国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

T.807

(05/2006)

T系列：远程信息处理业务的终端设备

信息技术 — JPEG 2000图像编码系统：安全的JPEG 2000

ITU-T T.807建议书

国际电信联盟

国际标准 ISO/IEC 15444-8
ITU-T T.807建议书

信息技术 — JPEG 2000图像编码系统：安全的JPEG 2000

摘　要

本建议书 | 国际标准的目标是提供一种语法，允许安全服务应用到 JPEG 2000 编码的图像数据上。安全服务包括机密性，完整性验证，源认证，条件访问，以及安全的可扩展流化和安全的代码转换。该语法允许这些安全服务应用到已编码的和未编码的部分图像数据，或全部图像数据上。当在 JPEG 2000 的固有特性元素上提供安全服务时，它还可以维持 JPEG 2000 的固有特性，如可扩展性，可访问到不同的空间区域，分辨率级别，色彩分量，以及质量层次等。

来　源

ITU-T 第 16 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2006 年 5 月 29 日批准了 ITU-T T.807 建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目 录

引言

在“数字化时代”，互联网为权利所有人提供了许多新的机会，可以使其著作（书、视频、音乐、图像等）进行电子化发行。

而与此同时，新的信息技术也从根本上简化了用户对内容的访问。与之同时出现的是盗版数字拷贝 — 具有与原作相同的质量 — 的普遍问题，以及在对等网络中的“文件共享”，这使得关于内容工业损失严重的持续诉求在不断地增长。

世界知识产权组织（WIPO）及其成员国（170 个）发挥了重要的作用，以便确保版权以及它所鼓励的文化的和智力的表现形式，在 21 世纪都能够得到良好地保护。 世界上每个国家的新数字经济，以及具有创造性的人们都将依赖于它。此外，在 1996 年 12 月，WIPO 版权条约（WCT）发布，其中有两个重要的条款（第 11 条和第 12 条）涉及了关于版权管理信息的技术措施和职责：

第 11 条

关于技术措施的义务

缔约各方应规定适当的法律保护和有效的法律补救办法，制止规避由作者为行使本条约或《伯尔尼公约》所规定的权利而使用的、对就其作品进行未经该有关作者许可或未由法律准许的行为加以约束的有效技术措施。

第 12 条

关于版权管理信息的义务

(1) 缔约各方应规定适当和有效的法律补救办法，制止任何人明知、或就民事补救而言有合理根据知道其行为会诱使、促成、便利或包庇对本条约或《伯尔尼公约》所涵盖的任何权利的侵犯而故意从事以下行为；

(i) 未经许可去除或改变任何权利管理的电子信息。

(ii) 未经许可发行、为发行目的进口、广播、向公众传播明知已被未经许可去除或改变权利管理电子信息的作品或作品的复制品。

(2) 本条中的用语“权利管理信息”系指识别作品、作品的作者、对作品拥有任何权利的所有人的信息，或有关作品使用的条款和条件的信息，和代表此种信息的任何数字或代码，各该项信息均附于作品的每件复制品上或在作品向公众进行传播时出现。

该条约为保护知识产权提供了一种坚实的基础。在 2004 年，大约有 50 个国家认可了该条约。因此，期望在 JPEG 2000 中推荐的工具和保护方法必须能够确保事务的安全性，并对内容进行保护（IPR），对技术进行保护等。

安全问题，如认证，数据完整性，版权保护和知识产权保护，私密性，条件访问，机密性，事务跟踪等仅仅是列举了一小部分，在 JPEG 2000 作为目标的许多成像应用中都是重要特性之一。

对保护数字内容的技术方法进行了描述，这可以通过多种途径获得，例如数字水印，数字签名，加密，元数据，认证以及完整性检测等。

JPEG 2000 标准的第 8 部分计划以规范的方式提供工具和解决方案，来允许应用程序产生、使用、并交换安全的 JPEG 2000 码流。这被称为是 **JPSEC**。

国际标准
ITU-T建议书

信息技术 — JPEG 2000图像编码系统：安全的JPEG2000

1 范围

本建议书 | 国际标准为保护 JPEG 2000 码流规定了框架、概念和方法。本建议书 | 国际标准的范围是要定义：

1） 一个标准的码流语法，其中包含了解释安全图像数据的信息；

2） 一个标准的注册JPSEC工具的过程，同时注册机构将发布一个唯一的标识符；

3） JPSEC工具在典型应用案例中的参考性示例；

4） 关于如何实现安全服务及其相关元数据的参考性指南。

本建议书 | 国际标准的范围没有描述特定的安全成像应用，也没有为安全成像限制特定的技术，但是创建了一个框架，使得安全成像技术可以进一步地演进扩展。

2 规范性参考文献

下列建议书和国际标准中的条款，在本建议书 | 国际标准中的引用而构成本建议书 | 国际标准的条款。在出版时，所指出的版本是有效的。所有的建议书和国际标准均会得到修订，本建议书 | 国际标准的使用者应查证是否有可能使用下列建议书 | 国际标准的最新版本。IEC 和 ISO 的各成员有目前有效的国际标准的目录。国际电联电信标准化局有目前有效的 ITU-T 建议书的清单。

– ITU-T Recommendation T.800 (2002) | ISO/IEC 15444-1:2004, *Information technology – JPEG 2000 image coding system: Core coding system.*

– ITU-T Recommendation T.801 (2002) | ISO/IEC 15444-2:2004, *Information technology – JPEG 2000 image coding system: Extensions.*

3 术语和定义

就本建议书 | 国际标准而言，下列定义适用。ITU-T T.800 建议书 | ISO/IEC 15444-1 的第 3 节中定义的定义适用于本建议书 | 国际标准。

3.1 access control 访问控制：防止对资源的未授权使用，包括防止以某种未授权方式来使用资源。

3.2 authentication 认证：对某个系统实体所声明的身份进行验证的过程。

3.2.1 source authentication 源认证：验证一个源实体（也称为用户/参与方）实际上是不是被声明的源实体。

3.2.2 fragile/semi-fragile image authentication 脆弱/半脆弱性图像认证：对图像源认证和图像数据/图像内容完整性验证的过程，应当能够检测到信号的任何变化，并能够标识出在哪里发生了变化，以及在变化前信号可能是什么样的。

注 — 它主要作用是提供对某个文档的认证。脆弱性图像认证和半脆弱性图像认证的区别在于，前者是对图像数据的完整性进行验证，而后者是对图像内容的完整性进行验证。

3.3 confidentiality 机密性：一种特性，即信息不能对未授权的个人、实体或过程可用，或者不能泄漏给未授权的个人、实体或过程。

3.4 data splitting 数据分割：通过对数据加密并将其存储在处于不同服务器的文件的不同部分，以此来保护敏感数据不被未授权访问的一种方法。

注 — 当分割后的数据被访问时，各部分将被获取、组合并解密。一个未授权个人需要知道包含各部分数据的服务器的位置，并能够访问到每个服务器，知道什么数据要组合，并知道如何对其进行解密。

3.5 decryption, deciphering 解密：加密的相反转换。

3.6 digital signature 数字签名：将数据附加在数据单元上，或者对数据单元执行一个密码学的转换，以便允许数据单元的接收者来验证数据单元的源和完整性，并且保护不被伪造，如被接收者伪造。

3.7 encryption 加密：通过某种密码学算法来产生密文的一种可逆的转换，即隐藏了数据的信息内容。

注 — 加密算法的一个可替换术语是密码（cipher）。

3.8 fingerprints 指纹：一个对象的特征，可以将其从其他类似的对象中区分开来，使得对象的拥有者可以跟踪授权用户是否非法地将其分发。

注 — 在这一方面，指纹常常在叛逆者追踪问题的上下文中被讨论。

3.9 hash function 哈希函数：将比特串映射为固定长度的比特串的函数，满足下面两个特性：

注 — 对于一个给定的输出，要找到一个输入来映射到此输出上，在计算上是不可行的。对于一个给定的输入，要找到第二个输入可以映射到相同的输出上，在计算上也是不可行的。计算的不可行性依赖于用户特定的安全需求和环境。

3.10 integrity 完整性：可用于保护资产的准确性和完全性的一种特性。

3.10.1 image data integrity 图像数据完整性：数据未以一种未授权方式被修改或被破坏的特性。

3.10.2 image content integrity 图像内容完整性：在图像的感知到的含义被修改后，确保图像内容没有被未授权方修改。

注 — 允许对图像执行内容保留操作，而不触发完整性告警。

3.11 JPSEC application JPSEC 应用：为了提供指定的安全服务，通过解释 JPSEC 语法有能力处理 JPSEC 码流的任何软件或硬件过程。

注 — 一个JPSEC应用可使用一个或多个JPSEC工具。

示例 — 一个JPSEC应用能够读取加密后的JPSEC码流，当获得适当的密钥后对其进行解密，并且能够恢复出JPEG 2000原始的明文的图像数据。

3.12 JPSEC codestream JPSEC 码流：使用 JPEG 2000 编码和 JPSEC 安全工具对某个图像进行编码和保护而形成的比特序列。

3.12.1 JPSEC creator JPSEC 创建者：为了提供某些 JPSEC 服务，而根据一个图像，一个 JPEG 2000 码流或其他 JPSEC 码流而创建了一个 JPSEC 码流的实体。

3.12.2 JPSEC consumer JPSEC 消费者：接收到一个 JPSEC 码流，并且根据此码流恢复一个 JPSEC 服务的实体。

3.13 JPSEC service JPSEC 服务：为 JPEG 2000 图像的处理提供了安全性的一种服务。 该服务对安全攻击进行反击，并且使用了一个或多个 JPSEC 工具。

3.14 JPSEC registration authority JPSEC 注册机构：一个实体，负责为标识一个 JPSEC 工具而发放一个唯一的 ID，并且负责对描述 JPSEC 工具的参数列表进行存储。

3.15 JPSEC tool JPSEC 工具：使用安全技术来实现某个安全服务的硬件或软件过程。

3.15.1 JPSEC normative tool JPSEC 标准工具：使用本建议书 | 国际标准的标准部分所规定的预先定义的工具模板进行解密，认证或哈希（散列）的 JPSEC 工具。

3.15.2 JPSEC non-normative tool JPSEC 非标准工具：由 JPSEC 注册机构或某个用户自定义应用给定的某个标识号所规定的 JPSEC 工具。

3.15.3 JPSEC user-defined tool JPSEC 用户自定义工具：由某个用户自定义应用定义的一种 JPSEC 非标准工具。

3.15.4 JPSEC registration authority tool JPSEC 注册机构工具：由 JPSEC 注册机构定义的一种 JPSEC 非标准工具。

3.16 JPSEC tool description JPSEC 工具描述：对 JPSEC 工具所使用的参数的一种描述。

注 — 然而，JPSEC工具描述不能描述所使用的算法或方法。一个JPSEC工具描述由两部分组成：参数列表及其取值。在JPSEC标准工具情况下，参数列表由本标准给定。在JPSEC非标准工具的情况下，参数列表可能由注册机构给定。在这两种情况下，参数列表都在SEC标记段和INSEC标记段中指定。

3.17 key 密钥：可以控制加密和解密操作的符号序列。

3.17.1 symmetric keys 对称密钥：一对密钥，为了这对密钥，发起者和接收者都使用同一个私密密钥，或者使用两个密钥，但这两个密钥在一个密码系统中可以通过彼此很容易计算出来。

3.17.2 asymmetric key pair 非对称密钥对：一对相关联的密钥，其中私钥定义了私密变换，而公钥定义了公共变换。

3.17.2.1 private key 私钥：某个实体的非对称密钥对中的密钥，该密钥不能被泄漏。

3.17.2.2 public key 公钥：某个实体的非对称密钥对中的密钥，该密钥可以被公开。

3.18 key generation, key generating function 密钥生成，密钥生成功能：一种功能，该功能将多个参数作为输入，其中至少有一个应当是私密的，并且将一个对应于所使用的算法和应用的密钥作为输出。

注 — 该功能应当具有一种特性，即如果之前不知道私密输入的情况下，是不可能通过计算推导出输出的。

3.19 key management 密钥管理：根据某个安全策略，对密钥进行的生成、存储、分发、删除、归档和应用。

3.20 marker emulation 标记竞争：由于加密过程而产生的密文，且包含了一个 JPEG 起始编码。

3.21 message authentication code algorithm, cryptographic check function, cryptographic checksum function 消息认证码算法，密码校验功能，密码校验和功能：计算某个功能的算法，该算法将比特流和一个密钥映射为一个固定长度的比特流，并且满足下列两个特性：

- 对于任意密钥和任意输入串，该功能都能够进行有效计算；
- 对于任何固定密钥，如果没有预先给定关于密钥的知识，则要根据任意新输入的串来计算出功能值在计算上是不可行的，即使给定了输入串集合以及相应的功能值的知识在计算上也是不可行的，如，第i个输入串的值可能是在观察到前面的第i－1个功能值后才被选择的。

注 — 计算的可行性依赖于用户的特定安全需求和环境。

3.21.1 message authentication code (MAC) 消息认证码（MAC）：作为某个 MAC 算法的输出的比特流。

3.22 non-repudiation 不可否认：将某个实体与其参与的事务绑定起来，这样事务在以后就不会被否定（否认）。

注 — 也就是说，某个事务的接收者能够向某中立的第三方证明所声明的发送者确实发送了此事务。

3.23 packet 包：JPEG 2000 第一部分比特流中的一部分，其组成包括一个包头和压缩的图像数据，该图像数据来自一个拼贴组件的一个分辨率的一个选区的一层。

注 — 此定义不同于通过网络进行数据传输时使用的术语“包”。

3.24 protection 保护：让内容安全的过程。

3.24.1 protection template 保护模板：某种保护方法的操作所必需的模板或参数字段的列表。

3.24.2 protection method 保护方法：用于创建或处理被保护内容的方法，如加密、解密、认证和完整性验证。

3.25 security 安全：与定义、实现并维护机密性、完整性、可用性、责任制和可靠性相关的全部方面。

注 — 一个产品、系统或服务被认为是安全的，其扩展的含义可以是其用户可以信赖它是以一种计划好的方式运行（或将要运行）的。这常常在对实际的或感知到的威胁进行评估时的上下文中考虑。

3.26 signalling syntax 信号化语法：对 JPSEC 码流格式的规范，包含了处理安全的 JPEG 2000 图像所需要的所有信息。

3.27 transcoding 代码转换：一种操作，将压缩的码流作为输入，并且通过对其进行适配或转换来产生一个压缩码流作为输出，并具有某些期望的特性。

示例 — 输出的压缩码流与输入的压缩码流相比，可能表示一种具有更低空间分辨率或更低比特率的图像。

3.27.1 secure transcoding 安全的代码转换：对一个被保护的输入的压缩内容执行代码转换或适配操作，而不需要对内容进行解保护。

注 — 使用术语“安全的代码转换”，相对比于“代码转换”，主要是要强调在执行代码转换操作时没有危及到安全。安全的代码转换也可能指的是在一个加密域内执行代码转换。

3.28 watermark 水印：为了传送隐藏的数据，不被感知地加入到封面信号中的信号。

3.28.1 watermarking 加水印：不被感知地将表示某些信息的数据插入到多媒体数据中的过程，采用下面两种方法之一：

- 有损耗的方法，意味着一旦加入水印，将不能够恢复准确的封面信号。
- 无损耗的方法：意味着在提取出水印后，还可以恢复准确的封面信号。

4 符号和缩写

就本建议书 | 国际标准而言，下列缩写适用。

BAS	字节对齐段
FBAS	字段字节对齐段
G	粒度
GL	粒度级别
INSEC	内部码流安全标记
IP	关于技术的知识产权
IPR	关于内容的知识产权
JPSEC	安全的JPEG 2000
KT	密钥模板
LSB	最低有效位
MAC	消息认证码
MSB	最高有效位
PD	处理域
PKI	公钥基础设施
PO	处理顺序
RA	注册机构
RBAS	范围字节对齐段
SEC	安全标记
T	模板
V	值
VL	值列表
ZOI	影响区

5 JPSEC语法（标准的）

5.1 JPSEC框架概述

JPSEC 为保护 JPEG 2000 编码的数据定义了一个框架。本建议书 | 国际标准的核心是给出安全的 JPEG 2000 图像的语法规范，即 *JPSEC 码流*。该语法的目标是 JPEG 2000 编码的数据，并允许对全部码流或部分码流进行保护。在所有情形下，被保护的数据（即 JPSEC 码流）必须遵循本建议书 | 国际标准所定义的标准语法。

JPSEC 码流与多个 *JPSEC 安全服务*相关联，包括机密性与源和内容的认证。

信号化语法规定了：

— 哪些安全服务与图像数据相关联；

— 要求使用哪些*JPSEC*工具来发布相应的服务；

— 如何应用JPSEC工具；

— 哪部分图像数据被保护。

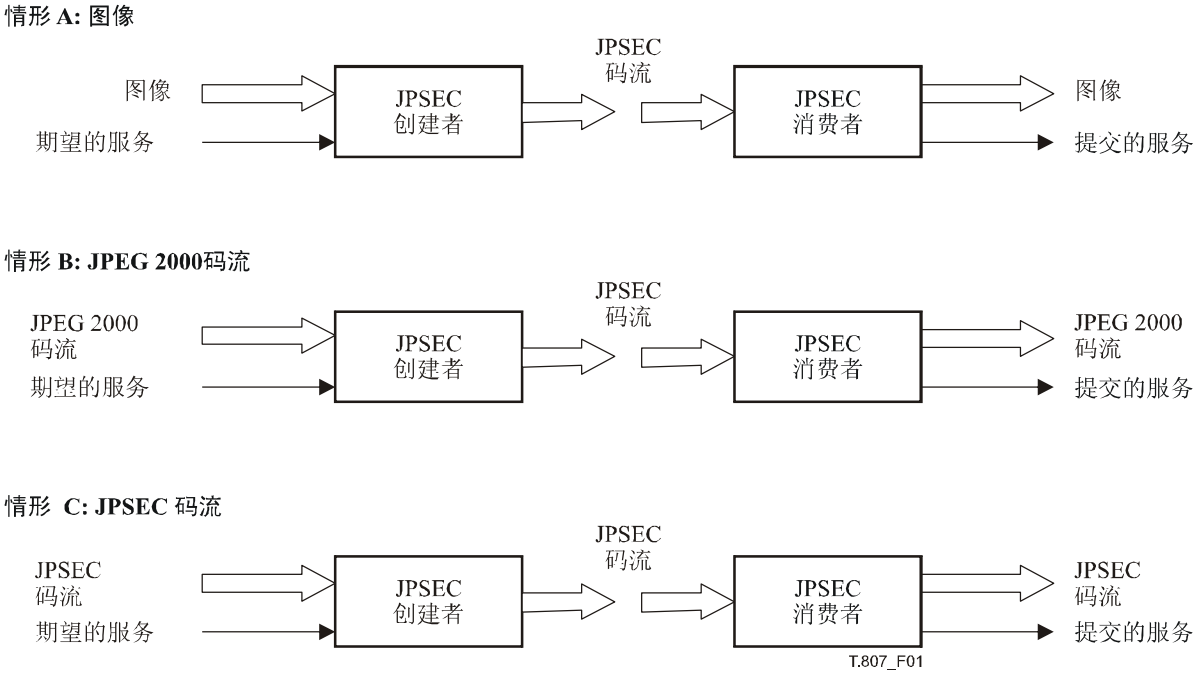


图 1－JPSEC框架概念步骤的概述

JPSEC 码流的语法是标准的。其目标是允许 JPSEC 应用程序可以以一种互操作的方式使用 JPSEC 码流（见图 1）。JPSEC 消费者应用程序解释 JPSEC 码流，识别并应用所标示的 JPSEC 工具，提交相应的安全服务，并因此传递所输出的 JPEG 2000 码流或图像以便进行后续处理，例如由某个图像观察器进行处理。

如图 1 中的情形 C 所示，JPSEC 码流可能是从另一个 JPSEC 码流中创建的。当多个 JPSEC 工具在不同的时间，或通过不同的实体被应用到相同的内容时，这种情况就可能会发生。当这种情况发生时，在创建操作和消费操作中应用 JPSEC 工具的顺序可能是很重要的。

信号化语法标识了一个 JPSEC 消费者所使用的工具。这些工具可能是由本标准的标准部分来定义的，也可能是由注册机构定义的，或者是由私有工具定义的。标准定义的工具支持机密性（通过加密工具），并支持对源和内容的认证。它们允许最高类型的互操作，因为消费过程的各自独立的实现能够处理相同的 JPSEC 码流，并且能够恢复具有相同行为的相应服务。

创建 JPSEC 码流的方式不在本建议书 | 国际标准的定义范围之内。JPSEC 创建者必须产生包含适当的 JPSEC 信号的 JPSEC 码流。JPSEC 码流可以采用多种方式创建。例如，可以将一个 JPSEC 工具应用到图像像素上，或应用到小波系数上，或应用到量化的小波系数上，或应用到包上等。

一个消费者可以实现一种或多种 JPSEC 工具。例如，它可以有能力使用 AES 块密码以 ECB 模式执行解密，并且有能力使用 SHA-128 哈希和一个 RSA 公钥来执行签名验证。由于具备这些能力，它有能力执行机密性和认证等安全服务。

在 JPSEC 框架中，JPSEC 工具可以通过私有定义的模板来规范，也可以通过一个 *JPSEC 注册机构*进行注册。由模板定义的 JPSEC 工具具有独特的处理行为，因此不需要唯一的标识符。而那些由注册机构规定的 JPSEC 工具都与一个唯一的标识符号相关联，这些标识符由一个公共注册处提供。

5.2 JPSEC安全服务

本节的目标是列出并解释在本建议书 | 国际标准的范围内所定义的功能性。

JPSEC 工具被用于实现安全功能。JPSEC 是一种开放的框架，这意味着它在未来是可扩展的。目前，它关注于如下几个方面：

— 通过加密和选择性加密的机密性

一个JPSEC文件可以支持将一个（图像和/或元数据）数据（明文）转换为一种隐含了数据原始含义的格式（密文）。选择性加密指的是并不是对所有的图像和/或元数据进行加密，而是对图像和/或元数据的一部分进行加密。

— 完整性验证

一个JPSEC文件可以支持对图像和/或元数据的检测操作，以此来验证它们的完整性。有两种类型的完整性验证：

1） 图像数据完整性验证，这种情况下，即使图像数据中只有一个比特出错也会引起验证失败（即验证将返回“无完整性”）。这种验证也常被称为是脆弱的图像（完整性）验证。

2） 图像内容完整性验证，在这种情况下，即使图像数据发生了某些偶然的变化，但只要那些变化没有改变从用户视觉系统所感知到的图像内容，则验证结果仍然是成功的；换句话说，是图像的感知含义没有改变。这种验证也常常被称为是半脆弱的图像（完整性）验证。

那些脆弱的或半脆弱的图像完整性验证可能会在图像数据/图像内容中标识出完整性出现问题的地点。解决方案可能包括：

1） 密码方法，例如消息认证码（MAC），数字签名，密码校验和/或带密钥的哈希（散列）函数。

2） 基于水印的方法。本建议书 | 国际标准没有为水印技术定义标准的模板，尽管它支持使用水印技术的非标准工具。

3） 上述两类方法的组合。

— 源认证

一个JPSEC文件可以支持对产生此JPSEC文件的用户/参与方的身份进行验证。这包含的方法如数字签名或消息认证码（MAC）。

— 条件访问

一个JPSEC文件可以支持一种机制和策略，以便准予或限制对图像数据或其中部分图像数据的访问。例如，在看到更高分辨率的图像之前，允许先观看一个低分辨率的图像（预览）。

— 已注册内容的确定

一个JPSEC文件可以在一个内容注册机构中注册。它可以支持一种匹配方法，将（所声明的）图像数据/图像内容与已注册的图像数据/图像内容相匹配。例如，这种匹配方法可以是：读取一个放置在元数据中的文件标识符（许可证），然后检查该许可证与在执行注册过程时已经上载的信息是否一致。许可证中可能已经包含了足够的信息，以便能够从内容注册机构请求信息，获知该文件在何地注册，并验证该文件是否符合标识符等。

— 安全的可扩展流化和安全的代码转换

一个JPSEC文件或包序列可以支持一些方法，使得相同或不同的节点都能够执行流化和代码转换，而不需要对内容进行解密或解保护。一个示例是这样一种情况，被保护的JPEG 2000内容首先流化，并流到一个中间网络节点或代理上，该中间网络节点或代理随后又对被保护的JPEG 2000内容执行了代码转换，而所采用的方式保证了端到端的安全性。

5.3 设计和实现安全的JPSEC系统的注解

本建议书 | 国际标准支持一个丰富的和灵活的安全服务集。例如，加密原语可能以各种不同的方式被应用，以便满足不同的目标，这些目标包括从对整个 JPEG 2000 码流进行加密，到仅对码流的一小部分进行选择性加密等。然而，很重要的是要强调，在实现任何安全系统时都必须非常小心，包括基于 JPSEC 的系统。

强烈推荐任何安全系统的设计者都必须仔细考虑为所使用的安全原语所推荐的指南。对大多数使用 JPESC 标示的安全原语而言，相关的 ISO/IEC 标准都对它们的正确用法提供了重要的指南。 例如，对于使用一个块密码和一个相关联的块密码方式（见表 29）的加密来说，关于块密码方式的选择和操作的指南在 ISO/IEC 10116 中给出。

另外，在许多安全应用中，认证是一种最重要的安全服务。即使是当机密性作为一种目标安全服务时，它也应当通过认证来加强，以便防止各种形式的攻击。特别地，即使在许多以机密性为主要目标的成像应用中，也建议同时使用认证。

密钥管理不在 JPSEC 的定义范围之内，然而，它的重要程度仍必须要强调。在许多密码系统中，极其重要的是对控制操作的加密密钥的管理。如果这些密钥被危及到，则整个系统的安全性都会被危及到，而且在这种方式中，威胁有可能是检测不到的。因此，强制要求密钥的产生、分发、存储和销毁都应当在某种安全级别上，至少应当与其保护的数据的安全级别相同。此外，由于密钥被泄漏的机会将随着时间而增长，因此密钥应当仅在一个固定的密钥生命周期中使用，这也是极其重要的。关于密钥的使用和管理的更多信息，见 ISO/IEC 11770。

由于伴随所有的安全系统，密码操作的使用对用户必须是完全不透明的。即除了输出外，用户必须不能发现关于密码操作的任何信息。例如，用户必须不能够访问到这样的信息，即为什么一个密码操作未能成功产生一个输出。类似地，用户必须不能够发现任何额外的信息，即使他/她采取了测量“旁路”的方式，例如定时和/或功率分析等。简而言之，用户必须不能够注意到任何应用输出中的任何不同，而不论该应用目前正在做什么，因为如果不这样的话，所引起的信息泄漏可能会潜在地危及到系统的安全性。

综上所述，强烈建议任何安全系统，包括基于 JPSEC 的系统的设计者，都要特别注意系统设计的细节，以确保得到一个安全的系统。

5.4 字节对齐段（BAS）

5.4.1 字节对齐段

为了能够为类和模式提供可扩展的信号化，本建议书 | 国际标准使用了一种可变长度的数据结构，称为“字节对齐段”（BAS）。如果字段的数量可扩展，则这样的参数字段使用字段 BAS（FBAS）结构来表示。而如果参数值具有很大的范围，则这样的参数值使用范围 BAS（RBAS）结构来扩展表示。

如图 2 中所表示的，BAS 由一个或多个 BAS 字节组成。每个 BAS 字节的最高有效位（MSB）指示了后续 BAS 字节是否存在，如果 MSB = 1，则有一个后续的 BAS 字节跟随其后，而如果 MSB = 0，则不存在一个后续的 BAS 字节，且此 BAS 结构已结束。每个 BAS 字节的剩余最低有效位都级联起来，形成一个比特列表，以不同的方式用于不同的 BAS 参数。通常，它们与一个具有多元素的参数列表结合起来使用，其中，每个 BAS 比特都被设置为 1 或 0，分别标记与相关元素相对应的信息。选择这种灵活的结构，是因为它为后续标准的演进提供了可扩展性，它允许新的参数以一种可扩展的方式来标示。

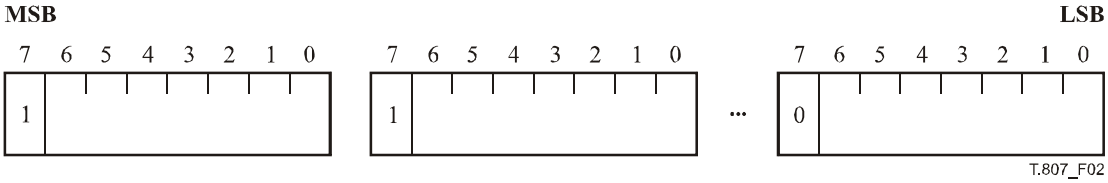


图 2－字节对齐段（BAS） 结构

5.4.2 字段BAS（FBAS）

字段 BAS（FBAS）是 BAS 的一种类型，其中 BAS 字节中的剩余比特都被用于设置相应字段为 1 或 0。FBAS 用法的一个示例是影响区的描述类（DCzoi），其中我们可以指定图像的多种描述法，包括拼贴索引，分辨率级别，和色彩分量等。如果我们这样做，则可以将相对应于拼贴，分辨率和色彩的三个 BAS 比特都标记为 1。

例如，如果我们希望表示一个具有 9 个字段的字段 BAS，f1 到 f9，则我们需要使用最多两个 BAS 字节。如果这两个字节为字节"a"和字节"b"，且每个字节的最高有效位分别为 a0 和 b0，则该 FBAS 应当如下所示：

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

a0 和 b0 为指示比特。字段 f1 到 f7 在比特 a1 到 a7 中表示，字段 f8 在比特 b1 中表示，字段 f9 在比特 b2 中表示。剩余的比特 b3 到 b7 被保留，且都被设置为 0。

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

当在一个 JPSEC 流中使用时，本例中的 FBAS 可以被表示为一个或两个字节，依赖于字段的实际取值。这是因为实际上字段的缺省值都为 0。因此，如果字段 f8 和 f9 没有被设置（即它们的值均为 0），则 BAS 的第二个字节是不需要的，且 a0 被置为 0。另一方面，如果字段 8 或字段 9 被设置，则需要两个字节。在这种情况下，a0 被置为 1，而 b0 被置为 0。

需要注意的是这些字段比特是“左对齐的”。这就允许我们可以随时间以一种兼容的方式增加更多的字段。

5.4.3 范围BAS (RBAS)

范围 BAS（RBAS）可用于对表示某个值的比特的范围或数量进行扩展。有两种类型的 RBAS，RBAS-8 和 RBAS-16。

RBAS-8 包含一个或多个 RBAS 字节，这些字节包含了表示该值的比特。 同 FBAS 一样，每个字节中的第一个比特都指示是否有另一个 RBAS 字节相随。

与 FBAS 不同的是，RBAS 是“右对齐的”。因此，如果一个值具有 9 个有效位 v1 到 v9，其中 v1 为最高有效位，则它应当以两个 BAS 字节来表示：

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

取值如下：

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

如果该值较小，即比特 v1 和 v2 为 0，则还可以使用上述的两个字节表示，其中 v1 和 v2 被置为 0，或者可以使用一个字节的 RBAS，如下所示：

0 v3 v4 v5 v6 v7 v8 v9

RBAS-16 可被用于表示那些典型地大于 7 个比特但小于 15 个比特的值。在这种情况下，第一个 RBAS 块为两个字节，其中第一个比特为指示符，而后面的 15 个比特为表示该值的比特，然后当每次使用典型的 BAS 结构时，则剩余的字节会扩展一个字节，在典型的 BAS 结构中，每个字节的第一个比特都是后续 BAS 字节的指示符。

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

如果有一个参数值具有 22 个比特，则它可以以三个字节的 RBAS-16 结构表示，如下所示，其中 a0 和 c0 为指示符比特，指示了是否有一个 BAS 比特相随。任何剩余的 BAS 字节都是传统的一字节 BAS 段。

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

因此，指示符比特应当被设置如下：

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

不论 RBAS-8 还是 RBAS-16，值的比特都是“右对齐的”。

注意，当拼写 JPSEC 的创建者和消费者时，很重要的是要注意大端/小端的表示。

5.5 主安全标记（SEC）

5.5.1 安全标记段

本节中，我们为 JPSEC 的信号化提出了一种简单灵活的但是很强大的语法。出于此目的，定义了一个 SEC 标记段，并将其置于主头部。SEC 标记段语法用于描述为保护 JPEG 2000 图像所必须的所有信息。为了实现此目的，它引用了根据第 5.8 节描述的模板所规定的 JPSEC 标准工具，或者引用了 JPSEC 非标准工具，这些非标准工具可能已经由 JPSEC 注册机构注册为一个 *priori*，或者被定义为专有的，并且它已经做了相关指配来处理与这些工具相关的参数。

一个 JPSEC 码流可以使用一种或多种 JPSEC 工具来保护。每种工具都或者是一个 JPSEC 标准工具，或者是一个 JPSEC 非标准工具。这些工具的参数都被信号化在一个或多个 SEC 标记段中，被置于码流的主头部，且处于 SIZ 标记段之后。当使用了多个 SEC 标记段时，它们被级联起来，并且必须连续地出现在主头部。在大多数情况下，所有的 JPSEC 参数都能够被信号化在一个 SEC 标记段中。然而，在某些情况下，信号化后的长度可能会超出最大的标记段长度。如果这种情况发生，则可以为信号化使用附加的 SEC 标记段。

图 3 显示了 SEC 标记段的语法。该标记段由 SEC 标记 0xFF65 来指示。L_{SEC} 是 SEC 标记段的长度，此长度包含 L_{SEC} 的两个字节，但不包含 SEC 标记自身的两个字节。Z_{SEC} 是 SEC 标记段的索引。对于出现在码流中的第一个标记段，Z_{SEC} 应当被设置为 0。P_{SEC} 是一个参数字段，描述了与整个码流相关的安全参数，并仅存在于第一个 SEC 标记段中，即 $Z_{SEC} = 0$ 时。该语法支持使用多种 JPSEC 工具，并被标示在一个或多个标记段中。如果使用了多个 JPSEC 工具，则一个 JPSEC 消费者应当按照这些工具出现在码流中的顺序来处理这些工具。

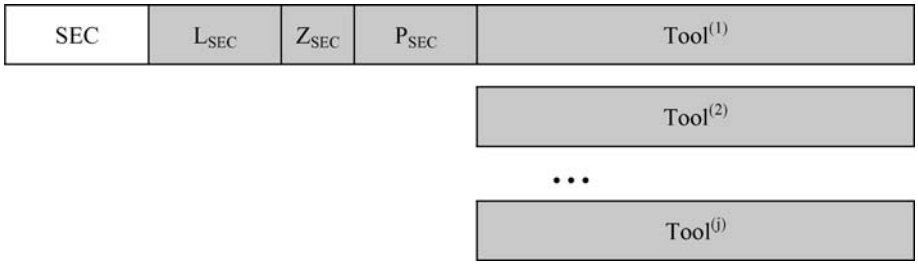


图 3－主安全标记段语法

SEC: 标记码。表 1 显示了主安全标记段的符号和参数的长度及取值。

L_{SEC}: 标记段的长度，以字节计数（包括 L_{SEC} 自身，但是不包括标记）。

Z_{SEC}: 在当前的头部，此标记段相对于所有其他 SEC 标记段的索引。该字段使用 RBAS 结构。

P_{SEC}: 码流安全参数的参数字段。该字段仅出现在第一个 SEC 标记段中，即当 Z_{SEC} 为 0 时。

$Tool^{(i)}$: 对应于 JPSEC 工具 *i* 的参数。如果标示有多个 JPSEC 工具，则一个 JPSEC 消费者应当按照这些工具出现在 JPSEC 码流中的顺序来处理每个工具。

表 1－主要的安全参数的取值

参　　数	长度（比特）	取　　值
SEC	16	0xFF65
L_{SEC}	16	$2 \ldots (2^{16} - 1)$
Z_{SEC}	8 + 8 * n (RBAS)	$0 \ldots 2^{7+7*n}$
P_{SEC}	0，当 $Z_{SEC} > 0$ 时， 否则是可变的	当 $Z_{SEC} = 0$ 时，见表 2
$Tool^{(i)}$	可变的	见 5.6.2 和 5.6.3

图 4 显示了当使用了多个 SEC 标记段时，安全参数在主头部中的语法。在这种情况下，JPSEC 工具相关的参数处于不同的 SEC 标记段中。每个标记段都起始于 SEC 标记，即 0xFF65，并在其后跟随标记段的长度和索引。第一个标记段索引应当被设置为 0，且后续的每个标记段索引都应当按照其出现的顺序加 1。仅有第一个标记段中包含码流的安全参数，P_{SEC}。所有的标记段都包含关于一个或多个 JPSEC 工具的参数。

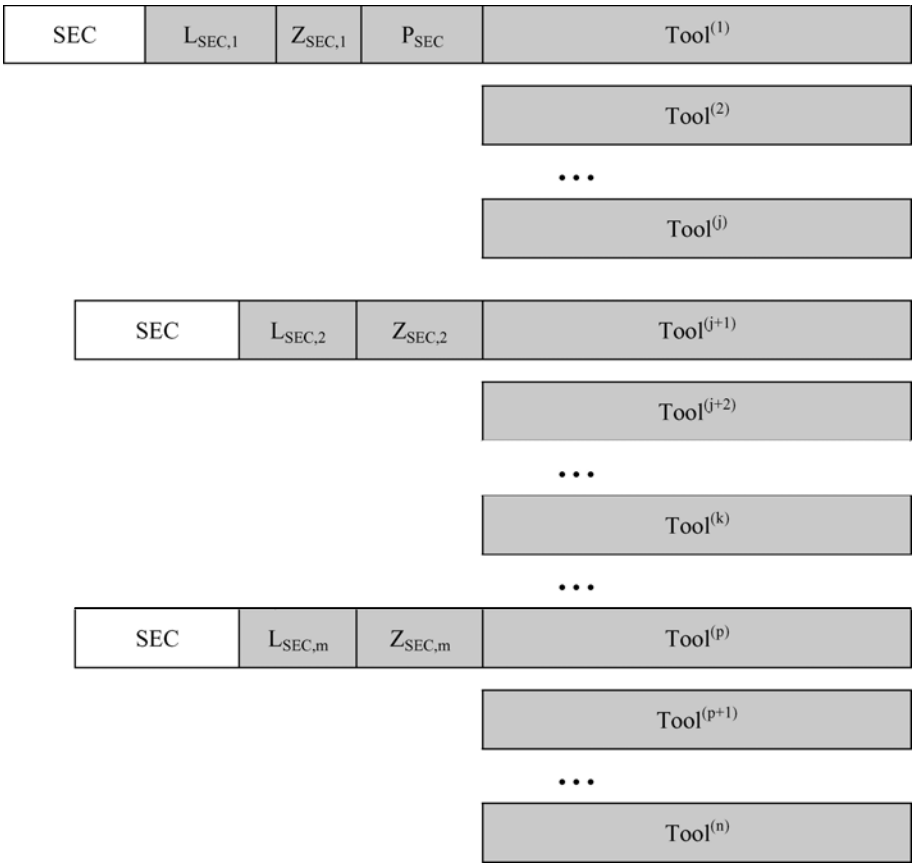


图 4－当使用多个标记段时的主安全标记语法

如果需要，一个 JPSEC 工具的描述可能会横跨多个 SEC 标记段，例如，当所需的长度超过了最大的 SEC 标记长度时，可能会发生这种情况。由于对工具描述的长度进行了完全地规定，因此 JPSEC 创建者只要简单地将工具分到不同的 SEC 标记段即可。然后，解码器应当将所有的段级联起来，减去 SEC 标记以及 L_{SEC} 和 Z_{SEC} 的值后，再相应地对工具进行解释。

P_{SEC} 是一个参数字段，描述了整个码流的安全参数，而不是一个特定工具的安全参数。这被用于指示某些事件，如是否遵循 JPEG 2000 第一部分，或者是否使用 INSEC 标记等。P_{SEC} 参数如图 5 所示。

图 5－码流安全参数（P_{SEC}）语法

F_{PSEC}: 一个标记，指示是否使用了 INSEC 标记段，是否使用了多个 SEC 标记段，是否修改了原始的 JPEG 2000 第一部分码流数据，以及是否定义了 TRLCP 标签的用法等。本字段使用 FBAS 结构。

N_{tools}: 在码流中使用的 JPSEC 工具的个数。本字段使用 RBAS 结构。

I_{max}: 在码流中使用的工具实例的最大索引值。本字段使用 RBAS 结构。

P_{TRLCP}: 定义 TRLCP 标签格式的参数字段。当 $F_{TRLCP} = 1$ 时，本字段存在。

表 2－第一个SEC标记段中的码流安全参数（P_{SEC}）

参　　数	长度（比特）	取　　值
F_{PSEC}	可变的（FBAS）	见表 3
N_{tools}	8 + n * 8 (RBAS)	1 ... 2^{7+7*n}
I_{max}	8 + n * 8 (RBAS)	0 ... 2^{7+7*n}
P_{TRLCP}	0，当 F_{TRLCP} = 0 时 32，当 F_{TRLCP} = 1 时	见表 4

F_{PSEC} 是一个 FBAS 结构，用于指示一系列的与 JPSEC 码流相关的参数标记。由 F_{PSEC} 所表示的字段见表 3。若在 JPSEC 码流中使用了 INSEC 标记，则 F_{INSEC} 应当被设置为 1。若在 JPSEC 码流中使用了多个 SEC 标记字段，则 $F_{multiSEC}$ 应当被设置为 1。若在 JPSEC 码流中，原始的 JPEG 2000 数据被修改，则 F_{mod} 应当被设置为 1。注意，如果使用了 INSEC 标记，则原始的 JPEG 2000 数据就被修改了，因此 F_{INSEC} 和 F_{mod} 都应当被设置为 1。若 TRLCP 标签的用法在 P_{SEC} 中进行了定义，则 F_{TRLCP} 应当被设置为 1。如果它被定义，则 TRLCP 标签描述符，P_{TRLCP}，应在 P_{SEC} 参数字段中规定。如果在 JPSEC 码流中有任何一个工具使用了 TRLCP 标签，则必须规定 TRLCP 标签的用法。

表 3－F_{PSEC} 取值的语义（FBAS）

BAS字段	BAS比特个数	取值（比特）	语　　义
F_{INSEC}	1	0	未使用 INSEC
		1	使用了 INSEC
$F_{multiSEC}$	2	0	使用了一个 SEC 标记段
		1	使用了多个 SEC 标记段
F_{mod}	3	1	原始的 JPEG 2000 数据被修改
		0	相反情况
F_{TRLCP}	4	0	TRLCP 标记的用法没有在 P_{SEC} 中定义
		1	TRLCP 标记的用法在 P_{SEC} 中定义

JPSEC 定义了一个被称为 TRLCP 标签的结构，该结构被用来唯一地标识一个 JPEG 2000 包。一个 JPEG 2000 包可以通过它的拼贴索引，分辨率级别索引，层索引，分量索引，以及选区索引等被唯一指定。一个 TRLCP 标签被定义为一种具有固定比特数量的数据单元，用于规定这些索引值中的每一个。每一个索引的比特数量在 P_{SEC} 中设置。P_{TRLCP} 是一个参数字段，描述了当 TRLCP 标签应当在 JPSEC 工具中使用时，TRLCP 应具有的格式。该字段仅在 F_{TRLCP} = 1 时才存在。P_{TRLCP} 包含图 6 中所示的下列变量。

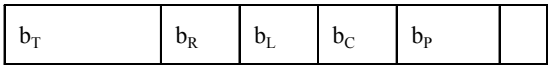


图 6－TRLCP标签描述符（P_{TRLCP}）的语法

b_T: 在 TRLCP 标签中，表示拼贴索引的比特数为 b_T + 1。
b_R: 在 TRLCP 标签中，表示分辨率索引的比特数为 b_R + 1。
b_L: 在 TRLCP 标签中，表示层索引的比特数为 b_L + 1。
b_C: 在 TRLCP 标签中，表示分量索引的比特数为 b_C + 1。
b_P: 在 TRLCP 标签中，表示选区索引的比特数为 b_P + 1。

表 4－TRLCP标签描述符（P_{TRLCP}）的参数字段

参　　数	长度（比特）	取　　值
b_T	8	0 ... (2^8 – 1)
b_R	4	0 ... 15
b_L	5	0 ... 31
b_C	5	0 ... 31
b_P	8	0 ... (2^8 – 1)
填充	2	0

每个由此而产生的 TRLCP 标签长度是包含所有比特的最小的整数个字节长度。TRLCP 标签的格式包含了对应于拼贴索引，分辨率级别索引，层索引，分量索引，以及选区索引的比特，并且按照上述顺序。如果有额外的比特需要填充到字节中，以便满足整数个字节长度的需要，则此 TRLCP 标签将被置于可能的最低有效位，且额外比特被设置为 0。注意如果这些额外比特存在的话，它们将是 TRLCP 标签的 MSB。

5.5.2 多个JPSEC工具的应用

在许多应用中，有必要在一个单独的 JPEG 2000 码流中应用多个 JPSEC 工具。例如，可能同时应用加密和认证来保护一个 JPEG 2000 图像。应用多个 JPSEC 工具的通常情况在图 3、4 和 7 中进行了说明，其中，应用了 N 个工具。JPSEC 的消费者将按照在 SEC 标记段中放置的顺序来读取这 N 个工具，如图 3 或图 4 所示，并且按照同样的顺序执行对 JPSEC 码流的 JPSEC 处理。需要注意的是，当 JPSEC 消费者以顺序 1，2，...，N，与从 SEC 标记段中读取的顺序相同，来应用 JPSEC 工具时，在 JPSEC 码流的创建过程中，这些 JPSEC 工具却是以相反的顺序在应用，即 N，N – 1，…，2，1，如同图 7 中显示的那样。需要注意的是，选择如图所示的工具编号方式是为了强调 JPSEC 消费者应用 JPSEC 工具的顺序与 JPSEC 创建者是相反的。然而，JPSEC 工具的任何编号方式都是可接受的，只要在 JPSEC 码流中的每个 JPSEC 工具都被给定一个用于标识目的的唯一编号即可。

一般来说，JPSEC 工具的创建和使用彼此是以相反的顺序来进行的。例如，如果 JPSEC 创建者应用了 N 个 JPSEC 工具，则 JPSEC 消费者典型地也将应用相同的 N 个 JPSEC 工具，但是以相反的顺序来应用。对多个 JPSEC 工具的正确使用可以通过按照正确的顺序依次使用 N 个工具来保证，并且可以要求消费者的任何中间状态都要与创建者的相应状态相匹配。例如，图 7 中，在工具 1 的 JPSEC 使用完成后，消费者的状态应当与在 JPSEC 创建过程中，应用了工具 2 后的状态相同。作为状态的这个特定例子，字节范围应当是一致的，因此在应用工具 1 时增加的任何字节都应当在 JPSEC 消费者删除工具 1 时被删除。

在某些应用程序中，对于一个 JPSEC 消费者而言，可能期望采用不同于如上所述的方式来使用多个 JPSEC 工具。例如，JPSEC 消费者可能会选择以不同的顺序来使用多个工具，或者在使用中跳过某些工具。此外，JPSEC 消费者还可能更喜欢应用某些 JPSEC 工具，而不删除它们，如检查一个数字签名但并不将其删除。在这些情况下，应当仔细考虑以便确保不按照原顺序处理或跳过某些工具进行处理不会导致不正确的或某些没有意料到的后果。这种行为是不推荐的，除非 JPSEC 应用程序已经完全能够意识到潜在的后果。

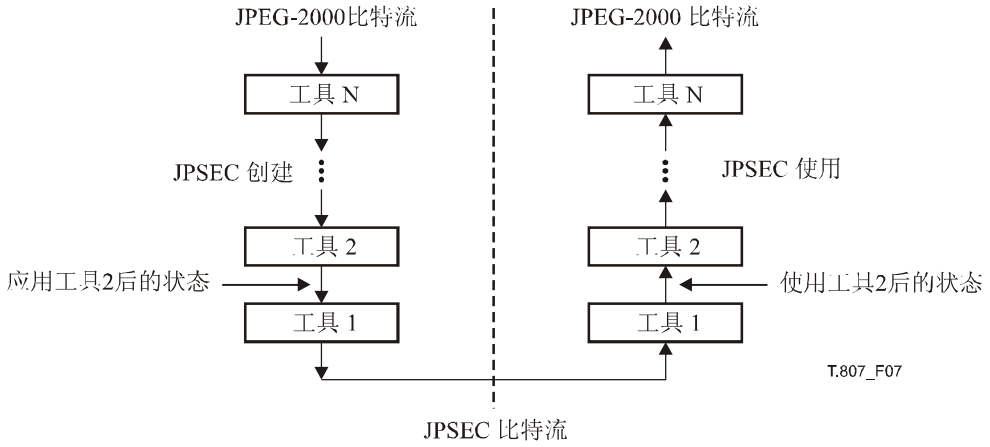


图 7－多个JPSEC工具的使用

5.6 JPSEC工具

5.6.1 JPSEC工具的语法

正如之前所提到的，有两种类型的 JPSEC 工具。JPSEC 标准工具根据第 5.8 节所描述的保护方法模板来规定，并且被称为是 JPSEC 标准工具。JPSEC 非标准工具是由一个 JPSEC 注册机构或一个特定的 JPSEC 应用程序基于它们的 ID 号而规定的，它们分别被称为是 JPSEC 注册机构工具或 JPSEC 用户自定义工具。JPSEC 标准工具的语法在第 5.6.2 节中讨论。JPSEC 非标准工具的语法在第 5.6.3 节中讨论。

JPSEC 工具的语法在图 8 中显示。JPSEC 工具的语法有三个主要部分，分别描述了：

1） 通过标识符描述了什么样的工具被应用；

2） 通过一个影响区结构，描述了此工具在哪里被应用；以及

3） 通过一个更详细的参数字段，描述了工具是如何被应用的。

例如，使用此语法，一个 JPSEC 工具语法可以指定应当使用一个加密工具（什么工具）在处于某个特定字节范围内的最低分辨率分量上（在哪里应用工具），并且以 CBC 模式使用 AES 解密，并使用一个特定的初始向量和密钥集合（如何使用工具）。

图 8－JPSEC工具语法（$Tool^{(i)}$）

t: 工具类型。第一个 BAS 比特取值为 0 表示是一个 JPSEC 标准工具。第一个 BAS 比特取值为 1 表示是一个 JPSEC 非标准工具。本字段使用 FBAS 结构。

i: 工具实例索引（可被用作一个唯一标识符）。本字段使用 RBAS 结构。

ID: JPSEC 工具 *i* 的标识值。对于 JPSEC 标准工具，ID = ID_T 为 8 个比特，并且规定了模板类型。对于 JPSEC 非标准工具，ID = ID_{RA}，在图 10 和表 8 中定义。

L_{ZOI}: ZOI 的长度，以字节计数（不包含 L_{ZOI}）。本字段使用 RBAS 结构。

ZOI: JPSEC 工具 *i* 的影响区。

L_{PID}: P_{ID} 的长度，以字节计数（不包含 L_{PID}）。本字段使用 RBAS 结构。

P_{ID}: JPSEC 工具 *i* 的参数。

表 5－JPSEC工具参数的取值

参　　数	长度（比特）	取　　值
t	8 + 8 * n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 2)$ $(2^{7+7*n} - 1)$，保留
ID	8，当 t = 0 时 可变，当 t = 1 时	见表 6 见图 10 和表 8
L_{ZOI}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
ZOI	可变的	见 5.7
L_{PID}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
P_{ID}	可变的	表 7，当 t = 0 时， 由 JPSEC 注册机构管理，当 t = 1 时

每个 JPSEC 工具都具有如下语法。第一个字节标识了该工具是一个 JPSEC 标准工具，还是一个 JPSEC 非标准工具，并且为工具分配了一个实例标识符。该字节后紧跟一个工具标识符 **ID**。之后跟随的是 L_{ZOI}，指示了后续的影响区字段 ZOI 的长度，之后是影响区自身，描述了 JPSEC 工具在数量流的哪里被应用。之后跟随 L_{PID}，指示了后续的参数字段 P_{ID} 的长度，该参数字段是用来为 JPSEC 工具传送一个或多个参数的字段。

工具的第一个字节使用了单字节的 FBAS 结构，其中第一个 BAS 比特表示工具类型，取值为 0 指示是一个 JPSEC 标准工具，取值为 1 指示是一个 JPSEC 非标准工具。之后跟随一个实例索引，i，使用 RBAS 结构来表示。该实例索引应当是工具在码流中的一个唯一标识符，且不能被码流中的其他工具重复，即使其他工具是在不同的 SEC 标记段中也不可以。当使用 INSEC 标记时，此实例索引是尤其关键的（和必须的），因为每一个 INSEC 标记段都包含它所应用的工具的实例索引。建议 JPSEC 创建者所应用的第一个工具的实例索引为 1，然后每一个新增加的工具在应用于保护者时都按顺序递增索引。

另外，每一个 JPSEC 工具都具有一个 ID 号，该 ID 号对于 JPSEC 标准工具是 8 个比特，对于 JPSEC 非标准工具是 32 个比特。对于 JPSEC 标准工具，该 ID 号描述了使用哪种保护方式模板，即它规定了解密模板，认证模板，或哈希模板。对于 JPSEC 非标准工具，第一个比特指示了它是一个 JPSEC 注册机构工具，还是一个 JPSEC 用户自定义工具。在任何一种情况下，该 ID 号都指示了此特定工具。一个 JPSEC 注册机构可以确保合法的 ID 号是唯一的。然而，一个使用用户自定义 ID 号的 JPSEC 应用程序在选择一个 ID 号时就可能会出现风险，即该 ID 号也被其他 JPSEC 应用程序所使用，因此应当慎重地使用此方式。

当每一个 JPSEC 工具被应用在 JPSEC 创建者处时，表 2 中显示的 P_{SEC} 参数字段应当被更新。例如，P_{SEC} 参数字段中包含一个 I_{max} 参数，该参数指定了 JPSEC 码流中的工具所使用的最大实例索引。当有一个新的工具被应用时，它必须被分配一个唯一的实例索引。一个 JPSEC 保护者可能会查阅 P_{SEC} 参数字段中给定的 I_{max} 参数，来决定分配给 JPSEC 工具的实例索引值，例如，它可能会选择一个比当前的 I_{max} 值大 1 的值，因此相应地，I_{max} 的值需要加 1。

5.6.2 JPSEC标准工具

JPSEC 标准工具使用第 5.6.1 节中描述的 JPSEC 工具语法，并在图 8 中显示，其中工具类型 t = 0，且 ID 的长度为 8 个比特。JPSEC 标准工具是基于第 5.8 节所描述的保护方式模板。有三种类型的保护方式模板；工具所使用的类型由工具标识符 ID = ID_T 所指定，使用表 6 中所显示的取值。

表 6－JPSEC标准工具模板ID的取值（ID_T）

取　　值	保护方式模板
0	保留
1	解密模板
2	认证模板
3	哈希模板
4	空工具
	其他所有值都保留供 ISO 使用

在使用 JPSEC 标准工具的情况下，参数字段 P_{ID} 具有图 9 中所示的结构。P_{ID} 包含四个主要的字段：保护方式模板 T，它的处理域 PD，它的粒度 G，以及它的值列表 V。每个字段的语法分别在第 5.8，5.9，5.10 和5.11 节中给出。这些字段共同描述了工具是如何被应用的。保护方式模板 T 为标准工具 ID 所指定的解密模板、认证模板或哈希模板描述了特定的保护方式。它还可能会指定为空工具，在这种情况下，表示没有使用任何一个模板，但可能仍会使用其他功能性。例如，可能会指定影响区来表示图像区域以及它们相应的字节范围。处理域 PD 描述了此保护方式被应用的区域。粒度 G 描述了保护方式被应用的粒度。值列表 V 包含一系列的值，这些值可能被每个保护方式在更细的粒度上所需。对于解密模板，此值列表可被用于指定一个将要使用的更细粒度的初始值集合。对于认证模板，此值列表包含了一个 MAC 值集合或数字签名集合。对于哈希模板，此值列表包含了一个哈希值集合。在所有情况下，此值列表都包含了由粒度字段 G 所指定的粒度的取值。

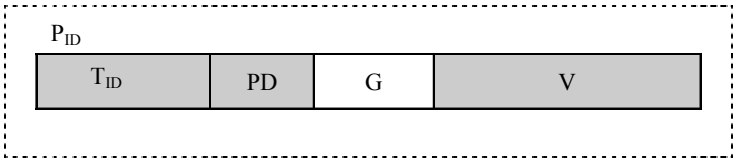


图 9－JPSEC标准工具（t = 0）的参数（P_{ID}）语法

T_{ID}: JPSEC 标准工具的模板参数，模板标识符为 ID_T。

PD: JPSEC 标准工具的处理域。

G: JPSEC 标准工具的粒度。

V: JPSEC 标准工具的值列表，例如初始向量，MAC 值，数字签名，或哈希值等，依赖于模板 ID。

注意模板参数依赖于模板 ID。但处理域、粒度和值列表独立于模板 ID。

表 7－JPSEC标准工具参数的取值

参　　数	长度（比特）	取　　值
T_{ID}	0，当 $ID_T = 4$ 时 否则为可变的	N/A 见 5.8
PD	可变的	见5.9
G	24	见 5.10
V	可变的	见5.11

5.6.3　JPSEC非标准工具

在某些情况下，对于一个 JPSEC 应用程序而言，有能力应用一个扩展到 JPSEC 标准工具之外的工具可能是有用的。这种能力通过使用一个 JPSEC 非标准工具来支持。这可以使一个人不仅可以使用 JPSEC 标准工具中的许多元素，包括 ZOI 和 JPSEC 模板，另外还可以增加灵活性，即可以按照与工具的 ID 值相关联的不同方式使用参数。

JPSEC 非标准工具使用第 5.6.1 节中描述的 JPSEC 工具语法，并在图 8 中显示，其中工具类型 t = 1，且标识符 ID_{RA} 包含一个命名空间和一个 ID 号，如同图 10 和表 8 中的定义。

有两种类型的 JPSEC 非标准工具：

1） JPSEC注册机构工具：JPSEC非标准工具，其信号化是由一个注册机构规定的。

2） JPSEC用户自定义工具：JPSEC非标准工具，其信号化是由一个JPSEC应用程序规定的。

这两种类型的 JPSEC 非标准工具都使用 32 个比特的 $ID_{RA,id}$ 标识符来进行标示，如表 9 所示，其中第一个比特为 0 的标识符是由一个注册机构来定义的，而第一个比特为 1 的那些标识符是由一个特定的 JPSEC 应用程序来定义的。

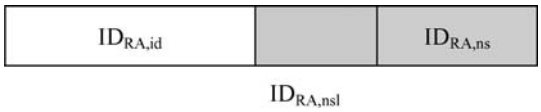


图 10－ID_{RA} 语法

$ID_{RA,id}$: RA 工具和用户自定义工具的工具标识符。

$ID_{RA,nsl}$: 字段 $ID_{RA,ns}$ 的长度，以字节计数。本字段使用 RBAS 结构。

$ID_{RA,ns}$: 一个字符串，包含了指定的 RA 工具或用户自定义工具的命名空间。

表 8－ID_{RA} 语法中参数的取值

参　　数	长度（比特）	取　　值
$ID_{RA,id}$	32	见表 9
$ID_{RA,nsl}$	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
$ID_{RA,ns}$	可变的	一个包含了命名空间的串

表 9－JPSEC非标准工具ID的取值（$ID_{RA,id}$）

$ID_{RA,id}$	含　　义
0x00 00 00 00 ... 0x7F FF FF FF	JPSEC 注册机构工具。其取值应当由 JPSEC 注册机构所管理。
0x80 00 00 00 ... 0xEF FF FF FF	JPSEC 用户自定义工具。其取值可以由一个特定的 JPSEC 应用程序定义。
0xF0 00 00 00 ... 0xFF FF FF FF	保留供 ISO 使用。

对于 RA 工具，字段 $ID_{RA,ns}$ 是注册此工具的注册机构（RA）的命名空间。由于每个 RA 都具有一个唯一的命名空间，因此 $ID_{RA,id}$ 和 $ID_{RA,ns}$ 共同标识了一个 RA 工具。对于用户自定义工具，字段 $ID_{RA,ns}$ 由开发者来选择。为了减少 ID 冲突的风险，建议开发者在选择他们的命名空间时应当寻求保证唯一性的方法，例如通过选择他们的组织机构或公司的域名来实现。然而，需要注意的是，对于用户自定义工具，是没有办法来保证命名空间的唯一性的，因此 ID 冲突可能出现，因此在使用用户自定义工具时必须仔细考虑。

P_{ID} 字段被用于为 JPSEC 非标准工具 *i* 传送一个或多个参数。P_{ID} 字段的格式在 JPSEC 定义范围内没有完全给出。如果使用了一个注册机构，则该格式在注册机构中注册，并给定一个 ID。如果没有使用注册机构，且工具是用户自定义的，则仅指定该字段的长度，而如何适当地使用此字段是由用户来决定的。

然而，JPSEC 确实允许在为 JPSEC 非标准工具定义的 P_{ID} 字段中使用为 JPSEC 标准工具所定义的语法结构。例如，一个 JPSEC 非标准工具可以使用分别在第 5.8，5.9，5.10 和5.11 节中描述的保护方式模板，处理域，粒度，以及值列表等。

该语法是非常灵活的，可以涵盖大量的安全技术，如图像数据完整性，访问控制以及权限保护方法等。因此，它提供了一个丰富的功能性集合，同时又是简单明了的。

5.7 影响区（ZOI）语法

5.7.1 引言

影响区（ZOI）可被用于描述一个 JPSEC 工具所覆盖的区域。在覆盖区域内的数据（由 ZOI 来确定）被称为是受影响的数据。JPSEC 标准工具应当使用 ZOI 来描述它们的覆盖区域。JPSEC 非标准工具可能使用 ZOI 来描述它们的覆盖区域，或者也可能使用其他替代方式。如果使用了其他替代方式，则 ZOI 的长度为 0，即它不存在。

影响区（ZOI）描述了每个 JPSEC 工具的覆盖区域。该覆盖区域可以通过与图像相关的参数来描述，如通过分辨率或图像区；或者也可以通过与非图像相关的参数来描述，如通过码流段或包索引。在某些情况下，与图像相关的参数和与非图像相关的参数会一起使用，在这些情况下，ZOI 则描述了这些区域之间的相对应性。例如，可使用 ZOI 来指示由图像相关的参数所指定的分辨率和图像区，与由非图像相关的参数所指定的码流段之间是相对应的。这就允许将 ZOI 用作元数据，来标示图像的某些部分位于 JPSEC 码流的什么位置。

图 11 显示了 ZOI 的概念结构。ZOI 包含一个或多个区。若在一个单独的 ZOI 中使用了多个区，则该 ZOI 通过它们的联合来定义。这就指示该 JPSEC 工具应当应用到所有的区上。一个 ZOI 中的每个区通过三个功能单元来描述：描述类，参数模式和参数项（取值）。本建议书 | 国际标准定义了两个描述类：与图像相关的描述类和与非图像相关的描述类。这些参数可以使用一定数量的模式来规范，例如通过一个单独的值，通过多个列表值，或者通过一个范围等。然后，相对应于模式的参数值或参数项被列出。

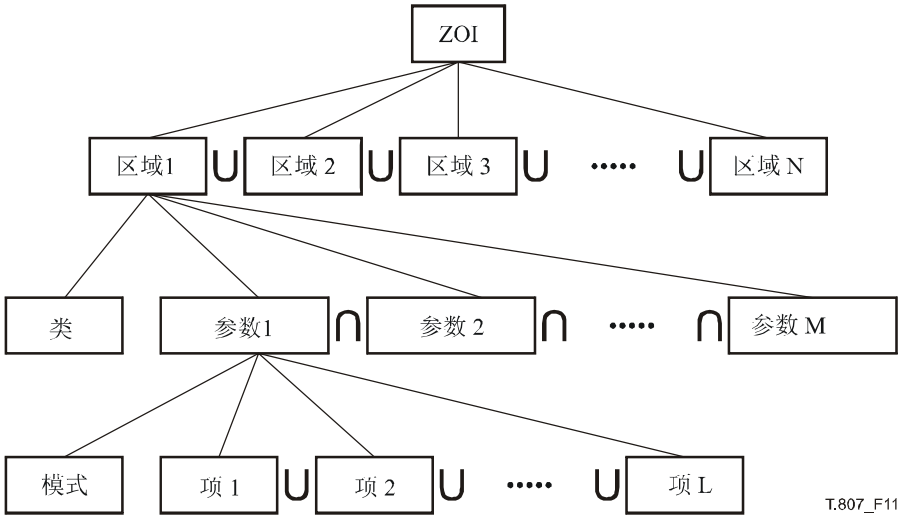


图 11－影响区的概念结构

5.7.2 ZOI语法

图 12 显示了 ZOI 语法。ZOI 可能包含一个或多个区。它也可能为空，在这种情况下，NZzoi 应为 0。当这种情况发生时，工具的影响是通过其他方式来规范的，如通过 INSEC 标记，或通过一个 JPSEC 非标准保护工具所定义的参数。

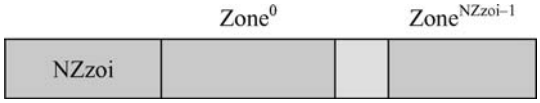


图 12－ZOI语法

NZzoi: 区域的数量。本字段使用 RBAS 结构。

Zone^{k}: 区域。它的结构在第5.7.3 节中规范。

表 10－影 OI）参数的取值

参　　数	长度（比特）	取　　值
NZzoi	8 + 8 * n (RBAS)	0 ... (2^{7+7*n} – 2) (2^{7+7*n} – 2)，保留
Zone^{k}	可变的	见5.7.3

5.7.3 区域语法

区域包含一个区域描述类字段指示符，其后跟随该类的参数。区域描述类使用 FBAS 结构。如图 13 中所示，每个字节中的第二个最高有效位，被标记为"x"，指示了一个特定描述类的用法。本建议书 | 国际标准定义了两个描述类：与图像相关的描述类和与非图像相关的描述类（见表 12）。表 13 和 14 分别为与图像相关的描述类和与非图像相关的描述类定义了字段指示符号码。在每个字节中，跟随在描述类标记之后的六个级联起来的被标记为"y"的比特，指示了某个给定描述类内的一个特定描述的用法。在每个类的比特号上，如果比特值为"1"，则指示相应的参数字段存在。参数的数量应当与取值为'1'的区域描述类字段指示符的数量相同，并且应当按照类字段指示符被标示的顺序出现。区域描述类具有变长数量的字节数；当 MSB 等于 1 时，则表示有另一个区域描述类字节紧随其后。最后一个描述类字节的 MSB 等于 0。如果同时使用了与图像相关的描述类和与非图像相关的描述类，则与图像相关的描述类字节应当处于与非图像相关的描述类字节之前。当有大量的项都使用此结构来表示时，列表中的第一项应当对应于第一个字节的可用的最高有效位比特。

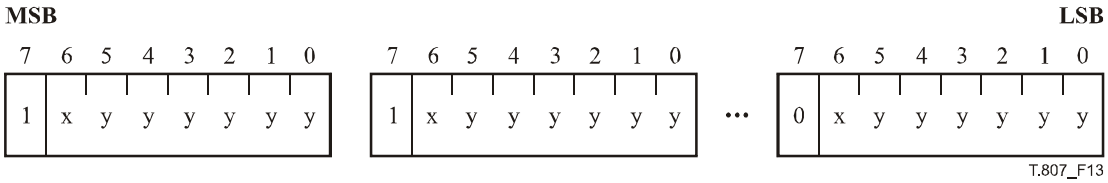


图 13－区域描述类结构（DCzoi）

图 14 显示了区域语法。

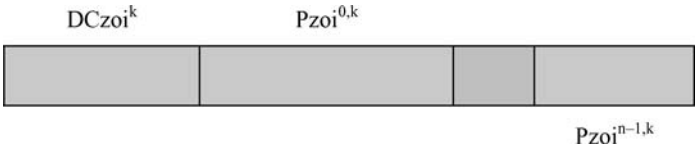


图 14－包含一个描述类和一个或多个参数集的区域语法

DCzoi^{k}: 第 k 个区域描述类。本字段使用 FBAS 结构。

Pzoi^{i,k}: 相对应于所指定的区域描述类（DCzoi^{k}）的区域参数。见第 5.7.6 节。

根据被设置为 1 的比特的个数，$DCzoi^k$ 指定了存在的 *n* 个区域描述类字段。对于每一个区域描述类字段，都存在一个 $Pzoi^{i,k}$ 区域参数字段。这些字段顺次出现，其顺序与出现在 $DCzoi^k$ 中的标记的顺序相同。

表 11－区域参数的取值

参　　数	长度（比特）	取　　值
$DCzoi^k$	可变的（FBAS）	根据表 12 中的值集而变化
$Pzoi^{i,k}$	可变的	关于本字段的语法，见5.7.6

表 12－描述类指示符的取值

取　　值	描　述　类
0	与图像相关的描述类。后续的比特号在表 13 中定义
1	与非图像相关的描述类。后续的比特号在表 14 中定义

表 13－与图像相关的描述类

比　特　号	语　　义
1	图像区
2	JPEG 2000 第一部分定义的拼贴
3	JPEG 2000 第一部分定义的分辨率级别
4	JPEG 2000 第一部分定义的层
5	JPEG 2000 第一部分定义的分量
6	JPEG 2000 第一部分定义的选区
7	TRLCP（拼贴-分辨率-层-分量-选区）标签
8	JPEG 2000 第一部分定义的包
9	JPEG 2000 第一部分定义的子带
10	JPEG 2000 第一部分定义的码块
11	ROI(s)
12	比特率
13	用户自定义。具体细节通过其他方式来指定（例如 JPSEC ID）
	所有其他值都被保留

表 14－与非图像相关的描述类

比　特　号	语　　义
1	JPEG 2000 第一部分定义的包
2	（填充的）字节范围（起始于第一个 SOD 标记之后的第一个字节）
3	（填充的）字节范围（起始于第一个 SEC 标记之后的第一个字节）
4	当使用填充时，未被填充的字节范围
5	TRLCP（拼贴-分辨率-层-分量-选区）标签
6	失真值
7	相对重要性
8	用户自定义。具体细节通过其他方式来指定（例如 JPSEC ID）
	所有其他值都被保留

包索引是在一个拼贴内被顺序编号的，因此在跨拼贴时可能不是唯一的。此外，在一个拼贴内，如果包的索引超出了最大值 65535，则包索引可能会回滚。由于这个原因，为包定义索引需要更详细地描述。当一个拼贴内的包索引没有超出 65535 个时，则在表 13 中描述的包索引是由 SOP Nsop 参数给定的包索引来定义的，该参数在 JPEG 2000 第一部分标准的表 A.40 中定义。注意，当最大值没有超过 65536 时，一个单独的 JPEG 2000 包可能由一个拼贴索引和一个包索引来唯一地指定。当包索引超出了 65535 个包时，则 JPEG 2000 第一部分的包索引被定义为回滚到 0。在这种情况下，包索引不能够唯一地标识一个包，因此不应被使用。在这种情况下，推荐改为使用 TRLCP 标签。请注意，如果包索引回滚并重复，则要求具有唯一包索引的那些安全服务是有漏洞的。

当使用 TRLCP 标签时，它的格式必须在 P_{SEC} 参数字段中定义，如表 2 所示。特别地，TRLCP 标签的格式由表 4 中的 P_{TRLCP} 参数字段来规范。这定义了在 ZOI 中，TRLCP 标签的长度。

与非图像相关的描述类可能也同时有多个字段集合。当这种情况发生时，不同参数字段的模式应当具有相同数量的项（此规则的一个例外在下面描述），且这些项之间应当以相同的顺序按照一一对应的方式来相互对应。例如，如果一个区域使用字节范围和包范围，则每一种都应当具备相同数量的范围项，且其中的第一个字节范围应对应于第一个包范围，依次类推。

针对上述要求每个字段都具有相同数量的项的规则有一个例外。例外发生在这种情况下，即其中一个字段 f1 包含一个项，但该项指定了一个包含 N 个元素的项的范围（如同第 5.7.6 节描述的范围模式），而另一个字段 f2 是通过 N 个项的列表来指定的。在这种情况下，仅包含一个项（范围）的字段 f1 被解释为如同含有 N 个项。由 f1 的范围所规定的这 N 个项应当与 f2 中所列的 N 个项一一对应。因此，一个项范围可以与一个单独的项相关联，也可以与多个项相关联（其中每个项对应范围中的每个项）。

为字节分配索引或者是从第一个 SOD 标记之后的第一个字节开始，或者是从第一个 SEC 标记之后的第一个字节开始。在这两种情况下，第一个字节都应被标记为字节 0。

失真字段（失真字段同相对重要性字段一起）提供能力来标示 ZOI 所指定的区域的重要性。失真参数规定了指定的数据段对减少失真的贡献，不论此指定的数据段是一个包集合，还是一个字节范围，还是指定的与图像相关的区域等。失真通过总方差来表示，使用 Mzoi 中标示的一个字节或两个字节来描述。相对失真参数可被用于规定指定数据段的相对重要性，使用 Mzoi 中标示的一个字节、两个字节或四个字节的值来描述。关于这些字段的其他细节及格式在第 5.7.3.2 节中描述。

TRLCP 标签指定了被保护包的拼贴，分辨率，层次，分量以及所处码流中的选区等。该标记被用来在 ZOI 中指定这些参数，因为要在被保护的码流中推导出这些信息可能是很困难的。

需要注意的如果仅使用了与图像相关的描述，则该字段是可以被终止的。因此，如果没有使用与非图像相关的描述，则可以不需要表示这些与非图像相关的描述。

5.7.3.1 字节范围字段

与非图像相关的描述类允许以字节范围来描述 ZOI。一般来说，应当使用表 14 中的第 2 个和第 3 个元素来表示大多数工具的字节范围，例如认证和没有填充的加密/解密等。然而，有一些保护方法，如带填充的加密/解密，会改变数据的长度。当这种情况发生时，有必要同时指明填充的字节范围和未被填充的或原始的字节范围。在这种情况下，根据保护工具的需要，填充的字节范围可由表 14 中的第 2 个或第 3 个元素来指明（注意这两个元素不能被同时使用）。另外，未被填充的字节范围由表 14 中的第 4 个元素来指明。未被填充的字节范围应当使用与填充字节范围相同的描述模式来进行指定，并且具有相同数量的项。这些项应当以相同的顺序以一对一的方式相互对应。

5.7.3.2 失真字段和相对重要性字段

失真字段同相对重要性字段一起可以提供能力来标示 ZOI 所指定的区域的重要性。

使用失真字段将一个失真与 ZOI 所指定的一个区域关联起来。当相关联的区域不能被解码时，失真值指定了可能引起的总方差（或方差的和）失真。总方差失真是用于图像和视频处理的一个基本的失真测量值，且可被用于推导出通用的平均方差（MSE）失真和峰值信噪比（PSNR）。失真字段使用一个单字节描述或双字节描述来表示，这些单字节描述和双字节描述如下所述，且选择单字节描述还是双字节描述是通过指定本字段长度的 Mzoi 参数值来明确的。相对重要性字段可用于描述由相关联的 ZOI 所指定的不同区域之间的相对重要性，而不必要将其绑定到一个特定的失真测量值上。相对重要性字段的长度也是通过 Mzoi 来指定的。这些字段的更详细信息将在下面小节进行讨论。

5.7.3.2.1 单字节失真字段

总方差失真使用一个单字节的失真字段来表示，并使用一个伪浮点类型的表示法。失真字段中可用的 8 个比特所处位置如图 15 所示，而表 15 提供了在准确性和动态范围之间进行的一种适当的平衡。需要注意的是一个符号比特并不是必须的，因为失真是非负的。为了涵盖一个足够动态的区域，使用了 16 进制表示，且其中 4 个比特用于表示指数（exp）。尾数（m）使用 4 个比特来表示。因此完整的失真值 D 如下所示：

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

其中，m 取值范围为 $0 \le m \le 15$，且指数取值范围为 $0 \le exp \le 15$。一个取值为零的失真值通过 m = 0 和 exp = 0 来表示，即失真字段为 0。通过为尾数 m 分配 4 个比特，则精确度在 $\frac{1}{2} \times (1/2^4) = 1/32$ 或大约 3%之内。使用 4 个比特来表示指数，并使用 16 进制表示，则动态范围从 0 到 max，其中 max 的值由 m = 15 和 exp = 15 确定，相对应的失真值为 $15 \times 16^{15} = 1.7 \times 10^{19}$。

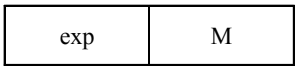


图 15－失真字段语法

exp: 失真字段值的指数（16 进制）

m: 失真字段值的尾数。

表 15－失真字段参数的取值

参　　数	长度（比特）	取　　值
exp	4	0 ... 15
m	4	0 ... 15

需要注意的是，当使用这种格式的失真时，比较两个失真值哪个更大可以通过简单地比较两个作为无符号字符的失真值即可实现。尤其是，执行这种比较时，不需要将伪浮点格式转换为实际的总失真来判断哪个失真值更大或更小。这种特性可以简化在各种应用中的处理。

5.7.3.2.2 双字节失真字段

在双字节格式中，失真值应被表示为一个双字节的伪浮点格式。失真的伪浮点格式定义如下。此格式被用于 ITU-T T.800 建议书 | ISO/IEC 15444-1 的第 E.1.1.1 节（等于 E.3），来表示 JPEG 2000 的量子化步长。每个 16 比特的数字包含了测量值的指数（5 个比特）和尾数（11 个比特）。特别地，测量值的浮点值 *V* 由如下公式给出：

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

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

其中，ε 为无符号整数，从参数的前五个最高有效位中获得，μ 是一个无符号整数，从剩余的 11 个比特中获得。$V = \infty$ 的特殊情况对应于 $\mu = 0$ 且 $\varepsilon = 31$。注意如果取值下溢，则将其设置为零。

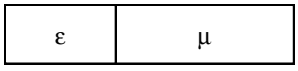


图 16－失真字段语法

ε: 双字节失真字段值的指数。

μ: 双字节失真字段值的尾数。

表 16－失真字段参数的取值

参　　数	长度（比特）	取　　值
ε	5	0 ... 31
μ	11	0 ... $(2^{11} - 1)$

计算ε和μ的算法在本建议书｜国际标准中不是一个必选部分。一个可能的技术执行的步骤如下所述（提供了一个转换数字 12.25 的一个示例）。如果 $V = 0$，则设置$\varepsilon = \mu = 0$。否则：

— 将V转换为一个二进制数字（$12.25_{10} = 1100.01_2$）；

— 将数字规范化；这意味着在二进制的小数点左边应当只有一个数字，并且通过适当的2的幂次来表示此原始值。1100.01规范化后的格式为：1.10001×2^3；

— 指数即为2的幂次，以余数符号来表示。指数的偏移量为15；因此对于本例，指数表示为18_{10}（10010_2）；

— 尾数表示有效位，即除了二进制小数点左面的一个比特之外，该比特总是1，因此不需要被存储；可能还会附加一些0以便获得11个比特。对于本例，尾数为10001000000。

5.7.3.2.3 相对重要性字段

相对重要性字段 *r* 可被用于描述不同编码单元之间的相对重要性，而没有必要将其绑定到一个特定的失真测量值上。这就允许人们可以描述编码单元之间的相对重要性或优先级，而不需要显式地描述一个比另一个重要多少。相关数据之间的这种相对重要性通过一个 n 字节的字段来指明，它可以支持 2^{8n} 种可能的等级，如图 17 和表 17 所示，其中本字段的字节个数 *n* 则由 Mzoi 来自指定。例如，通过使用一个单字节的相对重要性字段，可以支持总共 256 种可能的等级。值越大对应的重要性越大，类似于失真字段的模式。

图 17－相对重要性字段语法

r: 相对重要性的取值

表 17－相对重要性字段参数的取值

参　　数	长度（比特）	取　　值
r	8 * n	0 ... $(2^{8n} - 1)$

5.7.3.2.4 关于失真字段和相对重要性字段的附加注释

由于在单字节失真字段和单字节相对重要性字段中，都是取值越大对应的重要性越大，这就使得以相同的模式来比较这两个数据单元成为可能，而不必关心失真字段是否指定了一个实际的失真或一个相对的重要性。这可能会简化应用。

可以使用失真和相对重要性字段来指定头部。各种类型数据的丢失，如主头部和拼贴部分头部，或者 SEC 头部等，将不能够对相关图像数据进行解码。JPSEC 创建者可能会希望为这种数据分配失真值，有两种方法：

1） 或者使用最高失真值（下面将规定）来标记头部或关键数据；

2） 或者描述当图像或图像的一部分不能够被解码时，将产生的总失真。

于是，创建者在如何标记头部方面具有某些灵活性。

在单字节字段中，最高失真值是一个全 1 的字节（0xFF）。注意，对于单字节总方差失真字段和单字节相对重要性字段，这个值都是最高的可能失真值。对于双字节失真字段，最高失真值为全 1 的两个字节（0xFFFF）。对于长度为 n 个字节的相对重要性字段，最高重要性为全 1 的 n 个字节。

5.7.3.2.5 失真字段和相对重要性字段的联合使用

失真字段和相对重要性字段可被同时用于描述 ZOI 所指定的区域。在这种情况下，两个字段都指定了方差失真，然而，失真字段指定的是失真的递减，而相对重要性字段指定的是总失真。特别地，失真字段指定的是如果 ZOI 被解码后，它将产生的失真的递减。这里有一个假设，即解码 ZOI 所需的所有信息都是可用的，且集中于 ZOI 所产生的失真增减。相对重要性字段指定的是当 ZOI 不可用时引起的总失真，即它指定了当给定的 ZOI 不能够解码时所引起的总失真，这不仅统计了 ZOI 本身的值所引起的失真（如同失真字段所表示的），而且还统计了由于 ZOI 不能够解码而引起的压缩比特流的其他部分所产生的失真。与不同的 ZOI 相关联的总失真可以为不同 ZOI 的相对重要性提供一种有用的测量值。当这两个字段同时使用时，它们将使用相同的失真数学表达式，如同在失真字段中标识的那样。

5.7.3.3 比特率字段

比特率字段被用于指定小波系数域内的被保护区。它标识了最高有效位平面，该平面的压缩比特率是由本字段来指定的。MSB 的选择使用了第一部分中规定的率失真优化过程。例如，当比特率取值为 2.5 时，则被保护区包含压缩比特率为 2.5 比特每像素的所有小波系数的 MSB。比特率字段的语法在图 18 和表 18 中显示。所指定的比特率由如下公式给定：

$$R = I_R + F_R/16$$

例如，一个值为 0 的比特率由 $I_R = 0$ 和 $F_R = 0$ 表示；一个值为 2.5 的比特率由 $I_R = 2$ 和 $F_R = 8$ 表示。

图 18－比特率字段语法

I_R: 指定的比特率的整数部分。

F_R: 指定的比特率的小数部分。

表 18－比特率字段参数的取值

参　　数	长度（比特）	取　　值
I_R	4	0 ... 15
F_R	4	0 ... 15

5.7.4 多个参数之间的关系

5.7.4.1 综述

如果与图像相关的描述类同时具有多个字段集，则由此形成的区域应当是这些字段的交集。例如，一个区域可以指定在第二个拼贴中具有最低分辨率。字段的联合可以通过在 ZOI 中使用多个区域来指定。

与非图像相关的描述类也可能同时具有多个字段集。当这种情况发生时，不同参数字段的模式应当具有相同数量的项（此规则的一个例外在下面描述），且这些项之间应当以一一对应的方式相互对应。例如，如果区域使用了字节范围和包范围，则每一种都必须具备相同数量的范围项，且其中第一个字节范围应对应于第一个包范围，依次类推。

针对上述要求每个字段都具有相同数量的项的规则有一个例外。例外发生在这种情况下，即其中一个字段 f1 包含一个项，该项指定了一个包含 N 个元素的项范围（如同第 5.7.6 节描述的范围模式），而另一个字段 f2 是通过 N 个项的列表来指定的。在这种情况下，仅包含一个项（范围）的字段 f1 被解释为如同含有 N 个项的列表。由 f1 中的范围所规定的这 N 个项应当与 f2 中所列的 N 个项一一对应。因此，一个项范围可以与一个单独的项相关联，也可以与多个项相关联（其中每个项对应范围中的每个项）。

5.7.4.2 示例

同图 11 中所示，区域描述类结构可以同时具有多个字段集，其中，N 个字段是与图像相关的描述（$D_i^1, D_i^2, \cdots, D_i^N$），M 个字段是与非图像相关的描述（$D_n^1, D_n^2, \cdots, D_n^M$）。语义可以被理解为 $\{D_i^1 \cap D_i^2 \cap \cdots \cap D_i^N\} = D_n^1 = D_n^2 = \cdots = D_n^M$，也就是说，N 个与图像相关的描述的交集对应于 M 个与非图像相关的描述中的每一个，另外，M 个与非图像相关的描述也是相互对应的。这种关系可以通过下面的三个示例作更进一步地描述。

在第一个示例中，区域描述具有两个与图像相关的描述，一个是分辨率 2，另一个是层 3。在这种情况下，受影响的数据是分辨率 2 和层 3 的交集，如图 19 所示。

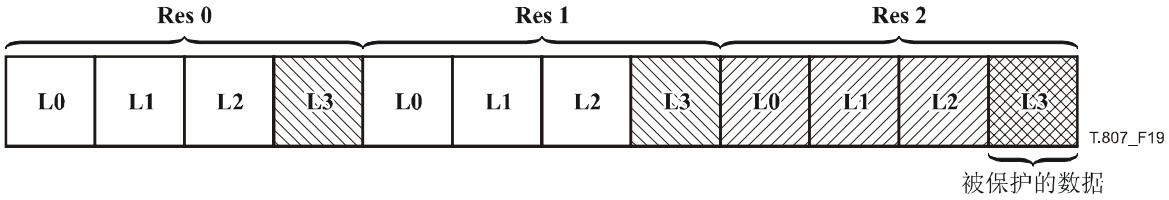


图 19－使用与图像相关的描述的ZOI示例

在第二个示例中，区域描述具有两个与图像相关的描述（分辨率 2 和层 3），以及一个与非图像相关的描述（包范围为 80-100）。在这种情况下，受影响的数据是分辨率 2 和层 3 的交集。此外，还指示了受影响的数据包含在范围从 80 到 100 的包中。

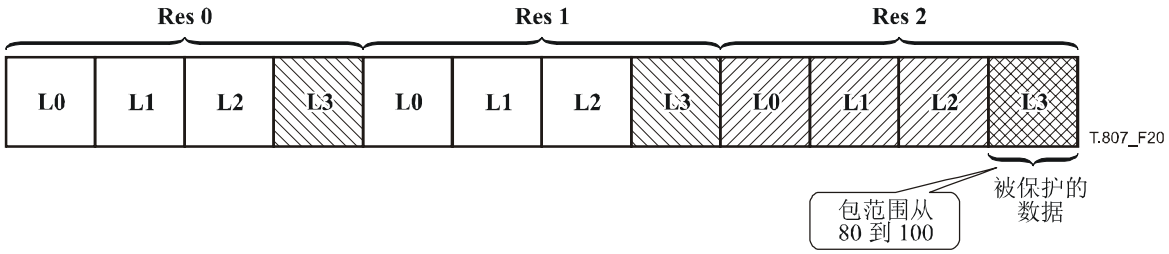


图 20－使用与图像相关的和与非图像相关的描述的ZOI示例

在第三个示例中，区域描述具有两个与图像相关的描述（分辨率 2 和层 3），以及两个与非图像相关的描述（包范围为 80-100，以及字节范围为 856-1250）。同样的，受影响的数据为分辨率 2 和层 3 的交集，且受影响的数据被包含在范围为从 80 到 100 的包内。此外，这些包和受影响的数据还位于范围在 856-1250 之间的字节中。

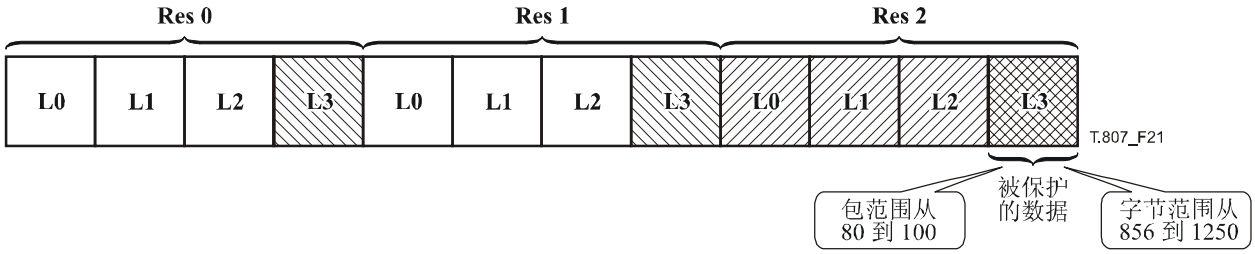


图 21－使用与图像相关的和与非图像相关的描述的第二个ZOI示例

5.7.5 保护跟随在SEC标记后的任何数据

上述的讨论大量地集中于支持 JPEG 2000 码流的保护服务上。然而，主头部中的许多元素，包括 JPSEC 指示，也应当是被保护的，并且 ZOI 和保护方法也可以用于此目的。

特别地，与非图像相关的描述类中的字节范围模式可以被用来指定一个 JPSEC 工具应当被应用在跟随在 SEC 标记之后的任何数据上。正如前面所描述的，SEC 头部的第一个字节为 1 指示的是字节范围。跟随在 SEC 标记之后的、并且能够被保护的数据包括 SEC 段以及主头部中的大部分内容。注意，JPEG 2000 主头部的所有部分，除了 SIZ 标记段之外，都可以被移动到 SEC 标记之后，因此都可以使用上述方法来保护它们。如果 JPEG 2000 的 SIZ 标记段要被保护，则必须在一个更高的层次上来执行，如在文件格式层。

用于保护 SEC 段的 JPSEC 工具一般来说应当是 SEC 段中的第一个工具。这就使得消费者可以首先恢复 SEC 段数据，这些数据然后可被用于处理码流的剩余部分。

5.7.6 区域描述参数语法（Pzoi）

图 22 显示了 ZOI 描述参数的语法。

图 22－ZOI描述参数语法

Mzoi: ZOI 描述模式。本字段使用 FBAS 结构。

Nzoi: Izoi 的个数。本字段使用 RBAS 结构。

Izoi^{i}: 项。

表 19－Pzoi^{i} 参数的取值

参　　数	长度（比特）	取　　值
Mzoi	可变的（FBAS）	见表 20
Nzoi	0 8 + 8 * n (RBAS)	当 Mzoi 的第 2 个比特取值为 0 时。 2 ... (2^{7+7*n} – 1)
Izoi^{i}	可变的	依赖于 Mzoi 中指定的模式

表 20－Mzoi 参数的取值

FBAS比特号	取值（比特）	语　　义
1	0	指定的区域是受 JPSEC 工具影响的区域
	1	指定区域的补集是受影响的区域
2	0	指定了单个项
	1	指定了多个项
3, 4	00	矩形模式。一个矩形区域，其中第一个值对指定了左上角，第二个值对指定了右下角，并且这两个角都包含在内。对于每一个角，第一个值为水平位置，第二个值为垂直位置。标定指数应当从 0 起始，并应当使用 JPEG 2000 第一部分中定义的参考栅格。
	01	范围模式。一个值的范围，其中第一个值指定了起始索引，第二个值指定了最后一个索引，并且这两个值都包含在内。
	10	索引模式。指定了一个单独的值。
	11	最大模式。指定了一个最大的值。
5, 6	00	Izoi^{i} 使用 8 个比特的整数
	01	Izoi^{i} 使用 16 个比特的整数
	10	Izoi^{i} 使用 32 个比特的整数
	11	Izoi^{i} 使用 64 个比特的整数

表 20－Mzoi 参数的取值

FBAS比特号	取值（比特）	语　　义
7, 8	00	$Izoi^i$ 使用一个维度来描述
	10	$Izoi^i$ 使用两个维度来描述
	01	$Izoi^i$ 使用三个维度来描述
9	0	偏移量，当长度模式没有使用时
	1	偏移量，当使用了长度模式时：指定了初始偏移量，以及后续的各连续字节的长度。此标记的存在应当取代第 3 个和第 4 个比特所指定的模式。
		所有其他值都保留

如果使用了 TRLCP 标签，则它们的长度通过表 4 中指定的 P_{TRLCP} 来定义。在这种情况下， M_{ZOI} 参数的第 5 个和第 6 个比特的值将被取代。

长度模式中的偏移量可被用于有效地表示一系列的连续段，例如一系列的连续字节范围。其中，第一个值指定了起始偏移量，后续值指定了每个连续段的长度。如果本字段用于表示 n 个段，则 Nzoi 应当被设置为 n + 1。

5.8　保护方法模板语法（T）

5.8.1　概述

保护方法模板包含了第 5.6.1 节描述的特定 JPSEC 工具的参数。例如，它们可被用于第 5.6.2 节描述的 JPSEC 标准工具中。同样的，它们也可被用于第 5.6.3 节描述的 JPSEC 非标准工具中。有三种类型的保护方法模板：解密模板，认证模板和哈希模板。一个 JPSEC 标准工具所使用的模板通过其 ID 来指定，如表 6 所示，在表 21 中再次给出，并指向了定义它们的相应小节。

正如在第5.6.2 节中描述的那样，保护方法模板 T，与 JPSEC 工具的处理域 PD，粒度 G，以及值列表 V 一起，描述了一个 JPSEC 工具是如何被应用的。

表 21－模板ID的取值（ID_T）

取　　值	保护方法模板
0	保留
1	解密模板。见5.8.2。
2	认证模板。见5.8.3。
3	哈希模板。见 5.8.4。
4	空工具
	所有其他值都保留供 ISO 使用

5.8.2　解密模板（$T = T_{decry}$, 当t = 0且ID = 1时）

解密模板，T_{decry}，用于与解密器沟通关于如何解密接收到的码流。图 23 显示了解密模板的语法。表 22 显示了解密模板的符号和参数的长度及取值。

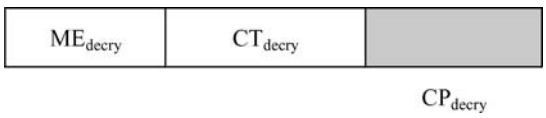


图 23－解密模板的语法

ME_{decry}: 假的标记竞争记号，指示了是否有一个假的标记竞争出现在加密后的数据中。一个假的标记竞争可能会对与 JPEG 2000 第一部分解码器的兼容性产生不利影响。本字段使用 FBAS 结构。

CT_{decry}: 密码类型标识。

CP_{decry}: 密码参数。

表 22－解密模板参数的取值

参　　数	长度（比特）	取　　值
ME_{decry}	8 + 8 * n (FBAS)	表 23
CT_{decry}	16	表 24
CP_{decry}	可变的	当 $CT_{decry} < 0x6000$ 时，见 5.8.2.1。 当 $0x6000 \le CT_{decry} < 0xC000$ 时，见 5.8.2.2。 当 $CT_{decry} \ge 0xC000$ 时，见5.8.2.3。

表 23－标记竞争记号的取值（ME_{decry}）

取　　值	方 法 类 型
01xx xxxx	加密数据没有包含一个假的标记竞争
00xx xxxx	相反情况
	所有其他值都保留供 ISO 使用

标记竞争记号的缺省值为 0。此标记可能被设置为 1，来指示 JPSEC 加密数据中没有包含一个假的标记竞争。一个 JPSEC 创建者可能会选择保持此标记为其缺省值 0。

表 24－密码标识符的取值（CT_{decry}）

取　　值	密 码 类 型
0 ... 0x5FFF	块密码（见表 25）
0x6000 ... 0xBFFF	流密码（见表 26）
0xC000 ... 0xFFFF	非对称密码（见表 27）

表 25－块密码标志符的取值（CT_{decry}）

取　　值	密 码 类 型
0x0000	空 （没有加密）
0x0001	AES (ISO/IEC 18033-3)
0x0002	TDEA (ISO/IEC 18033-3)
0x0003	MISTY1 (ISO/IEC 18033-3)
0x0004	Camellia (ISO/IEC 18033-3)
0x0005	CAST-128 (ISO/IEC 18033-3)
0x0006	SEED (ISO/IEC 18033-3)
	所有其他值都保留供 ISO 使用

表 26－流密码标识符的取值（CT_{decry}）

取　　值	密 码 类 型
0x6000	SNOW 2 (ISO/IEC 18033-4)
	所有其他值都保留供 ISO 使用

表 27－非对称密码标识符的取值（CT_{decry}）

取　　值	密 码 类 型
0xC000	RSA-OAEP (ISO/IEC 18033-2)
	所有其他值都保留供 ISO 使用

5.8.2.1 块密码模板（用于块密码的CP_{decry}）

块密码模板用于与块解密器沟通关于如何解密接收到的码流。图 24 显示了块密码的模式，填充模式，块长度以及密码信息等。

一些块密码模式可以使用初始向量。对于这些模式，工具的初始向量可以使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。特别地，初始向量仅被用于 ID M_{bc} > 0x80 的那些模式，例如 CBC，CFB，OFB 和 CTR 等。在 CTR 情况下，它并不是一个真正的 IV，而是一个计数器。值列表 V 中指定的初始向量的长度应当被设置为块长度 SIZ_{bc}。

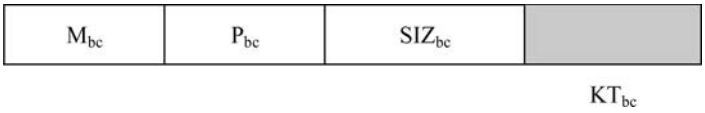


图 24－块密码模板的语法

M_{bc}: 块密码模式。第一个比特指示此工具是否使用初始向量。当 M_{bc} < 0x8 时，不使用 IV，否则本模式要求一个或多个 IV 值。

P_{bc}: 填充模式。

SIZ_{bc}: 块的长度，以字节计数。

KT_{bc}: 密钥模板（见 5.8.5）。它拥有此块密码所使用的密钥的信息。

表 28－块密码模板的取值

参　　数	长度（比特）	取　　值
M_{bc}	6	表 29
P_{bc}	2	表 30
SIZ_{bc}	8	1 ... 256
KT_{bc}	可变的	见5.8.5

表 29－块密码模式的取值（M_{bc}）

取　　值	模 式 类 型
0	保留
0x xxxx	没有使用 IV 的模式
1x xxxx	使用了一个 IV 的模式
x0 xxxx	比特未被填充
x1 xxxx	比特被填充
0x 0001	ECB (ISO/IEC 10116)
1x 0010	CBC (ISO/IEC 10116)
1x 0011	CFB (ISO/IEC 10116)
1x 0100	OFB (ISO/IEC 10116)
1x 0101	CTR (ISO/IEC 18033-2)
	所有其他值都保留供 ISO 使用

注 1 — 对于所有模式都要求实现时要小心，因为不恰当的实现可能会导致漏洞。需要注意的是即使ECB被正确实现，当出现了相同的块时，也还会有信息泄漏。在ISO/IEC 10116中包含了指南。

注 2 — 只有当表29中的M_{bc}指定了比特被填充时，表30中的取值才会出现。当比特没有被填充时，P_{bc} 应当被设置为00。

表 30－块密码的填充模式（P_{bc}）

取　　值	填 充 类 型
00	密文挪用（RFC 2040）
01	PKCS#7-填充（PKCS#7）
	所有其他值都保留供 ISO 使用

注 3 — 当使用填充时，必须进行小心的系统设计以避免潜在的安全漏洞，例如选择密码攻击。

5.8.2.2 流密码模板（用于流密码的CP_{decry}）

流密码模板用于与流解密器沟通关于如何解密接收到的码流。图 25 显示了流密码模板的语法。表 31 显示了流密码模板的取值。

流密码的初始向量使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。在值列表 V 中指定的初始向量的长度应当被设置为在密钥信息模板 KT_{sc} 中定义的密钥的长度。

KT_{sc}

图 25－流密码模板的语法

KT_{sc}: 密钥信息模板（见5.8.5）。它拥有此流密码所使用的密钥的信息。

表 31－流密码模板的取值

参　　数	长度（比特）	取　　值
KT_{sc}	可变的	见 5.8.5

5.8.2.3 非对称密码模板（用于非对称密码的CP_{decry}）

非对称密码模板用于与非对称密码的解密器沟通关于如何解密接收到的码流。图 26 显示了非对称密码模板的语法。表 32 显示了非对称密码模板的取值。

对于使用非对称密码模板的工具，工具的粒度字段（G）指定了密码被应用的粒度。然而，没有使用值列表字段（V）来表示任何值。因此，值列表字段中元素的个数（N_v）应当被设置为 0。

KT_{sy}

图 26－非对称密码模板的语法

KT_{sy}: 密钥信息模板（见5.8.5）。它拥有此非对称密码所使用的密钥的信息。

表 32－非对称密码模板的取值

参　　数	长度（比特）	取　　值
KT_{sy}	可变的	见 5.8.5

5.8.3 认证模板（T = T_{auth}，当t = 0且ID = 2时）

认证模板，T_{auth}，被用于与验证者沟通关于如何验证接收到的码流的真实性。有三种通用类型的认证方法：基于哈希的认证，基于密码的认证和数字签名。基于哈希的认证方法和基于密码的认证方法，一般也都被称为消息认证码（MAC），且它们的用于认证的计算值一般被称为 MAC 值。认证模板的语法在图 27 中显示，表 33 显示了认证模板符号和参数的长度及取值。

在许多安全应用中，认证是一项最重要的安全服务。即使是当机密性作为一种目标安全服务时，它也应当通过认证来加强，以防止各种形式的攻击。特别地，推荐对 SEC 标记段的一部分进行认证。另外，还应当对认证模板参数（T_{auth}）和认证消息进行认证。尤其是，影响区应当指定将要被认证的内容和认证模板参数（T_{auth}）。

图 27－认证模板的语法

M_{auth}: 认证方法。
P_{auth}: 认证参数。

表 33－认证模板参数的取值

参　　数	长度（比特）	取　　值
M_{auth}	8	表 34
P_{auth}	可变的	当 M_{auth} = 0 时，见5.8.3.1 当 M_{auth} = 1 时，见 5.8.3.2 当 M_{auth} =2 时，见 5.8.3.3

表 34－认证方法（M_{auth}）

取　　值	方　　法
0	基于哈希的 MAC
1	基于密码的 MAC
2	数字签名
	所有其他值都保留供 ISO 使用

5.8.3.1 基于哈希的认证（基于哈希的MAC的P_{auth} ）

基于哈希的认证 MAC 被用于与验证者沟通关于如何验证接收到的码流的真实性。图 28 显示了基于哈希的认证模板语法，表 35 显示了参数的取值。

MAC 值使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。在值列表 V 中指定的 MAC 值的长度应当被设置为由 SIZ_{HMAC} 定义的 MAC 的长度。

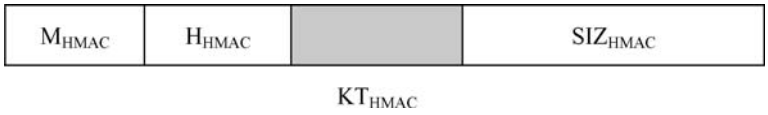


图 28－基于哈希的认证模板

M_{HMAC}: 基于哈希的认证方法标识符。
H_{HMAC}: 哈希标识符。
KT_{HMAC}: 密钥模板。
SIZ_{HMAC}: MAC 的长度（比特）。

表 35－基于哈希的认证模板参数的取值

参　　数	长度（比特）	取　　值
M_{HMAC}	8	表 36
H_{HMAC}	8	表 37
KT_{HMAC}	可变的	见 5.8.5
SIZ_{HMAC}	16	0 ... 65535

表 36－基于哈希的认证方法标识符（M_{HMAC}）

取　　值	基于哈希的认证方法
0	保留
1	HMAC (ISO/IEC 9797-2)
	所有其他值都保留供 ISO 使用

表 37－哈希函数标识符（H_{HMAC}）

取　　值	哈 希 函 数
0	保留
1	SHA-1 (ISO/IEC 10118-3)
2	RIPEMD-128 (ISO/IEC 10118-3)
3	RIPEMD-160 (ISO/IEC 10118-3)
4	MASH-1 (ISO/IEC 10118-4)
5	MASH-2 (ISO/IEC 10118-4)
6	SHA-224 (ISO/IEC 10118-3)
7	SHA-256 (ISO/IEC 10118-3)
8	SHA-384 (ISO/IEC 10118-3)
9	SHA-512 (ISO/IEC 10118-3)
10	WHIRLPOOL (ISO/IEC 10118-3)
	所有其他值都保留供 ISO 使用

注意，如果 SIZ_{HMAC} 少于哈希的常规长度，则它是对应哈希第一个 SIZ_{HMAC} 比特的一个删节版。

5.8.3.2 基于密码的认证模板（基于密码的MAC的P_{auth}）

基于密码的认证 MAC 被用于与验证者沟通关于如何验证接收到的码流的真实性。图 29 显示了其认证模板，表 38 显示了密钥长度和带密钥的哈希函数。基于密码的认证模式的一个示例是 CBC-MAC。在这些用于认证的块密码技术中，初始向量的长度为一个块大小，且取值为 0。块大小是块密码的缺省值。注意，如果 SIZ_{CMAC} 少于基于密码的认证 MAC 的常规长度，则它是对应此 MAC 的第一个 SIZ_{CMAC} 比特的一个删节版。

注意，如果数据比特的数量不是密码块大小的整数倍，则最后的输入块将是一个部分数据块，并向左对齐，然后用零附加在后面以便构成一个完整的密码块。另外还要注意，CBC-MAC 应当仅仅被应用于具有固定已知长度的数据。

MAC 值使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。在值列表 V 中指定的 MAC 值的长度应当被设置为由 SIZ_{CMAC} 定义的 MAC 的长度。

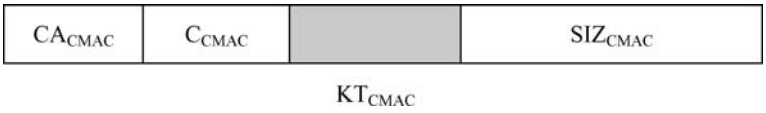


图 29－基于密码的认证模板语法

CA_{CMAC}: 基于密码的认证方法。

C_{CMAC}: 块密码标识符值。

KT_{CMAC}: 密钥模板。

SIZ_{CMAC}: MAC 的长度（比特）。

表 38－MAC模板的取值

参　　数	长度（比特）	取　　值
CA_{CMAC}	8	表 39
C_{CMAC}	8	表 25
KT_{CMAC}	可变的	见 5.8.5
SIZ_{CMAC}	16	0 ... 65535

表 39－基于密码的认证方法（C_{CMAC}）

取　　值	方　　法
0	CBC-MAC MAC 算法 1 (ISO/IEC 9797-1)
1	CBC-MAC MAC 算法 2 (ISO/IEC 9797-1)
2	CBC-MAC MAC 算法 3 (ISO/IEC 9797-1)
3	CBC-MAC MAC 算法 4 (ISO/IEC 9797-1)
	所有其他值都保留供 ISO 使用

5.8.3.3 数字签名模板（数字签名的P_{auth}）

数字签名被用于与验证者沟通关于如何验证接收到的码流的真实性，同时出于身份认证和不可否认的目的而验证发送者的身份。图 30 定义了其模板，表 40 列出了取值。

数字签名使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。在值列表 V 中指定的数字签名值的长度应当被设置为可以容纳由 SIZ_{DS} 定义的长度。由于值列表的长度是由字节而不是比特来表示的，因此其长度应当是可以容纳 SIZ_{DS} 的最小的字节数。每个值都使用最低有效位比特来表示，且额外的 MSB 比特应当被设置为 0。

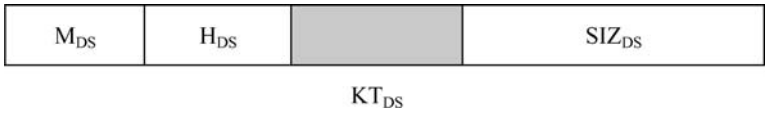


图 30－数字签名模板的语法

M_{DS}: 数字签名方法。

H_{DS}: 哈希函数。

KT_{DS}: 密钥模板（见5.8.5）。它拥有与验证数字签名所需的公钥或证书相关的所有信息。

SIZ_{DS}: 数字签名的长度（比特）。

表 40－数字签名模板的取值

参　　数	长度（比特）	取　　值
M_{DS}	8	表 41
H_{DS}	8	表 37
KT_{DS}	可变的	见 5.8.5
SIZ_{DS}	16	0 ... 65535

表 41－数字签名方法（M_{DS}）

取　　值	方　　法
1	RSA (ISO/IEC 14888-2)
2	Rabin (ISO/IEC 14888-2)
3	DSA (ISO/IEC 14888-3)
4	ECDSA (ISO/IEC 14888-3)
	所有其他值都保留供 ISO 使用

5.8.4　哈希模板（T = T_{hash}，当t = 0且ID = 3时）

哈希模板，T_{hash}，被用于传送计算哈希值的参数。表 42 显示了哈希模板中符号和参数的长度及其值。

注意，与第 5.8.3.1 节中讨论的基于哈希的认证模板相比较，该模板使用了一个哈希函数和一个密钥，而本哈希模板没有使用私钥。本哈希模板可被用于检测一个偶然错误或数据的一个偶然改变，但它并不能够防止对数据的恶意修改。为了防止对数据的恶意修改，必须使用一个认证模板，因为认证模板所使用的私钥可以防止数据不被发现地被篡改。

哈希值使用第 5.10 节描述的工具的粒度字段（G）和第 5.11 节描述的值列表字段（V）来指定。在值列表 V 中指定的哈希值的长度应当被设置为由 SIZ_{hash} 定义的哈希值长度。

H_{hash}	SIZ_{hash}

图 31－哈希模板的语法

H_{hash}: 哈希函数标识符。

SIZ_{hash}: 哈希值的长度（字节）。

表 42－哈希模板参数的取值

参　　数	长度（比特）	取　　值
H_{hash}	8	表 37
SIZ_{hash}	8	0 ... 255

5.8.5 密钥信息模板（KT）

密钥信息模板用于传送密钥信息。图 32 定义了此模板，表 43 列出了取值。

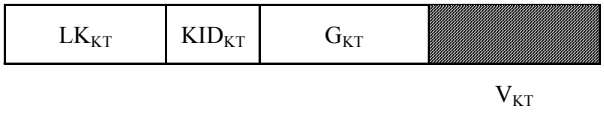


图 32－密钥信息模板的语法

LK_{KT}: 密钥的长度，以比特计数。

KID_{KT}: 密钥信息标识符。它指示了值列表 V_{KT} 中的值的含义。在解密模板中，此值必须被设置为 2（查询私钥的 URI）。在数字签名情况下，本字段的值空缺。

G_{KT}: 表示密钥信息修改粒度的粒度字段。

V_{KT}: 表示密钥信息修改列表的值列表字段。

注意在使用私钥的情况下（解密模板），公钥和证书是没有意义的：密钥模板应当拥有关于密钥所在位置的某些信息（如 URI）。

密钥信息可以使用第 5.10 节描述的工具的粒度字段（G_{KT}）和第 5.11 节描述的值列表字段（V_{KT}）中的一个或多个值来表示。这两个字段（G_{KT} 和 V_{KT}）共同决定了值列表（V_{KT}）中的密钥值是如何应用到被保护的图像数据上的，如第 5.10 节和第 5.11 节中的描述。

值列表中的密钥信息可以采用表 44 中规定的格式之一。当 $KID_{KT}=1$ 时，则每个值采用第 5.8.5.1 节中描述的 X.509 证书模板来指定。当 $KID_{KT}=2$ 时，则每个值采用证书或私钥的一个 URI 来指定。

表 43－密钥模板的取值

参　　数	长度（比特）	取　　值
LK_{KT}	16	1 ... 65535
KID_{KT}	8	表 44
G_{KT}	24	见 5.10
V_{KT}	可变的	见5.11

表 44－密钥信息标识符的取值（KID_{KT}）

取　　值	密钥信息标识符
0	保留
1	X.509 证书(ISO/IEC 9594-8)
2	证书或私钥的 URI
	所有其他值都保留供 ISO 使用

5.8.5.1 X.509证书模板

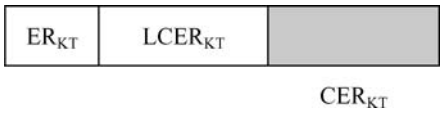


图 33－X.509证书的语法

ER_{KT}: X.509 证书的编码规则。

$LCER_{KT}$: X.509 证书（CER_{KT}）的长度，以字节计数。

CER_{KT}: X.509 证书。

表 45－X.509证书的取值（KI_{KT}，当KID_{KT} = 2时）

参　　数	长度（比特）	取　　值
ER_{KT}	8	0 ... 255 （见表 46）
$LCER_{KT}$	16	1 ... 65535
CER_{KT}	可变的	–

表 46－编码规则的取值（ER_{KT}）

取　　值	编码规则标识符
0	保留
1	DER (RFC 3217)
2	BER (RFC 3394)
	所有其他值都保留供 ISO 使用

5.9　　处理域语法（PD）

处理域语法用于指示 JPSEC 工具被应用在哪个域。可能的域包括像素域，小波系数域，量化的小波系数域以及码流域。

图 34－处理域的语法

PD: 处理域。本字段使用 FBAS 结构。

F_{PD}: 提供关于处理域的更详细信息的处理域字段。本字段使用 FBAS 结构。

表 47－处理域参数

参　　数	长度（比特）	取　　值
PD	可变的(FBAS)	见表 48
F_{PD}	可变的(FBAS)	小波系数域和量化的小波系数域，见表 49。 码流域，见表 50。

表 48－处理域（PD）参数的取值

FBAS比特号	取　　值	语　　义
1	1	像素域。保护方法应用在图像的像素上。
	0	相反情况
2	1	小波系数域。保护方法应用在小波系数上。
	0	相反情况
3	1	量化的小波系数域。保护方法应用在量化的小波系数上。
	0	相反情况
4	1	码流域。保护方法应用在算术编码器产生的码流上。
	0	相反情况

注意，字段 PD 应当有且仅有一个比特被设置为 1，因为每种 JPSEC 工具只能被应用到一个域上。

在图像像素域，小波系数域和量化的小波系数域，为了应用安全工具，二维数据必须被转换为一维数据。这种转换应当通过以光栅扫描顺序来对二维的图像数据进行扫描而完成。

表 49－小波系数域和量化的小波系数域情况下处理域字段（F_{PD}）参数的取值

FBAS比特号	取　　值	语　　义
1	0	保护方法应用于标记比特
	1	保护方法应用于最高有效位比特

表 50－码流域情况下处理域字段（F_{PD}）参数的取值

FBAS比特号	取　　值	语　　义
1	0	保护方法应用于包头和包体
	1	保护方法仅应用于包体

字段（F_{PD}）被用于提供关于处理域的更详细信息。根据 PD 的不同取值，此字段（F_{PD}）具有不同的语义。例如，在小波系数域和量化的小波系数域情况下，F_{PD} 的第一个比特用于指示 JPSEC 工具是否是应用于最高有效位。在码流域情况下，F_{PD} 的第一个比特用于指示 JPSEC 工具是仅应用于包体，还是同时应用于包头和包体；在像素域情况下，此字段（F_{PD}）保留。

5.10　粒度语法（G）

粒度用于指示每种保护方法的保护单元。表 53 定义了可能的粒度。图 35 显示了粒度的语法。

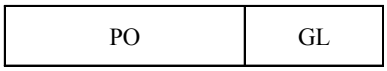


图 35－粒度的语法

PO: 处理顺序。

GL: 粒度级别。

表 51－粒度参数的取值（G）

参　　数	长度（比特）	取　　值
PO	16	见表 52
GL	8	见表 53

表 52－处理顺序的取值（PO）

取值 MSB　LSB	处 理 顺 序
0 000 000 000 000 000	按照影响区中与图像相关的参数所指定的顺序
1 000 000 000 000 000	按照影响区中与非图像相关的比特流参数指定的顺序
1 000 000 000 000 001	按照影响区中与非图像相关的包参数指定的顺序
0 000 001 010 011 100	拼贴-分辨率-层-分量-选区
0 000 011 100 001 010	拼贴-分量-选区-分辨率-层
0 000 010 001 011 100	拼贴-层-分辨率-分量-选区
0 000 100 011 001 010	拼贴-选区-分量-分辨率-层
0 000 001 100 011 100	拼贴-分辨率-选区-分量-层
	所有其他值都保留

表 53－粒度级别的取值（GL）

取值 MSB　LSB	粒　　度
0000 0000	拼贴
0000 0001	拼贴-部分
0000 0010	分量
0000 0011	分辨率级别
0000 0100	层
0000 0101	选区
0000 0110	包
0000 0111	子带
0000 1000	码块
0000 1001	ZOI 中指定的全部区域
1000 0000	在与非图像相关的 ZOI 中指定的项
1000 0001	在与非图像相关的 ZOI 中指定的区域
	所有其他值都保留

如果要处理 ZOI 指定的全部区域，则粒度级别应当是“ZOI 中指定的区域”。

5.11　值列表语法（V）

值列表字段被用于指定随着工具的应用而变化的值，以及随着与之相应的粒度改变而变化的值。它被用于标示变化的值，如密钥，初始向量，MAC 值，数字签名，以及哈希值等。值列表字段首先指定列表中值的个数以及每个值的长度。然后列出这些值本身。

正如在第 5.6.2 节讨论的那样，对于 JPSEC 标准工具，值列表字段为每个模板都表示了不同的参数。对于解密模板，它表示初始向量 IV_{bc} 或 IV_{sc}，依赖于使用的是块密码还是流密码。对于认证模板，它为基于哈希的认证和基于密码的认证表示了 MAC 值 VAL_{MAC}。对于数字签名模板，它表示数字签名 SIG_{DS}。对于哈希模板，它表示哈希值 HV_{hash}。模板的某些用法是不需要指定值的，如并不是所有的解密方式都使用初始向量。在这些情况下，值列表字段应当将 N_v 和 S_v 设置为等于 0，这样值列表字段 VL 就没有元素了。如果仅需要指定一个单独的值，如在整个图像中如果仅需要一个单独的密钥，则 N_v 将被设置为 1，这样在值列表中就包含一个单独的值。

图 36－值列表字段的语法

N_V: 值列表 VL 中值的个数，如果 $N_V = 0$，则本字段结束。本字段使用 RBAS 结构。

S_V: 值列表 VL 中的每个值的长度，以字节计数。本字段使用 RBAS 结构。

VL: 值的列表。

表 54－值列表字段（V）参数的取值

参　　数	长度（比特）	取　　值
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，当 NV = 0 时 N_V * S_V，其他情况下	N/A 根据模板取值

5.12 ZOI，粒度（G）和值列表（VL）之间的关系

ZOI，PO 和 GL 被一起使用来确保所应用的 JPSEC 工具具有唯一的行为，而不用考虑 JPEG 2000 码流的进展顺序。换句话说，作为结果的签名、MAC 值和加密码流是独立于 JPEG 2000 码流的进展顺序的。影响区（ZOI）使用其全部字段指定了被 JPSEC 工具所保护的 JPEG 2000 码流的那部分；而另一方面，处理顺序（PO）指定了 JPSEC 工具处理码流的顺序；粒度级别（GL）指定了保护单元，该保护单元包含了处于重新排序后的码流中的相邻字节序列。最后，每个保护单元都对应值列表（VL）中的一个值，其顺序便是它们出现在重新排序后的码流中的顺序。这种关系可以使用一个示例来说明，在该示例中，JPEG 2000 码流具有一个拼贴，3 个分辨率级别和 3 个层，且分量和区域的个数是不重要的。其进展顺序为初始 JPEG 2000 码流中的 RLCP，影响区为分辨率 0 和 1，以及处理顺序（PO）为 TRLCP。图 37 和 38 分别显示了当粒度级别（GL）分别为分辨率和层时，码流如何重新排序，以及如何从每个保护单元映射到值列表（VL）。

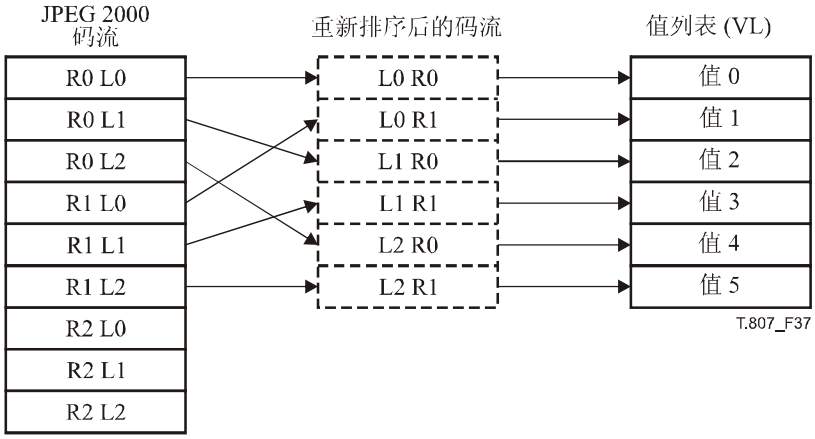


图 37－粒度级别（GL）为分辨率

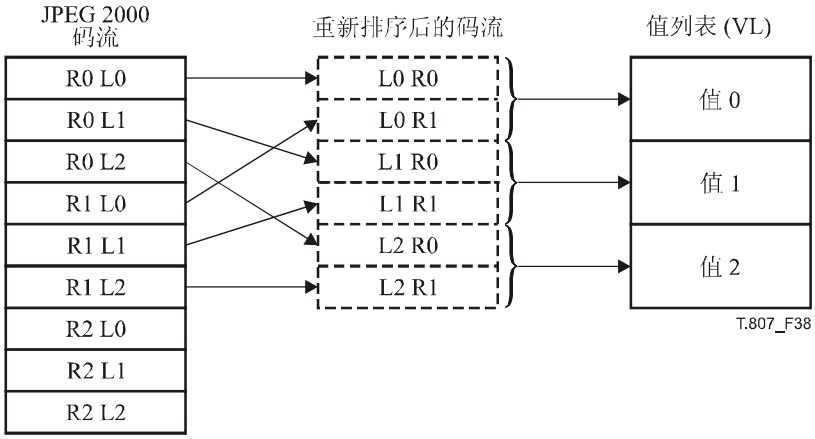


图 38－粒度级别（GL）为层

注 — 重新排序后的码流仅用于产生值列表（VL）中的值。最终的JPSEC码流将与初始的JPEG 2000码流具有相同的进展顺序。

5.13 内部码流安全标记（INSEC）

内部码流安全标记（INSEC）为传送安全信息提供了一种额外的方法。它是可选的，可与 SEC 安全标记一起使用。特别地，它与一种 JPSEC 非标准工具一起使用。

更确切地说，SEC 标记出现在主头部中，它给出了用来保护图像的 JPSEC 工具的全部信息。INSEC 标记出现在比特流数据本身，它为由工具实例索引参数所标识的 JPSEC 非标准工具给出了附加的参数或可替代的参数。因此，INSEC 标记中的工具实例索引应当对应于主头部中的工具实例索引之一。

INSEC 标记段可置于比特流数据中。它利用了这样一个事实，即 JPEG 2000 中的算术解码器在遇到一个终止标记（即两个字节，其值大于 0xFF8F）时，将停止读取比特流中的字节。

在 INSEC 标记段中携带的信息是与之前或之后的安全码块相关的，除非遇到另一个 INSEC 标记。

需要注意的是包含 INSEC 标记将会导致可能出现一个不符合 JPEG 2000 第一部分的文件。注意某些解码器可能会难以处理一个处于包中间的标记。在包的任何一个地方插入，都会使得在包头中指示的包长度失效。另外，关于加密和 INSEC 标记之间也可能会有问题，因为：

a） 在加密时缺少标记竞争的限制；和/或

b） 当存在加密时，没有能力定位标记本身。

INSEC 标记的语法在图 39 中定义。

图 39－内部码流安全标记语法

INSEC: 标记码。表 55 显示了内部码流安全标记段中的符号和参数的长度及取值。

L_{INSEC}: 标记段的长度，以字节计数（不包括标记本身）。注意 INSEC 标记段必须是字节对齐的。

i: 对应于 SEC 标记段中的工具实例索引参数之一的工具实例索引，因此标识了本 INSEC 标记所涉及的 JPSEC 工具实例。本字段使用 RBAS 结构。

R: INSEC 信息的相关区域。本字段使用 FBAS 结构。

AP: 保护方法的附加参数或可替代参数。编码者应当总是要确保编码者不能在此参数中竞争一个标记。

表 55－内部码流安全参数的取值（INSEC）

参　　数	长度（比特）	取　　值
INSEC	16	0xFF94
L_{INSEC}	16	2 ... $(2^{16} - 1)$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
R	可变的 (FBAS)	见表 56
AP	可变的	由注册机构或应用程序定义

表 56－相关区域的取值（R）

FBAS比特号	取　　值	相 关 区 域
0	0	之前的码块
	1	之后的码块

由于 INSEC 与 JPSEC 非标准工具一起使用，因此附加参数或可替代参数的格式由工具自身来定义，而工具由工具 ID 来标识。特别地，JPSEC 非标准工具是由某个注册机构或专用的 JPSEC 应用程序来定义的。因此，如果允许的话，这些工具的定义中应当包含 INSEC 的用法。

6 标准语法的用法示例（参考性）

6.1 ZOI示例

本节包含的示例显示了影响区语法是如何被使用的。

在下面的示例中，用于 Pzoi，Mzoi 和 Izoi 中的上标对应于与图像相关的项和与非图像相关的项的索引，这些索引在 DCzoi 的 BAS 结构中标示，并按照它们出现在 DCzoi 中的顺序。

6.1.1 示例1

本节显示了这样一个示例，即在左上角为（100，120）和右下角为（180，210）所确定的图像区域中分辨率级别大于 3 的部分是受影响的。在本例中，需要 9 个字节。

表 57－示例1的ZOI

参　数			长度（比特）	取值（按顺序）	导 出 含 义
NZzoi			8 (RBAS)	1	区域数量为 1
$Zone^0$	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	101000_b	按顺序指定图像区域和分辨率
	$Pzoi^1$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 比特的整数
			1	1_b	Izoi 使用两个维度来描述
		$Izoi^1$	8	$0110\ 0100_b$	Xul 为 100
			8	$0111\ 1000_b$	Yul 为 120
			8	$1011\ 0100_b$	Xlr 为 180
			8	$1101\ 0010_b$	Ylr 为 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	后面没有跟随字节对齐段
			1	1_b	指定区域的补集受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	11_b	最大模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^3$	8	$0000\ 0010_b$	指定了分辨率级别≤2。（即根据最大模式和补集切换，指定的是分辨率级别 > 3）。

6.1.2 示例2

本节显示了这样一个示例，即在子带 1 中左上角索引为 5，右下角索引为 10 的范围内，分辨率级别为 0 的码块是受影响的。在本例中，需要 10 个字节。

表 58－示例2的ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域数量为 1
Zone[0]	DCzoi[1]		1	1_b	后面跟随了字节对齐段
			1	0_b	与图像相关的描述类
			6	001000_b	指定了分辨率级别
	DCzoi[2]		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	001100_b	指定了子段和码块
	Pzoi[3]	Mzoi[3]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[3]	8	$0000\ 0000_b$	分辨率级别索引为 0
	Pzoi[9]	Mzoi[8]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[8]	8	$0000\ 0001_b$	子带 1 被指定
	Pzoi[10]	Mzoi[9]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[9]	8	$0000\ 0101_b$	左上角的码块索引为 5
			8	$0000\ 1010_b$	右下角的码块索引为 10

6.1.3 示例3

本节显示了这样一个示例，即从字节 10 到 100，以及从字节 10000 到 12000 的数据段是受影响的。在本例中，需要 12 个字节。

表 59－示例3的ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域的数量为 1
$Zone^0$	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010000_b	SOD 标记之后的字节范围被指定
	$Pzoi^2$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	1_b	指定了多个项
			2	01_b	范围模式
			2	01_b	Izoi 使用 16 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Nzoi^2$	8	$0000\ 0010_b$	数据段的数量为 2
		$Izoi^{21}$	16	$0000\ 0000_b$ $0000\ 1010_b$	起始字节位置为第 10 个字节
			16	$0000\ 0000_b$ $0110\ 0100_b$	终止字节位置为第 100 个字节
		$Izoi^{21}$	16	$0010\ 0111_b$ $0001\ 0000_b$	起始字节位置为第 10000 个字节
			16	$0010\ 1110_b$ $1110\ 0000_b$	终止字节位置为第 12000 个字节

6.1.4 示例4

本节显示了这样一个示例，即分辨率级别为 0，且 10 到 100 的字节段对应于分辨率级别为 0 的数据。在本例中，需要 10 个字节。

表 60－示例4的ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域数量为 1
$Zone^0$	$DCzoi^1$		1	1_b	后面跟随了字节对齐段
			1	0_b	与图像相关的描述类
			6	001000_b	按顺序指定分辨率级别
	$DCzoi^2$		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010000_b	指定了字节范围
	$Pzoi^1$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^1$	8	$0000\ 0000_b$	分辨率级别为 0

表 60－示例4的ZOI

参　数			长度（比特）	取值（按顺序）	导 出 含 义
$Zone^0$	$Pzoi^2$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	01_b	范围模式
			2	01_b	Izoi 使用 16 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^1$	16	0000 0000 0000 1010_b	起始字节位置为第 10 个字节
			16	0000 0000 0110 0100_b	终止字节位置为第 100 个字节

6.1.5　示例5

本节显示了这样一个示例，即在左上角拼贴索引为 0，右下角拼贴索引为 5 的拼贴中，分辨率级别大于 3，且在左上角拼贴索引为 10，右下角拼贴索引为 15 的拼贴中，层等于或小于 5 的部分是受影响的。在本例中，需要 13 个字节。

表 61－示例5的ZOI

参　数			长度（比特）	取值（按顺序）	导 出 含 义
NZzoi			8 (RBAS)	2	区域的数量为 2
$Zone^0$	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	01 1000_b	按顺序指定了拼贴和分辨率级别
	$Pzoi^2$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^2$	8	0000 0000_b	左上角拼贴索引为 0
			8	0000 0101_b	右下角拼贴索引为 5
	$Pzoi^3$	$Mzoi^3$	1	0_b	后面没有跟随字节对齐段
			1	1_b	指定区域的补集受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	11_b	最大模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^3$	8	0000 0010_b	指定分辨率级别≤2。（即根据最大模式和补集切换，指定的是分辨率 > 3）。

表 61－示例5的ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
Zone[1]	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	010100_b	按顺序指定了拼贴和层
	Pzoi[2]	Mzoi[2]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[2]	8	$0000\ 1010_b$	左上角拼贴索引为 10
			8	$0000\ 1111_b$	右下角拼贴索引为 15
	Pzoi[4]	Mzoi[4]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	11_b	最大模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[4]	8	$0000\ 0101_b$	采用最大模式指定了层 ≤ 5

6.1.6　示例6

本节显示了这样一个示例，即从字节 10 到 100 的头部段是受影响的。在本例中，需要 8 个字节。

表 62－示例6的ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域的数量为 1
Zone[0]	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	001000_b	SEC 标记之后的字节范围被指定
	Pzoi[3]	Mzoi[3]	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	01_b	范围模式
			2	01_b	Izoi 使用 16 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		Izoi[3]	16	$0000\ 0000$ $0000\ 1010_b$	起始字节位置为第 10 个字节
			16	$0000\ 0000$ $0110\ 0100_b$	终止字节位置为第 100 个字节

6.2 密钥信息模板示例

6.2.1 示例1

表 63 显示了这样一个示例，即使用一个单独的私钥（128 个比特）来解密一个码流，此私钥使用 URI 来标识，且在解密阶段基于 URI 从密钥服务器中获取到。

表 63－示例1的密钥信息

参　数		长度（比特）	取　值	导出含义
LK_{KT}		16	128	密钥长度为 128 个比特
KID_{KT}		8	2	指定了私钥的 URI
G_{KT}	PO	16	000 001 010 011 100 0_b	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	0000 1001_b	保护单元为 ZOI 中指定的全部区域
V_{KT}	N_V	16 (RBAS)	1	值列表 V 中的值的数量为 1
	S_V	8 (RBAS)	19	密钥信息的长度为 19 个字节
	V1	152	https://server/file	私钥可从 https://server/file 中获取

6.2.2 示例2

表 64 显示了这样一个示例，即采用一个 X.509 证书来认证一个码流，其中 X.509 证书嵌在 KI_{KT} 中，且编码方法为 DER。

表 64－示例2的密钥信息

参　数			长度（比特）	取　值	导出含义
LK_{KT}			16	1024	密钥的长度为 1024 个比特
KID_{KT}			8	2	指定了 X.509 证书
G_{KT}	PO		16	000 001 010 011 100 0_b	处理顺序为拼贴-分辨率-层-分量-选区
	GL		8	0000 1001_b	保护单元为 ZOI 中指定的全部区域
V_{KT}	N_V		16 (RBAS)	1	值列表 V 中的值的数量为 1
	S_V		8 (RBAS)	可变的	X.509 证书的长度
	V1	ER_{KT}	8	1	X.509 证书根据编码方法 DER 来编码
		$LCER_{KT}$	16	可变的	CER_{KT} 的长度
		CER_{KT}	可变的	证书值	带有 1024 个比特公钥的证书被嵌入

6.2.3 示例3

表 65 显示了这样一个示例，即采用一个单独的公钥来认证一个码流，其中公钥嵌在 KI_{KT} 中。

表 65－示例3的密钥信息

参　数		长度（比特）	取　值	导出含义
LK_{KT}		16	1024	密钥的长度为 1024 个比特
KID_{KT}		8	1	指定了密钥
G_{KT}	PO	16	000 001 010 011 100 0_b	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	0000 1001_b	保护单元为 ZOI 中指定的全部区域
V_{KT}	N_V	16 (RBAS)	1	值列表 V 中的值的数量为 1
	S_V	8 (RBAS)	256	公钥的长度为 256 个字节
	V1	2048	公钥值	公钥被嵌入

6.2.4 示例4

表 66 显示了这样一个示例，即采用多个私钥来解码一个码流，其中不同的私钥用于不同的层。

表 66－示例4的密钥信息

参　数		长度（比特）	取　值	导出含义
LK_{KT}		16	128	密钥的长度为 128 个比特
KID_{KT}		8	3	指定了私钥的 URI
G_{KT}	PO	16	$000\ 001\ 010\ 011\ 1000_b$	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	$0000\ 0100_b$	保护单元为层
V_{KT}	N_V	16 (RBAS)	3	值列表 V 中的值的数量为 3
	S_V	8 (RBAS)	16	每个 Vn 的长度为 16 个字节
	V1	128	https://server/1	第一层的私钥从 https://server/1 处获得
	V2	128	https://server/2	第二层的私钥从 https://server/2 处获得
	V3	128	https://server/3	第三层的私钥从 https://server/3 处获得
	V4	128	https://server/4	第四层的私钥从 https://server/4 处获得

6.3 JPSEC标准工具示例

下面的示例描述了如何使用 ZOI 和密钥模板来执行基本的安全服务，如对某个 JPEG 2000 编码的图像执行加密和认证。

6.3.1 示例1

某个图像按照 JPEG 2000 编码，且具有三个分辨率。在本例中，为了提供预览能力，没有对第一个分辨率进行加密，第二个和第三个分辨率分别使用密钥 k1 和 k2 进行了加密。在这种情况下，输入图像按照 RLCP 进展顺序进行编码，并且具有一个拼贴，3 个分辨率，3 个层，Nc 个分量，以及 Np 个选区（分量和选区的数量在本特例中并不重要）。采用 AES，以 CBC 模式执行加密，且没有填充（采用密文挪用），使用密钥 0 来对分辨率 1 进行加密，使用密钥 k2 来对分辨率 2 进行加密，而分辨率 0 没有被加密。

JPSEC 标示了一个 JPSEC 消费者应当如何解密 JPSEC 码流。首先，标示了解密模板的工具模板 ID。然后指定了两个 ZOI，一个是为分辨率 1 及其相应的字节范围 B0-B1，另一个是为分辨率 2 及其相应的字节范围 B2-B3。解密模板参数指示应用了 AES 加密，且没有被填充（采用密文挪用）。密钥信息以及不同的密钥被应用到不同的分辨率上的事实通过密钥信息参数来标示。特别地，密钥粒度随着分辨率一起指定，这样每个分辨率就都具有一个不同的密钥，而处理顺序被标示为 TRLCP。对于每个分辨率的密钥信息都包含在密钥的值列表中。在码流上执行加密，就同时对包头和包体进行了加密。加密粒度为分辨率，处理时按照 TRLCP 顺序来执行，与原始的码流顺序是相同的。由于两个分辨率被分别加密，因此需要两个初始向量（IV），这些都包含在值列表中。

需要注意的是包的密文结果是由处理顺序指定的，因此独立于输入码流的进展顺序；然而，加密后的包置于输出码流中的位置遵循的是输入码流包的顺序。

表 67－示例1的SEC标记段

参　数			长度（比特）	取　值	含　义
SEC			16	0xFF65	SEC 标记
L_{SEC}			16 (RBAS)	0x82	SEC 标记段的长度为 130 个字节
Z_{SEC}			8 (RBAS)	0	此 SEC 标记段的索引
P_{SEC}	F_{PSEC}		1	0_b	后面没有跟随 FBAS 结构
		F_{INSEC}	1	0_b	没有使用 INSEC
		$F_{multiSEC}$	1	0_b	使用了一个 SEC 标记段
		F_{mod}	2	00_b	原始的 JPEG 2000 数据被修改
		F_{TRLCP}	1	0_b	TRLCP 标签的用法没有在 P_{SEC} 中定义
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	安全工具的数量为 1
	I_{max}		8 (RBAS)	0000000_b	最大的工具示例索引为 0
t			8 (FBAS)	0	JPSEC 标准工具
i			8 (RBAS)	0	工具实例索引
ID_T			8	1	解密模板
L_{zoi}			16 (RBAS)	0x17	ZOI 的长度为 23 个字节
ZOI			184	见表 68	本工具的影响区
L_{PID}			16 (RBAS)	0x5e	P_{ID} 的长度为 94 个字节
P_{ID}			752	见表 69	本技术的参数

表 68－ZOI示例

参　数			长度（比特）	取值（按顺序）	导 出 含 义
NZzoi			8 (RBAS)	2	区域的数量为 1
$Zone^0$	DC_{ZOI}^1		1	1_b	后面跟随了字节对齐段
			1	0_b	与图像相关的描述类
			6	001000_b	指定了分辨率
	$DCzoi^2$		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010000_b	SOD 标记之后的字节范围被指定
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		I_{ZOI}	8	$0000\ 0001_b$	指定了分辨率 1
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	01_b	范围模式
			2	01_b	Izoi 使用 16 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^{21}$	16	0x31CC	起始字节位置在第 12748 个字节。（B0）
			16	0xA3E8	终止字节位置在第 41960 个字节。（B1）

表 68－ZOI示例

参　数			长度（比特）	取值（按顺序）	导出含义
$Zone^{1}$	DC_{ZOI}^{1}		1	1_b	后面跟随了字节对齐段
			1	0_b	与图像相关的描述类
			6	001000_b	指定了分辨率
	DCzoi[2]		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010000_b	SOD 标记之后的字节范围被指定
	$Pzoi^{0,1}$	$Mzoi^{1}$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		I_{ZOI}^{1}	8	$0000\ 0010_b$	指定了分辨率 2
	$Pzoi^{0,2}$	$Mzoi^{2}$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_{b2}	指定了单个项
			2	01_b	范围模式
			2	10_b	Izoi 使用 32 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^{2}$	32	0xA3EE	起始字节位置在第 41966 个字节。（B2）
			32	0x21101	终止字节位置在第 135425 个字节。（B3）

表 69－P_{ID} 示例

参　数		长度（比特）	取　值	含　义
T_{ID}		432	见表 70	解密模板
PD		8 (FBAS)	0_b	后面没有跟随字节对齐段
			0_b	没有使用像素域
			0_b	没有使用小波系数域
			0_b	没有使用量化的小波系数域
			1_b	使用了码流域
			000_b	保留供 ISO 使用
F_{PD}		8 (FBAS)	0_b	后面没有跟随 FBAS 字节
			1_b	仅有包体被加密
			000000_b	保留供 ISO 使用
G	PO	16	$000\ 001\ 010\ 011\ 100\ 0_b$	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	$0000\ 0011_b$	保护单元为分辨率级别
V	N_V	16 (RBAS)	2	值列表中值的数量为 2
	S_V	8 (RBAS)	16	每个 Vn 的长度为 16 个字节
	V1	128	IV0	R1 的初始向量值
	V2	128	IV1	R2 的初始向量值

表 70－解密模板示例

参　数		长　度	取值 （按顺序）	导 出 含 义
ME_{decry}		8	0	出现了标记竞争
CT_{decry}		16	0001_b	块密码（AES）
CP_{decry}	M_{bc}	6	100000_b	CBC 模式。比特没有被填充
	P_{bc}	2	00_b	密文挪用
	SIZ_{bc}	8	16	块长度（16 个字节，128 个比特）
	KT_{bc}	392	见表 71	密钥模板

表 71－密钥模板示例

参　数		长度（比特）	取　值	导 出 含 义
LK_{KT}		16	128	密钥长度为 128 个比特
KID_{KT}		8	2	私钥的 URI
G_{KT}	PO	16	0 000 001 010 011 100_b	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	0000 0011_b	保护单元为分辨率级别
V_{KT}	N_V	32 (RBAS)	2	值列表中值的数量为 2
	S_V	8 (RBAS)	19	每个 Vn 的长度为 19 个字节
	V1	152	https://server/key1	分辨率 1 的私钥可从 https://server/key1 中获得
	V2	152	https://server/key2	分辨率 2 的私钥可从 https://server/key2 中获得

6.3.2　示例2

在这种情况下，认证应用于如上所述的同一个 JPEG 2000 编码的图像上。在本例中，所有的三个分辨率以及每个分辨率的三个层都被认证，且对每个分辨率的认证都使用不同的密钥。由于有三个分辨率，因此有三个密钥，同时由于每个分辨率有三层，因此每个分辨率将有三个 MAC 值。这样，针对整个 JPSEC 图像总共将会有 9 个 MAC 值。特别地：

- 分辨率0拥有的MAC值为M0，M1，M2（每层一个），并使用密钥0
- 分辨率1拥有的MAC值为M3，M4，M5（每层一个），并使用密钥1
- 分辨率2拥有的MAC值为M6，M7，M8（每层一个），并使用密钥2

本例显示了如何标示认证，以及如何通过 ZOI 和粒度工具来提供灵活性。正如前面的示例，输入图像按照 RLCP 进展顺序进行编码，且具备 1 个拼贴，3 个分辨率，3 个层，Nc 个分量和 Np 个选区（在本特例中，分量和选区的数量并不重要）。认证使用 HMAC 来执行，并使用 SHA-1 算法。

JPSEC 标示了一个 JPSEC 消费者如何验证或认证 JPSEC 的被保护内容。首先，标示了认证模板的工具模板 ID。然后，使用 ZOI 来标示有三个分辨率，并标示每个分辨率的相关字节范围。认证模板参数标示了 HMAC 被应用，并使用 SHA-1 算法。密钥信息模板提供了关于密钥的信息，包括密钥粒度为分辨率，并且为密钥的值列表中的三个密钥都提供了信息。认证的处理域被指定为是码流，且包括包头。认证的工具粒度被指定为层，因此每个分辨率有三个 MAC，总共有 9 个 MAC 值。值列表中包含 9 个 MAC 值。上述处理顺序被标识为 TRLCP，同原始码流顺序相同。

需要注意的是在粒度字段中使用处理顺序可以确保产生相同的 MAC 值，而独立于码流的进展顺序。

需要注意的是在本例示范 MAC 用法的同时，也可以使用相同的方法来标示多个数字签名的用法。

表 72－SEC标记段

参　数			长度（比特）	取值（按顺序）	导出含义
SEC			16	0xFF65	SEC 标记
L_{SEC}			16	0x0099	SEC 标记段的长度
Z_{SEC}			8 (RBAS)	0	本 SEC 标记段的索引
P_{SEC}	F_{PSEC}		1	0_b	后面没有跟随 FBAS 结构
		F_{INSEC}	1	0_b	没有使用 INSEC 标记段
		$F_{multiSEC}$	1	0_b	在本码流中仅有一个 SEC 标记段
		F_{mod}	1	0_b	原始 JPEG 2000 数据未被修改
		F_{TRLCP}	1	0_b	没有使用 TRLCP 标签
		Padding	3	000_b	没有使用 TRLCP 标签
	N_{tools}		7	1	在本码流中仅使用了一个工具
	I_{max}		7	0	最大的工具实例索引为 0
$Tool^0$	t		8 (FBAS)	0	JPSEC 标准工具
	i		8 (RBAS)	0	工具实例索引
	ID_T		8	2	本标准工具使用一个认证模板
	L_{ZOI}		16 (RBAS)	0x20	ZOI 的长度为 32 个字节
	ZOI		256	表 73	图像的覆盖区域
	L_{PID}		16 (RBAS)	0x6c	P_{ID} 的长度为 108 个字节
	P_{ID}		928	表 74	JPSEC 工具的参数

表 73－ZOI的信号化

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域的数量为 1
$Zone^0$	DC_{zoi}^1		1	1_b	后面跟随了字节对齐段
			1	0_b	与图像相关的描述类
			6	001000_b	按顺序指定了分辨率级别
	DC_{zoi}^2		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010000_b	指定了字节范围
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	01_b	范围模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^1$	8	0	范围的起始为 0
			8	2	范围的终止为 2

表 73－ZOI的信号化

参　数			长度（比特）	取值（按顺序）	导出含义
$Zone^0$	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	1_b	指定了多个项
			2	01_b	范围模式
			2	10_b	Izoi 使用 32 个比特的整数
			1	0_b	Izoi 使用一个维度来描述
		N_{ZOI}	8 (RBAS)	3	I_{ZOI} 的数量为 3
		$Izoi^1$	32	104	起始字节位置为第 104 个字节
			32	12762	终止字节位置为第 12762 个字节
		I_{ZOI}^2	32	12768	起始字节位置为第 12768 个字节
			32	41980	终止字节位置为第 41980 个字节
		I_{ZOI}^3	32	41986	起始字节位置为第 41986 个字节
			32	135445	终止字节位置为第 135445 个字节

表 74－P_{ID} 信号化参数

参　数					长度（比特）	取值（按顺序）	导出含义
T_{auth}	M_{auth}				8	0	认证方法：基于哈希的认证
	P_{auth}	M_{HMAC}			8	1	使用 HMAC 进行认证
		H_{HMAC}			8	1	使用 SHA-1 进行散列
		KT_{HMAC}	LK_{KT}		16	128	密钥的长度（比特）
			KID_{KT}		8	3	KI_{KT} 包含了私钥的 URI
			G_{KT}	PO	16	0 000 001 010 011 100_b	顺序为拼贴-分辨率-层-分量-选区
				GL	8	00000011_b	密钥粒度为分辨率
			V_{KT}	N_V	16 (RBAS)	3	列表中有三个密钥
				S_V	8 (RBAS)	8	每个密钥的长度为 8 个字节
				VL	64	*Key*0	第一个密钥为 *key*0，对应分辨率 0
					64	*Key*1	第二个密钥为 *key*1，对应分辨率 1
					64	*Key*2	第三个密钥为 *key*2，对应分辨率 2
		SIZ_{HMAC}			16	20	MAC 的长度为 20
PD					8 (FBAS)	0_b	后面没有跟随字节对齐段
						0_b	没有使用像素域
						0_b	没有使用小波系数域
						0_b	没有使用量化的小波系数域
						1_b	使用了码流域
						000_b	保留供 ISO 使用
F_{PD}					8 (FBAS)	0_b	后面没有跟随 FBAS 字节
						0_b	包头和包体都被加密
						000000_b	保留供 ISO 使用

表 74－P_{ID} 信号化参数

参　数		长度（比特）	取值（按顺序）	导出含义
G	PO	16	0000010100111000_b	顺序为拼贴-分辨率-层-分量-选区
	GL	8	00000100_b	工具粒度为层
V	N_V	32 (RBAS)	9	共有 9 个 MAC（每个分辨率有 3 个 MAC）
	S_V	8 (RBAS)	20	每个 MAC 的长度为 20 个字节
	VL	160	*M*0	第一个 MAC 为 *M*0
		160	*M*1	第二个 MAC 为 *M*1
		160	*M*2	第三个 MAC 为 *M*2
		160	*M*3	第四个 MAC 为 *M*3
		160	*M*4	第五个 MAC 为 *M*4
		160	*M*5	第六个 MAC 为 *M*5
		160	*M*6	第七个 MAC 为 *M*6
		160	*M*7	第八个 MAC 为 *M*7
		160	*M*8	第九个 MAC 为 *M*8

6.4　失真字段示例

本节提供了几个关于失真字段用法的简单示例。

6.4.1　示例1

本示例基于第 6.1.3 节中的 ZOI 示例而构造，用来显示失真值是如何与那个示例中的 ZOI 所标示的两个数据段相关联的。正如前面所讨论的，第 6.1.3 节中的示例 3 标示了两个数据段：（1）字节 10 到 100 和（2）字节 10000 到 12000。为了将失真字段与这两个数据段相关联起来，需要两个步骤。首先，在 DCzoi 中标示失真字段。第二，使用 $Pzoi^2$ 来标示失真值。因此，对第 6.1.3 节中的 ZOI 示例 3 的修改就仅仅是在 DCzoi 中设置失真字段比特，并且加入 $Pzoi^2$ （表 75 中的最后 9 行）。

表 75－将失真字段与两个数据段关联起来（第6.1.3节中的ZOI示例3 的扩展）

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域的数量为 1
$Zone^0$	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	010001_b	指定了 SOD 标记之后的字节范围，且指定了相关联的失真字段
	$Pzoi^2$	$Mzoi^2$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	1_b	指定了多个项
			2	01_b	范围模式
			2	01_b	Izoi 使用 16 个比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Nzoi^2$	8 (RBAS)	2	数据段的数量为 2
		$Izoi^{2,1}$	16	$0000\ 0000\ 0000\ 1010_b$	起始字节位置为第 10 个字节
			16	$0000\ 0000\ 0110\ 0100_b$	终止字节位置为第 100 个字节

表 75－将失真字段与两个数据段关联起来（第6.1.3节中的ZOI示例3 的扩展）

参　数			长度（比特）	取值（按顺序）	导出含义
$Zone^0$	$Pzoi^2$	$Izoi^{2,2}$	16	0010 0111 0001 0000_b	起始字节位置为第 10000 个字节
			16	0010 1110 1110 0000_b	终止字节位置为第 12000 个字节
	$Pzoi^6$	$Mzoi^6$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	1_b	指定了多个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 个比特来表示每个失真值
			1	0_b	Izoi 使用一个维度来描述
		$Nzoi^6$	8 (RBAS)	2	数据段的数量为 2
		$Izoi^{6,1}$	8	D1 值	第一段的失真值
		$Izoi^{6,2}$	8	D2 值	第二段的失真值

6.4.2　示例2

本示例描述了失真值如何与 JPEG 2000 包相关联。DCzoi 指定了 4 个包的范围，同时也标示了失真字段。$Pzoi^1$ 给出了包的范围，而 $Pzoi^2$ 描述了与每个包相关联的失真。注意 $Pzoi^1$ 指定的是长度为 4 的一个范围，而 $Pzoi^2$ 指定的是 4 个值，范围中的每个项都与一个值相关联，例如每个包都与一个失真相关联。

表 76－信号化一个包范围并将失真与每个包相关联起来

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8 (RBAS)	1	区域的数量为 1
$Zone^0$	DCzoi		1	0_b	后面没有跟随字节对齐段
			1	1_b	与非图像相关的描述类
			6	100001_b	指定了包，并且指定了相关联的失真字段
	$Pzoi^1$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	0_b	指定了单个项
			2	01_b	范围模式
			2	00_b	Izoi 使用 8 比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Nzoi^1$	8 (RBAS)	1	数据段的数量为 1
		$Izoi^{11}$	8	0000 0000_b	起始包为第 0 号
			8	0000 0011_b	终止包为第 3 号
	$Pzoi^6$	$Mzoi^6$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域受 JPSEC 工具的影响
			1	1_b	指定了多个项
			2	10_b	索引模式
			2	00_b	Izoi 使用 8 个比特来表示每个失真值
			1	0_b	Izoi 使用一个维度来描述
		$Nzoi^6$	8 (RBAS)	4	数据段的数量为 4
		$Izoi^{6,1}$	8	D1 值	第一个包的失真值
		$Izoi^{6,2}$	8	D2 值	第二个包的失真值
		$Izoi^{6,3}$	8	D3 值	第三个包的失真值
		$Izoi^{6,4}$	8	D4 值	第四个包的失真值

7 JPSEC注册机构

7.1 概要介绍

JPSEC 注册机制为非标准的安全工具提供了一种无二义性的标识，并将其加入到附件 B 的列表中，这些非标准的安全工具遵循 JPSEC 标准，并且可以进一步被提议或开发为一个非标准的 JPSEC 工具。这种注册由一个 JPSEC 注册机构来执行。它应当符合 JTC 1 导则。这些新的 JPSEC 工具的注册通过本节所定义的过程来控制。

申请者可能会递交他们希望包含在 JPSEC 参考列表中的技术。注意 JPSEC 工具的用法是通过出现在码流中的 JPSEC 标记来指定的。当某个申请者发现一个未知的 JPSEC ID 时，它可以绑定到一个 JPSEC 注册机构，并且获得关于工具的注册信息。

7.2 注册申请者的合格条件

合格的申请者应当是被它们的国家机构所认可的组织。

7.3 注册申请表

注册一个新的 JPSEC 工具的申请表应当由 JPSEC 注册机构发布在网站上。

该网站应当包含这样一些窗体，如注册申请，请求更新，分配或更新的通知，以及申请拒绝等。

所有的窗体都应包含：

- 申请者组织的名称；
- 申请者组织的地址；
- 该组织内联系人的姓名、职位、信箱/电子邮件地址，电话号码/传真号码等。

注册申请和请求更新的窗体还应当包含如下条目：

- JPSEC工具名称（必选）。
- JPSEC工具类型，例如数字签名，水印，加密，扰码，密钥生成和管理，认证（可选）。
- 描述性的技术摘要（必选）。
- 描述性的工具概述（必选）。
- 操作示例用例描述（可选）。
- 参数语法规范，包含可能的取值（可选）。
- 最优用法的指南（可选）。
- IPR状态，如拥有者，权利持有人（可选）。
- IPR使用条件（必选）。
- 使用限制，如输出条件（可选）。
- 关于实现工具下载的信息（可选）。
- 附加的注解、动机、参考等（可选）。
- 对所选申请表条目的机密性要求（可选）。
- 工具注册的时间长度要求（可选）。

JPSEC 注册机构也应当提供辅导材料来帮助申请者准备申请表。

7.4 对申请表的检查和响应

本节定义了 JPSEC 注册机构对申请表进行检查和响应的过程，以确保公平性。

应当设立一个技术检查委员会来检查申请表。这个委员会由 ISO/IEC JTC 1/SC 29/WG 1 的成员和 JPSEC 注册机构的成员组成。在申请表提交的 9 个月之内，检查委员会应在 WG1 会议上检查申请表。

检查委员会根据第 7.5 节定义的拒绝标准，对申请表接受或拒绝。

如果被接受，则一个新的 JPSEC 工具将被分配一个标识符（ID），并可在指定的一段时间内使用。ID 的语法应当符合第 5.6.3 节。检查委员会批准在第 7.3 节中所列的 JPSEC 工具描述信息。然后，此 ID 便可用于在 JPSEC 码流中进行标示。

一旦申请表被检查并被接受，则 JPSEC 注册机构应通知申请者，对其注册请求给出肯定响应或否定响应。在给申请者的响应中，应当包括对技术检查结果的一个简短解释，并且应当在申请表提交后的九个月内返回给申请者。

如果登记者相信拒绝响应是有错的，或者有更进一步的信息需要澄清相关问题或利害关系时，可以对否定响应进行上诉。如果登记者要求在注册机构过程之外进行额外检查时，他可以在下一个适当的 WG1 工作组会议中提交此案例，由更广泛的 WG1 委员会来检查。然后，根据专家的要求，他可能会被要求提供更多的信息，这些专家在 WG1 权力机构的领导下，将给出一个最终的、明确的响应是接受还是拒绝。为了能让 WG1 对一个已经被拒绝的申请表进行检查，登记者必须通过其国内组织重新提交此建议，并指明为什么这次提交需要 WG1 来考虑。

7.5 对申请表的拒绝

拒绝一个申请表的标准如下所述：

- 申请者不符合条件。
- 没有付正当的费用（如果需要时）。
- 已经存在一个已批准的已注册项，包含了与本次提交相同的内容。
- 申请表中的信息不完整，或不可理解。
- 将其包含在注册处的理由不充足。候选JPSEC工具应当证明它提供了一种有用的安全服务，并给出相关的用例。
- 注册机构认为在提交的工具中不具备足够的创意，可以通过一个现存的已经批准的项目很容易地实现。
- 提交中包含错误，或者不符合标准的JPSEC规范或标准。
- 技术描述不充分。
- 机密性条件不适当。

7.6 标识符的分配和对象定义的记录

检查过程以及上述的语法确保了一个已分配的 ID 在注册处是唯一的，相同的 ID 并没有分配给另一个对象。

在分配完成后，ID 和相关联的信息应被存储在注册处，且 JPSEC 注册机构应当在九个月内向申请者通知此分配。

在 ID 分配的同时，JPSEC 工具的定义也应当被记录在注册处。

7.6.1 ID的重用

标识符可能由注册机构重用。例如，当标识符过期后，或者它们被自动放弃或被回收后，就可以重用了。

ID 拥有者可能通过一个更新请求自动地放弃他们的 ID。

7.6.2 回收

一个 JPSEC 注册机构可能会由于技术原因或由于工具误用而回收一个标识符。当这种情况发生时，应当通过一个更新通知向标识符拥有者发出通知。

7.7 维护

出于维护注册处的目的，JPSEC 注册机构应实现机制来维护注册处的完整性，包括对所保存记录的足够备份。

一个 ID 拥有者可能会通过一个更新请求来更新相关的 JPSEC 工具的信息。

JPSEC 注册机构应当提供机制来维护申请表中已批准的条目的机密性。

7.8 注册的公布

一般来说，当注册信息被公布后，信息技术用户团体的利益可以得到最好的服务。在一些情况下，可能对关于某个特定注册的某些数据或所有数据的机密性有所要求，这些要求或者是永久性的，或者是对注册过程中的某些部分有要求。

JPSEC 注册机构应当公布注册信息，并按照与 JPSEC 工具所要求的机密性相一致的方式。

在需要公布时，电子版和打印的纸质版本都是必需的。如果某个 JPSEC 注册机构要提供出版物，则它必须保留其出版物的准确的发行记录。

7.9 注册处信息要求

JPSEC 注册机构应当在其注册处电子化公布非标准的 JPSEC 工具的列表，以及与它们相关的信息，并按照与 JPSEC 工具所要求的机密性相一致的方式。

对于每个 JPSEC 工具，注册处都应当包含下列信息：

- 所分配的ID；
- 原始申请者的名字；
- 原始申请者的地址；
- 最初分配的日期；
- 最后一次修改分配的日期，如果允许的话（可修改）；
- 目前所有者的名字（可修改）；
- 目前所有者的地址（可修改）；
- 组织内联系人的姓名、职位，邮政编码/电子邮件地址，电话号码/传真号码（可修改）；
- 最后一次修改的日期（可修改）。

它还应当包含申请者所提供的关于 JPSEC 工具的信息，如第 7.3 节所指定的信息，以及批准的信息等。

附 件 A

指南和用例

（本附件是本建议书 | 国际标准的组成部分）

A.1 一个JPSEC应用类

A.1.1 引言

本节对可能如何实现一个 JPSEC 应用类给出一个概念描述。这个应用类举例说明了一个安全的 JPEG 2000 图像分发的场景。下面的小节概括描述了一个概念上的 JPSEC 应用，包括互相通信的 JPSEC 实体和信息等。这种描述是概念上的，并不是试图定义一个具体的实现，也不是为某个实现规定需求；特定的应用可能包含，也可能不包含下面描述中所标识的那些实体。

A.1.2 一个安全的JPEG 2000图像分发的概况

图 A.1 显示了安全的 JPEG 2000 图像分发的一个 JPSEC 应用类的概况。在这些应用中，JPSEC 应用可能会被要求为 JPEG 2000 提供不同的安全服务，例如图像交换的机密性，图像源和内容的认证等。

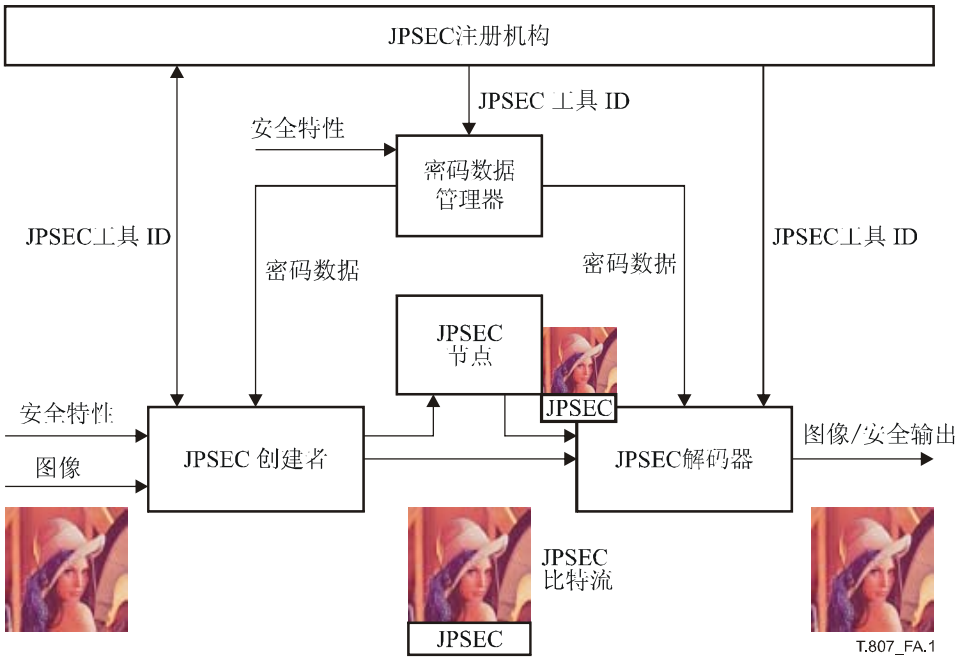


图 A.1－一个安全的JPEG 2000图像分发应用的概况

在安全的 JPEG 2000 图像分发的应用中，可以标识出如下步骤：

步骤1：某个JPSEC创建者创建了一个JPSEC码流。

步骤2：该JPSEC码流通过某个或某些JPSEC节点被分发。

步骤3：该JPSEC码流被某个JPSEC消费者接收并恢复。

步骤 1：JPSEC 码流的创建

创建者负责创建安全的 JPEG 2000 码流。该码流可能从位图数据或 JPEG 2000 压缩数据中创建。一个 JPSEC 创建者应用各种不同的安全技术，如对某个给定的图像数据进行加密，签名生成，以及 ICV（完整性检查值）生成。

为保护图像数据，创建者定义了哪个安全参数特性与此图像相关联。一个“安全参数特性”包含如下属性：

— 影响区（每个保护方法的覆盖区域）；

— 处理域（每个保护方法所要处理的域）；

— 粒度（每个保护方法的单元）；

— JPSEC工具标识（所应用的密码算法和相关联的参数）。

步骤 2：JPSEC 码流分发

一个 JPSEC 码流可被传送到某个 JPSEC 消费者处，采取的方式或者直接通过网络传送，或者通过一个中介（如 CD-ROM）传送。它还可以通过一个 JPSEC 节点来传送，该节点可以对 JPSEC 码流应用不同类型的额外处理，如代码转换。

如果 JPSEG 安全工具方法在 JPSEC 码流的安全特性参数中提出要求（例如为了加密，或为了认证），则 JPSEC 创建者必须通过一个独立的（‘安全的’）通道，向 JPSEC 消费者分发相应的密码数据。此数据，如密码或数字签名，可以被手工管理或通过一个密码数据管理器自动管理。

步骤 3：JPSEC 码流的处理恢复

根据所应用的安全参数特性，JPSEC 码流由一个 JPSEC 消费者过程来处理：这意味着要应用适当的安全技术，如解密，认证和完整性检查。此外，对于每个 JPSEC 工具安全方法，JPSEC 创建者和 JPSEC 消费者可能使用不同类型的密码数据。

作为 JPSEC 消费者的输出，一个解密后的图像数据和/或安全输出，如一个验证结果，将被产生。

JPSEC 创建者，JPSEC 消费者和密码数据管理器可能会引用 JPSEC 注册机构，以便获取关于某个特定 JPSEC 工具 ID 的必要的处理指示。

下面的小节提供了符合某个 JPSEC 服务的概念上的 JPSEC 实体的更详细的信息。图 A.2 显示了将要使用的图例描述。

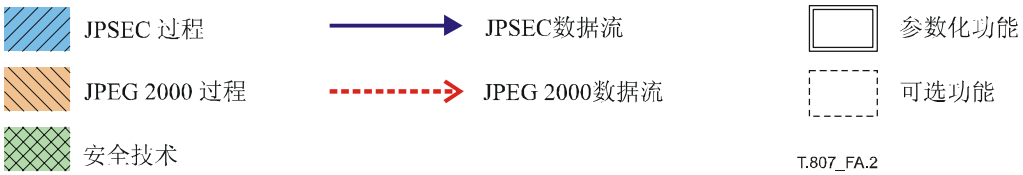


图 A.2－图例描述

— **JPSEC过程**：使用本建议书 | 国际标准中定义的工具的一个过程。

— **JPEG 2000过程**：在ITU-T T.800建议书 | ISO/IEC 15444-1（JPEG 2000第一部分）中定义的一个过程。

— **安全技术**：一种众所周知的安全技术，或者在本建议书 | 国际标准中定义，或者在其他标准或文档中定义。

— **JPSEC 数据流**：传送本建议书 | 国际标准中定义的信息的一个数据流。点划线表示是可选的。

— **JPEG 2000 数据流**：在ITU-T T.800建议书 | ISO/IEC 15444-1（JPEG 2000第一部分）中定义的一个数据流。

— **参数化功能**：一种功能，具有多个可替换的功能，可由应用程序选择。

— **可选功能**：一种功能，可以可选地应用在某个JPSEC应用中。

A.1.3 加密和解密过程

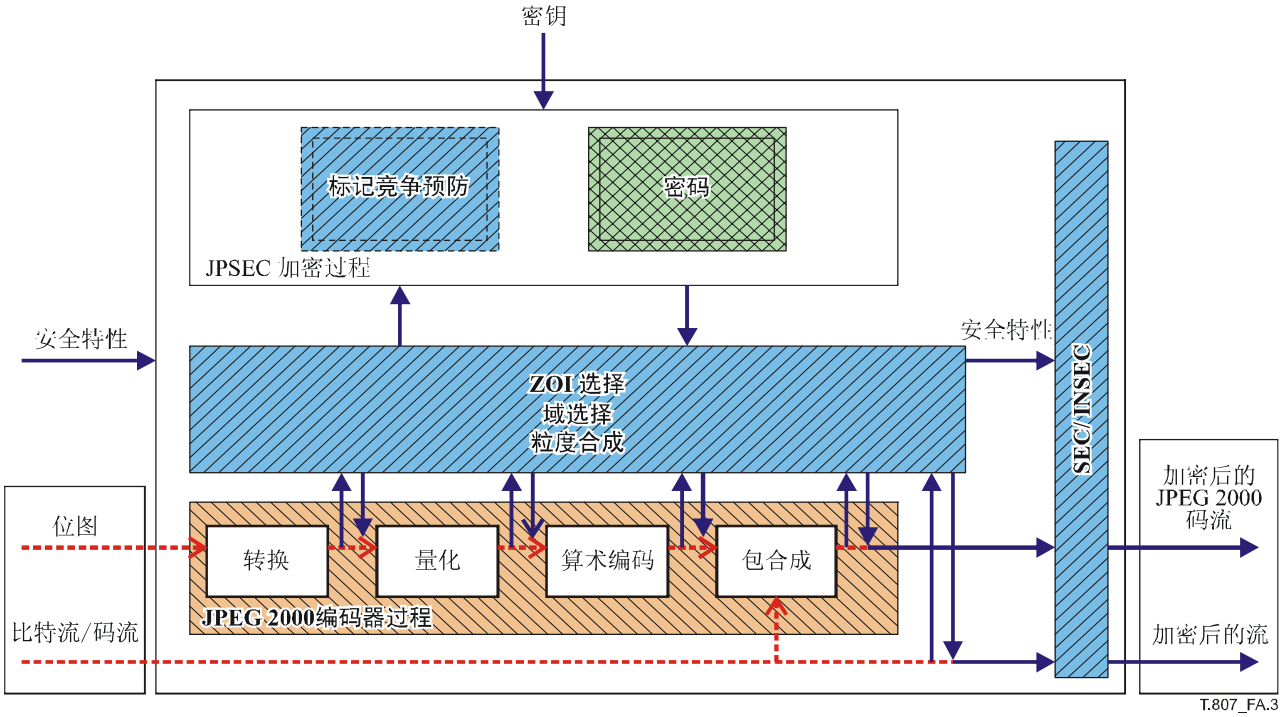


图 A.3－加密过程

图 A.3 显示了某个 JPSEC 创建者的加密过程示例的概况。本过程包含下述处理：

— 根据指定的处理域抽取数据；

— 根据指定的影响区选择被抽取数据中的一部分（即一个部分加密）；

— 使用指定的安全技术加密所选数据。此外，还可能基于粒度信息以单元方式加密数据。在这种情况下，不同的单元可以使用不同的密钥；

— 以密文数据代替明文数据；

— （可选地）应用一个标记竞争预防机制；

— 在SEC和/或INSEC标记段中构造安全参数特性。

需要注意的是一般来说，JPSEC 加密过程所产生的 JPSEC 码流与 JPEG 2000 的第一部分不是后向兼容的。在经过适当的解密后，图像数据将被传送到一个符合第一部分的解码器处。可能会应用一个标记竞争预防机制，来避免在加密后的码流中出现标记段竞争。

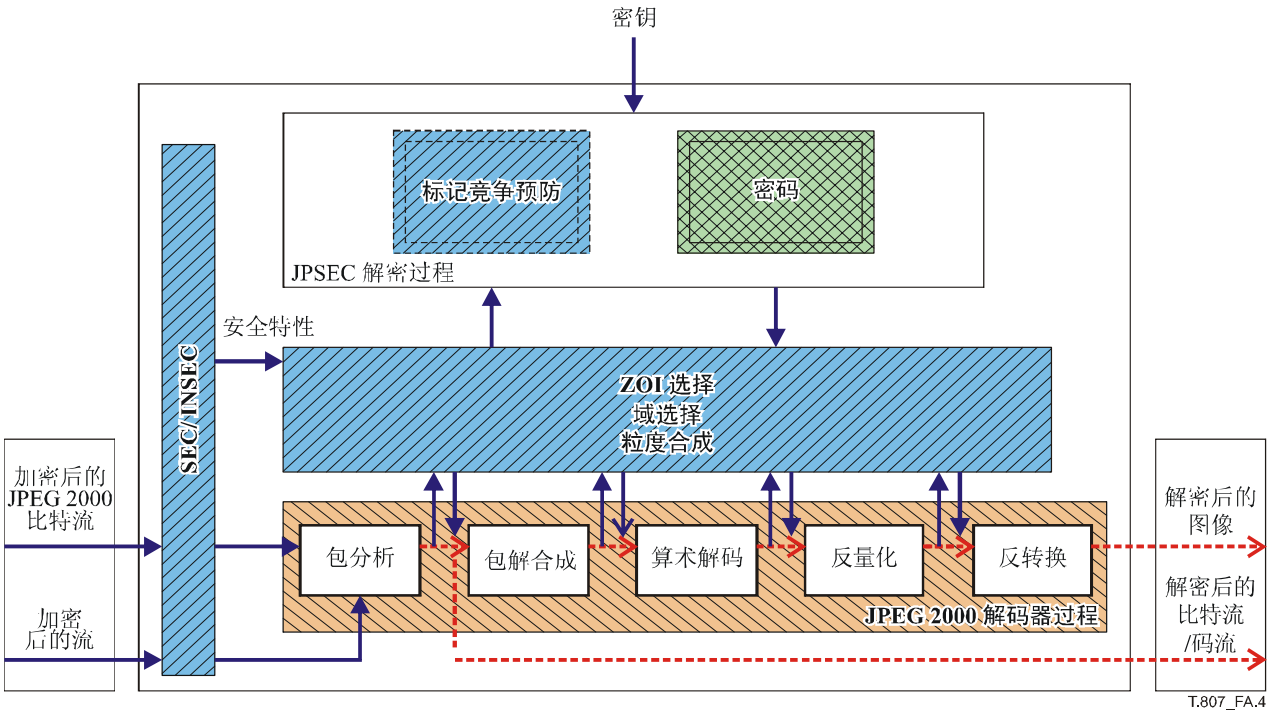


图 A.4－解密过程

图 A.4 显示了某个 JPSEC 消费者的解密过程示例的概况。本过程包含下述处理：

— 解析SEC和/或INSEC标记段中的安全参数特性；

— 根据所标示的处理域抽取数据；

— 根据所保留的密钥选择所抽取的数据中的一部分（即一个部分的解密）；

— 使用一个标示的安全技术对所选数据进行解密。此外，还可能基于粒度信息以单元方式解密数据；

— 以解密后的数据取代加密后的数据；

— 应用一个标记竞争预防机制，如果在加密过程中应用过的话。

A.1.4 签名产生和认证过程

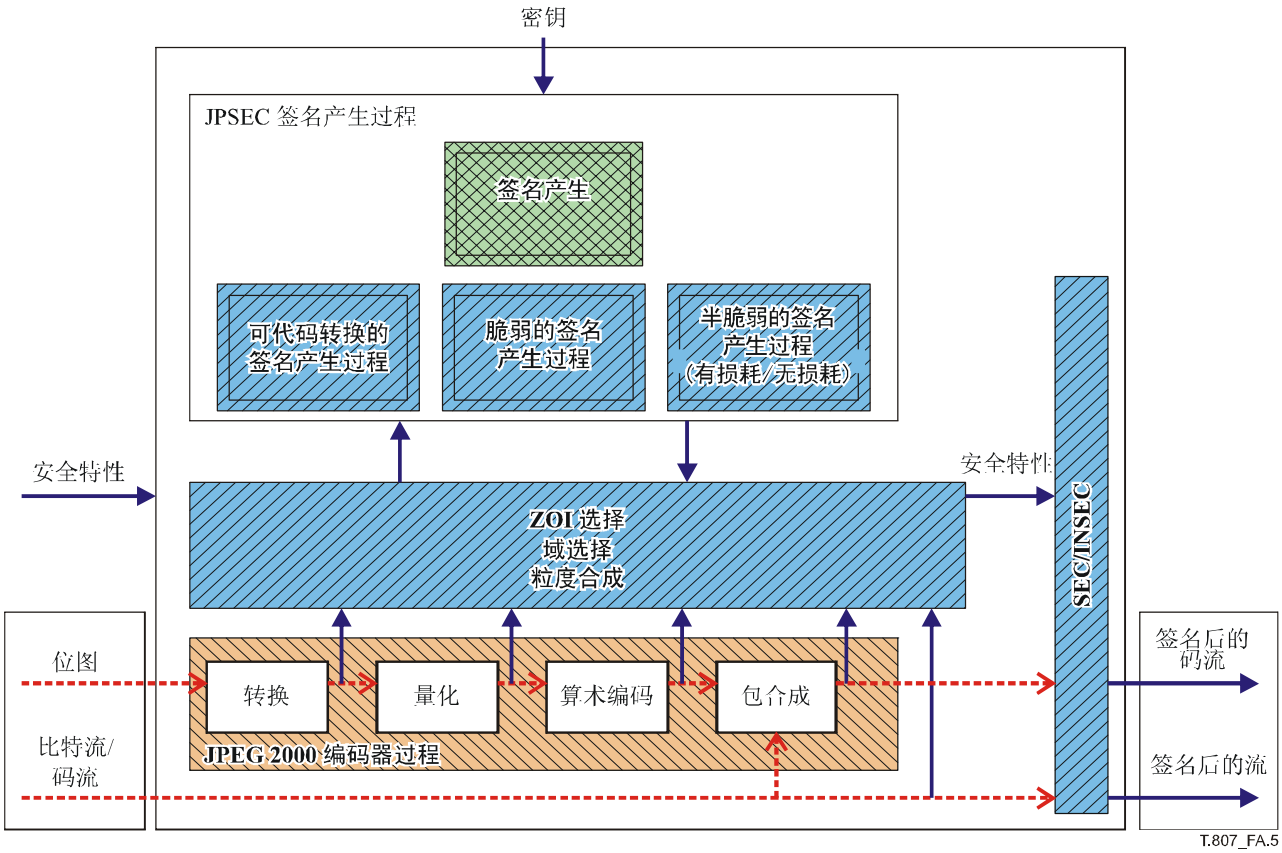


图 A.5－签名产生过程

图 A.5 显示了某个 JPSEC 创建者的签名产生过程示例的概况。本过程包含下述处理：

— 根据指定的处理域抽取数据；

— 根据指定的影响区选择被抽取数据中的一部分（即部分签名）；

— 使用指定的安全技术，计算适用于所选择数据的数字签名。此外，还可能基于粒度信息以单元方式产生数字签名；

— 将安全参数特性，包括计算后的数字签名，组合到SEC和/或INSEC标记段中。

需要注意的是在 JPSEC 中，定义了三种认证模式：“脆弱模式”，“半脆弱模式（有损耗的/无损耗的）”，以及“可代码转换的模式”。一个“脆弱模式”的认证可以检测到码流中任何一个单比特的修改，而一个“半脆弱模式”的认证可以检测到任何故意的改变，但可以将偶然的失真保持到一个预定义的范围内。此外，一个“代码转换模式”的认证可以验证码流的源部分。

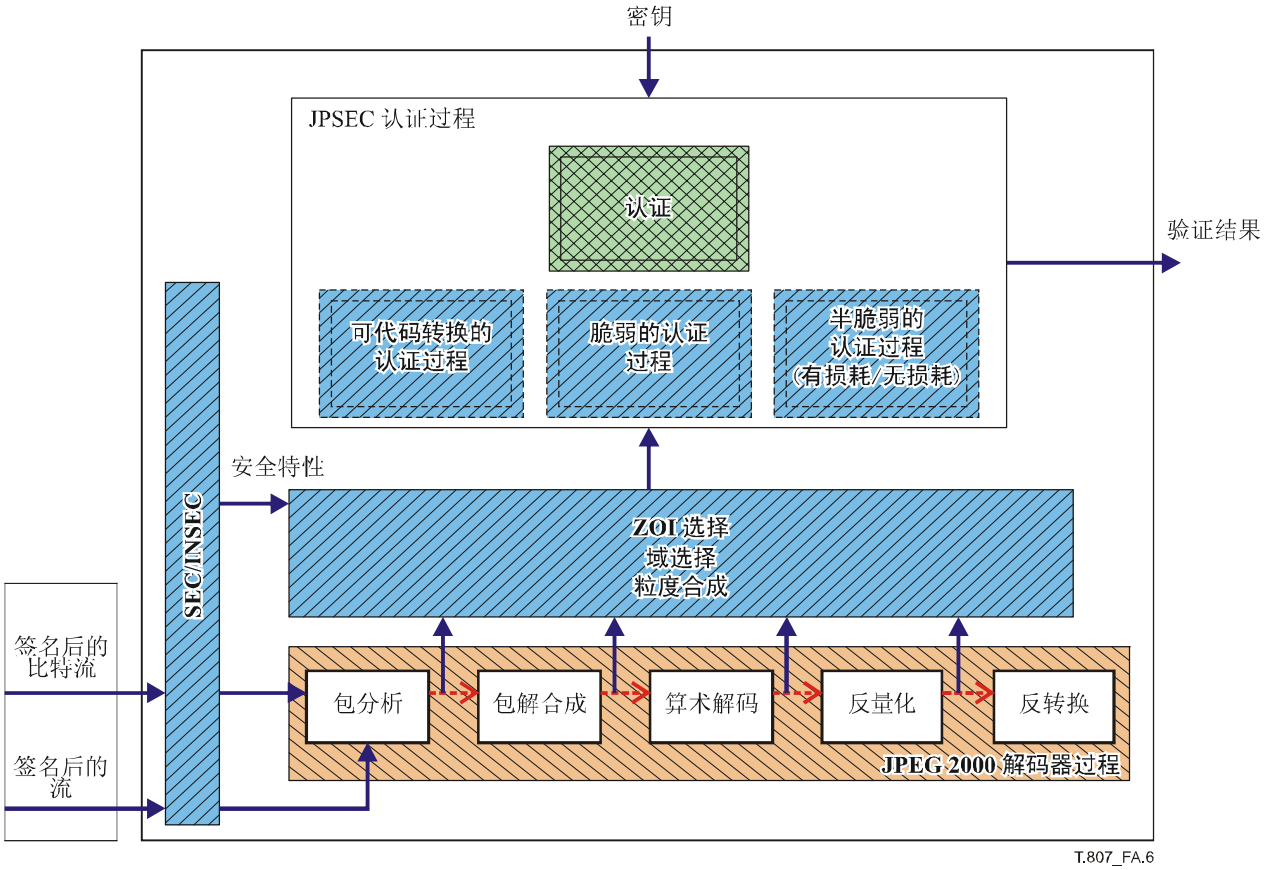


图 A.6－认证过程

图 A.6 显示了某个 JPSEC 消费者的认证过程示例的概况。本过程包含下述处理：

— 在一个标示的处理域内抽取数据；

— 根据标示的影响区选择被抽取数据中的一部分；

— 使用标示的安全技术验证所选数据。此外，还可能基于粒度信息以单元方式验证所选数据。

A.1.5 ICV（完整性检查值）产生和完整性检查过程

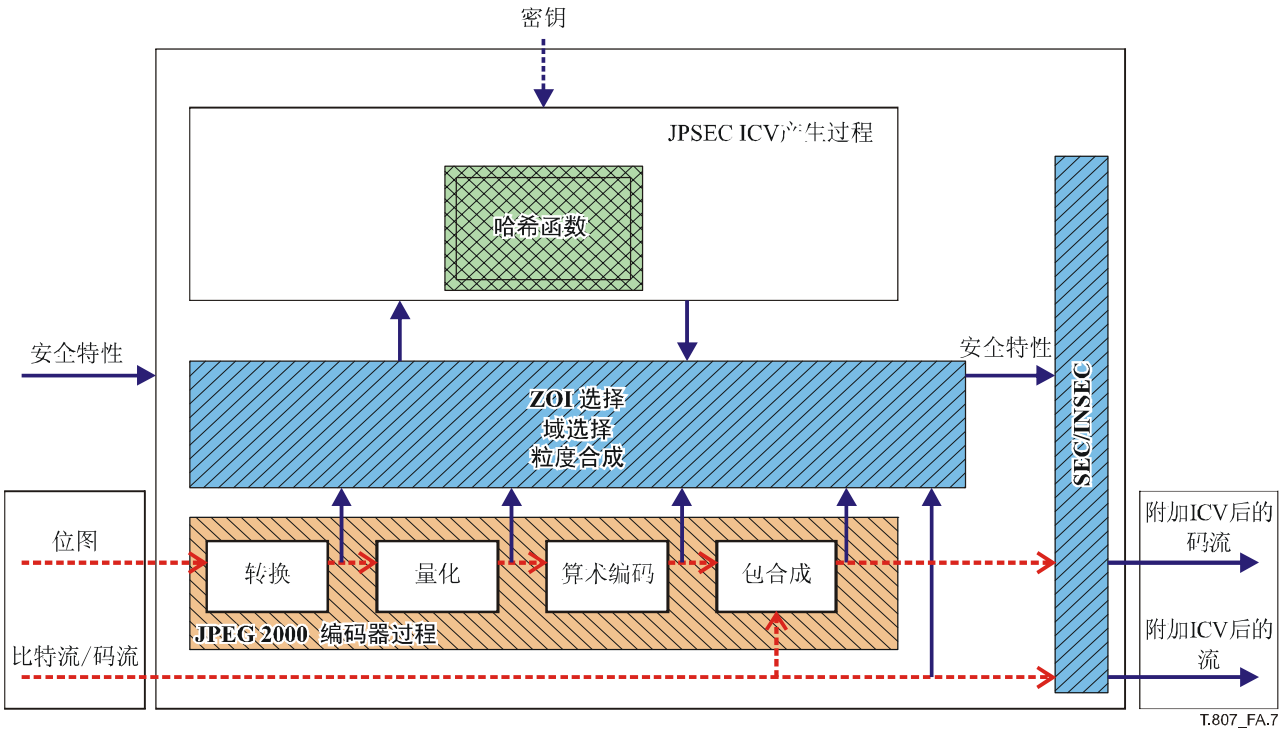


图 A.7－ICV（完整性检查值）产生过程

图 A.7 显示了某个 JPSEC 创建者的 ICV 产生过程示例的概况。本过程包含下述处理：

— 在一个指定的处理域内抽取数据；

— 根据指定的影响区选择被抽取数据中的一部分；

— 使用指定的安全技术，计算适用于所选择数据的ICV。此外，还可能基于粒度信息以单元方式产生ICV；

— 将安全参数特性，包括计算出的ICV，合成到SEC和/或INSEC标记段中。

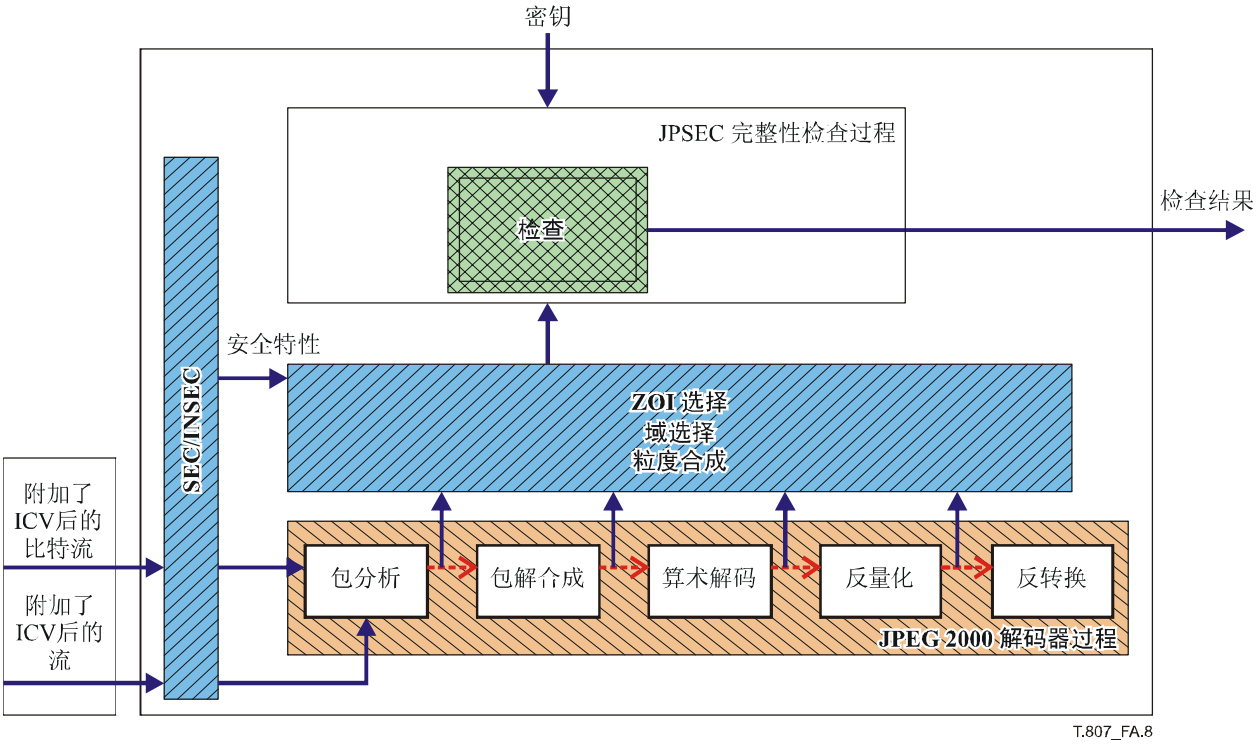


图 A.8－完整性检查过程

图 A.8 显示了某个 JPSEC 消费者的完整性检查过程示例的概况。本过程包含下述处理：

— 根据所标示的处理域抽取数据；

— 根据所标示的影响区选择被抽取数据中的一部分；

— 使用所标示的安全技术验证所选数据。此外，还可能基于粒度信息以单元方式验证所选数据。

附 件 B

技 术 示 例

（本附件是本建议书 | 国际标准的组成部分）

B.1 引言

JPSEC 语法允许标准的和非标准的安全工具应用到 JPEG 2000 图像上。本节描述了十个资料性的技术示例来演示不同的 JPSEC 用法。这些示例仅仅是资料性的，并没有被 JPSEC 标准所核准。然而，提供它们是为了显示标准的灵活性。

这些技术示例包括：

— 用于JPEG 2000的一种灵活的访问控制模式；
— 用于JPEG 2000图像的一种统一的认证框架；
— 用于JPEG 2000码流的一种简单的基于包的认证方法；
— 用于JPEG 2000访问控制的加密工具；
— 用于JPEG 2000访问控制的密钥生成工具；
— 用于条件访问控制的小波和比特流域扰码；
— 用于JPEG 2000码流的渐进式访问；
— 用于JPEG 2000码流的可扩展认证；
— 基于数据分割和数据吸引的JPEG 2000数据机密性和访问控制系统；
— 安全的可扩展的流化和安全的代码转换。

B.2 用于JPEG 2000码流的一种灵活的访问控制模式

B.2.1 安全服务

一个访问控制模式允许根据分辨率、质量层，拼贴和选区等的任意组合来恢复出 JPEG 2000 码流。

B.2.2 典型应用

它为通过各种媒体进行的内容分发提供了保护，包括的媒体如互联网，数字电缆电视，卫星广播以及 CD-ROM 等。一般来说，该技术适用于这样的应用，即一个码流在发布侧仅被加密一次，但在用户侧，根据不同的优先级，这个被保护码流可以采用多种方式解密。

B.2.3 动机

在超级分发模式中，发布者自由地发布被保护内容，但秘密地发布内容密钥。一个希望访问到部分码流的用户可以将其请求发送到密钥服务器。然后，密钥服务器会根据用户的优先级响应一个适当的解密密钥。该用户就可以访问到所允许的图像部分了。

B.2.4 技术概述

一个被保护的 JPEG 2000 码流是通过发布者对每个包进行加密而产生的。技术的核心是如何管理一棵密钥树，该密钥树由任意顺序的拼贴，分量，分辨率，层，选区，甚至码块构成。为了简单地描述此技术，假设此密钥树的顺序为 RLCP（分辨率-层-分量-选区），且每个分辨率都具有相同数量的选区。假设有下面的示例，给定一个单向的哈希函数 h(.)，考虑这样一个 JPEG 2000 图像码流，具有 n_T 个拼贴 s，n_C 个分量，n_L 个层，且每个拼贴-分量都具有 n_R 个分辨率，每个分辨率具有 n_P 个选区。同时有一个用于 JPEG 2000 码流的主密钥 K 。构造一棵密钥树如下：

1） 为每个拼贴 $t = 0$，1，...，$n_T - 1$，产生密钥 $k^t = h(K \,|\, "T" \,|\, t)$，其中，"|"表示级联，"T" 表示字母 T 的ASCII码。
2） 为每个 $r = n_R - 2$，...，1，0，产生密钥 $k^r = h(k^{r+1})$，其中，$k^{n_R - 1} = h(k^t \,|\, "R")$，且"R"表示字母 R 的ASCII码。

3） 为每个$r = n_R - 1$，... ，1，0，$l = n_L - 2$，... ，1，0，计算密钥$k^{rl} = h(k^{r(l+1)})$，其中，$k^{r(n_L-1)} = h(k^r|"L")$，且"*L*"表示字母*L*的ASCII码。

4） 为每个$r = n_R - 1, ... , 1, 0$，$l = n_L - 1, ... , 1, 0$，$c = 0, 1, ... , n_C - 1$，计算密钥$k^{rlc} = h(k^{rl}|"C"|c)$，其中，"*C*"表示字母*C*的ASCII码，而*c* 表示此分量的索引。

5） 为每个$r = n_R - 1, ... , 1, 0, l = n_L - 1, ..., 1, 0, c = 0, 1, ... , n_C - 1, p = 0, 1, ... , n_R - 1$，产生密钥$k^{rlcp} = h(k^{rlc}|"P"|p)$，其中，"*P*"表示字母*P*的ASCII码，而*p*表示此选区的索引。

被保护码流的产生是通过对每个包体采用适当的密钥（密钥树中的一个叶子）进行加密而完成的。

为了从一个被保护码流中恢复出子图像部分，用户需要获取到适当的访问密钥（例如由某个密钥服务器准予）。这些访问密钥能够精确地恢复出对应于所请求的子图像包的密钥树叶子。密钥的重新构造过程类似于密钥树的生成过程。这些叶子被用于解密相应的包。

B.2.5 码流语法

表 B.1 显示了 SEC 段的结构。*ZOI* 字段标示了被准予的参数，P_{ID} 字段标示了用于此访问控制模式的保护方法参数。PM_{ID} 字段总是被设置为 1，表示使用的是解密模板。TP_{ID} 字段标示了用于此访问控制模式的附加参数。*KTO* 为密钥树的生成顺序。字段 L_{aki} 指示了访问密钥信息的长度。

表 B.1－此模式的示例参数

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

参　　数		长度（比特）	取　　值	含　　义
t		8 (FBAS)	1	注册机构保护工具
i		8 (RBAS)	实例值	工具实例标识符
ID_{RA}	$ID_{RA,id}$	32	工具 *ID* 值	注册的 ID
	$ID_{RA,nsl}$	8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$	168	命名空间	此工具注册的 RA 的命名空间
L_{ZOI}		16 (RBAS)	[2 ... $2^{16}-1$]	ZOI 的长度
ZOI		可变的	见5.7	此模式的影响区
L_{PID}		16 (RBAS)	[2 ... $2^{16}-1$]	L_{PID} + P_{ID} 的长度
P_{ID}		可变的	见表 B.2	此模式的参数

表 B.2－P_{ID}

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

参　　数	长度（比特）	取　　值	含　　义
ID_T = 1	8	总是设置为 1	解密模板的标签
T_{decry}	可变的	解密模板值	解密模板
TP_{ID}	可变的	见表 B.3	此模式的附加信息

表 B.3－TP_{ID}

KTO	L_{aki}	AK_{Info}

参　　数	长度（比特）	取　　值	含　　义
KTO	8	0 ... (2^8 – 1)	密钥树顺序。它可能不同于码流的进展顺序。暂时规定如下： 0x00: LRCP　0x01: RLCP 0x02: RPCL　0x03: PCRL 0x04: CPRL　others: 保留
L_{aki}	16	0 ... (2^{16} – 1)	访问密钥信息的长度，如果 L_{aki} = 0，则没有 AK_{Info} 字段出现
AK_{Info}	可变的	见表 B.4	访问密钥的信息（例如密钥的长度，密钥的数量等）

表 B.4－AK_{info}

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

参　　数	长度（比特）	取　　值	含　　义
L_{uk}	16	0 ... (2^{16} – 1)	用户密钥的长度
UK	L_{uk}	NaN	用户密钥信息
E_{ak}	16	见表 24	用于加密访问密钥的密码
N_{ak}	16	0 ... (2^{16} – 1)	访问密钥的数量
AK	N_{ak} * K_{bc}	NaN	访问密钥

B.2.6　结论

本技术可以使发布者用一个主密钥来保护一个 JPEG 2000 码流。允许将被保护的码流发布到任意数量的用户处，但是包的密钥要保持私密。密钥服务器根据用户的优先级为用户产生不同的访问密钥。这些用户根据他们的访问密钥产生准予的包密钥，并得到不同的被准予的图像。也就是说，该技术具有一个特性，被称为“一次加密，多种访问”。

B.3　用于JPEG 2000图像的一种统一认证框架

B.3.1　操作描述

此 JPSEC 工具提供了下列 JPSEC 服务：图像数据/内容完整性验证和源认证，即基于数字签名模式的用于 JPEG 2000 图像的脆弱/半脆弱认证。

由于本工具既支持脆弱认证，又支持半脆弱认证，因此它可被用于各种不同的应用场景中，包括图像分发，图像流化，医学成像及军事成像，司法执行，电子商务以及电子政务等。

在普遍的环境中，图像可能会经历各种不同类型的偶然失真，如代码转换和格式变换。传统的基于密码学的认证技术是在数据完整性级别来保护 JPEG 2000 图像的，而对于保留内容的失真类型也不能够幸免。因此需要半脆弱性认证技术在图像内容级别上来保护 JPEG 2000 图像。此工具统一了图像数据认证和图像内容认证，并且提出了一种新的概念，称为最低认证比特率（LABR）。也就是说，如果图像经过代码转换，到一个不低于 LABR 的比特率，则它将被认为是可信的，否则被认为是不可信的。认证可能是脆弱认证或半脆弱认证。在半脆弱认证模式下，当图像被认为是不可信时，该工具能够标识出发生改变的地点。

B.3.2　技术概述

为了提供脆弱认证和半脆弱认证，一组技术可被应用在此 JPSEC 信息工具上。它们包括特征选择，数字签名，有损耗和无损耗的数据隐藏，以及 ECC（错误校正码）等。根据用户指定的 LABR，并基于对 JPEG 2000 结构的分析，选择适当的特征，然后产生数字签名。对于半脆弱认证，使用 ECC 来增强鲁棒性级别。奇偶校验位（PCB）

被当作水印插入到图像中，这样可以标识出攻击的位置。数据嵌入可以有两种不同的导入方式：有损耗的和无损耗的。如果是有损耗的数据隐藏，则在数据隐藏后不能恢复原始的图像。另一方面，如果是无损耗的数据隐藏，则图像以一种可逆的方式被修改，即如果被标记的图像没有被改变，则原始图像可以被恢复。无损耗的半脆弱认证对 JPEG 2000 是有用的，因为标准支持有损耗到无损耗的压缩。特别地，这对于医学成像和远程成像应用是很有用的，在这些情况下，无损耗是一个基本的需求。

类似于用于控制和表示图像压缩强度的压缩比特率，LABR（最低认证比特率）参数被用于在数量上控制保护强度。例如，当一个 JPEG 2000 图像使用一个 2 bpp（比特每像素）的 LABR 进行保护时，则只要代码转换后的比特率大于或等于 2 bpp，则图像的任何代码转换后的版本都被所提议的系统恢复为可信的。

图 B.1 显示了如何使用工具来保护图像。

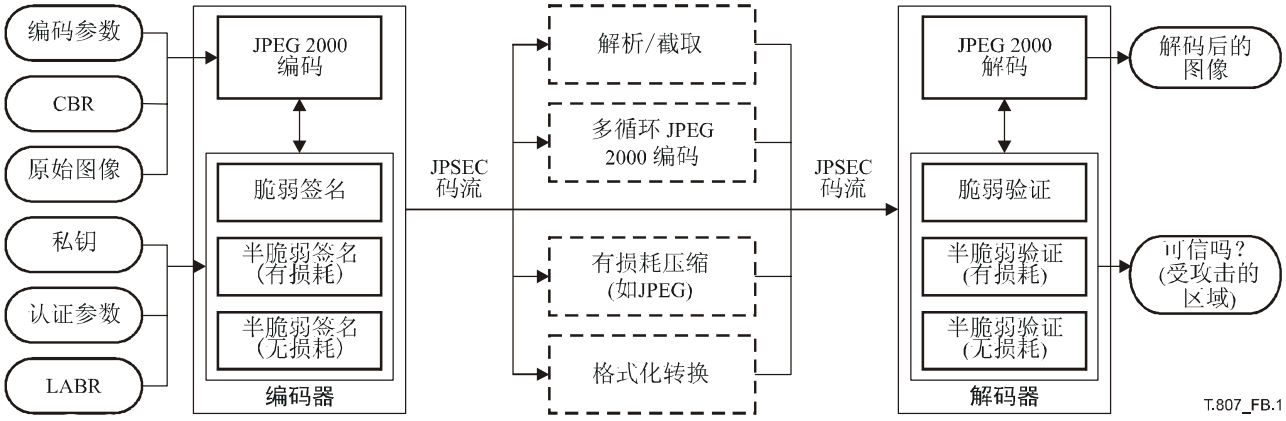


图 B.1－为JPEG 2000使用统一认证框架的图像保护

依赖于所选择的认证方法，本工具可以使用不同的信号化语法。对于脆弱认证，它使用 JPSEC 标准工具语法，如第 5.8.3 节的定义。对于半脆弱认证，它使用 JPSEC 非标准工具语法，如表 B.5 所显示。此外，如果本工具没有使用 INSEC 标记时，则 F_{INSEC} 应当被设置为 0，且 F_{mod} 应当被设置为 1，因为此 JPSEC 工具所产生的码流仍然遵循 JPEG 2000 第一部分。

表 B.5－半脆弱认证语法

参　数				长度（比特）	取　值	导出含义
t				8 (FBAS)	1	使用了非标准的工具语法
i				8 (RBAS)	0 ... (2^7 – 1)	工具实例索引
ID_{RA}	$ID_{RA,id}$			32	0 ... (2^{32} – 1)	由 RA 分配的 ID 号码
	$ID_{RA,nsl}$			8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$			168	*命名空间*	此工具注册的 RA 的命名空间
L_{ZOI}				16 (RBAS)	0 ... (2^{16} – 1)	ZOI 的长度
ZOI				可变的	*ZOI 值 s*	由工具所保护的图像中的覆盖区域
L_{PID}				16 (RBAS)	0 ... (2^{16} – 1)	P_{ID} 和 L_{PID} 的长度，以字节计数
P_{ID}	ID_T			8	2	使用了认证模板，在表 21 中定义
	T_{auth}	M_{auth}		8	2	使用了数字签名方法，如表 34 的定义
		P_{auth}	M_{DS}	8	见表 41	使用的数字签名算法，如 DSA 或 RSA
			H_{DS}	8	见表 37	使用的哈希函数
			KT_{DS}	可变的	*密钥模板值*	公钥存储在 KT_{DS} 中。本工具仅使用一个公钥
			SIZ_{DS}	16	0 ... (2^{16} – 1)	数字签名的长度，以字节计数

表 B.5－半脆弱认证语法

参　数			长度（比特）	取　值	导出含义
P_{ID}	PD		1	0_b	FBAS 结构终止
			1	0_b	没有使用像素域
			1	0_b	没有使用小波系数域
			1	1_b	使用了量化的小波系数域
			1	0_b	没有使用码流域
			3	000_b	保留供 ISO 使用
	G	PO	16	处理顺序值	处理顺序
		GL	8	0000 1001	粒度级别：保护单元是 ZOI 中标识的全部域
	V	N_V	16	1	列表中数字签名的个数为 1
		S_V	8 (RBAS)	1 ... $(2^8 – 1)$	数字签名的长度，以字节计数
		VL	8* S_V	数字签名值	由工具产生的数字签名
	LABR	$LABR_{int}$	8	0 ... $(2^8 – 1)$	LABR 的整数部分
		$LABR_{fra}$	8	0 ... $(2^8 – 1)$	LABR 的小数部分
	Threshold		8	[0 ... $2^8 – 1$]	门限值（仅对无损耗的认证有效）
	Shuffle		8	[0 ... $2^8 – 1$]	为了嵌入水印比特所需的置乱的数量（仅对无损耗的认证有效）

本工具的唯一 ID 由注册机构来分配。关于工具的描述可以使用所分配的 ID 从注册机构（RA）处下载。

B.3.3　结论

总而言之，本工具有如下特性：

- 通过将脆弱认证和半脆弱认证综合在一个框架中，可以对JPEG 2000图像进行图像数据级别认证和图像内容级别认证。此外，半脆弱认证还包括有损耗方式和无损耗方式。
- 具有应对各种偶然失真的鲁棒性，这些失真可能由代码转换，格式变换，有损耗的压缩和JPEG 2000编码的多循环等引起。因此，本工具可用于在普遍的环境中保护JPEG 2000图像。
- 对JPEG 2000图像的可扩展的保护。特别地，本工具能够保护任何拼贴，分量，分辨率，层，选区或码块等。
- 与被称为“公钥基础设施”的达到最新技术发展水平的信息安全框架相兼容，此基础设施是目前存在的国际标准如X.509的基础。
- 由一个被称为LABR的单独参数来控制一种量化的保护强度，这可以为终端用户带来很多的便利。
- 当图像被认为是不可信时，有能力定位可能受到攻击的图像区域。这可以有助于在视觉上使用户信服。
- 支持有损耗到无损耗的保护，对应于对JPEG 2000编码标准的有损耗到无损耗压缩。因此，该工具具有非常广泛的应用，包括医学成像和远程成像应用。

B.4 用于JPEG 2000码流的一种简单的基于包的加密方法

B.4.1 操作描述

本节介绍了一种用于 JPEG 2000 图像的选择性加密技术。它是基于包级别的加密，并且基于一种标准的鲁棒的密码算法。

本技术所专注的安全服务是 JPEG 2000 图像的机密性，通过对码流进行加密而实现。从而使用此技术可以获得 IPR 保护以及私密性保护。

本方法支持代码转换，可扩展性，以及其他内容处理的功能性，而不需要访问密钥，也不需要执行解密和再加密。它不会干预编码和解码过程，且对压缩效率有非常有限的不利影响，而对差错恢复没有任何不利影响。这样一种方法对具有各种不同安全级别的场景和应用的实现具有最大的灵活性。

本技术可能被内容制作者使用来限制对图像内容的访问，或者被内容提供者使用来确保将内容机密地发布给终端用户。

B.4.2 技术概述

本技术的组成是在对图像进行压缩后，再对码流进行加密，如图 B.2 所示。

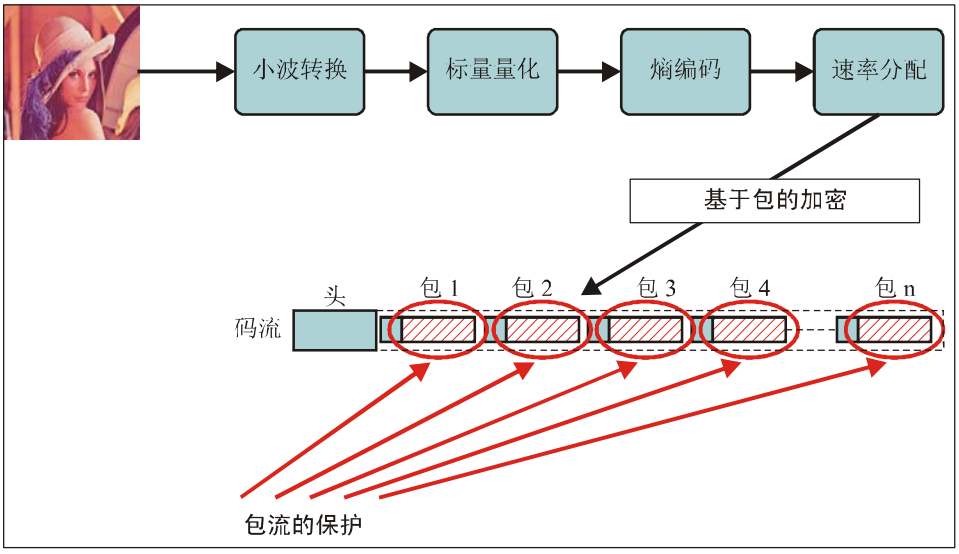


图 B.2－基于包的加密原则

本 JPSEC 工具的输入可以是多个与图像相关的参数：分辨率级别，质量层，分量，选区或拼贴。只有相对应这些输入参数的包开销才被处理。因此，被保护的码流就保持了一种规范的 JPEG 2000 结构。一旦码流被加密，则 SEC 标记段将被加入到主头部，以便允许任何 JPSEC 消费者在稍后可以正确地解密图像。

本方法使用了众所周知的标准底层算法来对包进行选择性加密：DES 或 AES 方法，并采用[22]中描述的标准模式，如 ECB，CBC，CFB，OFB 和 CTR。当然任何其他块密码算法也都可以使用：这里给出了 DES 和 AES 只是作为标准密码的一个示例。

B.4.2.1 信号化示例

本技术可以通过标准化一节中的基于模板的语法来信号化。下面是本技术信号化的一个示例（见表 B.6），该表在 ZOI 中指定了一个区域，当然也可以更多，都遵循与区域 ^{0} 相同的语法。

表 B.6－影响区的示例，具有空间坐标，分辨率和层

参　数			长度（比特）	取值（按顺序）	导出含义
NZzoi			8	1 (RBAS)	区域的数量为 1
Zone[0]	DCzoi		1	0	后面没有跟随字节对齐段
			1	0	与图像相关的描述类
			6	101100	按顺序指定了图像区域，分辨率级别，质量层和分量
	Pzoi[1]	Mzoi[1]	1	0	后面没有跟随字节对齐段
			1	0	指定的区域是受保护方法影响的区域
			1	0	指定了单个项
			2	00	矩形模式
			2	00	Izoi 使用 8 个比特的整数
			1	1	Izoi 使用两个维度来描述
		Izoi[1]	8	0110 0100	Xul 为 100
			8	0111 1000	Yul 为 120
			8	1011 0100	Xlr 为 180
			8	1101 0010	Ylr 为 210
	Pzoi[3]	Mzoi[3]	1	0	后面没有跟随字节对齐段
			1	1	指定区域的补集是受保护方法影响的区域
			1	0	指定了单个项
			2	11	最大模式
			2	00	Izoi 使用 8 个比特的整数
			1	0	Izoi 使用一个维度来描述
		Izoi[3]	8	0000 0010	指定了分辨率级别为≤ 2。（即根据最大模式和补集切换，指定的是分辨率级别 > 3）
	Pzoi[4]	Mzoi[4]	1	0	后面没有跟随字节对齐段
			1	0	指定的区域是受保护方法影响的区域
			1	0	指定了单个项
			2	11	最大模式
			2	00	Izoi 使用 8 个比特的整数
			1	0	Izoi 使用一个维度来描述
		Izoi[4]	8	0000 0101	根据最大模式，指定了层≤ 5

表 B.7－解密模板描述，在AES-192/CBC的情况下

参　数					长度（比特）	取　值	导出含义
P_{PM}	ME_{decry}				8	0000 0000	空：没有标记竞争预防方法
	CT_{decry}				16	0x0003	密码标识符：AES（块密码）
	CP_{decry}	M_{bc}			6	10 0000	密码模式：CBC
		P_{bc}			2	01	填充模式（PKCS#7-填充）
		SIZ_{bs}			8	0001 0000	块长度：16 个字节（128 比特）
		KT_{bc}	LK_{KT}		16	0x00C0	密钥长度：192 个比特
			KID_{KT}		8	0000 0011	密钥信息是一个 URI
			LKI_{KT}		16	0x0021 (=33)	URI 的长度：33 个字节
			KI_{KT}		264	https://server/path/secretkey.pem	此 URI 是一个 https URL；它必须被使用 JPSEC 的应用程序所理解。如何有效地获取密钥不在本标准的范围之内。
			G_{KT}	PO	16	0 000 001 010 011 100	处理顺序为 TRLCP
				GV	8	0000 1001	密钥的粒度为 ZOI 中的全部区域
			V_{KT}	Nv	16	0x0001	KI_{KT} 中的单一密钥值；值没有在 V_{KT} 中指定
				Sv	16	0010 0001	URI 的长度：33 个字节
				VL	264	https://server/path/secretkey.pem	本 URI 是一个 https URL；它必须被使用 JPSEC 的应用程序所理解。如何有效地获取密钥不在本标准的范围之内。

表 B.8－处理域语法

参　数	长度（比特）	取　值	导出含义
PD	1	0_b	后面没有跟随字节对齐段
	1	0_b	不在像素域中
	1	0_b	不在小波系数域中
	1	0_b	不在量化的小波系数域中
	1	1_b	在码流域中处理
	3	000_b	未使用

表 B.9－粒度和取值列表的语法

参　数		长度（比特）	取　值	导出含义
G	PO	16	0 000 001 010 011 100	处理顺序为 TRLCP
	GV	8	0000 0110	保护单元为包
V	N_V	16	1	指定的 IV 值的个数
	Sv	8	16	IV 长度，以字节计数
	VL	128	值	IV 值

B.4.3　结论

本节中介绍的技术演示了如何对 JPEG 2000 图像进行选择性加密。它是基于包级别的加密，并且使用标准的鲁棒的加密算法。它可以使用第 5.8 节定义的模板来信号化，并且支持各种级别的复杂度。

B.5 用于JPEG 2000访问控制的加密工具

B.5.1 提出的安全服务

本技术提供了一种加密工具，可以防止在一个加密后的码流中出现标记竞争。

B.5.2 典型应用

本技术允许对 JPEG 2000 码流进行选择性加密或全部加密。这种选择性加密方法可被用于仅显示一个被允许的图像，如一个粗略的，低质量的图像，以及一个被部分扰码的图像等。

B.5.3 潜在用户，实现模型及动机

基本上，本技术是对 JPEG 2000 码流进行基于包的加密，并采用众所周知的密码算法。特别地，本技术防止了在加密后的码流中出现标记竞争。因此，即使作为结果的加密后的码流输入给一个与 JPEG 2000 第一部分相兼容的解码器，该解码器也不能够损毁或正确地播放此被保护的图像。

B.5.4 技术概述

（1） 加密

步骤 1 使用众所周知的密码算法对 2 个字节的码进行临时加密。

步骤 2 如果临时加密后的码或其相关联的码大于 0xFF8F，则这两个字节的码不能被加密。

否则，被临时加密后的码作为加密后的码输出。

步骤 3 移动到下一个 2 个字节的码上，然后继续步骤 1 和步骤 2。

根据第一部分的规范，明文中的所有 2 个字节的码都应当小于 0xFF90。更进一步说，如果临时加密后的码或其相关联的码大于 0xFF8F，则这两个字节的码不能被加密。由此引起的结果是密文中所有的 2 个字节的码都小于 0xFF90。

如果明文的长度为奇数，则有必要进行一个异常处理；最后一个字节不被加密，或者使用一个额外的字节来填充。

（2） 解密

步骤 1 使用与加密相同的密码算法对 2 个字节的码进行临时解密。

步骤 2 如果临时解密后的码或其相关联的码大于 0xFF8F，则这两个字节的码不能被解密。否则，被临时解密后的码作为解密后的码输出。

步骤 3 移动到下一个 2 个字节的码上，然后继续步骤 1 和步骤 2。

加密前的原始明文中的所有 2 个字节的码都应当小于 0xFF90。因此，有可能作出结论说，如果临时解密后的码或其相关联的码大于 0xFF8F，则这两个字节的码是没有被加密的。

B.5.5 信号化方法

表 B.10 显示了本技术的示例参数。本技术的任何参数都应当根据 JPSEC 中标识的语法来进行信号化。特别地，本技术应当使用“解密”模板，“包”粒度，和“比特流”处理域，并具有适当的 ZOI。

表 B.10－本技术的示例参数

参　数		长度（比特）	取　值	含　义
SEC		16	0xFF65	SEC 标记
L_{SEC}		16	可变的	SEC 标记段的长度
Z_{SEC}		8	1 （示例）	本 SEC 标记段的索引
P_{SEC}		1	0	后面没有跟随 FBAS 字节
	F_{INSEC}	1	1 （示例）	使用了 INSEC
	$F_{multiSEC}$	1	0_b	使用了一个 SEC 标记段
	F_{mod}	1	1_b	原始的 JPEG 2000 数据被修改
	F_{TRLCP}	1	0_b	没有定义 TRLCP 标签的用法
	Padding	3	000_b	未使用
	N_{tools}	8 (RBAS)	1	安全工具的数量为 1
	I_{max}	8 (RBAS)	0	最大的工具实例索引为 0
t		8 (FBAS)	1	RA 保护，JPSEC 非标准的工具
i		8 (RBAS)	0000000_b	工具实例索引
ID_{RA}	$ID_{RA,id}$	32	0	注册的 ID
	$ID_{RA,nsl}$	8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$	168	命名空间	本工具所注册的 RA 的命名空间
L_{zoi}		16	9	ZOI 的长度为 9 个字节
ZOI		可变的	见表 B.11（示例）	本工具的影响区
L_{PID}		16	可变的	L + T + PD + G 的长度
P_{ID}		可变的	见表 B.12（示例）	本技术的参数

表 B.11－本密钥生成工具的示例ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NDzoi			8	1	区域的数量为 1
$Zone^0$	Dczoi		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	101000_b	按顺序指定了图像区域和分辨率级别
	$Pzoi^1$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域是受保护方法影响的区域
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 个比特的整数
			1	1_b	Izoi 使用两个维度来描述
		$Izoi^1$	8	$0110\ 0100_b$	Xul 为 100
			8	$0111\ 1000_b$	Yul 为 120
			8	$1011\ 0100_b$	Xlr 为 180
			8	$1101\ 0010_b$	Ylr 为 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	后面没有跟随字节对齐段
			1	1_b	指定的区域不是受保护方法影响的区域
			1	0_b	指定了单个项
			2	11_b	最大模式
			2	00_b	Izoi 使用 8 个比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^3$	8	$0000\ 0010_b$	指定了分辨率级别 > 3

表 B.12－本技术的P_{ID}

参　　数		长度（比特）	取　　值	含　　义
T		可变的	见表 B.13	解密模板
PD		8	$0000\ 1000_b$	后面没有跟随 FBAS 字节。在码流域进行处理。
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100\ 0_b$	处理顺序为拼贴-分辨率-层-分量-选区。
	GL	8	$0000\ 0110_b$	保护单元为包
Skip		8	0	本工具的 *Skip* 参数

表 B.13－本技术的解密模板示例

参　　数		长度（比特）	取值（按顺序）	导 出 含 义
ME_{decry}		8	1	没有出现标记竞争
CT_{decry}		16	1	块密码（AES）
CP_{decry}	M_{bc}	6	$10\ 0010_b$	使用了 OFB 模式。（比特未被填充）
	SIZ_{bc}	16	128	块长度（128 比特）
	KT_{bc}	可变的	*密钥模板值*	密钥模板
	IVsc	128	*初始向量值*	初始向量值

B.5.6　结论

本节描述了用于 JPEG 2000 码流的一种加密技术。本技术的一个最突出的优势是可以防止在加密后的码流中出现标记竞争。

B.6　用于JPEG 2000访问控制的密钥生成工具

B.6.1　提出的安全服务

本技术根据 JPEG 2000 的分等级结构，提供了一种用于 JPEG 2000 的与图像相关的访问控制。

B.6.2　典型应用

本技术的一个典型应用是安全的图像分发，仅有授权用户才能够播放所接收到的图像。例如，可以自由地显示一个粗略的图像，但仅有拥有密钥的用户才能够对具有高分辨率的图像进行解码。

B.6.3　潜在用户，实现模型及动机

本技术支持生成密钥，这些密钥在一个安全的 JPEG 2000 图像的分发中使用。本技术基于一种与图像相关的访问控制，例如基于图像区域，分辨率和图像质量等。本技术的原则是分等级地产生加密和解密密钥，使用的是密码学中的单向哈希函数，如一个哈希函数。

B.6.4 技术概述

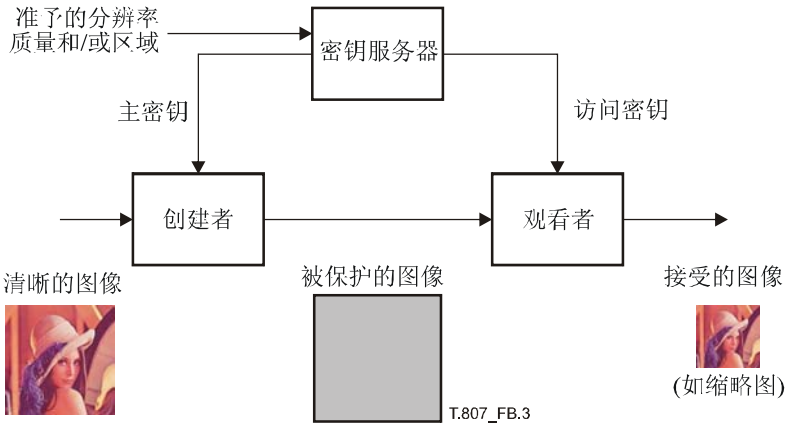


图 B.3－本技术的概述

在加密阶段，一个密钥服务器产生一个主密钥。然后，一个创建者使用由主密钥所产生的包密钥来对图像进行加密。在解密阶段，一个密钥服务器根据准予的分辨率、质量和/或区域等产生一个访问密钥。然后，观看者使用由访问密钥所产生的包密钥对加密后的图像进行解密。需要注意的是这些密钥都是基于安全的哈希链而顺序生成的。

特别地，本技术使用了下述的访问控制策略："如果某个用户可以访问到一个分辨率级别/层，则该用户也可以访问到更低的分辨率级别/层"。而另一方面，即使某个用户可以访问到一个拼贴，该用户也根本不能够访问到其他拼贴。

本技术的一个重要优势是需要从一个密钥服务器传递到某个观看者的密钥的数量远远低于传统的方式。这就意味着本技术在存储方面允许更小的负荷。

B.6.5 信号化方法

表 B.14 显示了本技术中使用的推荐参数。任何参数都应当根据 JPSEC 中确定的语法来进行信号化。特定地说，本工具应当使用"解密"模板，"包"粒度，以及"比特流"处理域，并具有适当的 ZOI。

表 B.14－本技术中推荐的参数

参　数		长度（比特）	取　值	含　义
SEC		16	0xFF65	SEC 标记
L_{SEC}		16	0 ... 255	SEC 标记段的长度
Z_{SEC}		8	0	本 SEC 标记段的索引
P_{SEC}		1	0	后面没有跟随 FBAS 字节
	F_{INSEC}	1	1	使用了 INSEC
	$F_{multiSEC}$	1	0_b	使用了一个 SEC 标记段
	F_{mod}	1	1_b	原始的 JPEG 2000 数据被修改
	F_{TRLCP}	1	0_b	没有定义 TRLCP 标签的用法
	Padding	3	000_b	未使用
	N_{tools}	8 (RBAS)	1	安全工具的数量为 1
	I_{max}	8 (RBAS)	0	最大的工具实例索引为 0
t		8 (RBAS)	1	JPSEC 非标准工具
i		8 (RBAS)	0	本工具的实例索引

表 B.14－本技术中推荐的参数

参　数		长度（比特）	取　值	含　义
ID_{RA}	$ID_{RA,id}$	32	5	本工具的注册 ID
	$ID_{RA,nsl}$	8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$	168	*命名空间*	本工具所注册的 RA 的命名空间
L_{zoi}		16	可变的	本工具的 ZOI 的长度
ZOI		可变的	*ZOI 值*	本工具的影响区
L_{PID}		16	可变的	L + T + PD + G 的长度
P_{ID}		可变的	见表 B.16	本技术的参数

表 B.15－本密钥生成工具的示例ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NDzoi			8	1	区域的数量为 1
$Zone^0$	Dczoi		1	0_b	后面没有跟随字节对齐段
			1	0_b	与图像相关的描述类
			6	101000_b	按顺序指定了图像区域和分辨率级别
	$Pzoi^1$	$Mzoi^1$	1	0_b	后面没有跟随字节对齐段
			1	0_b	指定的区域是受本保护方法影响的区域
			1	0_b	指定了单个项
			2	00_b	矩形模式
			2	00_b	Izoi 使用 8 个比特的整数
			1	1_b	Izoi 使用两个维度来描述
		$Izoi^1$	8	$0110\ 0100_b$	Xul 为 100
			8	$0111\ 1000_b$	Yul 为 120
			8	$1011\ 0100_b$	Xlr 为 180
			8	$1101\ 0010_b$	Ylr 为 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	后面没有跟随字节对齐段
			1	1_b	指定的区域是不受本保护方法影响的区域
			1	0_b	指定了单个项
			2	11_b	最大模式
			2	00_b	Izoi 使用 8 个比特的整数
			1	0_b	Izoi 使用一个维度来描述
		$Izoi^3$	8	$0000\ 0010_b$	指定了分辨率级别为 > 3

表 B.16－本技术的P_{ID}

参　　数		长度（比特）	取　　值	含　　义
T		可变的	见表 B.17	解密模板
PD		8	$0000\ 1000_b$	后面没有跟随 FBAS 字节。在码流域进行处理。
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	$0000\ 0110_b$	保护单元为包
H		16	见第 5.8.3.1 节中的表 37	本密钥生成工具的哈希函数
L_k		8	0 ... 255	访问密钥信息的长度
AK_{info}		可变的	访问密钥值	访问密钥信息（本信息使用 T 中的 KT_{bc} 进行加密）

表 B.17－本技术中的解密模板的示例

参　　数		长度（比特）	取值（按顺序）	导 出 含 义
ME_{decry}		8	1	没有出现标记竞争
CT_{decry}		16	3	块密码（AES）
CP_{decry}	M_{bc}	6	10 0010	使用了 OFB 模式。（比特未被填充）
	SIZ_{bc}	16	128	块长度（128 个比特）
	KT_{bc}	可变的	见 5.8.5	密钥模板
	IVsc	128	初始向量值	初始向量值

B.6.6　结论

本节描述了用于 JPEG 2000 码流的一种与图像相关的访问控制技术。本技术的一个重要优势是被管理和被访问的密钥个数远远少于传统方式。

B.7　用于条件访问控制的小波和比特流域扰码

B.7.1　摘要

对一个图像进行访问控制在安全成像中是一种重要的功能性。通常，对一个具有小分辨率的粗略图像或一个低质量的图像进行访问是可以的，但是要访问到一个高分辨率或高质量的图像就需要授权。本节中，提出了一种可以进行条件访问控制的技术。该方法最初出现在[23]中。从根本上说，它在图像中增加了伪随机噪音。授权用户已知伪随机序列，因此能够移除这些噪音。而另一方面，未授权用户仅能够访问到严重失真的图像。系统由三个主要组件构成：扰码，伪随机数生成器和加密算法。为了能够完整地使用和维护 JPEG 2000 的特性，扰码是被选择性地应用到组成码流的码块上的。从而，在图像的特定部分所引入的失真级别是可控的。这就使得可以根据分辨率、质量或感兴趣的区域对图像进行访问控制。

B.7.2　技术概述

本系统由三个主要的组件构成：

- 扰码：支持两种方法。扰码可以或者在量化的小波系数上执行，或者直接在码流中的比特上执行。在第一种情况下，每个码块中的系数标记都被伪随机地反转。在第二种情况下，码流中的比特被伪随机地反转。
- 伪随机数生成器（PRNG）：PRNG是用于驱动扰码的。它基于一个种子值。在本技术的一个建议的实现中，为伪随机数生成器（PRNG）使用了一种具有64比特种子的SHA1PRNG算法[24] 。需要注意的是其他的PRNG算法也可以同样使用。
- 加密算法：为了将种子传送给授权用户，它们被加密并被插入到码流中。在本技术的一个建议的实现中，使用了RSA算法来进行加密[25]。其他的加密算法也可以同样使用。密钥的长度可以在图像被保护时选择。

图 B.4 和 B.5 分别对应于小波和比特流域扰码的两种情况。

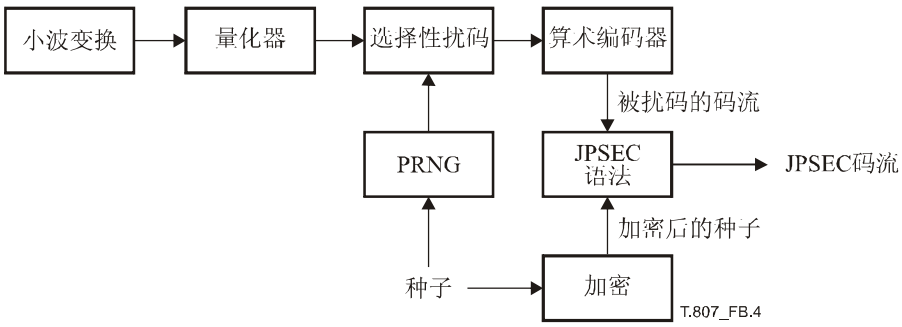


图 B.4－小波域扰码的块状图

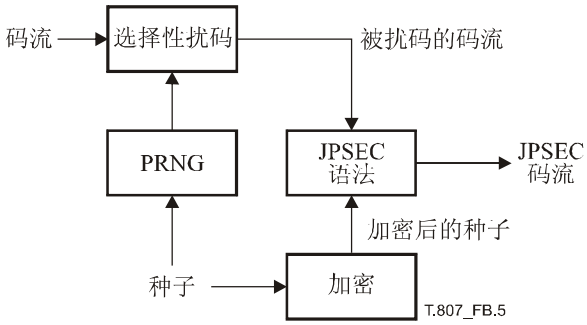


图 B.5－比特流域扰码的块状图

为了提高系统的安全性，从一个码块到另一个码块，种子是可变的。此外，还可以使用不同的加密密钥定义不同层次的访问。下面给出的语法是非常灵活的，并且支持使用多种子和多密钥。

B.7.3 码流语法

在本例中，使用了 SEC 标记段和 INSEC 标记段。码流语法定义如下。SEC 标记段使用的是非标准工具的工具语法。INSEC 标记段被用来标示哪个码块被扰码，以及使用了哪些种子。

B.7.3.1 SEC标记段的语法

用于非标准工具的工具语法被使用。在多密钥的情况下，在 SEC 标记段中使用了工具的多个实例。更具体地说是出现了具有相同 ID 的多个实例 i = 0, 1, 2, ... ，每个实例都对应于一个不同的密钥标识 $KeyID^{(i)}$。如下所示。见图 B.6。

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

图 B.6－在多密钥情况下非标准保护工具的语法

其中，P_{ID} 具有下列语义：

表 B.18－P_{ID}的语法和语义

参　　数	长度（比特）	含　　义
N_s	16	本实例使用的种子的个数
KeyID	32	解密时使用的密钥标识
Data	可变的	加密后的种子

B.7.3.2 INSEC标记段的语法

为了将使用哪个种子来保护哪个码块的信息包含在内，还使用了内部码流安全标记（INSEC）。在本例中，它在安全的码块之前加入，来指示使用哪个种子来保护这个/这些码块。但该标记并不是直接标识了种子本身，而是包含了一个索引，该索引指向主头部 SEC 标记段中的种子。正如例中所示，INSEC 信息应用于下列码块，R 总是等于 1。AP 的语法在小波扰码和比特流扰码中的情况是不同的。

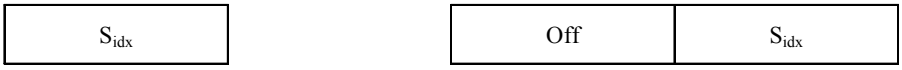


图 B.7－AP的语法：小波域扰码（左侧），比特域扰码（右侧）

具有下述语义：

表 B.19－AP的语法和语义

参　　数	长度（比特）	含　　义
Off	16	第一个被扰码的字节在码块比特流中的偏移量
S_{idx}	16	码块的种子索引

在多密钥的情况下，工具实例 i 和种子索引 S_{idx} 的组合唯一地标识了本 INSEC 标记段指向的是哪个种子/密钥。

B.7.4 结论

在本节中，描述了一种用于 JPEG 2000 图像的条件访问控制的安全工具。本技术在码流的所选部分引入了一种伪随机噪音。因此，对于一个不知如何移除此噪音的未授权的解码者而言，解码后的图像将有很大的失真。

本技术的安全性依赖于用在伪随机数生成器和种子加密中的特定算法的安全性，在我们推荐的实现中，分别使用了 SHA1PRNG 和 RSA。SHA1PRNG 是一种安全的 PRNG，因为知道序列中的某些数字并不能够推导出整个序列的知识。在本例中，PRNG 种子为 64 个比特，这将使得强破坏性的攻击成为不可行。种子的加密使用的是 RSA，并使用用户自定义的密钥长度。如果有足够的密钥长度可用，则 RSA 被认为是一种安全的算法。

B.8 用于JPEG 2000码流的渐进式访问

B.8.1 提出的安全服务

本方法根据码流中的一种进展顺序，为 JPEG 2000 提供了一种与非图像相关的访问控制。

B.8.2 典型应用

本技术的一个典型应用是安全的图像分发，其中仅有授权用户才能够播放接收到的图像。特别地，本技术适用于根据码流中的进展顺序进行访问控制。

B.8.3 潜在用户，实现模型及动机

在设计访问控制模式时，其挑战是如何在安全性、有效性和灵活性之间达到一种微妙的平衡。这种用于 JPEG 2000 码流的访问控制技术构造了一个哈希链来为每个包产生密钥，这样可以对码流中的包进行加密。因此，仅具备正确的安全许可的用户才能够对码流中的与被准予图像部分相对应的包进行解密。

B.8.4 技术概述

在加密阶段，一个密钥服务器生成一个主密钥。然后，一个创建者使用由主密钥产生的包密钥对码流进行加密。在解密阶段，一个密钥服务器根据准予的包产生一个访问密钥。然后，观看者使用由访问密钥所产生的包密钥对加密后的码流进行解密。

特别地，本技术使用了下述访问控制策略："如果某个用户能够访问到一个包，则该用户也能够访问到此码流中的前面的包"。因此，我们称这样一种访问控制为"渐进式访问"。

本技术的重要优势是需要从一个密钥服务器传递到某个观看者的密钥的数量远远低于传统的方式。这就意味着本技术在存储方面允许更小的负荷。

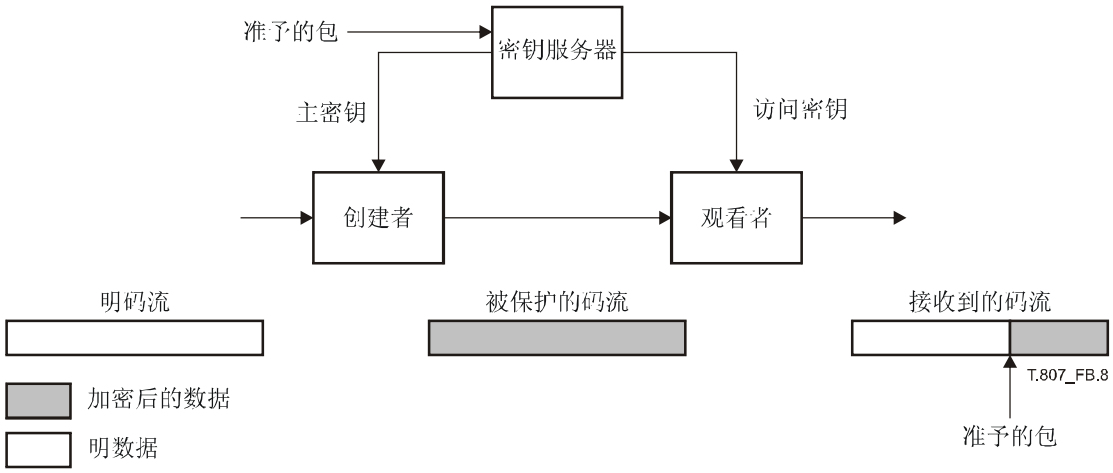


图 B.8－本技术的技术概述

B.8.5 信号化方法

表 B.20 显示了本技术的推荐参数。任何参数都应当根据 JPSEC 中标识的语法来信号化。特定地，本技术应当使用"解密"模板，"包"粒度，以及"比特流"处理域，并具有适当的 ZOI。

表 B.20－本工具的示例参数

参　数		长度（比特）	取　值	含　义
SEC		16	0xFF65	SEC 标记
L_{SEC}		16	可变的 0 ... 255	SEC 标记段的长度
Z_{SEC}		8	0	本 SEC 标记段的索引
P_{SEC}		1	0	后面没有跟随 FBAS 字节
	F_{INSEC}	1	1_b	使用了 INSEC
	$F_{multiSEC}$	1	0_b	使用了一个 SEC 标记段
	F_{mod}	1	1_b	原始的 JPEG 2000 数据被修改
	F_{TRLCP}	1	0_b	没有定义 TRLCP 标签的用法
	Padding	3	000_b	未使用
	N_{tools}	8 (RBAS)	1	安全工具的数量为 1
	I_{max}	8 (RBAS)	0	最大的工具实例索引为 0

表 B.20－本工具的示例参数

参　数		长度（比特）	取　值	含　义
t		8 (RBAS)	1	RA 保护工具
i		8 (RBAS)	0	实例索引
ID_{RA}	$ID_{RA,id}$	32	7	注册的 ID
	$ID_{RA,nsl}$	8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$	168	命名空间	本工具被注册的 RA 的命名空间
L_{zoi}		16 (RBAS)	可变的	ZOI 的长度
ZOI		可变的	见表 B.21（示例）	本工具的影响区
L_{PID}		16 (RBAS)	可变的	L + T + PD + G 的长度
P_{ID}		可变的	见表 B.22（示例）	本工具的参数

表 B.21－本技术的示例ZOI

参　数			长度（比特）	取值（按顺序）	导出含义
NDzoi			8	1	区域的数量为 1
$Zone^0$	DCzoi		1	0	后面没有跟随字节对齐段
			1	1	与非图像相关的描述类
			6	000100	指定了包
	$Pzoi^4$	$Mzoi^4$	0	1	后面没有跟随字节对齐段
			1	1	指定的区域不是受保护方法影响的区域
			1	1	指定了多个项
			11	2	最大模式
			00	2	Izoi 使用 8 个比特的整数
			00	2	Izoi 使用一个维度来描述
		$Izoi^{11}$	8	0000 1010	标识了包索引 > 10

表 B.22－本技术的P_{ID}

参　数		长度（比特）	取　值	含　义
T		可变的	见表 B.23	解密模板
PD		8	$0000\ 1000_b$	不存在后续的 BAS 字节。码流域
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	处理顺序为拼贴-分辨率-层-分量-选区
	GL	8	$0000\ 0110_b$	包含单元为包
H		16	见 5.8.3.1 节中的表 37	本密钥生成工具的哈希函数
L_k		8	0 ... 255	访问密钥信息的长度
AK_{info}		可变的	访问密钥值	访问密钥信息（本信息使用 T 中的 KT_{bc} 来加密）

表 B.23－本技术的解密模板的示例

参　数		长度 （比特）	取值 （按顺序）	导出含义
ME_{decry}		8	1	没有出现标记竞争
CT_{decry}		16	3	块密码（AES）
CP_{decry}	M_{bc}	6	10 0010	使用了 OFB 模式（比特没有被填充）
	SIZ_{bc}	16	128	块长度（128 比特）
	KT_{bc}	可变的	*密钥模板值*	密钥模板
	IVsc	128	*初始向量值*	初始向量值

B.8.6　结论

本节描述了用于 JPEG 2000 码流的一种访问控制技术。本技术的重要优势是被管理的和被访问的密钥的数量远远低于传统方式。本技术根据码流中的一种渐进顺序，提供了一种灵活的和有效的 JPEG 2000 访问控制。

B.9　用于JPEG 2000码流的可扩展认证

B.9.1　安全服务

本节提供了一种用于 JPEG 2000 码流的灵活的认证机制。它允许用户使用一个单独的数字签名来验证不同的子图像的真实性和完整性。

B.9.2　典型应用

在一些重要的应用领域，如政府、财政、健康卫生，以及法律等，客户通常会要求对所接收到的内容进行真实性认证。相应地，在内容分发中也需要一种可扩展的安全机制来对文档进行认证。

B.9.3　动机

在第三方出版应用中，一个图像的生产者会产生一个码流及其签名。然后，生产者将码流及其签名交付给一个第三方出版商。由于资源限制（如带宽，计算能力），用户可能会要求出版商提供代码转换后的码流。出版商于是将子图像数据及其真实性证据交付给用户。

B.9.4　技术概述

本模板提供了一种用于 JPEG 2000 码流的灵活的认证机制。它包括三个模块：签名，代码转换和验证。基本技术为 Merkle 树，该树将 JPEG 2000 的包组织起来。

B.9.4.1　签名模块

签名模块根据推荐的数字签名模式在一个输入的 JPEG 2000 码流中产生一个签名。被保护的码流是通过将 SEC 标记插入到原始的码流中而产生的。特别地，生产者：

- 读取一个JPEG 2000码流。
- 构造一棵哈希树，以便产生根值。每个叶节点的取值是一个包的哈希值。每个内部节点的取值是其孩子节点的哈希值。该树的结构类似于码流的进展顺序。
- 基于某个签名算法，使用一个私钥对哈希树的根值签名。
- 创建SEC参数。并将这些参数插入到SEC段中，以便产生一个可信的码流。

B.9.4.2 代码转换模块

它根据所要求的分辨率、层、分量和选区等，生成辅助的完整性令牌（SIT）以及一个经过代码转换后的码流。新码流的 SEC 包括 SIT 以及其他一些参数。特别地，出版商和/或其代理：

- 读取丢弃的包，这些包没有包含在代码转换后的码流中。
- 使用丢弃的包构造一棵哈希子树。
- 将子树的根值插入到SEC段中。

经过代码转换后的码流包括更新后的 SEC 段和除去丢弃包后的码流。

B.9.4.3 验证模块

验证模块检查被保护码流的真实性。根据所推荐的数字签名模式，验证者首先获取到公钥，然后：

- 读取所接收的码流。
- 根据接收到的包和码流头部，自底向上构造哈希树。如果有某些包被丢弃，则使用相应的SIT来替代子树。这样，根′值就构造好了。
- 根据特定的签名系统，验证根值与SEC段中的签名是否匹配。如果匹配，则码流被接受；否则拒绝所接收到的包。

B.9.5 码流语法

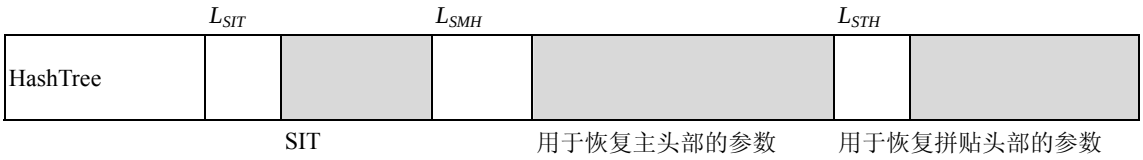
SEC 结构在表 B.24 中显示。它包括 SEC 标记，工具 ID，ZOI，认证模板，以及用于验证的安全参数。安全参数包括可以恢复码流头部的数据。

表 B.24－非标准工具语法

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

参　　数		长度（比特	值	语　　义
t		8 (RBAS)	1	注册机构保护工具
i		8 (RBAS)	实例值	工具实例标识符
ID_{RA}	$ID_{RA,id}$	32	*ID* 值	注册的 ID
	$ID_{RA,nsl}$	8 (RBAS)	21	$ID_{RA,ns}$ 的长度，以字节计数
	$ID_{RA,ns}$	168	命名空间	本工具注册的 RA 的命名空间
L_{ZOI}		16	[0 ... 2^{16} – 1]	ZOI 参数的长度
ZOI_{ID}		可变的	ZOI 值	区域参数
L_{ID}		16	[19 ... 2^{16} – 1]	参数的长度
ID_T		8	2	认证模板类 ID
T		可变的	认证模板值	认证/MAC 模板
TP_{ID}		可变的	见表 B.25	安全参数

表 B.25－安全参数



参　　数	长度（比特）	取　　值	含　　义
HashTree	8	0 ... (2^8 – 1)	哈希树的顺序。它可能不同于码流的进展顺序。暂时规定如下： 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL 其他: 保留
L_{SIT}	16	0 ... (2^{16} – 1)	SIT 的个数
SIT	可变的：L_{hash}*L_{SIT}	NaN	辅助的完整性令牌
L_{SMH}	16	0 ... (2^{16} – 1)	SMH 的长度
SMH	可变的		用于恢复主头部的参数
L_{STH}	16	0 ... (2^{16} – 1)	STH 的长度
STH	可变的		用于恢复拼贴头部的参数
a) 对于带密钥的 MAC 认证，（验证）密钥应当被独立交付。 b) NaN: 不是一个数字。 c) L_{hash} 是哈希值的长度，例如对 SHA-1 来说是 160。			

B.9.6　结论

本技术为 JPEG 2000 码流提供了一种灵活的认证机制。它具有“一次签名，多种方法验证”的特性。具体地说，当某个原始的 JPEG 2000 码流被签名一次后，由原始码流经过代码转换而来的各种不同的码流都可以仅根据对生产者的信任而被验证。这种特性可以与“压缩一次，多种方法解压缩”的功能性很完美地相匹配。这种方法与传统的图像认证方法形成对照，传统的方法允许一个签名仅能够认证一个图像。

B.10　基于数据分割和吸引的JPEG 2000数据机密性和访问控制系统

本节所描述系统的基础是，通过一个被称为*数据分割和吸引* 的过程，将一个原始的 JPEG 2000 文件分割为两个新的文件，这两个文件分别被称为 *Lured_jp2file*，此文件携带了被保护的内容，和 *Control_File*，此文件携带了访问被保护内容时所需的必要信息。只有在这两个文件通过*现场组合（Live_Composing）*过程进行实时组合时，才允许对原始的JPEG 2000文件进行重建。现场组合受访问控制规则和权限管理的控制。所描述的系统在JPEG 2000 数据的机密性和访问控制中，提供了一种高级别的鲁棒性和灵活性，并且基于低时间消耗和低成本的计算操作。

B.10.1　操作描述

B.10.1.1　提出的安全服务

— 机密性：一个Lured_jp2file文件携带了被保护的内容。如果仅对单个的Lured_jp2file文件进行解码，则恢复后的内容在视觉上是被扰码的，由此可以防止对原始内容的访问。只有通过现场组合过程，对存储在Control_File中的数据进行实时恢复时，才允许对原始内容进行访问。

— 访问控制：本系统可被用于在图像内容上执行访问控制：多个用户共享同一个Lured_jp2file文件，但是由于他们拥有不同的访问权限，因此不会允许他们访问到内容的同一个部分。

注意 IPR 保护：通过将内容访问与认证和权限管理链接起来，可以确保根据内容所有者的意愿和特权，对被保护内容的广播和使用进行有效地控制和跟踪，这可能是通过将此系统与加水印或指纹识别相结合而实现的。

B.10.1.2 典型应用

本系统所描述的一个关键思想是将原始的 JPEG 2000 分割为两个文件，第一个文件（Lured_jp2file）携带 99％的原始数据和 1％的被称为诱饵的虚拟数据，该文件可以通过任何传统的网络或媒体免费地分发、广播、交换或拷贝；第二个文件（Control_File）携带 1%的原始数据，再加上要访问 Lured_jp2file 中的被保护内容所绝对要求的一些信息。

另一个关键的思想是通过一种鉴定和权限管理步骤将访问与 Lured_jp2file 中携带的被保护内容链接起来，这种步骤的结果将触发信息的流化，而这些信息仅是在实时恢复一个未被扰码的内容时所需的。

最后，通过从安全的 control_files 文件服务器的日志文件中经过统计收集，可以对已经生效的使用进行跟踪和上报。

B.10.1.3 潜在用户，实现模型及动机

本节所描述系统的潜在用户是内容的创建者，拥有者和提供商，因为本系统可以确保一旦内容被保护，并携带在 Lured_jp2file 中，则仅有授权用户和被允许的用户才能够访问到原始内容。需要强调的很重要一点是仅有 99%的原始内容是可以免费提供的，而需要访问的原始内容的 1%只有在通过了认证和权限管理协议之后才能够被分发。

B.10.2 技术概述

图 B.9 显示了本系统的概述。

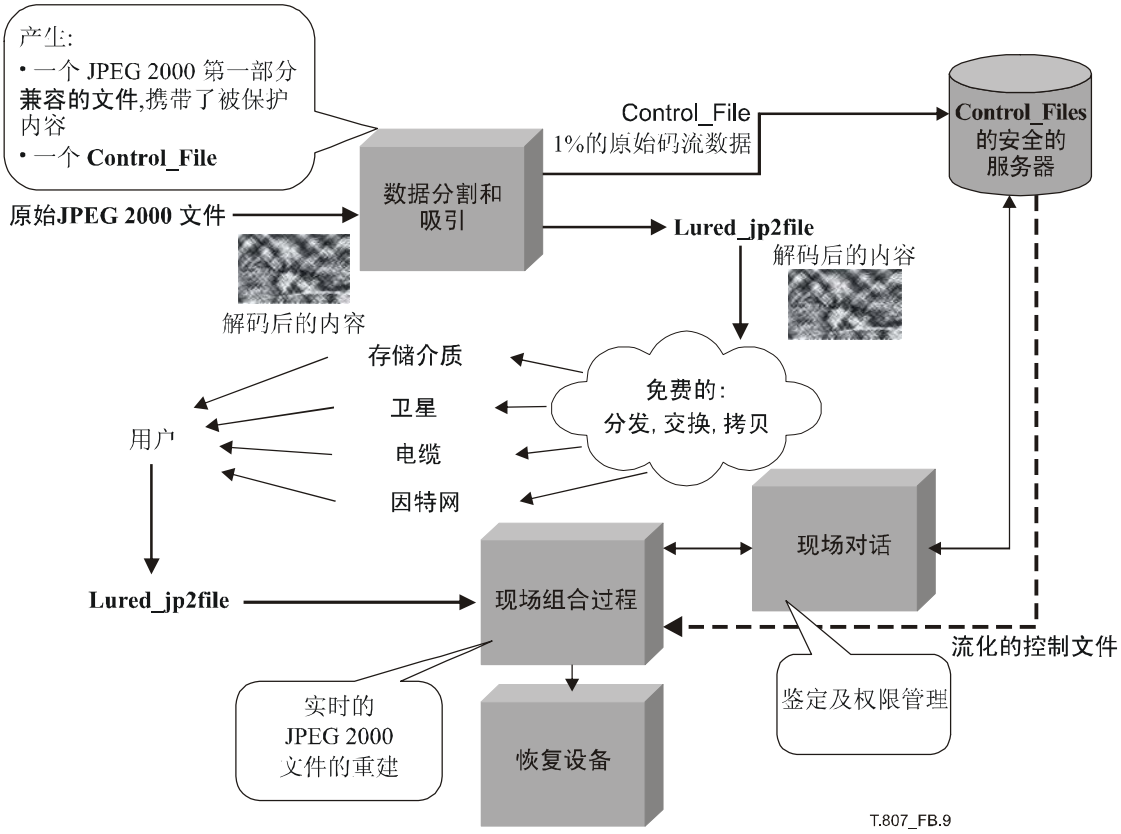


图 B.9－系统概述

一个输入的 JPEG 2000 文件通过一个名为*数据分割和吸引*的操作，被分割为两个新的文件。于是有两个新的文件生成：一个是 *Lured_jp2file*，携带了被保护的内容（JPSEC 内容），另一个是 *Control_File*。

通过数据分割和吸引过程，原始JPEG 2000文件中的某些部分被提取出来，并被诱饵所替换。一个Lured_jp2file携带大约有 99%的原始内容，而剩下的 1％是虚拟数据，被称为诱饵，即这种数据与原始数据之间没有任何一个预先的 已知的链接。不同于传统的加密，吸引过程不是基于密钥的。一个Lured_jp2file可以被任何用户免费地分发、交换或拷贝。Control_File中包含了从原始文件中抽取出的1%的原始数据。它被存储在一个 *Control_Files* 的安全的服务器 中。

当Lured_jp2file被任何一个遵循 JPEG 2000第一部分的解码器解码时，这些内容在视觉上显示是被扰码的。要访问到原始内容的唯一方法是根据 Control_File 来恢复抽取出的原始数据。现场组合 设备通过现场对话（*Live_Dialog*）协议与Control_Files的安全服务器相连，并且存在一个鉴定和权限管理协议：

— 如果用户拥有权限或同意内容访问的条件（例如付费或定购），则可以从Control_File中获取到抽取出的数据，因此可以实时地恢复原始的JPEG 2000文件。然而，根据用户的权限，对原始JPEG 2000的重建可能是部分的（例如仅允许对特定的拼贴，和/或色彩分量，和/或分辨率，和/或选区，和/或质量层等进行访问）或全部的；

— 如果用户不拥有权限或不接受条件，则仅显示被扰码后的内容。

所描述系统的主要特性为：

— 将原始的JPEG 2000文件分割 为两个文件，第一个文件携带了被保护的JPEG 2000的内容，其中仅有99％的原始数据，再加上1％的被称为诱饵的虚拟数据（Lured_jp2file），第二个文件存储了在重建原始的JPEG 2000内容时所需的某些原始信息数据（1％）；

— 内容在视觉上是被扰码的；

— 遵循JPEG 2000第一部分，且文件长度被保留；

— 具有低比特率和低计算成本 的保护系统。

所描述系统可与任何环境和/或操作系统一起使用。没有特殊的硬件和软件需求。

吸引过程将下列 SEC 标记插入到 Lured_jp2file 中：

表 B.26－本工具参数的取值

参　数				长度（比特）	取值（按顺序）	导出含义
SEC				16	0xFF65	SEC 标记
L_{SEC}				16	0xXXXX	SEC 标记段的长度
Z_{SEC}				8	1 ... 255	本标记段的索引
P_{SEC} (if Z_{SEC} = 1)	F_{INSEC}			1	0	没有使用 INSEC
	$F_{multiSEC}$			1	0	使用了一个 SEC 标记段
	F_{J2K}			2	1	JPSEC 流遵循 JPEG 2000 第一部分
	F_{TRLCP}			1	0	本字段中没有定义 TRLCP 标签的用法
	N_{tools}			7	1	在码流中使用了一个安全工具
	I_{max}			7	1	已经使用的最大的工具实例索引
	Padding			5	0	填充
$Tool^{(0)}$	t			8 (RBAS)	1	非标准的保护工具
	i			8 (RBAS)	0	工具实例索引
	ID_{RA}	$ID_{RA,id}$		32	ID	使用 RA 交付 ID 序号
		$ID_{RA,nsl}$		8 (RBAS)	21	$ID_{RA,ns}$ 的长度为 21 个字节
		$ID_{RA,ns}$		168	命名空间	本工具注册的 RA 的命名空间
	L_{ZOI}			16	长度值	L_{ZOI} + ZOI 的长度
	ZOI	NZ_{ZOI}		8	0...254	区域的个数
		$Zone^0$	DC_{ZOI}	1	0	后面没有跟随字节对齐段
				1	1	与非图像相关的描述类
				6	000010	指定了包索引
			$Pzoi^{0,0}$ Mzoi	1	0	后面没有跟随字节对齐段
				1	0	指定的区域是受保护方法影响的区域
				1	1	指定了多个项
				2	10	索引模式
				2	xx	Izoi 使用 8 比特或 16 比特或 32 比特的整数
				1	0	Izoi 使用一个维度来描述
			Nzoi	8	可变的	2 ... 255（包索引的编号）
			$Izoi^i$	xxx Nzoi	可变的	包索引
	L_{PID}			16	0 ... (2^{16} – 1)	L_{PID} + P_{ID} 的长度，以字节计数
	P_{ID}			可变的	可变的	Control_File 的 ID，Control_File 服务器的 URL 等；由 RA 提供的完整的语法

执行数据分割和吸引，和/或现场组合过程所需的工具，可以通过与注册机构相连接，并从注册机构处进行下载而获得。

B.11　安全的可扩展流化和安全的代码转换

B.11.1　摘要和动机

本节描述了一种方法，提供了用于 JPEG 2000 码流的机密性和认证保护服务，采取方式为：

1）　允许一个（潜在的不可信赖的）实体对JPSEC保护流进行安全的代码转换或适配，而不要求该实体对内容进行解保护或解密；以及

2）　允许一个客户验证代码转换操作是以一种合法的和许可的方式执行的。

通常代码转换是用来为客户适配 JPEG 2000 编码后的内容，而不同的客户具备各种不同的设备能力（例如小的显示尺寸或低比特率的网络连接等），并处于各种随时间变化的网络条件中。JPEG 2000 由于其内在的可扩展特性，尤其适用于代码转换应用。然而，如果在保护 JPEG 2000 码流时不小心，就可能会丢失可扩展特性。例如，当完整的码流被加密为一个单独的文件时就会发生这种情况。在这种情况下，对被保护码流进行代码转换的唯一方法是首先进行解密，然后对解密后的流进行代码转换和适配。由于代码转换器必须对内容解密，这就破坏了系统的端到端安全性。

设计 JPSEC 是为了能够对 JPSEC 的被保护内容进行安全的代码转换，在这里安全的代码转换被定义为“不需要对内容进行解保护（解密）的代码转换”。这是通过安全的可扩展的流化而获得的，这种流化组合了可扩展的编码，加密和信号化，且采取的方式是允许一个（潜在的不可靠的）服务器或中间网络节点或代理进行低复杂度的和安全的代码转换。这就使得 JPSEC 具有一种表面看起来是互相矛盾的特性，即中间网络的代码转换和端到端的安全性。例如，在图 B.10 中，媒质在发送者处加密，且仅在接收者处解密，而在所有的点上都保持被加密，包括：（左边）一个中间网络节点为每个 JPSEC 客户，都对被保护内容进行了安全的代码转换，（右边）一个不可靠的服务器进行了安全的代码转换，并在没有保护的情况下将 JPSEC 内容流化。

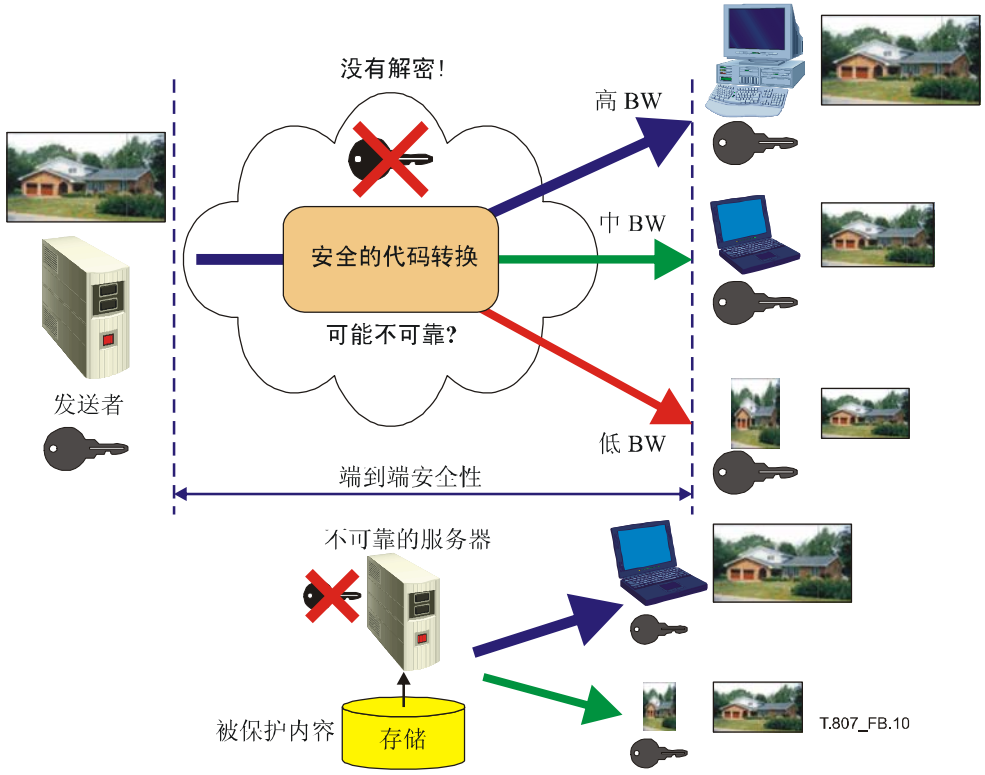


图 B.10－JPSEC具备端到端安全和中间网络的安全的代码转换

B.11.2 操作描述和两个示例用法

在第一个示例中，原始的 JPEG 2000 码流按照 RLCP 排序，并且目标是使用加密和认证来保护此码流，同时可以由分辨率在被保护码流上进行安全的代码转换。由于原始的 JPEG 2000 码流使用一种 RLCP 排序，因此每个分辨率分量都由一个毗邻的数据段来表示。可以对三个毗邻数据段中的每一个都执行加密。然后，JPSEC 头部指定了三个影响区，分别描述了用于每个段的分辨率分量、码流段和加密模板。认证也可以在三个数据段的每一个上面执行，或者在加密之前或者加密之后，依赖于所期望的功能性。这一点同时也在 SEC 头部中使用认证模板进行了规定。

为了在 JPSEC 码流上执行安全的代码转换，一个代码转换器简单地读取并解析 SEC 头部，标识了分辨率段的所在位置，然后保留或移除适当的数据段/分辨率。需要注意的是这种代码转换操作对应于一种简单的解析操作，且它不要求对数据进行解保护。认证是通过使用 MAC 值，对接收到的代码转换后的数据进行鉴别而完成的，其中，MAC 值是在 JPSEC 保护过程中被置于 SEC 头部的。

在第二个示例中，期望的目标仍然是允许由分辨率进行代码转换，从而保护码流；然而，本例更复杂一些是在于原始的 JPEG 2000 码流按照的是 PCRL 排序而不是 RLCP 排序，因此相对应于三个分辨率分量的数据段在原始码流中并不是相邻的。JPSEC 允许所期望的由分辨率执行的安全代码转换和缩放目标可以通过多种途径来实现。一种方法是对单个包进行加密，而留下包的头部不加密。这种方法保留了流的最高级别的可扩展性，但也需要最复杂的安全代码转换操作，因为代码转换器必须在包级别解析 JPSEC 流。另一个可以带来最简单的安全代码转换操作的极端方法是对数据重新排序，这样分辨率分量就可重新处于相邻的段中了，而且这些段的偏移量已经在 SEC 头部中标示出了。这可以以遵循 JPEG 2000 的方式得到，即通过对 JPEG 2000 的包重新排序，由 PCRL 排序改为 RLCP 排序，并且在 COD 标记段中标示出新的进展顺序，或者给出进展顺序改变（POC）标记段。由此发生的数据重新排序和保护转换在图 B.11 中所示。同样的，在主 SEC 头部中包含了 ZOI 参数，这些参数描述了与每个数据段相关联的与图像相关的参数和与比特流相关的参数，但是这次针对的是重新排序后的 JPEG 2000 码流。

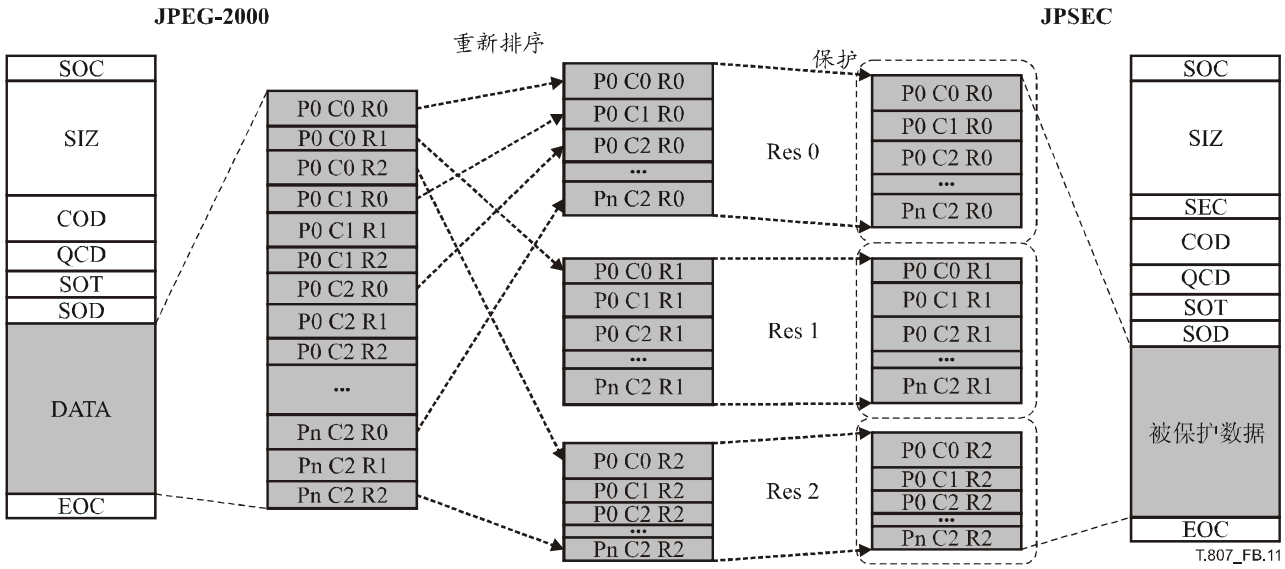


图 B.11－构造一个JPSEC码流的示例

B.11.3 码流语法

JPSEC 语法与模板保护工具一起，可被用于创建一个安全的可扩展的流化和安全的代码转换系统。特别地，影响区（ZOI）与解密模板、处理域以及粒度一起，可被用于完整地定义解密过程，被允许的 JPSEC 消费者应当使用此解密过程来对流进行解密。此外，ZOI 参数标示了代码转换节点可用来执行安全的代码转换的那些信息。

ZOI 规定了三个区域，每个表示一个分辨率，并为每个区规定了与加密后的比特有关的字节范围。解密保护模板、处理域，以及粒度的信号化语法在表 B.27 中所示。解密方法由解密保护模板来标示。在这种情况下，它指定了在 CTR 模式下以 AES 加密，并指定了块长度和密钥长度。处理域和粒度更进一步规定了解密是如何执行的。它标示了处理域为比特流本身，且包头部和包体都要被加密。通过改变处理域和粒度，可以指定不同的解密方法。例如，加密粒度可以或者为单个的包，或者仅为包体。此外，认证方法可以使用如上所述的同一个 ZOI 来规定，但具有跟随其后的认证模板。认证模板的语法在表 B.28 中显示，使用了 SHA-1 的 HMAC 来进行认证。当然，也可能会使用其他的 JPSEC 密码和 MAC。另外，所提议的解决方案也可能与其他数字签名、访问控制和密钥管理工具等一起使用。此外，使用失真字段（见 5.7.3.2）可以将每个包（或其他数据区域）与一个失真关联起来，用以实现速率-失真（R-D）优化后的安全的流化和安全的代码转换[26]，[27]和[28]。

表 B.27－模板保护工具，处理域和粒度参数的取值

参　数			长度（比特）	取值（按顺序）	导出含义
T_{decry}	ME_{decry}		8	0	标记段标签为空
	CT_{decry}		16	1	AES 加密
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	CTR，且无填充
		P_{bc}	2	0	CTR 模式没有使用填充
		SIZ_{bc}	8	128	块长度为 128 个比特
		KT_{bc}	可变的	密钥模板	密钥信息模板
PD			1	0_b	后面没有跟随字节对齐段（BAS）
			1	0_b	不是在像素域
			1	0_b	不是在小波系数域
			1	0_b	不是在量化的小波系数域
			1	1_b	在码流域处理
			3	000_b	未使用
G		PO	16	$0\ 0000\ 0101\ 0011\ 100_b$	处理顺序为 TRLCP
		GL	8	$0000\ 1001_b$	粒度为 ZOI 所指定的全部区域
V		N_V	16	1	指定了一个值
		Sv	8	16	长度为 16 个字节
		VL	128	当前值	CTR 模式的计数值

表 B.28－认证模板保护工具参数的取值

参　数			长度（比特）	取值（按顺序）	导出含义
T_{auth}	M_{auth}		8	0	基于哈希的 MAC
	P_{auth}	M_{HMAC}	8	1	HMAC
		H_{HMAC}	8	1	哈希 ID 为 SHA-1
		KT_{HMAC}	可变的	密钥值	见密钥模板
		SIZ_{HMAC}	16	80	MAC 长度为 80 个比特（从 160 删节而来）

B.11.4 结论

本节描述了对 JPSEC 的安全可扩展的流化和安全的代码转换，这会带来表面上看起来互相矛盾的两个特性：即端到端的安全性和在中间网络节点上的安全的代码转换。这就允许 JPSEC 码流不需要解密 就可以进行代码转换。此外，本方法还提供了一种认证，以验证代码转换是以一种合法的允许的方式执行的，且没有发生由错误或攻击者而引起的故意或恶意修改。这就允许一个（潜在的不可靠的）服务器或中间网络节点如代理，来执行安全的代码转换，同时允许一个 JPSEC 消费者来验证所接收到的内容是以一种合法的允许的方式进行代码转换的。

附 件 C

互操作性

（本附件是本建议书 | 国际标准的组成部分）

C.1 第1部分

有许多保护方法都可以应用在一个 JPEG 2000 码流上，来创建严格遵循 JPEG 2000 第一部分的 JPSEC 码流。我们使用术语“遵循第一部分”来指那些 JPSEC 码流，即这些码流为了 JPEG 2000 第一部分的解码器具有严格定义的行为，甚至包括那些不关注 JPSEC 的解码器。

一个遵循 JPEG 2000 第一部分的解码器将跳过那些它不能识别的标记段。一个 JPSEC 工具，如用于认证的 JPSEC 标准工具，将根据 JPEG 2000 数据计算而来的消息认证码插入到 SEC 标记段中，随同一起的还有一些参数，这些参数描述了 JPSEC 消费者可以使用的特定的认证方法。这些参数及其值告诉 JPSEC 消费者如何去验证所接收到的 JPSEC 码流是可信的。需要注意的是，JPSEC 认证工具不会操纵 JPEG 2000 数据。因此，一个接收到此 JPSEC 码流的遵循 JPEG 2000 第一部分的解码器将开始对 JPSEC 码流进行解码，然后它将跳过 SEC 标记段，并继续对 JPSEC 码流进行解码，就好像它是一个遵循 JPEG 2000 第一部分的流。用于认证的 JPSEC 标准工具共享这些特性，并且由此形成的结果也是一个遵循第一部分的码流。

JPSEC 允许对 JPEG 2000 和 JPSEC 码流执行加密和解密。当使用了加密时，JPEG 2000 数据当然是被修改了。严格来说，要加密后的流遵循第一部分是不可能的，因为它极有可能使得 JPEG 2000 第一部分的解码器看到了非法的值。克服此问题或至少减轻此问题的一个可能方法是使用 JPEG 2000 的容错能力。由于具有容错能力，则有可能具有加密后的 JPSEC 码流，而该码流为了 JPEG 2000 第一部分的解码器具有明确的行为。

JPSEC 具有的 P_{sec} 参数字段包含了用于整个码流的安全参数。这包括一个标记 F_{J2K}，该标记可能被设置为 1，来指示一个可被 JPEG 2000 第一部分的解码器进行解码的 JPSEC 码流。当 JPSEC 创建者将 JPSEC 工具应用到 JPEG 2000 码流上时，JPSEC 创建者可能会设置此值。需要指出的是一个 JPSEC 创建者可以接收一个被保护的 JPSEC 码流作为输入。如果某个 JPSEC 创建者接收到一个输入的 JPSEC 码流，且该码流的 F_{J2K} 标记被设置为指示了“遵循第一部分”，然后该创建者应用了一个不遵循第一部分的 JPSEC 工具，则它必须设置 F_{J2K} 标记为 0。

对于一个不遵循第一部分的 JPSEC 流，推荐使用一个文件扩展名.jp2 来指示可能不能使用一个 JPEG 2000 第一部分的解码器来对此被保护码流进行解码。

C.2 第2部分

JPEG 2000 第二部分修正案 2 中的关于扩展的能力标记段（CAP）可被用于指示使用了 JPSEC。特别地，第二部分使用参数 R_{siz} 来指示存在一个 CAP 标记段，该标记段包含一个参数 C_{cap}，可用于标示在码流中使用了哪些 JPEG 2000 部分。可以通过在 C_{cap} 中设置一个适当的比特来指示使用了 JPEG 2000 第八部分（JPSEC）。

因此，一个 JPSEC 创建者可能会设置 R_{siz} 参数来指示存在一个 CAP 标记段。它可能会通过插入或编辑此 CAP 标记段，来设置 C_{cap} 参数，用以指示使用了第八部分。

C.3 JPIP

C.3.1 JPIP和JPSEC之间的概要关系

JPIP 规定了一个协议，该协议由客户和服务器之间的结构化的系列交互所组成，使用的方法是规定哪个图像文件元数据，结构，以及部分或全部图像码流可能以某种有效的通信方式被交互。

JPIP 可以通过对 JPEG 2000 文件格式的各种不同扩展而进行裁减，正如在 ITU-T T.801 建议书 | ISO/IEC 15444-2，ITU-T T.802 建议书 | ISO/IEC 15444-3 和 ITU-T T.805 建议书 | ISO/IEC 15444-6 中定义的那样。然而，如果要获得一个简单级别的交互，只要允许一个单独的 JPEG 2000 文件或码流的一部分被传送即可，而这些其他的能力都不是必须的。

已经包含了对 JPIP 协议进行扩展的规定，用以支持目前的 JPEG 2000 标准，如 ITU-T T.802 建议书 | ISO/IEC 15444-3：运动的 JPEG 2000，和 ITU-T T.805 建议书 | ISO/IEC 15444-6，组合文档以及 JPEG 2000 的未来部分（目前有 JP3D，JPSEC 和 JPWL）。

JPSEC 为 JPEG 2000 图像提供了安全服务。JPSEC 语法支持两种类型的标记：SEC 和 INSEC。在 JPSEC 比特流的主头部中会出现一个或多个 SEC 标记。换句话说，JPSEC 处理了一个 JPEG 2000 码流，修改了 JPEG 2000 的主头部来构造一个新的 JPSEC“主头部”，并且如果适用的话会修改相应的 JPEG 2000 数据流来构造一个新的被保护数据流。INSEC 标记可能可选地出现在数据流的“数据”部分。与 SEC 标记相比，它指定了一些“更小尺寸的”或“本地区域的”参数，可被用作 SEC 标记的补充。

据观察，JPIP 正好在传输层之外，而 JPSEC 处于应用层。从这个观点来看，JPIP 为 JPSEC 提供了一种传输服务。也就是说，JPIP 提供了有效的工具在服务器和客户之间传递图像信息，包括主头部（所有的标记）和码流。本节关注于 JPIP 是如何被用于传输 JPSEC 内容的。

C.3.2 关于JPIP和JPSEC之间相互作用的特定问题

本节描述了一个 JPIP 发送者和一个接收者在传输 JPSEC 内容时必须要考虑的一些问题。

在 ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.5 节“主头部数据保管箱”中，JPP-和 JPT-流媒体类型都使用了主头部的数据保管箱。此数据保管箱由一个级联列表组成，该列表中包含了主头部中的所有标记和标记段，起始于 SOC 标记。它不包括 SOT，SOD 或 EOC 标记。然而，JPEG 2000 的主头部不包含 SEC 标记及其所在段。作为结果，JPIP FCD 2.0 的第 A.3.5 节中并没有指定要支持 JPSEC 中规定的 SEC 标记段。因此，必须修改 JPIP 发送者和接收者，使其能够识别可能出现在某个 JPSEC 码流主头部中的 SEC 标记段。

在 ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.2 节“选区数据保管箱”中，描述了对选区数据的支持。然而，JPIP FCD 2.0 的第 A.3.2 节中并没有指定它是否支持 JPSEC 中规定的 INSEC 标记及其所在段。因此，必须修改 JPIP 发送者和接收者，使其能够识别可能出现在某个 JPSEC 码流的数据部分中的 INSEC 标记段。

在 ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.3 节“拼贴头部数据保管箱”中，拼贴头部数据保管箱仅出现在 JPP-流媒体类型中。对于属于此类的数据保管箱，类内的标识符拥有拼贴的索引（起始于 0），该索引由数据保管箱所引用。此数据保管箱由用于拼贴 n 的标记和标记段组成。它不应当包含一个 SOT 标记段。是否包含 SOD 标记是可选的。此数据保管箱可能从一个合法的码流构造而成，其方法是将用于拼贴 n 的所有拼贴部分的头部中，除 SOT 和 POC 之外的所有标记段都级联起来。

在 ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.4 节“拼贴数据保管箱”中，拼贴数据保管箱应当仅与 JPT-流媒体类型一起使用。对于属于此类的数据保管箱，类内的标识符为数据保管箱所属的拼贴的索引（起始为 0）。每个拼贴数据保管箱都对应于一个字节串，该串由属于此拼贴的所有拼贴部分按顺序级联而构成，并包含它们的 SOT、SOD 以及所有其他相关的标记段。

正如上面所述，ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.4 节和第 A.3.5 节，描述了对拼贴部分头部和拼贴部分数据的支持。然而，ITU-T T.808 建议书 | ISO/IEC 15444-9 的第 A.3.4 节和第 A.3.5 节并没有指定它们是否支持 SEC 标记段和 INSEC 标记段。因此，必须修改 JPIP 发送者和接收者，使其能够识别并传输这些跟随被保护数据的标记段。

C.3.3 总结

通常来说，JPSEC 使其自身是适用于被 JPIP 所传输的。INSEC 标记用于码流中，来描述被某个或某些安全工具保护的一些“小的”特定的数据部分。它使得 JPSEC 更加灵活。为了让 INSEC 更鲁棒，服务层（目前我们指的是 JPIP）应当为 INSEC 及其所在段提供良好的服务质量或保护质量。为了达到此目标，JPIP 和 JPSEC 需要共同解决某些问题，并确保 JPIP 和 JPSEC 之间的相互作用。

C.4 JPWL

无线 JPEG 2000 或 JPWL（ITU-T T.810 建议书 | ISO/IEC 15444-11）扩展了 JPEG 2000 规范的基线，以便完成在某种有错误倾向的传输环境中对 JPEG 2000 图像进行有效的传输。更精确地说，JPWL 定义了一系列的工具和方法来保护码流不受传输错误的影响。它还定义了用于描述码流对传输错误敏感度的方法，以及描述驻留的传输错误在码流中所处位置的方法。

JPWL 明确地提出了对图像头部，前向纠错码（FEC）， 不平等差错保护（UEP），联合信源信道编码，数据分割和交织，以及鲁棒的算术编码等的保护。JPWL 没有与某个特定的网络或传输协议相链接，而是为 JPEG 2000 图像在有错误倾向的网络中进行鲁棒的传输提供了一种通用的解决方案。

JPWL 的主要功能性包括：

- 保护码流不受传输错误的影响；
- 描述码流的不同部分对传输错误敏感性的程度；
- 描述驻留的错误在码流中的位置。

JPWL 定义了四个标记段：错误保护能力（EPC），错误保护块（EPB），错误敏感度描述符（ESD），以及驻留错误描述符（RED）。

EPC 标记段指示在码流中使用了哪些 JPWL 标准工具和非正式工具。更精确地说，EPC 标示了 JPWL 所定义的其他三个标准的标记段，即错误敏感度描述符（ESD），驻留错误描述符（RED），以及错误保护块（EPB）是否出现在码流中。此外，EPC 还标示了非正式工具的使用，这些非正式工具之前已经注册在 JPWL RA 中。EPC 在 JPWL 码流中是必选的。

EPB 的主要功能是保护主头部和拼贴部分的头部。然而，它也还可以被用于保护码流的剩余部分。EPB 标记段中包含了用于保护码流的错误保护参数和冗余数据的相关信息。

ESD 标记段包含了码流对错误的敏感度的相关信息。当应用不平等差错保护（UEP）技术时，可以用到这些信息。简单直接地说，将使用更强大的代码来保护码流的最敏感部分。这些信息还可被用于进行选择性重传。最后，ESD 中携带的信息还可被用于其他非 JPWL 的应用，如高速率代码转换，或智能预取。

RED 标记段标示了驻留错误在码流中的存在。实际上，一个 JPWL 解码器可能不能纠正码流中的所有错误。而 RED 允许标示出这些驻留错误的所在位置。因此，为了更好地处理错误，该信息可能由某个 JPEG 2000 解码器所使用。例如，解码器可以请求重传、隐藏错误或者丢弃已被破坏的信息。

C.4.1 JPWL和JPSEC之间的概要关系

当 JPEG 2000 图像需要通过一个有错误倾向的无线信道进行保护和传输时，则需要结合 JPWL 和 JPSEC。

在发送侧，JPWL 错误敏感度典型地是在 JPEG 2000 编码时产生的。于是为了保护码流，JPSEC 工具被应用在码流上。最后，使用 JPWL 编码工具使得码流对于传输错误更加鲁棒。

在接收侧，首先应用 JPWL 解码工具来纠正可能的传输错误。在这一步骤中，JPWL 可能也会产生驻留的错误信息。最后，为了实现所选择的安全服务，应用了 JPSEC 工具。

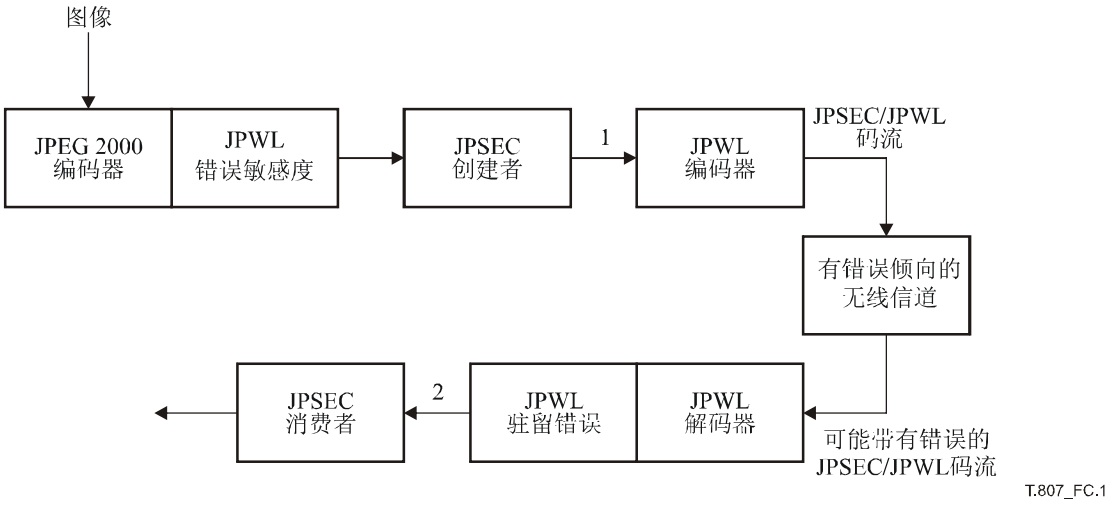


图 C.1－典型的JPWL和JPSEC的结合

C.4.2 关于JPWL和JPSEC之间互操作性的特定问题

在 JPWL 和 JPSEC 的互操作性方面，还必须要考虑许多问题，如下面所详细论述的：

1） JPWL错误保护能力（EPC）：此标记段的出现将影响字节范围。注意，此标记段在JPWL码流中是必选的。

2） JPWL错误保护块（EPB）：此标记段典型来说是作为最后一个步骤加入到发送者处的，而在接收侧，又是第一个被去除的。从原则上来说，它不应当影响JPSEC。

3） JPWL错误灵敏度描述符（ESD）：此标记段典型来说是在JPEG 2000第一部分编码时加入的，在这种情况下，它对后续的JPSEC操作应当是透明的。然而，JPSEC能够逆向地影响ESD在JPWL中的使用。特别地，只要ESD使用了字节范围，则JPSEC就不应当修改字节范围。此外，JPSEC操作不应当影响失真值；否则，ESD所携带的信息就会变得不相关。在后一种情况下，JPSEC创建者可以选择将ESD标记段去除。

4） JPWL驻留错误描述符（RED）：在JPWL解码之后，可以插入此标记段。因此，它可能会影响JPSEC字节范围。它可能还会对JPSEC认证技术产生影响。对于一个被破坏的码流来说，RED信息对于一个JPSEC消费者正确地处理此码流是有用的。

5） JPSEC SEC：此标记段的出现将会影响字节范围。注意，此标记段在一个JPSEC码流中是必选的。

6） JPSEC INSEC：此标记段的出现将会影响字节范围。注意此标记段出现在码流数据中。

在没有驻留错误的情况下，理想地说，JPWL 编码器和解码器应当是透明的。换句话说，在这种情况下，上图中处于点 1 和点 2 的流应当是严格相同的。

作为一个通用的建议，当与 JPWL 一起使用时，为了最小化与字节范围之间的问题，推荐 JPSEC 使用的字节范围要起始于 SOD 标记之后。另外，建议要限制 JPWL 标记段在主头部中的出现，并避免它们在拼贴部分头部中的出现。

附 件 D

专 利 声 明

（本附件不是本建议书 | 国际标准的组成部分）

注 — 附件D仅仅是一个ISO/IEC附件。向ITU递交了关于此文本的专利声明的公司列在IPR数据库中。见http://itu.int/ITU-T/ipr/。

国际标准化组织（ISO）和国际电工委员会（IEC）提请注意一个已经声明的事实，即遵循 ISO/IEC 15444 的本部分可能会包含有专利的使用。

ISO 和 IEC 对有关这些专利权的证据、有效性和范围不表示意见。

这些专利权的所有者已经向 ISO 和 IEC 保证他们将愿意在合理的和不歧视的条款和条件下，与世界范围内的申请者进行许可权的协商。在这一方面，这些专利权所有者的声明已经在 ISO 和 IEC 注册。相关信息可以从下面所列的公司处获得。

需要提前注意这种可能性，即 ISO/IEC 15444 本部分中的某些元素可能还受本附件所标识的专利权之外的那些专利权的影响。ISO 和 IEC 不对标识任何或全部这些专利权负有责任。

表 D.1－声明列表

序　　号	递交的实体
1	Canon Inc（佳能公司）
2	Columbia University（哥伦比亚大学）
3	EMITALL Surveillance
4	HP（惠普）
5	Institute for Infocomm Research（信息通信研究学院）
6	MediaLive
7	New Jersey Institute of Technology（新泽西技术学院）

参考资料

[1] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*
ISO/IEC 7498-2:1989, *Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[2] ISO/IEC 9796-2:2002, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*.

[3] ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

[4] ISO/IEC 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General*.

[5] ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*.

[6] ISO/IEC 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher*.

[7] ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

[8] ISO/IEC 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*.

[9] ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework.*

[10] ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*.

[11] ISO/IEC 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.

[12] ISO/IEC 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/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*.

[14] ISO/IEC 14888-1:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*

[15] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

[16] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 2 – Digital signatures*.

[17] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 3 – Key establishment*.

[18] ISO/IEC 15946-4:2004, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 4 – Digital signatures giving message recovery*.

[19] ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.

[20] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[21] ISO/IEC 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 July-3 August, 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)*, March 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 Sept. 2001.

[28] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming and Secure Transcoding with JPEG 2000, *IEEE Inter. Conf. on Image Processing (ICIP)*, Sept. 2003. http://lib.hpl.hp.com/techpubs/2003/ HPL-2003-117.html.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	**远程信息处理业务的终端设备**
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2007年，日内瓦