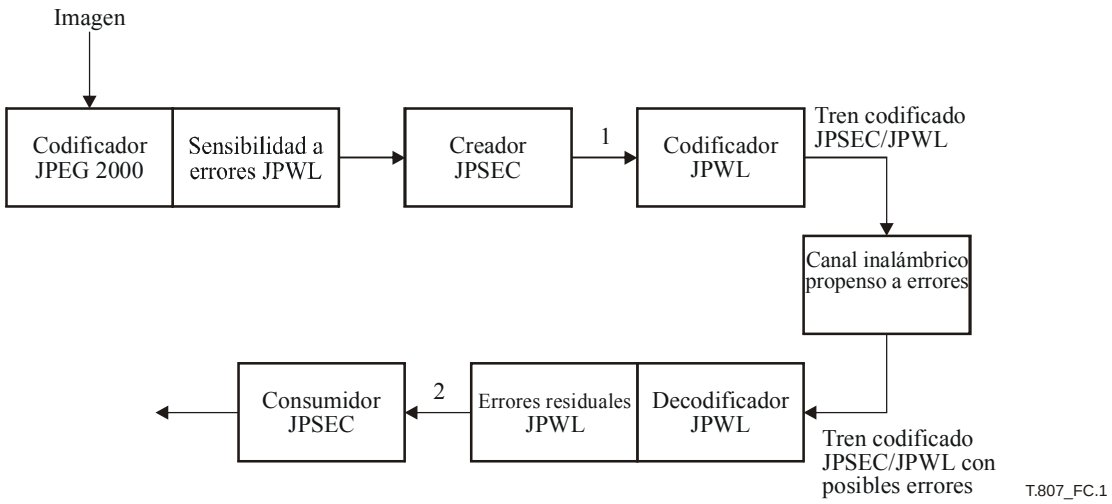


Figura C.1 – Combinación característica de JPWL y JPSEC

C.4.2 Asuntos específicos relacionados con la compatibilidad entre JPWL y JPSEC

Cabe tener presente una serie de problemas de compatibilidad entre JPWL y JPSEC, que se enumeran a continuación:

1) Capacidad de protección contra errores JPWL (EPC): la presencia de este segmento marcador afecta a gamas de byte. Obsérvese que este segmento marcador es obligatorio en los trenes codificados JPWL.

2) Bloque de protección contra errores JPWL (EPB): este segmento marcador se añade normalmente en la última fase de la transmisión y es lo primero que suprime el receptor. En principio no debería afectar a JPSE.

3) Descriptor de la sensibilidad de errores JPWL (ESD): este segmento marcador se añade normalmente durante la codificación JPEG 2000 Parte 1, en cuyo caso deberá ser transparente a las subsiguientes operaciones JPSEC. Sin embargo, JPSEC podría afectar negativamente a la utilización de ESD en JPWL. En particular, JPSEC no debería cambiar las gamas de bytes en caso de que el ESD las utilice. Además, las operaciones JPSEC no deberían afectar a los valores de distorsión; de lo contrario la información contenida en el ESD resultaría irrelevante. En este último caso, el creador JPSEC tiene la opción de suprimir el segmento marcador ESD.

4) Descriptor de errores residuales JPWL (RED): este segmento marcador puede insertarse después de la decodificación JPWL. Por consiguiente, puede afectar a las gamas de byte JPSEC. También puede tener incidencia en las técnicas de autenticación JPSEC. En el caso de que se corrompa el tren codificado, la información RED puede resultar útil para el consumidor JPSEC a fin de manipularlo adecuadamente.

5) JPSEC SEC: la presencia de este segmento marcador afecta a las gamas de byte. Obsérvese que este segmento marcador es obligatorio en el tren codificado JPSEC.

6) JPSEC INSEC: la presencia de este segmento marcador afecta las gamas de byte. Obsérvese que este segmento marcador figura en los datos del tren codificado.

En el caso en que no se produzcan errores residuales, el codificador y decodificador JPWL deberían ser en teoría transparentes. En otras palabras, en este caso los trenes en los puntos 1 y 2 de la figura anterior deberían ser totalmente idénticos.

Como recomendación general, cuando se utilice junto con JPWL, es preferible que JPSEC utilice las gamas de byte justo después del marcador SOD a fin de reducir los problemas con las gamas de byte. Además, es preferible restringir la presencia de segmentos marcadores JPWL al encabezamiento principal a fin de evitar su presencia en los encabezamientos de parte losa.

Anexo D

Declaración de patentes

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

NOTA – El anexo D es un anexo de la ISO/CEI únicamente. En la base de datos sobre DPI figura una lista de las empresas que han presentado declaraciones de patentes que conciernen a la UIT. Véase http://itu.int/ITU-T/ipr/.

La Organización Internacional de Normalización (ISO, *International Organization for Standardization*) y la Comisión Electrotécnica Internacional (CEI, *International Electrotechnical Commission*) desean poner de manifiesto que alegar la conformidad con esta parte de ISO/CEI 15444 puede implicar la utilización de patentes.

La ISO y la CEI se mantienen al margen en lo que respecta a la existencia, validez y alcance de estos derechos de patente.

Los titulares de estos derechos de patente han garantizado a la ISO y a la CEI que están abiertos a la negociación de licencias de manera razonable y no discriminatoria para todo aquel que lo solicite desde cualquier parte del mundo. A este respecto, las declaraciones de los titulares de estos derechos de patente están registradas con la ISO y la CEI. Puede obtenerse información al respecto de las empresas que se enumeran a continuación.

Obsérvese que existe la posibilidad de que algunos elementos de esta parte de ISO/CEI 15444 estén sujetos a derechos de patentes distintos de los indicados en este anexo. La ISO y la CEI no se hacen responsables en ningún caso de indicar algunos o todos los derechos de patente.

Cuadro D.1 – Lista de declaraciones

Número	Empresa
1	Canon Inc.
2	Columbia University
3	EMITALL Surveillance
4	HP
5	Institute for Infocomm Research
6	MediaLive
7	New Jersey Institute of Technology

BIBLIOGRAFÍA

[1] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

ISO/CEI 7498-2:1989, *Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[2] ISO/CEI 9796-2:2002, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*.

[3] ISO/CEI 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

[4] ISO/CEI 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General*.

[5] ISO/CEI 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*.

[6] ISO/CEI 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher*.

[7] ISO/CEI 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

[8] ISO/CEI 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*.

[9] ISO/CEI 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*.

[10] ISO/CEI 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*.

[11] ISO/CEI 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.

[12] ISO/CEI 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*..

[13] ISO/CEI TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*.

[14] ISO/CEI 14888-1:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

[15] ISO/CEI 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

[16] ISO/CEI 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 2 – Digital signatures*.

[17] ISO/CEI 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 3 – Key establishment*.

[18] ISO/CEI 15946-4:2004, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 4 – Digital signatures giving message recovery*.

[19] ISO/CEI 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.

[20] ISO/CEI 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[21] ISO/CEI 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*.

[22] DWORKIN (Morris): Recommendation for Block Cipher Modes of Operation, Methods and Techniques, *NIST Special Publication 800-38A*.

[23] GROSBOIS (R.), GERBELOT (P)., EBRAHIMI (T.): Authentication and access control in the JPEG 2000 compressed domain, *In Proc. of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV*, San Diego, 29 julio- 3 de agosto de 2001.

[24] http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html, Java Cryptography Architecture API Specification and reference.

[25] RIVEST (R.L.), SHAMIR (A.), ADLEMAN (L.M.): A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM (2) 21*, 1978, Page(s): 120-126.

[26] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Video Streaming for Wireless Networks, *IEEE Inter. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, marzo de 2001. Also available at www.hpl.hp.com/personal/John_Apostolopoulos/papers/SecureScalableStreaming_ICASSP01.pdf.

[27] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming Enabling Transcoding Without Decryption, *IEEE Inter. Conf. on Image Processing (ICIP)*, http://lib.hpl.hp.com/techpubs/2001/HPL_2001_320.html septiembre de 2001.

[28] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming and Secure Transcoding with JPEG 2000, *IEEE Inter. Conf. on Image Processing (ICIP)*, septiembre de 2003. http://lib.hpl.hp.com/techpubs/2003/HPL-2003-117.html

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	**Terminales para servicios de telemática**
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007