الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

T.807

(2006/05)

السلسلة T: المطاريف الخاصة بالشبكة التلماتية

تكنولوجيا المعلومات – نظام تشفير الصور JPEG 2000: توفير أمن النظام JPEG 2000

التوصيـــة ITU-T T.807

الاتحاد الدولي للاتصالات ITU

المعيار الدولي ISO/IEC 15444-8
التوصيـــة ITU-T T.807

تكنولوجيا المعلومات – نظام تشفير الصور JPEG 2000:
توفير أمن النظام JPEC 2000

ملخص

تهدف هذه التوصية | المعيار الدولي إلى توفير قواعد تتيح تطبيق خدمات الأمن على بيانات الصورة المشفرة بالنظام JPEG 2000. وتشمل خدمات الأمن هذه السرية والتحقق من التكاملية واستيقان المصدر والنفاذ الشرطي والتسيير المنتظم الأمين وتحويل الشفرة الأمين. وتتيح قواعد التركيب تطبيق خدمات الأمن هذه على بيانات صور مشفرة أو غير مشفرة كاملة أو جزئية. وذلك يحافظ على العناصرالداخلية للبيانات JPEG 2000 مثل قابلية القياس والنفاذ إلى مختلف الأمكنة وسويات الاستبانة والمكونات اللونية وطبقات النوعية مع توفير خدمات الأمن لهذه العناصر.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 29 مايو 2006 على التوصية ITU-T T.807 بموجب الإجراء المحدد في التوصية ITU-T A.8. ونُشِر أيضاً نص مماثل في المعيار ISO/IEC 15444-8.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) على الموقع http://www.itu.int/ITU-T/ipr/.

المحتـــويات

الصفحة

مقدّمة

تقدم شبكة الإنترنت في "العصر الرقمي" لأصحاب الحق فرصاً عديدة جديدة لتوزيع أعمالهم (من كتب وأفلام وموسيقى وصور وغيرها) توزيعاً إلكترونياً.

وفي الوقت ذاته، تيسر تكنولوجيا المعلومات الجديدة بطريقة جذرية وصول المستعملين إلى المحتويات. ويقترن ذلك بالمشكلة المستفحلة التي تتمثل بقرصنة النسخ الرقمية، المماثلة بجودتها للنسخ الأصلية. وبمشكلة "تقاسم الملفات" في الشبكات من نظير إلى نظير، مما يسفر عن الشكاوى المستمرة بشأن الخسائر الفادحة التي تتكبدها صناعة المحتويات.

وللمنظمة العالمية للملكية الفكرية (WIPO) وبلدانها الأعضاء (170) دور حاسم في ضمان استمرار صون حق المؤلف وأشكال التعبير الثقافي والفكري الذي يولده في القرن الحادي والعشرين.

والاقتصاد الرقمي الجديد والمبدعون في كل بلد من بلدان العالم يعتمد على هذا الحق. وقد أبرمت معاهدة الويبو بشأن حق المؤلف (WTC) في ديسمبر 1996 متضمنةً مادتين هامتين (11 و12) بشأن التدابير التكنولوجية والالتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق:

المادة 11
الالتزامات المتعلقة بالتدابير التكنولوجية

على الأطراف المتعاقدة أن تنص في قوانينها على حماية مناسبة وعلى جزاءات فعالة ضد التحايل على التدابير التكنولوجية الفعالة التي يستعملها المؤلفون لدى ممارسة حقوقهم بناء على هذه المعاهدة أو اتفاقية برن والتي تمنع من مباشرة أعمال لم يصرح بها المؤلفون المعنيون أو لم يسمح بها القانون، فيما يتعلق بمصنفاتهم.

المادة 12
الالتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق

(1) على الأطراف المتعاقدة أن تنص في قوانينها على جزاءات مناسبة وفعالة توقع على أي شخص يباشر عن علم أيًا من الأعمال التالية، أو لديه أسباب كافية ليعلم – بالنسبة إلى الجزاءات المدنية – أن تلك الأعمال تحمل على ارتكاب تعدّ على أي حق من الحقوق التي تشملها هذه المعاهدة أو اتفاقية برن أو تمكّن من ذلك أو تسهّل ذلك أو تخفيه:

"1" أن يحذف أو يغير، دون إذن، أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق؛

"2" وأن يوزع أو يستورد لأغراض التوزيع أو يذيع أو ينقل إلى الجمهور، دون إذن، مصنفات أو نسخاً عن مصنفات مع علمه بأنه قد حذفت منها أو غيرت فيها، دون إذن، معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.

(2) يقصد بعبارة "المعلومات الضرورية لإدارة الحقوق"، كما وردت في هذه المادة، المعلومات التي تسمح بتعريف المصنف ومؤلف المصنف ومالك أي حق في المصنف، أو المعلومات المتعلقة بشروط الانتفاع بالمصنف، وأي أرقام أو شفرات ترمز إلى تلك المعلومات، متى كان أي عنصر من تلك المعلومات مقترناً بنسبة عن المصنف أو ظاهراً لدى نقل المنصف إلى الجمهور.

وتشكل هذه المعاهدة أساساً متيناً لحماية الملكية الفكرية. ومنذ عام 2004، صدقت قرابة خمسون بلداً على هذه المعاهدة الهامة. وبناءً على ذلك يفترض أن تضمن الأدوات وطرق الحماية التي يوصي بها المعيار JPEG 2000 أمن المعاملات وحماية المحتويات (IPR) وحماية التكنولوجيات.

وتعد قضايا الأمن من قبيل الاستيقان وتكاملية البيانات وحماية حق المؤلف والملكية الفكرية والخصوصية والنفاذ المشروط والسرية وتتبع المعاملات على سبيل المثال لا الحصر، من بين القضايا الهامة في الكثير من تطبيقات التصويري التي يستهدفها النظام JPEG 2000.

ويمكن وصف الوسائل التكنولوجية لحماية المحتويات الرقمية وتخفيفها من خلال طرق كثيرة مثل العلامات المائية الرقمية والتواقيع الرقمية والتجفير والبيانات الشرحية والاستيقان والتحقق من التكاملية.

والغرض من الجزء 8 من المعيار JPEG 2000 هو توفير الأدوات والحلول المتمثلة في مواصفات تسمح للتطبيقات بتوليد تدفقات مشفرة JPEG 2000 أمينة واستهلاكها وتبادلها. وهو ما يعرف باسم **JPSEC**.

المعيار الدولي ISO/IEC 15444-8
التوصيـــة ITU-T T.807

تكنولوجيا المعلومات – نظام تشفير الصور JPEG 2000:
توفير أمن النظام JPEC 2000

1 مجال التطبيق

تحدد هذه التوصية | المعيار الدولي الأطر والمفاهيم والمنهجية اللازمة لتأمين التدفقات المشفرة JPEG 2000. وينطوي مجال تطبيق هذه التوصية | المعيار الدولي على تعريف ما يلي:

1) قواعد معيارية لتركيب البيانات المشفرة تحتوي على معلومات تتعلق بتفسير بيانات الصورة الأمينة؛
2) عملية معيارية لتسجيل أدوات النظام JPSEG لدى سلطة تسجيل تعطيها معرفات هوية فريدة؛
3) أمثلة معيارية لأدوات النظام JPSEC في حالات استعمال نمطية؛
4) خطوط توجيهية معيارية بشأن كيفية تطبيق خدمات الأمن والبيانات الشرحية المتصلة بها.

ولا يكمن مجال تطبيق هذه التوصية المعيار الدولي في وصف تطبيقات محددة للتصوير الأمين أو في قصر التصوير الأمين على تقنيات محددة وحسب، بل يشمل وضع إطار يتيح توسيعات لاحقة تتناسب مع تطور تقنيات التصوير من الأمين.

2 المراجع المعيارية

تتضمن التوصيات والمعايير الدولية التالية أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية | المعيار الدولي. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمعايير تخضع إلى المراجعة، نحث الأطراف المشاركة في الاتفاقات المستندة إلى هذه التوصية | المعيار الدولي على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. ويحتفظ أعضاء اللجنة الكهرتقنية الدولية والمنظمة الدولية للتقييس بسجلات المعايير الدولية سارية الصلاحية. وتتوفر في مكتب تقييس الاتصالات في الاتحاد الدولي للاتصالات قائمة توصيات القطاع ITU-T السارية الصلاحية:

- التوصية | المعيار الدولي ITU-T T.800 (2002) | ISO/IEC 15444-1:2004، *تكنولوجيا المعلومات – نظام تشفير الصور JPEG 2000: نظام التشفير الأساسي.*
- التوصية | المعيار الدولي ITU-T T.801 (2002) | ISO/IEC 15444-2:2004، *تكنولوجيا المعلومات – نظام تشفير الصور JPEG 2000: توسيعات.*

3 المصطلحات والتعاريف

تستخدم التعاريف التالية لأغراض هذه التوصية. وتنطبق التعاريف الواردة في الفقرة 3 من التوصية | المعيار ITU-T Rec. T.800 | ISO/IEC 15444-1 على هذه التوصية المعيار الدولي.

1.3 **التحكم في النفاذ**: الوقاية من استخدام موارد غير مرخص لها بما في ذلك الوقاية من استخدام موارد بطريقة غير مسموحة.

2.3 **الاستيقان**: عملية التحقق من هوية مزعومة لكيان النظام أو لأغراضه.

1.2.3 **استيقان المورد**: التحقق من أن كيان مورد ما (قول، مستعمل/طرف) هو بالحقيقة كيان المورد المزعوم.

2.2.3 **استيقان الصورة الهش وشبه الهش**: عملية تهدف إلى استيقان مورد الصورة والتحقق من تكامل محتويات الصورة و/أو بيانات الصورة في آن، وينبغي أن تكون قادرة على كشف كل تغيير في الإشارة وتحديد مكانه مع احتمال تحديد ما كانت عليه الإشارة قبل التغيير.

ملاحظة – تستخدم هذه العملية في إثبات صحة وثيقة ما. والفرق بين استيقان الصورة الهش وشبه الهش هو أن الأول يتحقق من تكامل بيانات الصورة والثاني من تكامل محتوى الصورة.

3.3 **السرية**: خاصية تتمثل في عدم تسرب المعلومات أو كشفها إلى أفراد أو كيانات أو عمليات غير مرخص لها.

4.3 **تجزئة البيانات**: طريقة لحماية مواد البيانات من النفاذ غير المسموح إليها من خلال تشفير بيانات الملف وتسجيل مختلف أجزائه في مخدمات بعيدة مختلفة.

ملاحظة – عند النفاذ إلى البيانات المجزأة تستخرج الأجزاء وتجمع ويفك تشفيرها. ويحتاج الشخص غير المرخص له أن يعرف مواقع المخدمات التي تحتوي على الأجزاء وأن يكون قادراً على النفاذ إلى كل منها وعلى تحديد البيانات التي يتوجب جمعها وكيفية فك تشفيرها.

5.3 **فك التشفير، فك التجفير**: تحويل معكوس للتجفير.

6.3 **توقيع رقمي**: بيانات مضافة إلى وحدة بيانات أو تحويل تجفير لهذه الوحدة يتيح لمقصد وحدة البيانات أن يختبر مورد الوحدة وتكاملها وأن يحميها من التزويد من قبل المقصد مثلاً.

7.3 **التجفير**: تحويل قابل للعكس للبيانات باستعمال خوارزمية تشفير تنتج نصاً مشفراً أي إخفاء محتوى معلومات البيانات.

ملاحظة – ثمة مصطلح رديف لخوارزمية التشفير وهو المجفر.

8.3 **البصمات**: خصائص غرض ما لتمييزه عن أغراض مماثلة أخرى بهدف تمكين صاحب الغرض من تتبع المستعملين ذوي الرخصة في حال توزيعهم الممنوع للأغراض.

ملاحظة – في هذا الصدد، تتم عادةً مناقشة البصمات في إطار مشكلة اقتفاء أثر الجريمة.

9.3 **وظيفة التظليل**: دالة تقابل بين سلسلات البتات وسلسلات البتات ذات الطول الثابت مع الوفاء بالخاصتين التاليتين:

ملاحظة – فيما يتعلق بخرج ما، يتعذر حسابياً إيجاد دخل يقابل هذا الخرج. وفيما يتعلق بدخل ما، يتعذر حسابياً إيجاد دخل ثانٍ يقابل نفس الخرج. وتتوقف الجدوى الحسابية على متطلبات الأمن الخاصة بالمستعمل وعلى البيئة.

10.3 **التكاملية**: وهي القدرة على المحافظة على دقة البيانات وتكاملها.

1.10.3 **تكاملية بيانات الصورة**: خاصية تبين عدم تأثر البيانات أو عدم إتلاف أجزائها بطريقة غير مسموح بها.

2.10.3 **تكاملية محتوى الصورة**: ضمان عدم تغيير محتوى الصورة من قبل أطراف غير مرخص لهم على نحو يؤثر على إدراك دلالتها.

ملاحظة – يتيح ذلك إجراء عمليات الحفاظ على محتوى الصورة دون إطلاق إنذار التكاملية.

11.3 **التطبيق JPSEC**: أي عملية صادرة عن برمجية أو عتاد وقادرة على التعامل مع تدفقات مشفرة JPSEC من خلال تفسير قواعد التركيب JPSEC بهدف توفير خدمات الأمن المحددة.

ملاحظة – يستخدم التطبيق JPSEC أداة JPSEC واحدة أو أكثر.

مثال – يكون التطبيق JPSEC قادراً على قراءة التدفقات المشفرة JPSEC وفك تشفيرها إن كانت مرفقة بالمفاتيح الملائمة، وعلى إعادة التدفق JPSEC 2000 إلى بيانات الصورة الواضحة الأصلية.

12.3 **تدفق مشفر JPSEC**: تتابع بتات ينتج من تشفير وأمن صورة تستخدم التشفير JPSEC 2000 وأدوات الأمن JPSEC.

1.12.3 **مستحدث JPSEC**: كيان يستحدث التدفق المشفر JPSEC انطلاقاً من صورة ما أو من تدفق مشفر JPSEC 2000 أو من تدفق مشفر JPSEC آخر بهدف توفير بعض خدمات JPSEC.

2.12.3 **مستهلك JPSEC**: كيان يستقبل تدفقاً مشفراً JPSEC ويقوم بإسداء خدمة JPSEC قائمة على التدفق المشفر.

13.3 **خدمة JPSEC**: خدمة توفر الأمن لدى الاطلاع على الصور JPSEC 2000. وتعمل هذه الخدمة على تعداد الهجمات وتستخدم إحدى الأدوات JPSEC أو مجموعة منها.

14.3 **سلطة التسجيل JPSEC**: كيان مسؤول عن تخصيص معرف هوية فريدة لأداة JPSEC مرجعية. وعن تسجيل قائمة معلمات وصف الأداة JPSEC.

15.3 **أداة JPSEC**: عملية صادرة عن برمجية أو عتاد تستخدم تقنيات أمنية من أجل توفير خدمات الأمن.

1.15.3 **أداة JPSEC معيارية**: أداة JPSEC تستخدم نماذج أدوات محددة مسبقاً لأغراض فك التشفير أو الاستيقان أو التظليل، يحددها الجزء المعياري من هذه التوصية | المعيار الدولي.

2.15.3 **أداة JPSEC غير معيارية**: أداة JPSEC تتحدد برقم تعرف هوية معين تخصصه سلطة التسجيل JPSEC أو أي تطبيق يحدده المستعمل.

3.15.3 **أداة JPSEC يحددها المستعمل**: أداة JPSEC غير معيارية يحددها تطبيق المستعمل.

4.15.3 أداة سلطة تسجيل JPSEC: أداة JPSEC غير معيارية تحددها سلطة التسجيل JPSEC.

16.3 وصف أداة JPSEC: وصف المعلمات التي تستخدمها الأداة JPSEC.

ملاحظة – لكن وصف أداة JPSEC لا يعطي وصفاً للخوارزمية أو الطريقة المستخدمتين. ويتألف من جزأين هما، قائمة المعلمات وقيم المعلمات. وفي حالة الأدوات JPSEC المعيارية تعطى قائمة المعلمات في المعيار. أما في حالة الأدوات JPSEC غير المعيارية فقد توفر سلطة التسجيل قائمة بالمعلمات. وفي كلتا الحالتين، تتحدد قيم المعلمات في قطعتي الوسم SEC وINSEC.

17.3 المفتاح: تتابع رموز يضبط عمليات التجفير وفك التجفير.

1.17.3 المفاتيح المتناظرة: زوج من المفاتيح يكون لمصدرها ومقصدها نفس المفتاح السري أو مفتاحان يمكن بسهولة حساب كل منهما استناداً إلى الآخر في نظام تشفيري.

2.17.3 زوج مفاتيح لا متناظرة: زوج من المفاتيح يعرف فيها المفتاح الخصوصي التحويل الخصوصي والمفتاح العمومي التحويل العمومي.

1.2.17.3 مفتاح خصوصي: مفتاح يشكل جزءاً من زوج مفاتيح لا متناظرة لكيان ما ينبغي عدم كشفه.

2.2.17.3 مفتاح عمومي: مفتاح يشكل جزءاً زوج مفاتيح لا متناظرة لكيان ما ويمكن جعله عمومياً.

18.3 توليد مفتاح، وظيفة توليد المفاتيح: وظيفة تأخذ عند الدخل عدداً من المعلمات تكون واحدة منها على الأقل سرية وتعطي عند الخرج مفاتيح ملائمة من أجل الخوارزمية والتطبيق المعنيين.

ملاحظة – يجب تزويد الوظيفة بخاصية تمنع استنتاج الخرج حسابياً إلا في حالة معرفة مسبقة للدخل السري.

19.3 إدارة المفاتيح: توليد وتسجيل وتوزيع وإلغاء وتصنيف وتطبيق المفاتيح وفقاً لسياسة الأمن.

20.3 محاكاة الواسم: نص تجفير ينتج عن عملية تشفير تضم شفرة بدء JPSEC.

21.3 خوارزمية شفرة استيقان الرسالة، وظيفة التحقق من التجفير، وظيفة المجموع التدقيقي للتجفير: خوارزمية حساب وظيفة تقابل سلسلات البتات والمفتاح السري مع سلسلات الطول الثابت للبتات مع الوفاء بالخاصتين التاليتين:

- يمكن حساب دالة كل مفتاح وكل سلسلة، داخلة بشكل فعال؛
- يتعذر رياضياً حساب قيمة دالة أي مفتاح ثابت دون معرفة مسبقة بالمفتاح استناداً إلى سلسلة جديدة ما داخلة حتى إذا عرف مجمل سلسلات الدخل وقيم الدالات المقابلة حيث قد يتم اختيار قيمة سلسلة دخل رقم i بعد مراقبة قيمة القيم الأولى i-1 للدالة.

ملاحظة – تتوقف الجدوى الحسابية على متطلبات الأمن المحددة للمستعمل وعلى بيئة الاستعمال.

1.21.3 شفرة استيقان الرسالة (MAC): سلسلة بتات تنتج عن خوارزمية التشفير MAC.

22.3 عدم الرفض: ربط كيان بمعاملة يشارك فيها الكيان على نحو لا يسمح بإنكار (رفض) المعاملة فيما بعد.

ملاحظة – يعني ذلك أن مستقبل معاملة ما قادر أن يثبت لطرف ثالث حيادي أن المرسل المزعوم قد أرسل المعاملة حقيقةً.

23.3 الرزمة: جزء من تدفق البتات المشفر وفقاً للجزء 1 من المعيار JPSEC 2000 والذي يضم رأسية الرزمة بيانات الصورة المضغوطة من طبقة واحدة للمنطقة باستبانة واحدة لمكونة رقعة واحدة.

ملاحظة – يختلف هذا المصطلح عن مصطلح "الرزمة" المستخدم في إرسال البيانات عبر الشبكة.

24.3 الحماية: عملية الغرض منها حماية المحتوى.

1.24.3 نموذج الحماية المعياري: نموذج معياري أو قائمة بمجالات المعلمات اللازمة لعمليات طريقة ما للحماية.

2.24.3 طريقة الحماية: طريقة تستخدم في إعداد محتوى محمي أو استعماله مثل التشفير وفك التشفير والاستيقان والتحقق من التكاملية.

25.3 الأمن: جميع الجوانب المتصلة بالتعريف والإنجاز والحفاظ على السرية والتكاملية والتيسر والتعداد والاستيقان والموثوقية.

ملاحظة – تعتبر المنتجات أو الأنظمة أو الخدمات آمنة عندما يستطيع مستعملوها أن يثقوا بأنها تعمل أو ستعمل حسبما يفترض لها. ويتم ذلك عادةً في سياق تقدير الأخطار الفعلية أو المحتملة.

26.3 قواعد تركيب التشوير: مواصفة نسق التدفق المشفر JPSEC الذي يضم جميع المعلومات اللازمة لاستعمال الصور JPSEC 2000 الأمينة.

27.3 تحويل الشفرة: عملية أخذ تدفق مشفر مضغوط داخل وتكييفه أو تحويله من أجل إنتاج تدفق مشفر مضغوط خارج بعد تزويده ببعض الخواص المطلوبة.

مثال – قد يمثل التدفق المشفر المضغوط الخارج صورة لها استبانة مكانية أو معدل ثبات أقل من استبانة التدفق المشفر المضغوط الداخل أو معدله.

1.27.3 تحويل الشفرة الأمين: إجراء عملية تحويل الشفرة أو تكييفها لمحتوى مضغوط محمي داخل دون إلغاء حماية المحتوى.

ملاحظة – يستخدم مصطلح تحويل الشفرة الأمين على عكس مصطلح تحويل الشفرة. من أجل التركيز على أن عملية التحويل تجري دون أي تهاود في الأمن. وقد يعني تحويل الشفرة الأمين إجراء تحويل شفرة في المجال المشفر.

28.3 علامة مائية: علامة غير مرئية تضاف إلى غطاء العلامة من أجل توصيل معلومات مخفية.

1.28.3 العلامة المائية: عملية تدخل بيانات غير مرئية تمثل معلومات في بيانات وسائط متعددة بإحدى الطريقتين التاليتين:

- طريقة تجارة وتعني أنه من غير الممكن استعادة غطاء العلامة تماماً بعد دمج العلامة المائية.
- طريقة دون خسارة وتعني إمكانية استعادة غطاء العلامة تماماً بعد استخراج العلامة المائية.

4 الرموز والمختصرات

تنطبق المختصرات التالية لأغراض هذه التوصية | المعيار الدولي:

BAS	قطعة أثمونات متراصفة *(Byte Aligned Segment)*
FBAS	قطعة أثمونات متراصفة للمجال *(Field Byte Aligned Segment)*
G	الخشونة *(Granularity)*
GL	سوية الخشونة *(Granularity Level)*
INSEC	وسم أمن تدفق مشفر داخل *(In-codestream security marker)*
IP	الملكية الفكرية المرتبطة بالتكنولوجيا *(Intellectual Property related to technology)*
IPR	حقوق الملكية الفكرية المرتبطة بالمحتوى *(Intellectual Property Rights related to content)*
JPSEC	نظام JPEG 2000 أمين *(Secure JPEG 2000)*
KT	نموذج معياري رئيسي *(Key Template)*
LSB	البتة الأقل دلالة *(Least Significant Bit)*
MAC	شفرة استيقان الرسالة *(Message Authentication Code)*
MSB	البتة الأكثر دلالة *(Most Significant Bit)*
PD	مجال المعالجة *(Processing Domain)*
PKI	بنية تحتية رئيسية عمومية *(Public Key Infrastructure)*
PO	أمر المعالجة *(Processing Order)*
RA	سلطة تسجيل *(Registration Authority)*
RBAS	قطعة أثمونات متراصفة للمدى *(Range Byte Aligned Segment)*
SEC	واسم الأمن *(Security marker)*
T	نموذج معياري *(Template)*
V	قيم *(Values)*
VL	قائمة القيم *(Value List)*
ZOI	منطقة التأثير *(Zone of Influence)*

5 قواعد تركيب النظام JPSEC (معيارية)

1.5 استعراض إطار النظام JPSEC

يحدد النظام JPSEC إطاراً لتوفر أمن البيانات المشفرة JPSEC 2000. والعنصر الأساسي لهذه التوصية | المعيار الدولي هو مواصفة قواعد تركيب الصورة JPSEC 2000 الأمينة أي *التدفق المشفر JPSEC*. وقواعد التركيب مستهدفة من خلال البيانات المشفرة JPSEC 2000 وهي

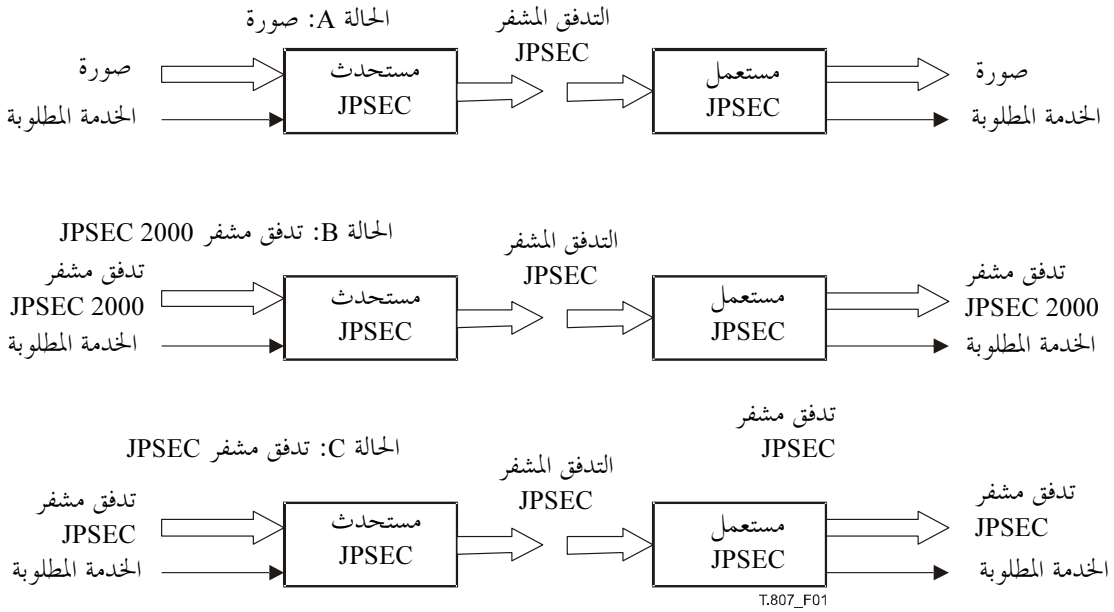
توفر حماية كامل التدفق المشفر أو أجزاء منه. وفي جميع الحالات، يجب على البيانات المحمية (أي التدفقات JPSEC) أن تلتزم بقواعد التركيب المعيارية المحددة في هذه التوصية | المعيار الدولي.

والتدفقات JPSEC مرفقة بعدد من *خدمات الأمن JPSEC* التي تشتمل على السرية واستيقان المصدر والمحتوى.

وتحدد قواعد التشوير ما يلي:

- خدمات الأمن المصاحبة لبيانات الصورة؛
- *الأدوات JPSEC* الضرورية لتوفير الخدمات المقابلة؛
- كيفية تطبيق الأدوات JPSEC؛
- الأجزاء التي ينبغي حمايتها من بيانات الصورة.

الحالة A: صورة



الشكل 1 – نظرة شاملة للمراحل النظرية في إطار النظام JPSEC

قواعد تركيب التدفق المشفر JPSEC معيارية. والغرض منها هو السماح للتطبيقات JPSEC أن تستخدم التدفقات المشفرة JPSEC بطريقة قابلة للتشغيل بينياً (الشكل 1). ويُفسر تطبيق مستعمل JPSEC التدفق المشفر JPSEC ويحدد الأدوات JPSEC المشار إليها ويطبقها ويسلم خدمات الأمن المقابلة ثم ينتقل إلى خرج التدفق المشفر JPSEC 2000 من أجل المعالجة اللاحقة في جهاز ترئية الصور مثلاً.

وكما تبين الحالة C من الشكل 1، يمكن استحداث التدفق المشفر JPSEC من تدفق مشفر JPSEC آخر. وقد يحدث ذلك عندما تطبق أدوات JPSEC متعددة على نفس المحتوى لكن في أوقات مختلفة أو من قبل كيانات مختلفة. وعند حدوث ذلك قد يكون ترتيب استخدام الأدوات JPSEC خلال بدء العمليات وتشغيلها مهماً.

وتحدد قواعد تركيب التشوير أدوات يستخدمها مستعمل JPSEC. وتتحدد الأدوات إما في الجزء المعياري من المعيار ذاته أو من قبل سلطة التسجيل أو بوسائل خاصة. وتوفر الأدوات المعيارية السرية (بين أدوات التشفير) واستيقان المصدر والمحتوى. كما توفر أكبر قدر من التشغيل البيني نظراً إلى أن التطبيقات المستقلة لعملية الاستهلاك قادرة على معالجة نفس التدفق المشفر JPSEC وتأدية الخدمات المقابلة مع نفس السلوك.

ولا تتطرق هذه التوصية | المعيار الدولي إلى طريق استحداث التدفق المشفر JPSEC. ويجب على معدّي النظام JPSEC توليد تدفقات مشفرة JPSEC تضم معلمات تشوير JPSEC الملائمة. ويمكن إعداد التدفقات المشفرة JPSEC بطرائق عدة. فعلى سبيل المثال، يمكن تطبيق أداة JPSEC على بيكسلات صورة أو على معاملات موجات صغير أو معاملات تكمية أو على رزم.

ويستطيع المستهلك تطبيق أداة JPSEC واحدة أو أكثر. فقد يكون قادراً مثلاً على إجراء فك تشفير باستخدام مجفر القدرة AES بالأسلوب ECB والتحقق من التوقيع باستعمال خوارزمية التقطيع SHA-128 والمفتاح العمومي RSA. وباستخدام هذه المقدرات يكون قادراً على توفير خدمتي الأمن السرية والاستيقان.

وتتحدد الأدوات JPSEC في الإطار JPSEC من خلال النماذج المعيارية المعرفة بصفة خصوصية أو المسجلة لدى *سلطة تسجيل JPSEC*. وللأدوات JPSEC التي تحددها النماذج المعيارية سلوك معالجة وحيد. وبالتالي فهي لا تتطلب تعرف هوية فريداً. أما الأدوات المحددة من سلطة التسجيل فترفق برقم تعرف هوية فريد يخصصه السجل العام.

2.5 خدمات الأمن JPSEC

تنطوي هذه الفقرة على تعداد وشرح الوظائف التي يتضمنها مجال تطبيق هذه التوصية المعيار الدولي.

وتستخدم الأدوات JPSEC في تطبيق وظائف الأمن. والنظام JPSEC إطار مفتوح أي قابل للتوسيع مستقبلاً. ويركز عموماً على الجوانب التالية:

- *السرية في التشفير والتشفير الانتقائي*

يستطيع ملف JPSEC تحويل بيانات الصورة و/أو البيانات الشرحية (نص مكتوب) من وإلى (نص مجفر)، مما يحجب المعنى الأصلي للبيانات. ويقصد بالتشفير الانتقائي عدم تشفير كامل الصورة و/أو البيانات الشرحية بل بعض أجزاء منها.

- *التحقق من التكاملية*

يستطيع ملف JPSEC توفير وسائل كشف التحويرات المدخلة على الصورة و/أو الشروحات والتحقق من تكاملها. وثمة صنفان من التحقق من التكاملية هما:

1) التحقق من تكاملية بيانات الصورة حيث تكفي بتة واحدة في بيانات الصورة أن تكون خاطئة حتى تؤدي إلى فشل التحقق (أي يعطي التحقق نتيجة "عدم التكاملية"). فغالباً ما يسمى هذا التحقق بالتحقق الهش من (تكاملية) الصورة.
2) التحقق من تكاملية محتوى الصورة حيث تسفر بيانات الصورة، حتى عند وجود بعض الخلل الطارئ فيها، عن تحقق ناجح طالما لم يتأثر محتوى الصورة بأي تغيير من وجهة نظر جهاز رؤية الإنسان، وبعبارة أخرى طالما لم يتغير فحوى الصورة المدرك. وغالباً ما يسمى هذا التحقق بالتحقق شبه الهش من (تكاملية) الصورة.

قد يحدد هذان النوعان من التحقق الهش وشبه الهش من تكاملية الصورة مواقع في بيانات الصورة أو محتواها حيث تطرح التكاملية بالمناقشة. وتضم الحلول ما يلي:

1) طرائق تجفير مثل شفرات استيقان الرسالة (MAC) أو علامات (تواقيع) رقمية أو مجموعات تدقيقية مجفرة أو عنونة منقطعة مع مفاتيح محسوبة.
2) طرائق العلامات المائية. ولا تحدد هذه التوصية | المعيار الدولي نموذجاً معيارياً لتقنية العلامات المائية لكنها تقدم أدوات غير معيارية تستعمل هذه التقنية.
3) جمع هذين النمطين من الطرائق.

- *استيقان المصدر*

يستطيع ملف JPSEC توفير تحقق من هوية المستعمل/الطرف الذي أعد الملف JPSEC. وقد يتضمن ذلك طرائق مثل التواقيع الرقمية أو مشفرة استيقان الرسالة (MAC).

- *النفاذ الشرطي*

يستطيع ملف JPSEC توفير آلية وسياسة تضمنان أو تمنعان النفاذ إلى بيانات الصورة أو إلى أجزاء منها. وقد يتيح ذلك مثلاً رؤية أولية استبانة منخفضة لصورة ما دون التمكن من رؤيتها باستبانة عالية.

- *تعرف هوية المحتوى المسجل*

يمكن تسجيل ملف JPSEC لدى سلطة تسجيل المحتويات. ويوفر ذلك طريقة مواءمة بيانات الصورة/محتوى الصورة (المزعومة) مع بيانات الصورة/محتوى الصورة المسجلة. على سبيل المثال، قد تكون الطريقة هذه قراءة معرف هوية ملف (لوحة التسجيل) موضوع ضمن البيانات الشرحية والتحقق من الانسجام بين لوحة التسجيل والمعلومات المنقولة لدى إجراء عملية التسجيل. وقد يحتوي لوحة التسجيل على قدر من المعلومات يكفي لطلب معلومات من سلطة تسجيل المحتويات عن وقت تسجيل الملف والتحقق من مطابقته مع معرف الهوية.

- *تدفق تدرجي أمين وتحويل شفرة أمين*

يوفر ملف JPSEC أو تتابع رزم طرائق مثل تلك التي تمكّن عقدة واحدة أو عقد مختلفة من القيام بالإرسال المتدفق وتحويل الشفرة دون اللجوء إلى فك تشفير المحتوى أو عدم حمايته. مثال لذلك الحالة التي يتدفق فيها محتوى JPSEC 2000 محمي إلى عقدة منتصف الشبكة أو إلى المخدم حيث يتم تحويل شفرة المحتوى JPSEC 2000 المحمي بطريقة تحافظ على الأمن من طرف إلى طرف.

3.5 تعليقات بشأن تصميم الأنظمة JPSEC الأمنية وتطبيقها

تقوم هذه التوصية | المعيار الدولي مجموعة كبيرة ومرنة من خدمات الأمن. على سبيل المثال، يمكن تطبيق بدائيات التشفير بطرق مختلفة من أجل تحقيق أهداف مختلفة تتراوح بين تشفير كامل التدفق المشفر JPSEC 2000 والتشفير الانتقائي لجزء صغير من التدفق المشفر. غير أنه من المهم التركيز على ضرورة توخي الحذر عند تطبيق أي نظام أمن بما في ذلك النظام القائم على المعيار JPSEC.

ويوصى بقوة بأن يراعي بدقة مصممو أي نظام أمن الخطوط التوجيهية الموصى بها والمتعلقة ببدائيات الأمن المستخدمة. وفيما يتعلق بمعظم بدائيات الأمن المذكورة التي تستخدم JPSEC فإن المعايير ISO/IEC المرفقة توفر إرشادات مهمة بشأن استعمالها الصحيح. وفيما يتعلق مثلاً بالتشفير الذي يستعمل خوارزمية تجفير لكل قدرة مع أسلوب تجفير قدر (الجدول 29)، تعطى الخطوط التوجيهية بشأن اختيار أسلوب مجفر القدرة والعمليات في المعيار ISO/IEC 10116.

إضافة إلى ذلك فإن الاستيقان في كثير من تطبيقات الأمن هو أهم خدمات الأمن. وحتى عندما تكون السرية مستهدفة في خدمة الأمن ينبغي زيادة الاستيقان من أجل الوقاية من مختلف أشكال الهجمات. ويوصى خصوصاً باستخدام الاستيقان أيضاً حتى في تطبيقات التصوير العديدة حيث تشكل السرية الهدف الأول.

وإدارة المفاتيح غير مشمولة في مجال تطبيقات النظام JPSEC غير أنه يجب التركيز على أهميتها. وأهم عنصر في أي نظام تشفيري هو إدارة مفاتيح التشفير التي تتحكم بالعمليات. وإذا كانت هذه المفاتيح مشبوهة، يكون أمن كامل النظام مهدداً إلى درجة عدم القدرة على كشف المواقع المشبوهة. وبالتالي يتحتم أن توليد المفاتيح وتوزيعها وتسجيلها وإتلافها مع مراعاة مستوى أمني مساوٍ على الأقل لنفس مستوى حماية البيانات. علاوة على ذلك، ونظراً إلى أن احتمالات تعرض مفتاح ما للشبهة تزداد مع الوقت، يتحتم أيضاً استعمال المفاتيح الصالحة لفترة زمنية محددة فقط. وللمزيد من المعلومات عن استعمال مفاتيح التشفير وإدارتها، انظر المعيار ISO/IEG 11770.

وكما هو الحال في جميع أنظمة الأمن، يجب أن يكون استخدام عمليات التشفير محجوباً تماماً من المستعمل. إذ ينبغي ألا يكون المستعمل قادراً على اكتشاف أي معلومة بشأن عمليات التشفير باستثناء تلك الخاصة بالخرج. فمثلاً، ينبغي ألا يكون المستعمل قادراً على النفاذ إلى معلومات عن سبب إخفاق عملية تجفير ما في إنتاج خرج. وكذلك ينبغي ألا يكون المستعمل قادراً على الحصول على معلومات زائدة حتى ولو لجأ إلى عملية قياس "القنوات الجانبية" مثل تحليل التواتر و/أو القدرة. وبإيجاز ينبغي ألا يكون المستعمل قادراً على ملاحظة أي فرق في خرج التطبيقات بغض النظر عما يقوم به التطبيق عادة، وإلا فقد يشكل تداخل المعلومات الناتج تمهيداً لأمن النظام.

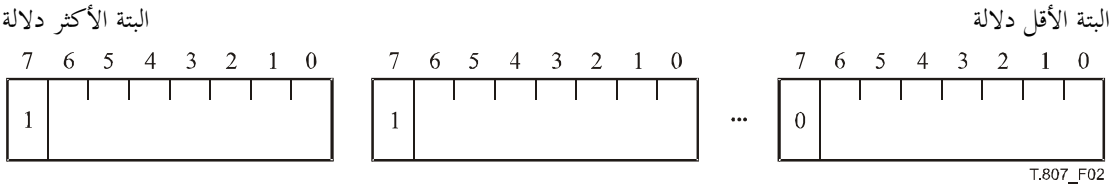
والخلاصة، إنه يوصى بقوة بأن يولي مصممو أنظمة الأمن بما فيها النظام القائم على المعيار JPSEC، اهتماماً خاصاً بالتفاصيل الدقيقة لتصميم النظام من أجل ضمان نظام أمين.

4.5 قطعة أثمونات متراصفة (BAS)

1.4.5 قطعة أثمونات متراصفة

حرصاً على توفير نظام إشارات قابل للتوسيع لاحقاً فيما يتعلق بالأصناف والأساليب، تستخدم هذه التوصية المعيار الدولي بنية بيانات الطول المتغير المسماة "قطعة أثمونات متراصفة" (BAS). وتظهر مجالات المعلمات التي يمكن توسيع عددها من خلال بنية القطعة BAS للمجال (FBAS). وتتمثل قيم المعلمات ذات الأمدية الكبيرة في شكل قابل للتوسيع في بنية قطعة BAS للمدى (RBAS).

والقطعة BAS، كما يبين الشكل 2، مؤلفة من تتابع واحداً وأكثر من أثمونات القطعة BAS. وتدل البتة الأكثر دلالة (MSB) في كل أثمون BAS على وجود أثمون BAS تال. وعلى وجه التحديد إذا كانت البتة MSB = 1 فإن ذلك يعني وجود أثمون BAS لاحق، أما إذا كانت البتة MSB = 0 فلا وجود لأثمون BAS لاحق والبنية BAS تنتهي. وتسلسل البتات الأقل دلالة المتبقية من كل أثمون BAS من قائمة بتات تستخدم في طرق مختلفة لمعلمات BAS مختلفة. وغالباً ما تستخدم بالترافق مع قائمة معلمات تضم عدداً من العناصر، وتضبط كل بتة BAS على القيمة 1 أو 0 كي تعلن من خلال تحكم المعلومات، عن عنصرها المقابل. وتم اختيار هذه البنية بسبب قابلية توسيعها بهدف احتواء التطورات اللاحقة للمعيار، إذ إنها تتيح إدخال معلومات جديدة بطريقة قابلة للتوسيع.



الشكل 2 – بنية قطعة أثمونات متراصفة (BAS)

2.4.5 قطعة أثمونات متراصفة للمجال (FBAS)

قطعة الأثمونات المتراصفة للمجال (FBAS) هي نمط قطعة BAS تُستخدم فيه البتات المتبقية من أثمونات القطعة BAS في إعطاء القيمة 1 أو 0. مثال لاستخدام القطعة FBAS هو صنف منطقة التأثير (DCzoi) حيث يمكننا تحديد أوصاف متعددة للصورة مثل دليل الرقعة وسوية الاستبانة ومكونة اللون. وفي هذه الحالة ينبغي إعطاء القيمة 1 لعلم البتات BAS الثلاث المقابلة للرقعة والاستبانة واللون.

وإذا أردنا على سبيل المثال تمثيل قطعة FBAS مع 9 مجالات، من f1 إلى f9، نحتاج عندئذٍ إلى استعمال قطعة BAS من أثمونين كحد أقصى. وإذا كانت الأثمونان هما الأثمون "a" والأثمون "b"، وكانت البتة الأكثر دلالة لكل أثمون هي a0 وb0 تكون قطعة المجال FBAS كالتالي:

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

والبتتان a0 وb0 هما البتتان المؤشرتان. وتتمثل المجالات من f1 إلى f7 في البتات من a1 إلى a7 والمجال f8 في البتة b1 والمجال f9 في البتة b2. أما البتات المتبقية من b3 إلى b7 فمحجوزة وتتخذ القيمة 0.

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

وعند استعمال القطعة FBAS لهذا المثال في تدفق JPSEC، يمكن تمثيلها في أثمون أو أثمونين تبعاً لقيمة المجال الفعلية. ويعود ذلك إلى أن قيمة المجالات بالتغيب هي 0. وبناءً على ذلك، إذا كان المجالان f8 وf9 دون قيمة (أي قيمتهما 0)، يكون الأثمون الثاني للقطعة BAS غير ضروري وتتخذ البتة a0 القيمة 0. ومن ناحية أخرى إذا كان المجال 8 أو المجال 9 موجودين فإن الأثمونين ضروريان. وفي هذه الحال، تتخذ البتة a0 القيمة 1 وb0 القيمة 0.

يلاحظ أن بتات المجال "متراصفة إلى اليسار". مما يتيح لنا إضافة المزيد من المجالات مع الوقت بطريقة موائمة.

3.4.5 قطعة BAS للمدى (RBAS)

تستخدم قطعة BAS للمدى في توسيع مدى أو عدد البتات المستخدمة في تمثيل قيمة ما. وثمة نوعان للقطعة RBAS هما RBAS-8 وRBAS-16.

ويضم النوع RBAS-8 أثموناً واحداً أو أكثر للقطعة RBAS يحتوي على بتات القيمة. وكما هو الحال في القطعة FBAS، تدل البتة الأولى من كل أثمون على إمكانية وجود أثمون RBAS آخر لاحق.

وعلى العكس من القطعة FBAS، فإن القطعة RBAS "متراصفة إلى اليمين". وبالتالي، إذا كان لقيمةٍ ما 9 بتات من v1 إلى v9 حيث v1 هي البتة الأكثر دلالة، فإن هذه القيمة تتمثل بأثمونيّ قطعة BAS هما:

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

على النحو التالي:

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

وإذا كانت القيمة صغيرة كأن تكون البتتان v1 وv2 صفراً، أمكن استخدام تمثيل الأثمونين أعلاه بإعطاء v1 وv2 قيمة صفر أو أمكن استخدام قطعة RBAS بأثمون واحد على النحو التالي:

0 v3 v4 v5 v6 v7 v8 v9

وقد يستخدم النوع RBAS-16 من أجل تمثيل قيم تزيد دائماً عن 7 بتات ويقل عن 15 بتة. وفي هذه الحالة، تكون أول مجموعة RBAS مؤلفة من بتتين، حيث البتة الأولى هي البتة المؤشرة ثم البتات التالية الخمس عشر هي بتات قيم. والأثمونات المتبقية تتوسع بزيادة أثمون واحد في المرة الواحدة وذلك باستعمال بنية BAS النموذجية حيث تكون البتة الأولى من كل أثمون مؤشراً للأثمونات BAS اللاحقة.

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

وإذا كانت قيمة معلمة ما 22 بتة، أمكن تمثيلها في بنية النوع RBAS-16 ذات الأثمونات الثلاثة كما هو مبين أدناه، حيث a0 وc0 هما بتتان مؤشرتان تدلان على إمكانية وجود أثمون BAS لاحق. ولا يكون أي من الأثمونات BAS المتبقية قطعة BAS تقليدية من أثمون واحد.

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

وبالتالي تكون قيم البتات المؤشرة كالتالي:

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

وفيما يتعلق بكلا النمطين RBAS-8 وRBAS-16 فإن بتات القيمة "متراصفة إلى اليمين" أيضاً.

وجدير بالذكر أنه من الضروري لدى كتابة مستحدثات JPSEC ومستعمليه الانتباه إلى البتة الأكثر دلالة/البتة الأقل دلالة.

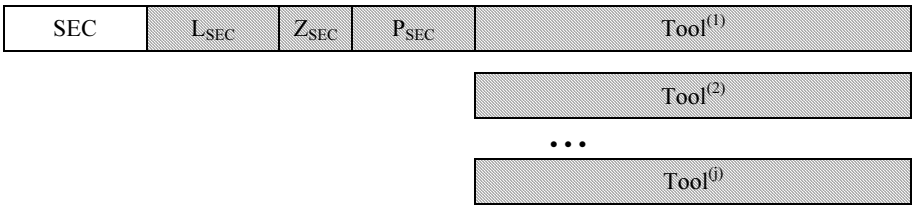
5.5 واسم الأمن الرئيسي (SEC)

1.5.5 قطع وسم الأمن

نقدم في هذه الفقرة قواعد تركيب نظام تشوير JPSEC بسيطة ومرنة ومتينة في نفس الوقت. وتتحدد قطع وسوم الأمن SEC لهذا الغرض وتوضع في الرأسية الرئيسية. وتتيح قواعد تركيب قطعة الوسم SEC وصف جميع المعلومات المطلوبة لتوفير أمن الصور JPSEC 2000. ولذا فإنها تحيل إلى الأدوات المعيارية JPSEC المحددة بالنماذج المعيارية المذكورة في الفقرة 8.5 أو بالأدوات JPSEC غير المعيارية التي سجلت مسبقاً في سلطة التسجيل JPSEC أو التي حددت على صعيد خاص، كما أنها تضع أحكاماً بشأن تناول المعلمات المتعلقة بهذه الأدوات.

وبالإمكان حماية تدفق مشفر JPSEC واحدة أو أكثر. وكل أداة هي أداة JPSEC معيارية أو أداة JPSEC غير معيارية. ويشار إلى معلمات هذه الأدوات في قطعة واسم SEC واحدة أو أكثر موجودة في الرأسية الرئيسية من التدفق المشفر بعد قطعة الواسم SIZ. وتكون الوسوم SEC المتعددة عند استخدامها سلسلة ويجب أن تظهر على التتالي في الرأسية الرئيسية. وفي معظم الحالات يمكن الإشارة إلى المعلمات JPSEC في قطعة واسم SEC واحدة. غير أن طول التشوير قد يتجاوز في بعض الحالات الحد الأقصى لحجم قطعة الواسم، وعندما يمكن استخدام قطع واسم SEC إضافية للتشوير.

ويبين الشكل 3 قاعدة تركيب قطعة الواسم SEC. ويشار إلى القطعة من خلال الواسم 0xFF65 وL_{SEC} هو طور قطعة الواسم SEC بما فيها الأثمونان الخاصان بالطول L_{SEC}، لكن دون الأثمونين الخاصين بالواسم SEC ذاته. وZ_{SEC} هو دليل قطعة الواسم SEC. وتعطى Z_{SEC} القيمة 0 لأول قطعة واسم تظهر في التدفق المشفر. وP_{SEC} وهو مجال معلمة تصف معلمات الأمن ذات الصلة بتكامل التدفق المشفر، ولا توجد إلا في أول قطعة واسم SEC، أي إذا كانت $Z_{SEC} = 0$. وتدعم قواعد التركيب استخدام أدوات JPSEC عدة تمت الإشارة إليها في قطعة واسم واحدة أو أكثر. وفي حال استخدم أكثر من أداة JPSEC واحدة يقوم مستعمل JPSEC بمعالجة الأدوات حسب الترتيب الذي تظهر فيه في التدفق المشفر.



الشكل 3 – قواعد تركيب قطعة واسم أمن رئيسية

SEC: شفرة واسم. يبين الجدول 1 حجوم وقيم الرموز والمعلمات الخاصة بقطعة واسم الأمن الرئيسية.

L_{SEC}: طول قطعة واسم بالأثمونات (بما فيه الطور L_{SEC} ذاته لكن دون الواسم).

Z_{SEC}: دليل قطعة هذا الواسم نسبةً إلى جميع قطع الوسوم SEC الأخرى الموجودة في الرأسية الحالية. ويستخدم هذا المجال البنية RBAS.

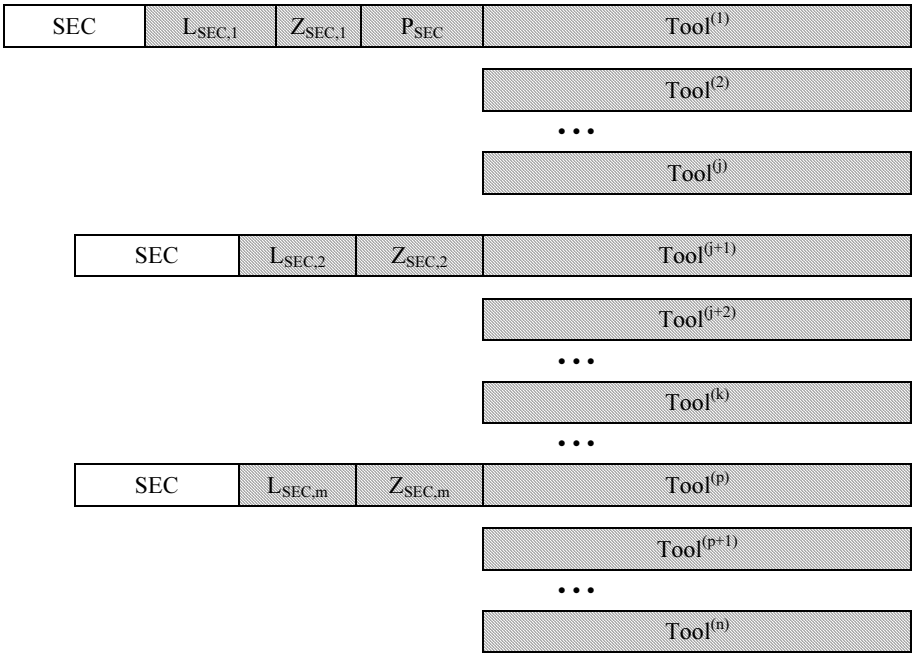
P_{SEC}: مجال المعلمة الخاص بمعلمات أمن التدفق المشفر. ولا يوجد هذا المجال إلاّ في أول قطعة واسم SEC، أي عندما تكون $Z_{EC} = 0$.

$Tool^{(i)}$: معلمات خاصة بالأداة JPSEC رقم *(i)*. إذا تمت الإشارة إلى أدوات JPSEC متعددة يقوم مستعمل JPSEC بمعالجة كل أداة حسب ترتيب ظهورها في التدفق المشفر JPSEC.

الجدول 1 – قيم معلمة الأمن الرئيسية

المعلمة	الحجم (بالبتات)	القيم
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, if $Z_{SEC} > 0$ وإلا متغير	إذا $Z_{SEC} = 0$، انظر الجدول 2
$Tool^{(i)}$	متغير	انظر الفقرتين 2.6.5 و3.6.5

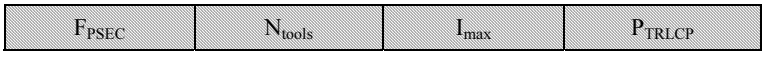
ويبين الشكل 4 قواعد تركيب معلمات الأمن في الرأسية الرئيسية عند استخدام قطع وسوم SEC متعددة. في هذه الحالة تظهر معلمات الأدوات JPSEC في قطع وسوم SEC مختلفة. وتبدأ كل قطعة واسم بالواسم SEC، 0xFF65، ثم يليها طول قطعة الواسم ودليلها. ويتخذ دليل أول قطعة واسم القيمة 0 ويزداد بمقدار واجد عند كل قطعة واسم حسب ترتيب ظهورها. وقطعة الواسم الأولى وحدها تحتوي على معلمات الأمن الخاصة بالتدفق المشفر P_{SEC}. وجميع قطع الوسوم تضم المعلمات الخاصة بأداة JPSEC واحدة أو أكثر.



الشكل 4 – قواعد تركيب واسم الأمن الرئيسي عند استخدام قطع وسوم متعددة

وبإمكان أداة JPSEC عند الضرورة أن تمتد على مدى عدة قطع وسوم SEC، مثال: يحدث ذلك إذا تطلبت طولاً يزيد عن الحد الأقصى لحجم الواسم SEC. وبما أن طول وصف الأداة محدد تماماً فإن مولد JPSEC يقسم ببساطة الأداة على قطع الوسوم SEC. وينبغي عندئذٍ لمفكك التشفير أن يمرر جميع القطع بالتسلسل ما عدا قيم الواسم SEC والطول L_{SEC} والحجم Z_{SEC} ثم يفسر الأدوات وفقاً لذلك.

وP_{SEC} هو مجال المعلمة التي تصف معلمات الأمن الخاصة بكامل التدفق المشفر ولينسى بأداة محددة. ويستخدم هذا المجال في الدلالة على أحداث مثل المطابقة مع الجزء 1 من المعيار JPSEC 2000. ويبين الشكل 5 المعلمات P_{SEC}.



الشكل 5 – قاعدة تركيب معلمات أمن التدفق المشفر (P_{SEC})

F_{PSEC}: تحكم للدلالة على استخدام قطعة الواسم INSEC واستخدام قطع وسوم SEC متعددة وتغيير بيانات التدفق المشفر الأصلي JPSEC 2000 Part 1 وتحديد استعمال الوسم TRLCP. ويستخدم هذا المجال بنية القطعة FBAS.

N_{tools}: عدد الأدوات JPSEC المستخدمة في التدفق المشفر. ويستخدم هذا المجال البنية RBAS.

I_{max}: أقصى قيمة لدليل حالة الأداة في التدفق المشفر. ويستخدم هذا المجال البنية RBAS.

P_{TRLCP}: مجال المعلمة لتمديد نسق الوسم TRLCP. ويوجد هذا المجال إذا كانت $F_{TRLCP} = 1$.

الجدول 2 – معلمات أمن التدفق المشفر (P_{SEC}) في أول قطعة واسم SEC

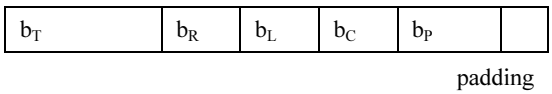
القيم	الحجم (بالبتات)	المعلمة
F_{PSEC}	متغير (FBAS)	انظر الجدول 3
N_{tools}	8 + n * 8 (RBAS)	$1 \ldots 2^{7+7*n}$
I_{max}	8 + n * 8 (RBAS)	$0 \ldots 2^{7+7*n}$
P_{TRLCP}	0, if $F_{TRLCP} = 0$ 32, if $F_{TRLCP} = 1$	انظر الجدول 4

وللمعلمة F_{PSEC} بنية القطعة FBAS. وتستخدم في الدلالة على عدد من أعلام المعلمات في التدفق المشفر. وتظهر المجالات التي تمثلها F_{PSEC} في الجدول 3. وتتخذ المعلمة F_{PSEC} القيمة 1 عند استخدام الوسوم INSEC في التدفق المشفر JPSEC. وتعطى المعلمة $F_{mulitSEC}$ القيمة 1 عند استخدام عدة قطع وسم SEC في التدفق المشفر JPSEC. وتعطى المعلمة F_{mod} القيمة 1 عند تغيير البيانات JPSEC 2000 الأصلية في التدفق المشفر JPSEC. ويلاحظ أنه عند استخدام الوسوم INSEC تتغير المطيات JPSEC 2000 الأصلية، وبالتالي تتخذ المعلمتان F_{INSEC} وF_{mod} القيمة 1. وتعطى المعلمة F_{TRLCP} القيمة 1 إذا تحدد استعمال الوسم TRLCP في المعلمة P_{SEC}. وفي حال تحديد هذا الاستعمال، فإن واصف الوسم TRLCP وهو P_{TRLCP} يتحدد في مجال المعلمة P_{SEC}. ويجب تحديد استعمال الوسم TRLCP إذا استخدمت أي أداة في التدفق المشفر JPSEC الوسوم TRLCP.

الجدول 3 – دلالة القيم F_{PSEC} (FBAS)

المجال BAS	رقم البتة BAS	القيمة (بالبتات)	الدلالة
FINSEC	1	0	الواسم INSEC غير مستعمل
		1	الواسم INSEC مستعمل
FmultiSEC	2	0	تستخدم قطعة واسم SEC واحدة
		1	تستخدم قطع وسوم SEC متعددة
Fmod	3	1	طرأ تغيير على البيانات JPSEC 2000 الأصلية
		0	لم يطرأ أي تغيير على البيانات JPSEC 2000 الأصلية
FTRLCP	4	0	استخدام الوسم TRLCP غير محدد في PSEC
		1	استخدام الوسم TRLCP محدد في PSEC

يحدد الواسم JPSEC بنيةً تسمى واسم TRLCP يمكن استخدامه في تعرف هوية الرزمة JPSEC 2000 دون لبس. ويمكن تحديد رزمة JPSEC 2000 دون لبس من خلال دليل رقعتها ودليل سوية استبانتها ودليل طبقتها ودليل مكونتها ودليل منطقتها. ويعرف وسم TRLCP بأنه وحدة بيانات له عدد ثابت من البتات المستخدمة في تحديد كل قيمة من قيم الأدلة هذه. ويوضح عدد البتات المستخدمة في المعلمة P_{SEC}. وP_{TRLCP} هو مجال معلمة يصف نسق الوسم TRLCP على النحو الذي يتعين استخدامه في الأدوات JPSEC. ولا يتواجد هذا المجال إلا إذا كانت F_{TRLCP} = 1. وتتضمن المعلمة P_{TRLCP} المتغيرات التالية المبينة في الشكل 6.



الشكل 6 – تركيب واصف الوسم TRLCP (P_{TRLCP})

b_T: عدد بتات تمثيل دليل الرقعة هو $b_T + 1$ في الوسم TRLCP.

b_R: عدد بتات تمثيل دليل سوية الاستبانة هو $b_R + 1$ في الوسم TRLCP.

b_L: عدد بتات تمثيل دليل الطبقة هو $b_L + 1$ في الوسم TRLCP.

b_C: عدد بتات تمثيل دليل المكونة هو $b_C + 1$ في الوسم TRLCP.

b_P: عدد بتات تمثيل دليل المنطقة هو $b_P + 1$ في الوسم TRLCP.

الجدول 4 – مجال المعلمة لواصف الوسم TRLCP (P_{TRLCP})

المعلمة	الحجم (بالبتات)	القيم
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 ... $(2^8 - 1)$
الحشو	2	0

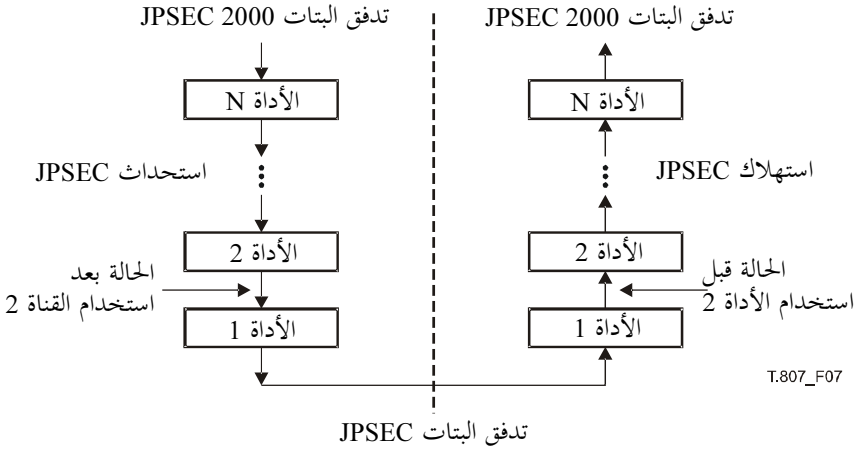
وحجم كل وسم TRLCP ناتج هو أصغر عدد صحيح في حجم الأثمونات الذي يضم جميع البتات. ويشمل نسق الوسم TRLCP على بتات دليل الرقعة ودليل سوية الاستبانة ودليل الطبقة ودليل المكونة ودليل المنطقة حسب هذا الترتيب المذكور. وعند الحاجة إلى بتات إضافية من أجل استيفاء شرط العدد الصحيح لحجم الأثمونات، فإن الوسم TRLCP يوضع في أقل البتات الممكنة دلالةً، وتعطى البتات الإضافية القيمة 0. ويلاحظ أن هذه البتات الإضافية ستكون في حال وجودها أكثر البتات دلالة في الوسم TRLCP.

2.5.5 تطبيق الأدوات JPSEC المتعددة

من الضروري في تطبيقات كثيرة استخدام أدوات JPSEC متعددة في تدفق مشفرة JPSEC 2000 واحد. فيجوز مثلاً استخدام كل من التشفير والاستيقان في حماية صورة JPSEC 2000. وتوضح الأشكال 3 و4 و7 الحالة العامة لاستخدام أدوات JPSEC متعددة حيث تستخدم عدد N من الأدوات. وسيقرأ مستهلك التدفق JPSEC الأدوات وعددها N حسب ترتيب مواقعها في قطعة الواسم SEC المبينة في الشكل 3 أو الشكل 4، ويطبقها بنفس الترتيب ليقوم باستهلاك JPSEC في التدفق المشفر JPSEC. وجدير بالذكر أنه بينما يطبق مستهلك التدفق JPSEC الأدوات JPSEC حسب الترتيب 1، 2، ... N كما يقرأها في قطعة الواسم SEC، فإن تطبيق هذه الأدوات JPSEC جرى حسب الترتيب العكسي أي N، N-1، ...، 2، 1، أثناء استحداث التدفق المشفر JPSEC، كما يبين الشكل 7. ويلاحظ أن اختيار ترقيم الأدوات في الشكل تم بحيث يبرز أن المستهلك JPSEC يطبق الأدوات JPSEC في عكس الترتيب الذي أجراه المستحدث JPSEC. غير أن أي ترقيم للأدوات JPSEC مقبول طالما أعطيت كل أداة JPSEC في التدفق المشفر JPSEC رقماً فريداً لتعرِّف هويتها.

وعموماً تستحدث الأدوات JPSEC وتستهلك بترتيب عكسي بين العمليتين. فإذا استخدم المستحدث JPSEC مثلاً عدد N من الأدوات JPSEC، يطبق المستهلك JPSEC عادةً نفس الأدوات لكن بالترتيب المعاكس. ويمكن ضمان استهلاك JPSEC صحيح لأدوات JPSEC متعددة من خلال استهلاك تتابعي للأدوات N حسب الترتيب الصحيح ومن خلال اشتراط توافق كل مرحلة وسيطة على صعيد المستهلك مع المرحلة المقبلة لها في المستحدث. مثال: في الشكل 7، ينبغي أن تكون الحالة في المستهلك بعد استهلاك JPSEC للأداة 1 مساوية للحالة الحاصلة بعد تطبيق الأداة 2 أثناء عملية الاستحداث JPSEC. وكمثال محدد للحالة ينبغي أن تكون أمدية الأثمونات متسقة، وبالتالي فإن كل أثمون مضاف أثناء تطبيق الأداة 1 ينبغي حذفه أثناء حذف الأداة 1 في المستهلك JPSEC.

وقد يستحسن، في بعض التطبيقات، أن يستخدم المستهلك JPSEC الأدوات JPSEC المتعددة على نحو مختلف عما ورد ذكره آنفاً. على سبيل المثال قد يختار المستهلك JPSEC أن يستخدم أدوات متعددة في ترتيب مختلف أو أن يتجاوز بعض الأدوات أثناء الاستخدام. كما يفضل المستهلك JPSEC تطبيق بعض الأدوات JPSEC دون أن يحذفها، كأن يتحقق من توقيع رقمي دون أن يزيله. وينبغي توخي الحذر في هذه الحالات من أجل ضمان ألا يؤدي تغيير الترتيب أو تجاوز بعض البيانات إلى نتائج خاطئة أو غير متوقعة. ولا يوصى بهذا السلوك إلاّ إذا كان التطبيق JPSEC محصناً تماماً ضد مثل هذه الاحتمالات المتشعبة.



الشكل 7 – استعمال أدوات JPSEC متعددة

6.5 الأدوات JPSEC

1.6.5 قواعد تركيب الأدوات JPSEC

هناك نمطان من الأدوات JPSEC كما ورد سابقاً: الأدوات JPSEC المعيارية وتتحدد في النماذج المعيارية لطريقة الحماية الوارد وصفها في الفقرة 8.5، وتعرف أيضاً بالأدوات JPSEC المعيارية، والأدوات JPSEC غير المعيارية وتتحدد في سلطة التسجيل JPSEC أو من خلال تطبيق JPSEC خاص يستند إلى رقم معرف هويتها وتسمى بأدوات سلطة التسجيل JPSEC أو أدوات JPSEC المحددة من قبل المستعمل على التوالي. وترد قواعد تركيب الأدوات JPSEC المعيارية في الفقرة 2.6.5، وقواعد تركيب الأدوات JPSEC غير المعيارية في الفقرة 3.6.5.

وتظهر قاعدة تركيب الأدوات JPSEC في الشكل 8، وفيها ثلاثة أجزاء تدل على:

1) الأداة المستخدمة وهويتها؛
2) مكان استخدام الأداة وبنية منطقة التأثير؛
3) كيفية استخدام الأداة وتفاصيل إضافية عن مجال المعلمة.

وكمثال، لدى استخدام هذه القواعد التركيبية، ستحدد قاعدة أداة JPSEC أداة فك التشفير اللازم استعمالها (ماهية الأداة) في أقل مكونة استبانة واقعة في مدى أثمونات ما (المكان) باستخدام خوارزمية فك التشفير AES بالأسلوب CBC ومجموعة محددة من متجهات التدميث ومفاتيحه (الكيفية).

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

الشكل 8 قاعدة تركيب الأداة JPSEC (الأداة [(i)])

t: نمط الأداة. تدل القيمة 0 في أول BAS على أداة JPSEC معيارية. وتدل القيمة 1 في أول بتة BAS على أداة JPSEC غير معيارية. ويستخدم هذا المجال البنية FBAS.

i: دليل حالة الأداة (يمكن استعماله كمعرف هوية مزيد). ويستخدم هذا المجال البنية RBAS.

ID: قيمة تعرف هوية الأداة JPSEC رقم *i*. وفيما يتعلق بالأدوات المعيارية JPSEC، فإن المعرف ID_T = ID وهو يتألف من 8 بتات ويحدد نمط النموذج المعياري. وفيما يتعلق الأدوات JPSEC غير المعيارية، فإن المعرف ID_{RA} = ID، وهو معرّف في الشكل 10 والجدول 8.

L_{ZOI}: طول المنطقة ZOI بالأثمونات (دون L_{ZOI}) ويستخدم هذا المجال البنية RBAS.

ZOI: منطقة تأثير الأداة JPSEC رقم *i*.

L_{PID}: طول P_{ID} بالأثمونات (دون L_{PID}). ويستخدم هذا المجال البنية RBAS.

PID: معلمات الأداة JPSEC رقم *i*.

الجدول 5 – قيم معلمات الأداة JPSEC

المعلمة	الحجم (بالبتات)	القيم
t	8 + 8 * n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 2)$ $(2^{7+7*n} - 1)$, reserved
ID	8، إذا t = 0 متغير، إذا t = 1	انظر الجدول 6 انظر الشكل 10 والجدول 8
L_{ZOI}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
ZOI	متغير	انظر الفقرة 7.5
L_{PID}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
P_{ID}	متغير	الجدول 7 إذا t = 0 بإدارة سلطة التسجيل JPSEC إذا t = 1

وكل أداة JPSEC مزودة بقواعد التركيب التالية: يبيّن الأثمون الأول ما إذا كانت الأداة JPSEC معيارية أم غير معيارية ويخصص لها معرف حالة. ثم يأتي معرف هوية الأداة **ID**، وتليه المعلمة L_{ZOI} التي تدل على طول منطقة مجال التأثير ZOI التالية وعلى منطقة التأثير ذاتها التي تشير إلى مكان استخدام الأداة JPSEC في تدفق البيانات. ثم ترد المعلمة L_{PID} التي تدل على طول مجال المعلمة التالية P_{ID} وهي مجال إرسال معلمة واحدة أو أكثر للأداة JPSEC.

ويستخدم الأثمون الأول من الأداة بنية FBAS ذات الأثمون الواحد التي تمثل أول بتة BAS فيها نمط الأداة، t، حيث تدل القيمة 1 فيها على أداة JPSEC معيارية والقيمة 2 على أداة JPSEC غير معيارية. ويلي ذلك دليل الحالة، *i*، الذي يظهر مستعملاً البنية RBAS. ويكون دليل الحالة معرف هوية فريداً للأداة داخل التدفق المشفر ولا يتكرر ذلك في أي أداة أخرى في نفس التدفق حتى إذا اختلفت الأداة في قطعة الواسم SEC. ودليل الحالة هام تحديداً (وضروري) عند استخدام الوسوم INSEC لأن كل قطعة واسم INSEC تضم دليل حالة الأداة التي تنطبق عليها. ويوصى بأن تعطى أول أداة مطبقة على المستحدث JPSEC دليل حالة قيمته 1، وبأن يشار إلى كل حالة أداة إضافية تتابعياً كلما استخدمت في نظام الحماية.

إضافةً إلى ذلك، تزود كل أداة JPSEC برقم ID من 8 بتات في الأداة JPSEC المعيارية، ومن 32 بتة في الأدوات JPSEC غير المعيارية. وفيما يتعلق بالأدوات JPSEC المعيارية، يذكر الرقم ID النموذج المعياري المستخدم في طريقة الحماية، أي أنه يصف النموذج المعياري لفك التشفير والنموذج المعياري للاستيقان والنموذج المعياري للتظليل. وفيما يتعلق بالأدوات JPSEC غير المعيارية، تدل البتة الأولى على ما إذا كانت أداة سلطة تسجيل JPSEC أم أداة JPSEC يحددها المستعمل. وفي كلتا الحالتين، يدل الرقم ID على الأداة المحددة. وتستطيع سلطة التسجيل JPSEC أن تضمن فرادة الأرقام ID الصحيحة. غير أن تطبيقاً JPSEC يستعمل أرقام ID يحددها المستعمل يخاطر باحتمال اختيار رقم ID يستعمله تطبيق JPSEC آخر، لذا ينبغي توخي الحذر في هذا الاستعمال.

وعند تطبيق كل أداة JPSEC على المستحدث JPSEC، يتم تحديث مجال المعلمة P_{SEC} المبين في الجدول 2. فمثلاً، يضم مجال المعلمة P_{SEC} المعلمة I_{max} التي تحدد أكبر دليل حالة مستخدم للأدوات في التدفق المشفر JPSEC. فعند استخدام أداة جديدة، يجب تخصيص دليل حالة فريد لها. وقد يحيل حامي JPSEC إلى المعلمة I_{max} المعطاة في مجال المعلمة P_{SEC} من أجل تحديد دليل الحالة لتخصيصه للأداة JPSEC. ويمكنه أن يختار مثلاً قيمة أكبر من القيمة I_{max} الجارية بمقدار واحد. وبالتالي ينبغي أن تزداد القيمة I_{max} في نظام الحماية بمقدار واحد أيضاً.

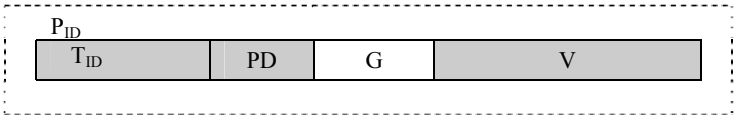
2.6.5 الأداة JPSEC المعيارية

تستخدم الأداة JPSEC المعيارية قاعدة تركيب الأداة JPSEC الواردة في الفقرة 1.6.5 والمبينة في الجدول 8، حيث نمط الأداة هو t = 0، وحجم معرف الهوية 8 بتات. وتستند الأدوات المعيارية JPSEC إلى النماذج المعيارية لطريقة الحماية التي يرد وصفها في الفقرة 8.5. ولهذه النماذج ثلاثة أنماط؛ ويتحدد النمط الذي تستعمله الأداة في معرف هوية الأداة، ID_T = ID الذي يستخدم القيم المبينة في الجدول 6.

الجدول 6 – قيم معرف هوية النموذج المعياري لأداة معيارية JPSEC (ID_T)

القيم	النموذج المعياري لطريقة الحماية
0	محجوز
1	نموذج معياري لفك التشفير
2	نموذج معياري للاستيقان
3	نموذج معياري للتظليل
4	الأداة NULL
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

يتخذ مجال المعلمة P_{ID} في حالة الأدوات المعيارية JPSEC البنية الواردة في الشكل 9. وتضم المعلمة P_{ID} أربعة مجالات رئيسية هي: النموذج المعياري لطريقة الحماية T، ومجال معالجتها PD، وتحببها G، وقائمة قيمها V. وترد قواعد تركيب كل من هذه المجالات في الفقرات 8.5 و9.5 و10.5 و11.5، على التوالي. ونصف هذه المجالات مجتمعةً الأداة المستخدمة. ويصف النموذج المعياري لطريقة الحماية T طريقة الحماية الخاصة بالنموذج المعياري لفك التشفير أو النموذج المعياري للاستيقان أو النموذج المعياري للتقطيع المحدد في معرف هوية الأداة المعيارية. وقد يحدد أيضاً الأداة NULL. وفي هذه الحالة لا يستخدم أي نموذج معياري وظائف أخرى. فعلى سبيل المثال، قد تتحدد منطقة التأثير من أجل إظهار مناطق الصورة وأمدية الأثمونات المقابلة لها. ويصف مجال المعالجة PD المجال الذي تستخدم فيه طريقة الحماية. ويصف التحبب G درجة التحبب التي تستخدم فيها طريقة الحماية. وتضم قائمة القيم V قائمة بالقيم التي قد تحتاجها كل طريقة حماية مع تحبب أكثر دقةً. وفيما يتعلق بالنموذج المعياري لفك التشفير، يمكن استعمال قائمة القيم في تحديد مجموعة تحبب أكثر دقةً لقيم التدميث التي ينبغي استعمالها. وفيما يتعلق بالنموذج المعياري للاستيقان، تضم قائمة القيم مجموعة من قيم الشفرات MAC أو التواقيع الرقمية. أما فيما يتعلق بالنموذج المعياري للتقطيع، فتضم قائمة القيم مجموعة قيم التقطيع. وفي جميع الحالات تشتمل قائمة القيم على تحبب القيم المحدد في مجال التحبب G.



الشكل 9 – قواعد تركيب المعلمات (P_{ID}) في الأدوات المعيارية JPSEC (t = 0)

T_{ID}: معلمات النموذج المعياري الخاصة بأداة JPSEC معيارية مع معرف هوية النموذج المعياري D_{IT}.

PD: مجال المعالجة في أداة JPSEC معيارية.

G: التحبب في أداة JPSEC معيارية.

V: قائمة القيم لأداة معيارية JPSEC، مثل متجهات التدميث أو القيم MAC أو التواقيع الرقمية أو قيم التقطيع تبعاً لمعرف هوية النموذج المعياري.

علماً بأن النموذج المعياري يعتمد على النموذج ID، بينما مجال المعالجة والتحبب وقائمة القيمة مستقلة عن النموذج ID.

الجدول 7 – قيم معلمات أداة معيارية JPSEC

المعلمة	الحجم (بالبتات)	القيمة
T_{ID}	0، إذا $4 = ID_T$ وإلاّ فمتغير	لا يوجد انظر 8.5
PD	متغير	انظر 9.5
G	24	انظر 10.5
V	متغير	انظر 11.5

3.6.5 الأداة JPSEC غير المعيارية

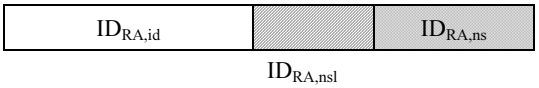
قد يكون من المفيد في بعض الحالات تزويد تطبيق JPSEC بمقدرة استخدام أداة تتجاوز الأدوات JPSEC المعيارية. وتتوفر هذه المقدرة من خلال استعمال أداة JPSEC غير المعيارية. مما يمكّن من استخدام عناصر كثيرة من الأدوات JPSEC المعيارية بما فيها المنطقة ZOI والنماذج المعيارية JPSEC لكنها تضيف إمكانية استخدام المعلمات بطريقة مختلفة مرفقة بقيمة معرف هوية الأداة.

وتستعمل الأداة JPSEC غير المعيارية قواعد تركيب الأدوات JPSEC الواردة في الفقرة 1.6.5 والمبينة في الشكل 8، حيث نمط الأداة هو t = 1. ويتألف معرف الهوية ID_{RA} من حيز للاسم ورقم معرف الهوية كما هو محدد في الشكل 10 والجدول 8.

وأدوات JPSEC غير المعيارية صنفان، هما:

1) أدوات سلطة التسجيل JPSEC: وهي الأدوات JPSEC غير المعيارية التي تحدد سلطة التسجيل نظام إشارتها.
2) الأدوات JPSEC التي يحددها المستعمل: الأدوات JPSEC غير المعيارية التي يحدد التطبيق نظام إشاراتها.

ويشار إلى هذين الصنفين من أدوات JPSEC غير المعيارية باستخدام معرف الهوية $ID_{RA,id}$ المؤلف من 32 بتة والمبين في الجدول 9. ومعرفات الهوية التي تبدأ ببتة قيمتها 0 محددة من سلطة التسجيل، أما تلك التي تبدأ ببتة قيمتها 1 فمحددة من تطبيق JPSEC ما.



الشكل 10 – قواعد تركيب ID_{RA}

$ID_{RA,id}$: معرف هوية أداة في أداة سلطة تسجيل وأداة يحددها المستعمل.

$ID_{RA,nsl}$: طول المجال $ID_{RA,ns}$ مقدراً بالأثمونات. ويستخدم هذا المجال البنية RBAS.

$ID_{RA,ns}$: سلسلة تحتوي على حيّز اسم أداة سلطة التسجيل أو الأداة التي يحددها المستعمل.

الجدول 8 – قيم المعلمات في قواعد تركيب المعرف ID_{RA}

المعلمة	الحجم (بالبتات)	القيم
$ID_{RA,id}$	32	انظر الجدول 9
$ID_{RA,nsl}$	8 + 8 * n (RBAS)	$0 \ldots (2^{7+7*n} - 1)$
$ID_{RA,ns}$	متغير	سلسلة تحتوي على حيز الاسم

الجدول 9 – قيم معرفات الهوية في الأدوات JPSEC غير المعيارية ($ID_{RA.id}$)

$ID_{RA,id}$	الدلالة
0x00 00 00 00 ... 0x7F FF FF FF	أداة سلطة تسجيل JPSEC. تدير سلطة التسجيل JPSEC القيم.
0x80 00 00 00 ... 0xEF FF FF FF	أداة JPSEC يحددها المستعمل. يمكن لتطبيق JPSEC ما أن يحدد القيم.
0xF0 00 00 00 ... 0xFF FF FF FF	قيم محجوزة لاستعمالات المنظمة ISO.

المجال $ID_{RA.ns}$ في أدوات سلطة التسجيل هو حيز اسم سلطة التسجيل (RA) التي سجلت لديها هذه الأداة. وبما أن لكل RA حيز اسم فريداً فإن المجالين $ID_{RA.id}$ و$ID_{RA,ns}$ يستعملون معاً من أجل تحديد هوية أداة RA. والمجال $ID_{RA,ns}$ في الأدوات التي يحددها المستعمل يختاره المصنعون.

وللحد من احتمالات تصادم معرفات الهوية. يوصى بأن يحرص المصنعون على الفرادة عند اختيارهم لحيز الاسم، كأن يختاروا اسم مجال منظمتهم أو شركتهم مثلاً. لكن يلاحظ فيما يتعلق بالأدوات التي يحددها المستعمل أنه قد يتعذر ضمان فرادة حيز الاسم، وبالتالي يمكن حدوث تصادم بالمعرفات وينبغي توخي الحذر عند استخدام، الأدوات التي يحددها المستعمل.

ويستعمل المجال P_{ID} في إرسال معلمة واحدة أو أكثر خاصة بالأداة JPSEC غير المعيارية رقم *i*. ولا يعطى نسق المجال P_{ID} بأكمله في مجال تطبيق المعيار JPSEC. وفي حال استخدام سلطة تسجيل يسجل النسق فيها مع معرف الهوية. وإذا لم تستخدم سلطة تسجيل وكانت الأداة محددة من المستعمل، عندئذٍ لا يتحدد إلاّ طول هذا المجال، وتقع مسؤولية استخدامه بطريقة ملائمة على المستعملين.

غير أن النظام JPSEC يوفر البنى التركيبية التي تحددها الأدوات JPSEC المعيارية من أجل استعمالها في المجال P_{ID} لأغراض الأدوات JPSEC غير المعيارية. ويمكن لأداة JPSEC غير معيارية مثلاً استعمال نماذج معيارية لطريقة الحماية ومجال المعالجة والتحبب ومجالات قائمة القيم الواردة في الفقرات 8.5 و9.5 و10.5 و11.5، على التوالي.

وقواعد التركيب هذه مرنة جداً وقادرة على توفير تنوع كبير من تقنيات الأمن مثل تكاملية بيانات الصورة والتحكم في النفاذ وطرق الحماية الصحيحة. ولذا فإنها تقدم مجموعة كبيرة من الوظائف البسيطة والمختصرة في نفس الوقت.

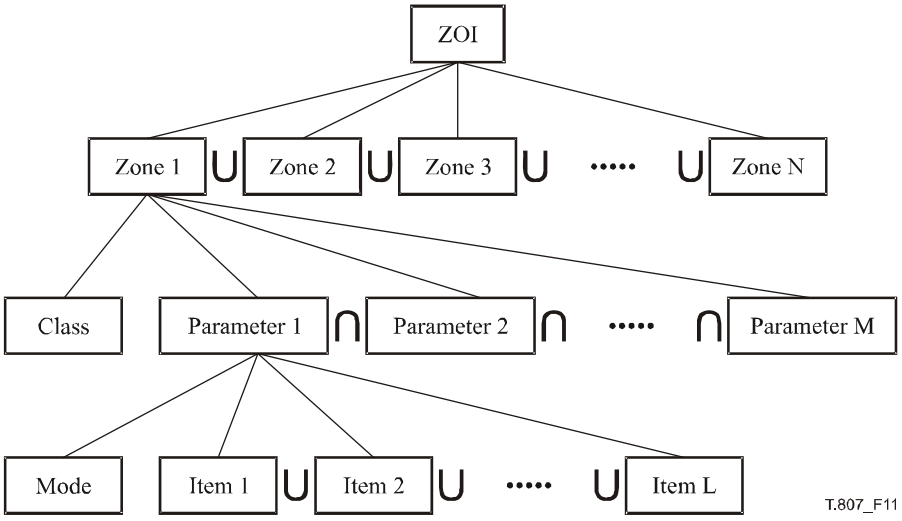
7.5 قواعد تركيب منطقة التأثير (ZOI)

1.7.5 مقدمة

يمكن استخدام منطقة التأثير (ZOI) في وصف منطقة تغطية أداة JPSEC. وتسمى البيانات الواقعة داخل منطقة التغطية (التي تحددها المنطقة ZOI) بالبيانات المتأثرة. وتستعمل أدوات JPSEC المعيارية المنطقة ZOI لوصف منطقة تغطيتها. ويمكن للأدوات JPSEC غير المعيارية أن تستخدم المنقطة ZOI في وصف منطقة تغطيتها أو أن تلجأ لطريقة أخرى. وفي حال استخدام طريقة بديلة يكون طول المنطقة ZOI القيمة 0، أي أنه لا يوجد.

وتصف منطقة التأثير (ZOI) منطقة تغطية كل أداة JPSEC. ويمكن وصف منطقة التغطية هذه باستعمال معلمات تتعلق بالصورة، مثل الاستبانة أو منطقة الصورة؛ أو باستعمال معلمات تتعلق بغير الصورة مثل قطع التدفق المشفر أو أدلة الرزم. وفي الحالات التي تستخدم فيها المعلمات المتعلقة بالصورة والمعلمات المتعلقة بغير الصورة معاً، فإن المنطقة ZOI تصف التقابل بين هاتين المنطقتين. فعلى سبيل المثال، يمكن استعمال المنطقة ZOI في الدلالة على أن الاستبانات ومنطقة الصورة التي تحددها المعلمات المتصلة بالصورة تقابل قطع التدفق المشفر التي تحددها المعلمات المتصلة بغير الصورة. وهذا يمكّن من استخدام المنطقة ZOI كبيانات شرعية تدل على مواقع بعض أجزاء الصورة في التدفق المشفر JPSEC.

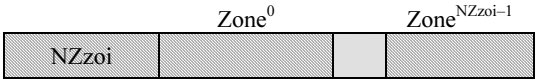
ويوضح الشكل 11 البنية النظرية للمنطقة ZOI التي تضم منطقة فرعية واحدة أو أكثر. وفي حال وجود مناطق متعددة ضمن منطقة ZOI واحدة، فإن هذه الأخيرة تتحدد في اتحاد المناطق. ويعني ذلك أنه ينبغي استعمال الأداة JPSEC في جميع هذه المناطق. ويتم وصف كل منطقة فرعية في المنطقة ZOI من خلال ثلاث وحدات أساسية هي: صنف الوصف وأسلوب المعلمة وبنود المعلمة (القيم). وتعرف هذه التوصية | المعيار الدولي صنفين للوصف هما: صنف الوصل المتعلق بالصورة وصنف الوصف المتعلق بغير الصورة. ويمكن تحديد هذه المعلمات باستعمال عدد من الأساليب مثل القيمة الوحيدة أو القيم المتعددة أو المدى. وترد قيم أو بنود المعلمات وفقاً للأسلوب.



الشكل 11 – بنية مفهوم منطقة التأثير

2.7.5 قواعد تركيب المنطقة ZOI

يبين الشكل 12 قواعد تركيب منطقة التأثير. وقد تضم هذه المنطقة الكبرى منطقة فرعية واحدة أو أكثر. وقد تكون فارغة أيضاً وفي مثل هذه الحالة يكون NZ_{zoi} يساوي 0. وعند حدوث ذلك، يتحدد تأثير الأداة بوسائل أخرى مثل الواسم INSEC أو المعلمات التي تحددهما أداة حماية JPSEC غير المعيارية.



الشكل 12 – قاعدة تركيب المنطقة ZOI

NZ_{zoi}: عدد المناطق. يستخدم هذا المجال البنية RBAS.

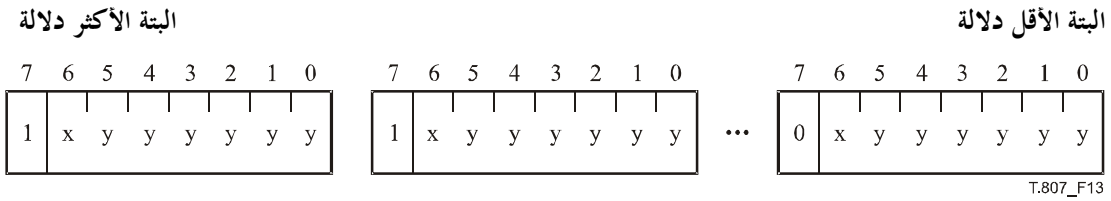
$Zone^k$: منطقة. وتحدد بنيتها في الفقرة 3.7.5.

الجدول 10 – قيم معلمات مجال منطقة التأثير (ZOI)

المعلمة	الحجم (بالبتات)	القيم
NZzoi	8 + 8 * n (RBAS)	$0 \ldots (2^{7+7*n} - 2)$ $(2^{7+7*n} - 2)$، محجوز
$Zone^k$	متغير	انظر 3.7.5

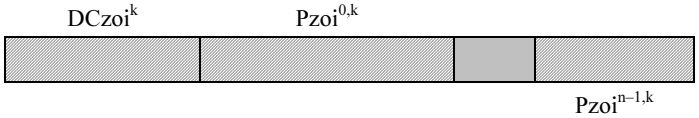
3.7.5 قواعد تركيب المنطقة

تضم المنطقة مؤشر مجال صنف وصف المنطقة تليه معلمات ذلك الصنف. ويستخدم صنف وصف المنطقة البنية FBAS. وكما هو مبين في الشكل 13، تدل البتة الثانية الأكثر دلالة من كل أثمون، ويشار إليها بـ "x"، على استخدام صنف الوصف. وتحدد هذه التوصية | المعيار الدولي صنفين للوصف هما: صنف وصف يتعلق بالصورة وصنف وصف يتعلق بغير الصورة (انظر الجدول 12). ويحدد الجدولان 13 و14 أرقام مؤشر المجال لأغراض صنف الوصف المتعلق بالصورة وصنف الوصف المتعلق بغير الصورة على التوالي. ويدل تسلسل البتات الست المشار إليها بـ "y" في كل أثمون يلي علم صنف الوصف على استخدام وصف محدد في صنف الوصف المعني. وتدل القيمة 1 للبتة في رقم بتة ما في كل صنف على وجود مجال المعلمة المقابلة. ويجب أن يكون عدد المعلمات نفس عدد مؤشرات مجال صنف وصف المنطقة ذات القيمة 1. ويجب أن تظهر حسب الترتيب المبين لمؤشر مجال الصنف. ولصنف وصف المنطقة عدد متغير من الأثمونات: وعندما تساوي البتة الأكثر دلالة 1، فإن أثموناً آخر لصنف وصف المنطقة يلي وتساوي البتة الأكثر دلالة (MSB) في الأثمون الأخير لصنف الوصف 0. وفي حال استخدام صنفي الوصف المتصل بالصورة والمتصل بغير الصورة، ينبغي عندئذٍ أن ترد أثمونات صنف الوصف المتصل بالصورة قبل أثمون صنف الوصف المتصل بغير الصورة. وعند تمثيل عدد من البنود التي تستخدم هذه البنية، فإن البند الأول في القائمة يقابل البتة الأكثر دلالة (MSB) المتاحة في الأثمون الأول.



الشكل 13 – بنية صنف وصف المنطقة (DCzoi)

ويبين الشكل 14 قواعد تركيب المنطقة.



الشكل 14 – قواعد تركيب منطقة مكونة من صنف الوصف ومجموعة معلمات واحدة أو أكثر

DC_{zoi}^k: صنف وصف المنطقة رقم k. ويستخدم هذا المجال البنية FBAS.

$DC_{zoi}^{i,k}$: معلمات المنطقة وفقاً لصنف وصف المنطقة المحددة (DCzoik). راجع الفقرة 6.7.5

يحدد الصنف DC_{zoi}^{k} عدد (n) المجالات الموجودة لصنف وصف المنطقة، استناداً إلى عدد البتات ذات القيمة واحد. ويوجد لكل مجال صنف وصف منطقة مجال معلمة منطقة $P_{zoi}^{i,k}$ واحد. وتظهر هذه المجالات تتابعياً حسب نفس ترتيب ظهور الأعلام في DC_{zoi}^{k}.

الجدول 11 – قيم معلمات المنطقة

المعلمة	الحجم (بالبتات)	القيم
$DCzoi^{k}$	متغير (FBAS)	تتغير وفق مجموعة القيم المبنية في الجدول 12
$Pzoi^{i,k}$	متغير	انظر الفقرة 6.7.5 للاطلاع على قواعد تركيب هذا المجال

الجدول 12 – قيمة مؤشر صنف الوصف

القيمة	صنف الوصف
0	صنف وصف متعلق بالصورة. تتحدد أرقام البتات التالية في الجدول 13
1	صنف وصف متعلق بغير الصورة. تتحدد أرقام البتات التالية في الجدول 14

الجدول 13 – صنف الوصف المتعلق بالصورة

رقم البتة	الدلالة
1	منطقة الصورة
2	الرقعة (الرقع) كما يعرفها الجزء 1 من المعيار JPSEC 2000
3	سوية (سويات) الاستبانة كما يعرفها الجزء 1 من المعيار JPSEC 2000
4	الطبقة (الطبقات) كما يعرفها الجزء 1 من المعيار JPSEC 2000
5	المكونة (المكونة) كما يعرفها الجزء 1 من المعيار JPSEC 2000
6	المنطقة (المناطق) كما يعرفها الجزء 1 من المعيار JPSEC 2000
7	الوسم (الوسوم) TRLCP (الموقعة – الاستبانة – الطبقة – المكونة – المنطقة)
8	الرزمة (الرزم) كما يعرفها الجزء 1 من المعيار JPSEC 2000
9	النطاق الفرعي (النطاقات الفرعية) كما يعرفها الجزء 1 من المعيار JPSEC 2000
10	فدرة (فدر) الشفرة كما يعرفها الجزء 1 من المعيار JPSEC 2000
11	منطقة (مناطق) ROI
12	معدل البتات
13	يعرفه المستعمل. وتتحدد التفاصيل بوسائل أخرى (مثال: المعرف JPSEC ID)
	جميع القيم الأخرى محجوزة

الجدول 14 – صنف الوصف المتعلق بغير الصورة

رقم البتة	الدلالة
1	الرزمة (الرزم) كما يعرفها الجزء 1 من المعيار JPSEC 2000
2	مدى (أمدية) الأثمونات (المملوءة) (بدءاً من الأثمون الأول بعد أول واسم SOD)
3	مدى (أمدية) الأثمونات (المملوءة) (بدءاً من الأثمون الأول بعد أول واسم SEC)
4	مدى (أمدية) الأثمونات غير المملوءة عند استخدام عملية الملء
5	الوسم (الوسوم) TRLCP (الرقعة – الاستبانة – الطبقة – المكونة – المنطقة)
6	قيمة (قيم) التشوه
7	الأهمية النسبية
8	يعرفه المستعمل. وتتحدد التفاصيل بوسائل أخرى (مثال: المعرف JPSEC ID)
	جميع القيم الأخرى محجوزة

أدلة الرزم في الرقعة مرقمة تتابعياً ولذلك قد لا تكون فريدة داخل الرقعة. إضافةً إلى ذلك قد تعود أدلة الرزم في الرقعة إلى الصفر عند تجاوز القيمة القصوى البالغة 65535. ولهذا السبب يرد وصف دليل الرزمة مع المزيد من التفاصيل. فعندما لا تتجاوز أدلة الرزم في رقعة ما 65535 رزمة فإن دليل الرزم الوارد في الجدول 13 يتحدد من خلال دليل الرزم الوارد في المعلمة SOP Nsop حسب تعريضها في الجدول A.40 الوارد

في الجزء 1 من المعيار JPSEC 2000. وجدير بالذكر أنه في حال عدم تجاوز القيمة القصوى وقدرها 65536 يمكن تحديد رزمة JPSEC 2000 واحدة من خلال دليل الرقعة ودليل الرزمة فقط. أما عندما تتجاوز أدلة الرزم مقدار 65535 رزمة، فإنه يتعين على دليل الرزمة حسب الجزء 1 من المعيار JPSEC 2000 أن يعود من جديد إلى صفر. وفي هذه الحالة لا يصحح دليل الرزمة لتعريف الرزمة دون وقوع لبس وينبغي عدم استخدامه. ويوصى عندئذٍ باستعمال الوسم TRLCP بديلاً له. ويرجى ملاحظة أن خدمات الأمن التي تتطلب أدلة رزم فريدة حساسة في حال رجوع دليل الرزمة إلى الصفر وتكرار التعداد.

وعندما يستخدم الوسم TRLCP ينبغي تحديد نسقه في مجال المعلمة P_{SEC} المبينة في الجدول 2.ويتحدد خصوصاً نسق الوسم TRLCP من خلال مجال المعلمة P_{TRLCP} الواردة في الجدول 4 يحدد حجم الوسوم TRLCP في المنطقة ZOI.

ويمكن لصنف الوصف المتعلق بغير الصورة أن يكون له أيضاً مجموعة مجالات متعددة في نفس الوقت. وفي هذه الحالة، يكون لأساليب المجالات المتعددة للمعلمة نفس عدد البنود (يرد لاحقاً استثناء واحدة لهذه القاعدة) وتتقابل هذه البنود بين البعض واحداً واحداً في نفس الترتيب. فإذا استخدمت المنطقة أمدية أثمونات وأمدية رزم مثلاً. ينبغي أن يكون لكل منها نفس عدد بنود المدى حيث يقابل أول مدى أثمونات أول مدى رزم وهكذا دواليك.

وهناك استثناء واحد للقاعدة الواردة أعلاه والتي تشترط نفس عدد البنود في كل مجال. ويكون ذلك عندما يضم أحد المجالات f1 البند 1 الذي يحدد مدى من البنود (كما يصفه مدى الأسلوب في الفقرة 6.7.5) وعندما يضم هذا المدى N عنصراً وعندما يتمدد مجال آخر، f2، من خلال قائمة من N بنداً. وهذه البنود N التي يحددها المدى في f1 تتقابل فيما بينها واحداً واحداً مع البنود N المعددة في المجال f2. وبناءً عليه يمكن إرفاق مدى بنود ما ببندٍ واحد أو ببنود متعددة (مدى لكل بند في المدى).

ويشار إلى الأثمونات إما في الأثمون الأول الذي يلي أول واسم SOD وإما في الأثمون الأول الذي يلي أول واسم SEC. وفي كلتا الحالتين يتم وسم الأثمون الأول على أنه أثمون 0.

وتوفر مجالات التشوه (مجالات التشوه والأهمية النسبية) مقدرة بيان أهمية المناطق التي تحددها المنطقة ZOI. وتحدد معلمة التشوه مساهمة قطعة البيانات المحددة في التجفيف من التشوه في سواء في مجموعة رزم أو في مدى أثمونات أو في منطقة تتعلق بالصورة المحددة. ويعبّر عن التشوه من حيث مجموع الخطأ التربيعي باستعمال الوصيف المكون من أثمون واحد أو الوصف المكون من الأثمونين المذكورين في المعلمة Mzoi. ويمكن استخدام معلمة التشوه النسبي من أجل تحديد الأهمية النسبية لقطع البيانات المحددة باستخدام قيم الأثمون الواحد أو الأثمونين أو الأربعة أثمونات المذكورة في Mzoi. ويرد المزيد من التفاصيل والأنساق الخاصة بهذه المجالات في الفقرة 2.3.7.5.

ويحدد الوسم TRLCP رقعة الرزمة المحمية واستبانتها وطبقتها ومكونتها ومنطقتها في التدفق المشفر. ويستخدم هذا الوسم في المنطقة ZOI في تحديد هذه المعلمات لأن هذه المعلمات قد تكون صعبة الإدراج في تدفق مشفر محمي.

ويلاحظ أنه عند استخدام الأوصاف المتعلقة بالصورة فقط، يمكن إغلاق المجال. وهكذا لا حاجة لتمثيل أوصاف تتعلق بغير الصورة في حال عدم استعمالها.

1.3.7.5 مجالات مدى الأثمونات

يسمح صنف الوصف المتعلق بغير الصورة للمنطقة ZOI أن توصف في أمدية الأثمونات. وينبغي عموماً استعمال العنصرين الثاني والثالث من الجدول 14 في تمثيل أمدية الأثمونات الخاصة بغالبية الأدوات مثل الاستيقان والتشفير/فك التشفير دون ملء. غير أن بعض طرائق الحماية مثل التشفير/فك التشفير مع الملء تغيّر طول البيانات. ومن الضروري عند حدوث ذلك تحديد كل من مدى الأثمونات المملوء ومدى الأثمونات غير المملوء أو مدى الأثمونات الأصلي. وفي هذه الحالة يتحدد مدى الأثمونات المملوء من خلال العنصرين الثاني والثالث من الجدول 14 تبعاً لاحتياجات أداة الحماية. (جدير بالملاحظة أنه لا يمكن استخدام هذين العنصرين معاً). وإضافةً إلى ذلك يتحدد مدى الأثمونات غير المملوء في العنصر الرابع من الجدول 14. وينبغي تحديد مدى الأثمونات غير المملوء باستعمال نفس أسلوب الوصف المستعمل في مدى الأثمونات المملوء نفس عدد البنود. وينبغي أن تتقابل هذه البنود مع بعضها البعض واحداً واحداً في نفس الترتيب.

2.3.7.5 مجال التشوه ومجال الأهمية النسبية

يوفر مجالا التشوه والأهمية النسبية مقدرة الإشارة إلى أهمية المناطق التي تحددها المنطقة ZOI.

ويستخدم مجال التشوه في إرفاق التشوه بالمنطقة التي تحددها ZOI. وتحدد قيمة التشوه الخطأ التربيعي للتشوه الكلي (مجموع الخطأ التربيعي) الذي قد ينجم إذا لم تتوافر المنطقة المصاحبة من أجل فك التشفير. وخطأ التشوه التربيعي الكلي هو قياس تشوه أساسي يستخدم في معالجة الصورة والإشارات الفيديوية، ويستخدم أيضاً في استنباط متوسط الخطأ التربيعي المشترك (MSE) للتشوه وقيمة الذروة لنسبة الإشارة إلى الضوضاء (PSNR). ويعبّر عن مجال التشوه باستعمال وصف الأثمون الواحد أو وصف الأثمونين حيث يرد لاحقاً وصف هذين النوعين. ويشار إلى اختيار أحد النوعين من خلال قيمة المعلمة Mzoi التي تحدد طول هذا المجال. ويمكن استخدام مجال الأهمية النسبية في وصف الأهمية النسبية في مختلف المناطق التي تحددها المعلمات ZOI المصاحبة دون ربطها بالضرورة بقياس تشوه معين. ويشار إلى طول مجال الأهمية النسبية أيضاً في المعلمة Mzoi. وترد دراسة المجالات مع المزيد من التفاصيل في الفقرات التالية.

1.2.3.7.5 مجال التشوه في أثمون واحد

يعبر عن مجموع الخطأ التربيعي للتشوه باستخدام مجال التشوه في أثمون واحد مع تمثيل بالفاصلة شبه العائمة. وتتوزع البتات الثماني الموجودة في مجال التشوه كما هو مبين في الشكل 15 والجدول 15 من أجل توفير التسوية الملائمة بين الدقة والمدى الدينامي. ويلاحظ أن بتة الإشارة غير ضرورية إذ أن التشوه غير سالب. ومن أجل تغطية مدى دينامي كافٍ، يستخدم الأساس 16 و4 بتات للأس (exp). ويعبر عن الجزء العشري من اللوغاريتم (m) باستعمال 4 بتات. وبالتالي تعطى القيمة D، التشوه الكلي في العلاقة التالية:

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

حيث قيمة m تقع في المدى $0 \le m \le 15$ وقيمة exp في المدى $0 \le exp \le 15$. وتتمثل قيمة تشوه قدرها 0 كالتالي m = 0 وexp = 0، علماً بأن مجال التشوه يساوي صفر. ويعطي توزيع 4 بتات للجزء العشري من اللوغاريتم m دقة مقدارها $1/32 = ½ \times (1/2^4)$ أو حوالي 3%. وعند إعطاء 4 بتات للأس واستعمال الأساس 16، يمتد المدى الديناميي من 0 إلى max، حيث يعطى max في العلاقة m = 15 وexp = 15 مما يعادل تشوهاً قدره $15 \times 16^{15} = 1{,}7 \times 10^{19}$.

exp	M

الشكل 15 – قاعدة تركيب مجال التشوه

exp: أس قيمة مجال التشوه (الأساس 16)

m: البند العشري للوغاريتم قيمة مجال التشوه

الجدول 15 – قيم معلمات مجال التشوه

المعلمة	الحجم (بالبتات)	القيم
exp	4	15 ... 0
m	4	15 ... 0

يلاحظ أن هذا النسق للتشوه يمكّن من إنجاز مقارنة بين تشوهين لتحديد الأكبر منهما من خلال مقارنة قيمتي التشوه كسمة دون علامة. ولإجراء هذه المقارنة تحديداً لا حاجة إلى التحويل من نسق الفاصلة شبه العائمة إلى مجموع التشوه الفعلي من أجل تحديد قيمة التشوه الأكبر أو الأصغر. وقد تسهل هذه الخاصية المعالجة في عدة تطبيقات.

2.2.3.7.5 مجال التشوه بأثمونين

يعبّر عن قيم التشوه في نسق الأثمونين بعدد مؤلف من أثمونين في نسق الفاصلة شبه العائمة. ويعرف هذا النسق على النحو التالي. يستخدم هذا النسق في الملحق 1.1.1.E (المعادلة E.3) بالتوصية | المعيار الدولي ISO/IEC 15444-1 | ITU-T Rec. T.800 من أجل التعبير عن حجم مرحلة تكمية المعيار JPSEC 2000. ويحتوي كل عدد من 16 بتة على الأس (5 بتات) والجزء العشري للوغاريتم (11 بتة) من قيمة القياس. وتعطى قيمة الفاصلة العائمة للقياس تحديداً في المعالة التالية:

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

حيث ε رقم صحيح دون علامة ناتج عن البتات الخمس الأولى الأكثر دلالة في المعلمة وμ رقم صحيح دون علامة ناتج عن البتات الإحدى عشرة المتبقية. وتعادل الحالة الحاصلة $V = \infty$ الحالة μ = 0 وε = 31. ويلاحظ أن القيم التي تقل عن التمثيل توضع على صفر.

ε	μ

الشكل 16 – قاعدة تركيب مجال التشوه

ε: أس قيمة مجال التشوه المؤلف من أثمونين.

μ: جزء عشري للوغاريتم قيمة مجال التشوه المؤلف من أثمونين.

الجدول 16 – قيم معلمة مجال التشوه

المعلمة	الحجم (بالبتات)	القيم
ε	5	31 ... 0
μ	11	$(1 - {}^{11}2)$ ... 0

لا تتحدد خوارزمية حساب ε وμ باعتبارها جزءاً أساسياً من التوصية | المعيار الدولي. وتنفذ تقنية ممكنة الخطوات التالية (يعطى مثال لتحويل الرقم 12.25). إذا $V = 0$، قيمة $\varepsilon = \mu = 0$. وإلاّ فينبغي:

- تحويل V إلى عدد اثنيني ($1100{,}01_2 = 12{,}25_{10}$)؛
- تقييس العدد؛ ويعني ذلك أنه ينبغي وجود رقم 1 إلى يسار النقطة الاثنينية والضرب في القوة المناسبة وقدرها اثنان من أجل تمثيل القيمة الأصلية. فالشكل المعياري للقيمة 1100,01 هو $1{,}10001 \times 2^3$؛
- الأس هو القوة 2 ممثلاً بترميز زائد. وانحياز الأس هو 15: ولذلك يتمثل الأس في هذا المثال بالقيمة (10010_2) 18_{10}؛
- الجزء العشري من اللوغاريتم يمثل البتات الأكثر دلالة، ما عدا البتة التي على يسار النقطة الاثنينية التي لها دائماً قيمة واحد وبالتالي لا تحتاج إلى تخزين؛ وبالإمكان إضافة أصفار للحصول على 11 بتة. وفي هذا المثال يكون الجزء العشري 10001000000.

3.2.3.7.5 مجال الأهمية النسبية

يمكن استخدام مجال الأهمية النسبية r في وصف الأهمية النسبية بين وحدات تشفير مختلفة دون ربطها بالضرورة بقياس تشوه محدد. وهذا يمكن من وصف الأهمية النسبية أو الأولوية بين وحدات التشفير دون التصريح عن نسبة زيادة أهمية وحدة ما نسبةً إلى الوحدات الأخرى. وتتحدد هذه الأهمية النسبية للبيانات المصاحبة من خلال مجال مكون من n أثمون يوفر 2^{8n} ترتيباً محتملاً كما يبين الشكل 17 والجدول 17 حيث عدد الأثمونات n في هذا المجال محدد من المعلمة Mzoi. فمثلاً عند استعمال مجال أهمية نسبية بأثمون واحد يتوفر ما مجموعه 256 ترتيباً ممكناً وبطريقة مماثلة تقابل زيادة القيم زيادة أهمية مجال التشوه.

الشكل 17 – قاعد تركيب مجال الأهمية النسبية

r: قيمة الأهمية النسبية

الجدول 17 – قيم معلمات مجال الأهمية النسبية

المعلمة	الحجم (بالبتات)	القيم
r	n * 8	$(1 - {}^{8n}2)$ ... 0

4.2.3.7.5 شرح إضافي لمجال التشوه ومجال الأهمية النسبية

نظراً إلى أن مقدار أهمية مجال تشوه في الأثمون الواحد ومجال الأهمية النسبية للأثمون الواحد يتناسب طرداً مع قيم هذين المجالين، فإنه من الممكن إجراء مقارنات بين وحدتي هذه البيانات بنفس الطريقة بغض النظر عما إذا كان مجال التشوه يحدد تشوهاً فعلياً أم أهمية نسبية؛ مما قد يسهل التطبيقات.

وقد تتحدد الرأسيات باستخدام مجالي التشوه أو الأهمية النسبية، وفقدان بعض أنماط من البيانات مثل رأسيات أجزاء الرقعة الرئيسية أو الرأسية SEC، يمنع فك تشفير بيانات الصورة ذات الصلة. وقد يرى المستحدث JPSEC أن يضيف بعض التشوه إلى البيانات باستخدام:

1) أعلى قيمة تشوه (محددة لاحقاً) للإشارة إلى الرأسية أو البيانات الحساسة؛ أو
2) وصف التشوه الإجمالي الذي قد ينتج في حال عدم قابلية الصورة أو جزء منها لفك التشفير.

وعندئذٍ يكون للمستحدث بعض المرونة في كيفية الإشارة إلى الرأسيات.

وأعلى قيمة تشوه في مجالات الأثمون الواحد هي أثمون متسلسل من الأرقام 1 (0xFF). وجدير بالملاحظة أن هذه القيمة هي أعلى قيمة تشوه ممكن لكل من مجموع الخطأ التربيعي لمجال التشوه ذي الأثمون الواحد ومجال الأهمية النسبية ذي الأثمون الواحد. وأعلى قيمة تشوه لمجال التشوه ذي الأثمونين هي أثمونين هي أثمونين متسلسلين من الأرقام 1 (0xFFFF). أما أعلى قيمة لمجال الأهمية النسبية طوله n أثموناً فهي قيمة n أثمون متسلسلة من الأرقام 1.

5.2.3.7.5 استخدام مشترك لمجال التشوه ومجال الأهمية النسبية

يمكن استخدام مجال التشوه ومجال الأهمية النسبية معاً في وصف المنطقة التي تحددها المعلمة ZOI. وفي هذه الحالة يحدد كلٍ من المجالين تشوه الخطأ التربيعي، لكن مجال التشوه يحدد التناقص المتزايد في التشوه بينما يحدد مجال الأهمية النسبية التشوه الإجمالي. وخصوصاً وأن مجال التشوه يحدد التناقص المتزايد في التشوه الذي تنتجه المنطقة ZOI إذا فك تشفيرها. وذلك يفترض أن جميع المعلومات المطلوبة لفك تشفير المنطقة ZOI متيسرة ويركز على التناقص المتزايد في التشوه الذي تنتجه المنطقة ZOI. ويحدد مجال الأهمية النسبية التشوه الإجمالي الذي يحدث في حال عدم تيسر المنطقة ZOI أي أنه يحدد التشوه الإجمالي الذي يحصل في حال عدم تيسر المنطقة ZOI المعنية من أجل فك التشفير من خلال حساب ليس فقط قيمة المنطقة ZOI فقط (كما يذكر مجال التشفير) ولكن حساب التشوه الناتج أيضاً لأن الأجزاء الأخرى من تدفق البتات المضغوط المرتبط بالمنطقة ZOI غير قابلة لفك التشفير. ويعطي التشوه الإجمالي المصاحب لمناطق ZOI مختلفة قياساً مفيداً للأهمية النسبية للمناطق ZOI المختلفة. وعند استعمال المجالين فإنهما يستعملان نفس التعابير الحسابية للتشوه كما هو مبين في مجال التشوه.

3.3.7.5 مجال معدل البتات

يستعمل مجال معدل البتات في تحديد المنطقة المحمية في مجال معاملات الموجات الصغيرة. وهو يحدد سويات البتات الأكثر دلالة التي يحدد هذا المجال معدل بتاتها المضغوطة. ويتم انتقال البتات الأكثر دلالة بإجراء عملية استمثال تشوه المعدل المحددة في الجزء 1. مثال، إذا كانت قيمة معدل البتات 2,5، فإن المنطقة المحمية تضم البتات الأكثر دلالة لمعاملات الموجات الصغيرة التي يبلغ معدل بتاتها المضغوطة 2,5 بتة للبيكسل الواحد. وتظهر قاعدة تركيب مجال معدل البتات في الشكل 18 والجدول 18. ويعطى معدل البتات المحدد في العلاقة:

$$R = I_R + F_R/16$$

مثلاً، يتمثل معدل بتات قدره صفر بالعلاقة $I_R = 0$ و$F_R = 0$وقيمة معدل بتات قدره 2,5 بالعلاقة $I_R = 2$ و$F_R = 8$.

I_R	F_R

الشكل 18 – قاعدة تركيب مجال معدل البتات

I_R: جزء العدد الصحيح من معدل البتات المحدد.

F_R: الجزء الكسري من معدل البتات المحدد.

الجدول 18 – قيم معلمات مجال معدل البتات

المعلمة	الحجم (بالبتات)	القيم
I_R	4	15 ... 0
F_R	4	15 ... 0

4.7.5 العلاقة بين المعلمات المتعددة

1.4.7.5 لمحة عامة

عندما يكون لصنف الوصف المتعلق بالصورة عدة مجالات معدّة في نفس الوقت فإن المنطقة الناتجة هي تقاطع هذه المجالات. فمثلاً قد تحدد منطقة ما أخفض سوية استبانة في الرقعة الثانية. ويمكن تحديد وحدة المجالات باستعمال المناطق المتعددة في ZOI.

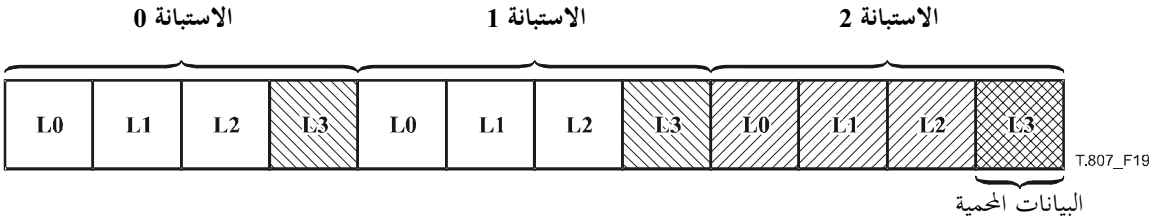
ويمكن أيضاً لصنف الوصف المتعلق بغير الصورة أن يكون له عدة مجالات منشطة في نفس الوقت. وعند حدوث ذلك، يكون للأساليب الخاصة بمختلف مجالات المعلمات نفس عدد البنود (باستثناء واحد لهذه القاعدة يرد أدناه)، وتتقابل هذه البنود بين بعضها البعض واحداً واحداً. فإذا كانت المنطقة على سبيل المثال تستخدم أمدية الأثمونات وأمدية الرزم، ينبغي أن يكون لكل منها نفس عدد بنود الأمدية، حيث مدى الأثمونات الأول يقابل أول مدى رزم وهكذا دواليك.

وهناك استثناء واحد للقاعدة المذكورة أعلاه بشأن شرط نفس عدد البنود في كل مجال. ويكون ذلك عندما يحتوي أحد المجالات f1 بنداً واحداً يحدد مدى من البنود (كما يصفه أسلوب المدى الوارد في 6.7.5) حيث يضم هذا المدى N عنصراً، وعندما يتحدد مجال آخر f2 من خلال قائمة تضم N بنداً. وفي هذه الحالة، فإن المجال f1 الذي لا يضم إلا بنداً واحداً (المدى) يفسر باعتباره قائمة من N بنداً. وهذه البنود N التي يحددها المدى في f1 تتقابل واحداً واحداً مع البنود N المعددة في f2. ولذلك يمكن إرفاق بنود مع بند واحد أو بنود متعددة (واحد لكل بند في المدى).

2.4.7.5 أمثلة

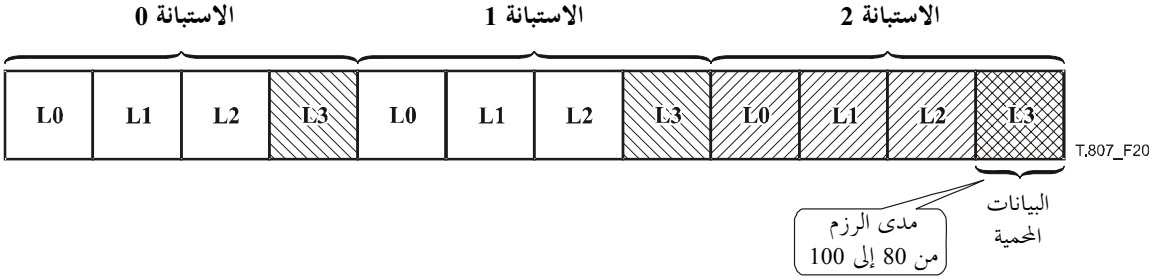
بإمكان بنية صنف وصف المنطقة أن تضم كما يوضح الشكل 11 مجالات متعددة موضوعة في نفس الوقت حيث المجالات N هي أوصاف تتعلق بالصورة ($D_i^1, D_i^2, ..., D_i^N$) والمجالات M أوصاف تتعلق بغير الصورة ($D_n^1, D_n^2, ..., D_n^M$). ويمكن فهم دلالتها كالتالي $\{D_i^1 \cap D_i^2 \cap ... \cap D_i^N\} = D_n^1 = D_n^2 = ... = D_n^M$ حيث إن تقاطع الأوصاف المتعلقة بالصورة N تتقابل مع الأوصاف M المتعلقة بغير الصورة وأن الأوصاف M المتعلقة بغير الصورة تتقابل بين بعضها البعض واحداً واحداً أيضاً. وتتوضح هذه العلاقة لاحقاً من خلال الأمثلة الثلاثة الواردة أدناه.

في المثال الأول، يحتوي وصف المنطقة على وصفين متعلقين بالصورة: أحدهما للاستبانة 2 والآخر للطبقة 3. وفي هذه الحالة فإن البيانات المحمية تقع في منطقة تقاطع الاستبانة 2 مع الطبقة 3 كما في الشكل 19.



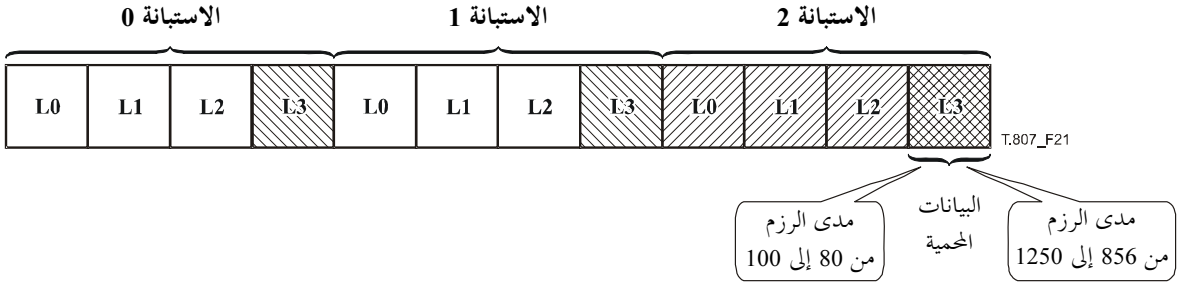
الشكل 19 – مثال منطقة التأثير باستخدام الأوصاف المتعلقة بالصورة

وفي المثال الثاني، يضم وصف المنطقة وصفين متعلقين بالصورة (وهما الاستبانة 2 والطبقة 3) ووصف متعلق بغير الصورة (وهو مدى الرزم -100 80). وفي هذه الحالة تقع البيانات المحمية في منطقة تقاطع الاستبانة 2 مع الطبقة 3. ومن ناحية أخرى يدل على أن البيانات المحمية توجد في مدى الرزم 80 و100.



الشكل 20 – مثال منطقة التأثير باستخدام وصفي الصورة وغير الصورة

وفي المثال الثالث، يضم وصف المنطقة وصفين متعلقين بالصورة (وهما الاستبانة 2 والطبقة 3) ووصفين متعلقين بغير الصورة (وهما مدى الرزم 80-100 ومدى الأثمونات 856-1250). ومرةً أخرى تقع البيانات المحمية عند تقاطع الاستبانة 2 مع الطبقة وفي مدى الرزم من 80 إلى 100. ومن ناحية أخرى تقع منطقة الرزم والبيانات المحمية في مدى الأثمونات 856-1250.



الشكل 21 – مثال ثان لمنطقة ZOI باستخدام وصفي الصورة وغير الصورة

5.7.5 حماية جميع البيانات التي تلي الواسم SEC

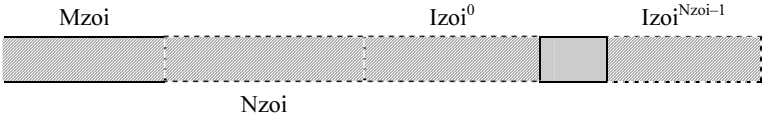
تركز الدراسة الواردة أعلاه على توفير خدمات الحماية للتدفق المشفر JPSEC 2000. غير أنه ينبغي حماية الكثير من عناصر الرأسية الرئيسية بما فيها التشوير JPSEC، ويمكن استعمال المنقطة ZOI وطرق الحماية لهذا الغرض.

ويمكن تحديداً استخدام أسلوب مدى الأثمونات لصنف الوصف المتعلق بغير الصورة في تحديد ضرورة استعمال أداة JPSEC في كل البيانات التي تلي الواسم SEC. وكما ورد سابقاً فإن الأثمون الأول للرأسية SEC هو الأثمون 1 للدلالة على مدى الأثمونات. وتضم البيانات التي تلي الواسم SEC والتي يمكن حمايتها، القطعة SEC والجزء الأكبر من الرأسية الرئيسية. ويلاحظ أنه يجوز نقل كامل الرأسية الرئيسية JPSEC 2000 ما عدا قطعة الواسم SIZ إلى ما بعد الواسم SEC ومن ثم يمكن حمايتها باستخدام النهج المذكور أعلاه. وإذا طلبت حماية قطعة الواسم JPSEC 2000 SIZ، توجب أن يتم ذلك على مستوى أعلى، أي في طبقة نسق الملف مثلاً.

وينبغي عموماً أن تكون الأدوات JPSEC الخاصة بحماية القطعة SEC أول أدوات في القطعة SEC. وذلك يمكّن المستهلك من معالجة بيانات القطعة SEC التي يمكن استعمالها بعدئذٍ في معالجة المتبقي من التدفق المشفر.

6.7.5 قاعدة تركيب معلمة وصف المنطقة (P_{zoi})

يبين الشكل 22 قاعدة تركيب معلمة وصف المنطقة ZOI.



الشكل 22 – قاعدة تركيب معلمة وصف المنقطة ZOI

Mzoi: أسلوب وصف المنقطة ZOI. ويستخدم هذا المجال البنية FBAS.

Nzoi: عدد البنود Izoi. ويستخدم هذا المجال البنية FBAS.

Izoi^i: بند.

الجدول 19 – قيم المعلمة Pzoi^i

المعلمة	الحجم (بالبتات)	القيم
Mzoi	متغير (FBAS)	انظر الجدول 20
Nzoi	0 8 + 8 * n (RBAS)	إذا كانت البتة رقم 2 في Mzoi تساوي 0 2 ... $(2^{7+7*n} - 1)$
Izoi^i	متغير	يرتبط بالأسلوب المحدد في Mzoi

الجدول 20 – قيم معلمات Mzoi

رقم بنة البنية FBAS	القيمة (بالبتات)	الدلالة
1	0	المناطق المحددة محمية بالأداة JPSEC
	1	تتمة المناطق المحددة محمية
2	0	يتحدد بند واحد
	1	يتحدد عدة بنود
3، 4	00	أسلوب المستطيل. منطقة على شكل مستطيل حيث يحدد أول زوج قيم الزاوية العلوية اليسرى، وثاني زوج قيم الزاوية السفلية اليمنى بحيث يتم احتواء كلتا الزاويتين. وتمثل أول قيمة لكل زاوية الوضع الأفقي والقيمة الثانية الوضع الشاقولي. ويبدأ ترقيم الأدلة بـ 0 ويستخدم الجدول المرجعي المعرف في الجزء 1 من المعيار JPSEC 2000.
	01	أسلوب المدى. مدى من القيم حيث تحدد القيمة الأولى بداية الدليل والقيمة الثانية نهايته. علماً بأن هاتين القيمتين تقعان ضمن المدى.
	10	أسلوب الدليل. ويحدد قيمة (قيم) واحدة.
	11	أسلوب الحد الأقصى. ويحدد القيمة القصوى.

الجدول 20 – قيم معلمات Mzoi

رقم بنة البنية FBAS	القيمة (بالبتات)	الدلالة
5، 6	00	المعلمة $Izoi^i$ تستعمل عدد صحيح من 8 بتات
	01	المعلمة $Izoi^i$ تستعمل عدد صحيح من 16 بتة
	10	المعلمة $Izoi^i$ تستعمل عدد صحيح من 32 بتة
	11	المعلمة $Izoi^i$ تستعمل عدد صحيح من 64 بتة
7، 8	00	توصف المعلمة $Izoi^i$ في بعد واحد
	10	توصف المعلمة $Izoi^i$ في بعدين
	01	توصف المعلمة $Izoi^i$ في ثلاثة أبعاد
9	0	يستخدم أسلوب تخالف الأطوال: يحدد أول تخالف نسبةً إلى أطوال
	1	الأثمونات المجاورة التالية. ويلغي وجود هذا العلم الأساليب المحددة في البتتين 3 و4
		جميع القيم الأخرى محجوزة

وعند استخدام الوسوم TRLCP، يتحدد طولها في المعلمة P_{TRLCP} كما هو محدد في الجدول 4. وفي هذه الحالة يبطل مفعول البتتين 5 و6 من المعلمة Mzoi.

ويمكن استخدام أسلوب تخالف الأطوال من أجل تمثيل فعّال لسلسلات قطع متتابعة مثل سلسلات أمدية أثمونات متعاقبة. وتحدد القيمة الأولى التخالف الأولي وتحدد القيم اللاحقة طول كل قطعة تلي. وإذا استخدم هذا المجال لتمثيل عدد n من القطع ينبغي أن تتخذ المعلمة عندئذٍ القيمة $n + 1$.

8.5 قاعدة تركيب النموذج المعياري طريقة الحماية

1.8.5 اعتبارات عامة

تضم النماذج المعيارية لطريقة الحماية معلمات تتعلق بأدوات JPSEC محددة ورد وصفها في الفقرة 1.6.5. وتستخدم مثلاً في الأدوات المعيارية JPSEC الواردة في الفقرة 2.6.5. كما يمكن استخدامها في الأدوات JPSEC غير المعيارية التي يرد وصفها في الفقرة 3.6.5. وهناك ثلاثة أنواع من النماذج المعيارية لطريقة الحماية هي: نموذج لفك التشفير ونموذج الاستيقان ونموذج التقطيع. ويتحدد النموذج الذي تستخدمه الأداة المعيارية JPSEC في معرف الهوية على النحو المبين في الجدول 6، وهنا أيضاً في الجدول 21 مع الإحالة إلى الفقرات التي يرد فيها تعريف الأدوات.

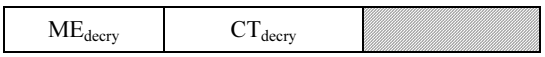
ويصف النموذج المعياري T لطريقة الحماية المصاحب لمجال المعالجة PD ودرجة التحبب G، وقائمة القيم V للأدوات JPSEC كيفية استخدام الأدوات JPSEC كما ترد في الفقرة 2.6.5.

الجدول 21 – قيم معرف هوية النموذج المعياري (IDT)

القيم	النموذج المعياري لطريقة الحماية
0	محجوز
1	نموذج لفك التشفير. انظر الفقرة 2.8.5.
2	نموذج للاستيقان. انظر الفقرة 3.8.5
3	نموذج للتقطيع. انظر الفقرة 6.8.5
4	الأداة NULL
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

2.8.5 نموذج معياري لفك التشفير ($T_{decry} = T$، إذا كانت $t = 0$ و$ID = 1$)

يستخدم النموذج المعياري لفك التشفير T_{decry} في إعلام مفكك التشفير بكيفية فك تشفير التدفق المشفر الواصل. ويبين الشكل 23 قاعدة تركيب نموذج فك التشفير. ويبين الجدول 22 الأطوال الخاصة بالنموذج المعياري لفك التشفير وقيم رموزه ومعلماته.



الشكل 23 – قاعدة تركيب نموذج فك التشفير

ME_{decry}: علم محاكاة واسم خاطئة يدل على حدوث محاكاة واسم خطأ في البيانات المشفرة. وقد تؤثر محاكاة الواسم الخاطئة بالمقابل على الامتثال لمفككات تشفير الجزء 1 من المعيار JPSEC 2000. ويستخدم هذا المجال البنية FBAS.

CT_{decry}: تعرف هوية نمط المشفر.

CP_{decry}: معلمة التشفير.

الجدول 22 – قيم معلمة النموذج المعياري لفك التشفير

المعلمة	الحجم (بالبتات)	القيمة
ME_{decry}	8 + 8 * n (FBAS)	الجدول 23
CT_{decry}	16	الجدول 24
CP_{decry}	متغير	إذا $CT_{decry} < 0x6000$، انظر الفقرة 1.2.8.5 إذا $0x6000 \leq CT_{decry} < 0xC000$، انظر الفقرة 2.2.8.5 إذا $CT_{decry} \geq 0xC000$، انظر الفقرة 3.2.8.5

الجدول 23 – قيم علم محاكاة الواسم (ME_{decry})

القيم	نمط الطريقة
01xx xxxx	لا تحتوي البيانات المشفرة على محاكاة واسم خاطئة
00xx xxxx	تحتوي البيانات المشفرة على محاكاة واسم خاطئة
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

قيمة علم محاكاة الواسم بالتغيب هي 0. ويجوز إعطاء القيمة 1 لهذا العلم من أجل الدلالة على أن البيانات المشفرة JPSEC لا تضم محاكاة واسم خاطئة. ويجوز لمستحدث JPSEC اختيار ترك هذا العلم على قيمته بالتغيب 0.

الجدول 24 – قيم معرف هوية المشفر (CT_{decry})

القيم	نوع المشفر
0 ... 0x5FFF	مشفر فدرة (انظر الجدول 25)
0x6000 ... 0xBFFF	مشفر تدفق (انظر الجدول 26)
0xC000 ... 0xFFFF	مشفر لا تناظري (انظر الجدول 27)

الجدول 25 – قيم معرف هوية مشفر فدرة

القيم	نوع المشفر
0x0000	(no encryption) NULL
0x0001	(ISO/IEC 18033-3) AES
0x0002	(ISO/IEC 18033-3) TDEA
0x0003	(ISO/IEC 18033-3) MISTY1
0x0004	(ISO/IEC 18033-3) Camellia
0x0005	(ISO/IEC 18033-3) CAST-128
0x0006	(ISO/IEC 18033-3) SEED
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

الجدول 26 – قيم معرف هوية مشفر تدفق (CT_{decry})

القيم	نوع المشفر
0x6000	(ISO/IEC 18033-4) SNOW 2
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

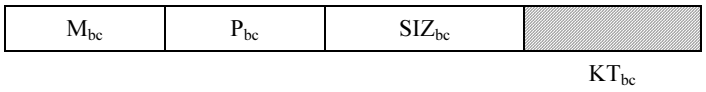
الجدول 27 – قيم معرف هوية مشفر لا تناظري (CT_{decry})

القيم	نوع المشفر
0xC000	(ISO/IEC 18033-2) RSA-OAEP
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

1.2.8.5 نموذج معياري لمشفر فدرة (CP_{decry} خاص بمشفرات الفدرة)

يستخدم النموذج المعياري لمشفر الفدرة في إعلام مفكك تشفير الفدرة بكيفية فك تشفير التدفق المشفر الواصل. ويبين الشكل 24 أسلوب مشفر الفدرة وأسلوب الملء وحجم الفدرة والمعلومات المتعلقة بالمفاتيح.

ويمكن لبعض أساليب مشفر الفدرة استخدام متجهات التدميث. وفيما يتعلق بهذه الأساليب تتحدد متجهات تدميث الأدوات باستعمال مجال تحبب الأداة (G) الذي يرد وصفه في 10.5 ومجال قائمة القيم (V) الوارد في 11.5. وعلى وجه التحديد لا تستعمل متجهات التدميث إلاّ لأغراض الأساليب مع معرف هوية ID $M_{bc} > 0x80$ مثل الأساليب CBC وCFB وOFB وCTR. وفي حالة الأسلوب CTR، ليس بالحقيقة متجه تدميث (IV) بل عدّاد ويجب إعطاء حجم قيمة التدميث المحدد في قائمة القيم V قيمة حجم الفدرة SIZ_{bc}.



الشكل 24 – قاعدة تركيب نموذج معياري لمشفر الفدر

M_{bc}: أسلوب مشفر الفدر. وتدل أول بتة على استعمال متجهات التدميث مع هذه الأداة. إذا كانت $M_{bc} < 0x8$، لا تستعمل متجهات التدميث، وإلاّ يتطلب الأسلوب قيمة متجهة تدميث واحد أو أكثر.

P_{bc}: أسلوب ملء.

SIZ_{bc}: حجم الفدرة بالأثمونات.

KT_{bc}: نموذج معياري للمفاتيح (انظر 5.8.5) يتضمن معلومات عن المفاتيح المستعملة في تشفير الفدر.

الجدول 28 – قيم نموذج معياري لمشفر فدرة

المعلمة	الحجم (بالبتات)	القيم
M_{bc}	6	الجدول 29
P_{bc}	2	الجدول 30
SIZ_{bc}	8	256 ... 1
KT_{bc}	متغير	انظر الفقرة 5.8.5

الجدول 29 – قيم أسلوب معياري لمشفر فدرة (Mbc)

المعلمة	نمط الأسلوب
0	محجوز
0x xxxx	أساليب تستعمل دون متجه التدميث
1x xxxx	أساليب تستعمل مع متجه التدميث
x0 xxxx	البتات غير مملوءة
x1 xxxx	البتات مملوءة
0x 0001	(ISO/IEC 10116) ECB
1x 0010	(ISO/IEC 10116) CBC
1x 0011	(ISO/IEC 10116) CFB
1x 0100	(ISO/IEC 10116) OFB
1x 0101	(ISO/IEC 18033-2) CTR
	جميع القيم الأخرى محجوزة لاستعمال المنظمة ISO

الملاحظة 1 – ينبغي توخي الحذر في تطبيقات جميع الأساليب، لأن التطبيقات الخاطئة قد تؤدي إلى سرعة الأعطاب. ويلاحظ حدوث تداخلات في المعلومات حتى في التطبيقات الصحيحة للأسلوب ECB عند ظهور فدر متشابهة. وترد الخطوط التوجيهية في المعيار ISO/IEC 10116.

الملاحظة 2 – لا تنطبق القيم الواردة في الجدول 30 إلا عندما يحدد الأسلوب M_{bc} في الجدول 29 أن البتات مملوءة. أما عندما تكون البتات غير مملوءة فإن المعلمة P_{bc} تتخذ القيمة 00.

الجدول 30 – أسلوب فك لتشفير الفدر (Pbc)

القيم	نمط الملء
00	Ciphertext stealing (RFC 2040)
01	PKCS#7-padding (PKCS#7)
	جميع القيم محجوزة لاستعمالات المنظمة ISO

الملاحظة 3 – يتعين لدى استعمال الملء وضع تصميم دقيق للنظام من أجل تفادي احتمال وقوع أخطاء الأمن، مثل الهجمات، شفرة مختارة.

2.2.8.5 نموذج معياري لمشفر التدفق (CP_{decry} لمشفرات التدفق)

يستخدم النموذج المعياري لمشفر التدفق في إعلام مفكك تشفير التدفق بكيفية فك تشفير التدفق المشفر الواصل. ويبين الشكل 25 قاعدة تركيب النموذج المعياري لمشفر التدفق. ويبين الجدول 31 قيم النموذج المعياري لمشفر التدفق.

وتتحدد متجهات تدميث مشفر التدفق باستعمال مجال تحبب الأداة (G) الذي يرد وصفه في الفقرة 10.5، ومجال قائمة القيم (V) الواردة في الفقرة 11.5. ويعطى حجم متجه التدميث المحدد في قائمة القيم V قيمة حجم المفتاح المحدد في النموذج المعياري لمعلومات المفاتيح KT_{sc}.

KT_{sc}

الشكل 25 – قاعدة تركيب النموذج المعياري لمشفر التدفق

KT_{sc}: نموذج معياري لمعلومات المفاتيح (5.8.5). ويتضمن معلومات عن المفاتيح التي يستخدمها مشفر التدفق.

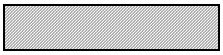
الجدول 31 – قيم النموذج المعياري لمشفر التدفق

المعلمة	الحجم (بالبتات)	القيم
KT_{sy}	متغير	انظر 5.8.5

3.2.8.5 نموذج معياري لمشفر لا تناظري (CP_{decry} لمشفرات لا تناظرية)

يستخدم النموذج المعياري لمشفر لا تناظري في إعلام مفكك التشفير اللاتناظري بكيفية فك تشفير التدفق المعياري الواصل. وبين الشكل 26 قاعد تركيب النموذج المعياري لمشفر لا تناظري. ويبين الجدول 32 قيم النموذج المعياري لمشفر لا تناظري.

وفيما يتعلق بالأدوات التي تستخدم النموذج المعياري لمشفر لا تناظري يحدد مجال تحبب الأداة (G) التحبب الذي يستخدم معه المشفر. لكن لا يستعمل قائمة القيم (V) في تمثيل أي قيم. وبالتالي يضبط عدد العناصر (N_v) في مجال قائمة القيم على القيمة 0.



الشكل 26 – قاعدة تركيب النموذج المعياري لمشفر لا تناظري

KT_{sy}: نموذج معياري لمعلومات المفاتيح (انظر 5.8.5). ويتضمن معلومات عن المفاتيح التي يستخدمها المشفر اللاتناظري.

الجدول 32 – قيم النموذج المعياري لمشفر تناظري

المعلمة	الحجم (بالبتات)	القيم
KT_{sy}	متغير	انظر 5.8.5

3.8.5 نموذج معياري للاستيقان ($T = T_{auth}$، إذا كانت t = 0 وID = 2)

يستخدم النموذج المعياري للاستيقان T_{auth} في إعلام المتحقق بكيفية التحقق من صحة التدفق المشفر الواصل. وهناك ثلاثة أصناف رئيسية لطرائق الاستيقان هي: الاستيقان القائم على التقطيع، وعلى أساس خوارزمية التجفير والتواقيع الرقمية. ومن ناحية أخرى تسمى طريقتا التقطيع والتجفير "شفرة استيقان الرسالة" (MAC)، وتسمى عموماً قيمها المحسوبة المستخدمة في الاستيقان "قيم الشفرة MAC". وتبين قواعد تركيب النموذج المعياري للاستيقان في الشكل 27، ويعرض الجدول 33 الأحجام وقيم الرموز والمعلمات الخاصة بالنموذج المعياري للاستيقان.

والاستيقان في تطبيقات أمن كثيرة هو أهم خدمات الأمن. وحتى عندما تكون السرية هي خدمة الأمن المستهدفة، ينبغي إضافة الاستيقان إليها للوقاية من الهجمات. ويوصى خصوصاً باستيقان أجزاء من قطعة الواسم SEC. وإضافة إلى ذلك، يتم الاستيقان بشأن كل من معلمات النموذج المعياري للاستيقان (T_{auth}) والرسالة الواجب استيقانها. وعلى وجه التحديد، تحدد منطقة التأثير وجوب استيقان كل من المحتويات والمعلمات في النموذج المعياري للاستيقان (T_{auth}).

الشكل 27 – قاعدة تركيب النموذج المعياري للاستيقان

M_{auth}: طريقة الاستيقان.

P_{auth}: معلمات الاستيقان.

الجدول 33 – قيم معلمات النموذج المعياري للاستيقان

المعلمة	الحجم (بالبتات)	القيم
M_{auth}	8	الجدول 34
P_{auth}	متغير	إذا M_{auth} = 0، انظر 1.3.8.5 إذا M_{auth} = 1، انظر 2.3.8.5 إذا M_{auth} 2=، انظر 3.3.8.5

الجدول 34 – طرائق الاستيقان (Mauth)

القيم	الطريقة
0	الطريقة MAC القائمة على التقطيع
1	الطريقة MAC القائمة على التجفير
2	التوقيع الرقمي
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

1.3.8.5 الاستيقان القائم على التقطيع (P_{auth} في الشفرة MAC القائمة على التقطيع)

تستخدم شفرة الاستيقان MAC القائمة على التقطيع في إعلام المتحقق بكيفية التحقق من صحة التدفق المشفر الواصل. ويبين الشكل 28 قواعد تركيب النموذج المعياري القائم على التقطيع، ويعرض الجدول 35 قيم المعلمات.

وتتحدد قيم الشفرة MAC باستعمال مجال التحبب (G) للأداة الوارد في الفقرة 10.5 ومجال قائمة القيم (V) الوارد في الفقرة 11.5. ويجب ضبط حجم الشفرة MAC المحدد في قائمة القيم V على حجم الشفرة MAC الذي تحدده المعلمة SIZ_{HMAC}.

الشكل 28 – النموذج المعياري للاستيقان القائم على التقطيع

M_{HMAC}: معرف هوية شفرة الاستيقان القائمة على التقطيع.

H_{HMAC}: معرف هوية التقطيع.

KT_{HMAC}: نموذج معياري للمفتاح.

SIZ_{HMAC}: حجم الشفرة MAC (بالبتات).

الجدول 35 – قيم معلمات النموذج المعياري للاستيقان القائم على التقطيع

المعلمة	الحجم (بالبتات)	القيم
M_{HMAC}	8	الجدول 36
H_{HMAC}	8	الجدول 37
KT_{HMAC}	متغيرة	انظر الفقرة 5.8.5
SIZ_{HMAC}	16	65535 ... 0

الجدول 36 – معرف هوية طريقة الاستيقان القائم على التقطيع (MHMAC)

القيم	طريقة الاستيقان القائم على التقطيع
0	محجوزة
1	HMAC (ISO/IEC 9797-2)
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

الجدول 37 – معرف هوية وظيفة التقطيع (HHMAC)

القيم	وظيفة التقطيع
0	متغيرة
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)
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

يلاحظ أنه إذا كان طول المعلمة SIZ_{HMAC} أقل من الطول الاسمي للتقطيع، تكون الصيغة المبتورة المقابلة للبتات SIZ_{HMAC} الأولى للتقطيع.

2.3.8.5 النموذج المعياري للاستيقان القائم على خوارزمية التجفير (P_{auth} في الشفرة MAC القائمة على التجفير)

تستخدم الشفرة MAC للاستيقان القائم على خوارزمية التجفير في إعلام المتحقق بكيفية التحقق من صحة التدفق المشفر الواصل. ويمثل الشكل 29 النموذج المعياري لهذا الاستيقان ويبين الجدول 38 طول المفاتيح والتقطيع الموزع على مفاتيح محسوبة. ومثال لمخطط استيقان قائم على خوارزمية التجفير هو الشفرة CBC-MAC. وفي هذه التقنيات للتجفير بالفدر لأغراض الاستيقان، يكون طول متجه التدميث مساوياً لفدرة واحدة وقيمته 0. وحجم الفدرة هو القيمة بالتغيب للتجفير بالفدر. ويلاحظ أنه إذا كان حجم المعلمة SIZ_{CMAC} أقل من الحجم الاسمي لشفرة MAC للاستيقان القائم على خوارزمية التجفير تكون الصيغة المبتورة المقابلة لبتات SIZ_{CMAC} الأولى من الطريقة MAC.

ويلاحظ أن عدد بتات البيانات ليس مضاعفاً لحجم فدرة التجفير وبالتالي تكون فدرة الدخل الأخيرة فدرة جزئية من البيانات مرصوفة إلى اليسار مع أصفار مضافة من أجل تشكيل فدرة تجفير كاملة. ويلاحظ أيضاً أن الشفرة CBC-MAC لا تطبق إلا على البيانات ذات الطول الثابت والمعروف.

وتحدد القيم MAC باستعمال مجال تحبب (G) للأداة الوارد في 10.5 وقيمة مجال قائمة القيم (V) الذي يرد وصفه في 11.5. ويعطى طول قيمة الشفرة MAC المحددة في قائمة القيم V قيمة حجم الشفرة MAC المحدد في المعلمة SIZ_{CMAC}.

الشكل 29 – قاعدة تركيب النموذج المعياري للاستيقان القائم على التجفير

CA_{CMAC}: طريقة الاستيقان القائم على التجفير

C_{CMAC}: قيمة معرِّف هوية التجفير بالفدر

KT_{CMAC}: نموذج معياري للمفتاح

SIZ_{CMAC}: حجم الشفرة MAC (بالبتات)

الجدول 38 – قيم النموذج المعياري للشفرة MAC

المعلمة	الحجم (بالبتات)	القيم
CA_{CMAC}	8	الجدول 39
C_{CMAC}	8	الجدول 25
KT_{CMAC}	متغير	انظر 5.8.5
SIZ_{CMAC}	16	65535 ... 1

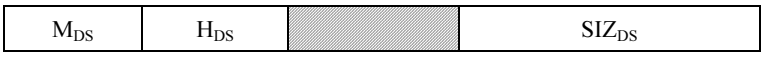
الجدول 39 – طريقة الاستيقان القائم على خوارزمية التجفير (C_{CMAC})

القيم	الطريقة
0	CBC-MAC MAC Algorithm 1 (ISO/IEC 9797-1)
1	CBC-MAC MAC Algorithm 2 (ISO/IEC 9797-1)
2	CBC-MAC MAC Algorithm 3 (ISO/IEC 9797-1)
3	CBC-MAC MAC Algorithm 4 (ISO/IEC 9797-1)
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

3.3.8.5 النموذج المعياري للتوقيع الرقمي (P_{auth} للتواقيع الرقمية)

يُستخدم التوقيع الرقمي في إعلام المتحقق بكيفية التحقق من صحة التدفق المشفر الواصل والتحقق من هوية المرسل من أجل تعرف الهوية وعدم الرفض. ويحدد الشكل 30 نموذجه المعياري، ويحدد الجدول 40 قيمه.

وتتحدد التواقيع الرقمية باستخدام مجال التحبب (G) الوارد في الفقرة 10.5 ومجال قائمة القيم (V) الوارد في الفقرة 11.5. ويعطى حجم قيمة التواقيع الرقمية المحددة في قائمة القيم V قيمة تناسب الحجم الذي تحدده المعلمة SIZ_{DS}. وبما أن حجم قائمة القيم ممثل بالأثمونات لا بالبتات يكون هذا الحجم هو أصغر عدد من الأثمونات قادر على استيعاب المعلمة SIZ_{DS}. وينبغي تمثيل كل قيمة بالبتات الأقل دلالة، وتوضع البتات الأكثر دلالة على القيمة 0.



KT_{DS}

الشكل 30 – قاعدة تركيب النموذج المعياري للتوقيع الرقمي

M_{DS}: طريقة التوقيع الرقمي.

H_{DS}: وظيفة التقطيع.

KT_{DS}: النموذج المعياري للمفتاح (انظر 5.8.5). ويتضمن جميع المعلومات المتعلقة بالمفتاح العمومي أو بالشهادة المطلوبة من أجل التحقق من التوقيع الرقمي.

SIZ_{DS}: حجم التوقيع الرقمي (بالبتات).

الجدول 40 – قيم النموذج المعياري للتوقيع الرقمي

المعلمة	الحجم (بالبتات)	القيم
M_{DS}	8	الجدول 41
H_{DS}	8	الجدول 37
KT_{DS}	متغير	انظر 5.8.5
SIZ_{DS}	16	65535 ... 0

الجدول 41 – طرائق التوقيع الرقمي (M_{DS})

القيم	الطريقة
1	RSA (ISO/IEC 14888-2)
2	Rabin (ISO/IEC 14888-2)
3	DSA (ISO/IEC 14888-3)
4	ECDSA (ISO/IEC 14888-3)
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

4.8.5 النموذج المعياري للتقطيع ($T_{hash} = T$ إذا كانت $t = 0$ و$ID = 3$)

يستخدم النموذج المعياري للتقطيع T_{hash} في إيصال المعلمات المستعملة في حساب التقطيع. ويبين الجدول 42 أحجام وقيم الرموز والمعلمات المتعلقة بالنموذج المعياري للتقطيع.

ويلاحظ أنه على عكس النموذج المعياري للاستيقان القائم على التقطيع المذكور في الفقرة 1.3.8.5 الذي يفترض استعمال التقطيع والمفتاح السري، فإن النموذج المعياري للتقطيع هذا لا يستخدم مفتاحاً. وعلى الرغم من أن هذا النموذج المعياري يُستخدم في كشف خطأ عارض أو تغيير طارئ في البيانات فإنه لا يقي من التأثير السيئ على البيانات. ومن أجل وقاية البيانات من هذه التأثيرات السيئة يجب استعمال نموذج معياري للاستيقان، إذ أن المفتاح السري المستعمَل في النموذج المعياري للاستيقان يقي البيانات من التأثيرات السلبية دون أن يكشفها.

وتتحدد قيم التقطيع باستعمال مجال تحبب الأدوات (G) المذكور في الفقرة 10.5 ومجال قائمة القيم (V) المذكور في الفقرة 11.5. وينبغي ضبط حجم قيمة التقطيع المحدد في قائمة القيم V على حجم قيمة التقطيع التي تحددها المعلمة SIZ_{hash}.

H_{hash}	SIZ_{hash}

الشكل 31 – قاعدة تركيب النموذج المعياري للتقطيع

H_{hash}: معرف هوية وظيفة التقطيع.

SIZ_{hash}: حجم قيمة التقطيع (بالأثمونات).

الجدول 42 – قيم معلمات النموذج المعياري للتقطيع

المعلمة	الحجم (بالبتات)	القيم
H_{hash}	8	الجدول 37
SIZ_{hash}	8	255 ... 0

5.8.5 النموذج المعياري لمعلومات المفتاح (KT)

يُستخدم النموذج المعياري لمعلومات المفتاح من أجل إرسال معلومات المفتاح. ويحدد الشكل 32 نموذجها المعياري، ويحدد الجدول 43 القيم.

LK_{KT}	KID_{KT}	G_{KT}	
			V_{KT}

الشكل 32 – قاعدة التركيب النموذجي المعياري لمعلومات المفتاح

LK_{KT}: طول المفتاح بالبتات.

KID_{KT}: معرّف هوية معلومات المفتاح. ويدل على معنى القيم الواردة في قائمة القيم V_{KT}. وفي النموذج المعياري لفك التشفير، ينبغي أن تكون هذه القيمة 2 (علماً بأن المعرف URI يتيح استنتاج المفتاح السرّي). وفي حالة التوقيع الرقمي تكون قيمة هذا المجال غير محددة.

G_{KT}: مجال التحبب من أجل تمثيل التحبب الذي تتغير فيه معلومات المفتاح.

V_{KT}: مجال قائمة ا لقيم من أجل تمثيل قائمة تغيير معلومات المفتاح.

يلاحظ في حالة المفتاح السري (نموذج معياري لفك التشفير) أنه لا معنى للمفتاح العمومي والشهادة: إذ ينبغي أن يتضمن النموذج المعياري للمفتاح بعض المعلومات عن موقع المفتاح (مثال: الموقع URI).

ويمكن تمثيل معلومات المفتاح بقيمة واحدة أو أكثر باستعمال مجال تحبب الأداة (G_{KT}) المذكور في الفقرة 10.5 ومجال قائمة القيم (V_{KT}) المذكور في الفقرة 11.5. ويحدد المجالان (G_{KT} وV_{KT}) معاً كيفية تطبيق قيم المفتاح الواردة في قائمة القيم (V_{KT}) على بيانات الصورة المحمية، كما يرد في الفقرتين 10.5 و11.5.

ويمكن لمعلومات المفتاح في قائمة القيم أن تأخذ أولاً الأشكال المحددة لها في الجدول 44. وإذا كان المعرف $KID_{KT} = 1$، تتحدد عندئذٍ كل قيمة بالنموذج المعياري للشهادة X.509 الواردة في الفقرة 1.5.8.5. أما إذا كان $KID_{KT} = 2$، فإن كل قيمة عندئذٍ تتحدد بموقع URI للشهادة أو للمفتاح السري.

الجدول 43 – قيم النموذج المعياري للمفتاح

المعلمة	الحجم (بالبتات)	القيم
LK_{KT}	16	65535 ... 1
KID_{KT}	8	الجدول 44
G_{KT}	24	انظر 5.10
V_{KT}	متغير	انظر 5.11

الجدول 44 – قيم معرف هوية معلومات المفتاح (KID_{KT})

القيم	معرِّف هوية معلومات المفتاح
0	محجوزة
1	الشهادة X.509 (ISO/IEC 9594-8)
2	موقع URI الخاص بالشهادة أو بالمفتاح السري
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

1.5.8.5 النموذج المعياري للشهادة X.509

الشكل 33 – قاعدة تركيب الشهادة X.509

ER_{KT}: قاعدة تشفير الشهادة X.509.

$LCER_{KT}$: طول الشهادة X.509 (CER_{KT}) بالأثمونات.

CER_{KT}: الشهادة X.509

الجدول 45 –قيم الشهادة X.509 (KI_{KT} إذا كانت $KID_{KT} = 2$)

المعلمة	الحجم (بالبتات)	القيم
ER_{KT}	8	0 ... 255 (انظر الجدول 46)
$LCER_{KT}$	16	65535 ... 1
CER_{KT}	متغير	–

الجدول 46 – قيم قاعدة التشفير (ER_{KT})

القيم	قاعدة تشفير المعرف
0	محجوزة
1	DER (RFC 3217)
2	BER (RFC 3394)
	جميع القيم الأخرى محجوزة لاستعمالات المنظمة ISO

9.5 قاعدة تركيب مجال المعالجة (PD)

تُستخدم قاعدة تركيب مجال المعالجة من أجل الدلالة على المجال الذي تُستخدم فيه الأداة JPSEC. وتضم المجالات الممكنة مجال عناصر الصورة (البيكسل) ومجال معامل الموجات الصغيرة ومجال معامل الموجات الصغيرة محددة الكمية ومجال التدفق المشفر.

PD	F_{PD}

الشكل 34 – قاعدة تركيب مجال المعالجة

PD: مجال المعالجة. ويستخدم هذا المجال البنية FBAS.

F_{PD}: مجال المعالجة من أجل توفير معلومات تفصيلية إضافية عن مجال المعالجة. ويستخدم هذا المجال البنية FBAS.

الجدول 47 – معلمات مجال المعالجة

المعلمة	الحجم (بالبتات)	القيم
PD	متغير (FBAS)	انظر الجدول 48
F_{PD}	متغير (FBAS)	في مجال معامل الموجات الصغيرة ومجال معامل الموجات الصغيرة محدودة الكمية، انظر الجدول 49. في ميدان التدفق المشفر، انظر الجدول 50.

الجدول 48 – قيم معلمات مجال المعالجة (PD)

رقم بتة FBAS	القيم	الدلالة
1	1	ميدان عناصر الصورة. تطبيق طريقة حماية على بيكسلات الصورة
	0	عدم تطبيق طريقة حماية على بيكسلات الصورة
2	1	مجال معامل الموجات الصغيرة. تطبيق طريقة حماية على معاملات الموجات الصغيرة
	0	عدم تطبيق طريقة حماية على معاملات الموجات الصغيرة
3	1	مجال معامل الموجات الصغيرة محدد القيمة. تطبيق طريقة حماية على معامل الموجة الصغيرة محدد القيمة
	0	عدم تطبيق طريقة حماية على معامل الموجة الصغيرة محدد القيمة
4	1	مجال التدفق المشفر. تطبيق طريقة حماية على التدفق المشفر المولد من مشفر حسابي
	0	عدم تطبيق طريقة حماية على التدفق المشفر المولد من مشفر حسابي

يلاحظ أن للمجال PD بتة واحدة فقط قيمتها 1، لأن كل أداة من الأدوات JPSEC قابلة للاستخدام في مجال واحد لا غير.

وينبغي في مجال عناصر الصورة ومجال معاملات الموجات الصغيرة ومجال معاملات الموجات الصغيرة محددة الكمية أن تتحول البيانات ثنائية الأبعاد إلى بعد واحد من أجل استخدام أدوات الأمن. ويتم هذا التحويل من خلال مسح بيانات الصورة ثنائية الأبعاد حسب ترتيب المسح الشبكي (التنقيطي).

الجدول 49 – قيم معلمات حقل مجال المعالجة (F_{PD}) في مجال معاملات الموجات الصغيرة ومجال معاملات الموجات الصغيرة محددة الكمية

رقم بتة FBAS	القيم	الدلالة
1	0	تطبيق طريقة حماية على بتة التشوير
	1	تطبيق طريقة حماية على البتة الأكثر دلالة

الجدول 50 – قيم معلمات حقل مجال المعالجة (F_{PD}) في مجال التدفق المشفر

رقم بتة FBAS	القيم	الدلالة
1	0	تطبيق طريقة حماية على رأسية الرزمة ومتنها
	1	تطبيق طريقة حماية على متن الرزمة فقط

يستخدم المجال (F_{PD}) في توفير معلومات إضافية عن مجال المعالجة. ولهذا المجال (F_{PD}) دلالات مختلفة بوجود قيم مختلفة لمجال المعالجة. فمثلاً، تستخدم البتة الأولى من المجال F_{PD} في مجال معاملات الموجات الصغيرة ومجال معاملات الموجات الصغيرة محددة الكمية من أجل الدلالة على تطبيق الأداة JPSEC على البتة الأكثر دلالة. وفي مجال التدفق المشفر تستعمل البتة الأولى من المجال F_{PD} للدلالة على استخدام الأداة JPSEC في متن الرزمة أم في رأسيتها ومتنها ؛ وفي مجال عناصر الصورة فإن المجال F_{PD} محجوز.

10.5 قاعدة تركيب التحبب (G)

يُستخدم التحبب في الدلالة على وحدة الحماية في كل طريقة حماية. ويحدد الجدول 53 سويات ممكنة للتحبب. ويبين الشكل 35 قاعدة تركيب التحبب.

PO	GL

الشكل 35 – قاعدة تركيب التحبب

PO: ترتيب المعالجة.

GL: سوية التحبب.

الجدول 51 – قيم معلمات التحبب (G)

المعلمة	الحجم (بالبتات)	القيم
PO	16	انظر الجدول 52
GL	8	انظر الجدول 53

الجدول 52 – قيم ترتيب المعالجة (PO)

القيم MSB LSB	ترتيب المعالجة
0 000 000 000 000 000	ترتيب تحدده منطقة تأثير المعلمات المتعلقة بالصورة
1 000 000 000 000 000	ترتيب تحدده منطقة تأثير معلمات تدفق البتات المتعلقة بغير الصورة
1 000 000 000 000 001	ترتيب تحدده منطقة تأثير معلمات الرزم المتعلقة بغير الصورة
0 000 001 010 011 100	رقعة – استبانة – طبقة – مكونة – منطقة
0 000 011 100 001 010	رقعة – مكونة – منطقة – استبانة – طبقة
0 000 010 001 011 100	رقعة – طبقة – استبانة – مكونة – منطقة
0 000 100 011 001 010	رقعة – منطقة – مكونة – استبانة – طبقة
0 000 001 100 011 100	رقعة – استبانة – منطقة – مكونة – طبقة
	جميع القيم الأخرى محجوزة

الجدول 53 – قيم سوية التحبب (GL)

القيم LSB MSB	التحبب
0000 0000	الرقعة
0000 0001	جزء الرقعة
0000 0010	مكونة
0000 0011	سوية استبانة
0000 0100	طبقة
0000 0101	منطقة
0000 0110	رزمة
0000 0111	نطاق فرعي
0000 1000	فدرة شفرة
0000 1001	إجمالي المنطقة التي تعرفها ZOI
1000 0000	بند معرف في منطقة ZOI متعلقة بغير الصورة
1000 0001	منطقة معرفة في منطقة ZOI متعلقة بغير الصورة
	جميع القيم الأخرى محجوزة

من أجل معالجة كامل المنطقة التي تحددها ZOI، ينبغي أن تكون سوية التحبب "منطقة محددة في المنطقة ZOI".

11.5 قاعدة تركيب قائمة القيم (V)

يستخدم مجال قائمة القيم في تحديد القيم التي تتغير عند استعمال الأداة وتحديد التحبب الذي تغير معها. ويستخدم ذلك الإعلام بتغير القيم مثل المفاتيح ومتجهات التدميث وقيم الشفرة MAC والتواقيع الرقمية وقيم التقطيع. ويحدد مجال قائمة القيم أولاً عدد القيم في القائمة وحجم كل منها. ثم يعدد القيم بحد ذاتها.

وكما ورد في الفقرة 2.6.5، يمثل مجال قائمة القيم، فيما يخص الأدوات JPSEC المعيارية، معلمة مختلفة لكل نموذج معياري. فهو يمثل في النموذج المعياري لفك التشفير متجهي التدميث IV_{bc} أو IV_{sc} تبعاً لاستخدام مشفر فدرة أو مشفر تدفق. ويمثل في النموذج المعياري للاستيقان قيمة الشفرة MAC، VAL_{MAC} للاستيقان القائم على التقطيع والاستيقان القائم على خوارزمية تجفير. ويمثل هذا المجال في النموذج المعياري للتوقيع الرقمي التوقيع الرقمي SIG_{DS}، ويمثل في النموذج المعياري للتقطيع قيمة التقطيع HV_{hash}. ولا تتطلب بعض استخدامات النماذج المعيارية قيماً للتحديد. وعلى سبيل المثال، لا تستعمل جميع أساليب فك التشفير متجهات التدميث. وفي هذه الحالات، ينبغي لمجال قائمة القيم أن تعطي المعلمتين N_v وS_v قيمة الصفر بحيث لا تبقى أي عناصر في قائمة القيم VL. وإذا احتاجت قيمة واحدة فقط للتحديد مثل استعمال مفتاح واحد في الصورة فإن N_v تتخذ قيمة واحد بحيث تتضمن قائمة القيم قيمة واحدة.

N_V	S_V	VL

الشكل 36 – قاعدة تركيب مجال قائمة القيم

N_V: عدد القيم في قائمة القيم VL وإذا كانت $N_V = 0$ ينتهي المجال. ويستعمل هذا المجال البنية RBAS.

S_V: حجم كل قيمة في قائمة القيم VL بالأثمونات. ويستعمل هذا المجال البنية RBAS.

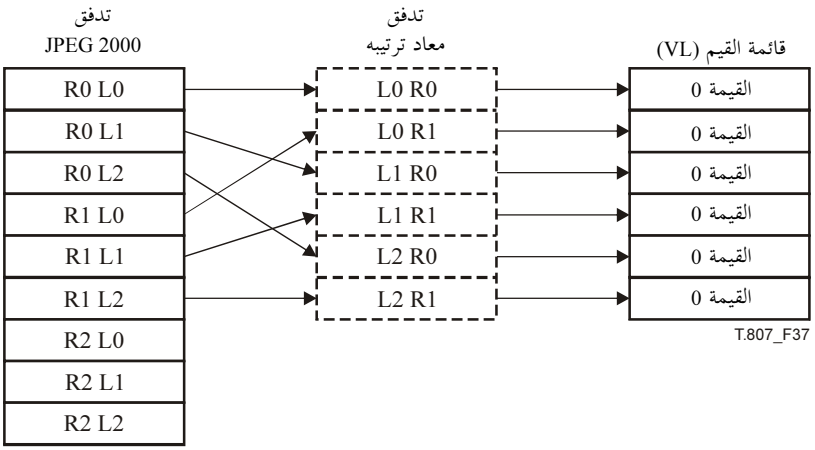
VL: قائمة القيم.

الجدول 54 – قيم معلمات مجال قائمة القيم (V)

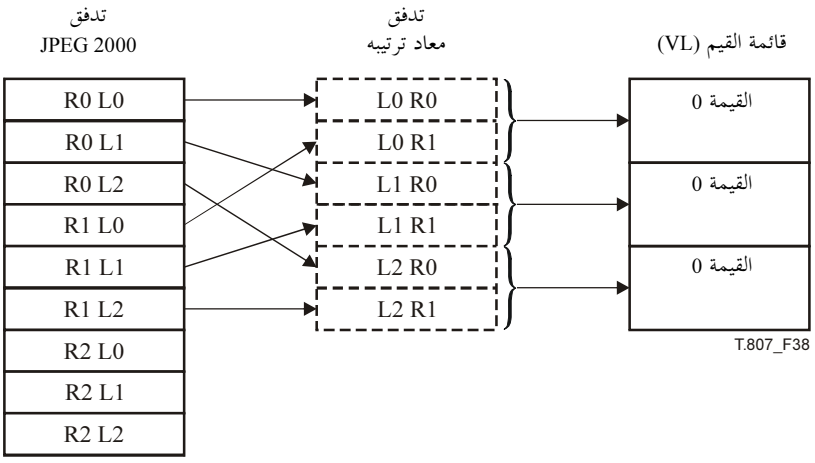
المعلمة	الحجم (بالبتات)	القيم
N_V	16 + 8 * n (RBAS)	$0 \ldots (2^{15+7*n} - 1)$
S_V	8 + 8 * n (RBAS)	$0 \ldots (2^{7+7*n} - 1)$
VL	0, if NV = 0 $N_V * S_V$, otherwise	N/A يحددها النموذج المعياري

12.5 العلاقات ما بين المنطقة ZOI والتحبب (G) وقائمة القيم (VL)

تستعمل المعلمات ZOI وPO وGL معاً بغية ضمان السلوك الموحد لأدوات JPSEC المستخدمة بغض النظر عن الترتيب التدرجي للتدفق المشفر JPEG 2000. وفي عبارة أخرى، فإن التوقيع الناتج وقيم الشفرة MAC والتدفق المشفر مستقلة عن الترتيب التدرجي للتدفق JPEG 2000. وتحدد منطقة التأثير (ZOI) بكاملها جزء التدفق JPEG 2000 الذي يتعين على الأداة JPSEC حمايته؛ ومن ناحية أخرى يحدد ترتيب المعالجة (PO) الترتيب الذي تعالج فيه الأداة JPSEC التدفق؛ وتحدد سويت التحبب (GL) وحدات الحماية التي تضم تتابع أثمونات متلاصقة في التدفق المعاد ترتيبه. وأخيراً تعادل كل وحدة حماية قيمةً في قائمة القيم (VL) حسب الترتيب الذي يظهر فيه التدفق المعاد ترتيبه. ويمكن توضيح العلاقة من خلال مثال واحد يكون فيه للتدفق JPEG 2000 رقعة واحدة وثلاث سويات استبانة وثلاث طبقات، أما عدد المكونات والمناطق فليس مهماً. والترتيب التدرجي هو RLCP في التدفق JPEG 2000 الأصلي ومنطقة التأثير 0 أو 1 وترتيب المعالجة (PO) هو TRLCP. ويبين الشكلان 37 و38 إعادة ترتيب التدفق التقابل بين كل وحدة حماية وقائمة القيم (VL) عندما تكون سوية التحبب (GL) استبانة أو طبقة حسب الحالة.



الشكل 37 – سوية التحبب (GL) هي استبانة



الشكل 38 – سوية التحبب (GL) هي طبقة

ملاحظة – لا يستعمل التدفق المعاد ترتيبه إلا في توليد القيم في قائمة القيم (VL). وسيكون للتدفق JPSEC النهائي نفس الترتيب التدرجي الموجود في التدفق JPEG 2000 الأصلي.

13.5 واسم الأمن داخل التدفق (INSEC)

يوفّر واسم الأمن داخل التدفق (INSEC) وسائل إضافية لإرسال معلومات الأمن. وهو خياري ويُستخدم مع واسم الأمن SEC. ويُستعمل خاصة مع أداة JPSEC غير معيارية.

ويوجد الواسم SEC تحديداً في الرأسية الرئيسية، ويعطي معلومات شاملة عن الأدوات JPSEC المستخدمة في حماية الصورة. ويوجد الواسم INSEC في بيانات تدفق البتات ذاتي ويعطي معلمات إضافية أو بديلة للأداة JPSEC غير المعيارية التي تحددها معلمة دليل حالة الأداة. ولذا يجب أن يقابل دليل حالة الأداة في الواسم INSEC إحدى أدلة حالة الأداة في الرأسية الرئيسية.

ويجوز وضع قطعة الواسم INSEC في بيانات تدفق البتات. وهي تستفيد من أن مفكك التشفير الحسابي في التدفق JPEG 2000 يوقف أثمونات القراءة في تدفق البتات عند وصول واسم النهاية (أي أثمونان بقيمة أكبر من 0xFF8F).

والمعلومات التي تشتمل عليها قطعة الواسم INSEC هامة لفدر الشفرة الأمنية السابقة واللاحقة وحتى وجود واسم INSEC آخر.

ويلاحَظ أنه ينجم عن إدراج وسوم INSEC ملفاً قد لا يمتثل للجزء 1 من المعيار JPEG 2000. ويلاحظ أيضاً أنه يمكن أن تلقى بعض مفككات التشفير صعوبات في معالجة واسم ما يرد وسط الرزمة. وسيسيء إدراج الوسوم في أي مكان داخل الرزمة إلى طول الرزمة الذي تدل عليه رأسية الرزمة. وقد يكون هناك أيضاً مشكلات في التشفير والوسوم INSEC ناجمة عن:

أ) نقص في قيود محاكاة الواسم في التشفير؛ و/أو

ب) عدم إمكانية تحديد موقع الواسم ذاته في وجود التشفير.

وقاعدة تركيب الواسم INSEC محددة في الشكل 39.

INSEC	L_{INSEC}	i	R	AP

الشكل 39 – قاعدة تركيب واسم الأمن داخل التدفق

INSEC: شفرة واسم. يبين الجدول 55 حجوم وقيم الرموز والمعلمات الخاصة بقطعة واسم الأمن داخل التدفق.

L_{INSEC}: طول قطعة الواسم بالأثمونات (لا تضم الواسم). يلاحظ أنه ينبغي أن تكون قطعة الواسم INSEC متراصفة الأثمونات.

i: دليل حالة الأداة الذي يقابل إحدى معلمات دليل حالة الأداة في قطعة الواسم SEC ويحدد بالتالي حالة الأداة JPSEC التي يحيل إليها هذا الواسم INSEC. ويستخدم هذا المجال البنية RBAS.

R: المنطقة التي تطبق فيها المعلومات INSEC. ويستخدم هذا المجال البنية FBAS.

AP: معلمات إضافة أو بديلة لطريقة الحماية. وينبغي التأكد دائماً من عدم محاكاة المشفر لواسم في هذه المعلمة.

الجدول 55 – قيم معلمة الأمن داخل التدفق (INSEC)

المعلمة	الحجم (بالبتات)	القيم
INSEC	16	0xFF94
L_{INSEC}	16	$2 \ldots (2^{16} - 1)$
i	8 + 8 * n (RBAS)	$0 \ldots (2^{7+7*n} - 1)$
R	متغير (FBAS)	انظر الجدول 56
AP	متغير	محددة من سلطة التسجيل أو من التطبيق

الجدول 56 – قيم منطقة الصلة

رقم البتة FBAS	القيم	منطقة الصلة
0	0	فدر الشفرة السابقة
	1	فدر الشفرة اللاحقة

وبما أن الواسم INSEC يستخدم بالترافق مع أدوات JPSEC غير المعيارية، فإن نسق المعلمات الإضافية أو البديلة يتحدد في الأداة ذاتها المعرَّفة بدورها في معرِّف هوية الأداة. وأدوات JPSEC غير المعيارية معرفة تحديداً من قبل سلطة تسجيل أو في تطبيقات JPSEC خاصة. وعليه، ينبغي أن يضم تعريف هذه الأدوات استخدام الواسم INSEC إن وُجد.

6 أمثلة لاستعمال قاعدة تركيب معيارية (على سبيل الإعلام)

1.6 أمثلة لمنطقة التأثير ZOI

تضم هذه الفقرة أمثلة تبين كيفية استعمال قاعدة تركيب منطقة التأثير.

وفي الأمثلة التالية، تقابل الرموز الدليلية العلوية في المعلمات Pzoi وMzoi وIzoi دليل البندين المتعلق بالصورة والمتعلق بغير الصورة التي تشير إليهما البنية BAS في المعلمة DCzoi حسب الترتيب الذي يظهران فيه داخل المعلمة DCzoi.

1.1.6 المثال 1

تقدم هذه الفقرة مثالاً يطال فيه التأثير سويات استبانة تتجاوز 3 في منطقة الصورة ذات الزاوية العلوية اليسرى (100، 120) والزاوية السفلية اليمنى (180، 210). وتتطلب الحالة في هذا المثال، 9 أثمونات.

الجدول 57 – منطقة التأثير في المثال 1

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	101000_b	تتحدد مناطق الصورة وسويات الاستبانة حسب الترتيب
	$Pzoi^1$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	0_b	يتحدد بند واحد
			2	00_b	أسلوب المستطيل
			2	00_b	تستعلم المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	1_b	توصف المعلمة Izoi في بُعدين
		$Izoi^1$	8	$0110\ 0100_b$	البعد Xul = 100
			8	$0111\ 1000_b$	البعد Yul = 120
			8	$1011\ 0100_b$	البعد Xlr = 180
			8	$1101\ 0010_b$	البعد Ylr = 210
	$Pzoi^3$	$Mzoi^3$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	مكمل المناطق المحددة تتأثر بالأداة JPSEC
			1	0_b	يتحدد بند واحد
			2	11_b	الأسلوب Max
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi ببُعد واحد
		$Izoi^3$	8	$0000\ 0010_b$	تتحدد سويات الاستبانة ≥ 2 (أي سويات الاستبانة > 3 تتحدد في الأسلوب Max وتبديل مكمل.)

2.1.6 المثال 2

تقدم هذه الفقرة مثالاً يطال فيه التأثير فدر شفرة دلل زاويتها العلوية اليسرى 5 ودليل زاويتها السفلية اليمنى 10 في النطاق الفرعي 1 وسوية الاستبانة 0 متأثرة. وتتطلب الحالة في هذا المثال 10 أثمونات.

الجدول 58 – منطقة التأثير في المثال 2

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DCzoi[1]		1	1_b	قطعة الأثمونات المتراصفة تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	001000_b	سويات الاستبانة محددة
	DCzoi[2]		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	001100_b	النطاقات الفرعية وفدر الشفرة محددة
	Mzoi[3]	Pzoi[3]	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
	Izoi[3]		8	$0000\ 0000_b$	دليل سوية الاستبانة 0
	Mzoi[8]	Pzoi[9]	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
	Izoi[8]		8	$0000\ 0001_b$	يتحدد النطاق الفرعي 1
	Mzoi[9]	Pzoi[10]	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	00_b	أسلوب المستطيل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
	Izoi[9]		8	$0000\ 0101_b$	دليل فدرة الشفرة للزاوية العلوية اليسرى 5
			8	$0000\ 1010_b$	دليل فدرة الشفرة للزاوية السفلية اليمنى 10

3.1.6 المثال 3

تقدم هذه الفقرة مثالاً للحالة التي تكون فيها قطع البيانات من الأثمونات 10 إلى 100 ومن الأثمونات 10000 إلى 12000 تحت التأثير. وتتطلب هذه الحالة 12 أثموناً.

الجدول 59 – منطقة التأثير في المثال 3

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف الوصف المتعلق بغير الصورة
			6	010000_b	تتحدد أمدية الأثمونات بعد الاسم SOD
	$Pzoi^2$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	1_b	تتحدد عدة بنود
			2	01_b	أسلوب المدى
			2	01_b	تستعمل المعلمة Izoi عدداً صحيحاً من 16 بتة
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Nzoi^2$	8	$0000\ 0010_b$	عدد قطع البيانات 2
		$Izoi^{21}$	16	$0000\ 0000_b$ $0000\ 1010_b$	تحديد موقع أثمون البدء هو الأثمون العاشر (أثمونات)
			16	$0000\ 0000_b$ $0110\ 0100_b$	تحديد موقع أثمون النهاية هو الأثمون المائة (أثمونات)
		$Izoi^{21}$	16	$0010\ 0111_b$ $0001\ 0000_b$	تحديد موقع أثمون البدء هو الأثمون 10000 (أثمونات)
			16	$0010\ 1110_b$ $1110\ 0000_b$	تحديد موقع أثمون البدء هو الأثمون 12000 (أثمونات)

4.1.6 المثال 4

تقدم هذه الفقرة مثالاً لحالة تكون فيها سوية الاستبانة 0 متأثرة وقطع الأثمون 10 من 100 تقابل بيانات سوية الاستبانة 0. وتتطلب هذه الحالة 10 أثمونات.

الجدول 60 – منطقة التأثير في المثال 4

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد فقط
$Zone^0$	$DCzoi^1$		1	1_b	قطعة الأثمونات المتراصفة تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	001000_b	تتحدد سويات الاستبانة بالترتيب
	$DCzoi^2$		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف الوصف المتعلق بغير الصورة
			6	010000_b	أمدية الأثمونات محددة
	$Pzoi^1$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد ببند واحد
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^1$	8	$0000\ 0000_b$	سوية الاستبانة 0

الجدول 60 – منطقة التأثير في المثال 4

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
$Zone^0$	$Pzoi^2$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	01_b	تستعمل المعلمة Izoi عدداً صحيحاً من 16 بتة
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^1$	16	0000 0000 0000 1010_b	تحديد موقع أثمون البدء هو الأثمون العاشر (أثمونات)
			16	0000 0000 0110 0100_b	تحديد موقع أثمون النهاية هو الأثمون المائة (أثمونات)

5.1.6 المثال 5

تقدم هذه الفقرة مثالاً لحالة تتأثر فيها سويات الاستبانة فوق 3 في الرقم ذات دليل الرقعة العلوية اليسرى 0، ودليل الرقعة السفلية اليمنى 5، وتتأثر فيها أيضاً الطبقات المساوية 5 أو أقل في الرقع ذات دليل الرقعة العلوية اليسرى 10 ودليل الرقعة السفلية اليمنى 15، وتتطلب هذه الحالة 13 أثمونا.

الجدول 61 – منطقة التأثير في المثال 5

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	2	عدد المناطق 2
$Zone^0$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف وصف متعلق بالصورة
			6	01 1000_b	تتحدد سويات الرقع والاستبانة بالترتيب
	$Pzoi^2$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	00_b	أسلوب المستطيل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^2$	8	0000 0000_b	دليل الرقعة العلوية اليسرى 0
			8	0000 0101_b	دليل الرقعة السفلية اليمنى 5
	$Pzoi^3$	$Mzoi^3$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	تؤثر الأداة JPSEC على مكملات المناطق المحددة
			1	0_b	يتحد بند واحد
			2	11_b	الأسلوب Max
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^3$	8	0000 0010_b	تتحدد سويات الاستبانة ≥ 2 (أي سويات الاستبانة أكبر من 3 تتحدد في الأسلوب Max وبتبديل المكمل)

الجدول 61 – منطقة التأثير في المثال 5

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
$Zone^1$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف وصف متعلق بالصورة
			6	010100_b	تتحدد الرقع والطبقات بالترتيب
	$Pzoi^2$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	00_b	أسلوب المستطيل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^2$	8	$0000\ 1010_b$	دليل الرقعة العلوية اليسرى 10
			8	$0000\ 1111_b$	دليل الرقعة السفلية اليمنى 15
	$Pzoi^4$	$Mzoi^4$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف وصف متعلق بالصورة
			1	0_b	تتحدد الرقع والطبقات بالترتيب
			2	11_b	الأسلوب Max
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^4$	8	$0000\ 0101_b$	تتحدد الطبقات ≥ 5 مع الأسلوب Max

6.1.6 المثال 6

تقدم هذه الفقرة مثالاً لحالة تتأثر فيها قطعة الرأسية من الأثمون 10 إلى الأثمون 100. وتتطلب هذه الحالة 8 أثمونات.

الجدول 62 – منطقة التأثير في المثال 6

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DCzoi		1	0_b	منطقة الأثمونات المتراصفة لا تلي
			1	1_b	صنف وصف متعلق بغير الصورة
			6	001000_b	تتحدد أمدية الأثمونات بعد الواسم SEC
	$Pzoi^3$	$Mzoi^3$	1	0_b	منطقة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC علا المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	01_b	تستعمل المعلمة Izoi عدداً صحيحاً من 16 بتة
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^3$	16	$0000\ 0000$ $0000\ 1010_b$	تحديد موقع أثمون البداية هو الأثمون 10 (أثمونات)
			16	$0000\ 0000$ $0110\ 0100_b$	تحديد موقع أثمون النهاية هو الأثمون 100 (أثمونات)

2.6 أمثلة النموذج المعياري لمعلومات المفاتيح

1.2.6 المثال 1

يقدم الجدول 63 مثالاً لحالة استعمال مفتاح سري واحد (128 بتة) في فك تشفير تدفق مستمر، حيث يُعرَّف المفتاح السري من خلال معرف هوية عالمي للموارد (URI) ويستنتج من عدم مفاتيح قائم على معرفات في مرحلة فك التشفير.

الجدول 63 – معلومات مفتاح المثال 1

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
LK_{KT}		16	128	طول المفتاح 128 بتة
KID_{KT}		8	2	يتحدد المعرف URI الخاص بالمفتاح السري
G_{KT}	PO	16	000 001 010 011 100 0_b	ترتيب المعالجة هو التالي: رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	0000 1001_b	وحدة الحماية هي كامل المنطقة المحددة في المعلمة ZOI
V_{KT}	N_V	16 (RBAS)	1	عدد القيم في قائمة القيم V هو 1
	S_V	8 (RBAS)	19	طول معلومات المفتاح 19 أثمونا
	V1	152	https://server/file	يمكن أخذ المفتاح السري من العنوان https://server/file

2.2.6 المثال 2

يقدم الجدول 64 مثالاً لحالة استعمال شهادة X.509 في استيقان التدفق حيث تكون الشهادة X.509 مدمجة في المعلمة KI_{KT} مع طريقة التشفير DER.

الجدول 64 – معلومات مفتاح المثال 2

المعلمة			الحجم (بالبتات)	القيمة	الدلالة الناتجة
LK_{KT}			16	1024	طول المفتاح 1024 بتة
KID_{KT}			8	2	تتحدد الشهادة X.509
G_{KT}	PO		16	000 001 010 011 100 0_b	ترتيب المعالجة هو التالي: رقعة – استبانة – طبقة – مكونة – منطقة
	GL		8	0000 1001_b	وحدة الحماية هي كامل المنطقة المحددة في المعلمة ZOI
V_{KT}	N_V		16 (RBAS)	1	عدد القيم في قائمة القيم V هو 1
	S_V		8 (RBAS)	متغيرة	طول الشهادة X.509
	V1	ER_{KT}	8	1	الشهادة X.509 مشفرة بطريقة التشفير DER
		$LCER_{KT}$	16	متغيرة	طول المعلمة CER_{KT}
		CER_{KT}	متغير	قيمة الشهادة	الشهادة مع المفتاح العمومي المكون من 1024 بتة مدمجان

3.2.6 المثال 3

يبين الجدول 65 أن مفتاح عمومي واحد مستعمل في استيقان تدفق مشفر حيث المفتاح العمومي مدمج في المعلمة KI_{KT}.

الجدول 65 – معلومات مفتاح المثال 3

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
LK_{KT}		16	1024	طول المفتاح 1024 بتة
KID_{KT}		8	1	يتحدد المفتاح العمومي
G_{KT}	PO	16	000 001 010 011 100 0_b	ترتيب المعالجة: رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	0000 1001_b	وحدة الحماية هي كامل المنطقة المحددة في المعلمة ZOI
V_{KT}	N_V	16 (RBAS)	1	عدد القيم في قائمة القيم V هو 1
	S_V	8 (RBAS)	256	طول المفتاح العمومي 256 أثمونا
	V1	2048	*قيمة المفتاح العمومي*	المفتاح العمومي مدمج

4.2.6 المثال 4

يبين الجدول 66 أن المفاتيح السرية المتعددة مستخدمة في فك تشفير التدفق حيث تُستعمل مفاتيح سرية مختلفة للطبقات المختلفة.

الجدول 66 – معلومات مفتاح المثال 4

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
LK_{KT}		16	128	طول المفتاح 128 بتة
KID_{KT}		8	3	يتحدد المعرف URI للمفتاح السري
G_{KT}	PO	16	000 001 010 011 1000_b	ترتيب المعالجة هو التالي: رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	0000 0100_b	وحدة الحماية طبقة
V_{KT}	N_V	16 (RBAS)	3	عدد القيم في قائمة القيم V هو 3
	S_V	8 (RBAS)	16	طول كل Vn هو 16 أثمونا
	V1	128	https://server/1	يؤخذ المفتاح السري للطبقة الأولى من العنوان https://server/1
	V2	128	https://server/2	يؤخذ المفتاح السري للطبقة الثانية من العنوان https://server/2
	V3	128	https://server/3	يؤخذ المفتاح السري للطبقة الثالثة من العنوان https://server/3
	V4	128	https://server/4	يؤخذ المفتاح السري للطبقة الرابعة من العنوان https://server/4

3.6 أمثلة الأدوات المعيارية JPSEC

تصف الأمثلة التالية كيفية استخدام منطقة التأثير ZOI والنماذج المعيارية للمفاتيح بغية توفير خدمات أمن أساسية مثل التشفير والاستيقان في صورة مشفرة JPEG 2000.

1.3.6 المثال 1

الصورة مشفرة حسب المعيار JPEG 2000 ولها ثلاث استبانات. وفي هذا المثال، لا تشفر الاستبانة الأولى من أجل توفير مقدرة الترئية السابقة، وتشفر الاستبانات الثانية والثالثة بالمفتاحين K1 وK2، على التوالي. وتشفر الصورة 5 الداخلة في هذه الحالة حسب الترتيب التدريجي RLCP ولها رقعة واحدة و3 استبانات و3 طبقات وعدد Np من المناطق (ليس لعدد المكونات والمناطق أي أهمية في هذا المثال تحديداً). ويتم التشفير باستعمال خوارزمية التجفير المتطور (AES) في الأسلوب CBC دون حشو (من خلال استخراج نص التجفير) واستعمال المفتاح k0 لتشفير الاستبانة 1 والمفتاح k2 لتشفير الاستبانة 2، أما الاستبانة 0 فتُترك دون تشفير.

ويبين المعيار JPSEC كيفية فك تشفير المستهلك للتدفق المشفر بهذه الطريقة. ويشار أولاً إلى معرف هوية النموذج المعياري لأداة التشفير وتتحدد منطقتا تأثير للاستبانة 1 مع مدى الأثمونات B1-B0 المقابل لها وللاستبانة 2 ومدى الأثمونات B3-B2 المقابل لها. وتحدد معلمات النموذج المعياري لفك التجفير أن التجفير AES مستخدم دون حشو (من خلال استخراج نص التجفير). ويشار في معلمات معلومات المفاتيح إلى معلومات استعمال المفاتيح واستخدام مفاتيح مختلفة للاستبانات المختلفة. ويتحدد تحبُّب المفتاح خصوصاً باعتباره استبانة، وبذلك يكون لكل استبانة مفتاح مختلف. ويشار إلى ترتيب المعالجة على أنه TRLCP. وتوجد معلومات المفتاح لكل استبانة في قائمة قيم المفاتيح. ويجري تشفير التدفق بتشفير رأسيات الرزم ومتون الرزم. وتحبب التشفير استبانة تجري فيها المعالجة حسب الترتيب TRLCP وهو نفس ترتيب التدفق الأصلي. وبما أن الاستبانتين تشفران كل على حدة فإنهما تتطلبان متجهي تدميث (IVs) موجودين في قائمة.

وجدير بالملاحظة أن نتائج نص مجفر الرزم تتحدد حسب ترتيب المعالجة ولذلك فإنها مستقلة عن ترتيب معالجة تدفق الدخل؛ ومع ذلك فإن موقع الرزم المجفرة في تدفق الخرج يتبع ترتيب رزم تدفق الدخل.

الجدول 67 – قطعة الواسم SEC في المثال 1

المعلمة			الحجم (بالبتات)	القيمة	الدلالة الناتجة
SEC			16	0xFF65	الواسم SEC
L_{SEC}			16 (RBAS)	0x82	طول قطعة الواسم SEC 130 أثمونًا
Z_{SEC}			8 (RBAS)	0	دليل قطعة الواسم SEC هذه
P_{SEC}	F_{PSEC}		1	0_b	البنية FBAS لا تلي
		F_{INSEC}	1	0_b	الواسم INSEC غير مستعمل
		$F_{multiSEC}$	1	0_b	تُستعمل قطعة واسم SEC واحدة
		F_{mod}	2	00_b	طرأ تغيير على البيانات JPEG 2000 الأصلية
		F_{TRLCP}	1	0_b	استعمال الواسم TRLCP غير محدد في المعلمة P_{SEC}
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	عدد أدوات الأمن واحد
	I_{max}		8 (RBAS)	0000000_b	دليل حالة الأداة القصوى صفر
t			8 (FBAS)	0	أداة JPSEC معيارية
i			8 (RBAS)	0	دليل حالة أداة
ID_T			8	1	نموذج معياري لفك التشفير
L_{zoi}			16 (RBAS)	0x17	طول منطقة التأثير 23 أثمونًا
ZOI			184	انظر الجدول 68	منطقة التأثير لهذه الأداة
L_{PID}			16 (RBAS)	0x5e	طول المعلمة P_{ID} 94 أثمونًا
P_{ID}			752	انظر الجدول 69	معلمات هذه التكنولوجيا

الجدول 68 – مثال لمنطقة التأثير (ZOI)

المعلمة			الحجم (بالبتات)	القيمة	الدلالة الناتجة
NZzoi			8 (RBAS)	2	عدد المناطق واحد
$Zone^0$	DC_{ZOI}^1		1	1_b	قطعة الأثمونات المتراصفة تلي
			1	0_b	صنف وصف متعلق بالصورة
			6	001000_b	الاستبانة محددة
	DCzoi[2]		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف وصف متعلق بغير الصورة
			6	010000_b	تتحدد أمدية الأثمونات بعد الواسم SOD
	Mzoi[1]	$Pzoi^{0,1}$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi في بُعد واحد

الجدول 68 – مثال لمنطقة التأثير (ZOI)

المعلمة			الحجم (بالبتات)	القيمة	الدلالة الناتجة
		I_{ZOI}	8	$0000\ 0001_b$	تتحدد الاستبانة 1
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	01_b	تستعمل المعلمة Izoi عدداً صحيحاً من 16 بتة
			1	0_b	توصف المعلمة Izoi في بُعد واحد
		$Izoi^{21}$	16	0x31CC	موقع أثمون البداية هو 12748 (أثمونات). (B0)
			16	0xA3E8	موقع أثمون النهاية هو 41960 (أثمونات). (B1)
$Zone^1$		DC_{ZOI}^1	1	1_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	001000_b	الاستبانة محددة
		$DCzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف الوصف المتعلق بغير الصورة
			6	010000_b	تتحدد أمدية الأثمونات بعد الواسم SOD
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_b	يتحدد بند واحد
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi عدد صحيح من 8 بتات
			1	0_b	توصف المعلمة Izoi ببعد واحد
		I_{ZOI}^1	8	$0000\ 0010_b$	الاستبانة 2 محددة
	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	تؤثر الأداة JPSEC على المناطق المحددة
			1	0_{b2}	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	10_b	تستعمل المعلمة Izoi عدد صحيح من 32 بتة
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Izoi^2$	32	0xA3EE	موقع أثمون البدء هو الأثمون 41966 (أثمونات). (B2)
			32	0x21101	موقع أثمون النهاية هو الأثمون 135425 (أثمونات). (B3)

الجدول 69 – مثال للمعلمة P_{ID}

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
T_{ID}		432	70انظر الجدول	نماذج معيارية لفك التجفير
PD		8 (FBAS)	0_b	قطعة الأثمونات المتراصفة لا تلي
			0_b	مجال البيكسل غير مستعمل
			0_b	مجال معامل الموجة الصغيرة غير مستعمل
			0_b	مجال معامل الموجة الصغيرة المكماة غير مستعمل
			1_b	مجال التدفق المشفر مستعمل
			000_b	محجوز لاستعمالات المنظمة ISO
F_{PD}		8 (FBAS)	0_b	الأثمون FBAS لا يلي
			1_b	لا يحفر إلا متن الرزمة
			000000_b	محجوز لاستعمالات المنظمة ISO
G	PO	16	$000\ 001\ 010\ 011\ 100\ 0_b$	ترتيب المعالجة هو رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	$0000\ 0011_b$	وحدة الحماية سوية الاستبانة
V	N_V	16 (RBAS)	2	عدد القيم في القائمة V هو 2
	S_V	8 (RBAS)	16	طول كل رقم في القائمة هو 16 أثموناً
	V1	128	IV0	قيمة متجه التدميث للمعلمة R1
	V2	128	IV1	قيمة متجه التدميث للمعلمة R2

الجدول 70 – مثال لنموذج فك التجفير

المعلمة		الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
ME_{decry}		8	0	تمت محاكاة الواسم
CT_{decry}		16	0001_b	مجفر الفدرة (AES)
CP_{decry}	M_{bc}	6	100000_b	الأسلوب CBC. البتات غير محشوة
	P_{bc}	2	00_b	استعارة نصف تجفير
	SIZ_{bc}	8	16	حجم الفدرة (16 أثموناً، 128 بتة)
	KT_{bc}	392	انظر الجدول 71	النموذج المعياري للمفتاح

الجدول 71 – مثال لنموذج معياري للمفتاح

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
LK_{KT}		16	128	طول المفتاح 128 بتة
KID_{KT}		8	2	معرف URI للمفتاح السري
G_{KT}	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	ترتيب المعالجة هو رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	$0000\ 0011_b$	وحدة الحماية هي سوية الاستبانة
V_{KT}	N_V	32 (RBAS)	2	عدد القيم في القائمة Vn هو 2
	S_V	8 (RBAS)	19	طول كل Vn هو 19 أثموناً
	V1	152	https://server/key1	يمكن أخذ المفتاح السري لسوية الاستبانة 1 من العنوان https://server/key1
	V2	152	https://server/key2	يمكن أخذ المفتاح السري لسوية الاستبانة 2 من العنوان https://server/key2

2.3.6 المثال 2

يطبق الاستيقان في هذه الحالة على نفس الصورة المشفرة JPEG 2000 كما يرد أعلاه. ويتم في هذا المثال استيقان جميع الاستبانات الثلاث والطبقات الثلاث لكل استبانة، حيث يستخدم مفتاح مختلف في كل استبانة. ونظراً لوجود ثلاث استبانات فهناك ثلاثة مفاتيح، ونظراً لوجود ثلاث طبقات في كل استبانة فهناك ثلاث قيم MAC لكل استبانة. وهكذا سيكون مجموع القيم MAC تسعة لكامل الصورة JPEG. وهي تحديداً،

- في الاستبانة 0 القيم MAC: M0 وM1 وM2 (واحدة لكل طبقة) وتستخدم المفتاح 0
- في الاستبانة 1 القيم MAC: M3 وM4 وM5 (واحدة لكل طبقة) وتستخدم المفتاح 1
- في الاستبانة 2 القيم MAC: M6 وM7 وM8 (واحدة لكل طبقة) وتستخدم المفتاح 2

ويوضح هذا المثال كيفية بيان الاستيقان والمرونة التي توفرها المنطقة ZOI وأدوات التحبب. وتشفر صورة الدخل كما في المثال السابق حسب الترتيب التدرّجي RLCP ولها رقعة واحدة وثلاث استبانات وثلاث طبقات ومكونات Nc ومناطق Np (عدد المكونات والمناطق غير ذات أهمية في هذا المثال بالذات). ويتم الاستيقان باستعمال الشفرة HMAC مع SHA-1.

ويبيِّن التشفير JPSEC قدرة مستهلك JPSEC على التحقق من محتوى محمي بالنظام JPSEC أو استيقانه. فمعرف هوية النموذج المعياري للأداة والخاص بالاستيقان أولاً ظاهر. ثم المنطقة ZOI مستخدمة للدلالة على وجود ثلاث استبانات وعلى أمدية الأثمونات المرفقة بكل استبانة. ومعلمات النموذج المعياري للاستيقان تدل على أن الشفرة HMAC مستخدمة مع SHA-1. والنموذج المعياري لمعلومات المفتاح يوفر المعلومات عن المفاتيح ومنها أن تحبب المفتاح هو الاستبانة وإضافة معلومات عن كل من المفاتيح الثلاثة في قائمة قيم المفاتيح. ويتحدد مجال المعالجة الخاص بالاستيقان باعتباره تدفقاً مشفراً يشتمل على رأسيات الرزم. ويتحدد تحبب الأداة الخاص بالاستيقان على أنه الطبقة، وبالتالي تضم كل استبانة ثلاث شفرات MAC، أي ما مجموعه تسع قيم للشفرة MAC. وتضم قائمة المقيم تسع قيم MAC. أما ترتيب المعالجة فيما يتعلق بالمثال الوارد أعلاه فهو الترتيب TRLCP أي نفس الترتيب الأصلي المستخدم في التدفق المشفر.

ويلاحظ أن استخدام ترتيب المعالجة في مجال التحبب يضمن أن تنتج نفس القيم MAC بمعزل عن ترتيب معالجة التدفق المشفر.

ويلاحظ أنه بما أن هذا المثال يبين استعمال الشفرات MAC فإنه يمكن اتباع نفس النهج في استعمال التواقيع الرقمية المتعددة.

الجدول 72 – قطعة الواسم SEC

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
SEC			16	0xFF65	الواسم SEC
L_{SEC}			16	0x0099	طول قطعة الواسم SEC
Z_{SEC}			8 (RBAS)	0	دليل قطعة الواسم SEC هذه
P_{SEC}	F_{PSEC}		1	0_b	البنية FBAS لا تلي
		F_{INSEC}	1	0_b	قطعة الواسم INSEC غير مستعملة
		$F_{multiSEC}$	1	0_b	توجد قطعة واسم SEC واحدة في هذا التدفق
		F_{mod}	1	0_b	لم تتغير البيانات JPEG 2000 الأصلية
		F_{TRLCP}	1	0_b	الواسم TRLCP غير مستعمل
		Padding	3	000_b	الواسم TRLCP غير مستعمل
	N_{tools}		7	1	لم تُستخدم إلا أداة واحدة في هذا التدفق
	I_{max}		7	0	أقصى دليل حالة أداة هو 0
$Tool^0$	t		8 (FBAS)	0	أداة JPSEC معيارية
	i		8 (RBAS)	0	دليل حالة الأداة
	ID_T		8	2	تستخدم هذه الأداة المعيارية نموذج استيقان
	L_{ZOI}		16 (RBAS)	0x20	طول المعلمة ZOI 32 أثموناً
	ZOI		256	الجدول 73	المنطقة المغطاة من الصورة
	L_{PID}		16 (RBAS)	0x6c	طول المعرف P_{ID} هو 108 أثموناً
	P_{ID}		928	الجدول 74	معلمات للأداة JPSEC

الجدول 73 – إشارات المعلمة ZOI

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DC_{zoi}^1		1	1_b	قطعة الأثمونات المتراصفة تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	001000_b	سويات الاستبانة محددة بالترتيب
	DC_{zoi}^2		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف الوصف المتعلق بغير الصورة
			6	010000_b	أمدية الأثمونات محددة
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	0_b	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	00_b	المعلمة Izoi تستخدم عدداً صحيحاً من 8 بتات
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Izoi^1$	8	0	بداية المدى 0
			8	2	نهاية المدى 2
$Zone^0$	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	1_b	تتحدد عدة بنود
			2	01_b	أسلوب المدى
			2	10_b	المعلمة Izoi تستعمل عدداً صحيحاً من 32 بتة
			1	0_b	توصف المعلمة Izoi ببعد واحد
		N_{ZOI}	8 (RBAS)	3	عدد المعلمات I_{ZOI} هو 3
		$Izoi^1$	32	104	موقع أثمون البداية 104 (أثمون)
			32	12762	موقع أثمون النهاية 12726 (أثمون)
		I_{ZOI}^2	32	12768	موقع أثمون البداية 12768 (أثمون)
			32	41980	موقع أثمون النهاية 41980 (أثمون)
		I_{ZOI}^3	32	41986	موقع أثمون البداية 41986 (أثمون)
			32	135445	موقع أثمون النهاية 135445 (أثمون)

الجدول 74 – معلمات تشوير المعرف P_{ID}

المعلمة				الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
T_{auth}	M_{auth}			8	0	طرائق الاستيقان: استيقان على أساس التقطيع
	P_{auth}	M_{HMAC}		8	1	الشفرة HMAC مستخدمة في الاستيقان
		H_{HMAC}		8	1	الشفرة SHA-1 مستخدمة في التقطيع
		KT_{HMAC}	LK_{KT}	16	128	طول المفتاح بالبتات
			KID_{KT}	8	3	تحتوي المعلمة KI_{KT} على المعرف URI الخاص بالمفتاح الخصوصي

الجدول 74 – معلمات تشوير المعرف P_{ID}

المعلمة					الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
			PO	G_{KT}	16	0 000 001 010 011 100_b	الترتيب هو رقعة – استبانة – طبقة – مكونة – منطقة
			GL		8	00000011_b	تحبب المفتاح هو الاستبانة
			N_V	V_{KT}	16 (RBAS)	3	يوجد 3 مفاتيح في القائمة
			S_V		8 (RBAS)	8	يبلغ طول كل مفتاح 8 أثمونات
			VL		64	Key0	المفتاح الأول هو *key*0 للاستبانة 0
					64	Key1	المفتاح الثاني هو *key*1 للاستبانة 1
					64	Key2	المفتاح الثالث هو *key*2 للاستبانة 2
		SIZ_{HMAC}			16	20	طول الشفرة MAC هو 20
PD					8 (FBAS)	0_b	قطعة الأثمونات المتراصفة لا تلي
						0_b	مجال البيكسل غير مستعمل
						0_b	مجال معامل الموجة الصغيرة غير مستعمل
						0_b	تكمية معامل الموجة الصغيرة غير مستعمل
						1_b	مجال التدفق مستعمل
						000_b	محجوزة لاستعمالات ISO
F_{PD}					8 (FBAS)	0_b	الأثمون FBAS لا يلي
						0_b	رأسية الرزمة ومتنها مجفران
						000000_b	محجوزة لاستعمالات المنظمة ISO
G			PO		16	00000101001 11000_b	الترتيب هو: رقعة – استبانة – طبقة – مكونة – منطقة
			GL		8	00000100_b	تحبب الأداة هو طبقة
V			N_V		32 (RBAS)	9	يوجد 9 شفرات MAC (3 لكل استبانة)
			S_V		8 (RBAS)	20	حجم كل MAC هو 20 أثمونا
			VL		160	*M*0	أول شفرة MAC هي *M*0
					160	*M*1	ثاني شفرة MAC هي *M*1
					160	*M*2	ثالث شفرة MAC هي *M*2
					160	*M*3	رابع شفرة MAC هي *M*3
					160	*M*4	خامس شفرة MAC هي *M*4
					160	*M*5	سادس شفرة MAC هي *M*5
					160	*M*6	سابع شفرة MAC هي *M*6
					160	*M*7	ثامن شفرة MAC هي *M*7
					160	*M*8	تاسع شفرة MAC هي *M*8

4.6 أمثلة لمجال التشوه

تقدم هذه الفقرة بعض الأمثلة البسيطة لاستخدام مجال التشوه.

1.4.6 المثال 1

يستند هذا المثال إلى المثال 3 للمعلمة ZOI الوارد في الفقرة 3.1.6 من أجل بيان كيفية ربط قيم التشوه بقطعتي بيانات تدل عليهما المعلمة ZOI في المثال المذكور. وكما ورد سابقاً يشير المثال 3 الوارد في الفقرة 3.1.6 إلى قطعتي بيانات هما: (1) الأثمونات من 10 إلى 100 و(2) الأثمونات

من 10000 إلى 12000. ويتطلب ربط مجالات التشوه بهاتين القطعتين مرحلتين اثنتين هما: أولاً الإشارة إلى مجال التشوه في المعلمة DCzoi، وثانياً الإشارة إلى قيم التشوه باستعمال المعلمة $Pzoi^2$. وبناءً عليه فإن التغييرات المدخلة إلى المثال 3 المذكور لا تتعدى وضع بتة مجال التشوه في المعلمة DCzoi وإضافة المعلمة $Pzoi^2$ (السطور التسعة الأخيرة من الجدول 75).

الجدول 75 – ربط مجال التشوه بقطعتي البيانات
(توسيع المثال 3 للمعلمة ZOI الوارد في الفقرة 3.1.6)

المعلمة			الطول (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق 1
$Zone^0$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف الوصف المتعلق بغير الصورة
			6	010001_b	أمدية الأثمونات بعد الواسم SOD محددة وكذلك مجالات التشوه المصاحبة
	$Pzoi^2$	$Mzoi^2$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	1_b	تتحدد عدة بنود
			2	01_b	أسلوب المدى
			2	01_b	المعلمة Izoi تستعمل عدد صحيح من 16 بتة
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Nzoi^2$	8 (RBAS)	2	عدد قطع البيانات 2
		$Izoi^{2,1}$	16	0000 0000 0000 1010_b	موقع أثمون البداية هو العاشر (أثمونات)
			16	0000 0000 0110 0100_b	موقع أثمون النهاية هو المائة (أثمونات)
$Zone^0$	$Pzoi^2$	$Izoi^{2,2}$	16	0010 0111 0001 0000_b	موقع أثمون البداية هو الأثمون 10000
			16	0010 1110 1110 0000_b	موقع أثمون النهاية هو الأثمون 12000
	$Pzoi^6$	$Mzoi^6$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	1_b	تتحدد عدة بنود
			2	10_b	أسلوب الدليل
			2	00_b	تستخدم المعلمة Izoi 8 بتات من أجل تمثيل كل قيمة تشوه
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Nzoi^6$	8 (RBAS)	2	عدد قطع البيانات 2
		$Izoi^{6,1}$	8	D1 value	قيمة التشوه للقطعة الأولى
		$Izoi^{6,2}$	8	D2 value	قيمة التشوه للقطعة الثانية

2.4.6 المثال 2

يصف هذا المثال كيفية ربط قيم التشوه بالرزم JPEG 2000. وتعيِّن المعلمة DCzoi مدى من 4 رزم ويشار أيضاً إلى مجال التشوه. وتعطي المعلمة $Pzoi^1$ مدى الرزم وتصل المعلمة $Pzoi^2$ التشوه المصاحب لكل من هذه الرزم. ويلاحظ أنه، بما أن $Pzoi^1$ تعين مدى طول قدره 4 فإن $Pzoi^2$ تحدد 4 قيم، وكل بند في المدى يصاحب قيمة واحدة، أي أن كل رزمة مرتبطة بتشوه واحد.

الجدول 76 – تشوير مدى الرزم وإرفاق قيم التشوه بكل رزمة

المعلمة			الطول (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8 (RBAS)	1	عدد المناطق واحد
$Zone^0$	DCzoi		1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	1_b	صنف وصف متعلق بغير الصورة
			6	100001_b	تتحدد الرزم ومجالات التشوه المصاحب
	$Pzoi^1$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	0_b	يتحدد بند واحد
			2	01_b	أسلوب المدى
			2	00_b	المعلمة Izoi تستعمل عدد صحيح من 8 بتات
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Nzoi^1$	8 (RBAS)	1	عدد قطع البيانات 1
		$Izoi^{11}$	8	$0000\ 0000_b$	رقم رزمة البداية 0
			8	$0000\ 0011_b$	رقم رزمة النهاية 3
	$Pzoi^6$	$Mzoi^6$	1	0_b	قطعة الأثمونات المتراصفة لا تلي
			1	0_b	المناطق المحددة تتأثر بالأداة JPSEC
			1	1_b	تتحدد عدة بنود
			2	10_b	أسلوب الدليل
			2	00_b	تستعمل المعلمة Izoi 8 بتات لتمثيل كل قيمة تشوه
			1	0_b	توصف المعلمة Izoi ببعد واحد
		$Nzoi^6$	8 (RBAS)	4	عدد قطع البيانات 4
		$Izoi^{6,1}$	8	القيمة D1	قيمة التشوه في الرزمة الأولى
		$Izoi^{6,2}$	8	القيمة D2	قيمة التشوه في الرزمة الثانية
		$Izoi^{6,3}$	8	القيمة D3	قيمة التشوه في الرزمة الثالثة
		$Izoi^{6,4}$	8	القيمة D4	قيمة التشوه في الرزمة الرابعة

7 سلطة تسجيل المعيار JPSEC

1.7 مقدمة عامة

تتيح آلية تسجيل المعيار JPSEC تعرف الهوية دون لبس لأدوات الأمن غير المعيارية التي تلحق بالمعيار JPSEC والتي يمكن اقتراحها مستقبلاً أو تطويرها كأدوات JPSEC غير معمارية تضاف إلى تلك الأدوات الواردة في الملحق B. وسلطة التسجيل JPSEC هي التي تقوم بهذا التسجيل الذي يمتثل لتوجيهات اللجنة JTC 1. وتتم مراقبة تسجيل هذه الأدوات الجديدة JPSEC من خلال العمليات المحددة في هذه الفقرة.

ويجوز لأصحاب الطلبات أن يقدموا تقنيات يودون ضمها إلى القائمة JPSEC المرجعية. ويجدر بالذكر أن استخدام الأداة JPSEC يتحدد في واسم JPSEC موجود في التدفق المشفر. وعندما يصادف التطبيق معرف هوية JPSEC غير معروف يمكنه الاتصال بسلطة التسجيل JPSEC RA والحصول على المعلومات المدونة لديها عن الأداة المعنية.

2.7 معايير القبول لطالبي التسجيل

الطالبون المؤهلون هم المنظمات المعترف بها من قبل هيئاتها الوطنية.

3.7 طلبات التسجيل

تنشر سلطة التسجيل JPSEC طلبات تسجيل أدوات JPSEC جديدة على موقع إلكتروني.

ويشتمل الموقع على استمارات طلب التسجيل وطلب التحديث والتبليغ عن تخصيص ما أو عن تحديثه ورفض الطلب.

وتحتوي جميع الاستمارات على ما يلي:

- اسم المنظمة صاحبة الطلب؛
- عنوان المنظمة صاحبة الطلب؛
- اسم الشخص الذي يمكن الاتصال به في المنظمة ومنصبه وعنوانه البريدي والإلكتروني ورقم هاتفه وفاكسه.

وتضم استمارات طلب التسجيل وطلب التحديث أيضاً البنود التالية:

- اسم الأداة JPSEC (إلزامي).
- نمط الأداة JPSEC، مثال: توقيع رقمي، وسم رقمي، تجفير، تخليط توليد وإدارة مفاتيح، استيقان ... (خياري).
- وصف تقني موجز (إلزامي).
- وصف عام للأداة (إلزامي).
- وصف حالة استعمال كمثال للتشغيل (خياري).
- مواصفة قواعد تركيب المعلمات مع بعض القيم الممكنة (خياري).
- خطوط توجيهية للاستعمال الأمثل (خياري).
- وضع حقوق الملكية الفكرية، مثال: المالك، صاحب الحق (خياري).
- شروط حقوق الملكية الفكرية للاستخدام (إلزامي).
- قيود الاستخدام مثل شروط التصدير (خياري).
- معلومات عن نسخ التطبيقات (خياري).
- شروحات إضافية، الأسباب الداعية، المراجع وغيرها (خياري).
- متطلبات السرية لمداخل التطبيق المختارة (خياري).
- المدة المطلوبة لتسجيل الأداة (خياري).

وتوفر سلطة التسجيل JPSEC أيضاً المواد التوجيهية التي تساعد المتقدمين بالطلبات على إعداد الطلبات.

4.7 استعراض الطلبات والرد عليها

تحدد هذه الفقرة العمليات التي تقوم بها سلطة التسجيل JPSEC للنظر في الطلبات والرد عليها ضماناً لإنصاف أصحاب الطلبات.

تنشأ لجنة تقنية للنظر في الطلبات. وتتألف هذه اللجنة من أعضاء في ISO/IEC JTC 1/SC 29/WG 1 وأعضاء في سلطة التسجيل JPSEC. وتتفحص هذه اللجنة الطلبات في اجتماع لفريق العمل 1 في غضون الأشهر التسعة التي تلي تاريخ تقديم الطلب.

وتقبل لجنة النظر في الطلبات الطلب أو ترفضه استناداً إلى معايير الرفض الواردة في الفقرة 5.7.

وفي حالة قبول الطلب، يخصص معرف هوية (ID) إلى الأداة JPSEC الجديدة لفترة محددة من الزمن. وينبغي أن تمتثل قواعد تركيب المعرف ID لأحكام الفقرة 3.6.5. وتوافق اللجنة على المعلومات الواردة في 3.7 والتي تصف الأداة JPSEC. ويستخدم بعدئذٍ المعرف ID في عمليات التشوير في التدفق JPSEC.

وبعد دراسة الطلب وقبوله تبلِّغ السلطة JPSEC RA صاحب الطلب بالرد الإيجابي أو السلبي على طلب التسجيل. ويتضمن الرد على صاحب الطلب شرحاً موجزاً لنتائج الفحص التقني ويرسل إليه في مدة أقصاها تسعة أشهر من تاريخ تقديم الطلب.

ويجوز الاعتراض على الرد السلبي، إذا ما اعتقد طالب التسجيل أن خطأ ما سبَّب الرفض، أو عندما يتطلب ذلك معلومات إضافية لتوضيح بعض المسائل أو المخاوف. وإذا طالب صاحب الطلب بدراسة إضافية تتجاوز إجراءات السلطة، يمكنه أن يقدم حالته لتنظر فيها اللجنة الموسعة لفريق العمل 1 في الاجتماع اللاحق المناسب للفريق WG 1. وقد يُطلب منه عند ذلك تقديم معلومات إضافية بناء على طلب الخبراء الذين سيقدمون بموجب سلطة الفريق WG 1، الرد النهائي الحاسم بالقبول أو بالرفض. ومن أجل الحصول على إمكانية أن يعيد الفريق WG 1 النظر في طلب مرفوض، يتعين على طالبي التسجيل أن يقدموا الاقتراح من جديد من خلال هيئاتهم الوطنية مع تحديد الأسباب الداعية لإعادة الفريق WG 1 النظر فيها.

5.7 رفض الطلبات

معايير رفض الطلبات هي التالية:

- عدم أهلية الطالب.
- عدم تسديد الرسوم المطلوبة (حسب الاقتضاء).
- وجود بند سبقت الموافقة عليه وتسجيله يشتمل على نفس المحتويات المقدمة في الطلب.
- المعلومات الواردة في الطلب منقوصة أو غير مفهومة.
- حجة الإدراج في سجل التسجيل واهية. وينبغي أن تبرهن الأداة JPSEC المرشحة على أنها توفر خدمة أمن مفيدة وأن تعطي أمثلة لحالات الاستعمال حسب الاقتضاء.
- اعتبار سلطة التسجيل أن الأداة المرشحة ينقصها الابتكار الكافي ويمكن بسهولة الاستعاضة عنها بأداة مرخصة ومعتمدة.
- وجود أخطاء في تقديم الطلب أو عدم امتثاله لمواصفات JPSEC المعيارية أو للمعيار JPSEC.
- الوصف التقني غير واف.
- شروط السرية غير مناسبة.

6.7 تخصيص معرفات الهوية وتسجيل تعاريف الأغراض

تؤكد إجراءات الدراسة والقواعد الواردة أعلاه أن المعرف ID المخصص فريد في السجل وأنه غير مخصص لغرض آخر.

وبعد إجراء التخصيص، يجب إدراج المعلومات المصاحبة للمعرف ID في السجل ويجب أن تُعلِم سلطة التسجيل JPSEC صاحب الطلب بهذا التخصيص في غضون الأشهر التسعة التالية للتخصيص.

ويسجل تعريف الأداة JPSEC في السجل لحظة تخصيص المعرف ID.

1.6.7 إعادة استعمال المعرفات ID

يجوز لسلطة التسجيل أن تعيد استعمال المعرفات ID. على سبيل المثال، تصبح المعرفات ID قابلة للاستعمال من جديد بعد انقضاء مدة صلاحيتها أو عندما يتم الاستغناء عنها طوعاً أو عندما يطالب بذلك.

ويجوز لمالكي المعرفات ID أن يتخلوا عنها من خلال تقديم طلب تحديث.

2.6.7 استرداد المعرف

يجوز لسلطة التسجيل JPSEC أن تطالب باسترداد معرف هوية لأسباب تقنية أو لإساءة استعمال الأداة. وفي هذه الحالة، يبلَّغ مالكو المعرفات في رسالة تبليغ بتحديث.

7.7 الصيانة

تطبق سلطة التسجيل JPSEC لأغراض صيانة السجل آليات من شأنها أن تحافظ على سلامة السجل بما في ذلك العمليات الملائمة للحفاظ على السجلات.

ويجوز لمالك معرف ID أن يحدِّث المعلومات المصاحبة للأداة JPSEC من خلال طلب تحديث.

ويتعين على سلطة التسجيل JPSEC أن توفر الآليات اللازمة للمحافظة على سرية المعلومات كما يُفترض في طلب التسجيل.

8.7 نشر السجل

تكمن مصلحة جماعة مستخدمي تكنولوجيا المعلومات عموماً في جعل معلومات السجل متاحة للجميع. غير أن السرّية، في بعض الحالات ضرورية فيما يتعلق بالبيانات الخاضعة لتسجيل ما أو بجزء منها، وذلك إما بشكل دائم أو أثناء بعض أجزاء عملية التسجيل.

وعلى سلطة التسجيل JPSEC أن تنشر معلومات السجل على نحو يتوافق ومتطلبات سرية الأداة JPSEC.

وعند لزوم النشر، فإن النسخ الإلكترونية والورقية إلزامية. وإذا كانت سلطة تسجيل JPSEC مسؤولة عن توفير النشر، فإن عليها أن تدقق في سجلات التوزيع المتعلقة بنشرها.

9.7 متطلبات معلومات السجل

تنشر سلطة التسجيل JPSEC إلكترونياً في سجلها قائمة الأدوات JPSEC غير المعيارية والمعلومات المصاحبة لهذه الأدوات بطريقة تتوافق ومتطلبات السرية للأداة JPSEC.

وفيما يلي المعلومات التي يتضمنها السجل والمتعلقة بكل أداة JPSEC:

- معرف الهوية (ID) المخصص؛
- اسم صاحب الطلب الأولي؛
- عنوان صاحب الطلب الأولي؛
- تاريخ التخصيص الأولي؛
- تاريخ آخر تغيير في التخصيص إن وجد (قابل للتحديث)؛
- اسم المالك الحالي (قابل للتحديث)؛
- عنوان المالك الحالي (قابل للتحديث)؛
- اسم الشخص الذي يمكن الاتصال به في المنظمة وصفته وعنوانه البريدي/الإلكتروني ورقم هاتفه وفاكسه؛
- تاريخ آخر تحديث طرأ (قابل للتحديث).

كما يشتمل السجل أيضاً على المعلومات المقدمة من صاحب الطلب حول الأداة JPSEC المقترحة، كما يرد في الفقرة 3.7، وعلى المعلومات التي حظيت بالموافقة.

الملحق A

خطوط توجيهية وحالات استخدام

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

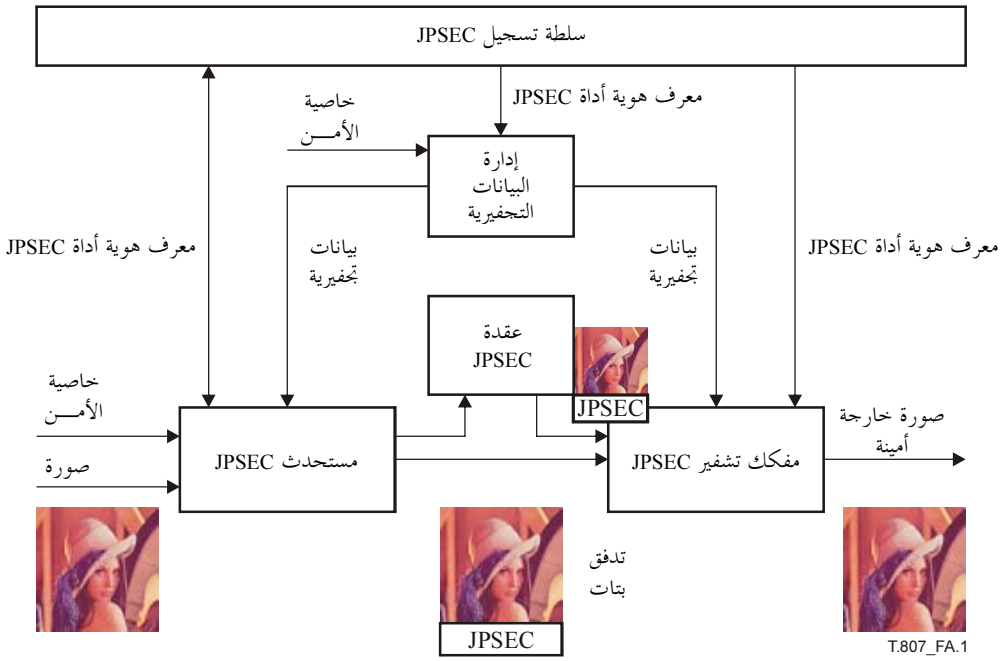
1.A صنف من التطبيقات JPSEC

1.1.A مقدمة

تقدم هذه الفقرة وصفاً نظرياً لكيفية تنفيذ صنف من التطبيقات JPSEC. ويمثل هذا الصنف سيناريوهات أمن توزيع الصور JPEG 2000. وتصف الفقرات التالية لمحة عامة لمفهوم التطبيق JPSEC بما فيه الكيانات JPSEC والمعلومات المتبادلة فيما بينها. وهذا الوصف مفاهيمي ولا يفترض أنه يصف التطبيق وصفاً عملياً أو يحدد متطلبات تطبيق معين؛ وقد تضم التطبيقات الخاصة أو لا تضم الكيانات المحددة في الوصف التالي.

2.1.A الشكل العام للتوزيع الأمين لصورة JPEG 2000

يبين الشكل 1.A منظراً عاماً لصنف من التطبيقات JPSEC لتوزيع أمين للصورة JPEG 2000. وقد يُطلب من التطبيق JPSEC في هذه التطبيقات توفير خدمات أمن مختلفة للصور JPEG 2000، مثل سرّية تبادل الصور والتحقق من مصدر الصور ومحتواها.



الشكل 1.A – منظر عام لتطبيق توزيع أمين للصور JPEG 2000

ويمكن في تطبيق التوزيع الأمين للصورة JPEG 2000 تحديد الخطوات التالية:

الخطوة 1: يستحدث المستحدث JPSEC التدفق المشفر JPSEC.

الخطوة 2: يوزّع التدفق المشفر JPSEC عبر عقدة JPSEC واحدة أو أكثر.

الخطوة 3: يستقبل المستهلك JPSEC التدفق المشفر JPSEC ويستعيده.

الخطوة 1: استحداث التدفق المشفر JPSEC

ينبغي للمستحدث أن يستحدث تدفقاً مشفراً JPEG 2000 أميناً. ويمكن استحداث هذا التدفق من بيانات مخطط البتات أو من البيانات JPEG 2000 المنضغطة. ويستخدم المستحدث JPSEC تقنيات أمن مختلفة مثل التجفير والتوقيع وقيمة التحقق التكاملية (ICV) في بيانات صورة معينة.

ويحدد المستحدث خاصية معلمات الأمن المصاحبة للصورة من أجل توفير أمن بيانات الصورة. وتضم "خاصية معلمات الأمن" النعوت التالية:

- منطقة التأثير (منطقة تغطية كل طريقة حماية)؛
- مجال المعالجة (المجال الذي تعالجه كل طريقة من طرق الحماية)؛
- تعرف هوية الأداة JPSEC (خوارزمية التجفير المستخدمة والمعلمات المتصلة بها).

الخطوة 2: إرسال تدفق مشفر JPSEC

يمكن نقل تدفق مشفر JPSEC إلى مستهلك JPSEC مباشرة عبر شبكة أو وسيط ما (مثل القرص CD-ROM). كما يمكن نقله عبر عقدة JPSEC وقد تستعمل عدة أنواع أخرى للعمل مثل تحويل الشفرة إلى تدفق شفرة JPSEC.

ويتعين على المستحدث JPSEC أن يعطي المستهلك JPSEC بيانات التجفير اللازمة في قناة مستقلة ('سرية') إذا ما اشترطت طرائق أو أدوات الأمن JPSEC ذلك في معلمة خاصية الأمن في التدفق المشفر JPSEC (مثل التجفير، أو للتحقق). وبالإمكان إدارة هذه البيانات ومنها مثلاً المفتاح أو التوقيع الرقمي يدوياً أو أوتوماتياً من قبل إدارة بيانات التجفير.

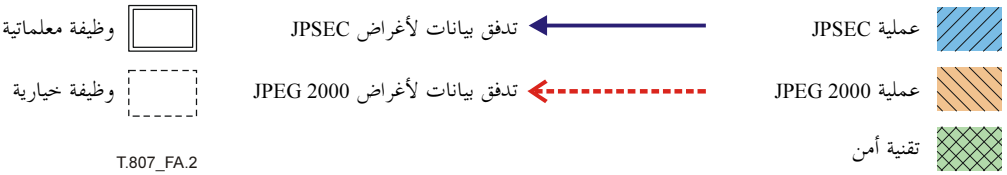
الخطوة 3: استعادة استهلاك التدفق المشفر JPSEC

التدفق المشفر JPSEC خاضع لمعالجة المستهلك JPSEC وفقاً لخاصية معلمات الأمن المطبقة. ويفترض ذلك تطبيق تقنيات أمن ملائمة مثل فك التجفير والاستيقان والتحقق من التكاملية. ومن ناحية أخرى يمكن للمستحدث JPSEC وللمستهلك JPSEC أن يستعملا أنواع مختلفة من بيانات التجفير لكل طريقة من طرائق أمن أداة JPSEC.

وتنتج بيانات و/أو أمن صورة مفككة التجفير كنتيجة التحقق مثلاً بمثابة ناتج عند المستهلك JPSEC.

ويمكن أن يحيل مستحدث JPSEC أو مستهلك JPSEC أو إدارة بيانات التجفير إلى سلطة التسجيل JPSEC من أجل الحصول على التعليمات اللازمة لمعالجة معرف هوية أداة JPSEC محدودة.

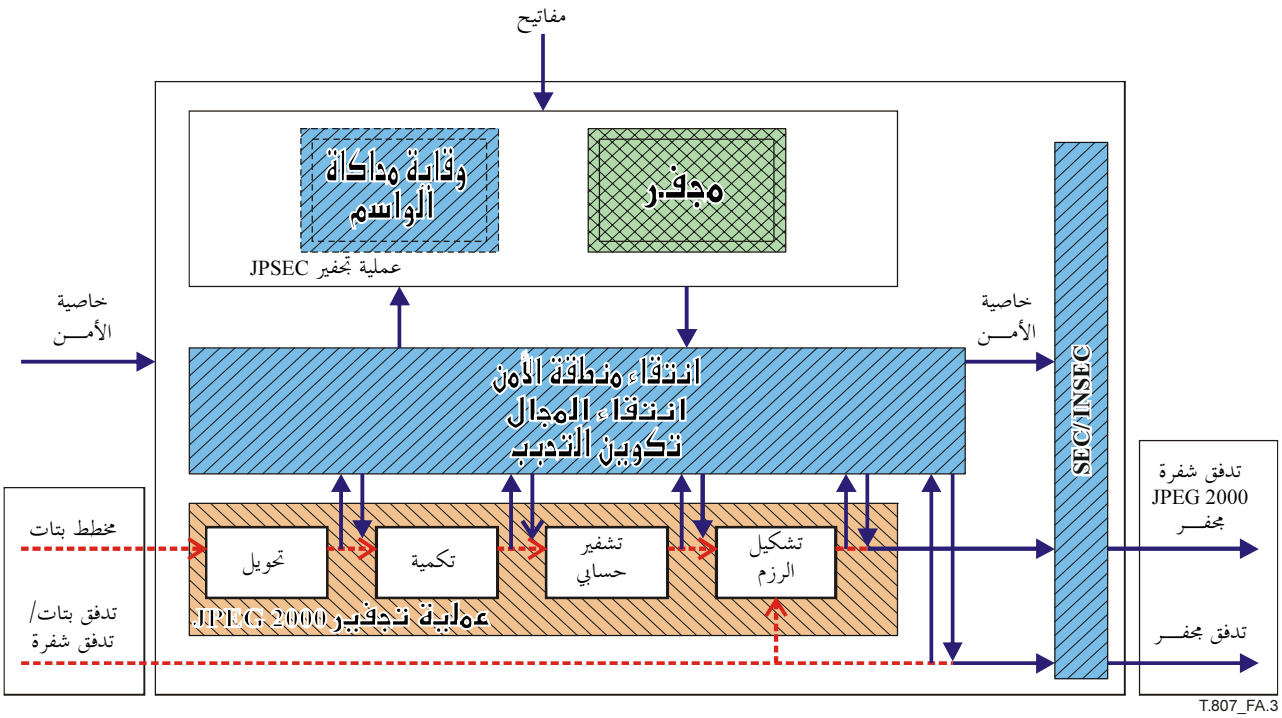
وتقدم الفقرات التالية مزيداً من التفاصيل عن الكيان المفهوم JPSEC حسب خدمة JPSEC ما. ويبين الشكل 2.A وصف الرموز الواجب استخدامه.



الشكل 2.A – وصف الرموز

- **عملية JPSEC**: عملية تستخدم الأدوات المعرفة في هذه التوصية | المعيار الدولي.
- **عملية JPEG 2000**: عملية معرفة في التوصية | المعيار الدولي ISO/IEC 15444-1 ITU-T Rec. T.800 (JPEG 2000) الجزء 1).
- **تقنية أمن**: تقنية أمن معروفة جيداً ومحددة إما في هذه التوصية | المعيار الدولي وإما في معيار أو وثيقة أخرى.
- **تدفق بيانات لأغراض المعيار JPSEC**: تدفق بيانات ينقل معلومات معرفة في هذه التوصية | المعيار الدولي. ويدل الخط المتقطع على صفة خياري.
- **تدفق بيانات لأغراض المعيار JPEG 2000**: تدفق بيانات لحزمة في التوصية | المعيار ISO/IEC 15444-1 ITU-T Rec. T.800 (JPEG 2000) الجزء 1).
- **وظيفة معلماتية**: وظيفة تضم عدة وظائف يمكن أن ينتقيها التطبيق.
- **وظيفية خيارية**: وظيفة يستطيع التطبيق JPSEC أن يستخدمها خيارياً.

3.1.A إجراء وصف نهاية التجفير

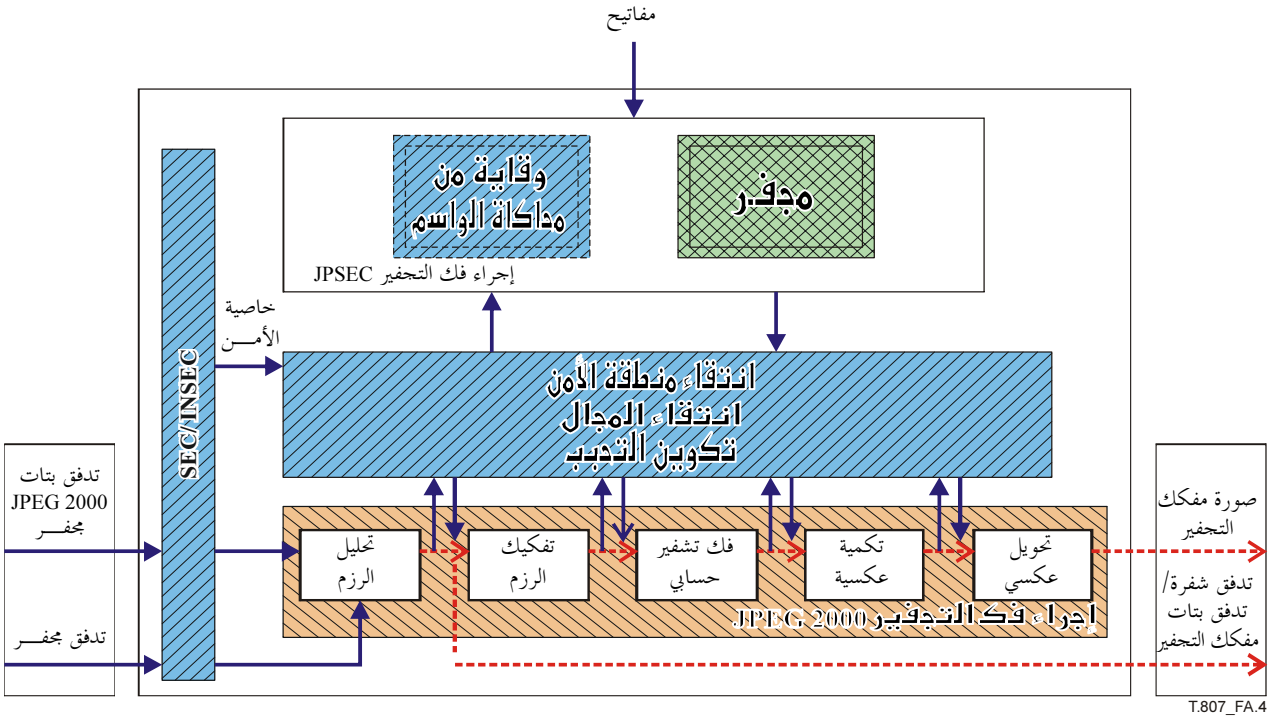


الشكل 3.A – إجراء التجفير

يبين الشكل 3.A المخطط العام لمثال إجراء التجفير الذي يقوم به المستحدث، JPSEC. ويضم هذا الإجراء العمليات التالية:

- استخراج بيانات وفقاً لمجال المعالجة المحدد؛
- انتقاء جزء من البيانات المستخرجة وفقاً لمنطقة التأثير المحددة (أي تجفير جزئي)؛
- تجفير البيانات المنتقاة باستعمال تقنية الأمن المحددة. كما يمكن تجفير البيانات في وحدة ما استناداً إلى التحبب. وفي هذه الحالة يمكن استخدام مفاتيح مختلفة لوحدات مختلفة؛
- استبدال بيانات النص المكتوب ببيانات مجفرة؛
- استخدام آلية وقاية محاكاة الواسم (خيارية)؛
- تشكيل خاصية معلمة الأمن في قطعة الواسم SEC و/أو INSEC.

ويلاحظ أن إجراء التجفير JPSEC يولّد عموماً تدفقات مشفرة JPSEC غير متوائمة مع الجزء 1 من المعيار JPEG 2000. ويفترض أن ترسل بيانات الصورة إلى مفكك تشفير يمتثل للمعيار الجزء 1 بعد عملية فك التشفير الملائمة. ويمكن استخدام آلية الوقاية من محاكاة الواسم من أجل تجنب محاكاة القطعة في التدفق المشفر المجفر.

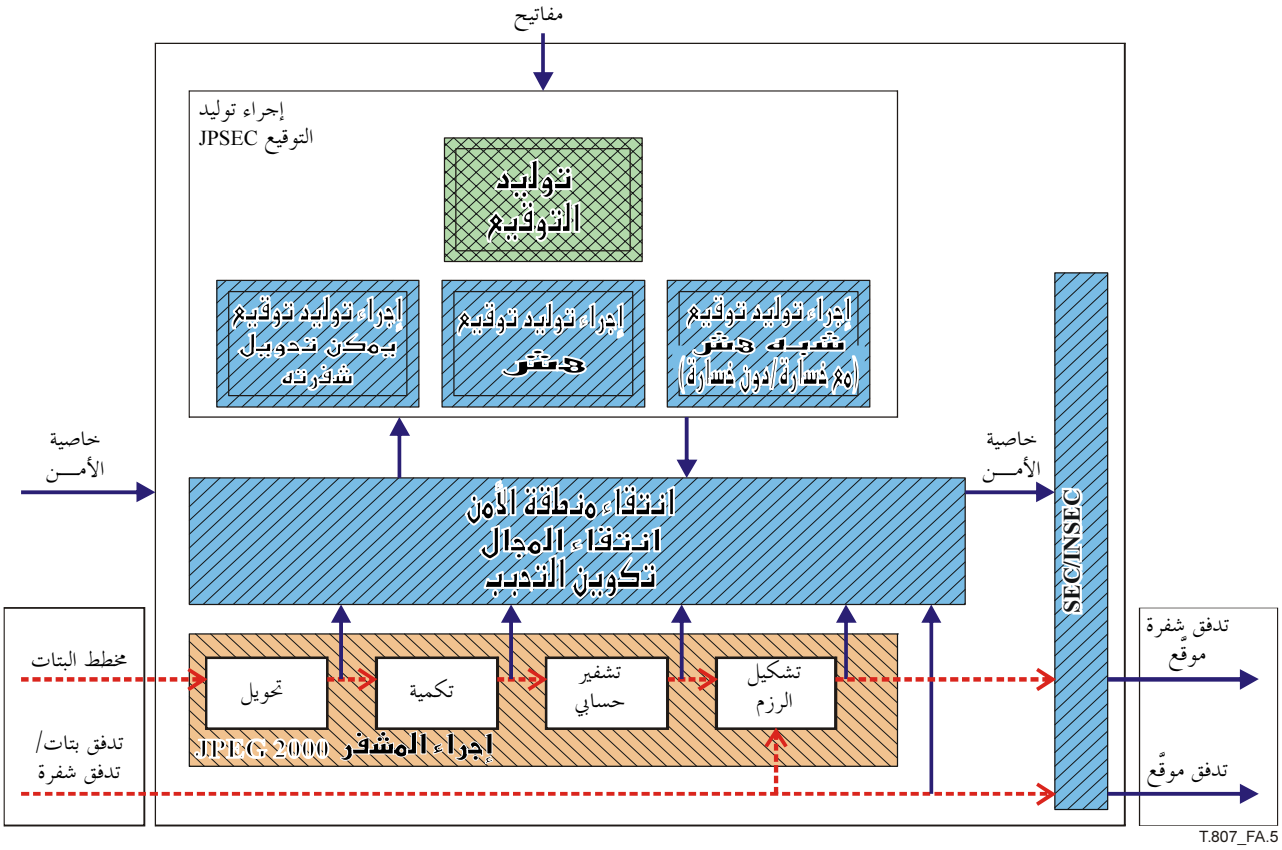


الشكل 4.A – إجراء فك التجفير

يبين الشكل 4.A المخطط العام لمثال إجراء فك التجفير عند مستهلك JPSEC ويضم هذا الإجراء العمليات التالية:

- تحليل خاصية معلمة الأمن في قطعة الواسم SEC و/أو INSEC؛
- استخراج البيانات وفقاً لمجال المعالجة المشار إليه؛
- انتقاء جزء من البيانات المستخرجة وفقاً للمفاتيح المحتفظ بها (أي فك تجفير جزئي)؛
- فك تجفير البيانات المنتقاة باستخدام تقنية الأمن المشار إليها. كما يمكن فك تجفير البيانات في وحدة ما استناداً إلى التحبب؛
- استبدال بيانات مجفرة ببيانات مفكوكة التجفير.
- استخدام آلية وقاية من محاكاة الواسم إن كانت مستخدمة في عملية التجفير.

4.1.A إجراء توليد التوقيع والاستيقان

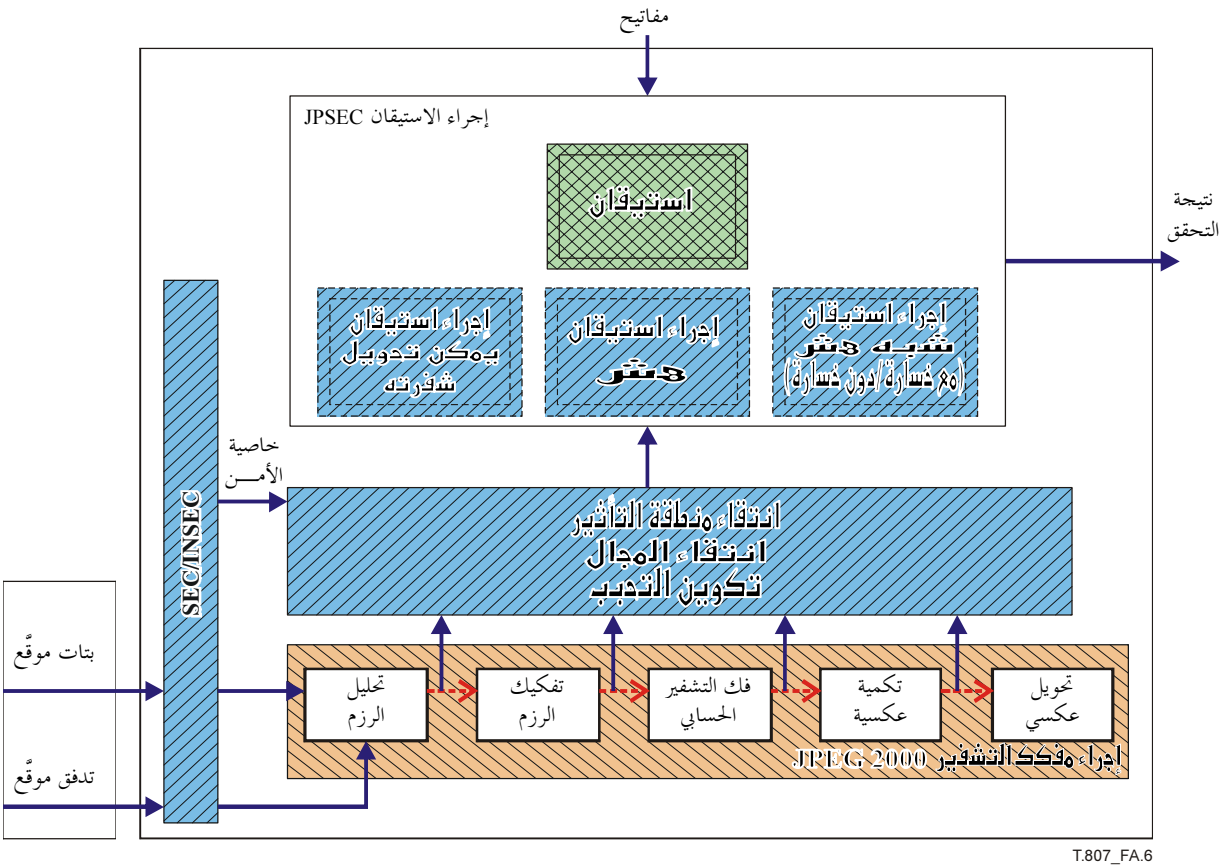


الشكل 5.A – إجراء توليد التوقيع

يبين الشكل 5.A المخطط العام لمثال إجراء توليد توقيع يقوم به المستحدث JPSEC. ويضم هذا الإجراء العمليات التالية:

- استخراج البيانات وفقاً لمجال المعالجة المحدد؛
- انتقاء جزء من البيانات المستخرجة وفقاً لمنطقة التأثير المحددة (أي توقيع جزئي)؛
- حساب التواقيع الرقمية المقابلة للبيانات المنتقاة باستخدام تقنية الأمن المحددة. كما يمكن توليد تواقيع رقمية في وحدة تستند إلى التحبب؛
- تكوين خاصية معلمة الأمن بما فيها التواقيع الرقمية المحسوبة في قطعة الواسم SEC و/أو INSEC.

ويلاحظ أن أساليب الاستيقان الثلاثة في المعيار JPSEC هي: "أسلوب هش" و"أسلوب شبه هش (مع خسارة/دون خسارة)"، و"أسلوب قابل للتحويل". ويمكن لاستيقان "الأسلوب الهش" أن يكشف أي تغيير في بتة واحدة في التدفق المشفر، ويمكن لاستيقان "الأسلوب شبه الهش" أن يكشف أي محاولة كشف غير مقصودة، ولكنه لا يستطيع مقاومة التشوهات المفاجئة إلا لدرجة محددة مسبقاً. أما استيقان أسلوب تحويل الشفرة فإنه قادر على التحقق من الطرف مصدر تدفق الشفرة.

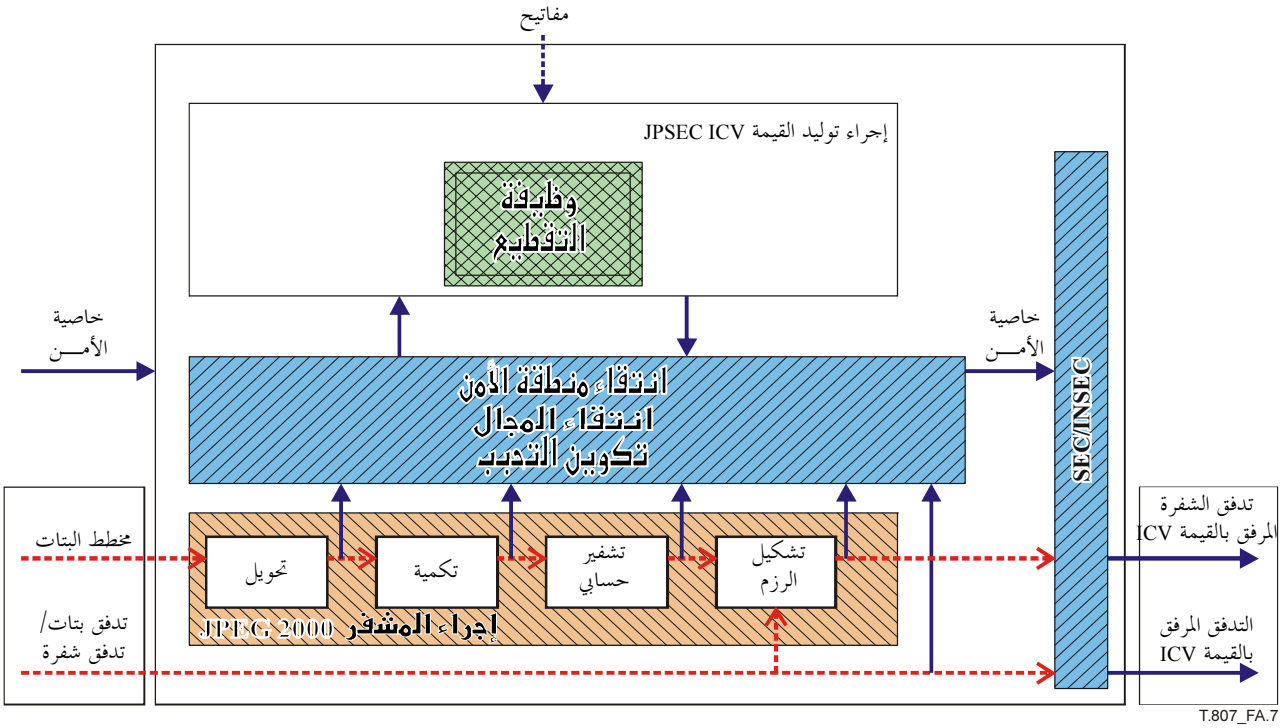


الشكل 6.A – إجراء الاستيقان

يبين الشكل 6.A المخطط العام لمثال إجراء الاستيقان عند مستهلك JPSEC. ويضم هذا الإجراء العمليات التالية:

- استخراج البيانات من مجال المعالجة المشار إليه؛
- انتقاء جزء من البيانات المستخرجة وفقاً لمنطقة التأثير المشار إليها؛
- التحقق من البيانات المنتقاة باستخدام تقنية الأمن المشار إليها. كما يمكن أيضاً التحقق من البيانات المنتقاة في وحدة ما استناداً إلى التحبب.

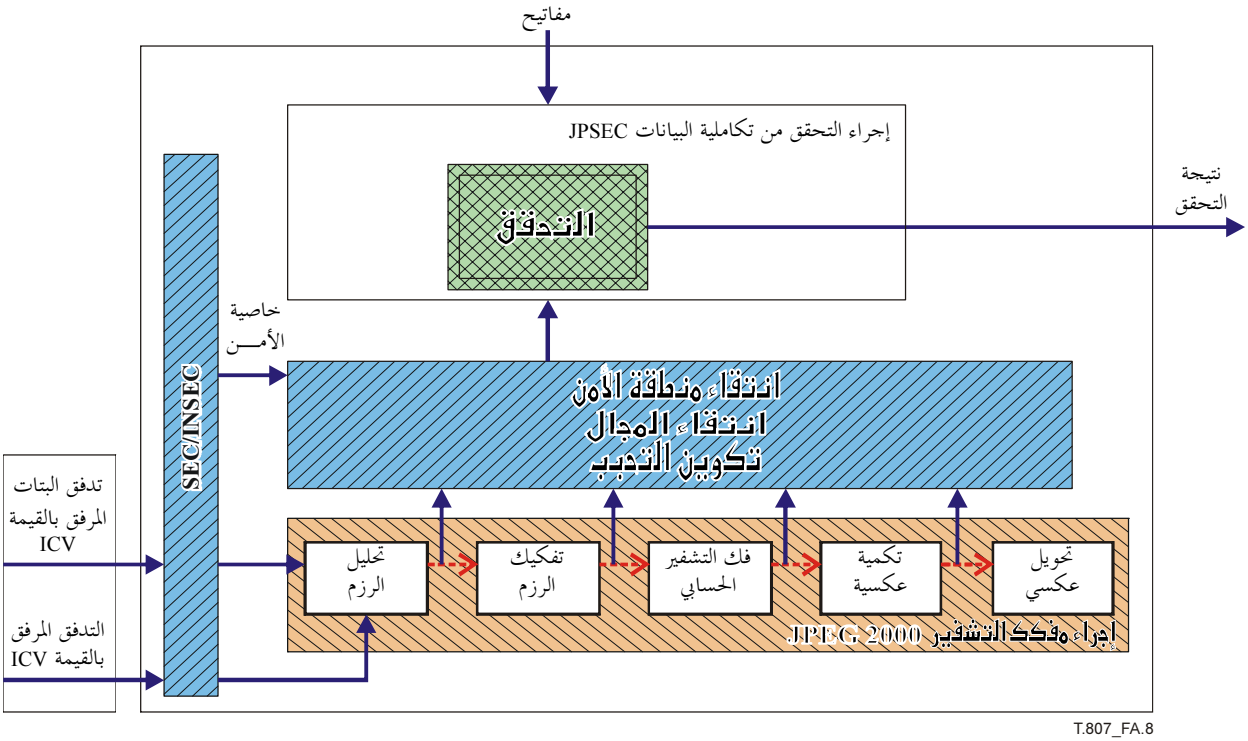
5.1.A إجراء توليد قيمة التحقق من التكاملية (ICV) والتحقق من التكاملية



الشكل 7.A – إجراء توليد قيمة التحقق من التكاملية (ICV)

يبين الشكل 7.A المخطط العام لمثال إجراء توليد القيمة ICV عند مستحدث JPSEC. ويضم هذا الإجراء العمليات التالية:

- استخراج البيانات من مجال المعالجة المشار إليه؛
- انتقاء جزء من البيانات المستخرجة وفقاً لمنطقة التأثير المحددة؛
- حساب القيم ICV المقابلة للبيانات المنتقاة باستخدام تقنية الأمن المحددة. كما يمكن أيضاً توليد قيم ICV في وحدة ما استناداً إلى التحبب؛
- تكوين خاصية معلمة الأمن بما فيها القيم ICV المحسوبة في قطعة واسم SEC و/أو INSEC.



الشكل 8.A – إجراء التحقق من التكاملية

يبين الشكل 8.A المخطط العام لمثال إجراء التحقق من التكاملية الذي يقوم به مستهلك JPSEC. ويضم هذا الإجراء العمليات التالية:

- استخراج للبيانات وفقاً لمجال المعالجة المشار إليه،
- انتقاء جزء من للبيانات المستخرجة وفقاً لمنطقة التأثير المشار إليها؛
- التحقق من للبيانات المنتقاة باستخدام تقنية الأمن المشار إليها. وكما يمكن أيضاً التحقق من للبيانات المنتقاة في وحدة ما استناداً إلى التحبب.

الملحق B

أمثلـــة تقنيـــة

(يشكّل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

1.B مقدمة

توفّر قواعد تركيب المعيار IPSEC أدوات الأمن المعيارية وغير المعيارية التي تُستخدم لأغراض الصور JPEG 2000. وتقدم هذه الفقرة على سبيل الإعلام عشرة أمثلة تقنية تبين استعمالات مختلفة للمعيار JPSEC. وترد هذه الأمثلة على سبيل الإعلام فقط ولا تؤخذ بعين الاعتبار في المعيار JPSEC. لكنها تعطى هنا لإظهار مرونة هذا المعيار.

وتضم الأمثلة التقنية ما يلي:

- نظام مرن لمراقبة النفاذ في المعيار JPEG 2000؛
- إطار استيقان موحد للصور JPEG 2000؛
- طريقة بسيطة لتجفير التدفقات المشفرة JPEG 2000 بأسلوب الرزم؛
- أداة تجفير لمراقبة النفاذ إلى النظام JPEG 2000؛
- أدوات توليد المفاتيح لمراقبة النفاذ إلى النظام JPEG 2000؛
- تخليط مجال تدفق البتات والموجات الصغيرة لأغراض مراقبة النفاذ الشرطية؛
- النفاذ التدريجي في التدفق المشفر JPEG 2000؛
- الاستيقان القابل للقياس للتدفقات المشفرة JPEG 2000؛
- سرية البيانات JPEG 2000 ونظام مراقبة النفاذ من خلال تقطيع البيانات وحجبها؛
- تدفق أمين قابل للقياس وتحويل شفرة أمين.

2.B نظام مرن لمراقبة النفاذ إلى التدفقات المشفرة JPEG 2000

1.2.B خدمة الأمن

يتيح نظام مراقبة النفاذ نقل التدفقات المشفرة JPEG 2000 وفقاً لأي تشكيلة من الاستبانات وطبقات النوعية والرقع والمناطق.

2.2.B التطبيق النموذجي

يوفر الحماية لتسليم المحتوى عبر وسائط متنوعة مثل الإنترنت والكبل التلفزيوني الرقمي والإذاعة الساتلية والأقراص المتراصة. وتُستخدم التكنولوجيا عموماً في التطبيقات التي يجفر فيها التدفق المشفر مرة واحدة فقط من جهة الناشر لكن التدفق المشفر المحمي فيجفر بعدة طرق حسب الامتيازات المختلفة في جهة المستعمل.

3.2.B الباعث

في نموذج التوزيع الأكبر يوزع الناشر المحتويات المحمية مجاناً ومفاتيح المحتويات بشكل أمين. فالمستعمل الذي يرغب في النفاذ إلى أجزاء من التدفق يرسل طلبه إلى المخدم الرئيسي الذي يجيب بدوره ويرسل مفاتيح فك التجفير المناسبة وفقاً لامتيازات المستعمل. ويستطيع المستعمل النفاذ إلى الصور الفرعية المتاحة.

4.2.B المخطط العام التقني

ينتج التدفق المشفر المحمي JPEG 2000 عن تشفي الناشر لكل رزمة منه. وأساس هذه التقنية هو كيفية استخدام تفرعات مفاتيح تُبنى حسب أي ترتيب للرقع والمكونات والاستبانات والطبقات والمناطق وفدر الشفرة. ومن أجل وصف التقنية بسهولة، يُفترض أن ترتيب تفرعات المفاتيح هو RLCP (استبانة – طبقة – مكونة – منطقة) وأن لكل استبانة نفس عدد المناطق. وفيما يلي وظيفة تقطيع h(.) باتجاه واحد ويُعتبر التدفق المشفر لصورة JPEG 2000 مع رقع n_T ومكونات n_C وطبقات n_L واستبانة n_R لمكونة الرقعة الواحدة ومناطق n_P للاستبانة الواحدة. ويُبنى تفرع المفاتيح بوجود مفتاح رئيسي K للتدفق المشفر JPEG 2000 على النحو التالي:

1) توليد المفتاح $k^t = h(K|"T"|t)$، لكل رقعة $t = 0, 1, \ldots, n_T-1$، حيث الرمز "|" يعني التسلسل، والرمز *"T"* شفرة الترميز ASCII للحرف T.

2) توليد المفتاح $k^r = h(k^{r+1})$، لكل $r = n_R - 2, \ldots, 1, 0$، حيث $k^{n_R - 1} = h(k^l | "R")$ و"R" تعني شفرة الترميز ASCII للحرف R.

3) حساب المفتاح $k^{rl} = h(k^{r(l+1)})$، لكل $r = n_R - 1, \ldots, 1, 0, l = n_L - 2, \ldots, 1, 0$، حيث $k^{r(n_L - 1)} = h(k^r | "L")$ وحيث "L" تعني شفرة الترميز ASCII للحرف L.

4) حساب المفتاح $k^{rlc} = h(k^{rl} | "C" | c)$، لكل $r = n_R - 1, \ldots, 1, 0, l = n_L - 1, \ldots, 1, 0, c = 0, 1, \ldots, n_C - 1$، حيث "$C$" تعني شفرة الترميز ASCII للحرف C وc تعني دليل هذه المكونة.

5) إنتاج المفاتيح $k^{rlcp} = h(k^{rlc} | "P" | p)$، لكل $r = n_R - 1, \ldots, 1, 0, l = n_L - 1, \ldots, 1, 0, c = 0, 1, \ldots, n_C - 1, p = 0, 1, \ldots, n_R - 1$، حيث "$P$" تعني شفرة الترميز ASCII للحرف P وp تعني دليل هذه المنطقة.

وينتج التدفق المشفر المحمى من خلال تجفير كل رزمة بالمفتاح المقابل لها (شِعَب من تفرع المفاتيح).

ومن أجل استلام صورة فرعية من التدفق المشفر المحمي يحصل المستعمل على مفاتيح النفاذ المناسبة (مضمونة من مخدم المفاتيح مثلاً). وهذه المفاتيح قادرة على أن تستعيد تماماً شِعَب تفرع المفاتيح المقابلة لرزم الصورة الفرعية المطلوبة. وتشبه عملية إعادة تكوين المفتاح عملية توليد تفرع المفاتيح. وتُستعمل الشعب في تجفير الرزم المقابلة.

5.2.B قواعد تركيب التدفق المشفر

يوضح الجدول 1.B بنية القطعة SEC، ويشير الحقل *ZOI* إلى المعلمات المضمونة، والحقل P_{ID} إلى معلمات طريقة الحماية لنظام مراقبة هذا النفاذ. ويتخذ الحقل PM_{ID} دائماً القيمة 1 للدلالة على استعمال النموذج الأساسي للتجفير. ويدل الحقل TP_{ID} على معلمات إضافية لنظام مراقبة النفاذ هذا. أما *KTO* فهو ترتيب توليد تفرع المفاتيح. ويدل الحقل L_{aki} على طول معلومة مفتاح النفاذ.

الجدول 1.B – مثال لمعلمات هذا النظام

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

المعلمة		الحجم (بالبتات)	القيم	الدلالة
t		8 (FBAS)	1	أداة حماية تقدمها سلسلة التسجيل
i		8 (RBAS)	قيمة الحالة	معرف هوية حالة الأداة
ID_{RA}	$ID_{RA,id}$	32	قيمة الأداة *ID*	معرف هوية مسجل
	$ID_{RA,nsl}$	8 (RBAS)	21	طول $ID_{RA,ns}$ بالأثمونات
	$ID_{RA,ns}$	168	مكان الأسهم	مكان اسم سلطة التسجيل بالتسجيل لهذه الأداة
L_{ZOI}		16 (RBAS)	[2 ... $2^{16} - 1$]	طول منطقة التأثير ZOI
ZOI		مغير	انظر 7.5	منطقة تأثير هذا النظام
L_{PID}		16 (RBAS)	[2 ... $2^{16} - 1$]	طول $P_{ID} + L_{PID}$
P_{ID}		متغير	انظر الجدول 2.B	معلمات هذا النظام

الجدول P_{ID} – 2.B

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

المعلمة	الحجم (بالبتات)	القيم	الدلالة
$ID_T = 1$	8	دائماً 1	وسم النموذج المرجعي للتجفير
T_{decry}	متغير	قيم النموذج المرجعي للتجفير	النموذج المرجعي للتجفير
TP_{ID}	متغير	انظر الجدول 3.B	معلومات إضافية عن هذا النظام

الجدول TP_{ID} – 3.B

KTO	L_{aki}	AK_{Info}

المعلمة	الحجم (بالبتات)	القيم	الدلالة
KTO	8	0 ... (2^8 – 1)	ترتيب تفرع المفاتيح. وقد يكون مختلفاً عن ترتيب تقدم التدفق المشفر، 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL القيم الأخرى: محجوزة
L_{aki}	16	0 ... (2^{16} – 1)	طول معلومة مفتاح النفاذ إذا كانت L_{aki} = 0، لا يتوفر الحقل AK_{Info}
AK_{Info}	متغير	انظر الجدول 4.B	معلومات عن مفتاح النفاذ (مثل طول المفتاح، عدد المفاتيح)

الجدول AK_{info} – 4.B

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

المعلمة	الحجم (بالبتات)	القيم	الدلالة
L_{uk}	16	0 ... (2^{16} – 1)	طول مفتاح المستعمل
UK	L_{uk}	NaN	معلومات مفتاح المستعمل
E_{ak}	16	See Table 24	المجفر المستخدم في تجفير مفاتيح النفاذ
N_{ak}	16	0 ... (2^{16} – 1)	عدد مفاتيح النفاذ
AK	N_{ak} * K_{bc}	NaN	مفاتيح النفاذ

6.2.B الخلاصة

تمكّن التكنولوجيا الناشر من حماية التدفق المشفر JPEG 2000 باستعمال مفتاح رئيسي. ويسمح بإرسال التدفق المشفر المحمي إلى أي عدد من المستعملين ولكن مفاتيح الرزم تبقى سرية. ويولد مخدم المفاتيح مفاتيح نفاذ مختلفة للمستعملين تبعاً لأولوياتهم. ويولد المستعملون مفاتيح رزم مأمونة من مفاتيح نفاذهم ويحصلون على صور مأمونة مختلفة. هذا يعني أن للتكنولوجيا خاصية تسمى "تجفير واحد ونفاذ متعدد الأشكال"

3.B إطار الاستيقان الموحد للصور JPEG 2000

1.3.B الوصف التشغيلي

تقدم هذه الأداة JPSEC خدمات النظام JPSEC التالية: التحقق من تكاملية بيانات/محتوى الصورة واستيقان المصدر أي الاستيقان الهش وشبه الهش للصور JPEG 2000 استناداً إلى خطط التوقيع الرقمي.

وبما أن هذه الأداة توفر طريقتي الاستيقان الهش وشبه الهش، فإنها تُستخدم في سيناريوهات تطبيق مختلفة بما فيها توزيع الصورة واستمرار الصورة والتصوير الطبي والعسكري وتنفيذ القوانين والتجارة الإلكترونية والإدارة الإلكترونية.

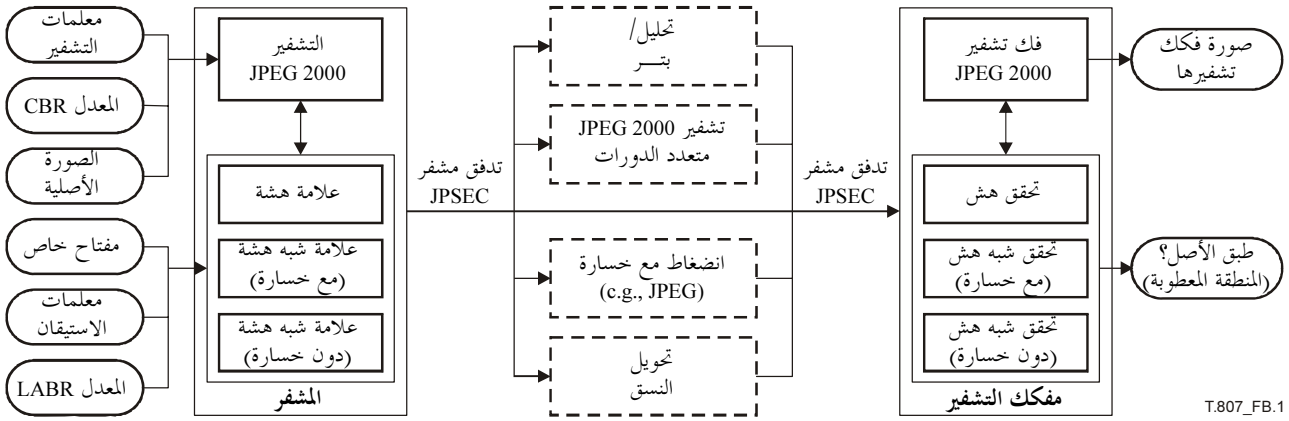
وقد تصادف الصور في بيئة الانتشار أنواعاً مختلفة من التشوهات العابرة مثل تحويل الشفرة وتحويل النَسق. وتحمي تقنيات الاستيقان القائمة على التجفير التقليدي الصور JPEG 2000 على صعيد تكامل البيانات ولا تستطيع أن تتصدى هذه الأنواع من تشوهات المحافظة على المحتوى. لكن تقنيات الاستيقان شبه الهش مطلوبة لحماية الصور JPEG 2000 على صعيد محتوى الصورة. وتوحد هذه الأداة استيقان بيانات الصورة ومحتواها وتقدم مفهوماً جديداً يسمى معدل بتات استيقان أقل (LABR). هذا وإن الصورة إذا ما تحولت شفرتها إلى معدل بتات لا يقل عن المعدل LABR فإنها ستنقل على أنها موثوقة وإلا فتكون غير موثوقة. وقد يكون الاستيقان استيقاناً هشاً أو شبه هش. والأداة قادرة في الاستيقان شبه الهش على تعرف المكانة الذي وقع فيه العطب عندما تبدو الصورة غير موثوقة.

2.3.B المخطط التقني العام

استخدمت هذه الأداة الإعلامية JPSEC مجموعة من التقنيات من أجل توفير الاستيقان الهش وشبه الهش. وتضم هذه التقنيات عناصر منتقاة وتوقيع رقمي وإخفاء بيانات مع خسارة ودون خسارة وشفرات تصحيح أخطاء. وتنتقي العناصر المقابلة وفق المعدل LABR الذي يحدده المستعملون استناداً إلى القليل المطبق على البنية JPEG 2000 وينتج بعدئذ التوقيع الرقمي. وتستخدم شفرة تصحيح الخطأ (ECC) فيما يتعلق بالاستيقان شبه الهش من أجل تعزيز مستوى المتانة. وتدمج بتات التحقق من التعادلية (PCB) في الصورة كعلامات مائية تتيح تحديد مواقع الصدمات. ويمكن دمج البيانات بطريقتين مختلفتين، طريقة مع خسارة وأخرى دون خسارة. وفي طريقة إخفاء البيانات مع خسارة لا يمكن استعادة الصورة الأصلية بعد إخفاء البيانات. أما في طريقة إخفاء البيانات دون خسارة فإن الصورة تتغير بطريقة قابلة للعكس، أي أن الصورة الأصلية يمكن استعادتها إذا لم تكن الصورة المعنية معطوبة. والاستيقان شبه الهش دون خسارة مفيد للمعيار JPEG 2000 إذ أنه يقدم الانضغاط مع خسارة ودون خسارة. وذلك بالغ الأهمية في التصوير الطبي وتطبيقات التصوير عن بعد، حيث يشكل عدم الخسارة متطلباً أساسياً.

وتستخدم معلمة المعدل LABR (معدل بتات أقل للاستيقان) المماثل لمعدل بتات انضغاط الصورة الذي يُستعمل لمراقبة شدة الانضغاط وخصائصه، في مراقبة كمية مقدرة الحماية. وعلى سبيل المثال، عندما تكون الصورة JPEG 2000 محمية بمعدل LABR قدره 2 bpp (بتة للبيكسل الواحد) فإن أي نسخة محوَّلة الشفرة من الصورة ستسلم وكأنها أصلية في النظام المقترح، طالما كان معدل البتات بعد تحويل الشفرة أكبر من 2 bpp أو مساوٍ له.

ويوضح الشكل 1.B كيفية استخدام هذه الأداة لحماية الصور.



الشكل 1.B – حماية الصورة باستعمال إطار استيقان موحد للمعيار JPEG 2000

يمكن لهذه الأداة أن تستخدم قواعد تشوير مختلفة تبعاً لطريقة الاستيقان المتبعة. فهي تستخدم لأغراض الاستيقان الهش قاعدة الأداة المعيارية JPSEC كما تعرف في الفقرة 3.8.5. وتستخدم لأغراض الاستيقان شبه الهش قاعدة الأداة غير المعيارية JPSEC كما تبين في الجدول 5.B. وإضافة إلى ذلك، تتخذ المعلمة F_{INSEC} القيمة 0 إذا لم تستعمل هذه الأداة الواسم INSEC وتعطي المعلمة F_{mod} القيمة 1 لأن التدفق المشفر الناتج عن الأداة JPSEC يمتثل أيضاً لمعيار الجزء 1 من JPEG 2000.

الجدول 5.B – قاعدة التركيب للاستيقان شبه الهش

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
t		8 (FBAS)	1	تستعمل قاعدة تركيب أداة غير معيارية
i		8 (RBAS)	0 ... $(2^7 - 1)$	دليل حالة الأداة
ID_{RA}	$ID_{RA,id}$	32	0 ... $(2^{32} - 1)$	رقم الهوية التي تخصصها هيئة التسجيل
	$ID_{RA,nsl}$	8 (RBAS)	21	طول الهوية $ID_{RA,ns}$ بالأثمونات
	$ID_{RA,ns}$	168	حيز الاسم	بتات اسم هيئة تسجيل الأداة
L_{ZOI}		16 (RBAS)	0 ... $(2^{16} - 1)$	طول منطقة التأثير
ZOI		متغير	قيم ZOI	المنطقة المغطاة في الصورة التي تحميها الأداة
L_{PID}		16 (RBAS)	0 ... $(2^{16} - 1)$	طول P_{ID} وL_{PID} بالأثمونات

الجدول 5.B – قاعدة التركيب للاستيقان شبه الهش

المعلمة			الحجم (بالبتات)	القيمة	الدلالة الناتجة
P_{ID}	ID_T		8	2	يستعمل النموذج المرجعي الاستيقان كما يحدده الجدول 21
	T_{auth}	M_{auth}	8	2	تستعمل طريقة التوقيع الرقمي كما يحددها الجدول 34
		P_{auth} M_{DS}	8	انظر الجدول 41	تستعمل خوارزمية التوقيع الرقمي مثل DSA وRSA
		H_{DS}	8	انظر الجدول 37	وظيفة التقطيع المستخدمة
		KT_{DS}	متغير	قيم نموذج المفتاح	يخزن المفتاح العمومي في KT_{DS}. وتستعمل هذه الطريقة مفتاح عمومي واحد فقط.
		SIZ_{DS}	16	$0 \ldots (2^{16} - 1)$	طول التوقيع الرقمي بالأثمونات
P_{ID}	PD		1	0_b	البنية FBAS مكتملة
			1	0_b	مجال البيكسل غير مستعمل
			1	0_b	مجال معامل الموجة الصغيرة غير مستعمل
			1	1_b	مجال معاملات الموجات الصغيرة المكماة مستعمل
			1	0_b	مجال التدفق المشفر غير مستعمل
			3	000_b	محجوز لاستعمالات المنظمة ISO
	G	PO	16	قيم أوامر المعالجة	أمر بالمعالجة
		GL	8	0000 1001	سوية التحبب: وحدة الحماية هي كامل المنطقة المحددة في منطقة التأثير
	V	N_V	16	1	عدد التواقيع الرقمية في القائمة هو 1
		S_V	8 (RBAS)	$1 \ldots (2^8 - 1)$	طول التوقيع الرقمي بالأثمونات
		VL	$8^* S_V$	قيمة التوقيع الرقمي	التواقيع الرقمية التي تولدها الأداة
	LABR	$LABR_{int}$	8	$0 \ldots (2^8 - 1)$	الجزء الصحيح من المعدل LABR
		$LABR_{fra}$	8	$0 \ldots (2^8 - 1)$	الجزء الكسري من المعدل LABR
	العتبة		8	$[1 \ldots 2^8 - 1]$	قيمة العتبة (للاستيقان دون خسارة فقط)
	الخلط		8	$[1 \ldots 2^8 - 1]$	عدد مرات الخلط التي يحتاجها دمج بتات العلامة. (للاستيقان دون خسارة فقط)

وينبغي أن تخصص هيئة التسجيل الهوية (ID) الفريدة لهذه الأداة. ويمكن الاطلاع على وصف الأداة من هيئة التسجيل (RA) باستخدام الهوية المخصصة.

3.3.B استنتاجات

يمكن تلخيص الخصائص المحققة في هذه الأداة بما يلي:

- استيقان الصور JPEG 2000 في بيانات الصورة أو محتوى الصورة بإدخال الاستيقان الهش وشبه الهش في إطار واحد. كما أن الاستيقان شبه الهش يتضمن الأسلوبين مع خسارة ودون خسارة.
- مقاومة تشوهات عابرة مختلفة قد يسببها تحويل الشفرة أو تحويل النسق والانضغاط مع خسارة والتشفير JPEG 2000 متعدد الدورات. غير أنه يمكن استعمال هذه الأداة من أجل حماية الصورة JPEG 2000 في بيئة ضارة.
- إمكانية قياس حماية الصورة JPEG 2000. وهذه الأداة على وجه التحديد قادرة على حماية أي رقعة أو مكونة أو استبانة أو طبقة أو منطقة أو مجموعة شفرات.
- المواءمة مع أحداث إطار أمني يسمى البنية التحتية للمفتاح العمومي الذي يشكل أساس المعايير الدولية الراهنة مثل المعيار X.509.
- شدة الحماية الكمية التي تتحكم بها معلمة واحدة تسمى المعدل LABR الذي يوفر الكثير من الراحة للمستعملين.

- مقدرة تحديد موقع مناطق الصورة التي جرت مهاجمتها احتمالاً أو بدت الصورة مختلفة عن الأصل. وقد يساعد ذلك على إقناع المشاهدين.
- توفير حماية مع خسارة ودون خسارة تقابل الانضغاط مع خسارة – دون خسارة لمعايير التشفير JPEG 2000. وهكذا فإن للأداة تطبيقات كثيرة بما فيها التصوير الطبي والتصوير عن بعد.

4.B طريقة التجفير على أساس الرزم لأغراض التدفقات المشفرة JPEG 2000

1.4.B الوصف التشغيلي

تعرض هذه الفقرة تقنية تجفير انتقائية لأغراض الصور JPEG 2000. وتقوم هذه التقنية على أساس تجفير سوية الرزم وعلى خوارزميات مشفر معياري قوي.

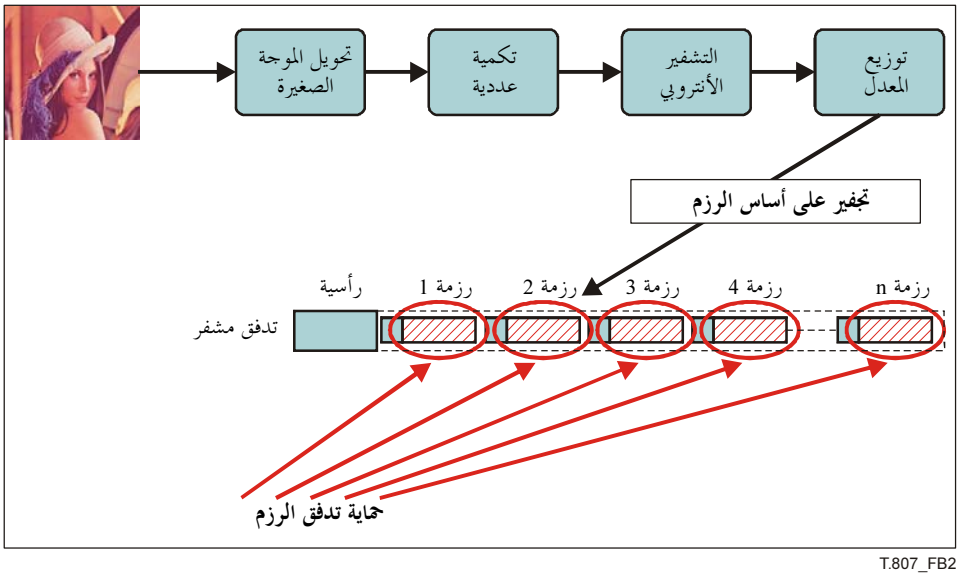
وخدمة الأمن التي تستعملها التقنية هي سرية الصور JPEG 2000 الناتجة عن تجفير التدفق المشفر. وبالتالي، يمكن تحقيق الحماية IPR وحماية الخصوصية باستخدام هذه التقنية.

ويدعم هذا النهج تحويل الشفرة وقابلية القياس ووظائف أخرى لمعالجة المحتوى دون أمكانية النفاذ إلى مفتاح التجفير أو فك التجفير أو إعادة التجفير. هو لا يدخل في عمليات التشفير وفك التشفير، وله تأثير سلبي محدود جداً على فعالية الانضغاط وليس له أي تأثير سلبي على مقاومة الأخطاء. ويتيح نهج من هذا القبيل مرونة قصوى في تنفيذ السيناريوهات والتطبيقات مع سويات أمن مختلفة.

ويمكن لمنتجي المحتويات استعمال التقنية بهدف الحد من النفاذ إلى محتوى الصور وكذلك للمزودين بالمحتويات من أجل ضمان سرية المحتوى الذي يستلمه المستعمل النهائي.

2.4.B المخطط العام التقني

تنطوي التقنية على تجفير التدفق المشفر بعد انضغاط الصورة كما يبين الشكل 2.B.



الشكل 2.B – مبدأ التجفير على أساس الرزم

يمكن للأداة JPSEC أن تتخذ عدة معلمات تتعلق بالصورة عند الدخل مثل: سويات الاستبانة أو طبقات النوعية أو المكونات أو المناطق أو الرقع. وعندئذٍ لا تعالج إلا الحمولة النافعة المقابلة لهذه المعلمات في الرزم. وهكذا يحافظ التدفق المشفر المحمي على بنية JPEG 2000 نظامية. وبعد تجفير التدفق تضاف قطعة الواسم SEC إلى الرأسية الرئيسية من أجل تمكين المستهلك JPSEC من فك تجفير الصورة بصورة صحيحة فيما بعد.

وتستخدم هذه الطريقة خوارزميات ذات صلة معروفة ومعيارية في تجفير الرزم انتقائياً: وهما الخوارزميتان DES أو AES المصاحبتان للأساليب المعيارية الواردة في المرجع [22] مثل ECB وCBC وCFB وOFB وCTR. ويمكن بالطبع استعمال أي خوارزميات تجفير أخرى؛ وترد هنا الطريقتان DES وAES كمثالين للمجفرات المعيارية.

1.2.4.B مثال لإرسال التقنية

يمكن الإشارة إلى هذه التقنية في قواعد التركيب القائمة على النموذج المعياري المبين في البند المعياري. ويرد أدناه مثال لتشوير هذه التقنية (الجدول 6.B) يحدد منطقة واحدة لمنطقة التأثير ، ويجوز بالطبع تحديد أكثر من منطقة واحدة، باتباع نفس القاعدة كما في المعلمة $Zone^0$.

الجدول 6.B – مثال منطقة التأثير مع إحداثيات مكانية واستبانات وطبقات

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NZzoi			8	1 (RBAS)	عدد المناطق واحد
$Zone^0$	DCzoi		1	0	قطعة الأثمونات المتراصفة لا تلي
			1	0	صنف الوصف المتصل بالصورة
			6	101100	مناطق الصورة ومستويات الاستبانة وطبقات النوعية والمكونات محددة بالترتيب
	$Pzoi^1$	$Mzoi^1$	1	0	قطعة الأثمونات المتراصفة لا تلي
			1	0	تتأثر المناطق المحددة بطريقة الحماية
			1	0	يتحدد بند واحد
			2	00	أسلوب المستطيل
			2	00	تستعمل المعالجة Izoi عدداً صحيحاً من 8 بتات
			1	1	توصف المعلمة Izoi ببعدين
		$Izoi^1$	8	0110 0100	100 = Xul
			8	0111 1000	120 = Yul
			8	1011 0100	180 = Xlr
			8	1101 0010	210 = Ylr
	$Pzoi^3$	$Mzoi^3$	1	0	قطعة الأثمونات المتراصفة لا تلي
			1	1	تتأثر المناطق المحددة بطريقة الحماية
			1	0	يتحدد بند واحد
			2	11	بأسلوب Max
			2	00	تستعمل المعالجة Izoi عدداً صحيحاً من 8 بتات
			1	0	توصف المعلمة Izoi ببعد واحد
		$Izoi^3$	8	0000 0010	سويات الاستبانة ≥ 2 محددة (أي سويات الاستبانة < 3 محددة بالأسلوب Max وتبديل إضافي)
	$Pzoi^4$	$Mzoi^4$	1	0	قطعة الأثمونات المتراصفة لا تلي
			1	0	تتأثر المناطق المحددة بطريقة الحماية
			1	0	يتحدد بند واحد
			2	11	بأسلوب Max
			2	00	تستعمل المعالجة Izoi عدداً صحيحاً من 8 بتات
			1	0	توصف المعلمة Izoi ببعد واحد
		$Izoi^4$	8	0000 0101	الطبقات ≥ 5 تتحدد بالأسلوب Max

الجدول 7.B – وصف النموذج المعياري لفك التجفير في حالة المعيار AES-192/CBC

المعلمة					الحجم (بالبتات)	القيمة	الدلالة الناتجة
P_{PM}				ME_{decry}	8	0000 0000	NULL: لا توجد طريقة وقاية من محاكاة الواسم
				CT_{decry}	16	0x0003	معرف هوية المجفر AES (فدرة المجفر)
	CP_{decry}	M_{bc}			6	10 0000	أسلوب المجفر: CBC
		P_{bc}			2	01	أسلوب الملء (ملء -PKCS#7)
		SIZ_{bs}			8	0001 0000	حجم الفدرة 16 أثمونًا (128 بتة)
		KT_{bc}	LK_{KT}		16	0x00C0	حجم المفتاح: 192 بتة
			KID_{KT}		8	0000 0011	معلومات المفتاح هي موقع URI
			LKI_{KT}		16	0x0021 (=33)	طول الموقع URI: 33 أثمونًا
			KI_{KT}		264	https://server/path/secretkey.pem	هذا المعرف URI هو موقع https URL؛ وينبغي تفسيره على أنه تطبيق يستخدم المعيار JPSEC. واستعادة المفتاح الفعلية تتجاوز هذا المعيار
			G_{KT}	PO	16	0 000 001 010 011 100	ترتيب المعالجة هو TRLCP
				GV	8	0000 1001	قيمة تحبب المفتاح هي كامل منطقة ZOI
			V_{KT}	Nv	16	0x0001	قيمة مفتاح واحد في KI_{KT}؛ قيم غير محددة في V_{KT}
				Sv	16	0010 0001	طول URI: 33 أثمونًا
				VL	264	https://server/path/secretkey.pem	هذا المعرف URI هو موقع https URL: وينبغي تفسيره على أنه تطبيق يستخدم المعيار JPSEC. واستعادة المفتاح الفعلية تتجاوز هذا المعيار.

الجدول 8.B – قواعد تركيب مجال المعالجة

المعلمة	الحجم (بالبتات)	القيمة	الدلالة الناتجة
PD	1	0_b	قطعة الأثمونات المتراصفة لا تلي
	1	0_b	لا توجد في مجال البيكسل
	1	0_b	لا يوجد في مجال معامل الموجات الصغيرة
	1	0_b	لا يوجد في مجال معامل الموجات المكماة
	1	1_b	عولج في مجال التدفق المشفر
	3	000_b	غير مستعمل

الجدول 9.B – التحبب وقواعد وضع قائمة القيم

المعلمة		الحجم (بالبتات)	القيمة	الدلالة الناتجة
G	PO	16	0 000 001 010 011 100	ترتيب المعالجة هو TRLCP
	GV	8	0000 0110	وحدة الحماية هي الرزمة
V	N_V	16	1	عدد القيم IV المحددة
	Sv	8	16	حجم القيمة IV بالأثمونات
	VL	128	القيمة	القيمة IV

3.4.B الخلاصة

تبين التقنية التي سبق عرضها في الفقرة أعلاه التجفير الانتقائي للصور JPEG 2000. وتقوم على أساس تجفير سوية الرزم وعلى خوارزميات تجفير متينة ومعيارية. ويمكن إرسالها باستخدام النماذج المعيارية المعرفة في الفقرة 8.5 وهي تقدم سويات تعقيد مختلفة.

5.B أداة التجفير لمراقبة النفاذ إلى المعيار JPEG 2000

1.5.B خدمات الأمن

توفر هذه التقنية أداة تجفير قادة على الوقاية من محاكاة الواسم في تدفق مشفر.

2.5.B تطبيقات نموذجية

تتيح هذه التقنية تجفيراً انتقائياً وكاملاً للتدفقات JPEG 2000. ويمكن استعمال طرائق التجفير الانتقائية هذه لعرض صورة تمت الموافقة عليها مثل صورة مصغرة أو منخفضة الجودة أو مشوشة جزئياً.

3.5.B المستعملون المحتملون ونماذج التنفيذ والبواعث

تستند هذه التنقية أساساً على التجفير على أساس الرزم للتدفق JPEG 2000 باستعمال خوارزمية تجفير معروفة. وتقي هذه التقنية خاصةً من محاكاة الواسم في التدفق المجفر. غير أنه حتى إذا وصل تدفق المجفر الناتج إلى مفكك تشفير متوائم مع الجزء 1 للمعيار JPEG 2000 فإنه يستبعد أن يتعطل مفكك التشفير ويبقى قادراً على عرض الصورة المحمية بشكل صحيح.

4.5.B المخطط العام التقني

(1) التجفير

الخطوة 1 تجفير مؤقت لشفرة من أثمونين باستعمال خوارزمية تجفير معروفة.

الخطوة 2 إذا كانت الشفرة المجفرة مؤقتاً أو الشفرة المرتبطة بها تزيد عن 0xFF8F، تكون شفرة الأثمونين غير مجفرة.

وإلا فالشفرة المجفرة مؤقتاً تخرج كشفرة مجفرة.

الخطوة 3 الانتقال إلى شفرة الأثمونين التالية ومتابعة الخطوتين 1 و2.

وينبغي أن يكون أثمونا الشفرة الموجودان في النص الواضح أقل من 0xFF90 وفقاً لمواصفة الجزء 1. وفضلاً عن ذلك، إذا كانت الشفرة المجفرة مؤقتاً أو الشفرة المرتبطة بها تزيد عن 0xFF8F تكون شفرة الأثمونين غير مجفرة. وبالتالي يكون أثمونا الشفرة موجودان في النص المجفر أقل 0xFF90.

وإذا كان طول النص الواضح عدداً مفرداً، فإن المعالجة تتطلب استثناءً، إذ إن الأثمون الأخير لا يجفَّر ولا يضاف عن طريق الحشو بوجود أثمون إضافي.

(2) فك التجفير

الخطوة 1 فك تجفير مؤقت لشفرة من أثمونين باستعمال خوارزمية المجفر كما في التجفير.

الخطوة 2 إذا تجاوزت الشفرة المفككة التشفير مؤقتاً أو الشفرة المرتبطة بها الطول 0xFF8F، كانت شفرة الأثمونين غير مفككة التشفير. وإلاَّ فتستخرج الشفرة المفككة التشفير مؤقتاً وكأنها شفرة مفككة التشفير.

الخطوة 3 الانتقال إلى شفرة الأثمونين التالية، والعودة إلى الخطوة 1 والخطوة 2.

تحدث جميع شفرات الأثمونين في النص الواضح الأصلي قبل التجفير أقل من 0xFF90. وهكذا فمن الممكن أخذ قرار بعدم تجفير شفرة الأثمونين إذا كانت الشفرة مفككة التشفير المؤقتة أو الشفرة المرتبطة بها تزيد عن 0xFF8F.

5.5.B طريقة التشوير

يبين الجدول 10.B مثالاً للمعلمات في هذه التقنية. ويتم تشوير معلمات هذه التقنية وفقاً للقواعد المحددة في المعيار JPSEC. وينبغي خصوصاً أن تستعمل هذه التقنية نموذج "فك التجفير" المعيار وتحبب "الرزمة" ومجال معالجة "تدفق البتات" مع منطقة التأثير الملائمة.

الجدول 10.B – مثال معلمات هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة	الدلالة
SEC		16	0xFF65	الواسم SEC
L_{SEC}		16	متغير	طول قطعة الواسم SEC
Z_{SEC}		8	1 (مثال)	دليل قطعة الواسم SEC
P_{SEC}		1	0	الأثمون FBAS لا يلي
	F_{INSEC}	1	1 (مثال)	تستعمل INSEC
	$F_{multiSEC}$	1	0_b	تستعمل قطعة واسم SEC واحدة
	F_{mod}	1	1_b	تم تعديل البيانات JPEG 2000 الأصلية
	F_{TRLCP}	1	0_b	استعمال الواسم TRLCP غير محدد
	Padding	3	000_b	غير مستعمل
	N_{tools}	8 (RBAS)	1	رقم أداة الأمن واحد
	I_{max}	8 (RBAS)	0	دليل الحالة القصوى للأداة صفر
t		8 (FBAS)	1	أداة حماية JPSEC غير معيارية مسجلة في هيئة التسجيل
i		8 (RBAS)	0000000_b	دليل حالة الأداة
ID_{RA}	$ID_{RA,id}$	32	0	معرف الهوية المسجل
	$ID_{RA,nsl}$	8 (RBAS)	21	طول $ID_{RA,ns}$ بالأثمونات
	$ID_{RA,ns}$	168	*حيز الاسم*	مكان اسم هيئة تسجيل هذه الأداة
L_{zoi}		16	9	طول منطقة التأثير 9 أثمونات
ZOI		متغير	انظر الجدول 11.B (مثال)	منطقة تأثير هذه الأداة
L_{PID}		16	متغير	طول L + T + PD + G
P_{ID}		متغير	انظر الجدول 12.B (مثال)	معلمات هذه التقنية

الجدول 11.B – مثال لمنطقة تأثير أداة توليد المفتاح

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NDzoi			8	1	عدد المناطق واحد
$Zone^0$	Dczoi		1	0_b	قطعة الأثمونات المتراصفة لا يلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	101000_b	مناطق الصورة وسويات الاستبانة محددة بالترتيب
	$Pzoi^1$	$Mzoi^1$	1	0_b	قطعة الأثمونات المتراصفة لا يلي
			1	0_b	المناطق المحددة متأثرة بطريقة الحماية
			1	0_b	يتحدد بند واحد
			2	00_b	أسلوب المستطيل
			2	00_b	تستخدم المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	1_b	المعلمة Izoi موصوفة في بعدين
		$Izoi^1$	8	0110 0100_b	100 = Xul
			8	0111 1000_b	120 = Yul
			8	1011 0100_b	180 = Xlr
			8	1101 0010_b	210 = Ylr
	$Pzoi^3$	$Mzoi^3$	1	0_b	قطعة الأثمون المتراصف لا يلي
			1	1_b	المناطق المحددة غير متأثرة بطريقة الحماية
			1	0_b	يتحدد بند واحد
			2	11_b	الأسلوب Max
			2	00_b	تستخدم المعلمة Izoi عدداً صحيحاً من 8 بتات
			1	0_b	المعلمة Izoi موصوفة ببعد واحد
		$Izoi^3$	8	0000 0010_b	سويات الاستبانة > 3 محددة

الجدول 12.B – المعلمة P_{ID} في هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة	الدلالة
T		متغير	انظر الجدول 13.B	النماذج المعيارية لفك التجفير
PD		8	0000 1000_b	الأثمون FBAS لا يلي. وهو معالج في حالة الدفق المستمر
G	PO	16	0 000 001 010 011 100 0_b	ترتيب المعالجة هو: رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	0000 0110_b	وحدة الحماية هي الرزمة
Skip		8	0	معلمة *Skip* لهذه الأداة

الجدول 13.B – مثال لنموذج المعياري لفك تجفير هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
ME_{decry}		8	1	لم تحصل محاكاة الواسم
CT_{decry}		16	1	مجفر الفدرة (AES)
CP_{decry}	M_{bc}	6	$10\ 0010_b$	يستعمل الأسلوب OFB (البتات غير محشوة)
	SIZ_{bc}	16	128	حجم الفدرة (128 بتة)
	KT_{bc}	متغير	*قيم النموذج المعياري للمفتاح*	النموذج المعياري للمفتاح
	IVsc	128	*قيمة المتجه الأولية*	قيمة المتجه الأولية

6.5.B الخلاصة

قدمت هذه الفقرة وصفاً لتقنية تجفير تدفقات مشفرة JPEG 2000. ومن أهم فوائد هذه التقنية هي أنها تقي من حدوث محاكاة الواسم في التدفق المجفر.

6.B أداة توليد مفاتيح التحكم في النفاذ إلى البيانات JPEG 2000

1.6.B خدمات الأمن المستهدفة

تقدم هذه التقنية خدمة التحكم في النفاذ إلى الصورة JPEG 2000 وفقاً لبنية التراتب في المعيار JPEG.2000.

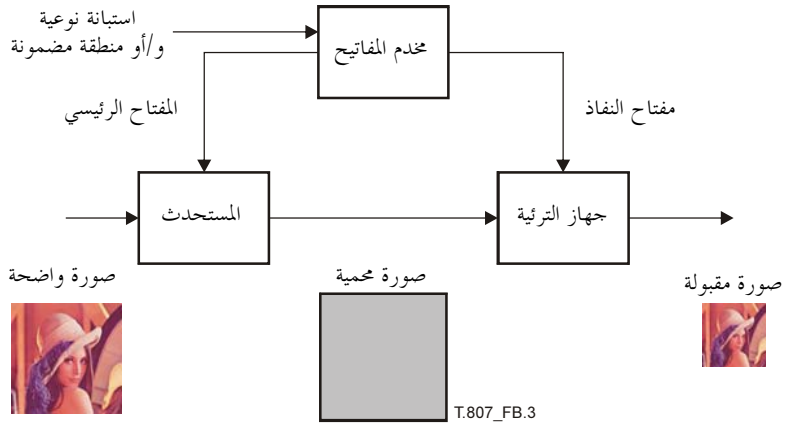
2.6.B تطبيقات نموذجية

أحد التطبيقات النموذجية لهذه التقنية هو التوزيع الأمين للصورة حيث لا يمكن لغير المستعمل المرخص له أن ينفذ إلى الصورة المعنية. فقد يكون مثلاً نموذج مصغَّر للصورة مسموحاً، لكن يبقى عرض الصورة باستبانة كبيرة غير ممكن إلاَّ للمستعمل المزود بالمفاتيح.

3.6.B المستعملون المحتملون ونموذج التنفيذ والبواعث

تقوم هذه التقنية بتوليد مفاتيح لاستخدامها في التوزيع الأمين لصور JPEG 2000. وتستند إلى آلية التحكم في النفاذ إلى الصورة مثل منطقة الصورة والاستبانة ونوعية الصورة. وتقوم هذه التقنية على مبدأ تأمين مفاتيح التجفير وفك التجفير تراتبياً باستخدام وظيفة التقطيع التجفيري باتجاه واحد مثل وظيفة التقطيع.

4.6.B المخطط العام التقني



الشكل 3.B – المخطط العام لهذه التقنية

يولد مخدم المفاتيح في هذه المرحلة المفتاح الرئيسي. ثم يحفر المستحدث صورةً باستعمال مفاتيح الرزم التي تتولد من المفتاح الرئيسي. ويولد مخدم مفاتيح في مرحلة فك التجفير مفتاح نفاذ وفق الاستبانة و/أو نوعية و/أو منطقة مضمونة. ثم يفك جهاز الترئية الصورة المجفرة باستعمال مفاتيح الرزم التي أنتجها مفتاح النفاذ. ويلاحظ أن هذه المفاتيح تتولد تتابعياً استناداً إلى سلسلة تقطيع أمينة.

وتستعمل هذه التقنية خصوصاً سياسة التحكم في النفاذ التالية: "إذا كان يحق لمستعمل ما النفاذ إلى سوية/طبقة استبانة ما فإنه يحق له أيضاً النفاذ إلى السويات/الطبقات الأدنى لهذه الاستبانة". ومن ناحية أخرى، لا يجوز لمستعمل يمكنه النفاذ إلى رقعة ما أن ينفذ إلى الرقع الأخرى بتاتاً.

والميزة الكبرى لهذه التقنية هي أن عدد المفاتيح المطلوبة للانتقال من مخدم مفاتيح إلى جهاز الترئية أقل بكثير مما تتطلبه الطريقة التقليدية. وذلك يعني أن هذه التقنية تتيح خفض الصبيب الضرورة لمقدرة الذاكرة.

5.6.B طريقة التشوير

يبين الجدول 14.B المعلمات التي توصي بها هذه التقنية. ويجب استخدام أي من هذه المعلمات وفقاً للقواعد المحددة في المعيار JPSEC. وينبغي خصوصاً لهذه التقنية أن تستخدم النموذج المعياري "لفك التجفير" وتحبب "الرزمة" ومجال معالجة "تدفق البتات" مع منطقة التأثير الملائمة.

الجدول 14.B – المعلمات الموصى بها في هذه التقنية

المعلمة		الحجم (بالبتات)	القيم	الدلالة
SEC		16	0xFF65	واسم الأمن SEC
L_{SEC}		16	0 ... 255	طول قطعة الواسم SEC
Z_{SEC}		8	0	دليل قطعة الواسم SEC هذه
P_{SEC}		1	0	الأثمون FBAS لا يلي
	F_{INSEC}	1	1	يُستعمل واسم INSEC
	$F_{multiSEC}$	1	0_b	تُستعمل قطعة واحدة للواسم SEC
	F_{mod}	1	1_b	تم تغيير البيانات JPEG 2000 الأصلية
	F_{TRLCP}	1	0_b	استعمال الواسم TRLCP غير محدد
	Padding	3	000_b	غير مستعمل
	N_{tools}	8 (RBAS)	1	رقم أداة الأمن واحد
	I_{max}	8 (RBAS)	0	أقصى دليل حالة أداة هو صفر
t		8 (RBAS)	1	أداة JPSEC غير معيارية
i		8 (RBAS)	0	دليل حالة لهذه الأداة
ID_{RA}	$ID_{RA,id}$	32	5	معرف الهوية المسجل لهذه الأداة
	$ID_{RA,nsl}$	8 (RBAS)	21	طول المعرف $ID_{RA,ns}$ مقدراً بالأثمونات
	$ID_{RA,ns}$	168	*حيز الاسم*	منطقة اسم الهيئة RA التي سجلت لديها الأداة
L_{zoi}		16	متغير	طول المنطقة ZOI في هذه الأداة
ZOI		متغير	*قيمة* ZOI	منطقة التأثير في هذه الأداة
L_{PID}		16	متغير	طول L + T + PD + G
P_{ID}		متغير	انظر الجدول 16.B	معلمات هذه التقنية

الجدول 15.B – مثال لمنطقة تأثير هذه الأداة لتوليد المفاتيح

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NDzoi			8	1	عدد المناطق هو واحد
$Zone^0$	Dczoi		1	0_b	قطعة الأثمون المتراصف لا تلي
			1	0_b	صنف الوصف المتعلق بالصورة
			6	101000_b	تتحدد مناطق الصورة وسويات الاستبانة حسب الترتيب
	$Pzoi^1$	$Mzoi^1$	1	0_b	قطعة الأثمون المتراصف لا تلي
			1	0_b	تتأثر المناطق المحددة بطريقة الحماية
			1	0_b	يتحدد بند واحد فقط
			2	00_b	أسلوب المستطيل
			2	00_b	تستعمل المعلمة Izoi عدد صحيح من 8 بتات
			1	1_b	يرد وصف المعلمة Izoi في بعدين
		$Izoi^1$	8	$0110\ 0100_b$	100 = Xul
			8	$0111\ 1000_b$	120 = Yul
			8	$1011\ 0100_b$	180 = Xlr
			8	$1101\ 0010_b$	210 = Ylr
	$Pzoi^3$	$Mzoi^3$	1	0_b	قطعة الأثمون المتراصف لا تلي
			1	1_b	لا تتأثر المناطق المحددة بطريقة الحماية
			1	0_b	يتحدد بند واحد فقط
			2	11_b	أسلوب Max
			2	00_b	تستعمل المعلمة Izoi عدد صحيح من 8 بتات
			1	0_b	يرد وصف المعلمة Izoi في بعد واحد
		$Izoi^3$	8	$0000\ 0010_b$	تتحدد سويات استبانة < 3

الجدول 16.B – المعرف P_{ID} في هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة	الدلالة
T		متغير	انظر الجدول 17.B	النماذج المعيارية لفك التشفير
PD		8	$0000\ 1000_b$	الأثمون FBAS لا يتبع. ويعالج في مجال التدفق المشفر.
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	ترتيب المعالجة هو: رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	$0000\ 0110_b$	وحدة الحماية هي الرزمة
H		16	انظر الجدول 37 في 1.3.8.5	دالة التقطيع لهذه الأداة
L_k		8	255…0	طول معلومات مفتاح النفاذ
AK_{info}		متغير	*قيمة مفتاح النفاذ*	معلومات مفتاح النفاذ (تشفر هذه المعلومات باستعمال المعلمة KT_{bc} في النموذج المعياري)

الجدول 17.B – مثال للنموذج المعياري لفك تشفير هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
ME_{decry}		8	1	لم تحدث محاكاة الواسم
CT_{decry}		16	3	فدرة تجفير (AES)
CP_{decry}	M_{bc}	6	10 0010	يستعمل أسلوب OFB. (بتات غير مملوءة)
	SIZ_{bc}	16	128	حجم الفدرة (128 بتة)
	KT_{bc}	متغير	انظر 5.8.5	نموذج معياري للمفتاح
	IVsc	128	*قيمة المتجه الأولي*	قيمة المتجه الأولي

6.6.B الخاتمة

تصف هذه الفقرة تقنية التحكم في النفاذ إلى الصورة في التدفق المشفر JPEG 2000 وأهم مميزات هذه التقنية هي أن عدد المفاتيح التي يتعين إدارتها والوصول إليها أقل بكثير من عدد المفاتيح في الحالة التقليدية.

7.B خلط مجال الموجات الصغيرة وتدفق البتات لأغراض التحكم في النفاذ الشرطي

1.7.B ملخص

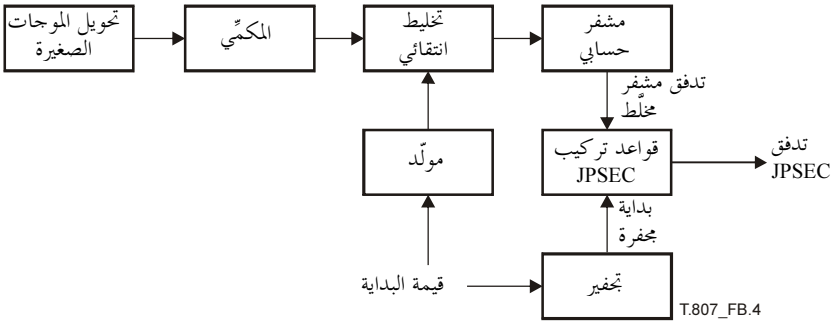
التحكم في النفاذ إلى صورة ما هو وظيفة هامة في ضمان أمن الصور. وغالباً ما يُستحسن إعطاء النفاذ إلى جزء صغير من الاستبانة أو إلى نوعية منخفضة للصورة، وإبقاء النفاذ إلى استبانات أعلى أو نوعيات أفضل رهناً بالحصول على ترخيص. وتقدم هذه الفقرة تقنية التحكم الشرطي في النفاذ. وقد سبق عرض الطريقة في المرجع [23]. وهي تضيف بشكل أساسي ضوضاء شبه عشوائية إلى الصورة. ويعرف المستعملون أصحاب الرخص هذا التتابع شبه العشوائي وبالتالي يمكنهم إزالة هذه الضوضاء. ومن جهة أخرى لا يستطيع المستعملون غير المرخص لهم النفاذ إلا إلى صور شديدة التشوه. ويتألف النظام من ثلاث مكونات رئيسية هي: التخليط ومولد الأرقام شبه العشوائية وخوارزمية التشفير. ومن أجل الاستفادة من خصائص النظام JPEG 2000 والحفاظ عليها دون مساس، تطبق عملية التخليط انتقائياً على فدر الشفرة المكونة للتدفق المشفر. ونتيجة لذلك يمكن ضبط سوية التشوه في أجزاء محددة من الصورة. ويمكّن ذلك من التحكم في الاستبانة أو النوعية أو المناطق الهامة في الصورة.

2.7.B المخطط التقني العام

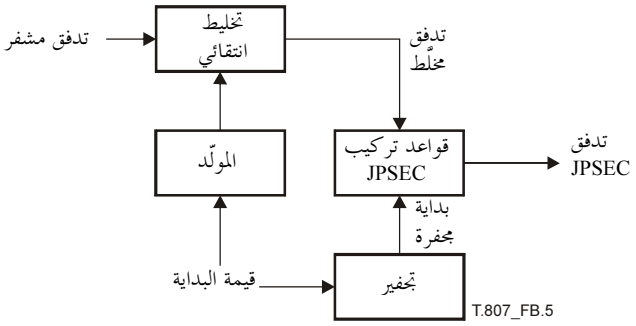
يتكون هذا النظام من ثلاثة عناصر رئيسية هي:

- التخليط: وهناك طريقتان في التخليط. فإما أن يتم تخليط لمعاملات الموجات الصغيرة المكمَّاة، وإما للبتات مباشرةً في التدفق المشفر. وتتحول علامات المعاملات في الحالة الأولى في كل فدرة شفرة بشكل شبه عشوائي. أما في الحالة الثانية فتتحول بتات التدفق بشكل شبه عشوائي.
- مولّد الأرقام شبه العشوائية (PRNG): يُستخدم المولِّد PRNG في توجيه عملية التخطيط. ويستند إلى قيمة بداية. ففي أحد التطبيقات المفضلة لهذه التقنية تُستخدم الخوارزمية SHA1PRNG [24] مع قيمة بداية من 64 بتة في مولد الأرقام شبه العشوائية (PRNG). وجدير بالذكر أنه بالإمكان استخدام خوارزميات PRNG أخرى أيضاً.
- خوارزمية التجفير: من أجل توصيل قيم البداية إلى المستعملين المرخص لهم، يتم تشفيرها وإدراجها في التدفق المشفر. وفي أحد التطبيقات المفضلة لهذه التقنية تُستخدم الخوارزمية RSA في التجفير [25]. كما يجوز استخدام خوارزميات تجفير أخرى. ويمكن انتقاء طول المفتاح في الوقت الذي تكون فيه الصورة محمية.

ويقابل الشكلان 4.B و5.B حالتي التخليط في مجالي الموجات الصغيرة ومجال تدفق البتات.



الشكل 4.B – مخطط إجمالي لتخليط مجال الموجات الصغيرة



الشكل 5.B – مخطط إجمالي لتخليط مجال تدفق البتات

وحرصاً على تعزيز أمن النظام، يمكن تغيير قيمة البداية في كل فدرة شفرة. ويمكن أيضاً تحديد عدة سويات نفاذ باستعمال مفاتيح تجفير مختلفة. وقواعد التركيب الواردة أدناه كبيرة المرونة وتوفر عدة قيم بداية وعدة مفاتيح.

3.7.B قواعد تركيب التدفق المشفر

يستخدم هذا المثال قطعتي الوسم SEC وINSEC. وتتحدد قواعد تركيب التدفق المشفَّر فيما بعد. وتستخدم قطعة الواسم SEC قواعد التركيب للأدوات غير المعيارية. أما قطعة الواسم INSEC فتُستعمل للإشارة إلى الفدرة المخلطة وقيم البدايات المستعملة.

1.3.7.B قواعد تركيب قطعة الواسم SEC

تستخدم قاعدة تركيب الأدوات غير المعيارية وتُستعمل في حالة المفاتيح المتعددة حالات أدوات متعددة في قطعة الواسم SEC. وبعبارة أدق توجد عدة حالات i = 0، 1، 2، ... مع نفس المعرف ID، تقابل كل منها معرف مفتاح مختلف $KeyID^{(i)}$، كما هو مبين في الشكل 6.B.

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

الشكل 6.B – قاعدة تركيب أداة حماية غير معيارية في حالة المفاتيح المتعددة

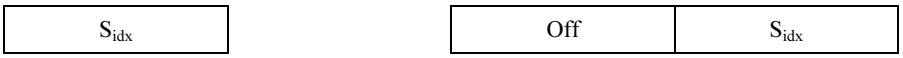
وفيما يلي دلالات المعلمات P_{ID}:

الجدول 18.B – قاعدة تركيب معرفات المعلمات P_{ID} ودلالتها

المعلمة	الطول (بالبتات)	الدلالة
N_s	16	عدد قيم البداية المستخدمة في هذه الحالة
KeyID	32	معرف هوية المفتاح الذي يتعين استخدامه في التجفير
بيانات	متغير	قيم البداية المجفرة

2.3.7.B قواعد تركيب قطعة الواسم INSEC

يُستخدم واسم الأمن داخل التدفق الداخل (INSEC) من أجل إدراج المعلومات التي تدل على قيمة البداية المستخدمة في حماية فدرة مشفرة معينة. ويدرج الوارم INSEC في هذا المثال قبل فدرة الشفرة المحمية للدلالة على قيمة البداية التي استُخدمت في حماية هذه الفدرة/الفدر. وبدلاً من الدلالة على قيمة البداية ذاتها، يحتوي الواسم على دليل يحيل إلى قيم البداية في قطعة الواسم SEC للرأسية الرئيسية. وتنطبق معلومات الواسم INSEC كما يظهر في المثال على فدر الشفرة التالية، علماً بأن R تساوي دائماً 1. وقاعدة تركيب المعلمة AP مختلفة في حالة تخليط الموجات الصغيرة وفي حالة تخليط تدفق البتات:



الشكل 7.B – قاعدة تركيب المعلمة AP: تخليط مجال الموجات الصغيرة (إلى اليسار)، وتخليط مجال تدفق البتات (إلى اليمين)

أما الدلالات فهي التالية:

الجدول 19.B – قاعدة تركيب المعلمة AP ودلالاتها

المعلمة	الطول (بالبتات)	الدلالة
Off	16	التخالف في تدفق بتات فدرة الشفرة لأول أثمون مخلَّط
Sidx	16	دليل قيم البداية في فدرة الشفرة.

ولا يدل جمع حالة الأداة i ودليل البداية S_{idx} في حالة المفاتيح المتعددة، إلاَّ على البداية/المفتاح الذي تحيل إليه قطعة الواسم INSEC هذه.

4.7.B استنتاجات

عرضت هذه الفقرة أداة أمن خاصة بالتحكم الشرطي في النفاذ إلى الصور JPEG 2000. وتدخل التقنية ضوضاء شبه عشوائية إلى الأجزاء المنتقاة من التدفق. وبالتالي تظهر الصورة مفككة التشفير شديدة التشوه في مفكك تشفير غير مرخص له لا يعرف كيفية إزالة هذه الضوضاء.

ويرتبط أمن التقنية بأمن الخوارزميات المحددة لمولد الأرقام شبه العشوائية ولتجفير قيم البداية في التطبيق المفضل للخوارزمية SHA1PRNG والخوارزمية RSA على التوالي. والخوارزمية SHA1PRNG مولد PRNG أمين، إذ لا يمكن استنتاج أي تتابع بمجرد معرفة بعض أرقامه. ويبلغ طول بداية المولد PRNG في هذا المثال 64 تبة، مما يجعل احتمال الهجوم الشامل متعذراً. ويتم تجفير قيم البدايات استناداً إلى الخوارزمية RSA باستعمال طول مفتاح محدد للمستعمل. وتعتبر الخوارزمية RSA خوارزمية أمنية شريطة استعمال طول كاف للمفتاح.

8.B النفاذ التدريجي للتدفق JPEG 2000

1.8.B خدمات الأمن المنشودة

تقدم هذه الطريقة طريقة التحكم في النفاذ غير المرتبط بالصورة في تدفق JPEG 2000 وفقاً لترتيب تدريجي في التدفق المشفَّر.

2.8.B

يتمثل التطبيق النموذجي لهذه التقنية في توزيع أمين للصورة حيث المستعمل المرخص له وحده قادر على استعمال الصورة المقبولة. وتناسب هذه التقنية خصوصاً التحكم في النفاذ وفقاً لترتيب تدريجي في التدفق المشفر.

3.8.B المستعملون المحتملون ونماذج التنفيذ والبواعث

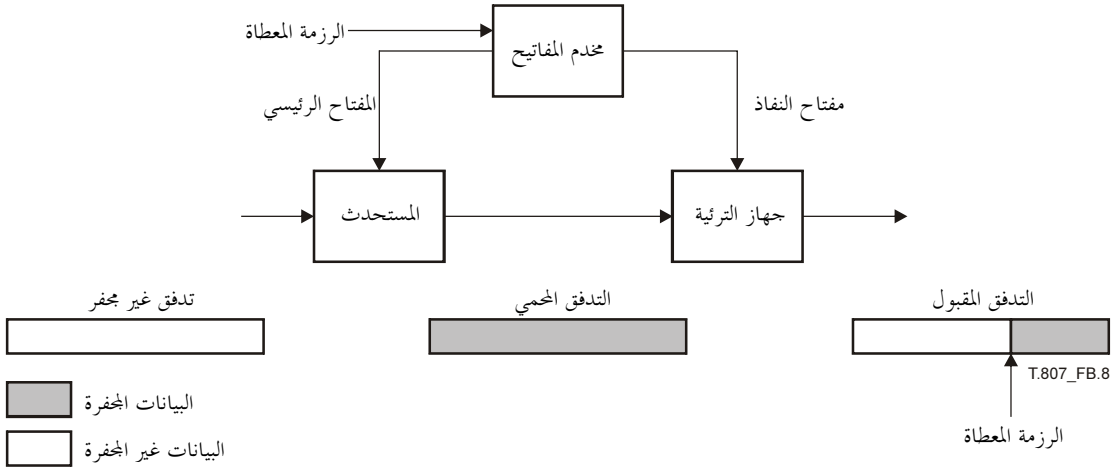
يكمن التحدي الأكبر في تصميم نظام التحكم في النفاذ في إيجاد توازن حساس بين الأمن والفعالية والمرونة. وتقيم هذه التقنية للتحكم في النفاذ إلى التدفق JPEG 2000 سلسلة تقطيع لتوليد مفاتيح لكل رزمة ولتجفير الرزم في التدفق. ولكن لا يجوز إلاّ للمستعملين ذوي الترخيص الأمني الصحيح بفك تجفير الرزم المقابلة للصورة المعطاة في التدفق.

4.8.B المخطط التقني العام

يولّد مخدم المفاتيح في مرحلة التجفير مفتاحاً رئيسياً. ثم يشفر المستحث تدفقاً مشفراً مستخدماً مفاتيح الرزم التي تتولد من المفتاح الرئيسي. ويولّد المخدم المفاتيح في مرحلة فك التجفير مفتاح نفاذ وفقاً للرزمة المعطاة. ثم يفكك جهاز الترئية التدفق المشفر باستعمال مفاتيح الرزم التي تنتج عن مفتاح النفاذ.

وتستخدم هذه التقنية خصوصاً سياسة التحكم في النفاذ التالية: "إذا استطاع مستعمل ما النفاذ إلى رزمة ما فإنه يستطيع أيضاً النفاذ إلى الرزم السابقة من التدفق". ويسمى هذا النوع من التحكم في النفاذ "النفاذ التدريجي".

وتكمن الفائدة الكبرى لهذه التقنية في أن عدد المفاتيح اللازمة للانتقال من مخدم مفاتيح إلى جهاز الترئية أقل بكثير مما هو عليه في التقنيات التقليدية. مما يعني أن هذه التقنية تتيح تقليص العيب الضروري لأغراض التخزين.



الشكل 8.B – المخطط التقني العام للتقنية

5.8.B طريقة التشوير

يقدم الجدول 20.B المعلمات التي توصي بها هذه التقنية. ويجب الإشارة إلى كل معلمة من هذه المعلمات وفقاً لقاعدة التركيب المحددة في النظام JPSEC. وينبغي تحديداً أن تستخدم هذه التقنية النموذج المعياري "لفك التجفير" وتحبب "الرزمة" ومجال معالجة "تدفق البتات" مع منطقة التأثير المناسبة.

الجدول 20.B – مثال معلمات هذه الأداة

المعلمة		الحجم (بالبتات)	القيم	الدلالة
SEC		16	0xFF65	الواسم SEC
L_{SEC}		16	متغير من 0 ... 255	طول قطعة الواسم SEC
Z_{SEC}		8	0	دليل قطعة الواسم SEC هذه
P_{SEC}		1	0	أثمون FBAS لا يلي
	F_{INSEC}	1	1_b	الواسم INSEC مستعمل
	$F_{multiSEC}$	1	0_b	تُستعمل قطعة واسم SEC واحدة
	F_{mod}	1	1_b	قيم تغيير بيانات JPEG 2000 الأصلية
	F_{TRLCP}	1	0_b	استخدام الواسم TRLCP غير محدد
	Padding	3	000_b	غير مستعمل
	N_{tools}	8 (RBAS)	1	عدد أدوات الأمن واحد
	I_{max}	8 (RBAS)	0	دليل حالة الأداة الأقصى هو صفر
t		8 (RBAS)	1	أداة حماية RA
i		8 (RBAS)	0	دليل الحالة
ID_{RA}	$ID_{RA,id}$	32	7	معرف الهوية المسجل
	$ID_{RA,nsl}$	8 (RBAS)	21	طول $ID_{RA,ns}$ بالأثمونات
	$ID_{RA,ns}$	168	namespace	مكان اسم السلطة RA التي سجلت لديها هذه الأداة
L_{zoi}		16 (RBAS)	متغير	طول المنطقة ZOI
ZOI		متغير	انظر الجدول 21.B (مثال)	منطقة تأثير هذه الأداة
L_{PID}		16 (RBAS)	متغير	طول G + PD + T + L
P_{ID}		متغير	انظر الجدول 22.B (مثال)	معلمات هذه الأداة

الجدول 21.B – مثال منطقة تأثير هذه التقنية

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
NDzoi			8	1	عدد المناطق واحد
$Zone^0$	DCzoi		1	0	قطعة الأثمون المتراصف لا تلي
			1	1	صنف الوصف غير المتصل بالصورة
			6	000100	الرزم محددة
	$Pzoi^4$	$Mzoi^4$	0	1	قطعة الأثمون المتراصف لا تلي
			1	1	لا تتأثر المناطق المحددة بطريقة الحماية
			1	1	تتحدد بنود متعددة
			11	2	الأسلوب MAX
			00	2	تستعمل المعلمة Izoi عدد صحيح من 8 بتات
			00	2	يرد وصف المعلمة Izoi في بعد واحد
		$Izoi^{11}$	8	0000 1010	دليل الرزمة > 10 معرفة

الجدول B.22 – معرِّفات المعلمات في هذه التقنية

المعلمة		الحجم (بالبتات)	القيم	الدلالة
T		متغير	انظر الجدول B.23	النماذج المعيارية لفك التحفير
PD		8	$0000\ 1000_b$	لا يوجد أثمون BAS لاحق. مجال التدفق المشفر
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	ترتيب المعالجة هو رقعة – استبانة – طبقة – مكونة – منطقة
	GL	8	$0000\ 0110_b$	وحدة الحماية هي الرزمة
H		16	انظر الجدول 37 في 1.3.8.5	وظيفة التقطيع لهذه الأداة لتوليد المفاتيح
L_k		8	0 ... 255	طول معلومات مفتاح النفاذ
AK_{info}		متغير	*قيمة مفتاح النفاذ*	معلومات مفتاح النفاذ (تشفر هذه المعلومات باستخدام النموذج KT_{bc} في T)

الجدول B.23 – مثال للنموذج المعياري لفك تجفير هذه التقنية

المعلمة		الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
ME_{decry}		8	1	لم تحدث محاكاة الواسم
CT_{decry}		16	3	تجفير الفدرة (AES)
CP_{decry}	M_{bc}	6	10 0010	يستعمل الأسلوب OFB. (البتات غير مملوءة)
	SIZ_{bc}	16	128	طول الفدرة (128 بتة)
	KT_{bc}	متغير	*قيمة النموذج المعياري للمفتاح*	نموذج معياري للمفتاح
	IVsc	128	*قيمة المتجه الأولي*	قيمة المتجه الأولي

B.6.8 الخلاصة

قدمت هذه الفقرة وصفاً لتقنية التحكم في النفاذ إلى التدفق المشفَّر JPEG 2000. وتكمن الفائدة الكبرى لهذه التقنية في أن عدد المفاتيح المستخدمة والتي يجب الحصول عليها أقل بكثير مما هو عليه في الحالات التقليدية. وتوفر هذه التقنية تحكماً مرناً وفعالاً في النفاذ إلى البيانات JPEG 2000 وفقاً لتدرُّج الترتيب في التدفق المشفَّر.

B.9 الاستيقان المرن في التدفقات المشفرة JPEG 2000

B.9.1 خدمة الأمن

تقدم هذه الفقرة آلية مرنة لاستيقان التدفقات JPEG-2000. وهي تتيح للمستعملين أن يتحققوا من صحة وتكامل الصور الفرعية المختلفة من خلال علامة رقمية واحدة.

B.9.2 تطبيق نموذجي

ثمة مجالات تطبيقات حرجة مثل المجالات الحكومية والمالية والطبية والحقوقية التي يتطلب فيها الزبائن عادة الاستيقان من المحتويات التي تصلهم. ولهذا السبب، فإن آلية أمن مرنة لاستيقان الوثائق مطلوبة لدى بث المحتويات.

B.9.3 البواعث

يولد منتج صورة في تطبيقات النشر التي يقوم بها طرف ثالث تدفقاً مشفراً مع توقيعه. ثم يرسل المنتج التدفق المشفر والتوقيع إلى طرف ثالث ناشر. ويمكن أن يطلب المستعملون من الناشر تدفقاً مشفراً محوَّل الشفرة بسبب الموارد المحدودة (مثل عرض النطاق، قدرة الحوسبة). وسيرسل الناشر إلى المستعمل بيانات الصورة الفرعية وبرهان استيقانها.

B.9.4 المخطط العام التقني

تقدم التقنية آلية مرنة لاستيقان التدفقات المشفَّرة JPEG-2000. وتضم ثلاث وحدات هي: التوقيع وتحويل الشفرة والتحقق. وهذه التقنية الأساسية هي تفرعات "ميركل" التي تنظم الرزم JPEG-2000.

1.4.9.B وحدة التوقيع

تولّد وحدة التوقيع توقيعاً على تدفق مشفَّر JPEG-2000 داخل وفقاً لخطة التوقيع الرقمي المفضلة. وينتج التدفق المشفر المحمي عند إدراج واسم SEC في التدفق المشفر الأصلي. ويتعين على المنتج خاصة:

- قراءة التدفق المشفر JPEG-2000.
- إقامة تفرعات تقطيع بحيث تنتج القيمة *الأصل*. وقيمة كل عقدة للتفرع هي قيمة تقطيع الرزمة. وقيمة كل عقدة داخلية هي تقطيع العقد الفرعية. وتشبه بنية التفرع الترتيب التدريجي للتدفق المشفر.
- توقيع قيمة الأصل لتفرع التقطيع باستعمال مفتاح خاص يستند إلى خوارزمية التوقيع.
- استحداث المعلمات SEC، وإدراجها في قطعة الواسم SEC بغية إنتاج تدفق مشفر صحيح.

2.4.9.B وحدة تحويل الشفرة

تنتج وحدة تحويل الشفرة إذنات تكاملية إضافية (SIT) وتدفق محوَّل الشفرة استناداً إلى الاستبانة والطبقة والمكونة والمنطقة المطلوبة. وتضم المعلمة SEC للتدفق المشفر الجديد الإذنات SIT وبعض المعلمات الأخرى. ويتعين خصوصاً على الناشر و/أو المخدم الوسيط:

- قراءة الرزم المستبعدة والتي لا يتضمنها التدفق محوَّل الشفرة.
- إقامة التفرعات الإضافية للتقطيع مع الرزم المستبعدة.
- إدراج قيم أصل التفرعات الإضافية في قطعة الواسم SEC.

ويضم التدفق المشفر محوَّل الشفرة قطعة الواسم SEC المحيَّنة والتدفق المشفر دون الرزم المستبعدة.

3.4.9.B وحدة التحقق

تقوم هذه الوحدة بالتحقق من صحة التدفق المشفر المحمي. ويحصل المحقق وفقاً لخطة التوقيع الرقمي المفضلة على المفتاح العمومي، ثم:

- يقرأ التدفق المشفَّر الواصل.
- يقيم تفرّعات التقطيع مع الرزم المستقبلة ورأسيات التدفق المشفر من الأسفل إلى الأعلى. وفي حال وجود بعض الرزم المستبعَدة، يستعيض عن التفرعات الإضافية بالإذنات SIT المقابلة لها. وهكذا يتم الحصول على قيمة *الأصل*.
- يتحقق من قيمة *الأصل* بمقارنتها مع التوقيع الوارد في القطعة SEC استناداً إلى نظام التوقيع الخاص. وفي حال توافقهما، يقبل التدفق المشفر؛ وإلاَّ فتُرفض الرزم الواصلة.

5.9.B قواعد تركيب التدفق المشفر

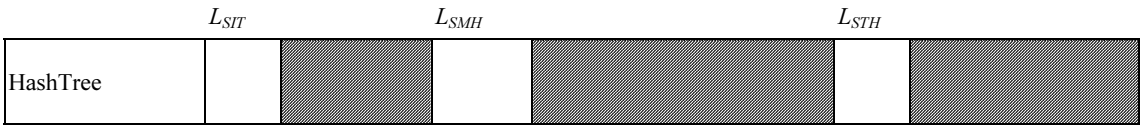
تظهر بنية القطعة SEG في الجدول 24.B. وتضم الواسم SEC ومعرف هوية الأداة والمنطقة ZOI والنموذج المعياري للاستيقان ومعلمات الأمن الخاصة بالتحقق. وتحتوي معلمات الأمن على بيانات تتيح إعادة تكوين رأسيات التدفق المشفر.

الجدول 24.B – قواعد تركيب أداة غير معيارية

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

المعلمة		الحجم (بالبتات)	القيم	الدلالة
t		8 (RBAS)	1	أداة حماية سلطة التسجيل
i		8 (RBAS)	*قيمة الحالة*	معرِّف هوية حالة الأداة
ID_{RA}	$ID_{RA,id}$	32	*قيمة معرِّف الهوية*	معرِّف هوية مسجَّل
	$ID_{RA,nsl}$	8 (RBAS)	21	طول المعرِّفات $ID_{RA,ns}$ بالأثمونات
	$ID_{RA,ns}$	168	*حيز الاسم*	مكان اسم سلطة التسجيل التي سجلت هذه الأداة لديها
L_{ZOI}		16	$[0 \ldots 2^{16} - 1]$	طول المعلمات الخاصة بمنطقة التأثير
ZOI_{ID}		متغير	قيم ZOI	معلمات المنطقة
L_{ID}		16	$[19 \ldots 2^{16} - 1]$	طول المعلمات
ID_T		8	2	معرف هوية صنف النموذج المعياري للاستيقان
T		متغير	*قيمة النموذج المعياري للاستيقان*	النموذج المعياري للاستيقان/التحكم MAC
TP_{ID}		متغير	انظر الجدول 25.B	معلمات الأمن

الجدول B.25 – معلمات الأمن



المعلمة	الحجم (بالبتات)	القيم	الدلالة
HashTree	8	0 ... (2^8 – 1)	ترتيب تفرع التقطيع. وقد يختلف عن ترتيب تدرج التدفق المشفّر وهو مؤقتاً: 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL القيم الأخرى: محجوزة
L_{SIT}	16	0 ... (2^{16} – 1)	عدد الإذنات SIT
SIT	متغير: L_{hash}*L_{SIT}	NaN	إذنة تكاملية إضافية
L_{SMH}	16	0 ... (2^{16} – 1)	طول الرأسية SMH
SMH	متغير		معلمات الاستعادة الرأسية الأساسية
L_{STH}	16	0 ... (2^{16} – 1)	طول الرأسية STH
STH	متغير		معلمات الاستعادة رأسية الرقعة

[a] ينبغي أن يرسل المفتاح (التحقق) لأغراض استيقان التحكم MAC المشفر على حدة.

[b] قيمة غير رقمية.

[c] L_{hash} هو طول قيمة التقطيع، مثال 160 لـــ SHA-1.

6.9.B الخلاصة

تتيح هذه التقنية آلية مرنة لاستيقان التدفق المشفر JPEG-2000. ولها خاصية "توقيع واحد وتحقق بطرق عديدة". وعملياً بعد توقيع التدفق JPEG-2000 الأصلي مرة واحدة يمكن التحقق من عدة تدفقات مشفرة محوَّلة من التدفق الأصلي وذلك من خلال الثقة بالمنتج وحده. وتتوافق هذه الخاصية تماماً مع وظيفة "انضغاط واحد وفك انضغاط بطرق عديدة". وذلك يتناقض مع الطريقة التقليدية لاستيقان الصورة التي تتطلب توقيعاً لاستيقان كل صورة.

10.B سرِّية البيانات JPEG-2000 ونظام التحكم في النفاذ القائم على فلق البيانات وحجبها

يقوم النظام الوارد وصفه في هذه الفقرة على الفلق من خلال عملية تسمى *"فلق البيانات وحجبها"* (*Data_Splitting and Luring*)، في ملف JPEG-2000 أصلي، تقسمه إلى ملفين يسميان *"الملف JP2 المحجوب"* الذي ينقل محتوى محميا و*"ملف التحكم"* الذي ينقل المعلومات الضرورية للنفاذ إلى المحتوى المحمل. ولا يمكن إعادة تكوين الملف JPEG-2000 الأصلي إلا من خلال جمع هذين الملفين في الوقت الفعلي في عملية *"إنشاء مباشر"*. ويتم الإنشاء المباشر باستعمال قواعد التحكم في النفاذ وإدارة الحقوق. ويقدم هذا النظام سوية عالية من المتانة والمرونة في التحكم في سرِّية البيانات JPEG-2000 والنفاذ إليها وعلى أساس الاقتصاد في الوقت وفي العمليات.

1.10.B الوصف التشغيلي

1.1.10.B خدمات الأمن المستهدفة

- السرّية: ينتقل الملف JP2 المحجوب محتوى محمياً. وبمجرد تشفير ملف JP2 محجوب واحد يصبح المحتوى المستعاد مشوشاً للرؤية وبالتالي يمنع الوصول إلى المحتوى الأصلي. ولا يمكن الوصول إلى هذا المحتوى الأصلي إلا عن طريق استعادة البيانات المخزنة في ملف التحكم من خلال عملية إنشاء مباشر وبالوقت الفعلي.

- التحكم في النفاذ: يمكن استخدام هذا النظام في التحكم في النفاذ إلى محتوى الصورة: فمثلاً، يتقاسم عدة مستعملين نفس الملف JP2 المحجوب، ولكن حقوق النفاذ التي يتمتعون بها مختلفة، ولذلك لا يستطيعون النفاذ إلى نفس الأجزاء من المحتوى.

ملاحظة عن حماية الحقوق IPR: يمكن ضمان تحكم وتتبع فعّالين لبث واستعمال محتوى محمي من خلال ربط النفاذ إلى المحتوى بالاستيقان وإدارة الحقوق وفقاً لإدارة مالك المحتوى وامتيازاته وربما من خلال إضافة العلامات المائية أو دمغ البصمات إلى هذا النظام.

2.1.10.B تطبيقات نموذجية

إحدى الصفات الرئيسية للنظام الموصوف هو تقسيم الملف الأولي JPEG 2000 إلى ملفين اثنين، ينقل الأول (الملف JP2 المحجوب) 99% من البيانات الأصلية و1% من البيانات الوهمية المسماة "بيانات الاستدراج" وتوزَّع وتذاع وتُنسخ ويتم تبادلها مجاناً عبر الشبكات أو الوسائط التقليدية، وينقل الثاني (ملف التحكم) مقدار 1% من البيانات الأصلية وبعض المعلومات التي يُشترط تواجدها معاً من أجل النفاذ إلى المحتوى المحمي الذي ينقله الملف الأول JP2 المحجوب.

أما الصفة الرئيسية الأخرى فهي ربط النفاذ إلى المحتوى المحمي الذي ينقله الملف JP2 المحجوب بمرحلتي تعرّف الهوية وإدارة الحقوق التي ستطلق نتائجهما تسيير المعلومات اللازمة المستخدمة من أجل استعادة محتوى غير مشوَّش (واضح) في الوقت الفعلي فقط.

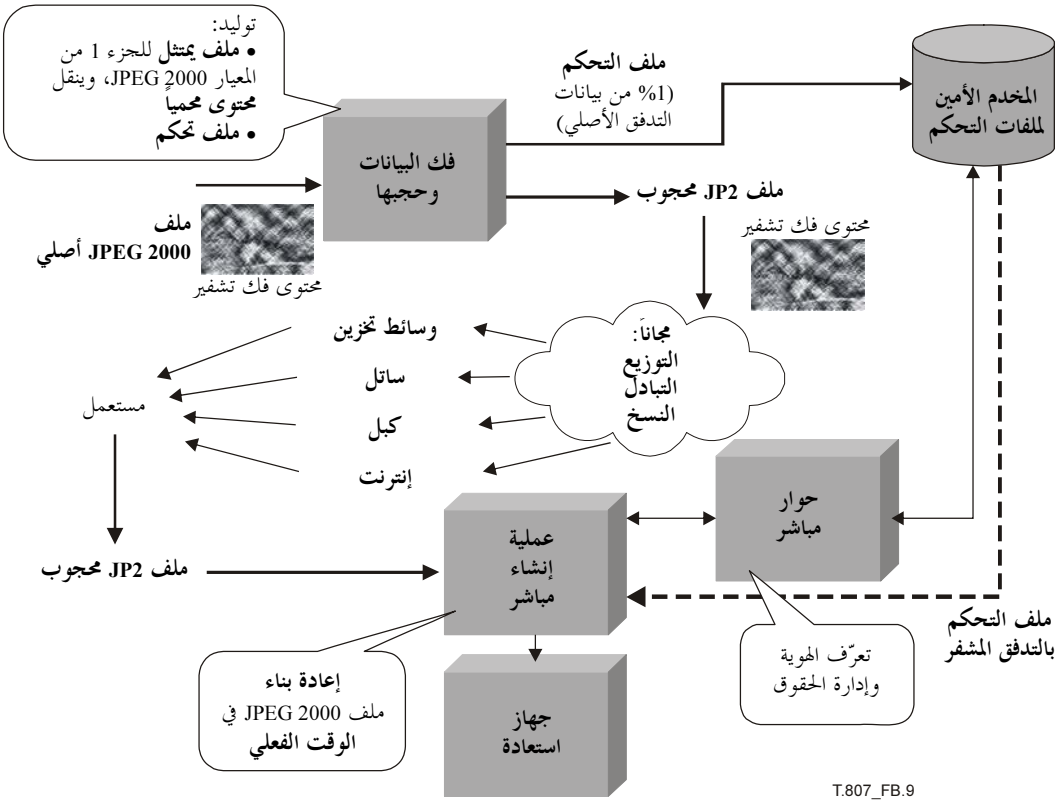
وأخيراً، يتم تفعيل متابعة الاستعمال وإصدار التقارير عنه من خلال الإحصاءات التي تُجمع من ملفات تسجيل الأمينة لمخدم ملفات التحكم.

3.1.10.B المستعملون المحتملون ونموذج التنفيذ والبواعث

المستعملون المتوقعون للنظام الموصوف هم مستحدثو المحتويات ومالكوها والمزودون بها، نظراً لأن النظام يضمن عدم السماح بالنفاذ إلى المحتوى الأصلي بعد تأمين حمايته ونقله في ملف JP2 محجوب إلاّ للمستعملين المرخص لهم ذلك وبعد استيقانهم. ولا بد من التشديد على أن 99% من المحتوى الأصلي متاح مجاناً بينما يتم توزيع النسبة 1% فقط اللازمة للنفاذ إلى المحتوى الأصل، بعد المرور ببروتوكولي الاستيقان وإدارة الحقوق.

2.10.B المخطط العام التقني

يبين الشكل 9.B المخطط العام للنظام.



الشكل 9.B – المخطط العام للنظام

ينقل ملف JPEG-200 داخل إلى ملفين في عملية تسمى *فلق البيانات وحجبها*. ثم ينتج ملفان جديدان هما: "*ملف JP2 محجوب*" ينقل محتوى محمياً (محتوى JPSEC)، و"*ملف تحكم*".

ويحدث خلال كل عملية فلق البيانات وحجبها أن تُستبعد بعض الأجزاء من الملف JPEG 2000 الأصلي وتحل محلها البيانات "الوهمية". وينقل الملف JP2 المحجوب حوالي 99% من المحتوى الأصلي بينما تشكل نسبة 1% المتبقية بيانات وهمية تسمى "بيانات الاستدراج" أي بيانات دون أي رابط معروف مسبقاً مع البيانات الأصلية. وعلى عكس التشفير التقليدي فإن عملية الحجب لا تستند إلى التشفير. ويجوز لأي مستعمل أن يوزع الملف JP2 المحجوب وينسخه ويتبادله مجاناً. ويحتوي ملف التحكم على 1% من البيانات الأصلية المستبعدة من الملف الأصلي. ويتم تخزينه في *مخدم أمين للملفات التحكم*.

وعندما يتم فك تشفير ملف JP2 محجوب في مفكك تشفير يمتثل للجزء 1 من المعيار JPEG-2000، يظهر المحتوى مشوشاً للرؤية. والسبيل الوحيد للنفاذ إلى المحتوى الأصلي هو استعادة البيانات الأصلية المستبعدة بفضل ملف التحكم. ويتصل جهاز *"الإنشاء المباشر"* بالمخدم الأمين للملفات التحكم باستعمال بروتوكول *"الحوار المباشر"*، ثم يتم تعرف الهوية وإدارة الحقوق على النحو التالي:

- إذا كان المستعمل يمتلك الحقوق اللازمة أو يوافق على شروط النفاذ إلى المحتوى (مثل دفع مبلغ من المال أو الاشتراك)، فإن البيانات المستبعدة تستعاد من ملف التحكم ويعاد تكوين الملف JPEG 2000 الأصلي في الوقت الفعلي. غير أن إعادة تكوين الملف JPEG-2000 الأصلي قد تكون إما جزئية (أي لا تسمح بالنفاذ إلاّ إلى طبقات خاصة من الرقعة و/أو المكونة اللونية و/أو الاستبانة و/أو المنطقة و/أو النوعية)، وإما كاملة؛
- وإذا كان المستعمل لا يمتلك الحقوق أو لا يقبل بالشروط المطلوبة، فإنه لا يستقبل إلاّ المحتوى المشوَّش.

والعناصر الرئيسية للنظام الموصوف هي:

- *فلق الملف JPEG 2000 الأصلي* إلى ملفين اثنين، ينقل الأول منهما المحتوى JPEG 2000 المحمي الذي يشكِّل 99% فقط من البيانات الأصلية، و1% من البيانات الوهمية المسماة بيانات الاستدراج (من الملف JP2 المحجوب)، ويحتوي الملف الثاني على بيانات المعلومات الأصلية (1%) اللازمة من أجل إعادة تكوين المحتوى JPEG 2000؛
- *تشويش رؤية* المحتوى؛
- الامتثال للجزء 1 من المعيار JPEG 2000 والمحافظة على حجم الملف؛
- نظام حماية *بمعدل بتات منخفض وتكاليف حاسوبية منخفضة*.

ويمكن استخدام هذا النظام في أي بيئة و/أو مع أي نظام تشغيل. ولا يحتاج إلى أي شروط خاصة للمعدات أو البرمجيات.

وتُدرج عملية الحجب الواسم SEC التالي في الملف JP2 المحجوب:

الجدول B.26 – قيم معلمات هذه الأداة

المعلمة						الطول (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
SEC						16	0xFF65	الواسم SEC
L_{SEC}						16	0xXXXX	طول قطعة الواسم SEC
Z_{SEC}						8	1 ... 255	دليل قطعة الواسم SEC
P_{SEC} (if Z_{SEC} = 1)	F_{INSEC}					1	0	الواسم INSEC غير مستعمل
	$F_{multiSEC}$					1	0	تُستعمل قطعة واسم SEC واحدة
	F_{J2K}					2	1	تدفق JPSEC يمتثل للجزء 1 من المعيار JPEG 2000
	F_{TRLCP}					1	0	استعمال واسم TRLCP غير محدد في هذا المجال
	N_{tools}					7	1	تُستخدم أداة أمن واحدة في التدفق المشفر
	I_{max}					7	1	أقصى دليل حالة للأداة
	عملية ملء					5	0	عملية ملء
أداة[0]	t					8 (RBAS)	1	أداة حماية غير معيارية
	i					8 (RBAS)	0	دليل حالة أداة
	ID_{RA}	$ID_{RA,id}$				32	ID	تستعمل السلطة RA لتسليم رقم تعرف الهوية
		$ID_{RA,nsl}$				8 (RBAS)	21	طول $ID_{RA,ns}$ 21 أثمونًا
		$ID_{RA,ns}$				168	*حيز الاسم*	حيز اسم السلطة RA التي سجلت هذه الأداة لديها
	L_{ZOI}					16	*قيمة الطول*	طول المعلمة L_{ZOI} + ZOI
	ZOI	NZ_{ZOI}				8	0...254	عدد المناطق
		$Zone^0$	DC_{ZOI}			1	0	قطعة الأثمون المتراصفة لا تلي
						1	1	صنف وصف غير متصل بالصورة
						6	000010	أدلة الرزم محددة
			$Pzoi^{0,0}$	Mzoi		1	0	قطعة الأثمون المتراصفة لا تلي
						1	0	المناطق المحددة متأثرة بطريقة الحماية
						1	1	تتحدد عدة بنود
						2	10	أسلوب الدليل
						2	xx	تستعمل المعلمة Izoi عدد صحيح من 8 أو 16 أو 32 بتة
						1	0	توصف المعلمة Izoi في بُعد واحد
				Nzoi		8	متغير	2 ... 255 (عدد أدلة الرزم)
				$lzoi^i$		xxx Nzoi	متغير	دليل الرزمة
	L_{PID}					16	0 ... $(2^{16} – 1)$	طول L_{PID} + P_{ID} بالأثمونات
	P_{ID}					متغير	متغير	معرف هوية ملف التحكم وموقع URL لمخدم ملف التحكم وغيرها؛ قواعد التركيب الكاملة توفرها السلطة RA

يمكن الحصول على الأوراق اللازمة لإجراء عمليات فلق البيانات وحجبها و/أو الإنشاء المباشر من خلال التوصيل مع سلطة التسجيل أو نقل العمليات من هذه السلطة.

11.B تسيير تدرجي أمين وتحويل شفرة أمين

1.11.B الملخص والبواعث

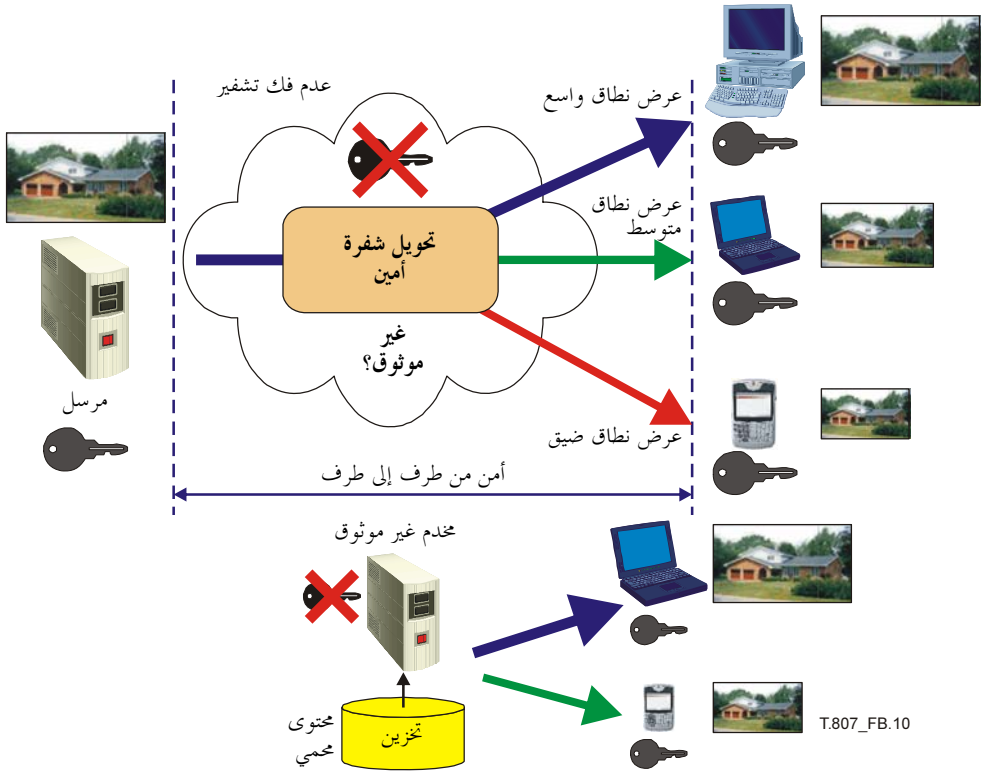
تصنِّف هذه الفقرة طريقة توفير خدمات حماية السرية والاستيقان للتدفقات JPEG 2000 بحيث:

1) تتيح لكيان ما (غير أمين احتمالاً) أن يحوِّل شفرة تدفقات JPSEC محمية أو يكيفها بطريقة أمينة دون أن يُطلب منه إزالة حماية المحتوى أو فك تشفيره؛ و

2) تتيح للزبون أن يؤكد أنَّ عملية تحويل الشفرة تمت بطريقة صالحة ومسموحة.

وغالباً ما يُشترط تحويل الشفرة في تكييف محتوى مشفر JPEG 2000 لخدمة زبائن يمتلكون أجهزة بمقدرات متنوعة (مثل أحجام عرض صغيرة أو توصيل شبكة بمعدل بتات منخفض) وظروف شبكة متغيرة زمنياً. خاصة وأن النظام JPEG 2000 يتلاءم جيداً مع تطبيقات تحويل الشفرة بسبب خواصه الملازمة القابلة للقياس. غير أن خاصية قابلية القياس قد تضيع إن لم تُتَّخذ كامل الحيطة في حماية التدفقات JPEG 2000. وعلى سبيل المثال، يقع ذلك عندما يشفر كامل التدفق المشفر في ملف واحد. وفي هذه الحالة ثمة طريقة واحدة لتحول شفرة التدفق المحمي وهي فك تشفيره أولاً ثم تحويل شفرته أو تكييف التدفق مفكك التشفير. وبما أن محوِّل الشفرة ملزم بفك شفرة المحتوى، فإن هذه العملية تقطع حبل الأمن من طرف إلى طرف في النظام.

وقد صُمم النظام JPSEC بهدف تعزيز تحويل شفرة أمين لمحتوى JPSEC المحمي حيث يتحدد تحويل الشفرة بأنه تحويل شفرة *دون إزالة حماية (فك تشفير) المحتوى*. ويتحقق ذلك في إطار تسيير تدرجي أمين يجمع التشفير المرن والتجفير والتشوير على نحو يتيح تحويل شفرة أمين وقليل التعقيد في مخدم (غير موثوق) أو مخدم أو عقدة مخدم وسيط في وسط الشبكة. ويمكّن ذلك النظام JPSEC من الحصول على خصائص قد تبدو متناقضة لتحويل شفرة في وسط الشبكة وتحقيق الأمن من طرف إلى طرف. ويظهر في الشكل 10.B مثال وسيط يشفَّر عند المرسِل ولا يفك تشفيره إلى عند المستقبل، ويبقى مشفراً طوال مساره في جميع النقاط: (إلى اليسار) تحوِّل عقدة وسط الشبكة شفرة المحتوى المحمي بأمن لكل زبون JPSEC، و(إلى اليمين) يحوِّل مخدم غير موثوق شفرة المحتوى JPSEC ويسيِّره بأمن دون أن يزيل عنه الحماية



الشكل 10.B – يتيح النظام JPSEC الأمن من طرف إلى طرف وتحويل الشفرة الأمين وسط الشبكة

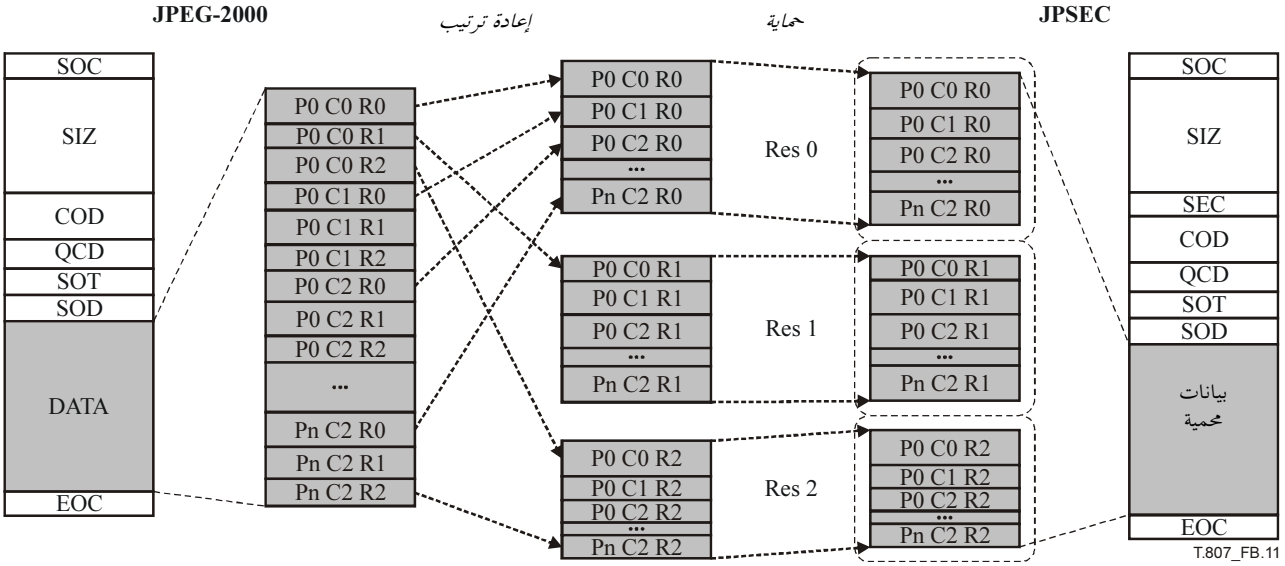
2.11.B الوصف التشغيلي ومثالان للاستعمال

في المثال الأول، ينتظم التدفق المستمر JPEG 2000 حسب الترتيب RLCP. والهدف هو حماية هذا التدفق وتشفيره واستيقانه مع تعزيز تحويل شفرة أمين في التدفق المحمي بدلالة الاستبانة. وبما أن التدفق المشفَّر JPEG 2000 الأصلي يستعمل الترتيب RLCP، فإن كل مكونة استبانة تتمثل في قطعة بيانات متجاورة. ويمكن إجراء التشفير في كل من القطع الثلاث للبيانات المتجاورة ثم تحدد الرأسية JPSEC ثلاث مناطق تأثير

تصف مكونة الاستبانة وقطعة التدفق المشفر والنموذج المعياري للتشفير المستخدم في كل قطعة. ويتم الاستيقان أيضاً في كل قطعة من القطع الثلاث للبيانات إما قبل التشفير أو بعده تبعاً للوظائف المطلوبة. ويتحدد ذلك أيضاً في الرأسية SEC باستعمال النموذج المعياري للاستيقان.

وحرصاً على إجراء تحويل شفرة أمين للتدفق JPSEC، يقرأ محول التشفير ببساطة الرأسية SEC ويحللها ويحدد مواقع قطع الاستبانة ثم يحتفظ بقطع البيانات/الاستبانات الملائمة أو يحذفها. وجدير بالذكر أن عملية تحويل الشفرة تعادل عملية تحليل بسيطة لا تستدعي إزالة حماية البيانات. ويتم الاستيقان من خلال استيقان البيانات محوَّلة الشفرة المستقبلة مع شفرة الاستيقان MAC التي توضع في الرأسية SEC خلال عملية حماية البيانات JPSEC.

وفي المثال الثاني، يتحدد الهدف المنشود مرة أخرى في حماية التدفق المشفر مع السماح بتحويل الشفرة من خلال الاستبانة؛ لكن هذا المثال أعقد بقليل من الترتيب RLCP أي أن قطع البيانات المقابلة لمكونات الاستبانة الثلاث ليست متجاورة في التدفق الأصلي. ويتيح النظام JPSEC تحقيق الهدف المنشود في تحويل شفرة أمين أو التدرج بالاستبانة في طرق عدة. إحداها تشفير رزم فردية مع ترك رأسيات الرزم دون تشفير. مما يبقي على أعلى مستوى من التدرج في التدفق لكنه يتطلب أعقد عملية تحويل أمين للشفرة، وذلك لأن محول الشفرة ملزم بتحليل التدفق JPSEC على مستوى الرزمة. أما الصعوبة الأخرى التي تنجم عن عملية تحويل الشفرة الأمين والأسهل هي إعادة ترتيب البيانات بحيث تصبح مكونات الاستبانة من جديد قطعاً متجاورة يظهر تخالفها في رأسية الواسم SEC. ويمكن تحقيق ذلك بطريقة متطابقة مع المعيار JPEG 2000 من خلال تغيير ترتيب الرزم JPEG 2000 من PCRL إلى RLCP ثم الإشارة إلى ترتيب التدرج الجديد في قطعة الواسم COD أو باستعمال قطعة واسم تغيير ترتيب التدرج (POC). ويبين الشكل 11.B نتيجة إعادة ترتيب البيانات وتحويل الحماية. ومرة أخرى تضم الرأسية الرئيسية للواسم SEC معلمات المنطقة ZOI التي تضف المعلمات المقابلة المتصلة بالصورة وبتدفقات البتات والمصاحبة لكل قطعة بيانات، لكن في التدفق المشفر JPEG 2000 معاد الترتيب هذه المرة.



الشكل 11.B – مثال لتشكيل تدفق مشفر JPSEC

3.11.B قواعد تركيب التدفق المشفر

يمكن استخدام قواعد التركيب JPSEC من أجل استحداث نظام تسيير تدفق تدرجي أمين وتحويل شفرة أمين مع أداة حماية النموذج. ومن الممكن خصوصاً استعمال منطقة التأثير (ZOI) مع نموذج فك التشفير ومجال المعالجة والتحبب من أجل التحديد الكامل لعملية فك التشفير التي ينبغي لمستهلك البيانات JPSEC الحاصل على ترخيص أن يستخدمها في فك تشفير التدفق. وعلاوة على ذلك، تشير معلمات المنطقة ZOI إلى المعلومات التي تستطيع عُقد تحويل الشفرة أن تستخدمها في تحويل شفرة أمين.

وتحدد المعلمة ZOI مناطق ثلاث، منطقة لكل استبانة، وأمدية أثمونات مصاحبة للبتات المشفرة لكل منطقة. وتظهر قواعد تركيب التشوير الخاصة بنموذج حماية فك التشفير ومجال المعالجة والتحبب في الجدول 27.B. وتظهر طريقة فك التشفير مع نموذج حماية فك التشفير. وفي هذه الحالة تحدد التجفير AES بالأسلوب CTR وكذلك حجم الفدرة وطول المفتاح. ويحدد مجال المعالجة والتحبب من ناحية أخرى كيفية إجراء فك التشفير. وتشير الطريقة إلى أن مجال المعالجة هو تدفق البتات ذاته وأن رأسيات الرزم ومتون الرزم مشفرة. ويمكن تحديد طرق مختلفة لفك التجفير من خلال تغيير مجال المعالجة والتحبب. مثال: يمكن أن يحسب تحبب التجفير على صعيد الرزم إفرادياً أو أن يقتصر على متون الرزم. كما أن طريقة الاستيقان تتحدد مع نفس منطقة التأثير الواردة أعلاه لكن مع النموذج المعياري التالي للاستيقان. ويبين الشكل 28.B قواعد تركيب النموذج المعياري للاستيقان. ويجوز بالطبع أيضاً استعمال خوارزميات تجفير JPSEC أخرى وشفرات MAC أخرى. إضافة إلى ذلك يمكن استعمال الحل المقترح مع تواقيع رقمية وطرق تحكم في النفاذ وأدوات إدارة مفاتيح أخرى. كما يمكن إرفاق التشوه بكل رزمة (أو منطقة أخرى

من البيانات) تستخدم مجال التشوه (انظر الفقرة 2.3.7.5) بغية إتاحة تسيير أمين مستمثل استناداً إلى تشوه المعدل (R-D) وتحويل شفرة أمين [26] و[27] و[28].

الجدول 27.B – قيم معلمات أدوات حماية النموذج ومجال المعالجة والتحبب

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
T_{decry}	ME_{decry}		8	0	علم محاكاة الواسم هو NULL
	CT_{decry}		16	1	تجفير الخوارزمية AES
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	أسلوب CTR دون حشو
		P_{bc}	2	0	الحشو غير مستعمل في الأسلوب CTR
		SIZ_{bc}	8	128	حجم الفدرة 128 بتة
		KT_{bc}	متغير	*نموذج مفتاح*	نموذج معلومات المفتاح
PD			1	0_b	قطعة الأثمونات المتراصفة (BAS) لا تلي
			1	0_b	خارج مجال البيكسل
			1	0_b	خارج مجال معامل الموجات الصغيرة
			1	0_b	خارج مجال معامل الموجات المكمى
			1	1_b	معالَج في مجال التدفق المشفر
			3	000_b	غير مستعمل
G	PO		16	$0\ 0000\ 0101\ 0011\ 100_b$	ترتيب المعالجة هو TRLCP
	GL		8	$0000\ 1001_b$	التحبب هو المساحة الكلية التي تحددها المعلمة ZOI
V	N_V		16	1	تتحدد قيمة واحدة
	Sv		8	16	الطول = 16 أثموناً
	VL		128	*Nonce value*	قيمة العدّاد في الأسلوب CTR

الجدول 28.B – قيم معلمات أدوات حماية نموذج الاستيقان

المعلمة			الحجم (بالبتات)	القيمة (بالترتيب)	الدلالة الناتجة
T_{auth}	M_{auth}		8	0	التحكم MAC على أساس التقطيع
	P_{auth}	M_{HMAC}	8	1	الشفرة HMAC
		H_{HMAC}	8	1	معرف هوية التقطيع في الخوارزمية SHA-1
		KT_{HMAC}	متغير	*قيمة مفتاح*	انظر نموذج المفتاح
		SIZ_{HMAC}	16	80	طول التحكم MAC = 80 بتة (مأخوذة من 160)

4.11.B استنتاجات

تصف هذه الفقرة تسييراً أميناً قابلاً للقياس وتحويل شفرة أميناً باستعمال المعيار JPSEC الذي يفرز الخواص المتضاربة ظاهرياً للأمن من طرف إلى طرف مع تحويل شفرة أمين في عقد وسط الشبكة. وذلك يسمح بتحويل شفرة التدفقات JPSEC دون فك التشفير المطلوب. وإضافة إلى ذلك، توفر الطريقة إمكانية الاستيقان من أن تحويل الشفرة أجري على نحو صحيح ومقبول، وعدم حدوث تغييرات غير مقصودة أو عن سوء نية نتيجة خطأ أو هجوم. ويتيح ذلك لمخدم (غير أمين) أو عقدة وسط الشبكة مثل المخدم الوسيط أن يجريا تحويل شفرة أمين وأن يوفرا للمستهلك JPSEC في نفس الوقت إمكانية استيقان أن المحتوى المستقبَل قد عولج على نحو صحيح ومقبول.

الملحق C

قابلية التشغيل البيني

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

1.C الجزء 1

ثمة عدد من طرق الحماية التي يمكن تطبيقها على التدفقات JPEG 2000 بهدف استحداث تدفقات JPSEC تبقي مطابقة تماماً للجزء 1 من المعيار JPEG 2000. ويُستخدم المصطلح "مطابق للجزء 1" للدلالة على التدفقات JPSEC ذات السلوك المحدد تماماً في مفككات تشفير المعيار JPEG 2000 الجزء 1، بما فيها تلك التي لا تعرف قواعد التركيب JPSEC.

ومفكك تشفير المعيار JPEG 2000 الجزء 1، يتخطى قطع الواسم التي لا يتعرف عليها. وتدرج أداة JPSEC مثل الأداة JPSEC المعيارية لاستيقان قيم شفرة استيقان الرسالة المحسوبة استناداً إلى البيانات JPEG 2000 داخل قطعة الواسم SEC مع المعلمات التي تصف طرق الاستيقان التي يجوز للمستعمل JPSEC استعمالها. وتُعلم هذه المعلمات والقيم المستعمل JPSEC بكيفية التحقق من صحة التدفق JPSEC المستقبل. وتجدر الإشارة إلى أن أداة الاستيقان JPSEC لا تتدخل في البيانات JPEG 2000. لذا، فإن مفكك تشفير الجزء 1 JPEG 2000 الذي يستقبل هذا التدفق JPSEC، يبدأ بفك تشفيره ثم يتجاوز قطعة الواسم SEC ويستمر في فك تشفير التدفق JPSEC كما لو كان تدفقاً JPEG 2000 الجزء 1. وتتقاسم الأدوات JPSEC المعيارية للاستيقان هذه الخصائص وبالتالي تُنتج أيضاً تدفقاً مطابقاً للجزء 1.

ويتيح المعيار JPSEC إجراء عمليات التجفير وفك التجفير في التدفقات المشفرة JPEG 2000 وJPSEC. وعند استعمال التجفير تتغير بالطبع البيانات JPEG 2000. ومطابقة الجزء 1 تحديداً غير ممكنة مع تدفقات مفككة التجفير إذ أنها ستلزم مفكك التشفير JPEG 2000 الجزء 1 باستقبال قيم غير مسموح بها. وإحدى الطرق الممكنة لتخطي هذه المشكلة أو للتخفيف منها على الأثقل هي استخدام مقدرات التفاوت المسموح في المعيار JPEG 2000. وقد يكون من الممكن عند استعمال قيم التفاوت المسموح بها الحصول على تدفقات JPSEC مجفرة ذات سلوك محدد مقبول من مفككات التشفير الجزء 1 JPEG 2000.

وللتدفق JPSEC مجال معلمة P_{sec} يحتوي على معلمات الأمن المخصصة لكامل التدفق. ويضم عَلَماً F_{J2K} يوضع على القيمة 1 للدلالة على أن التدفق JPSEC قابل للمعالجة في مفككات تشفير الجزء 1 JPEG 2000. ويجوز للمستحدث JPSEC أن يضع هذه المعلمة عند استخدامه للأدوات JPSEC على قيمة التدفق JPEG 2000. وقد ذكر أن المستحدث JPSEC يستطيع أن يقبل دخول تدفق محمي JPSEC. وإذا تلقى المستحدث JPSEC تدفقاً JPSEC داخلاً مع عَلَم F_{J2K} يشير إلى المطابقة للجزء 1 ثم يستخدم أداة JPSEC تفقده فيما بعد المطابقة للجزء 1، توجب على هذا المستحدث أن يضع العَلَم F_{J2K} على القيمة 0.

وفيما يتعلق بالتدفقات JPSEC غير المطابقة للجزء 1، يوصى باستعمال الملف jp2s. للدلالة على أن مفكك تشفير الجزء 1 من المعيار JPEG 2000 قد لا يكون قادراً على فك تشفير التدفق المحمي.

2.C الجزء 2

يُستخدم التعديل 2 للجزء 2 من المعيار JPEG 2000 الذي أدخل على قطعة واسم المقدرات الموسعة (CAP) في الدلالة على استعمال JPSEC. ويستعمل الجزء 2 تحديداً المعلمة R_{siz} للدلالة على وجود قطعة الواسم CAP التي تضم المعلمة C_{cap} التي يمكن استخدامها في الإشارة إلى الأجزاء JPEG 2000 المستعملة في التدفق. فبالإمكان الإشارة إلى استعمال الجزء 8 من المعيار JPEG 2000 (JPSEC) بوضع البتة الملائمة في المعلمة C_{cap}.

وبالتالي يمكن لمستحدث JPSEC أن يضع معلمةR_{siz} للإشارة إلى وجود قطعة واسم CAP. ويمكنه إدخال أو تحرير قطعة واسم CAP على نحو تدل فيه المعلمة C_{cap} على استعمال الجزء 8.

3.C المعيار JPIP

1.3.C العلاقة العامة بين المعيارين JPIP وJPSEC

يحدد المعيار JPIP بروتوكولاً ينطوي على سلسلات منتظمة من التفاعلات التي تقوم بين الزبون والمخدم وتسمح بتبادل تدفقات مشفرة لشروحات ملفات الصورة وبنيتها والصورة الجزئية أو الكاملة بطريقة فعالة في الاتصالات.

ويمكن تكييف المعيار JPIP من خلال توسيعات مختلفة لنسق الملف JPEG 2000 كما يرد تحديده في التوصيات | المعايير الدولية ITU-T T.801 | ISO/IEC 15444-2 وITU-T T.802 | ISO/IEC 15444-3 وISO/IEC 15444-6 | ITU-T T.805. ولكن من أجل بلوغ مستوى بسيط من التفاعلية التي تتيح نقل أجزاء من ملف أو تدفق JPEG 2000 واحد، لا يسمح بهذه المقدرات الإضافية.

وقد أدخلت أحكام تقضي بتوسيع البروتوكول JPIP ليشمل المعايير JPEG 2000 الحالية، مثل التوصية ITU-T T.802 | ISO/IEC 15444-3 والمعيار MJPEG 2000 والتوصية ITU-T T.805 | ISO/IEC 15444-6، وأنساق ملفات الصور المركبة والأجزاء اللاحقة للمعيار JPEG 2000 (حالياً JP3D وJPSEC وJPWL).

ويوفر المعيار JPSEC خدمات الأمن للصور JPEG 2000. وتقدم قواعد المعيار JPSEC نمطين من الوسوم: SEC وINSEC. ويظهر واسم SEC واحد أو أكثر في الرأسية الرئيسية لتدفق البتات JPSEC. وبعبارة أخرى يستخدم المعيار JPSEC تدفقات مشفرة JPEG 2000 ويغير رأسيتها الرئيسية ليشكل "رأسية رئيسية" JPSEC جديدة ويغير تدفق البيانات JPEG 2000 المرتبطة بها ليشكل تدفق بيانات محمياً جديداً حسب الاقتضاء. وقد تظهر الوسوم INSEC خيارياً في جزء "البيانات" من تدفق البيانات وذلك لتحديد بعض معلمات "الحجم الأصغر" أو "المنطقة المحلية" مقارنةً بالواسم SEC. وتستخدم هذه المعلمات كمكمِّلات للواسم SEC.

ويلاحظ أن البروتوكول JPIP يقع تماماً بعد طبقة النقل بينما يقع البروتوكول JPSEC في طبقة التطبيقات. ومن هذه الزاوية يقدم البروتوكول JPIP خدمة نقل إلى البروتوكول JPSEC. أي أن البروتوكول JPIP يوفر أدوات فعالة من أجل نقل معلومات الصورة بما فيها الرأسية الرئيسية (جميع الوسوم) والتدفقات المشفرة بين المخدمات والزبائن. وتتناول هذه الفقرة بالدراسة كيفية استخدام البروتوكول JPIP في نقل المحتوى JPSEC.

2.3.C مسائل محددة للتفاعلية بين البروتوكولين JPIP وJPSEC

تصف هذه الفقرة المسائل التي يجب أن يتفحصها مرسل ومستقبل البروتوكول JPIP عند نقل محتوى JPSEC.

وتنص الفقرة 5.3.A، "قطعة بيانات الرأسية الأساسية"، من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9 على أن نمطي الوسائل JPP وJPT يستخدمان قطعة بيانات الرأسية الأساسية. وتتألف قطعة البيانات هذه من قائمة متسلسلة من جميع الوسوم وقطع الوسوم التي ترد في الرأسية الأساسية بدءاً من الواسم SOC. ولا تضم أي وسوم SOT وSOD وEOC. غير أن الرأسية الأساسية JPEG 2000 لا تضم واسم SEC ولا قطعة هذا الواسم. ونتيجةً لذلك، لا تحدد الفقرة 5.3.A من المعيار JPIP FCD 2.0 توفير قطعة واسم SEC محددة في البروتوكول JPSEC وبالتالي، يجب تغيير مرسل ومستقبل البروتوكول JPIP بحيث يمكنهما التعرف على قطع الواسم SEC التي تظهر في الرأسية الأساسية لتدفق JPSEC.

وتصف الفقرة 2.3.A "قطع بيانات المنطقة"، من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9 كيفية توفيرها لبيانات المنطقة. غير أن الفقرة 2.3.A من المعيار JPIP FCD 2.0 لا تحدد أنها تدعم واسم INSEC ومنطقته المحددين في المعيار JPSEC. ولذلك يجب تعديل مرسل ومستقبل البروتوكول JPIP بحيث يتمكنان من التعرف على قطعة واسم INSEC قد ترد في جزء البيانات من تدفق مشفر JPSEC ما.

ولا تظهر قطع بيانات رأسية الرقعة حسب الفقرة 3.3.A، "قطع بيانات رأسية الرقعة"، من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9 إلاَّ في نمط وسائل التدفق JPP. وفي قطع البيانات التي تنتمي لهذا الصنف، يَحمل معرف هوية داخل الصف دليل الرقعة (بدءاً من 0) التي تحيل إليها قطعة البيانات. وتتكون قطعة البيانات من الوسوم وقطع الوسوم الخاصة بالرقعة n. ولا تضم قطعة الواسم SOT، أما إدخال الوسوم SOD فخياري. ويمكن تشكيل قطعة البيانات هذه من تدفق نظامي من خلال تسلسل جميع قطع الوسوم ما عدا SOT وPOC في جميع رأسيات أجزاء الرقعة n.

ولا تستخدم قطع بيانات الرقعة بموجب الفقرة 4.3.A "قطع بيانات الرقعة" من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9، إلاَّ مع نمط وسائط التدفق JPT. وفي قطع البيانات التي تنتمي لهذا الصنف، يحمل معرف الهوية داخل الصنف دليل الرقعة (بدءاً من 0) التي تعود إليها قطعة البيانات. وتقابل كل قطعة بيانات رقعة سلسلة من الأثمونات تتشكل من تسلسل جميع أجزاء الرقعة التي تعود إلى الرقعة بالترتيب مع الواسمين SOT وSOD التابعين لها وجميع القطع الأخرى المتصلة بالواسم.

وكما ذُكر أعلاه تصف الفقرتان 4.3.A و5.3.A من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9 توفير رأسية جزء الرقعة وبياناته. غير أن الفقرتين 4.3.A و5.3.A من التوصية | المعيار ITU-T T.808 | ISO/IEC 15444-9 لا تحددان توفير قطع الواسم SEC وقطع الواسم INSEC. وبالتالي، يجب تغيير المرسل والمستقبل JPIP بحيث يمكنهما التعرف على قطع الواسم هذه ونقلها مع البيانات المحمية.

3.3.C ملخص

يتكيف البروتوكول JPSEC عموماً بحيث يتمكن البروتوكول JPIP من نقله. ويستخدم الواسم INSEC في التدفق المشفر في وصف جزء "صغير" محدد من البيانات تحميه أداة/أدوات الأمن. كما يجعل هذا الواسم التدفق JPSEC أكثر مرونة. ولجعل الواسم INSEC أكثر متانة ينبغي أن توفر طبقة الخدمة (نعني JPIP هنا) نوعية الخدمة الجيدة أو الحماية اللازمة للواسم INSEC وقطعته. وحرصاً على تحقيق هذا الهدف لا بد من أن يعمل البروتوكولان JPIP وJPSEC على حل بعض المسائل والتأكد من توفير التفاعلية بين البروتوكولين JPIP وJPSEC.

4.C البروتوكول JPWL

يوسع المعيار JPEG 2000 دون سلك (JPWL) (التوصية | المعيار ITU-T T.810 | ISO/IEC 15444-11) المواصفة JPEG 2000 الأساسية لتشمل الإرسال الفعال للصور JPEG 2000 في بيئة إرسال معرضة للخطأ. ويعرف البروتوكول JPWL تحديداً مجموعة من الأدوات والطرائق لحماية التدفقات من أخطاء الإرسال. كما يعرف أيضاً سبل وصف حساسية التدفقات لأخطاء الإرسال ووصف مواقع أخطاء الإرسال المتبقية في التدفق.

ويتناول المعيار JPWL أساساً حماية رأسية الصورة وشفرات تصحيح الأخطاء الأمامي (FEC) والحماية النسبية من الأخطاء (UEP) وتشفير قناة المصدر المرفقة وتجزئة البيانات وتشذيرها والتشفير الحسابي الموثوق. ولا يرتبط المعيار JPWL بشبكة محددة أو بروتوكول نقل محدد، ولكنه يقدم حلاً نوعياً لإرسال أمين للصور JPEG 2000 في شبكات معرضة للأخطاء.

والوظائف الرئيسية للبروتوكول JPWL هي التالية:

- حماية التدفق المشفر من أخطاء الإرسال؛
- بيان درجة حساسية مختلف أجزاء التدفق لأخطاء الإرسال؛
- بيان مواقع الأخطاء المتبقية في التدفق المشفر.

ويحدد البروتوكول JPWL أربع قطع وسم هي: مقدرة الحماية من الخطأ (EPC) وفدرة الحماية من الخطأ (EPB) وواصف الحساسية للخطأ (ESD) وواصف الخطأ المتبقي (RED).

وتدل قطعة الواسم EPC على الأدوات JPWL المعيارية وغير المعيارية المستخدمة في التدفق. وتحدد بعبارة أدق وجود قطع الواسم المعيارية الثلاث الأخرى التي يعرفها المعيار JPWL في التدفق، وهي واصف الحساسية للأخطاء (ESD) وواصف الخطأ المتبقي (RED) وفدرة الحماية من الأخطاء (EPB). وإضافة إلى ذلك، يُشير الواسم EPC إلى استعمال أدوات معيارية سبق تسجيلها لدى هيئة التسجيل JPWL RA. والواسم EPC إلزامي في التدفق المشفر JPWL.

والوظيفة الأساسية للفدرة EPB هي حماية الرأسية الأساسية ورأسية جزء الرقعة. ويمكن استعمالها أيضاً لحماية بقية التدفق المشفر. وتضم قطعة الواسم EPB معلومات عن معلمات الحماية من الخطأ وبيانات متكررة تُستخدم في حماية التدفق المشفر من الأخطاء.

وتضمن قطعة الواسم ESD معلومات عن حساسية التدفق المشفر للأخطاء. ويمكن الاستفادة من هذه المعلومات عند تطبيق تقنية الحماية النسبية من الأخطاء (UEP). وبعبارة أوضح تستعمل شفرات أكثر قدرة لحماية أجزاء التدفق الأكثر حساسية. كما يمكن استخدام هذه المعلومات أيضاً في الإرساليات الانتمائية. وأخيراً تُستعمل المعلومات التي يحملها الواسم ESD في تطبيقات أخرى غير JPWL مثل تحويل شفرة فعال لمعدل أو القراءة المسبقة الذكية.

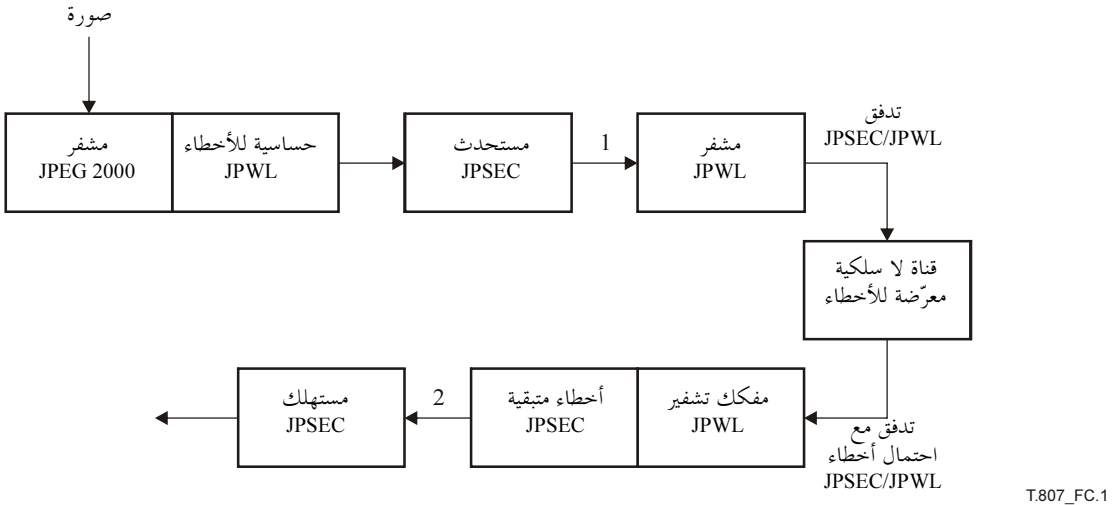
وتشير قطعة الواسم RED إلى وجود أخطاء متبقية في التدفق المشفر. وبالحقيقة قد يخفق مفكك تشفير JPWL في تصحيح الأخطاء في التدفق. بينما يوفر الواسم RED إمكانية الإشارة إلى موقع هذه الأخطاء المتبقية. ويمكن لمفكك التشفير JPEG 2000 بعدئذٍ الاستفادة من هذه المعلومات ليعمل بشكل أفضل للحماية من هذه الأخطاء. إذ يمكنه على سبيل المثال أن يطلب إعادة الإرسال أو محو الأخطاء أو استبعاد المعلومات الفاسدة.

1.4.C العلاقة العامة بين المعيارين JPWL وJPSEC

يُشترط الجمع بين المعيارين JPWL وJPSEC عندما تتطلب الصور JPEG 2000 ضمان أمنها وإرسالها في قنوات لا سلكية معرضة للأخطاء.

وتنتج حساسية البروتوكول JPWL للخطأ عادةً جهة الإرسال أثناء تشفير التدفق JPEG 2000. ثم تطبق أدوات البروتوكول JPSEC على التدفق من أجل توفير الأمن له. وتستخدم أخيراً أدوات التشفير JPWL لجعل التدفق أكثر مقاومة لأخطاء الإرسال.

وتُستخدم أولاً أدوات فك التشفير JPWL جهة الاستقبال، من أجل تصحيح أخطاء الإرسال المحتملة. وقد يُنتج أيضاً البروتوكول JPWL خلال هذه المرحلة معلومات عن أخطاء متبقية. وتطبَّق أخيراً الأدوات JPSEC بهدف تنفيذ خدمات الأمن المنتقاة.



الشكل 1.C – الطريقة النموذجية لجمع البروتوكولين JPWL وJPSEC

2.4.C مسائل محددة لقابلية التشغيل البيني بين البروتوكولين JPWL وJPSEC

ينبغي دراسة عدد من المسائل المتعلقة بقابلية التشغيل البيني بين البروتوكولين JPWL وJPSEC، وفيما يلي تفاصيلها:

1) مقدرة الحماية من الأخطاء (EPC) في البروتوكول JPWL: يؤثر وجود قطعة الواسم هذه على أمدية الأثمونات. وجدير بالذكر أن استعمال هذه القطعة إلزامي في التدفق المشفر JPWL.

2) فدرة الحماية من الأخطاء (EPB) في البروتوكول JPWL: تضاف قطعة الواسم هذه إلى المرسِل كمرحلة أخيرة وتلغى في أول مرحلة في المستقبل. وينبغي مبدئياً ألاّ تؤثر على البروتوكول JPSEC.

3) واصف الحساسية للأخطاء (ESD) في البروتوكول JPWL: تضاف قطعة الواسم هذه عادةً أثناء التشفير وفقاً للجزء 1 من المعيار JPEG 2000 الذي يكون شفافاً في مثل هذه الحالة للعمليات JPSEC اللاحقة. غير أن البروتوكول JPSEC قد يؤثر بالمقابل على استعمال الواصف ESD في البروتوكول JPWL. وينبغي خاصةً ألاّ يغير البروتوكول JPSEC امتدادات الأثمونات كلما استعمل الواصف ESD هذه الامتدادات. وإضافة إلى ذلك، ينبغي ألاّ تؤثر العمليات JPSEC على قيم التشوُّه؛ وإلاّ تصبح المعلومات التي ينقلها الواصف ESD دون فائدة. وفي هذه الحالة الأخيرة يبقى أمام المستحدث JPSEC خيار إلغاء قطعة الواسم ESD.

4) واصف الأخطاء المتبقية (RED) في البروتوكول JPWL: يمكن إدراج قطعة الواسم هذه بعد فك تشفير البروتوكول JPWL. وقد يؤثر ذلك بالتالي على امتدادات الأثمونات JPSEC. كما قد تؤثر على تقنيات استيقان البروتوكول JPSEC. وفي حال تدفق مشفر فاسد، قد تكون معلومات الواصف RED مفيدة للمستعمل JPSEC في معالجة هذا التدفق.

5) الواسم JPSEC SEC: يؤثر وجود قطعة الواسم هذه على امتدادات الأثمونات. وجدير بالذكر أن هذه القطعة إلزامية في التدفق JPSEC.

6) الواسم JPSEC INSEC: يؤثر وجود قطعة الواسم هذه على امتدادات الأثمونات. وتظهر قطعة الواسم هذه في بيانات التدفق المشفر.

وفي حال عدم وجود أخطاء متبقية، ينبغي نظرياً أن يكون المشفر ومفكك التشفير JPWL شفافين. وبعبارة أخرى، ينبغي في هذه الحالة أن يكون تدفقا النقطتين 1 و2 في الشكل الوارد أعلاه متماثلين تماماً.

ويوصى عموماً عند جمع البروتوكولين JPSEC وJPWL، بأن يستخدم البروتوكول JPSEC امتدادات الأثمونات بدءاً من نهاية الواسم SOD بهدف الحد من المشاكل التي تسببها امتدادات الأثمونات. كما يفضل أن يقتصر وجود قطعة الواسم JPWL على الرأسية الرئيسية وأن يتم تجنبه في رأسيات جزء الرقعة.

الملحق D

بيانات البراءات

(لا يشكل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

ملاحظة – الملحق D ملحق بالمعيار الصادر عن ISO/IEC. وترد أسماء الشركات التي تقدم بيانات البراءات إلى الاتحاد تتعلق بهذا النص في قاعدة بيانات حقوق الملكية الفكرية (IPR). ويرجى الاطلاع على العنوان التالي: http://itu.int/ITU-T/ipr/.

وتسترعي المنظمة الدولية للتقييس (ISO) واللجنة الدولية الكهرتقنية (IEC) الانتباه إلى إمكانية الادعاء بأن الامتثال لهذا الجزء من المعيار ISO/IEC 15444 قد تنطوي على استعمال البراءات.

ولا تتخذ المنظمة ISO واللجنة IEC أي موقف من القرائن المتعلقة بصحة حقوق البراءة أو صلاحيتها أو نطاق تطبيقها.

وق أكّد حاملو هذه البراءات للمنظمة ISO وللجنة IEC استعدادهم للدخول في مفاوضات بشأن منح التراخيص وفق أحكام وشروط معقولة وغير تمييزية مع من يطلبها في مختلف أرجاء العالم. وفي هذا الخصوص، فإن بيانات أصحاب الحقوق في هذه البراءات مسجلة في المنظمة ISO واللجنة IEC. ويمكن الحصول على معلومات بهذا الشأن من الشركات المذكورة أدناه.

ويوجَّه الانتباه إلى احتمال أن تخضع بعض عناصر هذا الجزء من المعيار ISO/IEC 15444 لحقوق براءات غير تلك المذكورة في هذا الملحق. والمنظمة ISO واللجنة IEC ليستا مسؤولتين عن تحديد أي من حقوق البراءات هذه أو كلها.

الجدول 1.D – قائمة البيانات

الرقم	الكيان مقدم الطلب
1	Canon Inc
2	Columbia University
3	EMITALL Surveillance
4	HP
5	Institute for Infocomm Research
6	MediaLive
7	New Jersey Institute of Technology

بيبليوغرافيـــا

[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.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	**المطاريف الخاصة بالخدمات التلماتية**
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2007