TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN 11777-8:2018

ISO/IEC 15444-8:2007

WITH AMENDMENT 1:2008

CÔNG NGHỆ THÔNG TIN – HỆ THỐNG MÃ HÓA HÌNH ẢNH JPEG 2000 – BẢN MẬT JPEG 2000

Information technology - JPEG 2000 image coding system - Secure issues for JPEG 2000 codestreams

HÀ NỘI - 2018

Mục lục

Lời nói đầu

TCVN 11777-8:2018 hoàn toàn tương đương ISO/IEC-15444-8:2007 (và With amendment 1:2008).

TCVN 11777-8:2018 do Học viện Công nghệ Bưu chính Viễn thông biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Hệ thống mã hóa hình ảnh JPEG 2000 – Bảo mật JPEG 2000

Information technology - JPEG 2000 image coding system: Security issues for JPEG 2000 codestreams

1 Phạm vi áp dụng

Tiêu chuẩn này quy định cụ thể khung làm việc, các khái niệm và phương pháp để bảo mật các dòng mã JPEG 2000. Phạm vi của tiêu chuẩn này định nghĩa:

1) cú pháp dòng mã chuẩn bao gồm thông tin giải thích dữ liệu ảnh bảo mật;

2) quy trình chuẩn đăng ký các công cụ JPSEC với một cơ quan đăng ký cung cấp một định danh duy nhất;

3) ví dụ tham khảo về các công cụ JPSEC trong các trường hợp sử dụng điển hình;

4) hướng dẫn tham khảo về cách triển khai các dịch vụ bảo mật và siêu dữ liệu liên quan.

Phạm vi của tiêu chuẩn này không mô tả các ứng dụng tạo ảnh bảo mật cụ thể hoặc hạn chế tạo ảnh bảo mật với các kỹ thuật cụ thể, nhưng nó tạo ra một khung làm việc cho phép mở rộng phát triển kỹ thuật tạo ảnh bảo mật trong tương lai.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả sửa đổi, bổ sung (nếu có).

ITU-T Recommendation T.800 (2002) | ISO/IEC 15444-1:2002, Information technology – JPEG2000 Image Coding System: Core coding system (*Công nghệ thông tin – Hệ thống mã hóa ảnh JPEG 2000: Hệ thống mã hóa lõi*).

ITU-T Recommendation T.801 (2002) | ISO/IEC 15444-2:2004, Information technology – JPEG 2000 image coding system: Extensions (*Công nghệ thông tin – Hệ thống mã hóa ảnh JPEG 2000: Phần mở rộng*).

ITU-T Recommendation T.803 (2002) | ISO/IEC 15444-4:2004, Information technology – JPEG 2000 image coding system: Conformance testing (*Công nghệ thông tin – Hệ thống mã hóa ảnh JPEG 2000: Kiểm tra sự phù hợp*).

ISO/IEC 13818-11:2004, Information technology – Generic coding of moving pictures and associated audio information – Part 11: IPMP on MPEG-2 systems *(Công nghệ thông tin - Mã hóa chung của hình ảnh động và thông tin âm thanh liên quan - Phần 11: IPMP trên các hệ thống MPEG-2).*

ISO/IEC 15444-6:2003, Information technology – JPEG 2000 image coding system – Part 6: Compound image file format *(Công nghệ thông tin – Hệ thống mã hóa ảnh JPEG 2000 – Định dạng tập tin ảnh hợp thành).*

ISO/IEC 15444-12:2005, Information technology – JPEG 2000 image coding system – Part 12: ISO base media file format (*Công nghệ thông tin – Hệ thống mã hóa ảnh JPEG2000 – Định dạng tập tin truyền thông dựa trên ISO).*

3 Thuật ngữ, định nghĩa

3.1

Kiểm soát truy cập (access control)

Phòng chống việc sử dụng trái phép nguồn tài nguyên, bao gồm cả phòng chống sử dụng nguồn tài nguyên theo một phương pháp trái phép.

3. 2

Xác thực (authentication)

Quy trình xác minh danh tính được yêu cầu bởi (hoặc cho) một thực thể hệ thống.

3. 2.1

Xác thực nguồn (source authentication)

Xác nhận rằng một thực thể nguồn đúng là thực thể nguồn được yêu cầu.

3. 2.2

Xác thực ảnh mảnh/bán mảnh (fragile/semi-fragile image authentication)

Quy trình cho xác thực nguồn ảnh và xác minh tính toàn vẹn nội dung ảnh/dữ liệu ảnh có thể phát hiện bất kỳ thay đổi trong tín hiệu, xác định vị trí thay đổi và tín hiệu gì đã thay đổi trước đó.

CHÚ THÍCH - Nó phục vụ chứng minh tính xác thực của tài liệu. Sự khác biệt giữa xác thực ảnh mảnh và bán mảnh là xác thực ảnh mảnh để xác minh tính toàn vẹn dữ liệu ảnh, còn xác thực ảnh bán mảnh để xác minh tính toàn vẹn nội dung ảnh.

3. 3

Tính bảo mật (confidentiality)

Thuộc tính mà thông tin không được cung cấp hoặc tiết lộ cho các cá nhân, các thực thể hoặc quy trình trái phép (không được xác thực).

3.4

Phân tách dữ liệu (data splitting)

Phương pháp để bảo vệ dữ liệu nhạy cảm khỏi truy cập trái phép bằng cách mã hóa dữ liệu và lưu trữ các phần khác nhau của tập tin trên các máy chủ khác nhau.

CHÚ THÍCH: - Khi truy cập dữ liệu phân tách thì các phần được lấy ra, kết hợp và giải mã. Người không được xác thực sẽ phải biết vị trí của các máy chủ chứa các phần, phải truy cập vào mỗi máy chủ, biết dữ liệu nào để kết hợp và làm thế nào để giải mã nó.

3.5

Giải mã (decryption, deciphering)

Quá trình chuyển đổi ngược của mã hóa.

3.6

Chữ ký số (digital signature)

Dữ liệu được thêm vào, hoặc biến đổi mật mã của, một đơn vị dữ liệu mà cho phép bên nhận đơn vị dữ liệu đó chứng minh nguồn gốc, tính toàn vẹn của đơn vị dữ liệu và bảo vệ chống lại sự giả mạo.

3.7

Mã hóa (encryption)

Chuyển đổi dữ liệu thành một bảng mã bằng một thuật toán mã hóa để ẩn các nội dung thông tin của dữ liệu.

CHÚ THÍCH: - Thuật ngữ thay thế cho thuật toán mã hóa là mật mã

3.8

Bản nhận dạng vân tay (fingerprints)

Đặc điểm của một đối tượng dùng để phân biệt với các đối tượng tương tự khác, cho phép chủ sở hữu theo dõi người dùng được ủy quyền phân phối chúng bất hợp pháp.

CHÚ THÍCH - Bản nhận dạng thường được thảo luận trong ngữ cảnh truy tìm kẻ phản bội.

3.9

Hàm băm (hash function)

Hàm chuyển đổi chuỗi bit có chiều dài bất kỳ thành chuỗi bit có chiều dài cố định, thỏa mãn hai thuộc tính sau:

CHÚ THÍCH: - Đối với một đầu ra cho trước, nó là tính toán không khả thi để tìm một đầu vào ánh xạ với đầu ra đó. Đối với một đầu vào cho trước, nó là tính toán không khả thi để tìm một đầu vào thứ hai ánh xạ với đầu ra tương tự. Tính khả thi tính toán phụ thuộc vào môi trường và yêu cầu bảo mật cụ thể của người sử dụng.

3.10

Tính toàn vẹn (integrity)

Thuộc tính bảo đảm tính chính xác và đầy đủ của thông tin, dữ liệu.

3.10.1

Tính toàn vẹn dữ liệu ảnh (image data integrity)

Thuộc tính đảm bảo dữ liệu không bị thay đổi hoặc bị phá hủy một cách trái phép.

3.10.2

Tính toàn vẹn nội dung ảnh (image content integrity)

Đảm bảo nội dung ảnh không bị sửa đổi bởi các bên trái phép, làm cho ý nghĩa nhận thức của nó bị thay đổi.

CHÚ THÍCH: - Nó cho phép các hoạt động bảo quản nội dung được thực hiện trên các ảnh mà không cần kích hoạt cảnh báo tính toàn vẹn.

3.11

Ứng dụng JPSEC (JPSEC application)

Mọi quy trình phần cứng hoặc phần mềm có khả năng sử dụng các dòng mã JPSEC bằng cách biên dịch cú pháp JPSEC để cung cấp các dịch vụ bảo mật cụ thể.

CHÚ THÍCH: - Một ứng dụng JPSEC sử dụng một hoặc một số công cụ JPSEC

3.12

Dòng mã JPSEC (JPSEC codestream)

Dãy bit thu được từ mã hóa và bảo mật hình ảnh bằng cách sử dụng các mã hóa JPEG 2000 và công cụ bảo mật JPSEC.

3.12.1

Thực thể JPSEC (JPSEC creator)

Thực thể tạo ra một dòng mã JPSEC từ một ảnh, một dòng mã JPEG 2000 hoặc một dòng mã JPSEC khác để cung cấp một số dịch vụ JPSEC.

3.12.2

Người sử dụng JPSEC (JPSEC consumer)

Là thực thể nhận một dòng mã JPSEC và đưa ra một dịch vụ JPSEC dựa trên dòng mã.

3.13

Dịch vụ JPSEC (JPSEC service)

Dịch vụ cung cấp bảo mật cho việc sử dụng ảnh JPEG 2000. Dịch vụ chống lại tấn công bảo mật và tận dụng một hoặc một vài công cụ JPSEC.

3.14

Cơ quan đăng ký JPSEC (JPSEC registration authority)

Bộ phận có trách nhiệm cung cấp một ID duy nhất tham chiếu với một công cụ JPSEC và lưu trữ danh sách tham số của mô tả công cụ JPSEC.

3.15

Công cụ chuẩn JPSEC (JPSEC tool)

Quy trình phần mềm hoặc phần cứng sử dụng kỹ thuật bảo mật để thực hiện dịch vụ bảo mật.

3.15.1

Công cụ quy chuẩn JPSEC (JPSEC normative tool)

Công cụ JPSEC sử dụng các mẫu công cụ được xác định trước để giải mã, xác thực hoặc băm được đặc tả bởi một phần quy chuẩn của tiêu chuẩn này.

3.15.2

Công cụ không quy chuẩn JPSEC (JPSEC non-normative tool)

Công cụ JPSEC được đặc tả bởi số nhận dạng được cho bởi Cơ quan đăng ký JPSEC hoặc bởi một ứng dụng định nghĩa theo người dùng.

3.15.3

Công cụ định nghĩa theo người dùng JPSEC (JPSEC user-defined tool)

Công cụ không quy chuẩn JPSEC được xác định bởi một ứng dụng định nghĩa theo người dùng.

3.15.4

Công cụ Cơ quan đăng ký JPSEC (JPSEC registration authority tool)

Công cụ không quy chuẩn JPSEC được xác định bởi Cơ quan đăng ký JPSEC.

3.16

Mô tả công cụ JPSEC (JPSEC tool description)

Mô tả các tham số được sử dụng bởi công cụ JPSEC.

3.17

Khóa (key)

Chuỗi các ký hiệu kiểm soát hoạt động của mã hóa và giải mã

3.17.1

Khóa đối xứng (symmetric keys)

Cặp khóa mà cả người khởi tạo và bên nhận đều sử dụng cùng khóa bí mật hoặc hai khóa có thể dễ dàng được tính từ khóa còn lại trong hệ thống mật mã.

3.17.2

Cặp khóa bất đối xứng (asymmetric key pair)

Cặp khóa quan hệ mà khóa riêng định nghĩa việc chuyển đổi riêng và khóa công khai định nghĩa việc chuyển đổi công khai.

3.17.2.1

Khóa riêng (private key)

Khóa của cặp khóa bất đối xứng của một thực thể mà sẽ không được tiết lộ.

3.17.2.2

Khóa công khai (public key)

Khóa của cặp khóa bất đối xứng của một thực thể có thể được công khai.

3.18

Chức năng tạo khóa (key generation, key generating function)

Chức năng mà từ một số tham số đầu vào (ít nhất một trong số đó phải bí mật), đưa ra các khóa đầu ra phù hợp với ứng dụng và thuật toán mong muốn.

3.19

Quản lý khóa (key management)

Tạo, lưu trữ, phân phối, xóa, đạt được và ứng dụng khóa phù hợp với chính sách bảo mật.

3.20

Mô phỏng mã đánh dấu (marker emulation)

Văn bản mật mã thu được từ quá trình mã hóa chứa một mã khởi tạo JPEG.

3.21

Thuật toán mã xác thực bản tin, hàm kiểm tra mật mã, hàm kiểm tra tổng mật mã (message authentication code algorithm, cryptographic check function, cryptographic checksum function)

Thuật toán để tính toán một hàm ánh xạ các chuỗi bit và một khóa bí mật vào các chuỗi bit có chiều dài cố định, đáp ứng hai thuộc tính sau:

- hàm được tính hiệu quả với bất kỳ khóa và bất kỳ chuỗi đầu vào nào;
- tính giá trị hàm trên bất kỳ chuỗi đầu vào mới nào thậm chí biết trước về tập các chuỗi đầu vào và giá trị hàm tương ứng, trong đó giá trị chuỗi đầu vào thứ i có thể được lựa chọn sau khi quan sát giá trị của hàm i-1 trước đó là tính toán không khả thi với bất kỳ khóa cố định và không biết trước.

CHÚ THÍCH: - Tính khả thi tính toán phụ thuộc vào môi trường và yêu cầu bảo mật cụ thể của người sử dụng.

3.21.1

Mã xác thực bản tin (MAC: message authentication code)

Chuỗi các bit là đầu ra của thuật toán MAC.

3.22

Tính không chối bỏ (non-repudiation)

Ràng buộc của một thực thể với giao dịch mà nó tham gia để giao dịch không bị bác bỏ sau đó (bị từ chối).

CHÚ THÍCH: - Bên nhận của một giao dịch có thể chứng minh cho một bên thứ ba trung lập rằng bên gửi được tuyên bố đã thực sự gửi các giao dịch.

3.23

Gói (packet)

Một phần của dòng bit JPEG 2000 Phần 1 (ITU-T Rec. T.800 | ISO/IEC 15444-1) bao gồm một mào đầu gói tin và dữ liệu ảnh được nén từ một lớp của phân khu ảnh của một độ phân giải của một khối ảnh thành phần.

CHÚ THÍCH: - Khái niệm này khác với thuật ngữ "gói" được sử dụng trong truyền dữ liệu qua mạng.

3.24

Bảo vệ (protection)

Quy trình để bảo vệ nội dung.

3.24.1

Khuôn mẫu bảo vệ (protection template)

Khuôn mẫu hoặc danh sách các trường tham số cần thiết để vận hành một phương pháp bảo vệ.

3.24.2

Phương pháp bảo vệ (protection method)

Phương pháp được sử dụng để tạo ra hoặc dùng nội dung được bảo vệ như mã hóa, giải mã, xác thực và kiểm tra tính toàn vẹn.

3.25

An toàn (security)

Tất cả các khía cạnh liên quan đến việc xác định, đạt được và duy trì tính bảo mật, tính toàn vẹn, tính sẵn có, chịu trách nhiệm, tính xác thực và độ tin cậy.

CHÚ THÍCH: - Một sản phẩm, hệ thống, hoặc dịch vụ được coi là bảo mật đến mức mà người sử dụng có thể tin rằng nó hoạt động (hoặc sẽ hoạt động) theo cách dự định. Điều này thường được xem xét trong ngữ cảnh đánh giá các mối đe dọa nhận thức hoặc thực tế.

3.26

Cú pháp báo hiệu (signalling syntax)

Tham số kỹ thuật của định dạng dòng mã JPSEC mà chứa tất cả các thông tin được yêu cầu để dùng ảnh JPEG 2000 bảo mật.

3.27

Chuyển mã (transcoding)

Hoạt động lấy một dòng mã được nén đầu vào và thích ứng hoặc chuyển đổi nó để tạo ra một dòng mã nén đầu ra có một số thuộc tính mong muốn.

3.27.1

Chuyển mã bảo mật (secure transcoding)

Hoạt động thực hiện chuyển mã, hoặc thích ứng một nội dung nén đầu vào được bảo vệ mà không bảo vệ nội dung.

CHÚ THÍCH: - Khái niệm chuyển mã bảo mật được sử dụng trái ngược với chuyển mã, nhấn mạnh rằng các hoạt động chuyển mã được thực hiện mà không ảnh hưởng đến bảo mật. Chuyển mã bảo mật cũng có thể được xem như thực hiện chuyển mã trong miền được mã hóa.

3.28

Thủy vân (watermark)

Tín hiệu ẩn thêm vào tín hiệu bao phủ để truyền tải dữ liệu ẩn.

3.28.1

Tạo thủy vân (watermarking)

Quy trình chèn dữ liệu đại diện cho một số thông tin vào dữ liệu đa phương tiện theo một trong hai cách sau đây:

- Cách tổn hao: tín hiệu bao phủ ban đầu sẽ không bao giờ có thể phục hồi khi thủy vân được nhúng.

- Các không tổn hao: tín hiệu bao phủ ban đầu có thể được phục hồi sau khi tách thủy vân.

3.29

Bộ giải mã thường (Normal decoder)

Bộ giải mã chuẩn là một quy trình để giải mã một dòng mã mà tuân thủ hoàn toàn với phần quy chuẩn của tiêu chuẩn mã hóa. Hành vi của nó không được xác định nếu nó cố gắng để giải mã một dòng mã không tuân thủ.

3.30

Bộ giải mã định dạng đáp ứng (Adaptive-format decoder)

Bộ giải mã định dạng đáp ứng là một quy trình để giải mã một dòng mã mà không tuân thủ hoàn toàn với phần quy chuẩn của tiêu chuẩn mã hóa. Nó sẽ tái tạo lại phương tiện (có thể với độ phân giải hoặc chất lượng thấp) ngay cả khi dòng mã có các gói bị thiếu hoặc mào đầu gói không phù hợp. Ví dụ, một

bộ giải mã định dạng thích ứng có thể hiểu một dòng mã được chuyển mã đơn giản, chẳng hạn như một dòng mã trong đó có các gói tin có độ phân giải cao nhất đã bị xóa bỏ.

3.31

Dòng sơ cấp (Elementary Stream (ES))

Dòng sơ cấp chứa một chuỗi các mẫu, mà mỗi mẫu có thể là một khung hình ảnh hoặc một phần tiếp theo của dữ liệu âm thanh. Một mẫu trong ES chứa dữ liệu phương tiện, cấu trúc dữ liệu byte, cấu trúc con trỏ, cấu trúc ngăn chứa, hoặc tổ hợp bất kỳ của các dữ liệu trên.

3.32

ES tự chứa (Self-Contained ES)

ES tự chứa chỉ chứa dữ liệu phương tiện mà định dạng của nó không được định nghĩa trong phụ lục E. ES tự chứa có thể được lưu trữ trong khung MDAT đồng vị trí với định dạng tập tin được đặc tả trong phụ lục E, hoặc được lưu trữ trong một tập tin riêng biệt có định dạng không được đặc tả trong phụ lục E.

3.33

ES soạn thảo (Composed ES)

ES soạn thảo có thể chứa một tổ hợp cấu trúc ngăn chứa, con trỏ và dữ liệu byte, nghĩa là các mẫu của nó được soạn thảo với dữ liệu từ các dòng sơ cấp khác. Một ES soạn thảo hoặc là dữ liệu bản sao (sử dụng cấu trúc dữ liệu byte) hoặc là dữ liệu tham chiếu (sử dụng con trỏ) từ các ES khác.

3.34

ES soạn thảo phân cấp (Scalable Composed ES)

ES soạn thảo phân cấp được tạo bởi các mẫu mà có thể không được giải mã bởi chính các mẫu đó. Nó có thể cần phải được kết hợp với các ES soạn thảo phân cấp khác để tạo thành một dòng mã có khả năng giải mã đầy đủ. ES soạn thảo phân cấp được thiết kế để hỗ trợ phân cấp, tức là, để làm cho dữ liệu phương tiện "có khả năng mỏng". Ví dụ, đối với một dòng mã JPEG 2000 chuyển động mà mỗi hình ảnh có ba lớp, nó có thể được chia thành 3 ES soạn thảo phân cấp: ES đầu tiên bao gồm tất cả dữ liệu lớp 0, ES thứ hai bao gồm tất cả dữ liệu lớp 1 và ES thứ ba gồm của tất cả dữ liệu lớp 2.

3.35

ES soạn thảo có khả năng giải mã (Decodable Composed ES)

ES soạn thảo có khả năng giải mã được tạo thành từ những mẫu mà có thể được giải mã bởi chính các mẫu đó. Nó được thiết kế cho đáp ứng đơn giản mà các bộ đáp ứng chỉ cần lấy dữ liệu được trỏ bởi cấu trúc con trỏ và loại bỏ băng ngoài để tạo thành một dòng mã phân cấp đầy đủ. Ví dụ, đối với một dòng mã JPEG 2000 chuyển động mà mỗi hình ảnh có ba lớp, nó có thể hình thành 3 ES soạn

thảo có khả năng giải mã gồm: ES đầu tiên bao gồm dữ liệu lớp 0, ES thứ hai bao gồm dữ liệu lớp 0 và lớp 1 và ES thứ ba gồm dữ liệu lớp 0, 1 và 2.

3.36

Bộ chuyển mã /Bộ thích ứng (Adaptor/transcoder)

Bộ chuyển mã /bộ thích ứng là một quá trình chuyển đổi dữ liệu phương tiện thành mức phân cấp thấp hơn, như độ phân giải thấp hơn hoặc tỷ lệ bit hoặc chất lượng thấp hơn, bằng cách loại bỏ các phần của tập tin. Bộ chuyển mã /bộ thích ứng có thể chuyển đổi dữ liệu phương tiện dựa trên thông tin đặc tả trong phục lục E. Một bộ chuyển mã /bộ thích ứng sẽ cập nhật các giá trị độ lệch byte trong các tham số định dạng tập tin bị tác động bởi quy trình này.

3.37

Bộ chuyển mã /Bộ thích ứng bảo mật (Secure adaptor/transcoder)

Bộ chuyển mã /Bộ thích ứng bảo mật là một quy trình chuyển đổi dữ liệu phương tiện được nhận thực hoặc mã hóa mà không cần thiết giải mã hoặc tạo lại MAC hoặc chữ ký. Vì vậy, bảo mật đầu cuối – đầu cuối còn lại dành cho dữ liệu phương tiện chuyển mã.

3.38

Bộ chuyển mã /Bộ thích ứng nhận biết JPEG 2000 (JPEG 2000-aware adaptor/transcoder)

Bộ chuyển mã /Bộ thích ứng nhận biết JPEG 2000 kết hợp một hoặc nhiều ES soạn thảo phân cấp để hình thành một dòng mã phương tiện có khả năng giải mã đầy đủ. Nó cần phải có khả năng tạo ra các mào đầu và mã đánh dấu của dòng mã phương tiện và sửa đổi chỉ số gói, do đó dòng mã được thích ứng được giải mã bởi một bộ giải mã thường. Nó cũng có thể thêm các gói trống để thay thế những gói bị loại bỏ, hoặc nó có thể chèn mã đánh dấu POC.

3.39

Bộ chuyển mã /Bộ thích ứng đơn giản (Simple adaptor/transcoder)

Bộ chuyển mã /Bộ thích ứng đơn giản có khả năng chuyển đổi dữ liệu dựa trên thông tin được đặc tả trong phụ lục E. Nó không có khả năng tạo ra các mào đầu phương tiện hoặc sửa đổi các chỉ số gói. Nó chỉ đơn giản là lấy dữ liệu được trỏ bởi cấu trúc con trỏ,loại bỏ các lớp bao và dòng mã thu được, được giải mã bởi bộ giải mã định dạng thích ứng, có thể đối phó với các gói tin bị mất và mào đầu không phù hợp.

3.41

Bộ chuyển mã /Bộ thích ứng xác thực (Authentication adaptor/transcoder)

Bộ chuyển mã /Bộ thích ứng xác thực loại bỏ dữ liệu mà không thể kiểm chứng với dữ liệu xác thực và dữ liệu phương tiện có sẵn. Ví dụ, trong một hệ thống trực tuyến, một số gói phương tiện có thể bị mất trong quá trình truyền. Một bộ nhận định dạng tập tin có thể tái tạo lại các dữ liệu nhận được hết khả

năng của mình dựa trên những dữ liệu có sẵn. Sau đó, một bộ chuyển mã /Bộ thích ứng xác thực có thể xác định dữ liệu có thể được xác nhận, và loại bỏ các gói tin không được xác minh. Các tập tin kết quả chỉ có chứa dữ liệu xác minh, được giải mã.

3.41

Ngăn chứa (Container)

Cấu trúc ngăn chứa được sử dụng để bao một mẫu trong một ES soạn thảo. Nó có thể chứa số lượng bất kỳ dữ liệu byte hoặc cấu trúc con trỏ, nhưng không được phép chứa một cấu trúc ngăn chứa khác.

3.42

Con trỏ (Pointer)

Cấu trúc con trỏ được sử dụng để tham chiếu một đoạn dữ liệu trong ES khác. Nó phải được chứa bên trong một cấu trúc ngăn chứa.

3.42

Dữ liệu byte (ByteData)

Cấu trúc dữ liệu byte được sử dụng để bao một đoạn dữ liệu mà được đặt vật lý trong một ES soạn thảo. Nó phải được chứa bên trong một cấu trúc ngăn chứa.

3.42

Mã 4CC (4CC Code)

Mã 4CC là một bộ định dạng 32-bit, thường có 4 ký tự có thể in. Một mã 4CC có thể được sử dụng để chỉ loại tập tin, loại khung định dạng tập tin, loại rãnh từ định dạng tập tin, loại mô tả mẫu định dạng tập tin và loại tham chiếu rãnh từ định dạng tập tin. Một mã 4CC phải được đăng ký với cơ quan đăng ký.

4 Chữ viết tắt

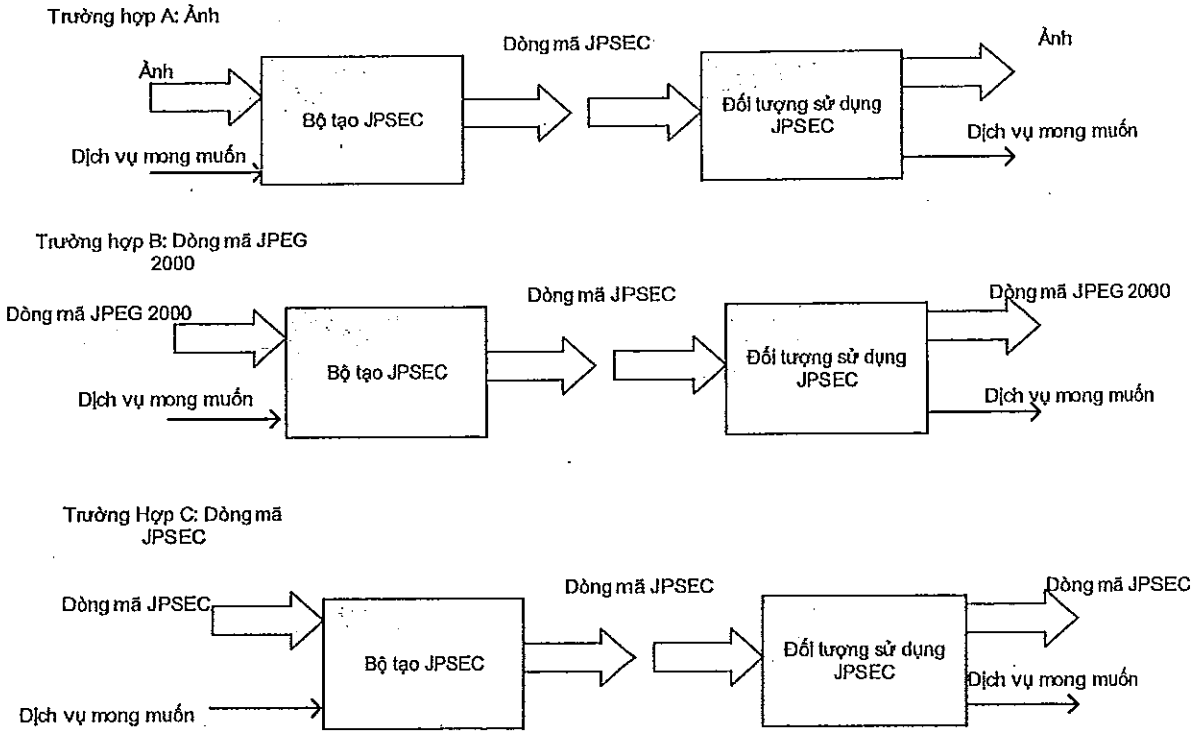
BAS	Byte Aligned Segment	Đoạn căn chỉnh byte
FBAS	Field Byte Aligned Segment	Đoạn căn chỉnh trường byte
G	Granularity	Độ chi tiết
GL	Granularity Level	Mức độ chi tiết
INSEC	In-codestream security marker	Mã đánh dấu bảo mật trong dòng mã
IP	Intellectual Property related to technology	Sở hữu trí tuệ liên quan đến công nghệ
IPR	Intellectual Property Rights related to content	Quyền sở hữu trí tuệ liên quan đến nội dung
JPSEC	Secure JPEG 2000	Bảo mật JPEG 2000

KT	Key Template	Khuôn mẫu khóa
LSB	Least Significant Bit	Bit có trọng số nhỏ nhất
MAC	Message Authentication Code	Mã xác thực bản tin
MSB	Most Significant Bit	Bit có trọng số lớn nhất
PD	Processing Domain	Miền xử lý
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
PO	Processing Order	Thứ tự xử lý
RA	Registration Authority	Cơ quan đăng ký
RBAS	Range Byte Aligned Segment	Đoạn căn chỉnh khoảng byte
SEC	Security marker	Mã đánh dấu bảo mật
T	Template	Khuôn mẫu
V	Values	Các giá trị
VL	Value List	Danh sách giá trị
ZOI	Zone of Influence	Vùng ảnh hưởng

5 Cú pháp JPSEC

5.1 Tổng quan khung làm việc JPSEC

JPSEC xác định một khung làm việc để bảo vệ dữ liệu được mã hóa JPEG 2000. Cốt lõi của tiêu chuẩn này là đặc điểm kỹ thuật của cú pháp ảnh JPEG 2000 bảo mật, dòng mã JPSEC. Cú pháp hướng tới dữ liệu được mã hóa JPEG 2000 và cho phép bảo vệ toàn bộ dòng mã hoặc các phần của dòng mã. Trong mọi trường hợp, dữ liệu được bảo vệ (nghĩa là dòng mã JPSEC) phải tuân theo cú pháp quy chuẩn trong tiêu chuẩn này.



Hình 1 - Tổng quan các bước khái niệm trong khung làm việc JPSEC

Để các dòng mã JPSEC gắn với một số dịch vụ bảo mật JPSEC bao gồm tính bảo mật, xác thực nguồn và nội dung.

Cú pháp báo hiệu xác định:

- Những dịch vụ bảo mật nào được kết hợp với dữ liệu ảnh;
- Những công cụ JPSEC nào được yêu cầu để cung cấp các dịch vụ tương ứng;
- Cách thức các công cụ JPSEC được áp dụng;
- Các phần nào của dữ liệu ảnh được bảo vệ.

Cú pháp của dòng mã JPSEC được quy chuẩn. Mục đích để cho phép các ứng dụng JPSEC sử dụng dòng mã JPSEC theo một cách tương thích (xem Hình 1). Ứng dụng người sử dụng JPSEC diễn giải dòng mã JPSEC, xác định và áp dụng các công cụ JPSEC được báo hiệu, cung cấp các dịch vụ bảo mật tương ứng và sau đó chuyển sang dòng mã JPEG 2000 đầu ra hoặc ảnh để xử lý tiếp theo, ví dụ như một trình xem ảnh.

Như trong trường hợp C của Hình 1, dòng mã JPSEC có thể được tạo ra từ một dòng mã JPSEC khác. Điều này có thể phát sinh khi nhiều công cụ JPSEC được áp dụng cho cùng một nội dung, nhưng ở thời điểm khác nhau hoặc bởi thực thể khác nhau. Khi điều này xảy ra, trình tự mà các công cụ JPSEC được áp dụng trong các hoạt động khởi tạo và tiêu thụ phải được chú ý.

Cú pháp báo hiệu xác định các công cụ được sử dụng bởi người sử dụng JPSEC. Công cụ được xác định bởi phần quy định của tiêu chuẩn hoặc bởi cơ quan đăng ký hoặc bởi các công cụ riêng. Các công cụ chuẩn hóa hỗ trợ tính bảo mật (thông qua các công cụ mã hóa) và xác thực nguồn, nội dung. Chúng tính đến loại tương tác cao nhất vì triển khai quá trình sử dụng độc lập với nhau nên có thể xử lý cùng các dòng mã JPSEC và hoàn lại các dịch vụ tương ứng với cách xử lý tương tự.

Cách thức mà các dòng mã JPSEC được tạo ra không nằm trong phạm vi của Tiêu chuẩn này. Để tuân thủ, bộ tạo JPSEC phải tạo ra dòng mã JPSEC bao gồm báo hiệu JPSEC thích hợp. Dòng mã JPEC có thể được tạo ra theo một số cách. Ví dụ, một công cụ JPSEC có thể được áp dụng cho các điểm ảnh hoặc nó được áp dụng với các hệ số sóng con, các hệ số lượng tử hóa hoặc các gói tin.

Người dùng có thể thực hiện một hoặc nhiều công cụ JPSEC. Ví dụ, có thể thực hiện giải mã bằng cách sử dụng thuật toán mã hóa khối AES trong chế độ ECB và xác minh chữ ký sử dụng hàm băm SHA và một khóa công khai RSA. Với những khả năng này, nó có thể thực hiện các dịch vụ bảo mật bảo mật và xác thực.

Trong khung làm việc JPSEC, công cụ JPSEC được quy định bởi các khuôn mẫu, xác định theo cách riêng, hoặc được đăng ký bởi một Cơ quan đăng ký của JPSEC. Công cụ JPSEC được đặc tả bởi các khuôn mẫu có cách xử lý duy nhất do đó không yêu cầu nhận dạng duy nhất. Những quy định cơ quan đăng ký có liên quan đến số nhận dạng duy nhất được cung cấp bởi đăng ký chung.

5.2 Dịch vụ bảo mật JPSEC

Mục tiêu trong điều này là liệt kê và giải thích các chức năng được bao gồm trong phạm vi của Tiêu chuẩn này.

Công cụ JPSEC được sử dụng để thực hiện các chức năng bảo mật. JPSEC là một khung làm việc mở, có nghĩa là nó có thể mở rộng trong tương lai. Hiện nay nó tập trung vào các khía cạnh sau:

- *Tính bảo mật thông qua mã hóa và mã hóa chọn lọc*

Một tập tin JPSEC có thể hỗ trợ chuyển đổi (ảnh và/hoặc siêu dữ liệu) dữ liệu (dạng thuần văn bản) thành một dạng (văn bản mật mã) che dấu ý nghĩa ban đầu của dữ liệu. Với mã hóa chọn lọc, không cần phải mã hóa toàn bộ ảnh và/hoặc siêu dữ liệu mà chỉ mã hóa một phần của ảnh và/hoặc siêu dữ liệu.

- *Xác minh tính toàn vẹn*

Một tập tin JPSEC có thể hỗ trợ phương pháp phát hiện các thao tác đối với ảnh và/hoặc siêu dữ liệu và do đó kiểm tra tính toàn vẹn của chúng. Có hai loại xác minh tính toàn vẹn:

1) Xác minh tính toàn vẹn dữ liệu ảnh mà chỉ một bit dữ liệu ảnh bị lỗi dẫn đến việc xác minh thất bại (ví dụ, xác minh trả về "không toàn vẹn"). Xác minh này cũng thường tham chiếu đến xác minh (tính toàn vẹn) ảnh mảnh.

2) Xác minh tính toàn vẹn nội dung ảnh mà một số thay đổi ngẫu nhiên của dữ liệu ảnh dẫn đến xác minh thành công miễn là sự thay đổi này không thay đổi nội dung ảnh dưới hệ thống thị giác của người xem; nói cách khác, ý nghĩa nhận thức ảnh không thay đổi. Xác minh này cũng thường tham chiếu đến xác minh (tính toàn vẹn) ảnh bán mảnh.

Xác minh tính toàn vẹn ảnh mảnh hoặc bán mảnh này có thể xác định các vị trí trong nội dung ảnh/ dữ liệu ảnh nơi mà tính toàn vẹn cần được xem xét. Giải pháp có thể bao gồm:

1) Phương pháp mật mã như mã xác thực bản tin (MAC), chữ ký số, tổng kiểm tra mật mã hoặc băm có khóa.

2) Phương pháp dựa trên công nghệ tạo thủy vân. Tiêu chuẩn này không xác định khuôn mẫu quy chuẩn cho công nghệ tạo thủy vân, mặc dù nó hỗ trợ các công cụ không quy chuẩn sử dụng công nghệ tạo thủy vân.

3) Sự kết hợp của hai phương pháp trên.

– *Xác thực nguồn*

Một tập tin JPSEC phải hỗ trợ xác minh danh tính của người dùng / bên mà tạo ra tập tin JPSEC. Nó bao gồm các phương pháp ví dụ như chữ ký số hoặc mã xác thực bản tin (MAC).

– *Truy cập có điều kiện*

Một tập tin JPSEC phải hỗ trợ cơ chế và chính sách để cấp hoặc hạn chế quyền truy cập vào dữ liệu ảnh hoặc các phần của chúng. Điều này cho phép xem ảnh trong chế độ phân giải thấp (xem trước) mà không cần phải xem với độ phân giải cao hơn.

– *Nhận dạng nội dung được đăng ký*

Một tập tin JPSEC có thể được đăng ký tại Cơ quan đăng ký nội dung. Nó hỗ trợ một phương pháp ánh xạ nội dung ảnh/dữ liệu ảnh (đã được công bố) với nội dung ảnh / dữ liệu ảnh đã được đăng ký. Ví dụ một phương pháp như: đọc một bộ định dạng tập tin (Giấy phép) được đặt bên trong siêu dữ liệu, kiểm tra sự phù hợp giữa tấm giấy phép này và các thông tin được tải lên khi quá trình đăng ký đã hoàn thành. Giấy phép có thể chứa đủ thông tin để có thể yêu cầu thông tin từ Cơ quan đăng ký nội dung mà tập tin đã được đăng ký và xác minh rằng tập tin tương ứng với định danh.

– *Chuyển mã bảo mật và tạo dòng phân cấp bảo mật*

Một tập tin JPSEC hoặc chuỗi các gói có thể hỗ trợ các phương pháp sao cho các nút giống và khác nhau có thể thực hiện tạo dòng và chuyển mã mà không cần phải giải mã hoặc không cần bảo vệ nội dung. Ví dụ, trường hợp nội dung JPEG 2000 được bảo vệ được truyền đến một điểm giữa mạng hoặc proxy mà tại đó lần lượt chuyển mã nội dung JPEG 2000 được bảo vệ theo cách giữ bảo mật đầu cuối đến đầu cuối.

5.3 Nhận xét về thiết kế và cài đặt hệ thống JPSEC bảo mật

Tiêu chuẩn này hỗ trợ một tập các dịch vụ bảo mật đầy đủ và mềm dẻo. Ví dụ, phương pháp mã hóa gốc có thể được áp dụng theo nhiều cách khác nhau để đạt được mục tiêu khác nhau, từ mã hóa toàn bộ dòng mã sử dụng JPEG 2000 đến mã hóa chọn lọc chỉ một phần nhỏ của dòng mã. Tuy nhiên, cần cẩn trọng khi thực hiện bất kỳ hệ thống bảo mật nào bao gồm cả hệ thống bảo mật dựa trên JPSEC.

Các nhà thiết kế của bất kỳ hệ thống bảo mật nào cần cẩn thận xem xét các nguyên tắc được khuyến nghị cho các hệ thống bảo mật gốc đang được triển khai. Đối với hầu hết các hệ thống bảo mật gốc sử dụng JPSEC, tiêu chuẩn ISO/IEC liên quan cung cấp chỉ dẫn quan trọng về việc sử dụng chính xác chúng. Ví dụ, để mã hóa bằng cách sử dụng một thuật toán mã khối và một chế độ mã hóa khối liên quan (Bảng 29), hướng dẫn để vận hành và lựa chọn chế độ mật mã khối được đưa ra trong ISO/IEC 10116.

Ngoài ra, trong nhiều ứng dụng bảo mật, xác thực là dịch vụ bảo mật quan trọng nhất. Ngay cả khi tính bảo mật chính là dịch vụ bảo mật đích, thì nó cần được tăng cường bằng cách xác thực để ngăn chặn các hình thức tấn công khác nhau. Cụ thể, trong nhiều ứng dụng tạo ảnh mà mục đích chính là tính bảo mật thì xác thực cần được sử dụng.

Quản lý khóa nằm ngoài phạm vi của JPSEC, tuy nhiên mức độ rủi ro của nó vẫn phải được nhấn mạnh. Hết sức quan trọng trong bất kỳ hệ thống mã hóa nào là quản lý các khóa bí mật mã dung để kiểm soát vận hành. Nếu các khóa bị tổn hại, thì bảo mật của toàn bộ hệ thống bị tổn hại mà sự tổn hại có thể không được phát hiện. Do đó, bắt buộc các khóa được tạo ra, phân phối, lưu trữ và tiêu hủy ở một mức độ bảo mật mà ít nhất là ngang bằng với các dữ liệu mà nó đang bảo vệ. Hơn nữa, do một khóa bị tổn hại tăng theo thời gian, nên các khóa chỉ được sử dụng cho một vòng đời khóa cố định. Để biết thêm thông tin về việc sử dụng và quản lý các khóa bí mật mã, xem ISO / IEC 11770.

Như với tất cả các hệ thống bảo mật, việc sử dụng các hoạt động mật mã phải trong suốt hoàn toàn với người dùng. Nghĩa là, người sử dụng không cần biết các thông tin về các hoạt động mật mã, ngoại trừ đầu ra. Ví dụ, người dùng sẽ không thể truy cập thông tin về lý do tại sao một hoạt động mật mã không thành công để sinh ra một đầu ra. Tương tự như vậy, người dùng sẽ không thể tìm ra bất kỳ thông tin them nào, ngay cả khi họ phải viện đến đo "kênh phụ" như phân tích công suất và/hoặc thời gian. Tóm lại, người dùng sẽ không thể nhận thấy bất kỳ sự khác biệt trong bất kỳ ứng dụng kết quả đầu ra, bất kể những gì mà các ứng dụng đang làm, vì nếu đây không phải là trường hợp rò rỉ thông tin thì cũng có thể dẫn đến khả năng thỏa hiệp bảo mật của hệ thống.

Tóm lại, các nhà thiết kế của bất kỳ hệ thống bảo mật nào bao gồm cả hệ thống dựa trên JPSEC phải chú ý đến các chi tiết của thiết kế hệ thống để đảm bảo một hệ thống bảo mật.

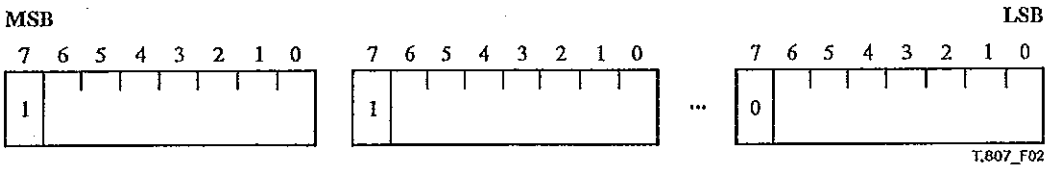
5.4 Đoạn căn chỉnh byte (BAS)

5.4.1 Đoạn căn chỉnh byte

Để cung cấp báo hiệu mở rộng cho các lớp và các chế độ, Tiêu chuẩn này sử dụng một cấu trúc dữ liệu chiều dài biến đổi được gọi là "đoạn căn chỉnh byte" (BAS). Các trường tham số với số các trường

có thể mở rộng được biểu diễn với cấu trúc Field BAS (FBAS). Giá trị tham số có khoảng rộng được biểu diễn với cấu trúc Range BAS (RBAS).

Như minh họa trong hình 2, BAS bao gồm một chuỗi của một hay nhiều byte BAS. Bit có trọng số lớn nhất (MSB) của mỗi byte BAS cho biết sự tồn tại của một byte BAS sau. Cụ thể, nếu MSB = 1 thì tiếp theo là byte BAS, trong khi nếu MSB = 0 thì không tồn tại byte BAS kế tiếp và cấu trúc BAS bị chấm dứt. Các bit có trọng số nhỏ nhất còn lại của mỗi byte BAS được nối để tạo thành một danh sách các bit được sử dụng theo nhiều cách khác nhau cho các tham số BAS khác nhau. Thông thường, chúng được sử dụng kết hợp với một danh sách tham số mà có một số lượng phần tử và mỗi bit BAS được thiết lập bằng 1 hoặc 0 cho thông tin cờ về thành phần tương ứng của nó.Cấu trúc linh hoạt này đã được lựa chọn vì phân cấp của nó đối với phát triển tương lai của tiêu chuẩn, vì nó cho phép các tham số mới được báo hiệu một cách mở rộng.



Hình 2 - Cấu trúc đoạn căn chỉnh byte (BAS)

5.4.2 Đoạn căn chỉnh trường byte (FBAS)

Một FBAS là một loại BAS mà các bit còn lại của byte BAS được sử dụng để thiết lập các trường thành 1 hoặc 0. Một ví dụ của việc sử dụng FBAS là lớp mô tả các vùng ảnh hưởng (DCzoi), nơi có thể đặc tả nhiều mô tả ảnh chẳng hạn như chỉ số khối ảnh, độ phân giải và thành phần màu sắc. Để làm điều này, thì lập cờ với 3 bít BAS tương ứng với khối ảnh, độ phân giải và màu sắc bằng 1.

Ví dụ, nếu muốn biểu diễn một Field BAS có 9 trường, từ f1 tới f9, sẽ cần phải sử dụng nhiều nhất là hai byte BAS. Nếu hai byte này là byte "a" và byte "b", và bit có trọng số lớn nhất của mỗi byte là a0 và b0, thì FBAS sẽ như sau:

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

a0 và b0 là các bit chỉ thị. Trường f1 tới f7 được biểu diễn bởi bit a1 tới a7, trường f8 là bởi bit b1 và trường f9 là bởi bit b2. Các bit còn lại b3 đến b7 được dành riêng và thiết lập bằng 0.

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

Khi được sử dụng trong một dòng JPSEC, FBAS trong ví dụ này có thể được biểu diễn bởi một hoặc hai byte, tùy thuộc vào giá trị thực tế của trường. Điều này xuất phát từ thực tế là giá trị mặc định của các trường là 0. Vì vậy, nếu các trường f8 và f9 không được thiết lập (ví dụ, giá trị của chúng là 0), thì byte thứ hai của BAS là không cần thiết và a0 được thiết lập bằng 0. Mặt khác, nếu trường 8 hoặc trường 9 được thiết lập, thì hai byte là cần thiết. Trong trường hợp này, a0 được thiết lập bằng 1 và b0 được thiết lập bằng 0.

Chú ý rằng các bit trường được "căn chỉnh bên trái" .Điều này cho phép thêm nhiều trường theo thời gian một cách thích hợp.

5.4.3Đoạn căn chỉnh khoảng byte (RBAS)

RBAS được sử dụng để mở rộng khoảng hoặc số lượng các bit được sử dụng để biểu diễn cho một giá trị. Có hai loại RBAS, RBAS-8 và RBAS-16.

Các RBAS-8 chứa một hoặc nhiều byte RBAS gồm các bit của giá trị. Như trong FBAS, bit đầu tiên của mỗi byte biểu thị có byte RBAS tiếp theo không.

Không giống như các FBAS, RBAS là "căn chỉnh bên phải". Vì vậy, nếu một giá trị có 9 bit có nghĩa từ v1 đến v9, trong đó v1 là bit có trọng số lớn nhất, thì nó sẽ được biểu diễn bằng hai byte BAS:

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

như sau:

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

Nếu giá trị nhỏ mà bit v1 và v2 là bằng không, thì biểu diễn hai byte trên có thể được sử dụng với v1 và v2 thiết lập bằng không, hoặc một byte RBAS được sử dụng như sau:

0 v3 v4 v5 v6 v7 v8 v9

Các RBAS-16 có thể được dùng để biểu diễn cho các giá trị mà thường là lớn hơn 7 bit nhưng ít hơn 15 bit. Trong trường hợp này, đoạn RBAS đầu tiên là hai byte mà bit đầu tiên là bit chỉ thị và 15 bit tiếp theo là bit giá trị, sau đó các byte còn lại mở rộng thêm một byte cùng lúc sử dụng cấu trúc BAS điển hình trong đó bit đầu tiên của mỗi byte là bít chỉ thị của byte BAS theo sau.

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

Nếu một giá trị tham số có 22 bit, thì nó có thể được biểu diễn bởi cấu trúc 3 byte RBAS-16 như bên dưới, trong đó a0 và c0 là các bit chỉ thị để xác định xem có hay không một byte BAS theo sau. Mọi byte BAS còn lại là các phân đoạn BAS một byte cơ bản.

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

Vì vậy, các bit chỉ thị sẽ được thiết lập như sau:

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

Đối với cả hai RBAS-8 và RBAS-16, các bit giá trị đều được "căn chỉnh bên phải".

5.5 Mã đánh dấu bảo mật chính (SEC)

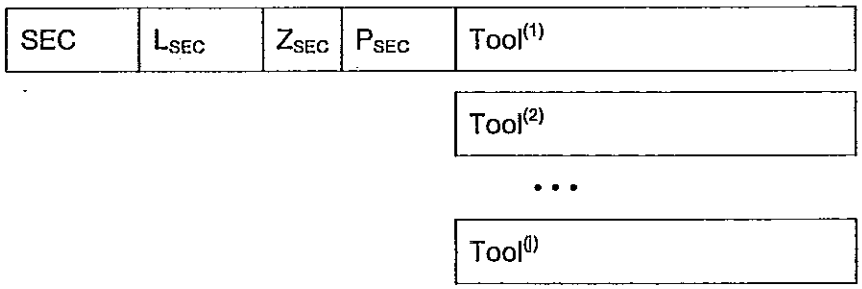
5.5.1 Đoạn mã đánh dấu bảo mật

Trong mục này, chúng ta trình bày một cú pháp đơn giản và linh hoạt nhưng mạnh mẽ cho báo hiệu JPSEC. Đoạn mã đánh dấu SEC được xác định cho mục đích này và được đặt trong mào đầu chính. Cú pháp đoạn mã đánh dấu SEC tính đến mô tả tất cả các thông tin cần thiết để bảo mật ảnh JPEG

2000. Để làm như vậy, cần tham chiếu đến các công cụ quy chuẩn JPSEC được quy định bởi các khuôn mẫu được mô tả trong 5.8 hoặc các công cụ không quy chuẩn JPSEC mà được đăng ký ưu tiên bởi Cơ quan đăng ký JPSEC hoặc theo cách riêng và nó tạo ra các quy định để xử lý các tham số liên quan đến những công cụ này.

Một dòng mã JPSEC có thể được bảo vệ bởi một hoặc nhiều công cụ JPSEC. Mỗi công cụ là một công cụ quy chuẩn JPSEC hoặc công cụ không quy chuẩn JPSEC. Các tham số cho những công cụ này được báo hiệu trong một hoặc nhiều đoạn mã đánh dấu SEC nằm trong mào đầu chính của dòng mã sau đoạn mã đánh dấu SIZ. Khi nhiều đoạn mã đánh dấu SEC được sử dụng, chúng được nối và xuất hiện liên tiếp trong mào đầu chính. Trong hầu hết các trường hợp, tất cả các tham số JPSEC có thể được báo hiệu trong đoạn mã đánh dấu SEC. Tuy nhiên, trong một số trường hợp độ dài của báo hiệu có thể vượt quá kích thước đoạn mã đánh dấu tối đa. Khi điều này xảy ra, các đoạn mã đánh dấu SEC bổ sung có thể được sử dụng để báo hiệu.

Hình 3 cho thấy cú pháp của đoạn mã đánh dấu SEC. Đoạn được báo hiệu bởi mã đánh dấu SEC 0xFF65. L_{SEC} là chiều dài của đoạn mã đánh dấu SEC, bao gồm 2 byte cho LSEC, nhưng không phải là hai byte cho bản thân mã đánh dấu SEC. Z_{SEC} là chỉ số đoạn mã đánh dấu SEC. Z_{SEC} được thiết lập bằng 0 cho đoạn mã đánh dấu đầu tiên xuất hiện trong dòng mã. P_{sec} là một trường tham số mô tả các tham số bảo mật liên quan đến toàn bộ dòng mã và chỉ tồn tại trong đoạn mã đánh dấu SEC đầu tiên, tức là nếu Z_{SEC} = 0. Cú pháp hỗ trợ việc sử dụng một số công cụ JPSEC được báo hiệu trong một hoặc nhiều đoạn mã đánh dấu. Nếu có nhiều hơn một công cụ JPSEC được sử dụng, thì người dùng JPSEC sẽ xử lý các công cụ theo thứ tự mà chúng xuất hiện trong dòng mã.



Hình 3 - Cú pháp đoạn mã đánh dấu bảo mật chính

SEC: mã mã đánh dấu. Bảng 1 cho thấy các kích thước và giá trị của các ký hiệu và các tham số cho đoạn mã đánh dấu bảo mật chính.

L_{SEC}: Chiều dài của đoạn mã đánh dấu tính theo byte (bao gồm cả L_{SEC} nhưng không bao gồm mã đánh dấu).

Z_{SEC}: Chỉ số của đoạn mã đánh dấu này liên quan đến tất cả các đoạn mã đánh dấu SEC khác có mặt trong mào đầu hiện tại. Trường này sử dụng cấu trúc RBAS.

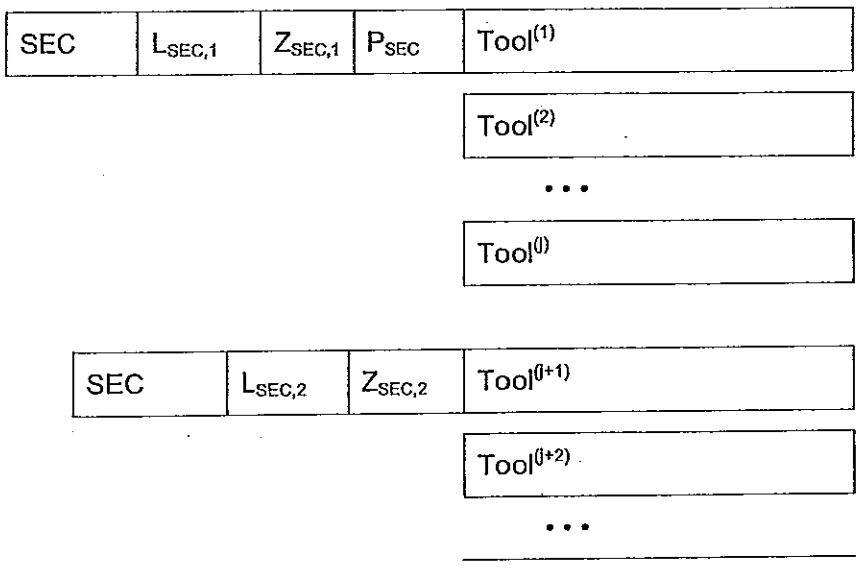
P_{SEC}: trường tham số cho các tham số bảo mật dòng mã. Trường này chỉ xuất hiện trong đoạn mã đánh dấu SEC đầu tiên, tức là khi Z_{SEC} bằng 0.

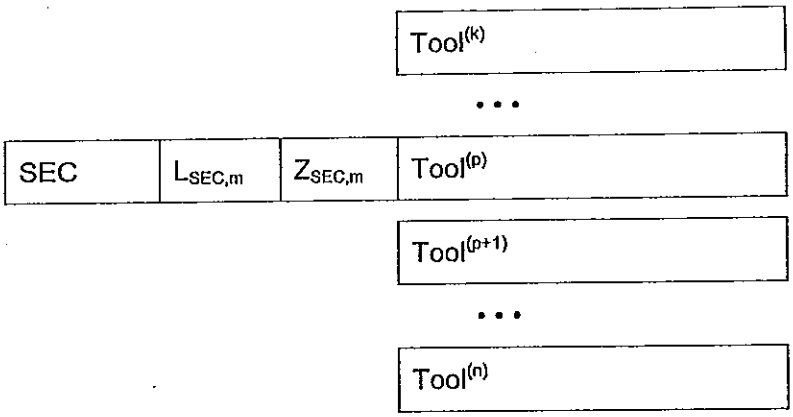
Tool$^{(i)}$: Các tham số cho công cụ JPSEC *i*. Nếu nhiều công cụ JPSEC được báo hiệu thì người sử dụng JPSEC sẽ xử lý mỗi công cụ theo thứ tự xuất hiện trong dòng mã JPSEC.

Bảng 1 - Các giá trị tham số bảo mật chính

Tham số	Kích thước (bit)	Giá trị
SEC	16	0xFF65
L_{SEC}	16	2 ... $(2^{16} - 1)$
Z_{SEC}	8 + 8 * n (RBAS)	0 ... 2^{7+7*n}
P_{SEC}	0, nếu $Z_{SEC} > 0$ Biến đổi, ngược lại	Nếu $Z_{SEC} = 0$, xem bảng 2
Tool$^{(i)}$	Biến đổi	Xem điều 5.6.2 hoặc 5.6.3

Hình 4 cho thấy cú pháp của các tham số bảo mật trong mào đầu chính khi nhiều đoạn mã đánh dấu SEC được sử dụng. Trong trường hợp này, các tham số công cụ JPSEC ở trong các đoạn mã đánh dấu SEC khác nhau. Mỗi đoạn mã đánh dấu bắt đầu với mã đánh dấu SEC 0xFF65 và được theo sau bởi chiều dài và chỉ số của đoạn mã đánh dấu. Chỉ số của các đoạn mã đánh dấu đầu tiên được thiết lập bằng 0 và sẽ tăng thêm một cho mỗi đoạn mã đánh dấu theo thứ tự nó xuất hiện. Chỉ có đoạn mã đánh dấu đầu tiên chứa các tham số bảo mật cho dòng mã, P_{sec}. Tất cả các đoạn mã đánh dấu chứa các tham số cho một hoặc nhiều công cụ JPSEC.

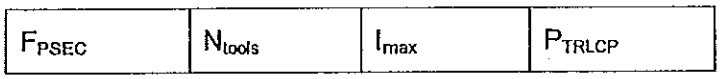




Hình 4 - Cú pháp mã đánh dấu bảo mật chính khi nhiều đoạn mã đánh dấu được sử dụng

Nếu cần thiết, mô tả công cụ JPSEC có thể kéo dài nhiều đoạn mã đánh dấu SEC, ví dụ như điều này có thể xảy ra nếu nó yêu cầu chiều dài vượt quá kích thước mã đánh dấu SEC tối đa. Khi chiều dài của mô tả công cụ được xác định hoàn toàn thì bộ tạo JPSEC chỉ đơn giản là chia tách công cụ trên đoạn mã đánh dấu SEC. Bộ giải mã sau đó sẽ nối tất cả các phân đoạn, trừ mã đánh dấu SEC và các giá trị L_{SEC} và Z_{SEC} và sau đó làm rõ các công cụ phù hợp.

P_{sec} là một trường tham số mô tả các tham số bảo mật cho toàn bộ dòng mã ngược lại với một công cụ đặc thù. Điều này được sử dụng để chỉ ra các sự kiện như tuân thủ JPEG 2000 Phần 1 hoặc sử dụng các mã đánh dấu INSEC. Các tham số P_{sec} được thể hiện trong hình 5.



Hình 5 - Cú pháp các tham số bảo mật dòng mã (P_{SEC})

F_{PSEC}: Cờ để chỉ ra nếu mã đánh dấu đoạn INSEC được sử dụng, nếu nhiều phân đoạn SEC mã đánh dấu được sử dụng, nếu dòng mã dữ liệu JPEG 2000 Phần 1 gốc đã được sửa đổi, và nếu sử dụng thẻ TRLCP được định nghĩa. Cấu trúc FBAS được sử dụng bởi trường này.

N_{tools}: Số các công cụ JPSEC được sử dụng trong dòng mã. Trường này sử dụng cấu trúc RBAS.

I_{max}: Giá trị chỉ số công cụ tối đa được sử dụng trong dòng mã. Trường này sử dụng cấu trúc RBAS.

P_{TRLCP}: Tham số trường để xác định định dạng của thẻ TRLCP. Trường này tồn tại nếu $F_{TRLCP} = 1$.

Bảng 2 - Các tham số bảo mật dòng mã (P_{SEC}) trong đoạn mã đánh dấu SEC đầu tiên

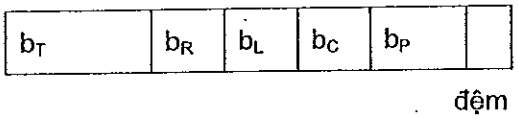
Tham số	Kích thước (bits)	Giá trị
F_{PSEC}	Biến đổi (FBAS)	Xem Bảng 3
N_{tools}	8 + n * 8 (RBAS)	1 ... 2^{7+7*n}
I_{max}	8 + n * 8 (RBAS)	0 ... 2^{7+7*n}
P_{TRLCP}	0, nếu $F_{TRLCP} = 0$ 32, nếu $F_{TRLCP} = 1$	Xem Bảng 4

F_{PSEC} là một cấu trúc FBAS dùng để chỉ số cờ tham số về dòng mã JPSEC. Các trường được biểu diễn bởi F_{PSEC} được thể hiện trong Bảng 3. F_{INSEC} được thiết lập để 1 nếu mã đánh dấu INSEC được sử dụng trong dòng mã JPSEC. $F_{multiSEC}$ được thiết lập bằng 1 nếu có nhiều đoạn mã đánh dấu SEC được sử dụng trong dòng mã JPSEC. F_{mod} được thiết lập bằng 1 nếu dữ liệu JPEG 2000 ban đầu đã bị thay đổi trong dòng mã JPSEC. CHÚ THÍCH rằng nếu các mã đánh dấu INSEC được sử dụng, thì các dữ liệu JPEG 2000 ban đầu được sửa đổi và do đó F_{INSEC}, f_{mod} được thiết lập bằng 1. F_{TRLCP} được thiết lập bằng 1 nếu sử dụng thẻ TRLCP được định nghĩa trong P_{sec}. Nếu nó được định nghĩa, thì mô tả thẻ TRLCP, P_{TRLCP}, được quy định trong trường tham số P_{sec}. Việc sử dụng thẻ TRLCP phải được xác định nếu bất kỳ công cụ trong dòng mã JPSEC sử dụng các thẻ TRLCP.

Bảng 3 - Ý nghĩa của các giá trị F_{PSEC} (FBAS)

BAS field	Số lượng bit BAS	Giá trị (bit)	Ý nghĩa
F_{INSEC}	1	0	INSEC không được sử dụng
		1	INSEC được sử dụng
$F_{multiSEC}$	2	0	1 đoạn mã đánh dấu SEC được sử dụng
		1	Nhiều đoạn mã đánh dấu SEC được sử dụng
F_{mod}	3	1	Dữ liệu JPEG 2000 gốc đã bị thay đổi
		0	Các trường hợp khác
F_{TRLCP}	4	0	Việc sử dụng thẻ TRLCP không được định nghĩa trong P_{SEC}
		1	Việc sử dụng thẻ TRLCP được định nghĩa trong P_{SEC}

JPSEC định nghĩa một cấu trúc gọi là thẻ TRLCP mà có thể được sử dụng để nhận dạng một gói tin JPEG 2000. Một gói tin JPEG 2000 có thể được xác định duy nhất bởi chỉ số khối ảnh, chỉ số mức độ phân giải, số lớp, chỉ số thành phần, và chỉ số phân khu ảnh của nó. Một thẻ TRLCP được định nghĩa là một đơn vị dữ liệu với một số cố định của các bit được sử dụng để đặc tả mỗi giá trị chỉ số này. Số bit cho mỗi chỉ số được thiết lập trong P_{sec}. P_{TRLCP} là một trường tham số mô tả các định dạng của thẻ TRLCP vì nó được sử dụng trong các công cụ JPSEC. Trường này chỉ tồn tại nếu $F_{TRLCP} = 1$. P_{TRLCP} bao gồm các biến sau trong hình 6.



Hình 6 - Cấu trúc bộ mô tả thẻ TRLCP (P_{TRLCP})

b_T: Số lượng các bit biểu diễn chỉ số khối ảnh là $b_T + 1$ trong thẻ TRLCP.

b_R: Số lượng các bit biểu diễn cho chỉ số mức phân giải là $b_R + 1$ trong thẻ TRLCP.

b_L: Số lượng các bit biểu diễn cho chỉ số lớp là $b_L + 1$ trong thẻ TRLCP.

b_C: Số lượng các bit biểu diễn cho chỉ số thành phần là $b_C + 1$ trong thẻ TRLCP.

b_P: Số lượng các bit biểu diễn cho chỉ số phân khu ảnh là $b_P + 1$ trong thẻ TRLCP.

Bảng 4 - Trường tham số cho bộ mô tả thẻ TRLCP (P_{TRLCP})

Tham số	Kích thước (bit)	Giá trị
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 ... $(2^8 - 1)$
đệm	2	0

Kích thước của mỗi thẻ TRLCP là kích thước byte số nguyên nhỏ nhất có chứa tất cả các bit. Các định dạng của thẻ TRLCP chứa các bit cho các chỉ số khối ảnh, chỉ số mức độ phân giải, chỉ số lớp, các chỉ số thành phần, và chỉ số phân khu ảnh theo thứ tự. Nếu các bit thêm cần điền vào yêu cầu kích thước byte số nguyên, thì thẻ TRLCP sẽ được đặt trong bit có trọng số nhỏ nhất có thể, và các bit thêm được thiết lập bằng 0. CHÚ THÍCH rằng các bit thêm sẽ là MSB của thẻ TRLCP nếu chúng tồn tại.

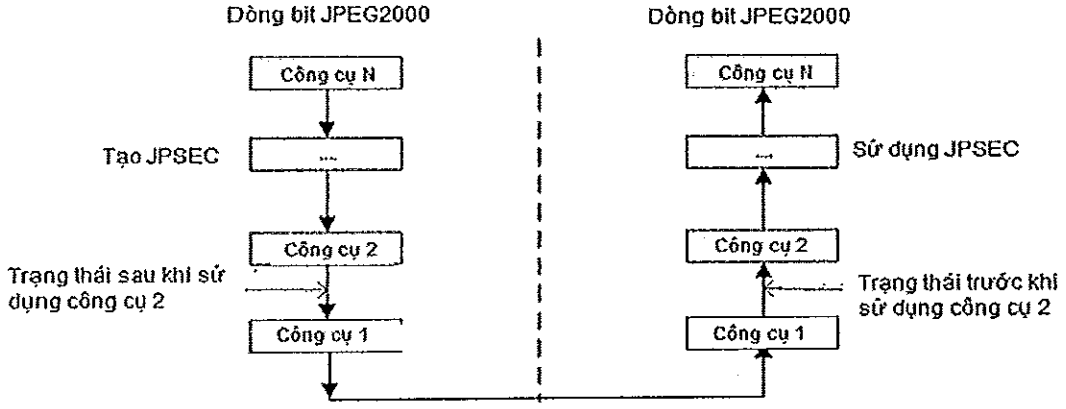
5.5.2 Ứng dụng của các công cụ JPSEC

Trong nhiều ứng dụng cần thiết phải áp dụng nhiều công cụ JPSEC cho một dòng mã JPEG 2000. Ví dụ, cả mã hóa và xác thực có thể được áp dụng để bảo vệ một ảnh JPEG 2000. Tình hình chung của việc áp dụng nhiều công cụ JPSEC được minh họa trong Hình 3, 4 và 7, trong đó N công cụ được áp dụng. Người dùng JPSEC sẽ đọc N công cụ theo thứ tự đặt trong đoạn mã đánh dấu SEC thể hiện trong hình 3 hoặc hình 4, và áp dụng chúng theo cùng thứ tự để thực hiện việc tiêu thụ JPSEC của dòng mã JPSEC. CHÚ THÍCH rằng trong khi người sử dụng JPSEC áp dụng các công cụ JPSEC theo thứ tự 1, 2, ..., N, được đọc từ các điểm mã đánh dấu đoạn SEC, trong quá trình tạo ra các JPSEC dòng mã những công cụ JPSEC đã được áp dụng theo thứ tự ngược lại, tức là, N, N - 1, 2,1 ..., như

minh họa trong hình 7. CHÚ THÍCH rằng số của các công cụ trong hình đã được lựa chọn để làm nổi bật rằng người sử dụng JPSEC áp dụng các công cụ JPSEC theo thứ tự ngược lại từ bộ tạo JPSEC. Tuy nhiên, số lượng các công cụ JPSEC bất kỳ được chấp nhận, miễn là mỗi công cụ JPSEC trong một dòng mã JPSEC có một mã số duy nhất cho mục đích nhận dạng.

Nói chung, các công cụ JPSEC được tạo ra và tiêu thụ theo thứ tự ngược nhau. Ví dụ, nếu bộ tạo JPSEC áp dụng N công cụ JPSEC, thì người sử dụng JPSEC thường áp dụng N công cụ JPSEC tương tự nhưng theo thứ tự ngược lại. Việc tiêu thụ JPSEC chính xác của nhiều công cụ JPSEC được đảm bảo bởi tiêu thụ liên tục N các công cụ theo thứ tự chính xác và bởi yêu cầu bất kỳ giai đoạn trung gian phía người sử dụng để phù hợp với trạng thái tương ứng tại bộ tạo. Ví dụ, trong hình 7, các trạng thái phía người sử dụng sau khi tiêu thụ JPSEC của công cụ 1 phải bằng với trạng thái sau khi áp dụng công cụ 2 trong quá trình tạo JPSEC. Một ví dụ cụ thể của trạng thái, các dãy byte nên thống nhất, do đó bất kỳ byte thêm nào khi áp dụng công cụ 1 cần phải loại bỏ khi loại bỏ công cụ 1 tại người sử dụng JPSEC.

Trong các ứng dụng nhất định, một người sử dụng JPSEC được mong muốn tiêu thụ nhiều công cụ JPSEC theo một cách khác với mô tả ở trên. Ví dụ, người sử dụng JPSEC có thể chọn tiêu thụ nhiều công cụ theo một thứ tự khác nhau, hoặc bỏ qua các công cụ nhất định trong việc tiêu thụ. Hơn nữa, người sử dụng JPSEC có thể thích áp dụng các công cụ JPSEC nhất định, mà không loại bỏ chúng, ví dụ, để kiểm tra chữ ký số nhưng không loại bỏ nó. Cần xem xét cẩn thận những trường hợp này để đảm bảo rằng việc xử lý không đúng trật tự hoặc bỏ qua không dẫn đến hậu quả không chính xác hoặc không mong muốn. Hành vi này không được khuyến khích trừ khi ứng dụng JPSEC hoàn toàn nhận thức được hậu quả tiềm tàng.



Hình 7 - Sử dụng các công cụ JPSEC

5.6 Các công cụ JPSEC

5.6.1 Cú pháp công cụ JPSEC

Như đã đề cập ở trên, có hai loại công cụ JPSEC. Công cụ quy chuẩn JPSEC được chỉ định với các phương pháp bảo vệ các mẫu mô tả trong 5.8 và cũng được biết đến như là công cụ quy chuẩn JPSEC. Các công cụ không quy chuẩn JPSEC được quy định bởi một Cơ quan đăng ký JPSEC hoặc

một ứng dụng JPSEC cụ thể dựa trên số ID của chúng và tương ứng được gọi là cơ quan đăng ký công cụ JPSEC hoặc các công cụ JPSEC do người dùng định nghĩa. Cú pháp cho các công cụ quy chuẩn JPSEC được thảo luận trong 5.6.2. Cú pháp công cụ không quy chuẩn JPSEC được thảo luận trong 5.6.3.

Cú pháp các công cụ JPSEC được thể hiện trong hình 8. Cú pháp cụ JPSEC có ba phần chính, mô tả:

1) Công cụ gì được áp dụng với nhận dạng của nó;

2) Công cụ này được áp dụng ở đâu với một cấu trúc vùng ảnh hưởng ; và

3) Công cụ này được áp dụng với một trường nhiều tham số chi tiết hơn như thế nào.

Ví dụ, sử dụng cú pháp này, một cú pháp công cụ JPSEC xác định rằng một công cụ giải mã phải sử dụng (cái gì) trên các thành phần có độ phân giải thấp nhất nằm trong một khoảng byte đặc biệt (ở đâu) sử dụng giải mã AES trong chế độ CBC với một tập các khóa và vectơ khởi tạo được quy định (như thế nào).

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

Hình 8 - Cú pháp công cụ JPSEC (Tool$^{(i)}$)

t: Loại công cụ. Giá trị 0 cho bit BAS đầu tiên chỉ ra công cụ quy chuẩn JPSEC. Giá trị 1 cho bit BAS đầu tiên thuộc công cụ không quy chuẩn JPSEC. Trường này sử dụng cấu trúc FBAS.

i: Chỉ số mẫu công cụ (có thể được sử dụng như một định danh duy nhất). Trường này sử dụng cấu trúc RBAS..

ID: Giá trị định danh cho công cụ JPSEC *i*. Đối với công cụ quy chuẩn JPSEC, ID = ID_T có 8 bit và xác định loại khuôn mẫu. Đối với Công cụ không quy chuẩn JPSEC, ID = ID_{RA} được xác định bởi hình 10 và Bảng 8.

L_{ZOI}: Chiều dài của ZOI theo Byte (không bao gồm LZOI). Trường này sử dụng cấu trúc RBAS.

ZOI: Vùng ảnh hưởng cho công cụ JPSEC *i*

L_{PID}: Chiều dài P_{ID} theo Byte (không bao gồm L_{PID}). Trường này sử dụng cấu trúc RBAS..

P_{ID}: Các tham số cho công cụ JPSEC *i*

Bảng 5 - Các giá trị tham số công cụ JPSEC

Tham số	Kích thước (bit)	Giá trị
t	8+8*n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8+8*n (RBAS)	0 ... $(2^{7+7*n}-2)$

		$(2^{7+7*n} - 1)$, dự trữ.
ID	8, Nếu t=0 Biến đổi, nếu t=1	Xem bảng 6 Xem Hình 10 và bảng 8
L_{ZOI}	16+8*n (RBAS)	$0 ... 2^{15+7*n}$
ZOI	Biến đổi	Xem 5.7
L_{PID}	16+8*n (RBAS)	$0 ... 2^{15+7*n}$
P_{ID}	Biến đổi	Bảng 7, nếu t=0 Được quản lý bởi Cơ quan đăng ký JPSEC nếu t=1

Mỗi công cụ JPSEC có cú pháp như sau. Một byte đầu tiên xác định nếu công cụ này là công cụ quy chuẩn JPSEC hoặc công cụ không quy chuẩn JPSEC và gán một định danh cho công cụ này. Tiếp theo là ID định danh công cụ. Tiếp theo là L_{ZOI}, cho biết chiều dài của vùng tiếp theo của trường ảnh hưởng ZOI và các vùng ảnh hưởng riêng của nó, mà mô tả nơi công cụ JPSEC được áp dụng trong dòng dữ liệu. Tiếp theo là L_{PID}, cho biết chiều dài của trường tham số sau P_{ID}, đó là một trường để truyền một hoặc nhiều tham số cho các công cụ JPSEC.

Các byte đầu tiên của công cụ này sử dụng cấu trúc FBAS một byte mà bit BAS đầu tiên biểu thị loại công cụ t, bằng 0 để chỉ định một công cụ quy chuẩn JPSEC và 1 để chỉ một công cụ không quy chuẩn JPSEC. Tiếp theo là chỉ số mẫu i, được biểu diễn bằng cách sử dụng cấu trúc RBAS. Chỉ số mẫu là một định danh duy nhất của công cụ trong dòng mã, do đó sẽ không được lặp lại bởi bất kỳ công cụ khác trong dòng mã, ngay cả khi nó ở một đoạn mã đánh dấu SEC khác. Chỉ số mẫu là đặc biệt quan trọng (và cần thiết) khi mã đánh dấu INSEC được sử dụng, vì mỗi đoạn mã đánh dấu INSEC chứa chỉ số mẫu của công cụ mà nó áp dụng. Khuyến nghị công cụ đầu tiên được áp dụng tại bộ tạo JPSEC có một chỉ số mẫu bằng 1, và mỗi công cụ bổ sung được đánh chỉ số tuần tự khi nó được áp dụng tại bộ bảo vệ.

Ngoài ra, mỗi công cụ JPSEC có một số ID 8 bit cho các công cụ quy chuẩn JPSEC và 32 bit cho Công cụ không quy chuẩn JPSEC. Đối với công cụ quy chuẩn JPSEC, số ID mô tả khuôn mẫu Khuôn mẫu phương pháp bảo vệ được sử dụng, ví dụ, nó xác định khuôn khuôn mẫu giải mã, xác thực mẫu, hoặc hàm băm. Đối với Công cụ không quy chuẩn JPSEC, bit đầu tiên cho biết đó là một công cụ Cơ quan đăng ký JPSEC hay một công cụ được định nghĩa bởi người dùng JPSEC. Trong mỗi trường hợp, số ID cho biết công cụ cụ thể. Một Cơ quan đăng ký JPSEC có thể đảm bảo rằng số ID hợp lệ là duy nhất. Tuy nhiên, một ứng dụng JPSEC mà sử dụng số ID được định nghĩa bởi người dùng có nguy cơ lựa chọn một số ID đã được sử dụng bởi một ứng dụng JPSEC khác , vì thế việc sử dụng phải thận trọng.

Khi mỗi công cụ JPSEC được áp dụng ở bộ tạo JPSEC, trường tham số P_{SEC} thể hiện trong Bảng 2 sẽ được cập nhật. Ví dụ, trường tham số P_{SEC} chứa tham số I_{max} mà xác định chỉ số mẫu tối đa sử dụng cho các công cụ trong dòng mã JPSEC. Khi một công cụ mới được áp dụng, nó phải được ấn định một chỉ số mẫu duy nhất. Bộ bảo vệ JPSEC tham khảo tham số I_{max} được đưa ra trong trường tham số P_{SEC} để xác định chỉ số mẫu để gán cho một công cụ JPSEC, ví dụ, nó có thể chọn một giá trị là một trong những giá trị lớn hơn giá trị I_{max} hiện tại, và sau đó nó phải tăng giá trị của I_{max} lên 1.

5.6.2 Công cụ quy chuẩn JPSEC

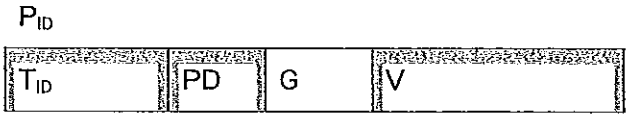
Công cụ quy chuẩn JPSEC sử dụng cú pháp công cụ JPSEC mô tả trong 5.6.1 và thể hiện trong hình 8, trong đó loại công cụ t = 0 và kích thước của ID là 8 bit. Công cụ quy chuẩn JPSEC dựa trên các khuôn mẫu phương pháp bảo vệ mô tả trong 5.8. Có ba loại khuôn mẫu Khuôn mẫu phương pháp bảo vệ ; loại được sử dụng bởi công cụ được đặc tả bởi định danh công cụ ID = ID_T sử dụng các giá trị thể hiện trong Bảng 6.

Bảng 6 - Các giá trị ID khuôn mẫu của công cụ quy chuẩn JPSEC (ID_T)

Giá trị	Khuôn mẫu phương pháp bảo vệ
0	Dự trữ
1	Khuôn khuôn mẫu giải mã
2	Khuôn mẫu xác thực
3	Khuôn mẫu hàm băm
4	Công cụ NULL
	Các giá trị khác được dự trữ cho việc sử dụng ISO

Trong trường hợp của các công cụ quy chuẩn JPSEC, trường tham số P_{ID} có cấu trúc thể hiện trong Hình 9. P_{ID} bao gồm bốn trường chính: khuôn mẫu Khuôn mẫu phương pháp bảo vệ T, miền xử lý PD, độ chi tiết G và danh sách giá trị V của nó -. Cú pháp cho từng trường được đưa ra tương ứng trong 5.8, 5.9, 5.10 và 5.11. Các trường này cùng mô tả cách công cụ được áp dụng. Khuôn mẫu phương pháp bảo vệ T mô tả các phương pháp bảo vệ đặc biệt cho khuôn khuôn mẫu giải mã, khuôn mẫu xác thực, hoặc khuôn khuôn mẫu hàm băm theo quy định của ID công cụ quy chuẩn . Nó cũng có thể đặc tả công cụ NULL, trong trường hợp này không có khuôn mẫu nào được sử dụng, nhưng các chức năng khác vẫn có thể được sử dụng. Ví dụ, các vùng ảnh hưởng có thể được chỉ định để đại diện cho các vùng ảnh và phạm vi byte tương ứng của chúng. Miền xử lý PD mô tả các trường mà các phương pháp bảo vệ được áp dụng. Độ chi tiết G mô tả các độ chi tiết mà các phương pháp bảo vệ được áp dụng. Danh sách giá trị V chứa một danh sách các giá trị cần thiết bởi mỗi phương pháp bảo vệ với độ chi tiết mịn hơn. Đối với khuôn mẫu giải mã, danh sách giá trị có thể được dùng để xác định một tập các giá trị khởi tạo mịn hơn được sử dụng. Đối với khuôn mẫu xác thực, danh sách giá trị bao gồm một tập hợp các giá trị MAC hoặc chữ ký số. Đối với các khuôn mẫu hàm băm, danh sách giá trị bao gồm

một tập các giá trị băm. Trong mọi trường hợp, danh sách giá trị có chứa độ chi tiết của các giá trị theo quy định của trường độ chi tiết G.



Hình 9 - Cú pháp các tham số (P_{ID}) cho các công cụ quy chuẩn JPSEC (t=0)

T_{ID}: Tham số khuôn mẫu công cụ quy chuẩn JPSEC với bộ định dạng khuôn mẫu ID_T.

PD: Miền xử lý miền cho công cụ quy chuẩn JPSEC.

G: Độ chi tiết cho công cụ quy chuẩn JPSEC.

V: Danh sách giá trị của các công cụ quy chuẩn JPSEC, ví dụ như, vectơ khởi tạo, giá trị MAC, chữ ký số, hoặc các giá trị hàm băm tùy thuộc vào mẫu ID.

CHÚ THÍCH rằng các tham số khuôn mẫu phụ thuộc vào ID khuôn mẫu. Tuy nhiên, trường xử lý, độ chi tiết, và danh sách giá trị không phụ thuộc vào ID khuôn mẫu.

Bảng 7 - Các giá trị tham số công cụ quy chuẩn JPSEC

Tham số	Kích thước (bits)	Giá trị
T_{ID}	0, Nếu $ID_T = 4$ Biến đổi, các trường hợp khác	N/A Xem 5.8
PD	Biến đổi	Xem 5.9
G	24	Xem 5.10
V	Biến đổi	Xem 5.11

5.6.3 Công cụ không quy chuẩn JPSEC

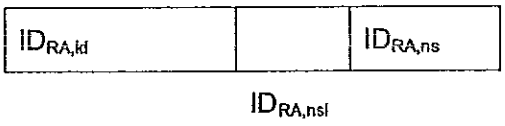
Trong một số trường hợp, có thể hữu ích cho một ứng dụng JPSEC có khả năng áp dụng một công cụ mở rộng ra ngoài các công cụ quy chuẩn JPSEC. Khả năng này được hỗ trợ bằng cách sử dụng một công cụ không quy chuẩn JPSEC. Điều này cho phép một người sử dụng nhiều yếu tố của công cụ quy chuẩn JPSEC, bao gồm cả ZOI và mẫu JPSEC, nhưng cho biết thêm tính linh hoạt của việc sử dụng các tham số một cách khác nhau liên kết với một công cụ giá trị ID. Các công cụ không quy chuẩn JPSEC sử dụng cú pháp JPSEC công cụ mô tả trong 5.6.1 và thể hiện trong hình 8, nơi mà các loại công cụ t = 1 và định danh IDRA bao gồm một không gian tên và số ID, theo định nghĩa của hình 10 và Bảng 8.

Có hai loại công cụ không quy chuẩn JPSEC:

1) Các công cụ Cơ quan đăng ký JPSEC: công cụ không quy chuẩn JPSEC có tín hiệu được xác định với một cơ quan đăng ký.

2) Các công cụ JPSEC do người dùng định nghĩa các công cụ: công cụ không quy chuẩn JPSEC có tín hiệu được xác định bởi một ứng dụng JPSEC.

Hai loại công cụ không quy chuẩn JPSEC được báo hiệu bằng cách sử dụng 32-bit IDRA, định danh id thể hiện trong Bảng 9, nơi mà các định danh mà bit đầu tiên là 0 được xác định bởi một cơ quan đăng ký, và những định danh có bit đầu tiên là 1 là xác định bởi một ứng dụng JPSEC cụ thể.



Hình 10 - Cú pháp ID_{RA}

$ID_{RA,id}$: Công cụ định danh cho công cụ RA và công cụ người dùng định nghĩa

$ID_{RA,nsl}$: Chiều dài của trường $ID_{RA,ns}$ theo bytes. Trường này sử dụng RBAS .

$ID_{RA,ns}$: Một chuỗi có chứa các không gian tên của công cụ RA quy định hoặc công cụ người dùng định nghĩa

Bảng 8 - Giá trị các tham số trong cú pháp ID_{RA}

Tham số	Kích thước (bits)	Giá trị
$ID_{RA,id}$	32	Xem Bảng 9
$ID_{RA,nsl}$	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
$ID_{RA,ns}$	Biến đổi	1 chuỗi chứa namespace

Bảng 9 - Giá trị ID cho các công cụ không quy chuẩn JPSEC ($ID_{RA,id}$)

$ID_{RA,id}$	Ý nghĩa
0x00 00 00 00 ... 0x7F FF FF FF	Công cụ xác thực đăng ký JPSEC. Các giá trị được quản lý bởi các cơ quan đã đăng ký JPSEC.
0x80 00 00 00 ... 0xEF FF FF FF	Công cụ JPSEC do người dung định nghĩa. Các giá trị có thể được định nghĩa bởi 1 ứng dụng JPSEC cụ thể.
0xF0 00 00 00 ... 0xFF FF FF FF	Dự trữ cho mục đích sử dụng ISO.

Đối với các công cụ RA, trường $ID_{RA,ns}$ là không gian tên của Cơ quan đăng ký (RA) mà công cụ này đã được đăng ký. Mỗi RA có một không gian tên duy nhất, các IDRA, id và $ID_{RA,ns}$ được sử dụng với nhau để xác định một công cụ RA. Đối với các công cụ người dùng định nghĩa, trường $ID_{RA,ns}$ được lựa chọn bởi các nhà phát triển. Để hạn chế nguy cơ xung đột ID, khuyến cáo rằng các nhà phát triển tìm kiếm sự duy nhất khi lựa chọn không gian tên của chúng, ví dụ, bằng cách chọn miền của tổ chức, công ty. Tuy nhiên, với các công cụ cho người dùng định nghĩa, không có cách nào để đảm bảo tính độc đáo của không gian tên, do đó ID xung đột có thể xảy ra và cần được xem xét cẩn thận khi sử dụng các công cụ người dùng định nghĩa.

Các trường P_{ID} được sử dụng để truyền tải một hoặc nhiều tham số cho các công cụ không quy chuẩn JPSEC *i*. Định dạng của trường P_{ID} không được đưa ra hoàn toàn trong phạm vi JPSEC. Nếu một cơ quan đăng ký được sử dụng, thì định dạng được đăng ký với cơ quan đăng ký cùng với các ID. Nếu cơ quan đăng ký không được sử dụng và công cụ này là người dùng định nghĩa, thì chỉ độ dài của trường này được xác định, sẽ cho người sử dụng một cách thích hợp để sử dụng trường này.

Tuy nhiên, JPSEC không cho phép các cấu trúc cú pháp quy định cho các công cụ quy chuẩn JPSEC được sử dụng trong các trường P_{ID} cho các công cụ không quy chuẩn JPSEC. Ví dụ, một công cụ không quy chuẩn JPSEC có thể sử dụng các trường Khuôn mẫu phương pháp bảo vệ , xử lý miền, độ chi tiết, và danh sách giá trị được mô tả tương ứng trong 5.8, 5.9, 5.10 và 5.11.

Cú pháp này rất linh hoạt và có thể chứa một loạt các kỹ thuật bảo mật, toàn vẹn dữ liệu ảnh, kiểm soát truy cập và phương pháp bảo vệ bản quyền. Do đó, nó cung cấp một tập đầy đủ các chức năng trong khi vẫn đơn giản và ngắn gọn.

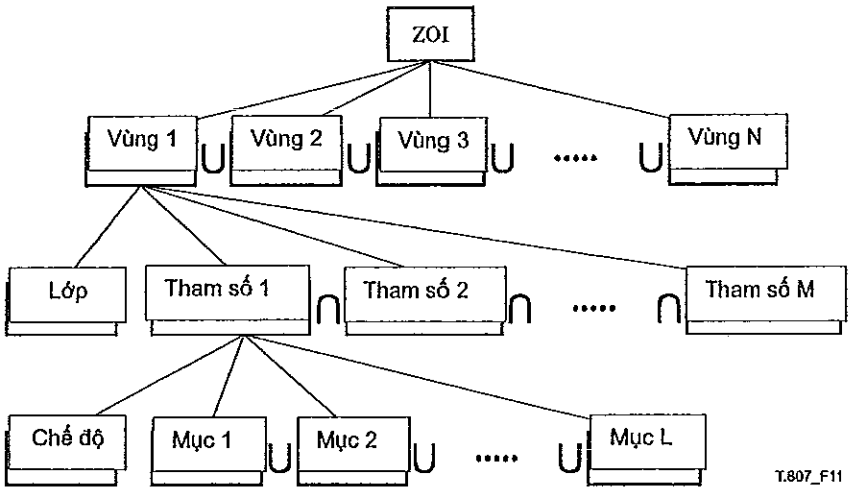
5.7 Cú pháp vùng ảnh hưởng (ZOI)

5.7.1 Giới thiệu

Vùng ảnh hưởng (ZOI) có thể được sử dụng để mô tả vùng phủ của một công cụ JPSEC. Các dữ liệu trong vùng phủ (đặc tả bởi ZOI) được xem như là dữ liệu bị ảnh hưởng. Công cụ quy chuẩn JPSEC sử dụng ZOI để mô tả vùng phủ của chúng. Công cụ không quy chuẩn JPSEC sử dụng ZOI để mô tả vùng phủ của chúng hoặc có thể sử dụng một phương pháp khác. Nếu phương pháp khác được sử dụng, thì chiều dài ZOI là 0, có nghĩa là nó không tồn tại.

Vùng ảnh hưởng (ZOI) mô tả vùng phủ của mỗi công cụ JPSEC. Vùng phủ này có thể được mô tả bởi các tham số liên quan đến ảnh, ví dụ như vùng ảnh hoặc độ phân giải; hoặc tham số không liên quan đến ảnh, ví dụ như các đoạn dòng mã hoặc chỉ số gói. Trong trường hợp các tham số liên quan đến ảnh và các tham số không liên quan đến ảnh được sử dụng cùng nhau, ZOI mô tả sự tương ứng giữa các vùng này. Ví dụ, ZOI được sử dụng để chỉ ra rằng độ phân giải và vùng ảnh đặc tả bởi các tham số liên quan đến ảnh tương ứng với đoạn dòng mã được đặc tả bởi các tham số không liên quan đến ảnh. Điều này cho phép ZOI được sử dụng như siêu dữ liệu mà các tín hiệu nơi một số phần của ảnh được đặt trong dòng mã JPSEC.

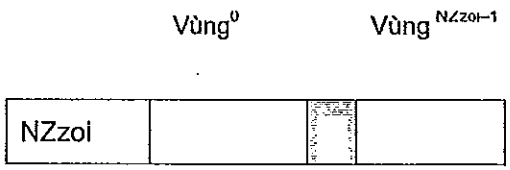
Hình 11 mô tả cấu trúc khái niệm của ZOI. Các ZOI chứa một hoặc nhiều vùng. Khi nhiều vùng được sử dụng trong một ZOI duy nhất, ZOI được xác định bởi sự kết hợp của chúng. Điều này cho thấy các công cụ JPSEC nên được áp dụng cho tất cả các vùng. Mỗi vùng trong một ZOI được mô tả bởi ba đơn vị cơ bản: lớp mô tả, chế độ tham số và các mục tham số (giá trị). Tiêu chuẩn này định nghĩa hai lớp mô tả: lớp mô tả liên quan đến ảnh và lớp mô tả không liên quan đến ảnh. Các tham số này có thể được xác định bằng cách sử dụng một số chế độ, ví dụ, bởi một giá trị duy nhất, nhiều giá trị được liệt kê hoặc bởi một khoảng. Các mục hoặc giá trị tham số sau đó được liệt kê cùng với chế độ.



Hình 11 - Cấu trúc khái niệm vùng ảnh hưởng

5.7.2 Cú pháp ZOI

Hình 12 cho thấy cú pháp ZOI. ZOI có thể chứa một hoặc nhiều vùng. Nó cũng có thể trống, trong trường hợp này NZ_{zoi} là 0. Khi điều này xảy ra, ảnh hưởng của công cụ được xác định bằng các phương tiện khác, chẳng hạn như mã đánh dấu INSEC hoặc các tham số xác định bởi một công cụ bảo vệ không quy chuẩn JPSEC.



Hình 12 - Cú pháp ZOI

NZzoi: Số lượng vùng. Trường này sử dụng cấu trúc RBAS.

Zone^{k}: Vùng. Cấu trúc của nó được mô tả cụ thể trong 5.7.3.

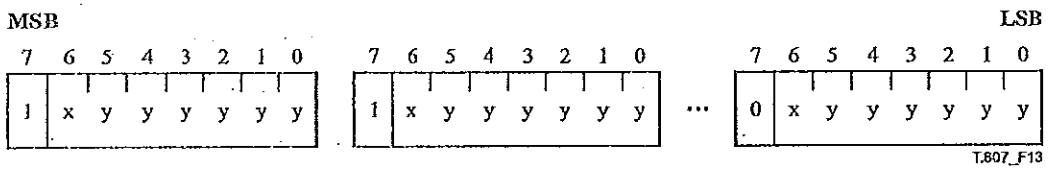
Bảng 10 - Giá trị tham số của trường vùng ảnh hưởng (ZOI)

Tham số	Kích thước (bit)	Giá trị
NZzoi	8 + 8 * n (RBAS)	0...(2^{7+7*n} – 2)

		$(2^{7+7^n} - 2)$, Dự trữ
Vùng^k	Biến đổi	Xem 5.7.3

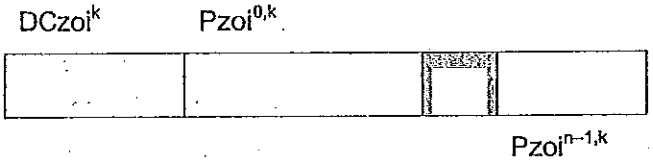
5.7.3 Cú pháp vùng

Vùng chứa một bộ chỉ thị trường lớp mô tả vùng theo các tham số của lớp đó. Lớp mô tả vùng sử dụng cấu trúc FBAS. Như trong hình 13, bit có trọng số lớn thứ hai trong mỗi byte, gắn nhãn "x", đánh dấu bằng cờ việc sử dụng một lớp mô tả cụ thể. Tiêu chuẩn này định nghĩa hai lớp mô tả: lớp mô tả liên quan đến ảnh và lớp mô tả không liên quan ảnh (xem Bảng 12). Bảng13 và 14 xác định số bộ chỉ thị trường tương ứng cho lớp mô tả liên quan đến ảnh và lớp mô tả không liên quan ảnh. Nối kết của sáu bit gắn nhãn "y", trong mỗi byte theo cờ lớp mô tả, cho biết việc sử dụng mô tả cụ thể trong lớp mô tả cho trước. Giá trị bit "1" tại số bit trong mỗi lớp chỉ ra rằng trường tham số tương ứng tồn tại. Số lượng các tham số giống với số lượng bộ chỉ thị trường lớp mô tả vùng thiết lập bằng "1" và xuất hiện theo thứ tự mà chỉ số trường lớp được báo hiệu. Lớp mô tả vùng có số các byte thay đổi; khi MSB bằng 1, thì có byte lớp mô tả khác tiếp theo. MSB của byte mô tả lớp byte cuối cùng bằng 0. Nếu cả lớp mô tả liên quan đến ảnh và lớp mô tả không liên quan ảnh đều được sử dụng, thì các byte lớp mô tả liên quan đến ảnh sẽ đứng trước byte lớp mô tả không liên quan ảnh. Khi số các mục được biểu diễn sử dụng cấu trúc này, thì mục đầu tiên trong danh sách sẽ tương ứng với các bit có trọng số lớn nhất khả dụng của byte đầu tiên.



Hình 13 - Cấu trúc lớp mô tả vùng (DCzoi)

Hình 14 thể hiện cú pháp vùng.



Hình 14 - Cú pháp vùng bao gồm lớp mô tả và 1 hoặc nhiều tập tham số

DCzoi^k:lớp mô tả vùng thứ k. Trường này sử dụng cấu trúc FBAS.

Pzoi^{i,k}: Tham số phân vùng tương ứng lớp mô tả vùng được đặc tả (DCzoi^k). Xem 5.7.6.

DCzoi^k xác định số n của các trường lớp mô tả vùng đang tồn tại, dựa trên số lượng các bit được thiết lập bằng một. Đối với mỗi trường lớp mô tả vùng, có tồn tại một trường tham số vùng Pzoi^{i,k}. Các trường này xuất hiện tuần tự theo thứ tự giống với các cờ xuất hiện trong DCzoi^k.

Bảng 11 - Giá trị tham số vùng

Tham số	Kích thước (bit)	Giá trị
$DCzoi^{k}$	Biến đổi (FBAS)	Biến đổi tùy theo tập giá trị của Bảng 12
$Pzoi^{l,k}$	Biến đổi	Xem 5.7.6 về cú pháp của trường này

Bảng 12 - Giá trị bộ chỉ thị lớp mô tả

Giá trị	Lớp mô tả
0	Lớp mô tả liên quan ảnh. Số các bit theo sau được định nghĩa trong Bảng 13
1	Lớp mô tả không liên quan ảnh. Số các bit theo sau được định nghĩa trong Bảng 14

Bảng 13 - Lớp mô tả liên quan ảnh

Số bít	Ngữ nghĩa
1	Miền ảnh
2	Khối ảnh được định nghĩa trong JPEG 2000 Phần 1
3	Mức phân giải được định nghĩa trong JPEG 2000 Phần 1
4	Lớp được định nghĩa trong JPEG 2000 Phần 1
5	Thanh phần được định nghĩa trong JPEG 2000 Phần 1
6	Phân khu được định nghĩa trong JPEG 2000 Phần 1
7	Thẻ TRLCP (Khối ảnh – phân giải-lớp-thành phần-phân khu)
8	Gói tin được định nghĩa trong JPEG 2000 Phần 1
9	Băng con được định nghĩa trong JPEG 2000 Phần 1
10	Khối mã được định nghĩa trong JPEG 2000 Phần 1
11	(Các) ROI
12	Tỉ lệ bít
13	Định nghĩa bởi người dùng. Chi tiết được định nghĩa theo cách khác (như JPSEC ID)
	Tất cả các giá trị khác được dự trữ

Bảng 14 - Lớp mô tả không liên quan đến ảnh

Số bít	Ngữ nghĩa
1	Các gói tin được định nghĩa trong JPEG 2000 Phần 1
2	Khoảng byte (đệm) (bắt đầu ở byte đầu tiên sau mã đánh dấu SOD đầu tiền)
3	Khoảng byte (đệm) (bắt đầu ở byte đầu tiên sau đánh đấu SEC đầu tiên)
4	Khoảng byte không đệm khi đệm được sử dụng
5	Thẻ TRLCP (Khối ảnh – phân giải-lớp-thành phần-phân khu)
6	Các giá trị méo
7	Tầm quan trọng liên quan
8	Định nghĩa bởi người dùng. Chi tiết được định nghĩa theo cách khác (ví dụ JPSEC ID)
	Tất cả các giá trị khác được dự trữ

Chỉ số gói tin được đánh số tuần tự trong một khối ảnh, do đó nó có thể không duy nhất trên toàn khối ảnh. Hơn nữa, chỉ số gói trong một khối ảnh có thể trôi qua khi giá trị tối đa của chúng vượt quá 65.535. Vì lý do này, đánh chỉ số gói tin được mô tả chi tiết. Khi các chỉ số gói trong một khối ảnh không vượt quá 65.535 gói, thì chỉ số gói tin mô tả trong Bảng 13 được xác định bởi chỉ số gói tin đưa ra bởi tham số Nsop SOP theo quy định tại Bảng A.40 trong tiêu chuẩn JPEG 2000 Phần 1. CHÚ THÍCH rằng khi giá trị tối đa không vượt quá 65.536, một gói tin JPEG 2000 có thể được xác định duy nhất với chỉ số khối ảnh và chỉ số gói. Khi các chỉ số gói tin vượt quá 65.535 gói, thì chỉ số gói JPEG 2000 Phần 1 được xác định để trôi về 0. Trong trường hợp này, chỉ số gói tin không xác định một gói tin duy nhất và không được sử dụng. Trong trường hợp này, phải sử dụng thẻ TRLCP thay thế. CHÚ THÍCH rằng các dịch vụ bảo mật yêu cầu chỉ số gói duy nhất dễ bị tổn hại nếu chỉ số gói trôi đi và lặp lại.

Khi thẻ TRLCP được sử dụng, định dạng của nó phải được xác định trong trường tham số P_{SEC} thể hiện trong Bảng 2. Cụ thể, định dạng thẻ TRLCP được xác định bởi các trường tham số P_{TRLCP} trong Bảng 4. Nó xác định kích thước của thẻ TRLCP trong ZOI.

Các lớp mô tả không liên quan đến ảnh có thể thiết lập nhiều trường cùng một lúc. Khi điều này xảy ra, các chế độ cho các trường tham số khác nhau có cùng số lượng mục (ngoại lệ cho quy tắc này được mô tả dưới đây), và các mục này phải tương ứng với nhau kiểu một-một theo thứ tự. Ví dụ, nếu vùng sử dụng khoảng byte và khoảng gói, thì mỗi khoảng phải có cùng một số lượng khoảng mục, trong đó khoảng byte đầu tiên tương ứng với khoảng gói đầu tiên, và tiếp theo tương tự như vậy.

Có một ngoại lệ cho quy tắc trên về yêu cầu số lượng mục giống nhau cho từng trường. Điều này xảy ra khi một trong các trường f1 chứa 1 mục mà đặc tả một khoảng các mục (như mô tả của chế độ khoảng trong 5.7.6), trong đó khoảng này chứa N phần tử và khi trường f2 được xác định bởi một danh sách N mục. Trong trường hợp này,trường f1 có duy nhất 1 mục (một khoảng) được xem như là một danh sách N mục. N mục này được xác định bởi khoảng trong f1 phải tương ứng kiểu một-một với N mục được liệt kê trong f2. Do đó, khoảng các mục có thể được liên quan đến một mục duy nhất hoặc nhiều mục (một cho mỗi mục trong khoảng).

Các byte được đánh chỉ số từ byte đầu tiên sau mã đánh dấu SOD đầu tiên hoặc từ byte đầu tiên sau mã đánh dấu SEC đầu tiên. Trong cả hai trường hợp, byte đầu tiên này được gắn nhãn là byte 0.

Các trường méo (cả trường méo và trường quan trọng liên quan) cung cấp khả năng để báo hiệu tầm quan trọng của vùng theo quy định của ZOI. Tham số méo xác định phần đóng góp giảm méo của đoạn dữ liệu đặc tả, có thể là một tập các gói tin hoặc một khoảng byte hoặc cho khu vực liên quan đến ảnh được quy định. Méo được thể hiện dưới dạng lỗi bình phương tổng, bằng cách sử dụng các giá trị một byte hoặc hai byte được báo hiệu trong Mzoi. Các tham số méo liên quan được sử dụng để xác định tầm quan trọng của đoạn dữ liệu quy định, bằng cách sử dụng giá trị một byte, hai byte hoặc bốn byte được báo hiệu trong Mzoi. Các chi tiết và các định dạng khác của các trường này được mô tả trong 5.7.3.2.

Thẻ TRLCP xác định một khối ảnh, độ phân giải, lớp, thành phần, và phân khu trong dòng mã của gói được bảo vệ. Thẻ này được sử dụng trong ZOI để xác định các tham số vì thông tin này khó để suy ra trong một dòng mã bảo vệ.

CHÚ THÍCH rằng khi chỉ mô tả liên quan đến ảnh được sử dụng, trường này được kết thúc. Vì vậy, không cần phải biểu diễn mô tả không liên quan đến ảnh nếu chúng không được sử dụng.

5.7.3.1 Trường khoảng byte

Lớp mô tả không liên quan đến ảnh cho phép ZOI được mô tả theo khoảng byte. Nói chung, yếu tố thứ 2 và thứ 3 của Bảng 14 phải được sử dụng để biểu diễn các khoảng byte cho hầu hết các công cụ như xác thực và mã hóa / giải mã mà không cần đệm. Tuy nhiên, một số phương pháp bảo vệ, chẳng hạn như mã hóa / giải mã có đệm, thay đổi độ dài của dữ liệu. Khi điều này xảy ra, cần thiết để xác định cả khoảng byte đệm và khoảng byte không đệm hoặc khoảng byte gốc. Trong trường hợp này, khoảng byte đệm được xác định bởi các yếu tố thứ 2 hoặc thứ 3 của Bảng 14 theo nhu cầu của các công cụ bảo vệ. (CHÚ THÍCH rằng hai yếu tố này không thể được sử dụng với nhau.) Ngoài ra, khoảng byte không đệm được xác định bởi các yếu tố thứ 4 của Bảng 14. Khoảng byte không đệm nên được xác định với chế độ mô tả giống như khoảng byte đệm và có cùng số lượng mục. Các mục này phải tương ứng với nhau theo kiểu một-một cách trong cùng thứ tự.

5.7.3.2 Trường méo và trường quan trọng liên quan

Trường méo và trường quan trọng liên quan cung cấp khả năng để báo hiệu tầm quan trọng của khu vực đặc tả bởi ZOI.

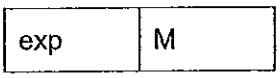
Trường méo được sử dụng để kết hợp méo với khu vực đặc tả bởi ZOI. Giá trị méo xác định méo lỗi bình phương tổng (hoặc tổng lỗi bình phương) mà cho kết quả nếu khu vực kết hợp không sẵn sàng giải mã. Méo lỗi bình phương tổng là một số đo méo cơ bản được sử dụng trong xử lý ảnh và video, và nó được sử dụng để thu được méo lỗi bình phương trung bình chung (MSE) và tỉ số tín hiệu trên tạp âm đỉnh (PSNR). Trường méo được biểu diễn bằng cách sử dụng mô tả một byte hoặc hai byte được mô tả dưới đây, và sự lựa chọn mô tả một byte hoặc hai byte được báo hiệu bởi giá trị tham số Mzoi xác định độ dài của trường này. Trường quan trọng liên quan được sử dụng để mô tả tầm quan trọng liên quan giữa các khu vực khác nhau theo quy định của các ZOI kết hợp, mà không nhất thiết phải được gắn liền với số đo méo cụ thể. Chiều dài của trường quan trọng liên quan cũng được báo hiệu bởi Mzoi. Các trường này sẽ được mô tả chi tiết hơn trong phần sau.

5.7.3.2.1 Trường méo 1 byte

Méo lỗi bình phương tổng được thể hiện bằng cách sử dụng trường méo một byte với biểu diễn loại dấu chấm động giả. 8 bit có sẵn trong trường méo được phân bổ như trong hình 15 và Bảng 15 để cung cấp sự cân bằng phù hợp giữa độ chính xác và khoảng động. CHÚ THÍCH rằng bit dấu là không cần thiết vì méo là không âm. Để bao phủ một khoảng động đầy đủ, cơ số 16 được sử dụng và 4 bit được sử dụng cho số mũ (exp). Phần định trị (m) được thể hiện sử dụng 4 bit. Do đó, giá trị méo tổng D được cho bởi:

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

trong đó m có giá trị trong khoảng $0 \leq m \leq 15$ và số mũ có một giá trị trong khoảng $0 \leq exp \leq 15$. Giá trị méo 0 được biểu diễn bởi m = 0 và exp = 0, nghĩa là trường méo bằng không. Bằng cách phân bổ 4 bit cho phần định trị m tính chính xác là $½ \times (1/2^4) = 1/32$ hoặc khoảng 3%. Với 4 bit cho số mũ và sử dụng cơ số 16, khoảng động là từ 0 đến tối đa trong đó tối đa được tính bởi m = 15 và exp = 15 tương ứng với méo $15 \times 16^{15} = 1,7 \times 10^{19}$.



Hình 15 - Cú pháp trường méo

exp: Số mũ của giá trị trường méo

m: Phần định trị của giá trị trường méo

Bảng 15 - Các giá trị tham số trường méo

Tham số	Kích thước (bit)	Giá trị
exp	4	0 ... 15
m	4	0 ... 15

CHÚ THÍCH rằng với định dạng méo này, so sánh giữa hai méo để xác định méo nào lớn hơn có thể thực hiện đơn giản bằng cách so sánh hai giá trị méo. Cụ thể, để thực hiện so sánh này không cần phải chuyển đổi từ định dạng dấu chấm động giả thành méo tổng thực tế để xác định giá trị của hai méo là lớn hơn hoặc nhỏ hơn. Thuộc tính này đơn giản hóa việc xử lý trong các ứng dụng khác nhau.

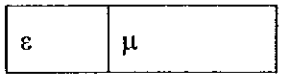
5.7.3.2.2 Trường méo hai byte

Trong định dạng hai byte, giá trị méo được thể hiện như là một số có hai byte trong định dạng dấu chấm động giả. Định dạng dấu chấm động giả cho méo được định nghĩa như sau. Định dạng này được sử dụng trong E.1.1.1 (phương trình E.3) của ITU-T Rec. T.800 | ISO / IEC 15.444-1 để thể hiện kích thước bước lượng tử hóa cho JPEG 2000. Mỗi số 16-bit chứa số mũ (5 bit) và phần định trị (11 bit) của giá trị số đo. Trong đó, giá trị dấu chấm động V của số đo được đưa ra bởi công thức sau:

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

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

Trong đó ε là số nguyên không dấu đạt được từ năm bit có trọng số lớn nhất đầu tiên của các tham số, và μ là số nguyên không dấu thu được từ 11 bit còn lại. Trường hợp đặc biệt V = ∞ tương ứng với μ = 0 và ε = 31. CHÚ THÍCH rằng các giá trị đó tràn dưới, biểu diễn được thiết lập bằng không.



Hình 16 - Cú pháp trường méo

ε: Số mũ của giá trị trường méo hai byte.

μ: Phần định trị của giá trị trường méo hai byte.

Bảng 16 - Các giá trị tham số trường méo

Tham số	Kích thước (bits)	Giá trị
ε	5	0 ... 31
μ	11	0 ... $(2^{11} - 1)$

Các thuật toán để tính toán ε và μ không là một phần bắt buộc của Tiêu chuẩn này. Một kỹ thuật có thể thực hiện các bước sau (một ví dụ về chuyển đổi số 12.25 được cung cấp). Nếu V = 0, đặt ε = μ = 0. Nếu không:

- Chuyển đổi V thành một số nhị phân ($12{,}25_{10} = 1100{,}01_2$);
- Chuẩn hóa số; điều này có nghĩa cần có một chữ số 1 bên trái của chấm nhị phân và nhân với lũy thừa 2 thích hợp để biểu diễn giá trị gốc. Dạng chuẩn hóa của 1100.01 là 1.10001×2^3;

- Số mũ là lũy thừa của 2, biểu diễn trong ký hiệu dư thừa. Độ lệch số mũ là 15; do đó trong ví dụ này số mũ được biểu diễn là 18_{10} (10010_2);

- Phần định trị đại diện cho bit quan trọng, ngoại trừ các bit bên trái của dấu nhị phân, nó luôn là một và do đó không cần phải lưu trữ; các số không có thể được nối thêm để có được 11 bit. Trong ví dụ này, phần định trị là 10001000000.

5.7.3.2.3 Trường quan trọng liên quan

Trường quan trọng liên quan r được sử dụng để mô tả tầm quan trọng liên quan giữa các đơn vị mã hóa khác nhau, mà không nhất thiết phải gắn liền với một số đo méo cụ thể. Điều này cho phép mô tả tầm quan trọng hoặc độ ưu tiên giữa các đơn vị mã hóa mà không mô tả một cách rõ ràng đơn vị này quan trọng hơn đơn vị khác bao nhiêu. Tầm quan trọng liên quan của các dữ liệu kết hợp được quy định bởi một trường n-byte hỗ trợ 2^{8n} xếp hạng dương như trong hình 17 và Bảng 17, trong đó số lượng các byte n cho trường này được xác định bởi Mzoi. Ví dụ, bằng cách sử dụng trường quan trọng liên quan một byte, tổng cộng 256 xếp hạng dương được hỗ trợ. Các giá trị tăng tương ứng với tầm quan trọng tăng, theo cách tương tự như trường méo.

Hình 17 - Cú pháp trường quan trọng liên quan

r: Giá trị quan trọng liên quan

Bảng 17 - Các giá trị tham số trường quan trọng liên quan

Tham số	Kích thước (bit)	Giá trị
r	8 * n	0 ... (2^{8n} – 1)

5.7.3.2.4 Nhận xét bổ sung về trường méo và trường quan trọng liên quan

Vì với trường méo một byte và trường quan trọng liên quan một byte, các giá trị lớn tương ứng với tầm quan trọng lớn nên có thể so sánh hai đơn vị dữ liệu này theo cùng một cách không phân biệt trường méo xác định méo thực tế hoặc tầm quan trọng liên quan. Điều này làm đơn giản hóa các ứng dụng.

Mào đầu có thể được xác định bằng cách sử dụng trường méo hoặc trường quan trọng liên quan. Sự mất mát của các loại dữ liệu khác nhau, chẳng hạn như các mào đầu phần khối ảnh, mào đầu chính hoặc mào đầu SEC, ngăn chặn việc giải mã dữ liệu ảnh liên quan. Các bộ tạo JPSEC có thể gán méo cho dữ liệu này bằng cách sử dụng:

1) Giá trị méo cao nhất (quy định tiếp theo) để báo hiệu các mào đầu hoặc dữ liệu quan trọng; hoặc

2) Để mô tả méo tổng mà được tạo ra nếu ảnh hoặc một phần của ảnh là không thể giải mã.

Bộ tạo có một số linh hoạt trong cách báo hiệu các mào đầu.

Giá trị méo cao nhất cho các trường một byte là một byte toàn 1 (0xFF). CHÚ THÍCH rằng giá trị này là giá trị méo dương cao nhất cho cả trường méo lỗi bình phương tổng một byte và cho trường quan

trọng liên quan một byte. Giá trị méo cao nhất trong trường méo hai byte là hai byte toàn 1 (0xFFFF). Độ quan trọng cao nhất cho trường quan trọng liên quan của chiều dài n-byte là giá trị n-byte toàn 1.

5.7.3.2.5 Sử dụng kết hợp trường méo và trường quan trọng liên quan

Trường méo và trường quan trọng liên quan có thể được sử dụng đồng thời để mô tả khu vực được đặc tả bởi ZOI. Trong trường hợp này, cả hai trường xác định méo lỗi bình phương, tuy nhiên trường méo quy định cụ thể việc giảm gia tăng méo trong khi trường quan trọng liên quan xác định méo tổng. Cụ thể, trường méo quy định việc giảm gia tăng méo mà ZOI sinh ra nếu được giải mã. Điều này giả định rằng tất cả các thông tin cần thiết để giải mã ZOI có sẵn và tập trung vào việc giảm gia tăng méo được sinh bởi ZOI. Các trường quan trọng liên quan xác định méo tổng phát sinh nếu ZOI không có sẵn, ví dụ, nó xác định méo tổng sẽ cho kết quả nếu ZOI đã cho không có sẵn để giải mã không chỉ đối với giá trị của chính ZOI (như thể hiện qua các trường méo) mà còn cho méo sinh ra bởi các phần khác của dòng bít nén phụ thuộc vào ZOI không giải mã được. Méo tổng kết hợp với các ZOI khác nhau cung cấp một số đo hữu ích cho tầm quan trọng liên quan của các ZOI khác nhau. Khi hai trường này được sử dụng chúng sẽ sử dụng biểu thức toán tương tự cho méo khi được báo hiệu bởi trường méo.

5.7.3.3 Trường tỷ lệ bit

Các trường tỷ lệ bit được sử dụng để xác định vùng được bảo vệ trong miền hệ số sóng con. Nó xác định mặt phẳng bít có trọng số lớn nhất mà tỷ lệ bit nén được xác định bởi trường này. Các MSB được lựa chọn bằng cách sử dụng quá trình tối ưu hóa méo tỷ lệ quy định tại Phần 1. Ví dụ, nếu giá trị tỷ lệ bit là 2,5, vùng được bảo vệ bao gồm các MSB của tất cả các hệ số sóng con có tỷ lệ bit nén là 2,5 bit cho mỗi điểm ảnh. Cú pháp của trường tỷ lệ bit được thể hiện trong hình 18 và Bảng 18. Các tỷ lệ bit quy định được cho bởi:

$$R=I_R+F_R/16$$

Ví dụ, tỷ lệ bit 0 được biểu diễn bởi $I_R=0$ và $F_R=0$; giá trị tỷ lệ bit 2,5 được biểu diễn bởi $I_R=2$ và $F_R = 8$.

Hình 18 - Cú pháp trường tỷ lệ bit

I_R: Phần nguyên của tỷ lệ bit quy định.

F_R: Phần phân số của tỷ lệ bit quy định.

Bảng 18 - Các giá trị tham số trường tỷ lệ bit

Tham số	Kích thước (bits)	Giá trị
I_R	4	0 ... 15
F_R	4	0 ... 15

5.7.4 Mối liên hệ giữa các tham số

5.7.4.1 Mô tả chung

Khi lớp mô tả có liên quan đến ảnh có nhiều trường thiết lập cùng một lúc, vùng kết quả sẽ là giao điểm của các trường này. Ví dụ, một vùng có thể xác định mức phân giải thấp nhất trong khối ảnh thứ 2. Tập hợp các trường có thể được xác định bằng cách sử dụng nhiều vùng trong ZOI.

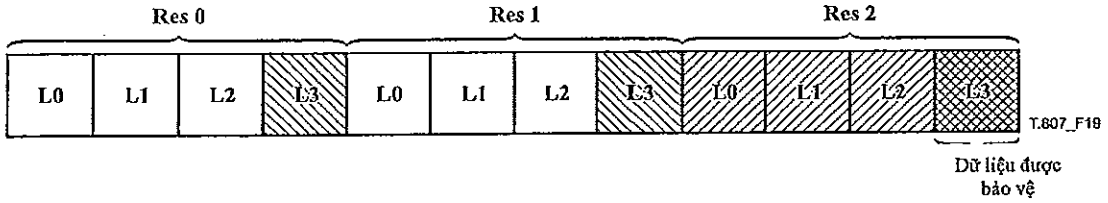
Lớp mô tả không liên quan đến ảnh cũng có thể thiết lập nhiều trường cùng một lúc. Khi điều này xảy ra, các chế độ cho các trường tham số khác nhau có cùng số lượng mục (ngoại lệ cho quy tắc này được mô tả dưới đây), và các mục này phải phù hợp với nhau theo kiểu một-một. Ví dụ, nếu vùng sử dụng các khoảng byte và khoảng gói, mỗi trường cần phải có cùng số lượng mục khoảng trong đó khoảng byte đầu tiên tương ứng với khoảng gói đầu tiên.

Ngoại lệ cho quy tắc trên về yêu cầu cùng số lượng mục cho từng trường. Điều này xảy ra khi một trong những trường f1 có 1 mục mà xác định một khoảng các mục (như mô tả bởi chế độ khoảng trong 5.7.6), trong đó khoảng này chứa N phần tử và khi trường f2 được xác định bởi danh sách N mục. Trong trường hợp này, trường f1 có duy nhất 1 mục (khoảng) được xem như là một danh sách N mục. N mục này được xác định bởi khoảng f1 phải tương ứng một-một với N mục được liệt kê trong f2. Do đó, một khoảng các mục có thể được kết hợp với một mục duy nhất hoặc nhiều mục (một cho mỗi mục trong khoảng).

5.7.4.2 Ví dụ

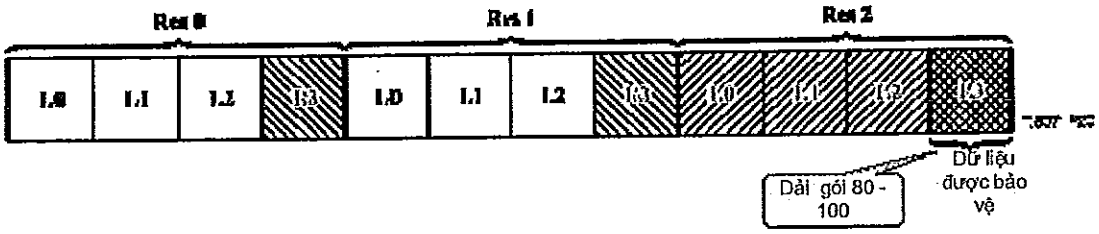
Như minh họa trong Hình 11, cấu trúc lớp mô tả vùng có thể có nhiều trường được thiết lập đồng thời, trong đó N trường là các mô tả liên quan đến ảnh (D_f^1, D_f^2, ... , D_f^N) và M trường là các mô tả không liên quan đến ảnh (D_f^1, D_f^2, ... , D_f^M). Ý nghĩa có thể được hiểu như l{ $D_f^1 \cap D_f^2 \cap ... \cap D_f^N$} = D_n^1 = D_n^2 = ...= D_n^M, có nghĩa là, các giao điểm của N mô tả liên quan đến ảnh tương ứng với từng mô tả trong M mô tả không liên quan ảnh, và ngoài ra, M mô tả không liên quan ảnh tương ứng với nhau. Mối quan hệ này được minh họa bởi ba ví dụ dưới đây.

Trong ví dụ đầu tiên, mô tả vùng có hai mô tả liên quan đến ảnh: một cho độ phân giải 2 và một cho lớp 3. Trong trường hợp này, dữ liệu bị ảnh hưởng là giao điểm của độ phân giải 2 và lớp 3, như minh họa trong Hình 19.



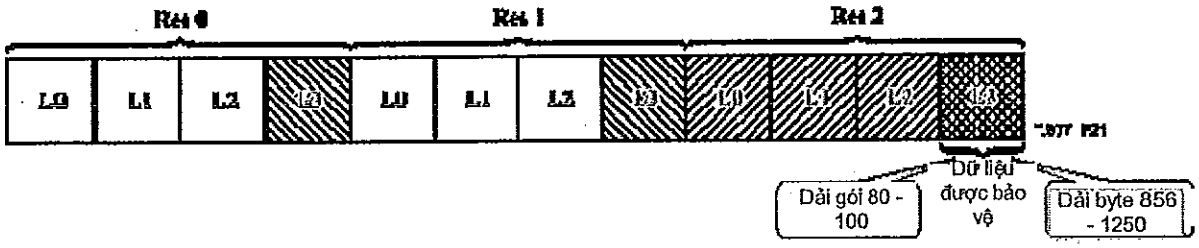
Hình 19 - Ví dụ ZOI sử dụng mô tả liên quan đến ảnh

Trong ví dụ thứ hai, mô tả vùng có hai mô tả liên quan đến ảnh (trong đó có độ phân giải 2 và lớp 3) và 1 mô tả không liên quan đến ảnh (đó là khoảng gói 80-100). Trong trường hợp này, dữ liệu bị ảnh hưởng là giao điểm của độ phân giải 2 và lớp 3. Hơn nữa, nó chỉ ra rằng dữ liệu bị ảnh hưởng được chứa trong các gói tin trong khoảng từ 80 đến 100.



Hình 20 - Ví dụ ZOI sử dụng mô tả liên quan và không liên quan đến ảnh

Trong ví dụ thứ ba, mô tả vùng có hai mô tả liên quan ảnh (trong đó có độ phân giải 2 và lớp 3) và hai mô tả không liên quan đến ảnh (trong đó có khoảng gói 80-100 và khoảng byte 856-1250). Dữ liệu bị ảnh hưởng là giao điểm của độ phân giải 2 và lớp 3, và dữ liệu bị ảnh hưởng được chứa trong các gói tin trong khoảng từ 80 đến 100. Ngoài ra các gói dữ liệu và khu vực bị ảnh hưởng này nằm trong khoảng byte 856-1250.



Hình 21 - Ví dụ ZOI thứ hai sử dụng các mô tả liên quan và không liên quan đến ảnh

5.7.5 Bảo vệ dữ liệu theo mã đánh dấu SEC

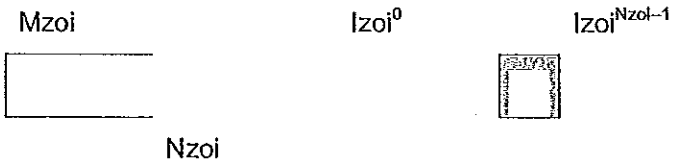
Các điều trên đã tập trung vào việc hỗ trợ các dịch vụ bảo vệ cho dòng mã JPEG 2000. Tuy nhiên, nhiều yếu tố của mào đầu chính bao gồm cả báo hiệu JPSEC cũng cần được bảo vệ và các phương pháp bảo vệ, ZOI cũng có thể được sử dụng cho mục đích này.

Cụ thể, chế độ khoảng byte của lớp mô tả không liên quan đến ảnh có thể được dùng để xác định rằng công cụ JPSEC phải áp dụng cho mọi dữ liệu sau mã đánh dấu SEC. Như đã mô tả trước, byte đầu tiên của mào đầu SEC là byte 1 để đánh chỉ số khoảng byte. Dữ liệu sau mã đánh dấu SEC và được bảo vệ bao gồm đoạn SEC và hầu hết mào đầu chính. CHÚ THÍCH rằng tất cả mào đầu chính JPEG 2000, ngoại trừ đoạn mã đánh dấu SIZ, có thể di chuyển sau mã đánh dấu SEC và do đó được bảo vệ bằng cách sử dụng phương pháp trên. Nếu đoạn mã đánh dấu SIZ JPEG 2000 được bảo vệ, nó phải được thực hiện ở một mức cao hơn, ví dụ, lớp định dạng tập tin.

Các công cụ JPSEC để bảo vệ đoạn SEC phải là các công cụ đầu tiên trong đoạn SEC. Điều này cho phép người sử dụng đầu tiên đưa ra các dữ liệu đoạn SEC, mà sau đó có thể được sử dụng để xử lý phần còn lại của dòng mã.

5.7.6 Cú pháp tham số mô tả vùng (Pzoi)

Hình 22 thể hiện cú pháp tham số mô tả ZOI



Hình 22 - Cú pháp tham số mô tả ZOI

Mzoi: Chế độ mô tả ZOI. Trường này sử dụng cấu trúc FBAS.

Nzoi: Số lượng Izoi. Trường này sử dụng cấu trúc RBAS.

Izoi^{i}: Mục.

Bảng 19 - Các giá trị tham số Pzoi^{i}

Tham số	Kích thước (bits)	Giá trị
Mzoi	Biến đổi (FBAS)	Xem bảng 20
Nzoi	0 8 + 8 * n (RBAS)	Nếu bit số 2 của Mzoi là 0. 2 ...(2^{7+7*n} – 1)
Izoi^{i}	Biến đổi	Phụ thuộc vào chế độ xác định trong Mzoi

Bảng 20 - Các giá trị tham số Mzoi

Số bit FBAS	Giá trị (bit)	Ý nghĩa
1	0	Các vùng xác định bị ảnh hưởng bởi công cụ JPSEC
	1	Phần bổ sung của các vùng xác định bị ảnh hưởng
2	0	Mục duy nhất được xác định
	1	Nhiều mục được xác định
3, 4	00	Chế độ hình chữ nhật. Một khoảng hình chữ nhật trong đó cặp giá trị đầu tiên xác định góc trên bên trái và cặp giá trị thứ hai xác định góc dưới bên phải, như vậy đã bao gồm cả hai góc. Đối với mỗi góc, giá trị đầu tiên sẽ là vị trí nằm ngang và giá trị thứ hai sẽ là vị trí dọc. Các chỉ số sẽ bắt đầu từ 0 và sẽ sử dụng lưới tham chiếu quy định tại JPEG 2000 Phần 1.
	01	Chế độ khoảng. Một khoảng các giá trị trong đó giá trị đầu tiên xác định chỉ số bắt đầu và giá trị thứ hai xác định chỉ số cuối.

Bảng 20 - Các giá trị tham số Mzoi

Số bit FBAS	Giá trị (bit)	Ý nghĩa
	10	Chế độ chỉ số. Xác định giá trị duy nhất (s).
	11	Chế độ tối đa. Xác định giá trị tối đa.
5, 6	00	Izoi[i] sử dụng số nguyên 8-bit
	01	Izoi[i] sử dụng số nguyên 16-bit
	10	Izoi[i] sử dụng số nguyên 32-bit
	11	Izoi[i] sử dụng số nguyên 64-bit
7, 8	00	Izoi[i] is được mô tả theo 1 chiều
	10	Izoi[i] is được mô tả theo 2 chiều
	01	Izoi[i] is được mô tả theo 3 chiều
9	0	Độ lệch với chế độ chiều dài không được sử dụng
	1	Độ lệch với chế độ dài được sử dụng: Xác định độ lệch ban đầu với độ dài các byte liên tiếp. Sự tồn tại của cờ này sẽ ghi đè lên các chế độ quy định trong bit 3 và 4.
		Các giá trị dự trữ

Khi thẻ TRLCP được sử dụng, kích thước của chúng được xác định bởi P_{TRLCP} theo quy định tại Bảng 4. Trong trường hợp này, các bit 5 và 6 của tham số M_{ZOI} được ghi đè.

Độ lệch với chế độ theo độ dài có thể được sử dụng để biểu diễn một chuỗi đoạn liên tiếp, ví dụ, một chuỗi các khoảng byte liên tiếp. Giá trị đầu tiên xác định độ lệch ban đầu, các giá trị tiếp theo xác định độ dài của mỗi đoạn liên tiếp. Nếu trường này được sử dụng để biểu diễn n đoạn, thì Nzoi phải được thiết lập bằng n + 1.

5.8 Cú pháp khuôn mẫu phương pháp bảo vệ (T)

5.8.1 Các vấn đề chung

Các khuôn mẫu phương pháp bảo vệ chứa các tham số để xác định các công cụ JPSEC được mô tả trong 5.6.1. Ví dụ, chúng được sử dụng trong các công cụ quy chuẩn JPSEC mô tả trong 5.6.2. Ngoài ra, chúng có thể được sử dụng trong công cụ không quy chuẩn JPSEC được mô tả trong 5.6.3. Có ba loại khuôn mẫu phương pháp bảo vệ: khuôn mẫu giải mã, khuôn mẫu xác thực và khuôn mẫu băm. Khuôn mẫu được sử dụng bởi công cụ quy chuẩn JPSEC được xác định bởi ID của nó như thể hiện trong Bảng 6 và một lần nữa ở đây trong Bảng 21 với tham chiếu đến các điều con thích hợp.

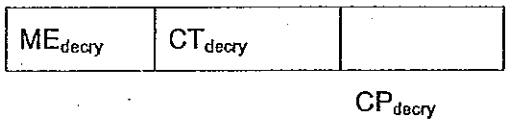
Như mô tả trong 5.6.2, khuôn mẫu phương pháp bảo vệ T cùng miền xử lý của công cụ JPSEC PD, độ chi tiết G và danh sách giá trị V mô tả cách thức công cụ JPSEC được áp dụng.

Bảng 21 -Các giá trị ID khuôn mẫu (ID_T)

Giá trị	Khuôn mẫu phương pháp bảo vệ
0	Dự trữ
1	Khuôn mẫu giải mã. Xem 5.8.2.
2	Khuôn mẫu xác thực. Xem 5.8.3.
3	Khuôn mẫu băm. Xem 5.8.4.
4	Công cụ NULL
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.2 Khuôn mẫu giải mã

Khuôn mẫu giải mã T_{decry} ($T = T_{decry}$, nếu t=0 và ID=1) được sử dụng để truyền thông bộ giải mã, để giải mã dòng mã nhận được. Hình 23 cho thấy cú pháp khuôn mẫu giải mã. Bảng 22 cho thấy các kích thước và giá trị của các ký hiệu và các tham số cho khuôn mẫu giải mã.



Hình 23 - Cú pháp khuôn mẫu giải mã

ME_{decry}: Cờ giả lập mã đánh dấu lỗi cho biết có giả lập mã đánh dấu lỗi xuất hiện trong dữ liệu mã hóa không. Một giả lập mã đánh dấu lỗi tác động đúng theo bộ giải mã JPEC 2000 phần 1. Trường này sử dụng cấu trúc FBAS.

CT_{decry}: định danh loại mật mã.

CP_{decry}: tham số mật mã.

Bảng 22 - Các giá trị tham số khuôn mẫu giải mã

Tham số	Kích thước (bit)	Giá trị
ME_{decry}	8 + 8 * n (FBAS)	Bảng 23
CT_{decry}	16	Bảng 24

CP_{decry}	Biến đổi	Nếu CT_{decry}<0x6000, Xem 5.8.2.1. Nếu 0x6000 ≤ CT_{decry}< 0xC000, Xem 5.8.2.2. Nếu CT_{decry}≥ 0xC000, Xem 5.8.2.3.

Bảng 23 - Các giá trị cờ giả lập mã đánh dấu (ME_{decry})

Giá trị	Loại phương pháp
01xx xxxx	Dữ liệu mã hóa không chứa giả lập mã đánh dấu lỗi
00xx xxxx	Trường hợp khác
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

Giá trị mặc định của cờ giả lập mã đánh dấu là 0. Cờ này có thể được thiết lập bằng 1 để chỉ ra rằng dữ liệu được mã hóa JPSEC không chứa giả lập mã đánh dấu lỗi. Một bộ tạo JPSEC có thể lựa chọn để cờ này theo giá trị mặc định của nó là bằng 0.

Bảng 24 - Giá trị bộ định danh mật mã (CT_{decry})

Giá trị	Loại mật mã
0 ... 0x5FFF	Mật mã khối (Xem Bảng 25)
0x6000 ... 0xBFFF	Mật mã dòng (Xem Bảng 26)
0xC000 ... 0xFFFF	Mật mã bất đối xứng (Xem Bảng 27)

Bảng 25 - Giá trị bộ định danh mật mã khối (CT_{decry})

Giá trị	Loại mật mã
0x0000	NULL (không mã hóa)
0x0001	AES (ISO/IEC 18033-3)
0x0002	TDEA (ISO/IEC 18033-3)
0x0003	MISTY1 (ISO/IEC 18033-3)
0x0004	Camellia (ISO/IEC 18033-3)
0x0005	CAST-128 (ISO/IEC 18033-3)
0x0006	XEMD (ISO/IEC 18033-3)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

Bảng 26 - Giá trị bộ định danh mật mã dòng (CT_{decry})

Giá trị	Loại mật mã
0x6000	SNOW 2 (ISO/IEC 18033-4)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

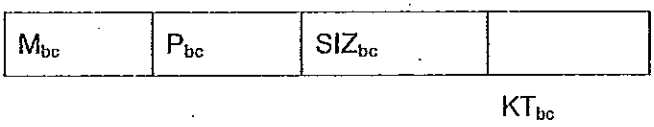
Bảng 27 - Giá trị bộ định danh mật mã bất đối xứng (CT_{decry})

Giá trị	Loại mật mã
0xC000	RSA-OAEP (ISO/IEC 18033-2)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.2.1 Khuôn mẫu mật mã khối

Khuôn mẫu mật mã khối được sử dụng để truyền thông bộ giải mã khối để giải mã dòng mã nhận được. Hình 24 cho thấy chế độ mật mã khối, chế độ đệm, kích thước khối và các thông tin khóa.

Một số chế độ mật mã khối sử dụng vector khởi tạo. Đối với các chế độ này, vectơ khởi tạo của công cụ được xác định sử dụng trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Cụ thể, vectơ khởi tạo chỉ được sử dụng cho các chế độ có ID M_{bc} > 0x80, ví dụ CBC, CFB, OFB, CTR. Trong trường hợp CTR, nó không thực sự là một IV mà là bộ đếm. Kích thước của vector khởi tạo quy định tại danh sách giá trị V được thiết lập cho kích thước khối SIZ_{bc}.



Hình 24 - Cú pháp khuôn mẫu mật mã khối

M_{bc}: Chế độ mật mã khối. Bit đầu tiên cho biết việc sử dụng vectơ khởi tạo với công cụ này. Nếu M_{BC} <0x8, IV không được sử dụng, nếu một hoặc nhiều giá trị IV được yêu cầu cho chế độ.

P_{bc}: Chế độ đệm.

SIZ_{bc}: Kích thước của khối theo Byte

KT_{bc}:khuôn mẫu khóa (xem 5.8.5). Chứa thông tin về các khóa được sử dụng bởi mật mã khối.

Bảng 28 - Giá trị khuôn mẫu mật mã khối

Tham số	Kích thước (bits)	Giá trị
M_{bc}	6	Bảng 29
P_{bc}	2	Bảng 30

SIZ_{bc}	8	1 ... 256
KT_{bc}	Biến đổi	Xem 5.8.5

Bảng 29 - Giá trị chế độ mật mã khối (M_{bc})

Giá trị	Loại chế độ
0	Dự trữ
0x xxxx	Các chế độ được sử dụng không có IV
1x xxxx	Các chế độ được sử dụng có IV
x0 xxxx	Các Bit không có đệm
x1 xxxx	Các Bit có đệm
0x 0001	ECB (ISO/IEC 10116)
1x 0010	CBC (ISO/IEC 10116)
1x 0011	CFB (ISO/IEC 10116)
1x 0100	OFB (ISO/IEC 10116)
1x 0101	CTR (ISO/IEC 18033-2)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

CHÚ THÍCH 1 - Triển khai thận trọng được yêu cầu cho tất cả các chế độ, bởi vì việc triển khai không đúng có thể dẫn đến lỗ hổng. CHÚ THÍCH rằng ngay cả khi thực hiện chính xác ECB, có rò rỉ thông tin khi các khối giống hệt nhau xuất hiện. Hướng dẫn này có trong ISO / IEC 10116.

CHÚ THÍCH 2 - Các giá trị trong Bảng 30 chỉ áp dụng khi M_{bc} trong Bảng 29 xác định rằng các được đệm. Khi bit không đệm, P_{bc} sẽ được thiết lập thành 00.

Bảng 30 - Chế độ đệm cho mật mã khối (P_{bc})

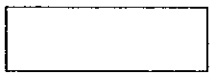
Giá trị	Loại mật mã khối
00	Lấy bản mã (RFC 2040)
01	Đệm PKCS#7 (PKCS#7)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

CHÚ THÍCH 3 - Khi sử dụng đệm, thiết kế hệ thống cần phải cẩn thận khi sử dụng để tránh lỗ hổng bảo mật tiềm tàng, chẳng hạn như các cuộc tấn công kiểu mật mã.

5.8.2.2 Khuôn mẫu mật mã dòng

Khuôn mẫu mật mã dòng được sử dụng để truyền thông bộ giải mã dòng để giải mã dòng mã nhận được. Hình 25 cho thấy cú pháp khuôn mẫu mật mã dòng . Bảng 31 cho thấy giá trị của khuôn mẫu mật mã dòng.

Vector khởi tạo mật mã dòng được xác định sử dụng trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Kích thước của vector khởi tạo được xác định tại danh sách giá trị V sẽ được thiết lập cho kích thước khóa quy định tại khuôn mẫu thông tin khóa KT_{sc}.



KT_{sc}

Hình 25 - Cú pháp khuôn mẫu mật mã dòng

KT_{sc}:Khuôn mẫu thông tin khóa (Xem 5.8.5). Lưu giữ thông tin về khóa sử dụng bởi mật mã dòng.

Bảng 31 - Các giá trị khuôn mẫu mật mã dòng

Tham số	Kích thước (bit)	Giá trị
KT_{sc}	Biến đổi	Xem 5.8.5

5.8.2.3 Khuôn mẫu mật mã bất đối xứng

Khuôn mẫu mật mã bất đối xứng mẫu được sử dụng để truyền thông các bộ giải mã bất đối xứng, để giải mã dòng mã nhận được. Hình 26 cho thấy cú pháp khuôn mẫu mật mã bất đối xứng. Bảng 32 cho thấy giá trị của khuôn mẫu mật mã bất đối xứng.

Đối với các công cụ sử dụng khuôn mẫu mật mã bất đối xứng mẫu, trường độ chi tiết của công cụ (G) xác định độ chi tiết mà mật mã được áp dụng. Tuy nhiên, trường danh sách giá trị (V) không được sử dụng để biểu diễn cho bất kỳ giá trị nào. Như vậy, số lượng các yếu tố (N_v) trong trường danh sách giá trị được thiết lập là 0.

KT_{sy}

Hình 26 - Cú pháp khuôn mẫu mật mã không đối xứng

KT_{sy}:Khuôn mẫu thông tin khóa (Xem 5.8.5). Lưu giữ thông tin về khóa sử dụng bởi mật mã không đối xứng.

Bảng 32 - Các giá trị khuôn mẫu mật mã không đối xứng

Tham số	Kích thước (bit)	Giá trị
KT_{sy}	Biến đổi	Xem 5.8.5

5.8.3 Khuôn mẫu xác thực

Khuôn mẫu xác thực T_{auth} ($T = T_{auth}$, nếu t=0 và ID=2) được sử dụng để truyền thông bộ kiểm chứng, để kiểm chứng tính xác thực của dòng mã nhận được. Có ba lớp chung của phương pháp xác thực: xác thực dựa trên hàm băm, xác thực dựa trên mật mã và chữ ký số. Hai phương pháp xác thực dựa trên băm và dựa trên mật mã cũng thường được gọi là mã xác thực bản tin (MAC), và các giá trị tính toán của chúng được sử dụng để xác thực thường được gọi là giá trị MAC. Cú pháp khuôn mẫu xác thực được thể hiện trong hình 27 và Bảng 33 cho thấy kích thước và giá trị của các ký hiệu và các tham số cho khuôn mẫu xác thực.

Trong nhiều ứng dụng bảo mật, xác thực là dịch vụ bảo mật quan trọng nhất. Ngay cả khi tính bảo mật là dịch vụ bảo vệ mục tiêu, cần được tăng cường bằng cách xác thực để ngăn chặn các cuộc tấn công. Đặc biệt, khuyến khích xác thực các phần của đoạn mã đánh dấu SEC. Ngoài ra, việc xác thực được thực hiện trên cả các tham số khuôn mẫu xác thực (T_{auth}) và bản tin để xác thực. Cụ thể, vùng ảnh hưởng xác định rằng cả nội dung và các tham số khuôn mẫu xác thực (T_{auth}) sẽ được xác thực.

M_{auth}	

P_{auth}

Hình 27 - Cú pháp khuôn mẫu xác thực

M_{auth}: Cú pháp xác thực.

P_{auth}: Tham số xác thực.

Bảng 33 - Các giá trị tham số khuôn mẫu xác thực

Tham số	Kích thước (bit)	Giá trị
M_{auth}	8	Bảng 34
P_{auth}	Biến đổi	Nếu M_{auth} = 0, xem 5.8.3.1 Nếu M_{auth} = 1, xem 5.8.3.2 Nếu M_{auth} =2, xem 5.8.3.3

Bảng 34 - Các phương phác xác thực (M_{auth})

Giá trị	Phương pháp
0	MAC dựa vào hàm băm
1	MAC dựa vào mật mã

2	Chữ ký số
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.3.1 Xác thực dựa vào hàm băm

MAC xác thực dựa vào hàm băm được sử dụng để truyền thông bộ kiểm chứng để kiểm chứng tính xác thực của dòng mã nhận được. Hình 28 cho thấy cú pháp khuôn mẫu xác thực dựa vào hàm băm và Bảng 35 cho thấy các giá trị tham số.

Các giá trị MAC được xác định bởi trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Kích thước của giá trị MAC xác định trong danh sách giá trị V được thiết lập thành kích thước MAC xác định bởi $SIZH_{MAC}$.

M_{HMAC}	H_{HMAC}		SIZ_{HMAC}
KT_{HMAC}			

Hình 28 - Khuôn mẫu xác thực dựa vào băm

M_{HMAC}: Bộ định danh phương pháp xác thực dựa vào băm

H_{HMAC}: Bộ định danh hàm băm.

KT_{HMAC}: Khuôn mẫu khóa.

SIZ_{HMAC}: Kích thước của MAC (bit).

Bảng 35 - Các giá trị tham số khuôn mẫu xác thực dựa vào băm

Tham số	Kích thước (bit)	Giá trị
M_{HMAC}	8	Bảng 36
H_{HMAC}	8	Bảng 37
KT_{HMAC}	Có thể thay đổi	Xem 5.8.5
SIZ_{HMAC}	16	0 ... 65535

Bảng 36 - Xác định phương pháp xác thực dựa vào băm (M_{HMAC})

Giá trị	Phương pháp xác thực vào băm
0	Dự trữ
1	HMAC (ISO/IEC 9797-2)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

Bảng 37 -Bộ định danh hàm băm (H_{HMAC})

Giá trị	Hàm băm
0	Dự trữ
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)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

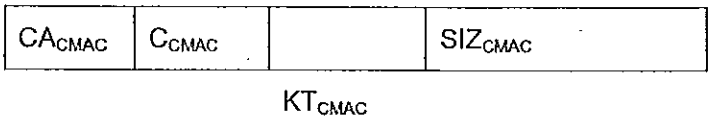
CHÚ THÍCH rằng nếu SIZ_{HMAC} nhỏ hơn kích thước định danh của hàm băm, thì nó là phiên bản cắt ngắn tương ứng với các bit SIZ_{HMAC} đầu tiên của hàm băm.

5.8.3.2 Khuôn mẫu xác thực dựa vào mật mã

MAC xác thực dựa vào mật mã được sử dụng truyền thông bộ kiểm chứng để kiểm chứng tính xác thực của dòng mã nhận được. Hình 29 là cú pháp khuôn mẫu và Bảng 38 biểu diễn kích thước khóa và băm có khóa. Một ví dụ về sơ đồ xác thực dựa vào mật mã là CBC-MAC. Trong các kỹ thuật mật mã khối để xác thực, vector khởi tạo là chiều dài khối và có giá trị 0. Chiều dài khối là mặc định cho mật mã khối. CHÚ THÍCH rằng nếu SIZ_{CMAC} nhỏ hơn kích thước danh định của MAC xác thực dựa vào mật mã thì nó là phiên bản cắt ngắn tương ứng với các bit SIZ_{CMAC} đầu tiên của MAC.

CHÚ THÍCH rằng, nếu số lượng các bit dữ liệu không phải là một bội số của chiều dài khối mật mã, thì khối đầu vào cuối cùng sẽ là một phần của khối dữ liệu, với các bit 0 được nối vào để tạo thành một khối mật mã đầy đủ. Cũng CHÚ THÍCH rằng CBC-MAC chỉ được áp dụng cho dữ liệu có độ dài cố định và đã biết.

Các giá trị MAC được xác định bởi trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Kích thước của giá trị MAC xác định trong danh sách giá trị V sẽ được thiết lập thành kích thước MAC xác định bởi SIZ_{CMAC}.



Hình 29 - Cú pháp khuôn mẫu xác thực dựa vào mật mã

CA_{CMAC}: Phương pháp xác thực dựa vào mật mã

C_{CMAC}: Giá trị bộ định danh mật mã khối

KT_{CMAC}: Khuôn mẫu khóa.

SIZ_{CMAC}: Kích thước của MAC (bit).

Bảng 38 - Giá trị khuôn mẫu MAC

Tham số	Kích thước (bit)	Giá trị
CA_{CMAC}	8	Bảng 39
C_{CMAC}	8	Bảng 25
KT_{CMAC}	Có thể thay đổi	Xem 5.8.5
SIZ_{CMAC}	16	0 ... 65535

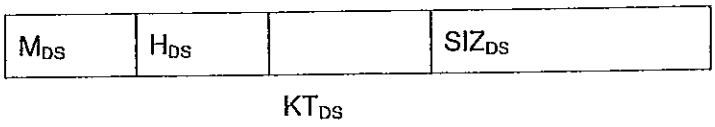
Bảng 39 - Phương pháp xác thực dựa vào mật mã (C_{CMAC})

Giá trị	Phương pháp
0	Thuật toán CBC-MACMAC 1 (ISO/IEC 9797-1)
1	Thuật toán CBC-MACMAC 2 (ISO/IEC 9797-1)
2	Thuật toán CBC-MACMAC 3 (ISO/IEC 9797-1)
3	Thuật toán CBC-MACMAC 4 (ISO/IEC 9797-1)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.3.3 Khuôn mẫu chữ ký số

Chữ ký số được sử dụng để truyền thông bộ kiểm chứng để kiểm chứng tính xác thực của dòng mã nhận được, cũng như kiểm chứng danh tính của người gửi cho mục đích định danh và không thoái thác. Hình 30 định nghĩa khuôn mẫu và Bảng 40 liệt kê các giá trị.

Chữ ký số được xác định sử dụng trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Kích thước của giá trị chữ ký số xác định trong danh sách giá trị V được thiết lập để phù hợp với kích thước được định nghĩa bởi SIZ_{DS}. Vì kích thước danh sách giá trị được biểu diễn bởi byte thay vì bit nên kích thước của nó phải là số lượng tối thiểu các byte có thể chứa SIZ_{DS}. Mỗi giá trị phải được biểu diễn với các bit có trọng số nhỏ nhất và các bit MSB thêm sẽ được thiết lập là 0.



Hình 30 - Cú pháp khuôn mẫu chữ ký số

M_{DS}: Phương pháp chữ ký số.

H_{DS}: Hàm băm.

KT_{DS}: Khuôn mẫu khóa (Xem 5.8.5). Chứa các thông tin liên quan đến khóa công khai và chứng thư yêu cầu để kiểm chứng chữ ký số.

SIZ_{DS}: Kích thước chữ ký số (bit).

Bảng 40 - Giá trị khuôn mẫu chữ ký số

Tham số	Kích thước (bit)	Giá trị
M_{DS}	8	Bảng 41
H_{DS}	8	Bảng 37
KT_{DS}	Có thể thay đổi	Xem 5.8.5
SIZ_{DS}	16	0 ... 65535

Bảng 41 - Các phương pháp chữ ký số (M_{DS})

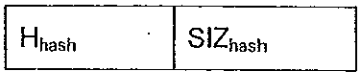
Giá trị	Phương pháp
1	RSA (ISO/IEC 14888-2)
2	Rabin (ISO/IEC14888-2)
3	DSA (ISO/IEC 14888-3)
4	ECDSA (ISO/IEC 14888-3)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.4 Khuôn mẫu hàm băm

Khuôn mẫu hàm băm T_{hash} ($T = T_{hash}$, Nếu t=0 and ID=3) được sử dụng để truyền thông các tham số sử dụng để tính toán hàm băm. Bảng 42 cho thấy kích thước và giá trị của các ký hiệu và các tham số cho khuôn mẫu băm.

CHÚ THÍCH rằng trái ngược với khuôn mẫu xác thực dựa vào băm trong 5.8.3.1 mà bao gồm việc sử dụng một hàm băm và một khóa bí mật thì khuôn mẫu hàm băm này không sử dụng khóa. Trong khi khuôn mẫu băm này có thể được sử dụng để phát hiện một lỗi ngẫu nhiên hoặc thay đổi ngẫu nhiên dữ liệu, nó không ngăn chặn thay đổi có hại của dữ liệu. Để ngăn chặn thay đổi có hại của dữ liệu, khuôn mẫu xác thực phải được sử dụng, do khóa bí mật được sử dụng bởi khuôn mẫu xác thực ngăn chặn các dữ liệu bị thay đổi mà không bị phát hiện.

Các giá trị băm được xác định sử dụng trường độ chi tiết của công cụ (G) được mô tả trong 5.10 và trường danh sách giá trị (V) được mô tả trong 5.11. Kích thước của các giá trị băm được quy định trong danh sách giá trị V được thiết lập thành kích thước giá trị băm được định nghĩa bởi SIZ_{hash}.



Hình 31 - Cú pháp khuôn mẫu hàm băm

H_{hash}: Bộ định danh hàm băm.

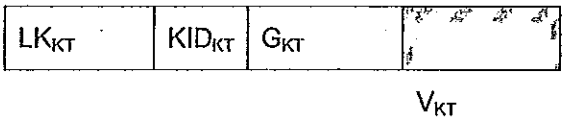
SIZ_{hash}: Kích thước giá trị băm (byte).

Bảng 42 - Giá trị tham số khuôn mẫu hàm băm

Tham số	Kích thước (bit)	Giá trị
H_{hash}	8	Bảng 37
SIZ_{hash}	8	0 ... 255

5.8.5 Khuôn mẫu thông tin khóa (KT)

Khuôn mẫu thông tin khóa được sử dụng để truyền thông thông tin khóa. Hình 32 định nghĩa khuôn mẫu và bảng 43 liệt kê các giá trị khuôn mẫu khóa.



Hình 32 - Cú pháp khuôn mẫu thông tin khóa

LK_{KT}: Chiều dài khóa theo bit.

KID_{KT}: Bộ định danh thông tin khóa. Nó chỉ ra ý nghĩa các giá trị trong danh sách giá trị V_{KT}. Trong khuôn mẫu giải mã, giá trị này phải thiết lập bằng 2 (URI để lấy khóa bí mật). Trong trường hợp chữ ký số, giá trị của lĩnh vực này là tự do.

G_{KT}: Trường độ chi tiết biểu diễn độ chi tiết với những thay đổi thông tin khóa .

V_{KT}: Trường danh sách giá trị biểu diễn danh sách thay đổi của thông tin khóa.

CHÚ THÍCH rằng trong trường hợp của khóa bí mật (khuôn mẫu giải mã), khóa công khai và chứng thư không có ý nghĩa: khuôn mẫu khóa phải giữ một số thông tin về vị trí của khóa (ví dụ, URI).

Thông tin khóa được biểu diễn với một hoặc nhiều giá trị sử dụng trường độ chi tiết của công cụ (G_{KT}) được mô tả trong 5.10 và trường danh sách giá trị (V_{KT}) được mô tả trong 5.11. Hai trường (G_{KT} và V_{KT}) cùng xác định cách các giá trị khóa trong danh sách giá trị (VKT) được áp dụng để bảo vệ dữ liệu ảnh, như mô tả trong 5.10 và 5.11.

Thông tin khóa trong danh sách giá trị có thể chọn một trong những hình thức xác định trong Bảng 44.

Nếu KID_{KT} = 1, thì mỗi giá trị được xác định với khuôn mẫu chứng thư X.509 được mô tả trong 5.8.5.1.

Nếu KID_{KT} = 2, thì mỗi giá trị được xác định với một URI cho chứng thư hoặc khóa bí mật.

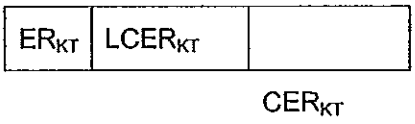
Bảng 43 - Giá trị khuôn mẫu khóa

Tham số	Kích thước (bit)	Giá trị
LK_{KT}	16	1 ... 65535
KID_{KT}	8	Bảng 44
G_{KT}	24	Xem 5.10
V_{KT}	Có thể thay đổi	Xem 5.11

Bảng 44 - Giá trị bộ định danh thông tin khóa (KID_{KT})

Giá trị	Bộ định danh thông tin khóa
0	Dự trữ
1	Chứng thư X.509 (ISO/IEC 9594-8)
2	URI cho chứng thư hoặc khóa bí mật
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.8.5.1 Khuôn mẫu chứng thư X.509



Hình 33 - Cú pháp chứng thư X.509

ER_{KT}: Quy luật mã hóa cho chứng thư X.509.

$LCER_{KT}$: Chiều dài chứng thư X.509 theo byte.

CER_{KT}: Chứng thư X.509.

Bảng 45 - Giá trị chứng thư X.509 (KI_{KT} nếu KID_{KT}=2)

Tham số	Kích thước (bit)	Giá trị
ER_{KT}	8	0 ... 255 (Xem Bảng 46)
$LCER_{KT}$	16	1 ... 65535
CER_{KT}	Biến đổi	–

Bảng 46 - Giá trị quy luật mã hóa (ER_{KT})

Giá trị	Bộ định danh quy luật mã hóa
0	Dự trữ
1	DER (RFC3217)
2	BER(RFC3394)
	Tất cả các giá trị khác được dự trữ cho sử dụng ISO

5.9 Cú pháp miền xử lý (PD)

Cú pháp miền xử lý được sử dụng để chỉ ra miền mà công cụ JPSEC được áp dụng. Các miền có thể bao gồm miền điểm ảnh, miền hệ số sóng con, miền hệ số sóng con được lượng tử hóa và miền dòng mã.

PD	F_{PD}

Hình 34 - Cú pháp miền xử lý

PD: Miền xử lý. Trường này sử dụng cấu trúc FBAS.

F_{PD}: Trường miền xử lý để cung cấp thông tin chi tiết thêm về miền xử lý. Trường này sử dụng cấu trúc FBAS.

Bảng 47 - Các tham số miền xử lý

Tham số	Kích thước (bit)	Giá trị
PD	Có thể thay đổi (FBAS)	Xem Bảng 48
F_{PD}	Có thể thay đổi (FBAS)	Trong miền hệ số sóng con và miền hệ số sóng con được lượng tử hóa, Xem Bảng 49. Trong miền dòng mã, Xem Bảng 50.

Bảng 48 - Giá trị tham số miền xử lý (PD)

Số lượng bit FBAS	Giá trị	Ý nghĩa
1	1	Miền điểm ảnh. Phương pháp bảo vệ được áp dụng vào các điểm ảnh.
	0	Các trường hợp khác
2	1	Miền hệ số sóng con. Phương pháp bảo vệ được áp dụng vào các hệ số sóng con.

	0	Các trường hợp khác
3	1	Miền hệ số sóng con được lượng tử hóa: Phương pháp bảo vệ được áp dụng vào các hệ số sóng con được lượng tử hóa.
	0	Các trường hợp khác
4	1	Miền dòng mã: Phương pháp bảo vệ được áp dụng vào dòng mã được tạo ra từ bộ mã số học.
	0	Các trường hợp khác

CHÚ THÍCH rằng trường PD sẽ có một và chỉ 1 bit thiết lập bằng 1, bởi vì mỗi công cụ JPSEC được áp dụng cho một miền duy nhất.

Trong miền điểm ảnh, miền hệ số sóng con và miền hệ số sóng con được lượng tử hóa, dữ liệu hai chiều phải chuyển đổi thành một chiều để áp dụng các công cụ bảo mật. Chuyển đổi này được thực hiện bằng cách quét dữ liệu ảnh hai chiều theo thứ tự quét mành.

Bảng 49 - Các giá trị tham số trường miền xử lý (F_{PD}) trong miền hệ số sóng con và miền hệ số sóng con được lượng tử hóa

Số lượng bit FBAS	Giá trị	Ý nghĩa
1	0	Phương pháp bảo vệ được áp dụng cho dấu bit
	1	Phương pháp bảo vệ được áp dụng cho bit có trọng số lớn nhất

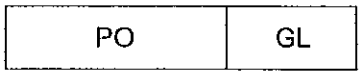
Bảng 50 - Giá trị tham số trường miền xử lý (F_{PD}) trong miền dòng mã

Số lượng bit FBAS	Giá trị	Ý nghĩa
1	0	Phương pháp bảo vệ được áp dụng vào cả mào đầu và thân của gói tin
	1	Phương pháp bảo vệ được áp dụng vào thân của gói tin

Trường (F_{PD}) được sử dụng để cung cấp thêm thông tin về miền xử lý. Với các giá trị khác nhau của PD, miền này (F_{PD}) có ý nghĩa khác nhau. Ví dụ, trong miền hệ số sóng con và miền hệ số sóng con được lượng tử hóa, bit đầu tiên của F_{PD} được sử dụng để cho biết công cụ JPSEC được áp dụng trên bit có trọng số lớn nhất hay không. Trong miền dòng mã, bit đầu tiên của F_{PD} được sử dụng để cho biết công cụ JPSEC được áp dụng chỉ trên thân gói tin hay cả mào đầu và thân của gói tin; trong miền điểm ảnh, miền này (F_{PD}) được dự trữ.

5.10 Cú pháp Độ chi tiết (G)

Độ chi tiết được sử dụng để chỉ đơn vị bảo vệ cho mỗi phương pháp bảo vệ. Bảng 53 định nghĩa các độ chi tiết có thể. Hình 35 biểu diễn cú pháp độ chi tiết.



Hình 35 - Cú pháp độ chi tiết

PO: Thứ tự xử lý.

GL: Mức độ chi tiết.

Bảng 51 - Giá trị tham số độ chi tiết (G)

Tham số	Kích thước (bit)	Giá trị
PO	16	Xem Bảng 52
GL	8	Xem Bảng 53

Bảng 52 - Giá trị thứ tự xử lý (PO)

Giá trị MSB LSB	Thứ tự xử lý
0 000 000 000 000 000	Thứ tự được xác định bởi các tham số liên quan đến ảnh vùng ảnh hưởng
1 000 000 000 000 000	Thứ tự được xác định bởi các tham số dòng bít không liên quan đến ảnh vùng ảnh hưởng
1 000 000 000 000 001	Thứ tự được xác định bởi các tham số gói tin không liên quan đến ảnh vùng ảnh hưởng
0 000 001 010 011 100	Khối ảnh – độ phân giải - lớp - thành phần - phân khu
0 000 011 100 001 010	Khối ảnh - thành phần - phân khu – độ phân giải - lớp
0 000 010 001 011 100	Khối ảnh - lớp – độ phân giải - thành phần - phân khu
0 000 100 011 001 010	Khối ảnh - phân khu - thành phần – độ phân giải - lớp
0 000 001 100 011 100	Khối ảnh – độ phân giải - phân khu - thành phần - lớp
	Các giá trị dự trữ

Bảng 53 - Giá trị mức độ chi tiết (GL)

Giá trị MSB LSB	Độ chi tiết
0000 0000	Khối ảnh
0000 0001	Phần khối ảnh

0000 0010	Thành phần ảnh
0000 0011	Độ phân giải
0000 0100	Lớp
0000 0101	Phân khu
0000 0110	Gói tin
0000 0111	Băng con
0000 1000	Khối mã
0000 1001	Vùng tổng được định danh trong ZOI
1000 0000	Mục được định danh trong ZOI không liên quan đến ảnh
1000 0001	Vùng được định danh trong ZOI không liên quan đến ảnh
	Các giá trị dự trữ

Để xử lý toàn bộ vùng xác định bởi ZOI, mức độ chi tiết phải là "vùng được định danh trong ZOI"

5.11 Cú pháp danh sách giá trị (V)

Trường danh sách giá trị được sử dụng để xác định giá trị thay đổi khi công cụ này được áp dụng và độ chi tiết mà nó thay đổi. Trường này được sử dụng để báo hiệu giá trị thay đổi như các khóa, vectơ khởi tạo, giá trị MAC, chữ ký số và giá trị băm. Trường giá trị danh sách trước tiên xác định số lượng các giá trị trong danh sách và kích thước của mỗi giá trị. Sau đó nó sẽ liệt kê các giá trị của chính nó. Như đã nêu trong 5.6.2, cho các công cụ quy chuẩn JPSEC, trường danh sách giá trị biểu diễn một tham số khác cho mỗi khuôn mẫu. Đối với khuôn mẫu giải mã, nó biểu diễn vectơ khởi tạo IV_{bc} hoặc IV_{sc} tùy thuộc vào mật mã khối hoặc mật mã dòng có được sử dụng hay không. Đối với khuôn mẫu xác thực, nó biểu diễn giá trị MAC VAL_{MAC} để xác thực dựa vào băm và dựa vào mật mã. Đối với khuôn mẫu chữ ký số, nó biểu diễn chữ ký số SIG_{DS}. Đối với khuôn mẫu hàm băm, nó biểu diễn giá trị băm HV_{hash}.

Một số cách sử dụng khuôn mẫu không yêu cầu giá trị được xác định, ví dụ, không phải tất cả các chế độ giải mã sử dụng vector khởi tạo. Trong những trường hợp này, trường danh sách giá trị phải thiết lập N_v và S_v bằng 0 để danh sách giá trị V_L không có phần tử. Nếu chỉ có một giá trị duy nhất cần phải được xác định, ví dụ, nếu một khóa duy nhất được sử dụng trên ảnh, thì N_v sẽ được thiết lập bằng 1 sao cho giá trị duy nhất có trong danh sách giá trị.

N_V	S_V	VL

Hình 36 - Cú pháp trường danh sách giá trị

N_V: Số lượng các giá trị trong danh sách giá trị V_L, Nếu N_V = 0, thì trường này kết thúc. Trường này sử dụng cấu trúc RBAS.

S_V: Kích thước của mỗi giá trị trong danh sách giá trị V_L theo byte. Trường này sử dụng cấu trúc RBAS.

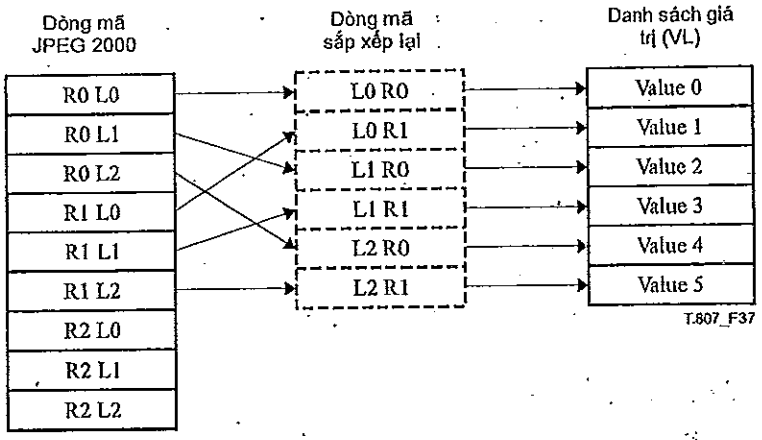
VL: Danh sách các giá trị.

Bảng 54 - Các giá trị tham số trường danh sách giá trị (V)

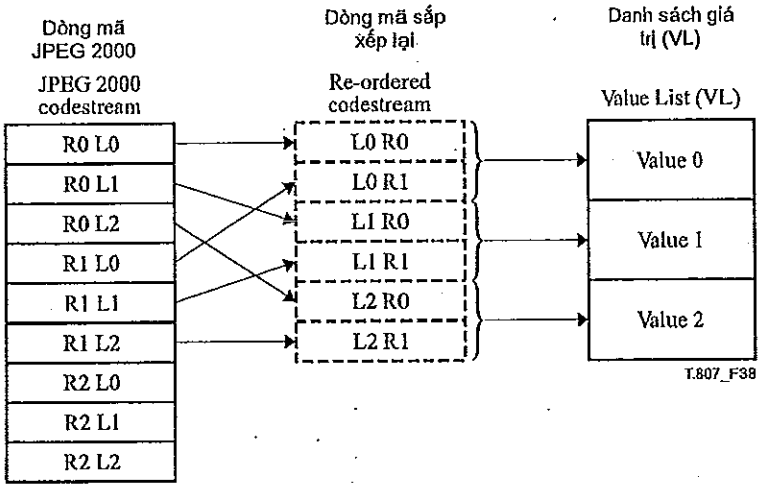
Tham số	Kích thước (bit)	Giá trị
N_V	16 + 8 * n (RBAS)	0 ... $(2^{16+7*n} - 1)$
S_V	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
VL	0, Nếu NV = 0 N_V * S_V, cách khác	N/A Xác định bởi khuôn mẫu

5.12 Mối quan hệ giữa ZOI, độ chi tiết (G) và danh sách giá trị (VL)

Các ZOI, PO và GL được sử dụng cùng nhau để đảm bảo cách xử lý duy nhất của các công cụ JPSEC được áp dụng, không phụ thuộc vào thứ tự lũy tiến của dòng mã JPEG 2000. Nói cách khác, chữ ký kết quả, giá trị MAC và dòng mã được mã hóa độc lập với thứ tự lũy tiến của dòng mã JPEG 2000. Vùng của ảnh hưởng (ZOI) xác định, toàn bộ hoặc một phần của dòng mã JPEG 2000 được bảo vệ bởi công cụ JPSEC; mặt khác, thứ tự xử lý (PO) xác định thứ tự mà công cụ JPSEC xử lý dòng mã; mức độ chi tiết (GL) xác định các đơn vị bảo vệ có chứa chuỗi byte liên tiếp trong dòng mã được sắp xếp lại. Cuối cùng, mỗi đơn vị bảo vệ tương ứng với một giá trị trong danh sách giá trị (VL), để chúng xuất hiện trong dòng mã được sắp xếp lại. Mối quan hệ có thể được minh bằng một ví dụ, trong đó dòng mã JPEG 2000 có 1 khối ảnh, 3 mức độ phân giải và 3 lớp, và số lượng các thành phần, phân khu ảnh là không quan trọng. Thứ tự lũy tiến là RLCP trong dòng mã JPEG2000 gốc, vùng ảnh hưởng có độ phân giải là 0 và 1, và thứ tự lũy tiến (PO) là TRLCP. Hình 37 và 38 minh họa việc sắp xếp lại của dòng mã và ánh xạ từ mỗi đơn vị bảo vệ vào danh sách giá trị (VL), khi độ chi tiết (GL) là độ phân giải và lớp.



Hình 37 - Mức độ chi tiết (GL) là độ phân giải



Hình 38 - Mức độ chi tiết (GL) là lớp

CHÚ THÍCH: - Dòng mã sắp xếp lại chỉ được sử dụng để tạo ra các giá trị trong danh sách giá trị (VL). Dòng mã JPSEC cuối sẽ có thứ tự lũy tiến giống với dòng mã JPEG 2000 gốc.

5.13 Mã đánh dấu bảo mật trong dòng mã (INSEC)

Mã đánh dấu bảo mật trong dòng mã (INSEC) cung cấp thêm một phương tiện để truyền tải thông tin bảo mật. Đây là tùy chọn và được sử dụng kết hợp với mã đánh dấu bảo mật SEC. Cụ thể, nó được sử dụng kết hợp với một công cụ không quy chuẩn JPSEC.

Chính xác hơn, mã đánh dấu SEC có mặt trong mào đầu chính và cung cấp thông tin tổng thể về các công cụ JPSEC áp dụng để bảo vệ ảnh. Mã đánh dấu INSEC có mặt trong chính dữ liệu dòng bít của nó và cung cấp cho các tham số bổ sung hoặc thay thế cho công cụ không quy chuẩn JPSEC được xác định bởi tham số chỉ số mẫu công cụ. Do đó, chỉ số mẫu công cụ trong mã đánh dấu INSEC sẽ tương ứng với một chỉ số mẫu công cụ trong mào đầu chính.

Đoạn mã đánh dấu INSEC có thể được đặt trong dữ liệu dòng bít. Nó sử dụng bộ giải mã số học trong JPEG 2000 ngừng đọc byte từ dòng bít khi nó gặp mã đánh dấu kết thúc (ví dụ, hai byte với giá trị lớn hơn 0xFF8F).

Thông tin chứa trong đoạn mã đánh dấu INSEC thích hợp với khối mã bảo mật trước hoặc sau, cho đến khi mã đánh dấu INSEC khác được tìm thấy.

CHÚ THÍCH rằng các mã đánh dấu INSEC có thể sinh ra một tập tin mà không phù hợp với JPEG 2000 Phần 1 Một số bộ giải mã có thể gặp khó khăn trong việc xử lý mã đánh dấu ở giữa gói. Việc chèn ở bất cứ nơi nào bên trong gói tin sẽ làm mất giá trị chiều dài của gói tin như được chỉ ra trong mào đầu gói. Ngoài ra, có thể có vấn đề với mã hóa và mã đánh dấu INSEC do:

a) Thiếu hạn chế giả lập mã đánh dấu trên mã hóa; và / hoặc

b) Không có khả năng xác định vị trí mã đánh dấu của chính nó trong sự hiện diện của mã hóa.

Cú pháp của các mã đánh dấu INSEC được định nghĩa trong Hình 39.

INSEC	L_{INSEC}	i	R	AP

Hình 39 - Cú pháp tạo bảo mật trong dòng mã

INSEC: Mã mã đánh dấu. Bảng 55 thể hiện kích thước và giá trị của các ký hiệu và các tham số cho đoạn mã đánh dấu bảo mật trong dòng mã.

L_{INSEC}: Chiều dài của đoạn mã đánh dấu theo byte (không bao gồm mã đánh dấu). CHÚ THÍCH rằng đoạn mã đánh dấu INSEC không phải là byte được căn chỉnh.

i: Chỉ số mẫu công cụ tương ứng với một trong các tham số chỉ số mẫu công cụ trong đoạn mã đánh dấu SEC và do đó định danh mẫu của công cụ JPSEC mà mã đánh dấu INSEC này tham chiếu đến. Trường này sử dụng cấu trúc RBAS.

R: Vùng thích hợp cho thông tin INSEC. Trường này sử dụng cấu trúc FBAS.

AP: Tham số bổ sung hoặc thay thế cho phương pháp bảo vệ. Bộ mã hóa phải đảm bảo rằng bộ mã hóa không mô phỏng một mã đánh dấu trong tham số này.

Bảng 55 - Các giá trị tham số bảo mật trong dòng mã (INSEC)

Tham số	Kích thước (bit)	Giá trị
INSEC	16	0xFF94
L_{INSEC}	16	2 ... $(2^{16} - 1)$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
R	Biến đổi (FBAS)	Xem Bảng 56
AP	Biến đổi	Được định nghĩa bởi ứng dụng hoặc tính xác thực đăng ký

Bảng 56 - Các giá trị vùng thích hợp (R)

Số lượng bit FBAS	Giá trị	Vùng thích hợp
0	0	Khối mã trước
	1	Khối mã sau

Bởi vì INSEC được sử dụng kết hợp với công cụ không quy chuẩn JPSEC nên định dạng của các tham số bổ sung hoặc thay thế được xác định bởi các công cụ của chính nó và được xác định bởi ID công cụ. Cụ thể, công cụ không quy chuẩn JPSEC được xác định bởi một cơ quan đăng ký hoặc bởi các ứng dụng JPSEC riêng. Do đó, định nghĩa của các công cụ này bao gồm việc sử dụng INSEC nếu nó được cho phép.

6 Ví dụ về sử dụng cú pháp quy chuẩn

6.1 Các ví dụ ZOI

Mục này đưa ra một số ví dụ cho thấy cách sử dụng cú pháp ZOI.

Trong các ví dụ sau, các chữ cái được sử dụng trong Pzoi, Mzoi và Izoi tương ứng với chỉ số của các phần tử liên quan đếnảnh và các phần tử không liên quan đến ảnh được báo hiệu bởi cấu trúc BAS trong DCzoi theo thứ tự chúng xuất hiện trong DCzoi.

6.1.1 Ví dụ 1

Mục này đưa ra một ví dụ về các mức phân giải lớn hơn 3 trong miền ảnh, miền ảnh đó có góc trên bên trái là (100, 120) và góc dưới bên trái (180, 210) đều bị ảnh hưởng. Trong ví dụ này cần 9 byte.

Bảng 57 - ZOI trong ví dụ 1

Tham số			Kích thước (bit)	Giá trị	Ý nghĩa
NZzoi			8 (RBAS)	1	Số vùng là 1
$Zone^0$	DCzoi		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Ảnh liên quan tới lớp mô tả
			6	101000_b	Các miền ảnh và các mức phân giải được quy định theo thứ tự
	$Pzoi^1$	$Mzoi^1$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Miền quy định không bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	00_b	Chế độ hình chữ nhật

			2	00_b	Izoi sử dụng nguyên 8 bít
			1	1_b	Izoi được mô tả theo hai kích thước
		Izoi[1]	8	0110 0100_b	Xul là 100
			8	0111 1000_b	Yul là 120
			8	1011 0100_b	Xlr là 180
			8	1101 0010_b	Ylr là 210
	Pzoi[3]	Mzoi[3]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	Phần bổ sung của các miền quy định không bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	11_b	Chế độ tối đa
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một kích thước
		Izoi[3]	8	0000 0010_b	Các mức phân giải ≤ 2 được quy định (ví dụ, với mức phân giải > 3 được quy định với chế độ tối đa và chuyển đổi bổ sung)

6.1.2 Ví dụ 2

Mục này đưa ra ví dụ mà các khối mã với các chỉ số góc trên bên trái là 5 và góc dưới bên phải là 10 trong băng con 1, mức phân giải 0 bị ảnh hưởng. Trong ví dụ này cần 10 byte.

Bảng 58 - ZOI trong ví dụ 2

Tham số		Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi		8 (RBAS)	1	Số vùng là 1
Zone[0]	DCzoi[1]	1	1_b	Đoạn căn chỉnh byte tuân theo
		1	0_b	lớp mô tả liên quan đến ảnh

			6	001000_b	Các mức phân giải được quy định
	DCzoi[2]		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	lớp mô tả liên quan đến ảnh
			6	001100_b	Các băng con và khối mã được quy định
	Pzoi[3]	Mzoi[3]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	10_b	Chế độ tối đa
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một chiều
		Izoi[3]	8	$0000\ 0000_b$	Chỉ số mức phân giải là 0
	Pzoi[9]	Mzoi[8]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	10_b	Chế độ cực đại
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một chiều
		Izoi[8]	8	$0000\ 0001_b$	Băng con 1 được quy định
	Pzoi[10]	Mzoi[9]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	00_b	Chế độ hình chữ nhật
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một chiều
		Izoi[9]	8	$0000\ 0101_b$	Chỉ số khối mã đối với ggóc trên bên trái là 5

			8	0000 1010_b	Chỉ số khối mã đối với góc dưới bên phải là 10

6.1.3 Ví dụ 3

Mục này đưa ra ví dụ mà các đoạn dữ liệu từ byte 10 cho tới byte 100 và từ byte 10000 cho tới byte 1200 bị ảnh hưởng. Trong ví dụ này cần 12 byte.

Bảng 59 - ZOI trong ví dụ 3

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	1	Số miền là 1
$Zone^0$	DCzoi		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	Đối tượng không liên quản lớp mô tả liên quan đến ảnh
			6	010000_b	Khoảng byte sau các điểm mã đánh dấu SOD được quy định
	$Pzoi^2$	$Mzoi^2$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	1_b	Nhiều phần tử được quy định
			2	01_b	Chế độ khoảng
			2	01_b	Izoi sử dụng trọn 16 bít
			1	0_b	Izoi được mô tả theo 1 chiều
		$Nzoi^2$	8	0000 0010_b	Số đoạn dữ liệu là 2
		$Izoi^{21}$	16	0000 0000_b 0000 1010_b	Vị trí byte khởi đầu là thứ 10 (bytes)
			16	0000 0000_b 0110 0100_b	Vị trí byte kết thúc là thứ 100 (bytes)
		$Izoi^{21}$	16	0010 0111_b 0001 0000_b	Vị trí byte bắt đầu là thứ 10000 (bytes)
			16	0010 1110_b 1110 0000_b	Vị trí byte kết thúc là 12000 (bytes)

6.1.4 Ví dụ 4

Mục này đưa ra ví dụ mà mức phân giải 0 bị ảnh hưởng và các đoạn byte 10 đến 100 tương ứng với dữ liệu đối với mức phân giải 0. Trong ví dụ này cần 10 byte.

Bảng 60 - ZOI trong ví dụ 4

Tham số			Kích thước(bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	1	Số vùng là 1
$Zone^0$	$DCzoi^1$		1	1_b	Đoạn căn chỉnh byte tuân theo
			1	0_b	lớp mô tả liên quan ảnh
			6	001000_b	Các mức phân giải được quy định theo thứ tự
	$DCzoi^2$		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	lớp mô tả không liên quan đến ảnh
			6	010000_b	Các khoảng byte được quy định
	$Pzoi^1$	$Mzoi^1$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	10_b	chế độ chỉ số
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo 1 hướng
		$Izoi^1$	8	$0000\ 0000_b$	Mức phân giải là 0
$Zone^0$	$Pzoi^2$	$Mzoi^2$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Các phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	01_b	Izoi sử dụng trọn 16 bít
			1	0_b	Izoi được mô tả theo một hướng
		$Izoi^1$	16	$0000\ 0000\ 0000\ 1010_b$	Vị trí byte bắt đầu là 10 (byte)

Bảng 60 - ZOI trong ví dụ 4

Tham số			Kích thước(bit)	Giá trị (theo thứ tự)	Ý nghĩa
			16	0000 0000 0110 0100_b	Vị trí byte kết thúc là 100 (bytes)

6.1.5 Ví dụ 5

Phần này đưa ra ví dụ các mức phân giải lớn hơn 3 trong những khối ảnh mà chỉ số khối ảnh trên bên trái là 0 và dưới cùng bên phải là 5, và các lớp bằng hoặc nhỏ hơn 5 ở những khối ảnh có chỉ trên bên trái là 10 và chỉ số khối ảnh dưới cùng bên phải là 15 bị ảnh hưởng. Trong ví dụ này, cần 13 byte.

Bảng 61 - ZOI trong ví dụ 5

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	2	Số vùng là 2
$Zone^0$	DCzoi		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	lớp mô tả liên quan đến ảnh
			6	01 1000_b	Các ô vuông xếp cạnh khối ảnh và các mức phân giải được quy định theo thứ tự
	$Pzoi^2$	$Mzoi^2$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Các phần tử đơn được quy định
			2	00_b	Chế độ vuông góc
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một hướng
		$Izoi^2$	8	0000 0000_b	Chỉ số của khối ảnh bên trái trên cùng là 0
			8	0000 0101_b	Chỉ số của khối ảnh bên phải dưới cùng là 5
	$Pzoi^3$	$Mzoi^3$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	Phần bù của các vùng quy định bị ảnh hưởng bởi công cụ JPSEC

Bảng 61 - ZOI trong ví dụ 5

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
			1	0_b	Phần tử đơn được quy định
			2	11_b	Chế độ tối đa
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một hướng
		Izoi[3]	8	$0000\ 0010_b$	Các mức phân giải ≤ 2 được quy định (ví dụ với các mức lớn hơn 3 được quy định với chế độ cực đại và chuyển đổi bổ sung)
Zone[1]	DCzoi		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	lớp mô tả liên quan đến ảnh
			6	010100_b	Khối ảnh và các lớp được quy định theo thứ tự
	Pzoi[2]	Mzoi[2]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	00_b	Chế độ vuông góc
			2	00_b	Izoi sử dụng trọng 8 bít
			1	0_b	Izoi được sử dụng theo một chiều
		Izoi[2]	8	$0000\ 1010_b$	Chỉ số của khối ảnh trên cùng bên trái là 10
			8	$0000\ 1111_b$	Chỉ số của "khối ảnh" bên phải dưới cùng là 15
	Pzoi[4]	Mzoi[4]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	11_b	Chế độ tối đa
			2	00_b	Izoi sử dụng trọn 8 bit
			1	0_b	Izoi được mô tả theo một hướng

Bảng 61 - ZOI trong ví dụ 5

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
		Izoi[4]	8	$0000\ 0101_b$	Các lớp ≤ 5 được quy định với chế độ cực đại

6.1.6 Ví dụ 6

Mục này đưa ra ví dụ mà đoạn mào đầu từ byte 10 đến 100 bị ảnh hưởng. Trong ví dụ này cần 8 byte.

Bảng 62 - ZOI trong ví dụ 6

Tham số			Kích thước(bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	1	Số vùng là 1
Zone[0]	DCzoi		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	lớp mô tả không liên quan đến ảnh
			6	001000_b	Các khoảng byte sau điểm mã đánh dấu SEC được quy định
	Pzoi[3]	Mzoi[3]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	01_b	Izoi sử dụng trọn 16 bit
			1	0_b	Izoi được mô tả theo một hướng
		Izoi[3]	16	$0000\ 0000$ $0000\ 1010_b$	Vị trí byte bắt đầu là 10 (bytes)
			16	$0000\ 0000$ $0110\ 0100_b$	Vị trí byte kết thúc là 100 (bytes)

6.2 Các ví dụ về mẫu thông tin khóa

6.2.1 Ví dụ 1

Bảng sau đưa ra ví dụ mà khóa bí mật đơn (128 bit) được sử dụng để giải mã một dòng mã, trong đó khóa bí mật được xác định bằng cách sử dụng URI và lấy từ máy chủ khóa dựa trên URI trong giai đoạn giải mã.

Bảng 63 - Thông tin khóa trong ví dụ 1

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
LK_{KT}		16	128	Độ dài của khóa là 128 bit
KID_{KT}		8	2	URI cho khóa bí mật được xác định
G_{KT}	PO	16	000 001 010 011 100 0_b	Thứ tự xử lý là khối ảnh – phân giải – lớp-thành phần-phân khu
	GL	8	0000 1001_b	Đơn vị bảo vệ là toàn bộ vùng được xác định trong ZOI
V_{KT}	N_V	16 (RBAS)	1	Số giá trị trong danh sách giá trị V là 1
	S_V	8 (RBAS)	19	Chiều dài thông tin khóa là 19 byte
	V1	152	https://server/file	Khóa bí mật có thể lấy từ https://server/file

6.2.2 Ví dụ 2

Bảng sau đưa ra ví dụ mà chứng thư X.509 được sử dụng để nhận thực một dòng mã, nơi mà chứng thư X.509 được nhúng vào KI_{KT} với phương pháp giải mã DER.

Bảng 64 - Thông tin khóa trong ví dụ 2

Tham số			Kích thước (bit)	Giá trị	Ý nghĩa
LK_{KT}			16	1024	Độ dại khóa là 1024 bit
KID_{KT}			8	2	Chứng thư X.509 được xác định
G_{KT}	PO		16	000 001 010 011 100 0_b	Thứ tự xử lý là khối ảnh – phân giải – lớp-thành phần-phân khu
	GL		8	0000 1001_b	Đơn vị bảo vệ là toàn bộ vùng được xác định trong ZOI
V_{KT}	N_V		16 (RBAS)	1	Số giá trị trong danh sách giá trị V là 1
	S_V		8 (RBAS)	Thay đổi	Độ dài của chứng thư X.509
	V1	ER_{KT}	8	1	Chứng thư X.509 được mã hóa với phương pháp DER
		$LCER_{KT}$	16	Thay đổi	Chiều dài của CER_{KT}

		CER_{KT}	Variable	Giá trị chứng thư	Chứng thư với khóa công khai 1024 bit được nhúng

6.2.3 Ví dụ 3

Bảng sau cho biết một khóa công khai đơn được sử dụng để xác thực một dòng mã, nơi mà khóa công được nhúng vào trong KI_{KT}.

Bảng 65 - Thông tin khóa trong ví dụ 3

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
LK_{KT}		16	1024	Chiều dài khóa là 1024 bits
KID_{KT}		8	1	Khóa công khai được xác định
G_{KT}	PO	16	000 001 010 011 100 0_b	Thứ tự xử lý là khối ảnh – phân giải – lớp-thành phần-phân khu
	GL	8	0000 1001_b	Đơn vị bảo vệ là toàn bộ vùng được xác định trong ZOI
V_{KT}	N_V	16 (RBAS)	1	Số giá trị trong danh sách giá trị V là 1
	S_V	8 (RBAS)	256	Độ dài của khóa công khai là 256 byte
	V1	2048	Giá trị khóa công khai	Khóa công khai được nhúng

6.2.4 Ví dụ 4

Bảng 66 cho biết nhiều khóa bí mật được sử dụng để mã hóa một dòng bit, nơi các khóa bí mật khác nhau được sử dụng cho các lớp khác nhau.

Bảng 66 - Thông tin khóa trong ví dụ 4

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
LK_{KT}		16	128	Độ dài khóa là 128 bit
KID_{KT}		8	3	URI cho khóa bí mật được xác định
G_{KT}	PO	16	000 001 010 011 1000_b	Thứ tự xử lý là khối ảnh – phân giải – lớp-thành phần-phân khu

	GL	8	$0000\ 0100_b$	Đơn vị bảo vệ là lớp
V_{KT}	N_V	16 (RBAS)	3	Số giá trị trong danh sách giá trị V là 3
	S_V	8 (RBAS)	16	Độ dài của mỗi Vn là 16 byte
	V1	128	https://server/1	Khóa bí mật đối với lớp 1 có thể lấy từ https://server/1
	V2	128	https://server/2	Khóa bí mật đối với lớp 2 có thể lấy từ https://server/2
	V3	128	https://server/3	Khóa bí mật đối với lớp 3 có thể lấy từ https://server/3
	V4	128	https://server/4	Khóa bí mật đối với lớp 4 có thể lấy từ https://server/4

6.3 Các ví dụ về công cụ chuẩn tắc JPSEC

Các ví dụ sau đây mô tả cách mà ZOI và các mẫu khóa có thể được sử dụng để thực hiện các dịch vụ bảo mật cơ bản như mã hóa và nhận thực trên ảnh được mã theo JPEG 2000

6.3.1 Ví dụ 1

Một ảnh được mã hóa với JPEG 2000 và có ba độ phân giải. Trong ví dụ này, độ phân giải thứ nhất không được mã hóa để cho phép xem trước, và các độ phân giải thứ 2 và thứ 3 được mã hóa với các khóa tương ứng k1 và k2. Ảnh đầu vào trong trường hợp này được mã hóa theo thứ tự tiến trình và có 1 khối ảnh, 3 độ phân giải, 3 lớp, các thành phần Nc và các giới hạn Np (số thành phần và phạm vi không quan trọng trong ví dụ cụ thể này). Việc mã hóa được thực hiện bằng cách sử dụng AES trong chế độ CBC mà không cần đệmsử dụng khóa k0 để mã độ phân giải 1 và sử dụng khóa k2 để giải mã độ phân giải 2, và độ phân giải 0 còn lại không được mã hóa.

JPSEC báo hiệu cách mà một người dùng JPSEC nên giải mã dòng mã. Đầu tiên, ID mẫu công cụ đối với khuôn mẫu giải mã này được báo hiệu. Hai ZOI được nhận ra cho độ phân giải 1 và khoảng byte tương ứng của nó B1-B2, và độ phân giải 2 và khoảng byte tương ứng B2- B3. Các tham số khuôn mẫu giải mã này chỉ ra rằng việc mã hóa AES được áp dụng mà không có đệm. Thông tin khóa và thực tế là các khóa khác nhau được áp dụng cho các độ phân giải khác nhau được báo hiệu với các tham số thông tin khóa. Quan trọng là độ chi tiết khóa được quy định như độ phân giải do đó mỗi độ phân giải có một khóa khác nhau, nơi mà thứ tự tiến trình được báo hiệu như TRLCP. Thông tin khóa đối với mỗi độ phân giải được chứa trong danh sách giá trị khóa. Việc mã hóa được thực hiện trên dòng mã, mã hóa cả mào đầu gói và thân gói. Mã hóa độ chi tiết là một giải pháp, tại đó tiến trình được thực hiện theo thứ tự TRLCP, thứ tự đó giống như dòng mã ban đầu. Do hai độ phân giải được mã hóa tách biệt, nên hai véc tơ khởi tạo (Ivs) được yêu cầu và chúng được chứa trong danh sách giá trị.

Chú ý rằng các kết quả văn bản mật mã của gói tin được quy định bởi thứ tự tiến trình và do đó không phụ thuộc vào thứ tự tiến trình của dòng mã đầu vào, tuy nhiên vị trí của các gói được mã hóa ở dòng mã đầu ra tuân theo thứ tự của các gói dòng mã đầu vào.

Bảng 67 - Đoạn mã đánh dấu SEC cho ví dụ 1

Tham số			Kích thước (bit)	Giá trị	Ý nghĩa
SEC			16	0xFF65	Mã đánh dấu SEC
L_{SEC}			16 (RBAS)	0x82	Độ dài của đoạn mã đánh dấu SEC là 130 byte
Z_{SEC}			8 (RBAS)	0	Chỉ số của đoạn mã đánh dấu này
P_{SEC}	F_{PSEC}		1	0_b	Cấu trúc FBAS không tuân theo
		F_{INSEC}	1	0_b	INSEC không được sử dụng
		$F_{multiSEC}$	1	0_b	Một đoạn mã đánh dấu SEC được sử dụng
		F_{mod}	2	00_b	Dữ liệu JPEG 2000 ban đầu đã bị chỉnh sửa
		F_{TRLCP}	1	0_b	Việc sử dụng mã đánh dấu TRLCP không được xác định trong Psec
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	Số công cụ bảo mật là 1
	I_{max}		8 (RBAS)	0000000_b	Chỉ số mẫu công cụ cực đại là 0
t			8 (FBAS)	0	Công cụ chuẩn tắc JPSEC
i			8 (RBAS)	0	Chỉ số mẫu công cụ
ID_T			8	1	Khuôn mẫu giải mã
L_{zoi}			16 (RBAS)	0x17	Độ dài của ZOI là 23 byte
ZOI			184	Xem bảng 68	Vùng ảnh hưởng đối với công cụ này
L_{PID}			16 (RBAS)	0x5e	Chiều dài của P_{ID} là 94 btye
P_{ID}			752	Xem bảng 69	Các tham số đối với kỹ thuật này

Bảng 68 - Ví dụ ZOI

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	2	Số vùng là 1
Zone 0	DC_{ZOI}^{1}		1	1_b	Đoạn căn chỉnh byte tuân theo
			1	0_b	lớp mô tả liên quan đến ảnh
			6	001000_b	Độ phân giải được quy định
	DCzoi[2]		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	Đối tượng không ản liên quan lớp mô tả
			6	010000_b	Các khoảng byte sau điểm đánh dấy SOD được quy định
	$Pzoi^{0,1}$	$Mzoi^{1}$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	10_b	Chế độ chỉ số
			2	00_b	Izoi sử dụng trọn 8 bít
			1	0_b	Izoi được mô tả theo một hướng
		I_{ZOI}	8	0000 0001_b	Độ phân giải 1 được quy định
	$Pzoi^{0,2}$	$Mzoi^{2}$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hương bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	01_b	Izoi sử dụng trọng 16 bít
			1	0_b	Izoi được mô tả theo một hướng
		$Izoi^{21}$	16	0x31CC	Vị trí byte khởi đầu là 12748 (byte). (B0)
			16	0xA3E8	Vị trí byte kết thúc là 41960 (byte). (B1)
Zone	DC_{ZOI}^{1}		1	1_b	đoạn căn chỉnh byte tuân theo

1			1	0_b	lớp mô tả liên quan đến ảnh
			6	001000_b	Độ phân giải được quy định
	DCzoi[2]		1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	1_b	Đối tượng không phải lớp mô tả liên quan đến ảnh
			6	010000_b	Các khoảng byte sau điểm mã đánh dấu SOD được quy định
	Pzoi[0, 1]	Mzoi[1]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Các phần tử đơn được quy định
			2	10_b	Chế độ chỉ số
			2	00_b	Izoi sử dụng trọn 8 bit
			1	0_b	Izoi được mô tả theo một hướng
		Izoi[1]	8	0000 0010$_b$	Độ phân giải 2 được quy định
	Pzoi[0, 2]	Mzoi[2]	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụi JPSEC
			1	0_{b2}	Phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	10_b	Izoi sử dụng trọn 32 bit
			1	0_b	Izoi được mô tả theo một hướng
		Izoi[2]	32	0xA3EE	Vị trí byte khởi đầu là 41966 (byte). (B2)
			32	0x21101	Vị trí byte kết thúc là 135425 (byte). (B3)

Bảng 69 - Ví dụ P_{ID}

Tham số	Kích thước (bit)	Giá trị	Ý nghĩa
T_{ID}	432	Xem Bảng 70	Các khuôn mẫu giải mã

PD		8 (FBAS)	0_b	Đoạn căn chỉnh byte không tuân theo
			0_b	Miền điểm ảnh không được sử dụng
			0_b	Miền hệ số sóng con không được sử dụng
			0_b	Miền hệ số sóng con đã lượng tử hóa không được sử dụng
			1_b	Miền dòng mã được sử dụng
			000_b	Dành cho việc sử dụng tiêu chuẩn ISO
F_{PD}		8 (FBAS)	0_b	byte FBAS không tuân theo
			1_b	Chỉ phần thân gói được mã hóa
			000000_b	Dành cho việc sử dụng tiêu chuẩn ISO
G	PO	16	000 001 010 011 100 0_b	Thứ tự tiến trình là khối ảnh-độ phân giải - lớp – thành phần – phạm vi
	GL	8	0000 0011_b	Đơn vị bảo vệ là mức phân giải
V	N_V	16 (RBAS)	2	Số giá trị trong danh sách giá trị V là 2
	S_V	8 (RBAS)	16	Độ dài của mỗi Vn là 16 byte
	V1	128	IV0	Giá trị véc tơ khởi tạo đối với R1
	V2	128	IV1	Giá trị véc tơ khởi tạo đối với R2

Bảng 70 - Ví dụ về khuôn mẫu giải mã

Tham số		**Kích thước**	**Giá trị (theo thứ tự)**	**Ý nghĩa**
ME_{decry}		8	0	Mô phỏng mã đánh dấu đã xảy ra
CT_{decry}		16	0001_b	Mật mã khối (AES)
CP_{decry}	M_{bc}	6	100000_b	Chế độ CBC. Các bit không được đệm
	P_{bc}	2	00_b	Việc đánh cắp bản mã
	SIZ_{bc}	8	16	Kích thước khối (16 bytes, 128 bits)
	KT_{bc}	392	Xem Bảng 71	Mẫu khóa

Bảng 71 - Ví dụ về mẫu khóa

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
LK_{KT}		16	128	Độ dài khóa là 128 bit
KID_{KT}		8	2	URI cho khóa bí mật
G_{KT}	PO	16	0 000 001 010 011 100_b	Thứ tự tiến trình là khối ảnh-độ phân giải - lớp – thành phần – ngoại vi
	GL	8	$0000\ 0011_b$	Đơn vị bảo vệ là mức độ phân giải
V_{KT}	N_V	32 (RBAS)	2	Số giá trị trong danh sách giá trị v là 2
	S_V	8 (RBAS)	19	Độ dài của mỗi Vn là 19 byte
	V1	152	https://server/key1	Khóa bí mật đối với độ phân giải mức 1 có thể lấy từ https://server/key1
	V2	152	https://server/key2	Khóa bí mật đối với độ phân giải mức 2 có thể lấy từ https://server/key2

6.3.2 Ví dụ 2

Trong trường hợp này, việc nhận thực được áp dụng cho cùng ảnh được mã hóa bởi JPEG 2000 ở trên. Trong ví dụ này, cả ba độ phân giải và ba lớp trên một độ phân giải được nhận thực, ở đó việc nhận thực của mỗi độ phân giải sử dụng một khóa khác nhau. Do có ba độ phân giải nên có 3 khóa và có ba lớp cho một độ phân giải nên sẽ có ba giá trị MAC cho mỗi độ phân giải. Vì thế tổng giá trị MAC là 9 đối với mỗi thực thể ảnh JPSEC. Cụ thể:

Độ phân giải 0 có các giá trị MAC là M0, M1, M2 (mỗi giá trị cho một lớp) sử dụng khóa 0

Độ phân giải 1 có các giá trị MAC là M3, M4, M5 (mỗi giá trị cho một lớp) sử dụng khóa 1

Độ phân giải 2 có các giá trị MAC là M6, M7, M8 (mỗi giá trị cho một lớp) sử dụng khóa 2

Ví dụ này minh họa việc nhận thực có thể được báo hiệu cũng như độ linh hoạt được cung cấp bởi ZOI và chi tiết công cụ. Vì trong ví dụ trước, ảnh đầu vào được mã hóa theo thứ tự tiến trình RLCP và có 1 khối ảnh, 3 độ phân giải, ba lớp, các thành phần Nc và các giới hạn Np (số thành phần và giới hạn không quan trọng trong ví dụ cụ thể này). Việc nhận thực được thực hiện bằng cách sử dụng HMAC với SHA – 1.

JPSEC báo hiệu cách một người sử dụng JPSEC co thể xác minh hoặc nhận thực nội dung được bảo vệ của JPSEC. Đầu tiên, ID mẫu công cụ đối với mẫu xác thực được báo hiệu. Sau đó ZOI được sử dụng để báo hiệu rằng có ba độ phân giải và các khoảng byte được liên kết đối với mỗi độ phân giải. CÁc tham số mẫu cho việc nhận thực này báo hiệu rằng HMAC được áp dụng bằng cách sử dụng SHA – 1. Mẫu thông tin khóa cung cấp thông tin về khóa bao gồm cả chi tiết khóa là độ phân giải và

cung cấp thông tin cho ba khóa trong danh sách giá trị đối với các khóa. Miền xử lý đối với việc nhận thực được quy định như dòng mã bao gồm cả mào đầu gói. Chi tiết công cụ cho việc nhận thực được quy định như lớp, vì có ba MAC đối với mỗi độ phân giải, tổng là có 9 giá trị MAC. Thứ tự tiến trình như trên đã được xác định là TRLCP, nó giống với thứ tự dòng mã ban đầu.

Chú ý rằng sử dụng thứ tự tiến trình trong phần độ chi tiết đảm bảo rằng các giá trị MAC giống nhau sẽ cho kết quả độc lập với thứ tự tiến trình của dòng mã.

Lưu lý rằng trong khi ví dụ này chứng minh việc sử dụng các MAC, một tiếp cận tương tự có thể được sử dụng để báo hiệu việc sử dụng nhiều chữ ký số.

Bảng 72 - Đoạn mã đánh dấu SEC

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
SEC			16	0xFF65	Mã đánh dấu SEC
L_{SEC}			16	0x0099	Độ dài của đoạn mã đánh dấu SEC
Z_{SEC}			8 (RBAS)	0	Chỉ số của đoạn mã đánh dấu SEC này
P_{SEC}	F_{PSEC}		1	0_b	Cấu trúc FBAS không tuân theo
		F_{INSEC}	1	0_b	Đoạn mã đánh dấu INSEC không được sử dụng
		$F_{multiSEC}$	1	0_b	Chỉ một đoạn mã đánh dấu SEC trong dòng mã này.
		F_{mod}	1	0_b	Dữ liệu JPEG 2000 nguyên bản không bị chỉnh sửa
		F_{TRLCP}	1	0_b	Gán thẻ TRLCP không được sử dụng
		Padding	3	000_b	Gán thẻ TRLCP không được sử dụng
	N_{tools}		7	1	Chỉ một công cụ được sử dụng trong dòng mã này
	I_{max}		7	0	Chỉ số mẫu công cụ tối đa là 0
$Tool^0$	t		8 (FBAS)	0	Công cụ chính tắc của JPSEC
	i		8 (RBAS)	0	Chỉ số mẫu công cụ
	ID_T		8	2	Công cụ thông tin này sử dụng một mẫu xác thực

	L_{ZOI}	16 (RBAS)	0x20	Độ dài của ZOI là 32 byte
	ZOI	256	Bảng 73	Vùng được phủ của ảnh
	L_{PID}	16 (RBAS)	0x6c	Độ dài của P_{ID} là 108 byte
	P_{ID}	928	Table 74	Các tham số cho công cụ JPSEC

Bảng 73 - Việc báo hiệu ZOI

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	1	Số vùng là 1
Zone^0	DC_{zoi}^1		1	1_b	Đoạn căn chỉnh byte tuân theo
			1	0_b	Ảnh liên quan lớp mô tả
			6	001000_b	Các mức độ phân giải được quy định theo thứ tự
	DC_{zoi}^2		1	0_b	Đoạn cản chỉnh byte không tuân theo
			1	1_b	Đối tượng không phải ảnh liên quan đến lớp mô tả
			6	010000_b	Các khoảng byte được quy định
	$Pzoi^{0,1}$	$Mzoi^1$	1	0_b	Đoạn căn chỉnh byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC.
			1	0_b	Phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	00_b	Izoi sử dụng trọn 8 bit
			1	0_b	Izoi được mô tả theo một hướng
		$Izoi^1$	8	0	Khởi đầu của khoảng này là 0
			8	2	Kết thúc của khoảng này là 2
Zone^0	$Pzoi^{0,2}$	$Mzoi^2$	1	0_b	Đoạn căn chỉnh byte không tuân theo

Bảng 73 - Việc báo hiệu ZOI

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
			1	0_b	Các vùng quy định bị ảnh hưởng bởi công cụ JPSEC.
			1	1_b	Nhiều phần tử được quy định
			2	01_b	Chế độ khoảng
			2	10_b	Izoi sử dụng trọn 32-bit
			1	0_b	Izoi được mô tả theo một hướng
		N_{ZOI}	8 (RBAS)	3	Số lượng I_{ZOI} là 3
		$Izoi^1$	32	104	Vị trí byte khởi đầu là 104 (bytes)
			32	12762	Vị trí byte kết thúc là 12762 (bytes)
		I_{ZOI}^2	32	12768	Vị trí byte khởi đầu là 12768 (bytes)
			32	41980	Vị trí byte kết thúc là 41980 (bytes)
		I_{ZOI}^3	32	41986	Vị trí byte khởi đầu là 41986 (bytes)
			32	135445	Vị trí byte kết thúc là 135445 (bytes)

Bảng 74 - Các tham số báo hiệu P_{ID}

Tham số				Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
T_{auth}	M_{auth}			8	0	Các phương pháp xác thực: xác thực dựa trên việc băm
	P_{auth}	M_{HMAC}		8	1	HMAC được sử dụng để xác thực
		H_{HMAC}		8	1	SHA-1 được sử dụng cho việc băm
		KT_{HMAC}	LK_{KT}	16	128	Độ dài khóa tính theo đơn vị bit
			KID_{KT}	8	3	KI_{KT} chứa URI đối với khóa riêng

Bảng 74 - Các tham số báo hiệu P_{ID}

Tham số					Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
			G_{KT}	PO	16	0 000 001 010 011 100_b	Thứ tự xử lý là khối ảnh-phân giải-lớp-thành phần-phân khu
				GL	8	00000011_b	Độ chi tiết khóa là phân giải
			V_{KT}	Nv	16 (RBAS)	3	Có ba khóa trong danh sách này
				S_V	8 (RBAS)	8	Kích thước của mỗi khóa là 8 byte
				VL	64	*Key0*	Khóa đầu tiên là key0, cho độ phân giải 0
					64	*Key1*	Khóa thứ hai là key1, cho độ phân giải 1
					64	*Key2*	Khóa thứ ba là key3, cho độ phân giải 3
		SIZ_{HMAC}			16	20	Kích thước của MAC là 20
PD					8 (FBAS)	0_b	Đoạn căn chỉnh byte không tuân theo
						0_b	Miền điểm ảnh không được sử dụng
						0_b	Miền hệ số sóng con không được sử dụng
						0_b	Miền hệ số Sóng con lượng tử hóa không được sử dụng
						1_b	Miền dòng mã được sử dụng
						000_b	Dành riêng cho việc sử dụng tiêu chuẩn ISO
F_{PD}					8 (FBAS)	0_b	Byte FBAS không tuân theo
						0_b	Cả mào đầu và thân gói đều được mã hóa

Bảng 74 - Các tham số báo hiệu P_{ID}

Tham số		Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
			000000_b	Dành riêng cho việc sử dụng tiêu chuẩn ISO
G	PO	16	0000010100111000_b	Thứ tự xử lý là khối ảnh-phân giải-lớp-thành phần-phân khu
	GL	8	00000100_b	Độ chi tiết của công cụ là lớp
V	N_V	32 (RBAS)	9	Có 9 MACs (3 MACs trên một độ phân giải)
	S_V	8 (RBAS)	20	Kích thước của mỗi MAC là 20 bytes
	VL	160	*M*0	MAC đầu tiên là *M*0
		160	*M*1	MAC thứ hai là *M*1
		160	*M*2	MAC thứ ba là *M*2
		160	*M*3	MAC thứ tư là *M*3
		160	*M*4	MAC thứ năm là *M*4
		160	*M*5	MAC thứ sáu là *M*5
		160	*M*6	MAC thứ bảy là *M*6
		160	*M*7	MAC thứ tám là *M*7
		160	*M*8	MAC thứ chín là *M*8

6.4 Các ví dụ trường méo

Mục này đưa ra một số ví dụ đơn giản về việc sử dụng trường méo.

6.4.1 Ví dụ 1

Ví dụ này được xây dựng dựa trên ví dụ 3 về ZOI trong 6.1.3 để cho thấy cách các giá trị méo có thể được liên kết với hai đoạn dữ liệu được báo hiệu bởi ZOI trong ví dụ trên như thế nào. Như đã tranh luận, ví dụ 3 trong 6.1.3 báo hiệu hai đoạn dữ liệu: (1) byte số 10 đến 100 và (2) byte 10000 cho đến 12000. Để gắn các trường méo với hai đoạn dữ liệu này cần hai bước. Thứ nhất, trường méo được báo hiệu trong Dczoi. Thứ hai, các giá trị méo được báo hiệu bằng cách sử dụng Pzoi[2]. Vì thế chỉ những thay đổi tới ví dụ 3 trong 6.1.3 là để thiết lập bít trường méo trong Dczoi, và Pzoi2 (9 dòng cuối trong bảng 75)

Bảng 75 - Việc gắn kết trường méo với hai đoạn dữ liệu

(phần mở rộng của ví dụ 3 về ZOI trong 6.1.3)

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi			8 (RBAS)	1	Số vùng là 1
$Zone^0$	DCzoi		1	0_b	Đoạn căn chỉnh byte này không tuân theo
			1	1_b	Đối tượng không phải là lớp mô tả liên quan đến ảnh
			6	010001_b	Các khoảng byte sau điểm mã đánh dấu SOD được quy định và các trường méo có liên kết được quy định
	$Pzoi^2$	$Mzoi^2$	1	0_b	Đoạn căn chỉnh byte này không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	1_b	Các phần tử đa được quy định
			2	01_b	Chế độ khoảng
			2	01_b	Izoi sử dụng 16 bit
			1	0_b	Izoi được mô tả theo một hướng
		$Nzoi^2$	8 (RBAS)	2	Số đoạn dữ liệu là 2
		$Izoi^{2,1}$	16	0000 0000 0000 1010_b	Vị trí byte bắt đầu là 10 (bytes)
			16	0000 0000 0110 0100_b	Vị trí byte kết thúc là 100 (bytes)
$Zone^0$	$Pzoi^2$	$Izoi^{2,2}$	16	0010 0111 0001 0000_b	Vị trí byte bắt đầu là 10000 (bytes)
			16	0010 1110 1110 0000_b	Vị trí byte kết thúc là 12000 (bytes)

Bảng 75 - Việc gắn kết trường méo với hai đoạn dữ liệu

(phần mở rộng của ví dụ 3 về ZOI trong 6.1.3)

Tham số			Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
	Pzoi[6]	Mzoi[6]	1	0_b	Đoạn căn chỉnh byte này không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	1_b	Các phần tử đa được quy định
			2	10_b	Chế độ chỉ số
			2	00_b	Izoi sử dụng 8 bit để biểu diễn mỗi một giá trị méo
			1	0_b	Izoi được mô tả theo một hướng
		Nzoi[6]	8 (RBAS)	2	Số lượng đoạn dữ liệu là 2
		Izoi[6,1]	8	D1 value	Giá trị méo cho đoạn đầu tiên
		Izoi[6,2]	8	D2 value	Giá trị méo cho đoạn thứ hai

6.4.2 Ví dụ 2

Ví dụ này mô tả cách mà các giá trị méo có thể được liên kết với các gói JPEG 2000. Dczoi quy định phạm vi của 4 gói và trường méo cũng được báo hiệu. Pzoi[1] cung cấp phạm vi của các gói và Pzoi[2] mô tả méo được liên kết với mỗi gói này. Chú ý rằng do Pzoi1 quy định khoảng dài 4 và Pzoi2 quy định 4 giá trị, mỗi phần tử trong phạm vi này được liên kết với một giá trị, như mỗi gói được liên kết với một méo.

Bảng 76 - Báo hiệu một loạt các gói dữ liệu và liên kết méo cho mỗi gói tin

Tham số		Kích thước (bit)	Giá trị (theo thứ tự)	Ý nghĩa
NZzoi		8 (RBAS)	1	Số vùng là 1
Zone[0]	DCzoi	1	0_b	Đoạn căn chỉnh byte này không tuân theo
		1	1_b	Đối tượng không lớp mô tả liên quan đến ảnh

			6	100001_b	Các gói được quy định và các trường méo có liên kết được quy định
	Pzoi[1]	Mzoi[1]	1	0_b	Đoạn căn chỉnh byte này không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	0_b	Phần tử đơn được quy định
			2	01_b	Chế độ khoảng
			2	00_b	Izoi sử dụng trọn 8 bit
			1	0_b	Izoi được mô tả theo một hướng
		Nzoi[1]	8 (RBAS)	1	Số đoạn dữ liệu là 1
		Izoi[11]	8	$0000\ 0000_b$	Gói bắt đầu là số 0
			8	$0000\ 0011_b$	Gói kết thúc là số 3
	Pzoi[6]	Mzoi[6]	1	0_b	Đoạn căn chỉnh byte này không tuân theo
			1	0_b	Các miền quy định bị ảnh hưởng bởi công cụ JPSEC
			1	1_b	Các phần tử đa được quy định
			2	10_b	Chế độ chỉ số
			2	00_b	Izoi sử dụng 8 bit để biểu diễn mỗi một giá trị méo
			1	0_b	Izoi được mô tả theo một hướng
		Nzoi[6]	8 (RBAS)	4	Số lượng đoạn dữ liệu là 4
		Izoi[6,1]	8	Giá trị D1	Giá trị méo đối với gói đầu tiên
		Izoi[6,2]	8	Giá trị D2	Giá trị méo đối với gói thứ hai
		Izoi[6,3]	8	Giá trị D3	Giá trị méo đối với gói thứ ba
		Izoi[6,4]	8	Giá trị D4	Giá trị méo đối với gói thứ tư

7 Tổ chức đăng ký JPSEC

7.1 Giới thiệu chung

Cơ chế đăng ký JPSEC cung cấp cho việc định danh rõ ràng các công cụ bảo mật không quy chuẩn mà tuân theo chuẩn JPSEC và tiếp tục được đề xuất hoặc phát triển như các công cụ JPSEC không quy chuẩn, bổ sung vào công cụ được liệt kê trong Phụ lục B. Việc đăng ký này được thực hiện bởi Cơ quan đăng ký JPSEC. Nó phải phù hợp với các chỉ dẫn JTC 1. Việc đăng ký các công cụ JPSEC mới này được giám sát bởi quy trình được định nghĩa trong tiểu mục này.

Các ứng viên có thể đệ trình các công nghệ mà họ muốn, đã có trong danh sách tham khảo của JPSEC. CHÚ THÍCH rằng việc sử dụng công cụ JPSEC được xác định với một mã đánh dấu JPSEC biểu diễn trong dòng mã. Khi một ứng dụng tìm thấy một ID JPSEC không rõ, nó có thể nối với JPSEC RA và nhận được thông tin đăng ký cho công cụ đó.

7.2 Tiêu chí đủ điều kiện của ứng viên đăng ký

Các ứng viên đủ điều kiện là các tổ chức được công nhận bởi các cơ quan chứng nhận quốc gia.

7.3 Đơn đăng ký

Các đơn đăng ký công cụ JPSEC mới sẽ được công bố bởi Cơ quan đăng ký JPSEC trên trang web.

Website này phải có các mẫu cho đơn đăng ký, yêu cầu cập nhật, thông báo chuyển nhượng hoặc cập nhật, hoặc là từ chối đơn.

Tất cả các mẫu phải bao gồm:

- Tên của tổ chức ứng viên;
- Địa chỉ của tổ chức ứng viên;
- Tên, chức danh, địa chỉ bưu điện/địa chỉ email, số điện thoại/số fax của người liên lạc trong tổ chức đó.

Mẫu đơn đăng ký và yêu cầu cập nhật cũng cần phải có những thành phần sau:

- Tên công cụ JPSEC (bắt buộc)
- Loại công cụ JPSEC, ví dụ như chữ ký số, tạo thủy vân, mã hóa, xáo trộn, tạo và quản lý khóa, xác thực (tùy chọn).
- Tóm tắt mô tả kỹ thuật (bắt buộc).
- Mô tả tổng quan công cụ (bắt buộc).
- Mô tả ví dụ hoạt động trường hợp sử dụng (lựa chọn).
- Đặc tả cú pháp các tham số, bao gồm các giá trị khả dĩ (tùy chọn).
- Hướng dẫn sử dụng hiệu quả (tùy chọn).
- Các trạng thái sở hữu trí tuệ, ví dụ như chủ sở hữu, quyền chủ sở hữu (tùy chọn).
- Điều kiện sử dụng sở hữu trí tuệ (bắt buộc).

- Các hạn chế sử dụng, ví dụ, các điều kiện xuất khẩu (tùy chọn)
- Thông tin cho việc thực hiện tải về (tùy chọn).
- Các góp ý bổ sung, động cơ thúc đẩy, các tham chiếu... (tùy chọn).
- Các yêu cầu về độ tin cậy của các mục đơn được chọn (tùy chọn)
- Khoảng thời gian yêu cầu để đăng ký công cụ (tùy chọn)

Cơ quan đăng ký JPSEC phải cung cấp các tài liệu hướng dẫn để hỗ trợ các ứng viên chuẩn bị đơn.

7.4 Đánh giá và phản hồi đơn

Điều này định nghĩa quy trình để Cơ quan đăng ký JPSEC đánh giá và phản hồi lại các đơn để đảm bảo không xảy ra sai sót.

Một ủy ban đánh giá kỹ thuật được thành lập để đánh giá các đơn. Ủy ban này là sự kết hợp giữa các thành viên ISO/IEC JTC 1/SC 29/WG 1 và các thành viên của cơ quan đăng ký JPSEC. Ủy ban đánh giá sẽ kiểm tra các đơn tại cuộc họp WG, cuộc họp này diễn ra không quá 9 tháng kể từ khi đơn được đệ trình.

Ủy ban đánh giá chấp nhận hoặc từ chối đơn, dựa trên các tiêu chí để từ chối được đưa ra trong 7.5.

Nếu được chấp nhận, công cụ JPSEC mới này sẽ được cấp một định danh (ID) trong khoảng thời gian quy định. Cú pháp ID đó phải phù hợp với 5.6.3. Ủy ban đánh giá phê duyệt thông tin mô tả công cụ JPSEC được liệt kê ra trong 7.3. Sau đó, ID này sẽ được sử dụng để báo hiệu trong dòng mã của JPSEC.

Khi đơn được đánh giá và chấp nhận, JPSEC RA thông báo cho ứng viên phản hồi tích cực hoặc không tích cực choi yêu cầu đăng ký. Phản hồi cho các ứng viên này phải bao gồm lời giải thích ngắn gọn về kết quả của đánh giá kỹ thuật và phải gửi lại cho ứng viên trong khoảng thời gian không quá chín tháng sau ngày nộp đơn.

Phản hồi không tích cực có thể bị khiếu nại nếu như người đăng ký tin là có sai sót nào đó trong quyết định từ chối, hoặc khi cần thêm thông tin để làm rõ vấn đề hoặc quan tâm. Nếu người đăng ký yêu cầu đánh giá bổ sung ngoài quy trình của Ủy ban đánh giá thì ứng viên đó có thể gửi trường hợp của mình cho Ủy ban WG 1 để đánh giá trong cuộc họp nhóm WG 1 tiếp theo. Sau đó, ứng viên đó có thể được các chuyên gia dưới quyền WG 1yêu cầu cung cấp thông tin bổ sung và các chuyên gia sẽ đưa ra kết luận cuối cùng chấp nhận hay là từ chối. Để một đơn bị từ chối được WG 1 đánh giá lại thì người nộp đơn phải nộp lại đề nghị thông qua cơ quan quốc gia để xác định tại sao yêu cầu đệ trình đòi hỏi phải xem xét bởi WG 1.

7.5 Từ chối đơn

Tiêu chí từ chối một đơn đăng ký như sau:

- Ứng viên không đủ điều kiện.

– Không thanh toán các lệ phí cần thiết (khi thích hợp)

– Mục đăng ký và phê duyệt đã tồn tại và chứa các nội dung định danh của đệ trình.

– Thông tin trong đơn không đầy đủ hoặc thông tin không thể hiểu được.

– Giải trình đưa vào đăng ký không đầy đủ. Công cụ JPSEC ứng cử phải chứng minh là nó cung cấp dịch vụ bảo mật hữu ích và đưa ra ví dụ các trường hợp sử dụng khi thích hợp.

– Cơ quan đăng ký đánh công cụ được đề xuất không đủ mới (độc đáo), công cụ này có thể dễ dàng được thực hiện với mục đang có và đã được phê duyệt.

– Việc nộp đơn có sai sót hoặc không phù hợp với tiêu chuẩn hoặc thông số kỹ thuật JPSEC quy chuẩn .

– Mô tả kỹ thuật chưa đủ.

– Điều kiện tính bảo mật không phù hợp.

7.6 Phân bổ định danh và ghi các định nghĩa đối tượng

Quy trình đánh giá và cú pháp ở trên đảm bảo rằng ID được cấp là duy nhất trong bộ đăng ký và ID này không được cấp cho đối tượng khác.

Sau khi cấp, ID đó và thông tin liên quan phải được đưa vào bộ đăng ký và cơ quan đăng ký JPSEC phải thông báo cho ứng viên được cấp trong vòng chín tháng.

Định nghĩa công cụ JPSEC phải được ghi trong bộ đăng ký khi ID được cấp.

7.6.1 Tái sử dụng các ID

Định danh có thể được tái sử dụng bởi cơ quan đăng ký. Ví dụ, các dđịnh danh sẵn sàng để tái sử dụng sau khi chúng hết hạn hoặc khi chúng bị bỏ 1 cách tự nguyện bỏ hoặc bị thu hồi.

Chủ sở hữu ID có thể tự nguyện bỏ ID của mình thông qua yêu cầu cập nhật.

7.6.2 Thu hồi

Cơ quan đăng ký JPSEC có thể thu hồi định danh vì lý do kỹ thuật hoặc do sử dụng sai công cụ. Khi đó, chủ sở hữu định danh sẽ được thông báo bởi thông báo cập nhật

7.7 Bảo trì

Để bảo trì một đăng ký, cơ quan đăng ký JPSEC phải thực hiện các cơ chế để duy trì tính toàn vẹn của đăng ký bao gồm việc sao lưu đầy đủ hồ sơ.

Chủ sở hữu ID phải cập nhật thông tin công cụ JPSEC có liên quan thông qua yêu cầu cập nhật.

Cơ quan đăng ký JPSEC phải cung cấp các cơ chế để duy trì tính bảo mật của các thành phần như trong đơn đăng ký.

7.8 Công bố đăng ký

Thông thường, cộng đồng người dùng công nghệ thông tin và truyền thông được phục vụ tốt nhất nếu thông tin đăng ký được công khai. Tuy nhiên trong một số trường hợp, cần bảo mật một số hoặc toàn bộ dữ liệu liên quan đến việc đăng ký cụ thể, hoặc vĩnh viễn hoặc là một phần nào đó của quy trình đăng ký.

Cơ quan đăng ký JPSEC sẽ công khai thông tin đăng ký theo cách phù hợp với yêu cầu tính bảo mật của công cụ JPSEC.

Trường hợp công bố được yêu cầu, bắt buộc phải có phiên bản giấy hoặc phiên bản điện tử. Nếu cơ quan đăng ký JPSEC cung cấp công bố, thì họ phải lưu giữ các bản ghi phân phối một cách chính xác liền quan đến công bố của họ.

7.9 Các yêu cầu về thông tin đăng ký

Cơ quan đăng ký JPSEC phải công bố dạng điện tử danh sách các công cụ JPSEC không quy chuẩn trong bộ đăng ký của họ, cũng như những thông tin liên quan tới chúng theo cách phù hợp với yêu cầu tính bảo mật của công cụ JPSEC.

Các thông tin sau đây phải có trong bộ đăng ký đối cho mỗi công cụ JPSEC:

- ID được cấp;
- Tên của ứng viên khởi tạo;
- Địa chỉ của ứng viên khởi tạo;
- Ngày cấp phát gốc;
- Ngày chuyển giao cuối cùng của cấp phát, nếu được phép (có thể cập nhật);
- Tên của chủ sở hữu hiện tại (có thể cập nhật);
- Địa chỉ của chủ sở hữu hiện tại (có thể cập nhật);
- Tên, chức danh, địa chỉ bưu điện/email, số điện thoại/fax của người liên lạc trong tổ chức (có thể cập nhật);
- Ngày cập nhật sau cùng (có thể cập nhật).

Bộ đăng ký cũng phải chứa thông tin được cung cấp bởi ứng viên về công cụ JPSEC như quy định trong 7.3 cũng như các thông tin chính.

Phụ lục A

(Quy định)

Các hướng dẫn và các trường hợp sử dụng

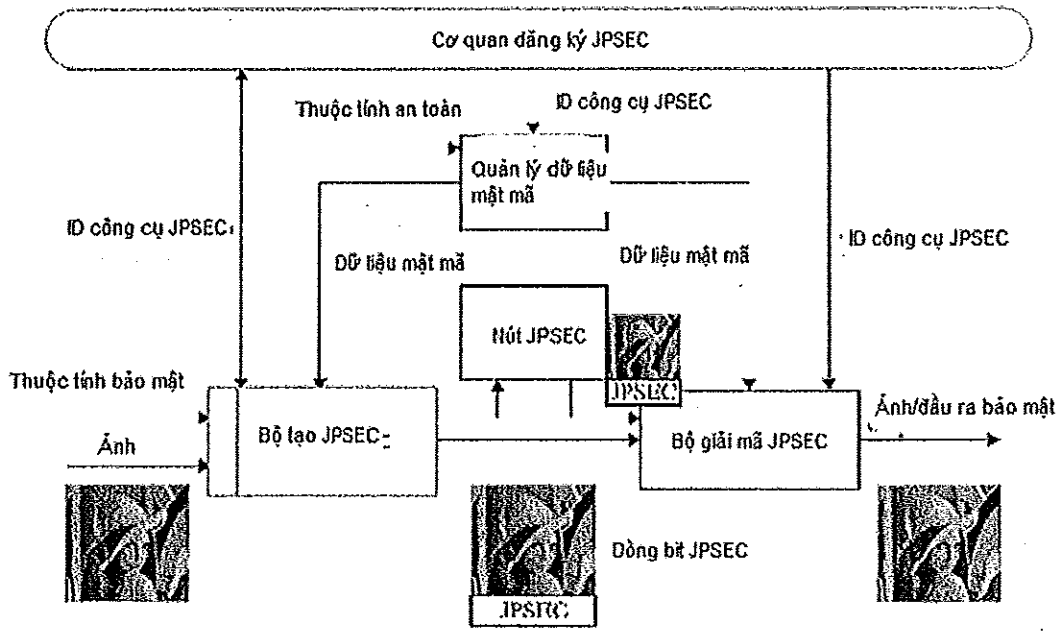
A.1 Lớp các ứng dụng JPSEC

A.1.1 Giới thiệu

Phần này đưa ra mô tả cách thức thực hiện lớp ứng dụng JPSEC. Lớp ứng dụng này minh họa kịch bản phân phối ảnh JPSEC 2000 bảo mật. Các mục sau đây mô tả tổng quan ứng dụng JPSEC bao gồm các thực thể JPSEC và thông tin được truyền giữa chúng. Mô tả này là ở mức khái niệm và không xác định thực hiện cụ thể mà cũng không đặc tả các yêu cầu thực hiện, các ứng dụng cụ thể có thể có hoặc không có các thực thể được như trong mô tả dưới đây.

A.1.2 Tổng quan về phân phối ảnh JPSEC 2000 bảo mật.

Hình A.1 biểu diễn tổng quan lớp các ứng dụng JPSEC trong phân phối ảnh JPSEC 2000 bảo mật. Trong các ứng dụng này, ứng dụng JSPEC được yêu cầu để cung cấp các dịch vụ bảo mật khác nhau cho JPSEC 2000, ví dụ như tính bảo mật của việc trao đổi ảnh, nhận thực nội dung và nguồn ảnh.



Hình A.1 – Ứng dụng phân phối ảnh JPEG 2000 bảo mật

Ứng dụng phân phối ảnh JPSEC 2000 bảo mật, bao gồm các bước sau:

Bước 1: Một dòng mã JPSEC được tạo bởi bộ tạo JPSEC

Bước 2: Dòng mã JPSEC được phân phối thông qua một hoặc một số nút JPSEC.

Bước 3: Dòng mã JPSEC được nhận và hoàn trả ra bởi người sử dụng JPSEC.

Trong ứng dụng phân phối ảnh JPEC 2000 bảo mật, bao gồm các bước sau:

Bước 1: Tạo dòng mã JPSEC

Bộ tạo chịu trách nhiệm tạo ra dòng bít JPEG 2000 bảo mật. Dòng mã này có thể được tạo từ dữ liệu bitmap hoặc từ dữ liệu nén JPEG. Một bộ tạo JPSEC áp dụng nhiều kỹ thuật bảo mật như mật mã hóa, tạo chữ ký, và tạo ICV (giá trị kiểm tra tính toàn vẹn) cho một dữ liệu ảnh cho trước.

Để bảo mật dữ liệu ảnh, bộ tạo xác định những đặc tính tham số bảo mật có liên quan tới ảnh. "Đặc tính tham số bảo mật" bao gồm những thuộc tính sau:

- Miền ảnh hưởng (vùng phủ của mỗi phương pháp bảo vệ)
- Miền xử lý (miền được xử lý bởi mỗi phương pháp bảo vệ)
- Độ chi tiết (đơn vị của mỗi phương pháp bảo vệ);
- Định danh công cụ JPSEC (thuật toán mật mã ảnh được áp dụng và các tham số liên quan)

Bước 2: Phân phối dòng mã JPSEC

Một dòng mã JPSEC có thể được chuyển tới người sử dụng JPSEC hoặc là trực tiếp thông qua mạng hoặc phương tiện truyền thông khác (như đĩa CD –ROM). Nó cũng có thể được chuyển thông qua các nút JPSEC, các nút đó có thể áp dụng nhiều kiểu xử lý bổ sung đối với dòng mã JPSEC, ví dụ như biến đổi mã.

Khi được yêu cầu bởi công cụ bảo mật JPSEC các phương pháp trong Tham số Thuộc tính Bảo mật (Security Property Parameter) của dòng mã JPSEC (ví dụ: để mật mã hóa hoặc để nhận thực), bộ tạo JPSEC phải phân phối tới người dùng JPSEC dữ liệu ảnh mật mã hóa tương ứng thông qua một kênh độc lập (bí mật). Dữ liệu này, như khóa hoặc chữ ký số, có thể được quản lý hoặc là thủ công hoặc là tự động bởi bộ phận quản lý dữ liệu mã hóa.

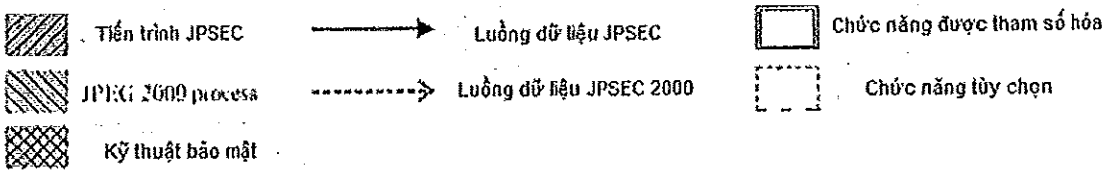
Bước 3: Sử dụng dòng mã JPSEC

Dòng mã JPSEC là đối tượng mà người dùng JPSEC xử lý tùy theo thuộc tính Tham số bảo mật được áp dụng: điều này có nghĩa là áp dụng các kỹ thuật bảo mật thích hợp, như giải mã, nhận thực và kiểm tra tính toàn vẹn. Ngoài ra, đối với mỗi phương pháp bảo mật công cụ JPSEC, bộ tạo JPSEC và người dùng JPSEC có thể sử dụng nhiều kiểu dữ liệu mật mã hóa.

Dữ liệu ảnh được giải mã và/hoặc đầu ra bảo mật, ví dụ kết quả xác thực, được đưa ra, đó là đầu ra của người dùng.

Bộ tạo JPSEC, người dùng JPSEC và bộ phận quản lý dữ liệu mật mã ảnh có thể tham khảo Cơ quan đăng ký JPSEC để có được các hướng dẫn xử lý một định danh công cụ JPSEC cụ thể.

Các phần nhỏ sau đây sẽ cung cấp thông tin chi tiết về thực thể JPSEC theo dịch vụ của JPSEC. Hình A.2 đưa ra mô tả các ghi chú được sử dụng.



Hình A.2 – Mô tả ghi chú

– **Tiến trình JPSEC**: một tiến trình sử dụng các công cụ được định nghĩa trong tiêu chuẩn này.

– **Tiến trình JPEG 2000**: một tiến trình được định nghĩa trong ITU-T Rec. T.800 | ISO/IEC 15444-1 (JPEG 2000 Phần 1).

– **Kỹ thuật bảo mật**: một kỹ thuật bảo mật nổi tiếng được định nghĩa trong tiêu chuẩn này và cũng được định nghĩa trong một số tiêu chuẩn hoặc tài liệu khác.

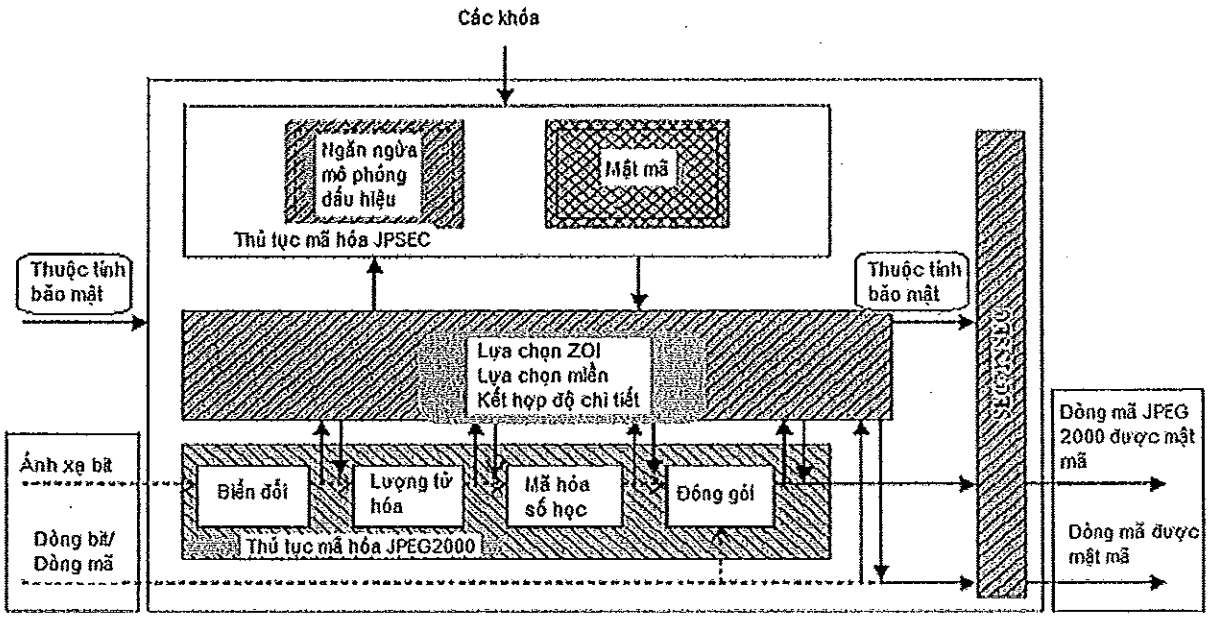
– **Dòng dữ liệu cho JPSEC**: dòng dữ liệu truyền thông thông tin được định nghĩa trong tiêu chuẩn này.

– **Dòng dữ liệu JPEG 2000**: dòng dữ liệu được định nghĩa trong ITU-T Rec. T.800 | ISO/IEC 15444-1 (JPEG 2000 Phần 1).

– **Chức năng tham số hóa**: một chức năng mà có vài chức năng thay thế, các chức năng đó có thể được lựa chọn bởi một ứng dụng.

– **Chức năng tùy chọn**: một chức năg có thể được lựa chọn áp dụng trong một ứng dụng JPSEC

A.1.3 Thủ tục mã hóa và giải mã



Hình A.3 – Thủ tục mã hóa

Hình A.3 đưa ra ví dụ tổng quan về thủ tục mã hóa đối với bộ tạo JPSEC. Thủ tục này bao gồm những xử lý sau:

– Trích xuất dữ liệu theo miền xử lý đã được quy định

– Lựa chọn một phần dữ liệu được trích xuất theo miền ảnh hưởng quy định (ví dụ một phần mã hóa)

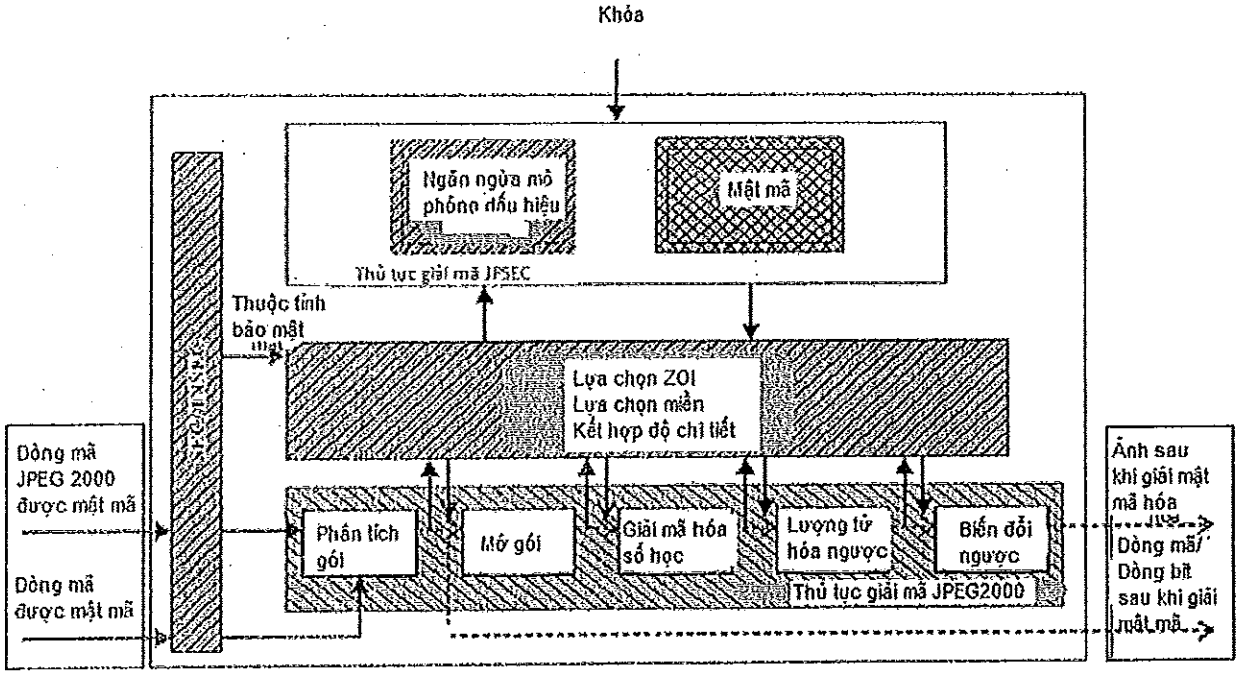
– Mã hóa dữ liệu được lựa chọn sử dụng kỹ thuật bảo mật quy định. Ngoài ra, mã hóa dữ liệu theo đơn vị dựa trên Độ chi tiết cũng phù hợp. Trong trường hợp này, các khóa khác nhau có thể được sử dụng cho các đơn vị khác nhau.

– Thay thế các dữ liệu thô bằng dữ liệu mã hóa;

– (Tùy chọn) áp dụng cơ chế phòng ngừa giả lập mã đánh dấu;

– Bố cục thuộc tính tham số bảo mật trong đoạn mã đánh dấu SEC và/hoặc INSEC

Chú ý rằng, thủ tục mã hóa JPSEC tạo ra dòng mã không tương thích ngược với JPEG 2000 phần 1. Dữ liệu ảnh được dự kiến để chuyển qua cho bộ giải mã phù hợp với Phần 1 sau khi giải mật mã thích hợp. Có thể áp dụng cơ chế bảo vệ giả lập mã đánh dấu để tránh sự mô phỏng đoạn mã đánh dấu trong dòng mã được mã hóa là phù hợp.



Hình A.4 – Thủ tục giải mã

Hình A.4 đưa ra ví dụ tổng quan về thủ tục giải mã cho người dùng JPSEC. Thủ tục này bao gồm những xử lý sau:

– Phân tích đặc tính tham số bảo mật trong đoạn mã đánh dấu SEC và/hoặc INSEC;

– Trích xuất dữ liệu theo Miền Xử lý được báo hiệu;

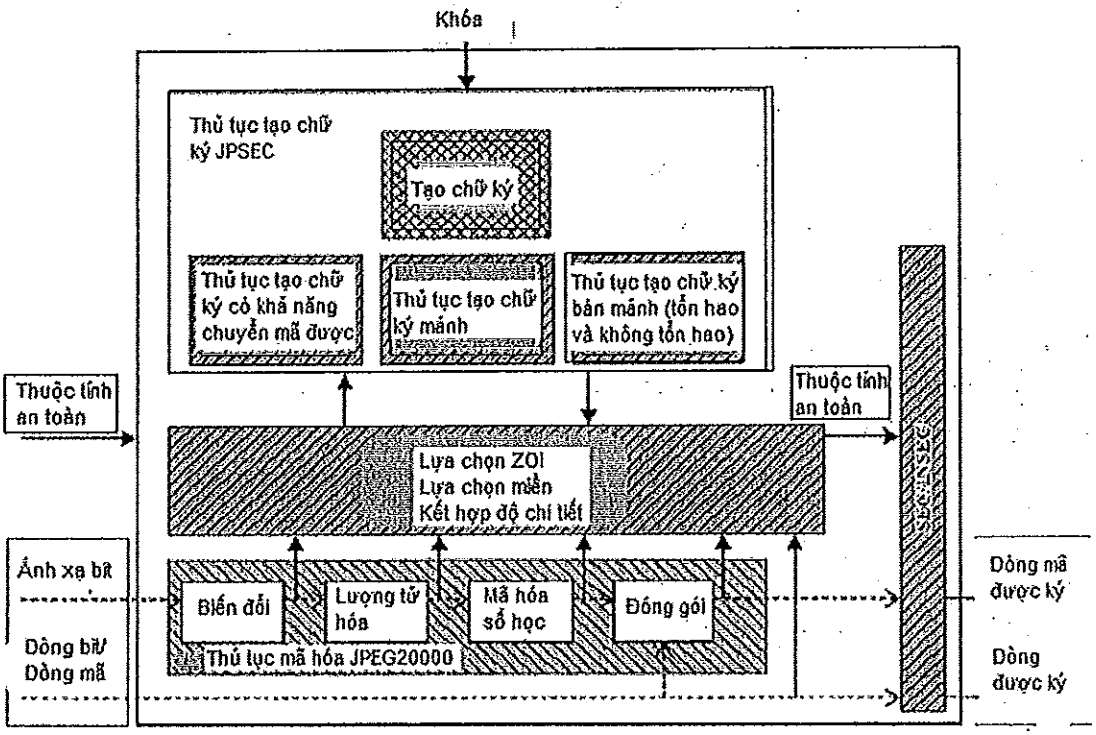
– Lựa chọn một phần dữ liệu đã trích xuất theo các khóa được giữ lại (ví dụ việc giải mã một phần);

– Giải mã dữ liệu đã chọn sử dụng kỹ thuật bảo mật được báo hiệu. Ngoài ra, có thể giải mã dữ liệu theo đơn vị dựa trên Độ chi tiết;

– Thay thế dữ liệu mã hóa bằng dữ liệu đã giải mã;

– Áp dụng cơ chế bảo vệ giả lập mã đánh dấu nếu được áp dụng ở tiến trình mã hóa.

A.1.4 Tạo chữ ký và thủ tục xác thực



Hình A.5 – Thủ tục tạo chữ ký

Hình A.5 đưa ra tổng quan một ví dụ thủ tục tạo chữ ký cho bộ JPSEC. Thủ tục này bao gồm các tiến trình sau:

– Trích xuất dữ liệu theo Miền Xử lý được quy định;

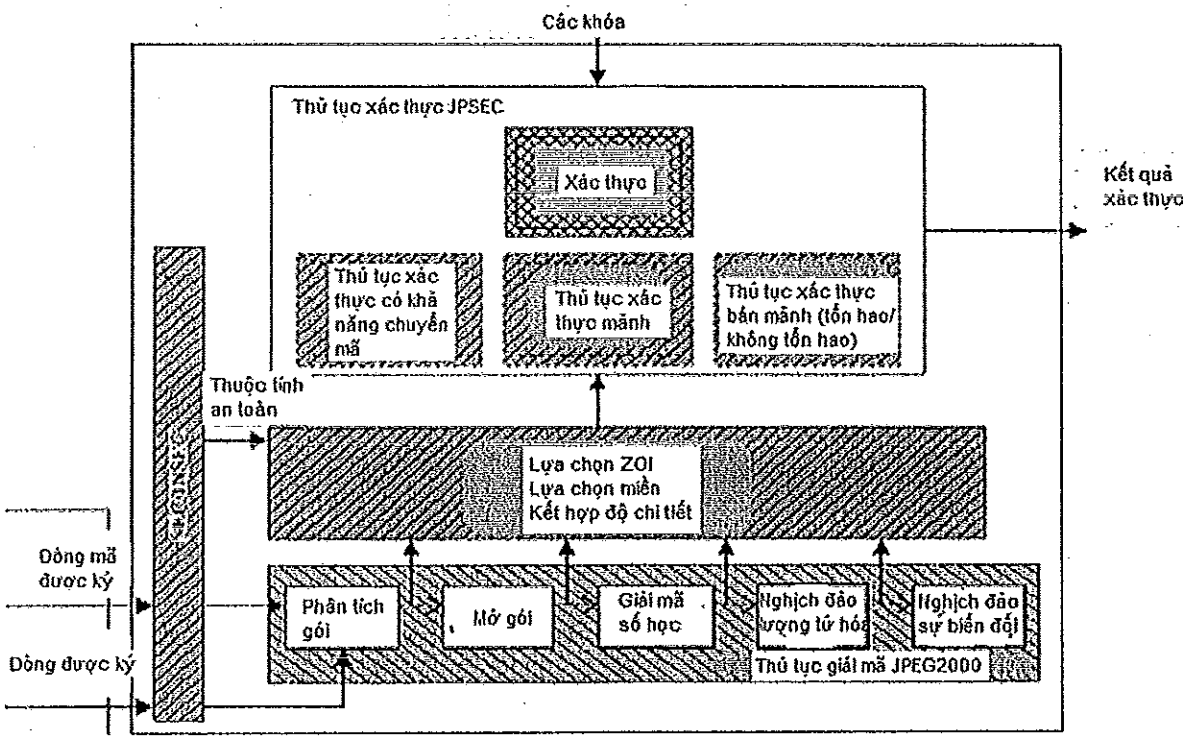
– Lựa chọn một phần dữ liệu đã trích xuất theo Miền ảnh hưởng đã quy định (ví dụ chữ ký cục bộ);

– Tính toán các chữ ký số tương ứng với dữ liệu đã chọn sử dụng kỹ thuật bảo mật đã quy định. Ngoài ra, có thể tạo chữ ký số trong một đơn vị dựa trên Độ chi tiết.

– Bố cục thuộc tính tham số bảo mật, bao gồm các chữ ký số đã được tính toán, trong đoạn mã đánh dấu SEC và/hoặc INSEC.

Chú ý rằng trong JPSEC, ba chế độ nhận thực được định nghĩa: "chế độ mảnh", chế độ bán mảnh", và chế độ có thể biến đổi mã được". Nhận thực chế độ mảnh có thể phát hiện bất kỳ sự chỉnh sửa nào

trong dòng mã, trong khi nhận thực chế độ "bán mảnh" có thể phát hiện bất kỳ sự dò tìm chủ tâm nào nhưng méo ngẫu nhiên tồn tại lên đến một mức độ nhất định. Ngoài ra, nhận thực chế độ chuyển mã có thể xác minh nguồn gốc một phần của dòng mã.



Hình A.6 – Thủ tục xác thực

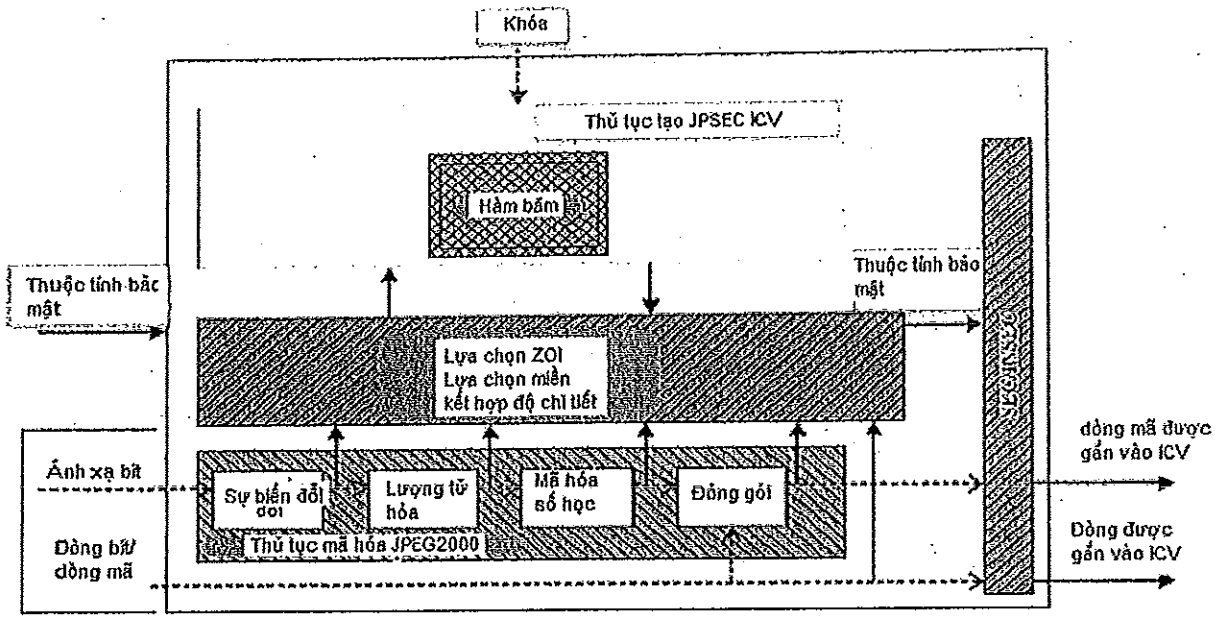
Hình A.6 đưa ra tổng quan ví dụ về thủ tục xác thực cho người dùng JPSEC. Thủ tục này bao gồm các tiến trình sau:

– Trích xuất dữ liệu trong miền xử lý được báo hiệu

– Lựa chọn một phần dữ liệu được trích xuất theo Miền ảnh hưởng được báo hiệu;

– Xác minh dữ liệu đã chọn sử dụng kỹ thuật bảo mật được báo hiệu, có thể xác minh dữ liệu đã chọn trong một đơn vị dựa trên Độ chi tiết.

A.1.5 Thủ tục tạo ICV (Giá trị kiểm tra tính toàn vẹn) và kiểm tra tính toàn vẹn



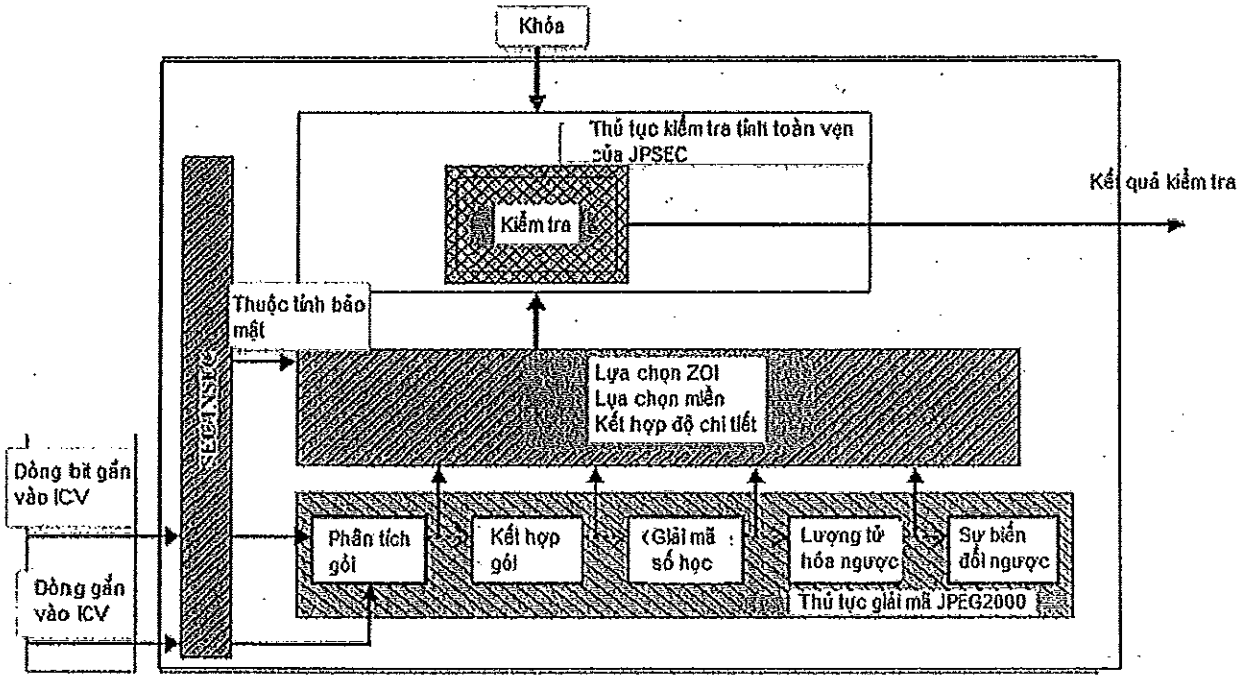
Hình A.7 –Thủ tục tạo ICV (giá trị kiểm tra tính toàn vẹn)

Hình A.7 đưa ra ví dụ tổng quan thủ tục tạo ICV cho bộ tạo JPSEC. Thủ tục này bao gồm những tiến trình sau:

– Trích xuất dữ liệu trong miền xử lý;

– lựa chọn một phần dữ liệu trích xuất theo Miền ảnh hưởng;

– Tính toán các ICV tương ứng với dữ liệu đã chọn sử dụng kỹ thuật bảo mật quy định. Ngoài ra có thể tạo các ICV trong đơn vị dựa trên Độ chi tiết;



Hình A.8 – Thủ tục kiểm tra tính toàn vẹn

Hình A.8 đưa ra ví dụ về thủ tục kiểm tra tính toàn vẹn cho người dùng JPSEC. Thủ tục này bao gồm các tiến trình sau:

– Trích xuất dữ liệu theo miền xử lý được báo hiệu;

– lựa chọn một phần dữ liệu trích xuất theo Miền ảnh hưởng;

– Xác minh dữ liệu đã chọn sử dụng kỹ thuật bảo mật được báo hiệu. Ngoài ra, có thể xác minh dữ liệu đã chọn trong đơn vị dựa trên Độ chi tiết.

Phụ lục B

(Quy định)

Các ví dụ công nghệ

B.1 Giới thiệu

Cú pháp JPSEC cho phép các công cụ bảo mật quy chuẩn và không quy chuẩn được áp dụng trong các ảnh JPEG 2000. Mục này miêu tả 10 ví dụ công nghệ thông tin, minh họa cho các cách sử dụng khác nhau của JPSEC. Các ví dụ này cung cấp khá nhiều thông tin và không được chấp nhận bởi chuẩn JPSEC. Tuy nhiên, chúng được cung cấp để thể hiện sự linh hoạt của tiêu chuẩn.

Các ví dụ công nghệ bao gồm:

- Giản đồ kiểm soát truy cập linh hoạt cho JPEG 2000;

- Khung xác thực thống nhất cho các ảnh JPEG 2000;

- Phương phát mật mã dựa trên gói đơn giản cho các dòng mã JPEG 2000;

- Công cụ mật mã cho kiểm soát truy nhập JPEG 2000

- Công cụ tạo khóa để kiểm soát truy nhập JPEG 2000

- Xáo trộn miền dòng bit và Sóng con đối với kiểm soát truy nhập có điều kiện

- Truy nhập lũy tiến đối với dòng mã JPEG 2000

- Xác thực mở rộng cho các dòng mã JPEG 2000

- Tính tin cậy dữ liệu JPEG 2000 và hệ thống kiểm soát truy nhập dựa trên việc phân chia dữ liệu và "thu hút" dữ liệu.

- Việc tạo dòng mở rộng bảo mật và việc chuyển đổi mã bảo mật.

B.2 Phương pháp kiểm soát truy nhập linh hoạt đối với các dòng mã JPEG 2000

B.2.1 Dịch vụ bảo mật

Lược đồ kiểm soát truy nhập cho phép sử dụng các dòng mã JPEG 2000 theo bất cứ giải pháp kết hợp các độ phân giải, các lớp chất lượng, các giới hạn và các khối ảnh nào.

B.2.2 Ứng dụng điển hình

Nó cung cấp sự bảo vệ cho nội dung phân phát thông qua các phương tiện khác nhau như Internet, Cáp số TV, vệ tinh và CD-ROM. Nhìn chung, công nghệ này khả thi đối với các ứng dụng nơi mà một dòng mã được mật mã chỉ một lần tại bên phát hành nhưng dòng mã được bảo vệ được giải mã nhiều cách theo các quyền khác nhau tại các bên người dùng.

B.2.3 Động lực

Trong mô hình siêu phân phối, nhà phát hành phân phối nội dung được bảo vệ một cách độc lập và các khóa nội dung một cách bảo mật. Một người dùng, người mà mong muốn truy nhập các phần của một dòng mã, sẽ gửi yêu cầu tới máy chủ khóa. Máy chủ khóa sẽ phản hồi các khóa giải mã tương ứng theo quyền của người dùng. Người dùng có thể truy nhập các ảnh con được cho phép.

B.2.4 Tổng quan công nghệ

Một dòng mã JPEG 2000 được bảo vệ được tạo ra nhờ việc mật mã hóa từng gói của bên phát hành. Nòng cốt của công nghệ này quản lý cây khóa, cây khóa này được xây dựng tại bất kỳ trật tự nào của các khối ảnh, các thành phần, độ phân giải, các lớp, các ranh giới và thậm chí là các khối mã hóa nào. Để miêu tả công nghệ một cách dễ dàng, ta giả định rằng trật tự cây khóa là RLCP và mỗi độ phân giải có cùng một số lượng phạm vi. Sau đây, cho một hàm băm một chiều h(.), xét một dòng mã ảnh JPEG 2000 với n_T khối ảnh, $n_C$thành phần, n_Llớp, n_g độ phân giải trên thành phần khối ảnh, n_P phạm vi trên độ phân giải. Với khóa chủ K đối với một dòng mã JPEG 2000. Xây dựng một cây khóa như sau:

1. Khởi tạo $k^t = h(K|"T"|t)$ cho mỗi lớp xếp t=0,1,..., $n_T - 1$. Trong đó "|" là phép ghép và "T" biểu thị mã ASCII của chữ cái T.

2. Khởi tạo $k^r = h(k^{r+1})$ cho mỗi r= $n_R - 2$,....,1,0 trong đó $k^{n_R-1} = h(k^t|"R")$ và "R" biểu thị mã ASCII của chữ cái R.

3. Tính toán khóa $k^{rl} = h(k^{r(l+1)})$, cho mỗi r= $n_R - 1$,....,1,0, $l = n_L - 2$,....,1,0 trong đó $k^{r(n_L-1)} = h(k^r|"L")$ và khi "L" biểu thị mã ASCII cho chữ cái L.

4. Tính toán khóa $k^{rlc} = h(k^{rl}|"C"|c)$ cho mỗi r= $n_R - 1$,....,1,0, $l = n_L - 1$,....,1,0, c=0,1,.... $n_c - 1$, trong đó "C" biểu thị mã ASCII của chữ cái C và c biểu thị chỉ số của thành phần này.

5. Tạo khóa $k^{rlcp} = h(k^{rlc}|"P"|p)$ cho mỗi r= $n_R - 1$,....,1,0, $l = n_L - 1$,....,1,0, c=0,1,.... $n_c - 1$,p=0,1...., $n_R - 1$ trong đó "P" biểu thị mã ASCII của chữ cái P và p biểu thị chỉ số của phạm vi này.

Dòng mã được bảo vệ được tạo ra bằng cách mã hóa mỗi thân gói tin với khóa tương ứng của nó (một lá của cây khóa).

Để diễn tả một ảnh con từ dòng mã được bảo vệ, người dùng lấy các khóa truy nhập tương ứng (được cấp từ một máy chủ khóa). Các khóa truy nhập này có thể tái tạo lại chính xác các lá cây khóa tương ứng với các gói tin của ảnh con được yêu cầu. Quá trình tái xây dựng lại khóa tương tự với khởi tạo cây khóa. Các lá được sử dụng để giải mã các gói tin tương ứng.

B.2.5 Cú pháp dòng mã

Bảng B.1 minh họa cấu trúc của đoạn SEC. Trường ZOI báo hiệu các tham số được cấp. Trường P_{ID} báo hiệu các tham số về phương pháp bảo vệ cho lược đồ kiểm soát truy nhập. Trường PM_{ID} luôn được thiết lập là 1 để nhận biết rằng khuôn mẫu giải mã được sử dụng. Trường TP_{ID} báo hiệu các

tham số bổ sung cho khung kiểm soát truy nhập. KTO là trật tự tạo cây khóa. Trường L_{akt} xác định chiều dài thông tin khóa truy nhập

Bảng B.1 – ví dụ về các tham số đối với lược đồ này

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

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
t		8 (FBAS)	1	Đấng kí sự cho phép của công cụ bảo vệ
i		8 (RBAS)	*Giá trị minh họa*	Xác định công cụ minh họa
ID_{RA}	$ID_{RA,id}$	32	*Giá trị công cụ ID*	Đăng ký ID
	$ID_{RA,nsl}$	8 (RBAS)	21	Chiều dài của $ID_{RA,ns}$ trong 1 byte
	$ID_{RA,ns}$	168	*Không gian tên*	Không gian tên của RA mà công cụ này đã được đăng ký
L_{ZOI}		16 (RBAS)	[2 ... 2^{16} – 1]	Độ dài của ZOI
ZOI		Biến đổi	Xem 5.7	Vùng ảnh hưởng đối với chương trình này
L_{PID}		16 (RBAS)	[2 ... 2^{16} – 1]	Độ dài L_{PID} + P_{ID}
P_{ID}		Biến đổi	Xem bảng B.2	Tham số đối với chương trình này

Bảng B.2 - P_{ID}

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

Tham số	Kích cỡ (bit)	Giá trị	Ý nghĩa
ID_T = 1	8	Luôn gán bằng 1	Gán cho giải mã mẫu
T_{decry}	Biến đổi	Giá trị giải mẫu	Giải mã mẫu
TP_{ID}	Biến đổi	Xem bảng B.3	Bổ sung thông tin cho chương trình này

Bảng B.3 - TP_{ID}

KTO	L_{akl}	AK_{Info}

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
KTO	8	0 ... (2^8 – 1)	Thứ tự cây khóa. Nó có thể khác nhau từ thứ tự tiến trình dòng mã, dự kiến, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL khác: dự phòng
L_{akl}	16	0 ... (2^{16} – 1)	Chiều dài khóa truy cập thông tin, nếu L_{akl}=0 thì trường hợp AK_{Info} không xảy ra
AK_{Info}	Biến đổi	Xem bảng B.4	Thông tin trên các khóa truy nhập (ví dụ, chiều dài của khóa, số lượng khóa)

Bảng B.4 - AK_{Info}

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

Tham số	Kích cỡ (bit)	Giá trị	Ý nghĩa
L_{uk}	16	0 ... (2^{16} – 1)	Chiều dài của khóa người sử dụng
UK	L_{uk}	NaN	Thông tin khóa người sử dụng
E_{ak}	16	Xem bảng 24	Thuật toán mã hóa được sử dụng để mã hóa các khóa truy

			nhập
N_{ak}	16	0 ... $(2^{16} - 1)$	Số lượng của khóa truy nhập
AK	$N_{ak} * K_{bc}$	NaN	Các khóa truy nhập

B.2.6 Kết luận

Công nghệ này cho phép bên phát hành bảo vệ một dòng mã JPEG 2000 với một khóa chủ. Dòng mã này được phép chuyển phát tới bất cứ số lượng người dùng nào, nhưng các khóa của gói được giữ bí mật. Server khóa khởi tạo các khóa truy nhập khác nhau cho người dùng theo những sự ưu tiên của họ. Người dùng khởi tạo các khóa gói từ các khóa truy nhập của họ và nhận những ảnh khác nhau. Điều đó nói lên rằng, công nghệ này có những thuộc tính gọi là "mật mã một lần, truy nhập nhiều cách".

B.3 Khung xác thực thống nhất cho các ảnh JPEG 2000

B.3.1 Mô tả hoạt động

Công cụ JPSEC này cung cấp các dịch vụ JPSEC sau: xác minh tính toàn vẹn của dữ liệu/nội dung ảnh và xác thực nguồn, ví dụ xác thực mảnh/bán mảnh cho các ảnh JPSEC 2000 dựa trên lược đồ chữ ký số.

Vì công cụ này hỗ trợ cả xác thực mảnh và bán mảnh, nó có thể được sử dụng trong các ngữ cảnh ứng dụng khác nhau bao gồm phân phối ảnh, tạo dòng ảnh, sự tạo ảnh trong quân sự và y tế , thi hành luật, thương mại điện tử và chính phủ điện tử.

Trong môi trường thông dụng, ảnh có thể trải qua các kiểu méo ngẫu nhiên khác nhau như chuyển mã và đổi định dạng. Các kỹ thuật xác thực dựa trên mã hóa truyền thống bảo vệ các ảnh JPEG 2000 ở mức toàn vẹn dữ liệu nhưng không thể bảo vệ được sự sai lệch nội dung. Vì thế, các kỹ thuật xác thực bán mảnh được yêu cầu để bảo vệ các ảnh JPEG 2000 ở mức nội dung ảnh. Công cụ này thống nhất cả hai việc xác thực dữ liệu ảnh, xác thực nội dung ảnh và đưa ra một khái niệm mới gọi là tỷ lệ bit xác thực thấp nhất (LABR). Đó là, nếu ảnh được chuyển mã thành tỷ lệ bit không nhỏ hơn LABR, nó sẽ được xem như là xác thực, mặt khác, là không xác thực. Việc xác thực có thể là mảnh hoặc bán mảnh. Trong xác thực bán mảnh, công cụ có thể nhận biết nơi diễn ra sự thay thế khi ảnh được cho là không được xác thực.

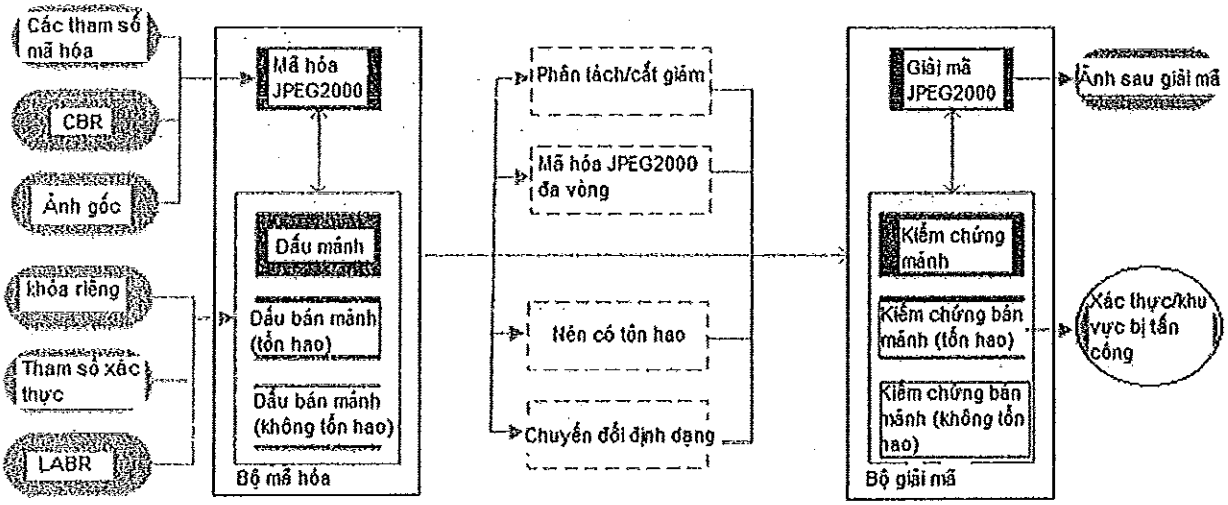
B.3.2 Tổng quan kỹ thuật

Để cung cấp xác thực mảnh và bán mảnh, nhóm các kỹ thuật được áp dụng trong công cụ JPSEC này. Bao gồm các lựa chọn đặc tính, chữ ký số, ẩn dữ liệu mất mát và không mất mát và các mã sửa lỗi ECC. Theo LABR được quy định bởi người dùng, các đặc tính tương ứng được lựa chọn dựa trên sự phân tích áp dụng cho cấu trúc JPEG 2000 và chữ kí số được khởi tạo sau đó. Đối với xác thực bán mảnh, ECC được sử dụng để tăng cường mức bền vững. Các bit kiểm tra chẵn lẻ được nhúng vào trong ảnh như dấu thủy vân để xác định vị trí tấn công. Dữ liệu nhúng có thể được thực hiện trong hai

cách khác nhau, đó là: tổn thất và không tổn thất. Với việc ẩn dữ liệu kiểu tổn thất, ảnh gốc không thể được tái tạo sau khi ẩn dữ liệu. Mặt khác, với ẩn dữ liệu không tổn thất, ảnh được sửa đổi trong cách ngược lại, ví dụ, ảnh ban đầu có thể được phục hồi nếu ảnh được mã đánh dấu không bị thay đổi. Xác thực bán mảnh không tổn hao hữu ích cho JPEG 2000 do chuẩn này hỗ trợ nén từ tổn thất đến không tổn thất. Đặc biệt, nó hữu ích với các ứng dụng tạo ảnh từ xa và tạo ảnh y khoa. Trong các trường hợp đó yêu cầu không tổn thất là một trong những yêu cầu cơ bản.

Tương tự với tỷ lệ bit nén ảnh, cái mà được sử dụng để kiểm soát và đặc tính hóa độ mạnh của thuật nén, tham số LABR được sử dụng để kiểm soát lượng độ mạnh bảo vệ. Ví dụ, khi một ảnh JPEG 2000 được bảo vệ với LABR là 2bpp(bit/pixel), bất kỳ phiên bản chuyển mã nào của ảnh sẽ được dùng như xác thực bởi hệ thống đã cho bằng với tỷ lệ bit sau chuyển mã lớn hơn hoặc bằng 2bpp.

Hình B.1 minh họa cách thức sử dụng công cụ này để bảo vệ các ảnh



Hình B.1 – Bảo vệ ảnh sử dụng khung xác thực thống nhất cho JPEG 2000

Công cụ này có thể sử dụng các cú pháp báo hiệu khác nhau phụ thuộc vào phương pháp xác thực được lựa chọn. Với xác thực mảnh, nó sử dụng cú pháp công cụ quy chuẩn JPSEC, như định nghĩa trong 5.8.3. Với xác thực bán mảnh, nó sử dụng cú pháp công cụ không quy chuẩn JPSEC, như minh họa trong bảng B.5. Thêm vào đó, F_{INSEC} nên được thiết lập về 0 vì điểm mã đánh dấu INSEC không được sử dụng bởi công cụ này, và F_{mod} nên được thiết lập là 1 bởi vì dòng mã kết quả của công cụ JPSEC này là tương thích với JPEG 2000 phần 1.

Bảng B.5 - Cú pháp cho Xác thực bán mảnh

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
t	8 (FBAS)	1	Cú pháp công cụ không quy phạm được sử dụng

Tham số				Kích cỡ (bits)	Giá trị	Ý nghĩa
i				8 (RBAS)	0 ... (2^7 – 1)	Chỉ số công cụ minh họa
ID_{RA}	$ID_{RA,id}$			32	0 ... (2^{32} – 1)	Số ID được chỉ định bởi RA
	$ID_{RA,nsl}$			8 (RBAS)	21	Độ dài của $ID_{RA,ns}$ theo byte
	$ID_{RA,ns}$			168	*Không gian tên*	Không gian tên của RA mà công cụ này đã đăng ký
L_{ZOI}				16 (RBAS)	0 ... (2^{16} – 1)	Độ dài của ZOI
ZOI				Biến đổi	*Các giá trị ZOI*	Vùng được bao phủ trong ảnh này được bảo vệ bởi công cụ
L_{PID}				16 (RBAS)	0 ... (2^{16} – 1)	Độ dài của P_{ID} và L_{PID} theo byte
P_{ID}	ID_T			8	2	Mẫu xác thực được sử dụng, như quy định tại Bảng 21
	T_{auth}	M_{auth}		8	2	Phương pháp Chữ ký số được sử dụng, như quy định tại Bảng 34
		P_{auth}	M_{DS}	8	Xem Bảng 41	Thuật toán chữ ký số được sử dụng, chẳng hạn như DSA hoặc RSA
			H_{DS}	8	Xem Bảng 37	Hàm Băm được sử dụng
			KT_{DS}	Biến đổi	*Giá trị khóa mẫu*	Khóa công khai được lưu trữ trong KTDS. Công cụ này sử dụng một khóa công khai duy nhất
			SIZ_{DS}	16	0 ... (2^{16} – 1)	Kích thước của chữ ký số theo byte
P_{ID}	PD			1	0_b	Cấu trúc FBAS được chấm dứt

Tham số			Kích cỡ (bits)	Giá trị	Ý nghĩa
			1	0_b	Miền điểm ảnh không được sử dụng
			1	0_b	Miền hệ số sóng con không được sử dụng
			1	1_b	Lượng tử hóa miền hệ số sóng con được sử dụng
			1	0_b	Miền dòng mã không được sử dụng
			3	000_b	Dành riêng cho việc sử dụng tiêu chuẩn ISO
	G	PO	16	*Các giá trị tiến trình xử lý*	Tiến trình đề nghị
		GL	8	0000 1001	Mức độ chi tiết: Đơn vị của việc bảo vệ là tổng diện tích được xác định trong ZOI
	V	N_V	16	1	Số lượng chữ ký số trong danh sách này là 1
		S_V	8 (RBAS)	1 ... (2^8 – 1)	Kích thước của chữ ký số theo byte
		VL	8* S_V	*Giá trị chữ ký kĩ thuật số*	Chữ ký số được tạo ra bởi công cụ này
	LABR	$LABR_{Int}$	8	0 ... (2^8 – 1)	Phần nguyên của LABR
		$LABR_{fra}$	8	0 ... (2^8 – 1)	Các phần phân đoạn of LABR
	Ngưỡng		8	[0 ... 2^8 – 1]	Giá trị ngưỡng. (Chỉ có giá trị đối với việc xác thực không mất mát)
	Ngẫu nhiên		8	[0 ... 2^8 – 1]	Số lượng các lần ngẫu nhiên để nhúng các bit thủy vân. (Chỉ có giá trị để xác thực không mất mát.)

ID duy nhất của công cụ này được ấn định bởi cơ quan đăng kí. Mô tả công cụ này có thể được tải về từ cơ quan đăng kí (RA) sử dụng IP được ấn định.

B.3.3 Kết luận

Tóm lại, công cụ này có các tính năng cụ thể sau đây:

- Việc xác thực cho các ảnh JPEG 2000 ở hoặc là mức dữ liệu ảnh hoặc là mức nội dung ảnh bằng cách tích hợp xác thực mảnh và bán mảnh trong một khung. Hơn nữa, xác thực bán mảnh bao gồm cả hai chế độ tổn thất và không tổn thất.

- Tính bền vững chống lại các méo ngẫu nhiên khác nhau như đã được bởi việc chuyển mã, sự chuyển đổi định dạng, nén kiểu tổn thất và mã hóa đa chu kỳ của JPEG 2000. Vì thế, công cụ này có thể được sử dụng để bảo vệ các ảnh JPEG 2000 trong môi trường rộng.

- Phân cấp việc bảo vệ các ảnh JPEG 2000. Đặc biệt, công cụ này có thể bảo vệ bất cứ khối ảnh, thành phần, độ phân giải, lớp, phạm vi hoặc khối mã nào.

- Tương thích với khung bảo mật thông tin hạ tầng khóa công khai, đó là nền tảng cơ bản của các tiêu chuẩn quốc tế đang có như X.509.

- Độ mạnh bảo vệ định lượng được kiểm soát bởi một tham số đơn được gọi là LABR, cái mà mang lại những sự thuận tiện cho người dùng cuối

- Khả năng xác định các vùng ảnh có thể bị tấn công nếu ảnh này không được xác thực. Nó có thể giúp thuyết phục người dung theo trực quan.

- Hỗ trợ bảo vệ tổn thất đến không tổn thất, tương ứng với nén tổn thất đến không tổn thất các chuẩn mã hóa JPEG 2000. Vì thế, công cụ có nhiều ứng dụng hơn bao gồm các ứng dụng tạo ảnh từ xa và ảnh y khoa.

B.4 Một phương pháp mật mã đơn giản dựa trên gói cho các dòng mã JPEG 2000

B.4.1 Mô tả hoạt động

Mục này trình bày một kỹ thuật mã hóa chọn lọc cho các ảnh JPEG 2000. Nó dựa trên một mật mã mức gói và các thuật toán mã hóa chuẩn.

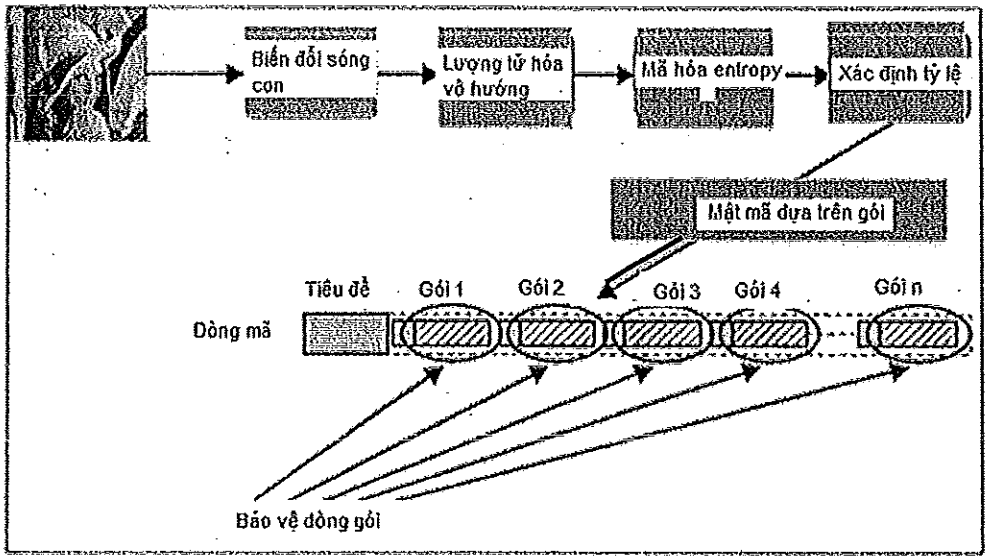
Dịch vụ bảo mật được xác định bởi kĩ thuật này là tính tin cậy của các ảnh JPEG 2000, đạt được thông qua việc mã hóa dòng mã này. Bởi vậy, việc bảo vệ IPR cũng như bảo vệ riêng có thể được thực hiện bằng cách sử dụng kỹ thuật này.

Phương pháp tiếp cận hỗ trợ chuyển mã, khả năng co giãn, và các chức năng xử lý nội dung khác mà không cần truy nhập khóa bí mật mã và để biểu thị việc giải mã và mật mã lại. Nó không can thiệp vào các quá trình xử lý mã hóa và giải mã và rất bị hạn chế tác động tiêu cực tới hiệu suất nén và không tác động tiêu cực tới khả năng phục hồi lỗi. Một tiếp cận như thế cho phép sự linh hoạt tối đa để thực hiện các ngữ cảnh và ứng dụng với các mức bảo mật khác nhau.

Kỹ thuật này có thể được sử dụng bởi các nhà sản xuất nội dung để giới hạn việc truy nhập tới nội dung ảnh hoặc bởi các nhà cung cấp nội dung để bảo đảm chuyển phát tin cậy nội dung tới người dùng cuối.

B.4.2 Tổng quan kỹ thuật

Kỹ thuật này bao gồm mật mã dòng mã sau khi nén ảnh như chỉ ra trong Hình B.2



Hình B.2 – Nguyên tắc mật mã dựa trên gói

Công cụ JPSEC này có thể sử dụng một vài tham số liên quan tới ảnh để làm đầu vào: độ phân giải, các lớp chất lượng, các thành phần, các phạm vi hoặc các khối ảnh. Chỉ những tải tin tương ứng với các tham số đầu vào này thì mới được xử lý. Vì thế, dòng mã được bảo vệ giữ một cấu trúc JPEG 2000 phổ biến. Một khi dòng mã được mã hóa, đoạn mã đánh dấu SEC được thêm vào mào đầu chính để cho phép bất kỳ người dùng JPSEC nào cũng có thể giải mã chính xác ảnh sau này.

Phương pháp này sử dụng các thuật toán theo các chuẩn phổ biến để mã hóa chọn lọc các gói tin: các phương pháp DES, AES như là ECB, CBC, CFB, OFB, CTR. Dĩ nhiên, bất kỳ thuật toán mật mã khối nào khác cũng có thể được sử dụng: DES và AES được đưa ra ở đây như những là ví dụ về mã hóa chuẩn.

B.4.2.1 Ví dụ báo hiệu

Kỹ thuật này có thể được báo hiệu với mẫu dựa trên cú pháp của phần quy chuẩn. Sau đây là một ví dụ của việc báo hiệu cho kỹ thuật này (xem bảng B.6), kỹ thuật quy định một vùng cho ZOI nhưng tất nhiên cũng có thể nhiều hơn, theo cú pháp như Miền^0

Bảng B.6 – Ví dụ của Miền ảnh hưởng với sự kết hợp không gian, các độ phân giải và các lớp

Tham số		Kích cỡ (bit)	Giá trị	Ý nghĩa
NZzoi		8	1 (RBAS)	Số lượng của một vùng
Zone^0	DCzoi	1	0	Các phân đoạn byte không tuân theo sự liên kết
		1	0	Ảnh liên quan các lớp mô tả
		6	101100	Miền ảnh, mức phân giải, các lớp chất lượng và các thành phần được quy định theo thứ tự

Pzoi[1]	Mzoi[1]	1	0	Các phân đoạn byte không tuân theo sự liên kết
		1	0	Các vùng quy định bị ảnh hưởng bởi các phương pháp bảo vệ
		1	0	Phần tử đơn được quy định
		2	00	Chế độ hình chữ nhật
		2	00	Izoi sử dụng trọn 8 bit
		1	1	Izoi được mô tả theo hai hướng
	Izoi[1]	8	0110 0100	Xul là 100
		8	0111 1000	Yul là 120
		8	1011 0100	Xlr là 180
		8	1101 0010	Ylr là 210
Pzoi[3]	Mzoi[3]	1	0	Các phân đoạn byte không tuân theo sự liên kết
		1	1	Các vùng quy định không bị ảnh hưởng bởi các phương pháp bảo vệ
		1	0	Mục duy nhất được quy định
		2	11	Chế độ tối đa
		2	00	Izoi sử dụng trọn 8 bit
		1	0	Izoi được mô tả theo hai hướng
	Izoi[3]	8	0000 0010	Độ phân giải ≤ 2 đã được quy định. (i.e., độ phân giải > 3 được quy định với chế độ tối đa và chuyển đổi bổ sung)
Pzoi[4]	Mzoi[4]	1	0	Các phân đoạn byte không tuân theo sự liên kết
		1	0	Các vùng quy định bị ảnh hưởng bởi các phương pháp bảo vệ
		1	0	Phần tử đơn được quy định
		2	11	Chế độ tối đa

			2	00	Izoi sử dụng trọn 8 bit
			1	0	Izoi được mô tả theo một hướng
		Izoi[4]	8	0000 0101	Số lớp ≤ 5 được quy định với tốc độ tối đa

Bảng B.7 – Mô tả mẫu giải mật mã trong trường hợp AES-192/CBC

Tham số					Kích cỡ (bits)	Giá trị	Ý nghĩa
P_{PM}	ME_{decry}				8	0000 0000	NULL: không có phương pháp ngăn chặn mô phỏng mã đánh dấu
	CT_{decry}				16	0x0003	Định danh mật mã: AES (mật mã khối)
	CP_{decry}	M_{bc}			6	10 0000	Chế độ mật mã: CBC
		P_{bc}			2	01	Chế độ đệm (PKCS#7-padding)
		SIZ_{bs}			8	0001 0000	Kích cỡ khối: 16 bytes (128 bits)
		KT_{bc}	LK_{KT}		16	0x00C0	Kích cỡ khóa: 192 bits
			KID_{KT}		8	0000 0011	Thông tin khóa là một URI
			LKI_{KT}		16	0x0021 (=33)	Độ dài của URI: 33 bytes
			KI_{KT}		264	https://server/path/secretkey.pem	URI này là một URL https; nó phải được hiểu bởi các ứng dụng sử dụng JPSEC. Khả năng thu hồi hiệu quả của khóa là vượt quá tiêu chuẩn.
			G_{KT}	PO	16	0 000 001 010 011 100	Thứ tự tiến trình là TRLCP
				GV	8	0000 1001	Độ chi tiết của khóa là tổng diện tích trong ZOI
			V_{KT}	Nv	16	0x0001	Giá trị khóa đơn trong KI_{KT}; Giá trị không quy định tại V_{KT}

				Sv	16	0010 0001	Chiều dài của URI: 33 bytes
				VL	264	https://server/path/secretkey.pem	URI này là một URL https; nó phải được hiểu bởi các ứng dụng sử dụng JPSEC. Khả năng thu hồi hiệu quả của khóa là vượt quá tiêu chuẩn.

Bảng B.8 – Cú pháp miền xử lý

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
PD	1	0_b	Các phân đoạn byte không tuân theo sự liên kết
	1	0_b	Không trong phạm vi điểm ảnh
	1	0_b	Không trong phạm vi hệ số sóng con
	1	0_b	Không trong miền lượng tử hóa hệ số sóng con
	1	1_b	Được xử lý trong phạm vi dòng mã
	3	000_b	Không được sử dụng

Bảng B.9 – Độ chi tiết và Cú pháp danh sách các giá trị

Tham số		Kích cỡ (bits)	Giá trị	Ý nghĩa rút ra
G	PO	16	0 000 001 010 011 100	Thứ tự xử lý là TRLCP
	GV	8	0000 0110	Đơn vị bảo vệ là các gói
V	N_V	16	1	Số lượng của các giá trị IV được quy định
	Sv	8	16	Kích thước IV theo byte
	VL	128	*Value*	Giá trị IV

B.4.3 Kết luận

Kỹ thuật được miêu tả trong mục này minh họa cho việc mã hóa chọn lọc các ảnh JPEG 2000. Nó dựa trên mật mã hóa mức gói và các thuật toán mã hóa tiêu chuẩn. Nó có thể được báo hiệu sử dụng các mẫu được định nghĩa trong 5.8 và hỗ trợ các mức phức tạp khác nhau.

B.5 Công cụ mật mã hóa đối với kiểm soát truy nhập JPEG 2000

B.5.1 Các dịch vụ bảo mật được đề cập

Công cụ này cung cấp một phương pháp mật mã hóa có thể ngăn ngừa mô phỏng mã đánh dấu trong một dòng mã được mật mã.

B.5.2 Ứng dụng điển hình

Công nghệ này cho phép mã hóa một cách đầy đủ và có tính chọn lọc các dòng mã JPEG 2000. Các phương pháp mã hóa có chọn lọc như thế có thể được sử dụng để hiển thị chỉ một ảnh đã được chấp nhận như một ảnh nhỏ, ảnh chất lượng thấp và một ảnh được mã hóa một phần.

B.5.3 Người sử dụng tiềm năng, mô hình thực hiện và các động cơ

Về cơ bản công nghệ này dựa trên mã hóa gói đối với dòng mã JPEG 2000 với thuật toán Cipher thông dụng. Đặc biệt, công nghệ này ngăn ngừa mô phỏng mã đánh dấu trong dòng mã được mã hóa. Vì thế, ngay cả khi dòng mã được mã hóa sinh ra là đầu vào của bộ giải mã tương thích trong phần 1 của JPEG 2000 thì bộ mã hóa này cũng không có sự cố và có thể biểu diễn ảnh bảo vệ này một cách chính xác.

B.5.4 Tổng quan công nghệ

(1) Mã hóa

Bước 1. Mã 2 byte được mã hóa tạm thời sử dụng thuật toán mã hóa phổ biến.

Bước 2. Nếu mã được mật mã hóa tạm thời này hoặc mã liên quan của nó là lớn hơn 0xFF8F thì mã 2 (byte) là không được mật mã hóa

Mặt khác, mã được mật mã hóa tạm thời này là đầu ra như mã được mã hóa

Bước 3. Chuyển tới mã 2 (byte) tiếp theo và tiếp tục thực hiện Bước 1 với bước 2

Tất cả mã 2byte trong tập tin văn bản gốc sẽ ít hơn 0xFF90 đặc tả trong phần 1. Hơn thế nữa, nếu mã được mật mã hóa tạm thời này hoặc mã liên quan của nó lớn hơn 0xFF8F thì mã 2byte không được mật mã. Cuối cùng, tất cả mã 2 (byte) trong văn bản mã hóa nhỏ hơn 0xFF90.

Nếu chiều dài của đoạn văn bản là lẻ, loại trừ việc cần phải xử lý; byte cuối cùng là không được mật mã hoặc được đệm vào một byte bổ sung.

(2) Giải mã

Bước 1. Mã 2byte là được giải mã tạm thời sử dụng thuật toán mã hóa như phía mã hóa.

Bước 2. Nếu mã được giải mã tạm thời hoặc mã liên quan của nó lớn hơn 0xFF8F thì mã 2byte không được giải mã. Mặt khác,mã được giải mật mã tạm thời là đầu ra như là mã được giải mật mã.

Bước 3. Chuyển tới mã 2byte tiếp theo và lặp lại bước 1 và bước 2

Tất cả mã 2byte trong văn bản gốc trước khi được mật mã hóa sẽ nhỏ hơn 0xFF90. Vì thế, khẳng định rằng mã 2byte không được mã nếu mã được giải mã tạm thời hoặc mã liên quan của nó lớn hơn 0xFF8F.

B.5.5 Phương pháp báo hiệu

Bảng B.10 đưa ra ví dụ các tham số cho công nghệ này. Bất kỳ tham số nào cho công nghệ này phải được báo hiệu theo cú pháp được chỉ ra trong JPSEC. Đặc biệt, công nghệ này nên sử dụng mẫu "giải mã" , Độ chi tiết "gói" và miền xử lý dòng bit cùng với ZOI thích hợp.

Bảng B.10 – Ví dụ về các tham số đối với công nghệ này

Tham số		Kích cỡ (bits)	Giá trị	Ý nghĩa
SEC		16	0xFF65	Mã đánh dấu SEC
L_{SEC}		16	Biến số	Chiều dài của đoạn mã đánh dấu SEC
Z_{SEC}		8	1 (ví dụ)	Chỉ số của đoạn mã đánh dấu SEC này
P_{SEC}		1	0	byte FBAS không tuân theo
	F_{INSEC}	1	1 (ví dụ)	INSEC được sử dụng
	$F_{multiSEC}$	1	0_b	Một đoạn mã đánh dấu SEC được sử dụng
	F_{mod}	1	1_b	Dữ liệu JPEG 2000 ban đầu đã được sửa đổi
	F_{TRLCP}	1	0_b	Sử dụng gán thẻ TRLCP không được định nghĩa
	Padding	3	000_b	Không được sử dụng
	N_{tools}	8 (RBAS)	1	Số công cụ bảo mật là 1
	I_{max}	8 (RBAS)	0	Chỉ số ví dụ công cụ tối đa bằng 0
t		8 (FBAS)	1	Bảo vệ RA với công cụ không quy chuẩn JPSEC

i		8 (RBAS)	0000000_b	Chỉ số ví dụ công cụ
ID_{RA}	$ID_{RA,id}$	32	0	ID được đăng ký
	$ID_{RA,nsl}$	8 (RBAS)	21	Chiều dài của $ID_{RA,ns}$ theo byte
	$ID_{RA,ns}$	168	*Không gian tên*	Không gian tên của RA với các công cụ đã được đăng ký
L_{zoi}		16	9	Chiều dài của ZOI là 9 byte
ZOI		Biến đổi	Xem bảng B.11 (ví dụ)	Vùng ảnh hưởng đối với công cụ này
L_{PID}		16	Biến số	Chiều dài là L + T + PD + G
P_{ID}		Biến đổi	Xem bảng B.12 (ví dụ)	Các tham số đối với công nghệ này

Bảng B.11 – ZOI ví dụ của công cụ khởi tạo khóa này

Tham số			Kích thước (bits)	Giá trị	Ý nghĩa
NDzoi			8	1	Số vùng là 1
Zone 0	Dczoi		1	0_b	Các phân đoạn byte không tuân theo sự
			1	0_b	Ảnh liên quan lớp mô tả
			6	101000_b	Các miền ảnh và các mức phân giải được quy định theo thứ tự
	Pzoi[1]	Mzoi[1]	1	0_b	Các phân đoạn byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi các phương pháp bảo vệ
			1	0_b	Phần tử đơn được quy định
			2	00_b	Chế độ phân khu
			2	00_b	Izoi sử dụng trọn 8 bit
			1	1_b	Izoi được mô tả theo hai chiều
		Izoi[1]	8	$0110\ 0100_b$	Xul là100

			8	0111 1000$_b$	Yul là120
			8	1011 0100$_b$	Xlr là 180
			8	1101 0010$_b$	Ylr là 210
	Pzoi[3]	Mzoi[3]	1	0$_b$	Các phân đoạn byte không tuân theo sự
			1	1$_b$	Các vùng quy định không bị ảnh hưởng bởi các phương pháp bảo vệ
			1	0$_b$	Phần tử đơn được quy định
			2	11$_b$	Chế độ tối đa
			2	00$_b$	Izoi sử dụng trọn 8 bit
			1	0$_b$	Izoi được mô tả theo một chiều
		Izoi[3]	8	0000 0010$_b$	Mức phân giải > 3 được quy định

Bảng B.12 – P_{ID} cho công nghệ này

Tham số		Kích cỡ (bits)	Giá trị	Ý nghĩa
T		Biến đổi	Xem Bảng B.13	Các khuôn mẫu giải mã
PD		8	0000 1000$_b$	byte FBAS không tuân theo. Được xử lý trong phạm vi dòng mã
G	PO	16	0 000 001 010 011 100 0$_b$	Thứ tự xử lý là xếp chồng-phân giải-các lớp-thành phần-các giới hạn
	GL	8	0000 0110$_b$	Đơn vị bảo vệ là gói
Skip		8	0	tham số *Skip* đối với công cụ này

Bảng B.13 – Ví dụ về khuôn mẫu giải mã của công nghệ này

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
ME_{decry}	8	1	Mô phỏng mã đánh dấu không xảy ra
CT_{decry}	16	1	Mã hóa khối (AES)

CP_{decry}	M_{bc}	6	$10\ 0010_b$	Chế độ OFB được sử dụng (các Bit không được đệm vào)
	SIZ_{bc}	16	128	Kích cỡ khối (128 bits)
	KT_{bc}	Biến đổi	*Các giá trị khóa mẫu*	Mẫu khóa
	IVsc	128	*Giá trị vecto ban đầu*	Giá trị vec-tơ khởi tạo

B.5.6 Kết luận

Mục này miêu tả kỹ thuật mã hóa cho dòng mã JPEG 2000. Ưu điểm quan trọng của công nghệ này là để ngăn chặn mô phỏng mã đánh dấu từ việc xuất hiện trong dòng mã được mã hóa.

B.6 Công cụ khởi tạo khóa cho kiểm soát truy nhập JPEG 2000

B.6.1 Các dịch vụ bảo mật được đề cập

Công nghệ này giới thiệu giám sát truy nhập có liên quan tới ảnh cho JPEG 2000 tuân theo cấu trúc phân lớp trong JPEG 2000.

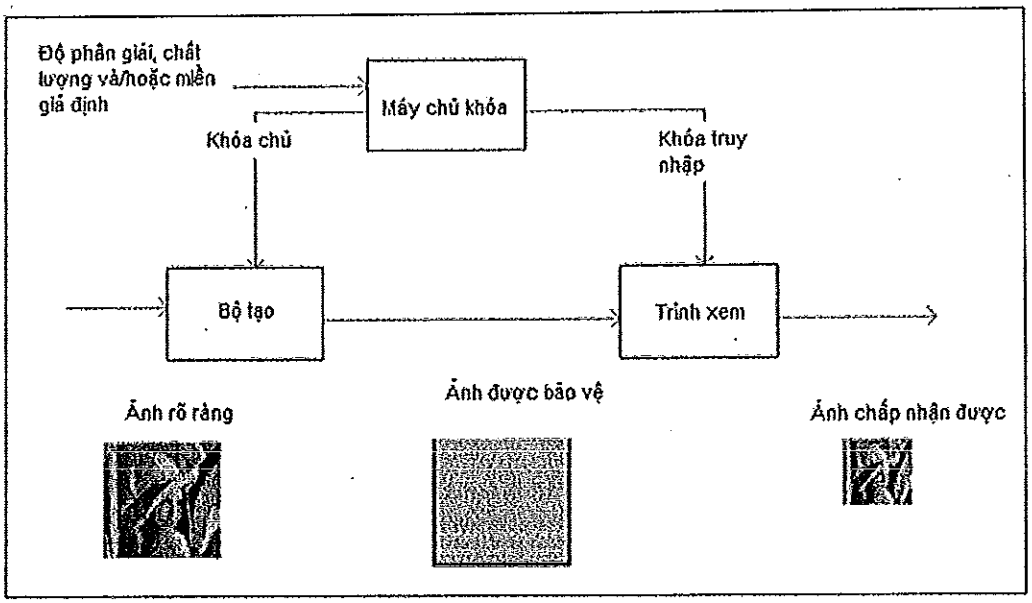
B.6.2 Các ứng dụng điển hình

Một ứng dung điển hình của công nghệ này là phân phối ảnh bảo mật, ở đó chỉ một người dùng được phép mới có thể trình diễn ảnh đã được thừa nhận. Ví dụ, một ảnh nhỏ thì có thể tự do hiển thị nhưng đối với ảnh có độ phân giải lớn thì chỉ có người dùng sở hữu khóa mới có khả năng giải mã được.

B.6.3 Những người dùng tiềm năng, mô hình thực hiện và những động lực thúc đẩy

Công nghệ này hỗ trợ tạo khóa để sử dụng trong việc phân phối JPEG 2000 bảo mật. Công nghệ này dựa trên giám sát truy nhập có liên quan đến ảnh, như là vùng ảnh, độ phân giải và chất lượng ảnh. Nguyên tắc của công nghệ này là tạo các khóa mã hóa và giải mã trong phân cấp bằng cách sử dụng hàm băm một chiều bằng mật mã như là một hàm băm.

B.6.4 Tổng quan công nghệ



Bảng B.3 – Tổng quan công nghệ

Trong giai đoạn mã hóa, máy chủ khóa tạo ra một khóa chủ. Sau đó, bộ tạo mã hóa một ảnh sử dụng các khóa gói được tạo ra từ khóa chủ. Trong giai đoạn giải mã, server khóa tạo một khóa truy nhập theo độ phân giải, chất lượng và/hoặc vùng được phép. Sau đó, bên nhận giải mã ảnh đã được mật mã hóa bằng cách sử dụng các khóa gói được khởi tạo từ khóa truy nhập. Chú ý rằng, các khóa này được khởi tạo liên tiếp dựa trên chuỗi băm bảo mật.

Đặc biệt, công nghệ này sử dụng chính sách kiểm soát truy nhập: "Nếu một người dùng có thể truy nhập một lớp/mức phân giải thì người dùng cũng có thể truy nhập tới các lớp/mức phân giải thấp hơn". Nhưng ngược lại, nếu một người dùng người dùng có thể truy nhập tới một khối ảnh thì người dùng đó không thể truy nhập đến các khối ảnh khác.

Ưu điểm quan trọng của công nghệ này là số khóa cần thiết để đi tiếp từ một máy chủ khóa tới người xem ít hơn nhiều so với trường hợp thông thường. Điều này có nghĩa là công nghệ này cho phép sử dụng không gian lưu trữ nhỏ hơn.

B.6.5 Phương pháp báo hiệu

Bảng B.14 cho thấy các tham số được khuyến nghị trong công nghệ này. Bất kỳ tham số nào cũng phải được báo hiệu theo cú pháp được xác định trong JPSEC. Đặc biệt, công nghệ này nên sử dụng mẫu "giải mật mã", lõi "gói" và miền xử lý "dòng bit" với ZOI thích hợp.

Bảng B.14 – Các tham số được khuyến nghị trong công nghệ

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
SEC	16	0xFF65	Mã đánh dấu SEC

Tham số		Kích cỡ (bits)	Giá trị	Ý nghĩa
L_{SEC}		16	0 ... 255	Chiều dài của đoạn mã đánh dấu SEC
Z_{SEC}		8	0	Chỉ số của đoạn mã đánh dấu SEC
P_{SEC}		1	0	byte FBAS không tuân theo
	F_{INSEC}	1	1	INSEC được sử dụng
	$F_{multiSEC}$	1	0_b	Một đoạn mã đánh dấu SEC được sử dụng
	F_{mod}	1	1_b	Dữ liệu JPEG 2000 ban đầu đã bị sửa đổi
	F_{TRLCP}	1	0_b	sử dụng mã đánh dấu gán TRLCP không được định nghĩa
	Padding	3	000_b	Không được sử dụng
	N_{tools}	8 (RBAS)	1	Số lượng công cụ bảo mật là 1
	I_{max}	8 (RBAS)	0	Chỉ số ví dụ công cụ tối đa bằng 0
t		8 (RBAS)	1	Công cụ không quy chuẩn JPSEC
i		8 (RBAS)	0	Chỉ số ví dụ cho công cụ này
ID_{RA}	$ID_{RA,id}$	32	5	ID đã đăng ký cho công cụ này
	$ID_{RA,nsl}$	8 (RBAS)	21	Chiều dài của $ID_{RA,ns}$ theo đơn vị byte
	$ID_{RA,ns}$	168	*Không gian tên*	Không gian tên của RA với các công cụ đã được đăng ký
L_{zoi}		16	Biến số	Chiều dài của ZOI đối với công cụ này
ZOI		Biến đổi	*Giá trị ZOI*	Miền ảnh hưởng đối với công cụ này

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
L_{PID}	16	Biến đổi	Chiều dài L + T + PD + G
P_{ID}	Biến đổi	Xem bảng B.16	Các tham số cho công nghệ này

Bảng B.15 – Ví dụ ZOI của công cụ khởi tạo khóa này

Tham số			Kích cỡ (bits)	Giá trị	Ý nghĩa
NDzoi			8	1	Số lượng Zones là 1
Zone 0	Dczoi		1	0_b	Các phân đoạn byte không tuân theo
			1	0_b	Các lớp mô tả liên quan đến ảnh
			6	101000_b	Miền ảnh và độ phân giải được quy định theo thứ tự
	Pzoi[1]	Mzoi 1	1	0_b	Các phân đoạn byte không tuân theo
			1	0_b	Các vùng quy định bị ảnh hưởng bởi các phương pháp bảo vệ này
			1	0_b	Phần tử đơn được quy định
			2	00_b	Chế độ hình chữ nhật
			2	00_b	Izoi sử dụng trọn 8 bit
			1	1_b	Izoi được mô tả theo hai hướng
		Izoi[1]	8	0110 0100_b	Xul là100
			8	0111 1000_b	Yul là 120
			8	1011 0100_b	Xlr là 180
			8	1101 0010_b	Ylr là 210
	Pzo	Mzoi	1	0_b	Các phân đoạn byte không tuân theo

	i[3]	[3]	1	1_b	Các vùng quy định không bị ảnh hưởng bởi các phương pháp bảo vệ
			1	0_b	Phần tử đơn được quy định
			2	11_b	Chế độ tối đa
			2	00_b	Izoi sử dụng trọn 8 bit
			1	0_b	Izoi được mô tả theo một hướng
		Izoi[3]	8	0000 0010$_b$	Mức độ phân giải > 3 được quy định

Bảng B.16 – P_{ID} cho công nghệ này

Tham số		Kích thước (bit)	Giá trị	Ý nghĩa
T		Variable	Xem bảng B.17	Các khuôn mẫu giải mã
PD		8	0000 1000$_b$	byte FBAS không tuân theo. Được xử lý trong phạm vi dòng mã.
G	PO	16	0 000 001 010 011 100$_b$	Thứ tự tiến trình là khối ảnh-độ phân giải-các lớp-thành phần-phạm vi
	GL	8	0000 0110$_b$	Đơn vị bảo vệ là gói
H		16	Xem bảng 37 trong 5.8.3.1	Hàm băm cho công cụ tạo khóa này
L_k		8	0 ... 255	Chiều dài thông tin khóa truy nhập
AK_{info}		Biến đổi	*Giá trị khóa truy cập*	Thông tin khóa truy nhập (thông tin này được mã hóa bằng cách sử dụng KT_{bc} theo T)

Bảng B.17 – Ví dụ về mẫu giải mật mã của công nghệ này

Tham số	Kích cỡ (bits)	Giá trị	Ý nghĩa
ME_{decry}	8	1	Mô phỏng mã đánh dấu không xảy ra
CT_{decry}	16	3	Mã hóa khối (AES)

CP_{decry}	M_{bc}	6	10 0010	Chế độ OFB được sử dụng (các Bit không có đệm)
	SIZ_{bc}	16	128	Kích thước khối (128 bits)
	KT_{bc}	Biến đổi	xem 5.8.5	Mẫu khóa
	IVsc	128	*Giá trị vecto ban đầu*	Giá trị véc tơ khởi tạo

B.6.6 Kết luận

Mục này miêu tả kỹ thuật giám sát truy nhập liên quan ảnh cho dòng mã JPEG 2000. Ưu điểm quan trọng của công nghệ này là số lượng khóa cần quản lý và truy nhập ít hơn nhiều so với trường hợp thông thường.

B.7 Sự xáo trộn miền dòng bit và Sóng con đối với giám sát truy nhập có điều kiện

B.7.1 Tổng quan

Giám sát truy nhập một ảnh là một chức năng quan trọng trong việc bảo mật ảnh. Thông thường, người ta muốn có một truy nhập vào một ảnh nhỏ có độ phân giải bé hoặc ảnh có chất lượng thấp, trong khi truy nhập tới ảnh chất lượng hơn hoặc có độ phân giải cao hơn đối tượng để xác thực.

Trong mục này, một kỹ thuật giám sát truy nhập có điều kiện được giới thiệu. Về cơ bản, nó bổ sung thêm nhiễu giả ngẫu nhiên tới ảnh. Người sử dụng được ủy quyền biết chuỗi giả ngẫu nhiên và vì thế có thể loại bỏ nhiễu này. Mặt khác, những người sử dụng không được ủy quyền chỉ được truy nhập tới một vài ảnh bị méo nghiêm trọng. Hệ thống này bao gồm ba thành phần cơ bản: Sự xáo trộn; bộ tạo số giả ngẫu nhiên và thuật toán mã hóa. Để có cái nhìn đầy đủ và giữ lại các thuộc tính của JPEG 2000, Xáo trộn được áp dụng một cách có chọn lọc vào các khối mã kết hợp dòng mã. Do đó, mức méo được giới thiệu trong các phần cụ thể của ảnh có thể được giám sát. Điều đó cho phéo kiểm soát truy nhập bởi độ phân giải, chất lượng hoặc các miền quan tâm của ảnh.

B.7.2 Tổng quan kỹ thuật

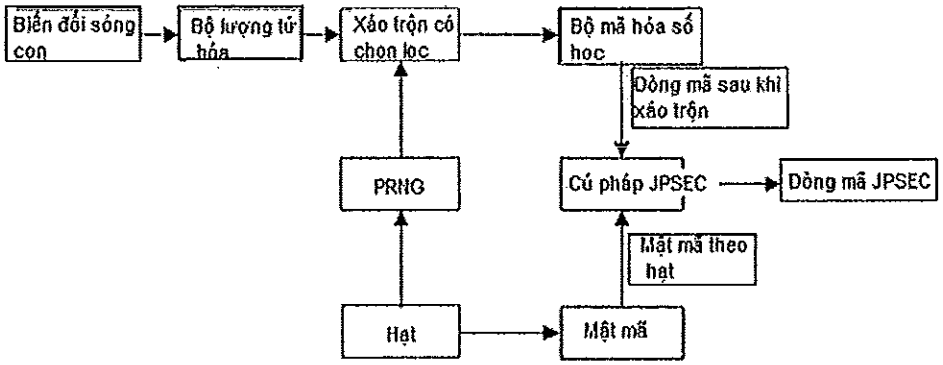
Hệ thống này bao gồm ba phần chính:

- Trộn: hai tiếp cận được hỗ trợ. Sự xáo trộn này hoặc là được tạo thành dựa trên các hệ số sóng con lượng tử hóa, hoặc trực tiếp trên các bit của dòng mã. Trong trường hợp đầu tiên, các mã đánh dấu của các hệ số trong mỗi khối mã được đảo ngược giả ngẫu nhiên. Trường hợp thứ hai, các bit của dòng mà được đảo ngược một cách giả ngẫu nhiên.

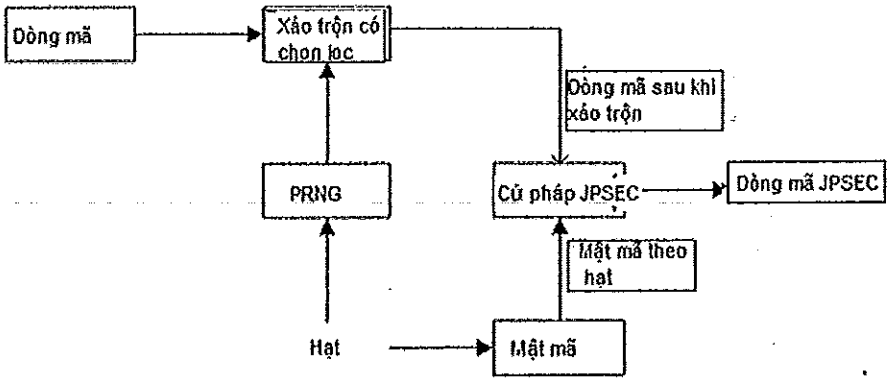
- Bộ tạo số giả ngẫu nhiên (PRNG): PRNG này được sử dụng để điều khiển Sự xáo trộn. Nó dựa trên giá trị khởi tạo(seed). Trong phương pháp được ưu tiên của kỹ thuật này, thuật toán SHA1PRNG [24] với một phần khởi tạo 64 bit được sử dụng cho bộ tạo số giả ngẫu nhiên (PRNG). Chú ý rằng các thuật toán PRNG khác cũng có thể được sử dụng.

- Thuật toán mã hóa: để truyền thông các phần khởi tạo tới những người được ủy quyền, chúng có thể được mã hóa và chèn vào dòng mã. Trong phương án được ưu tiên của kỹ thuật này, thuật toán RSA được sử dụng cho việc mã hóa. Các thuật toán mã hóa khác cũng có thể được sử dụng. Độ dài của khóa có thể được lựa chọn tại thời điểm ảnh được bảo vệ.

Hình B.4 và B.5 tương ứng với hai trường hợp Sóng con và trộn dòng bít



Hình B.4 - Sơ đồ khối trộn miền sóng mang con



Hình B.5 - Sơ đồ khối trộn miền dòng bít

Để Cải thiện tính bảo mật của hệ thống, phần khởi tạo này có thể được thay đổi từ khối mã này thành khối mã khác. Và một vài mức truy nhập có thể được định nghĩa, sử dụng các khóa mã hóa khác nhau. Cú pháp đưa ra dưới đây rất linh hoạt và hỗ trợ việc sử dụng nhiều phần khởi tạo và nhiều khóa.

B.7.3 Cú pháp dòng mã

Trong ví dụ này, cả hai đoạn mã đánh dấu SEC và INSEC đều được sử dụng. Cú pháp dòng mã được định nghĩa dưới đây. Đoạn mã đánh dấu SEC sử dụng cú pháp công cụ này cho các công cụ không chính tắc. Đoạn mã đánh dấu INSEC được sử dụng để báo hiệu khối mã nào được xáo trộn và phần khởi tạo nào được sử dụng.

B.7.3.1 Cú pháp cho đoạn mã đánh dấu SEC.

Cú pháp công cụ đối với các công cụ không chuẩn tắc được sử dụng. Trong trường hợp nhiều khóa, một vài trường hợp của công cụ này được sử dụng trong đoạn mã đánh dấu SEC. Cụ thể hơn, các

trường hợp i = 0, 1, 2... với định danh phần khởi tạo nhau được giới thiệu, mỗi một trường hợp tương ứng với định danh KeyID khóa khác nhau. Điều này được minh họa dưới đây. Xem hình B.6.

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

Hình B.6 – Cú pháp công cụ bảo vệ không chuẩn tắc trong trường hợp nhiều khóa

ý nghĩa của các trường P_{ID} như sau:

Tham số	Kích thước (bit)	Giá trị
N_s	16	Số phần khởi tạo sử dụng trong trường hợp này
KeyID	32	Định danh của khóa được sử dụng để giải mã
dữ liệu	Thay đổi	Các phần khởi tạo được mã hóa

B.7.3.2 cú pháp cho đoạn mã đánh dấu INSEC

Để có thông tin về phần khởi tạo nào được sử dụng để bảo vệ khối mã, mã đánh dấu bảo mật trong dòng mã (INSEC) được sử dụng. Trong ví dụ này, nó được bổ sung vào trước các khối mã được bảo mật, để biết giống nào đã được sử dụng để bảo vệ những khối mã này. Thay vì chỉ ra các phần khởi tạo của bản thân nó, công cụ mã đánh dấu chứa một chỉ số, chỉ số này tham chiếu tới các phần khởi tạo trong đoạn mã đánh dấu SEC mào đầu chính.

B.7.4 Các kết luận

Trong mục này, công cụ bảo mật được giới thiệu để kiểm soát truy nhập có điều kiện tới các ảnh JPEG 2000. Kỹ thuật này tạo ra nhiễu giả ngẫu nhiên tới các phần được lựa chọn của dòng mã. Sau đó, ảnh mã hóa xuất hiện nhiều méo đối với bộ mã trái phép, bộ đó không biết cách loại bỏ nhiễu này.

Bảo mật của kỹ thuật này phụ thuộc vào bảo mật của thuật toán quy định cho bộ tạo số giả ngẫu nhiên và sự mã hóa của phần khởi tạo, tương ứng với các phương pháp SHA1PRNG và RSA được ưu tiên. SHA1PRNG là một PRNG bảo mật, vì không biết một chuỗi được suy ra khi biết một vài số trong chuỗi. trong ví dụ này, phần khởi tạo PRNG là 64 bit, các bit đó tạo một tấn công tàn bạo là không khả thi. Những phần khởi tạo này được mã hóa với RSA bằng cách sử dụng độ dài khóa người dùng định nghĩa. RSA được coi là một thuật toán bảo mật, cung cấp khóa đủ dài được sử dụng.

B.8 Truy nhập tiến trình đối với dòng mã JPEG 2000

B.8.1 Các dịch vụ bảo mật được xác định

Phương pháp này cung cấp một đối tượng không ảnh liên quan đến giám sát truy nhập JPEG 2000 theo một tiến trình trong dòng mã.

B.8.2 Các ứng dụng đặc thù

Một ứng dụng đặc thù của công nghệ này là phân phối ảnh bảo mật, khi đó chỉ những người được ủy quyền mới có thể biểu diễn một ảnh đã được chấp nhận. Đặc biệt, công nghệ này thích hợp cho giám sát truy nhập tuân theo trật tự một tiến trình trong một dòng mã.

B.8.3 Người sử dụng tiềm năng, mô hình thực hiện và các động cơ

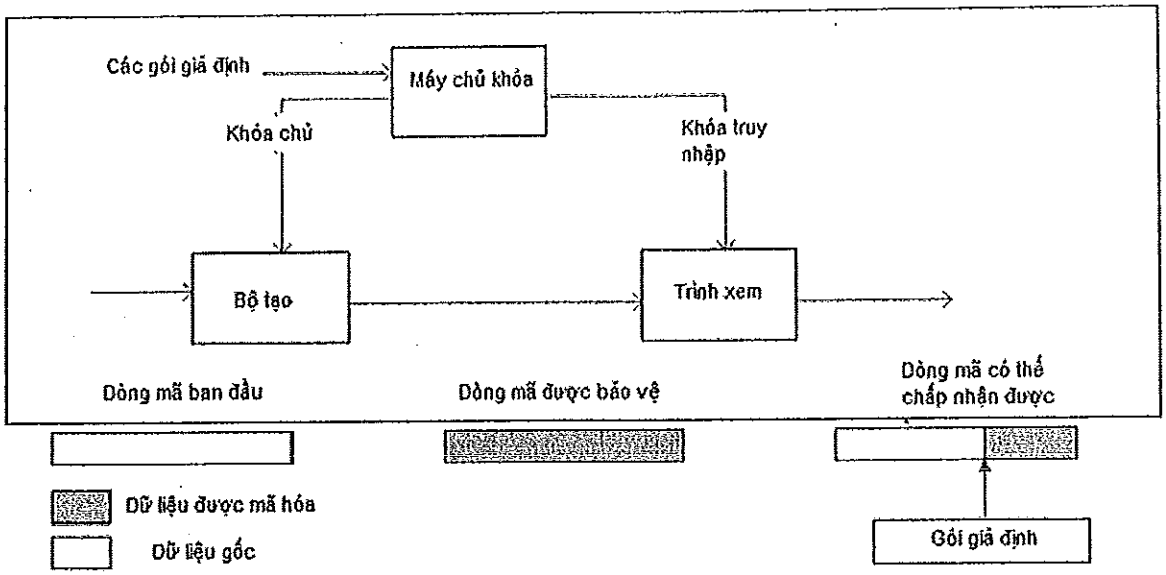
Thách thức trong việc thiết kế lược đồ giám sát truy nhập là việc cân bằng giữa các yếu tố bảo mật, tính hiệu quả và tính linh hoạt. Kỹ thuật giám sát truy nhập đối với dòng mã JPEG 2000 là xây dựng chuỗi băm để tạo ra các khóa cho mỗi gói và từ đó mã hóa các gói trong dòng mã. Vì thế, chỉ người sử dụng được phân quyền phép mới có thể giải mã gói tin đó tương ứng với ảnh gốc trong dòng mã.

B.8.4 Tổng quan công nghệ

Trong giai đoạn mã hóa, máy chủ khóa tạo ra một khóa chủ. Sau đó, bộ tạo mật mã hóa một dòng mã sử dụng các khóa gói, các khóa này được tạo ra từ khóa chủ. Trong giai đoạn giải mã, máy chủ khóa tạo ra một khóa truy nhập tuân theo gói gốc ban đầu. Sau đó, người xem giải mã dòng mã đã được mã hóa sử dụng các khóa gói được tạo ra từ khóa truy nhập.

Đặc biệt, công nghệ này sử dụng chính sách giám sát truy nhập sau: "Nếu một người dung có thể truy nhập một gói, sau đó người dùng này cũng có thể truy nhập vào các gói phía trước trong một dòng mã". Vì thế, chúng ta có thể gọi loại giám sát truy nhập là "Truy nhập lũy tiến".

Ưu điểm quan trọng của công nghệ này là số khóa cần để đi tiếp từ một máy chủ khóa đến người sử dụng ít hơn nhiều so với trường hợp thông thường. Điều này có nghĩa là công nghệ này cho phép sử dụng ít bộ nhớ hơn.



Hình B.8 –Tổng quan kỹ thuật

B.8.5 Phương pháp báo hiệu

Bảng B.20 đưa ra các tham số khuyến nghị. Mỗi tham số cần được báo hiệu theo cú pháp được xác định trong JPSEC. Đặc biệt, công nghệ này sẽ sử dụng mẫu "giải mật mã hóa", độ kết hạt "gói" và miền tiến trình "dòng bit" với ZOI tương ứng.

Bảng B.20 – Ví dụ về các tham số

Tham số		Kích thước (bits)	Giá trị	Ý nghĩa
SEC		16	0xFF65	Mã đánh dấu SEC
L_{SEC}		16	Thay đổi 0 ... 255	Độ dài của đoạn mã đánh dấu SEC
Z_{SEC}		8	0	Chỉ số của đoạn mã đánh dấu SEC
P_{SEC}		1	0	Byte FBAS không tuân theo
	F_{INSEC}	1	1_b	INSEC được sử dụng
	$F_{multiSEC}$	1	0_b	Một đoạn mã đánh dấu SEC được sử dụng
	F_{mod}	1	1_b	Dữ liệu JPEG 2000 nguyên bản đã bị chỉnh sửa

Bảng B.20 – Ví dụ về các tham số

Tham số		Kích thước (bits)	Giá trị	Ý nghĩa
	F_{TRLCP}	1	0_b	Việc sử dụng thẻ ghi TRLCP không được định nghĩa
	Padding	3	000_b	Không được sử dụng
	N_{tools}	8 (RBAS)	1	Số công cụ bảo mật là 1
	I_{max}	8 (RBAS)	0	Chỉ số mẫu công cụ tối đa bằng 0
t		8 (RBAS)	1	Công cụ bảo vệ RA
i		8 (RBAS)	0	Chỉ số mẫu
ID_{RA}	$ID_{RA,id}$	32	7	ID đã được đăng ký
	$ID_{RA,nsl}$	8 (RBAS)	21	Độ dài của $ID_{RA,ns}$ theo byte
	$ID_{RA,ns}$	168	*Không gian tên*	Không gian tên của RA với công cụ này được đăng ký
L_{zoi}		16 (RBAS)	Thay đổi	Độ dài của ZOI
ZOI		Thay đổi	Xem bảng B.21	Miền ảnh hưởng đối với công cụ này
L_{PID}		16 (RBAS)	Thay đổi	Độ dài L + T + PD + G
P_{ID}		Thay đổi	Xem bảng B.22	Các tham số cho công cụ này

Bảng B.21 – Ví dụ ZOI

Tham số			Kích thước (bits)	Giá trị (theo thứ tự)	Ý nghĩa
NDzoi			8	1	Số miền là 1
Zone[0]	DCzoi		1	0	Đoạn byte căn chỉnh không tuân theo
			1	1	đối tượng không lớp mô tả liên quan đến ảnh
			6	000100	Các gói được quy định
	Pzoi[4]	Mzoi[4]	0	1	Đoạn căn chỉnh byte không tuân theo
			1	1	Các miền quy định không bị ảnh hưởng bởi phương pháp bảo vệ
			1	1	Nhiều phần tử được quy định
			11	2	Chế độ cực đại
			00	2	Izoi sử dụng trọn 8 bit
			00	2	Izoi được mô tả theo một hướng
		Izoi[11]	8	0000 1010	Chỉ số gói > 10 được định danh

Bảng B.22 – Giá trị P_{ID}

Tham số		Kích thước (bits)	Giá trị	Ý nghĩa
T		Thay đổi	Xem bảng B.23	Các mẫu mã hóa
PD		8	$0000\ 1000_b$	Byte BAS theo sau không tồn tại. Miền dòng mã
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Thứ tự xử lý là khối ảnh-độ phân giải-lớp-thành phần-phân khu
	GL	8	$0000\ 0110_b$	Đơn vị bảo vệ là gói
H		16	xem 37 trong 5.8.3.1	Hàm băm cho công cụ tạo khóa này
L_k		8	0 ... 255	Độ dài thông tin khóa truy nhập
AK_{Info}		Thay đổi	*Giá trị khóa truy nhập*	Thông tin khóa truy nhập (thông tin này được mã hóa sử dụng KT_{bc} trong T)

Bảng B.23 – Ví dụ về mẫu mã hóa của công nghệ này

Tham số		Kích thước (bits)	Giá trị (in order)	Ý nghĩa
ME_{decry}		8	1	Giả lập mã đánh dấu không xảy ra
CT_{decry}		16	3	Mật mã khối (AES)
CP_{decry}	M_{bc}	6	10 0010	Chế độ OFB được sử dụng. (các bit không được đệm)
	SIZ_{bc}	16	128	Kích thước khối (128 bits)
	KT_{bc}	Variable	Các giá trị mẫu khóa	Mẫu khóa
	IVsc	128	Giá trị vec – tơ ban đầu	Giá trị vec – tơ ban đầu

B.8.6 Kết luận

Mục này mô tả công nghệ giám sát truy nhập cho dòng mã JPEG 2000. Ưu điểm chính là số lượng khóa được quản lý và được truy nhập là nhỏ hơn nhiều so với các trường hợp khác. Công nghệ này cho phép giám sát truy nhập JPEG 2000 linh hoạt và hiệu quả theo tiến trình thứ tự trong dòng mã.

B.9 Tính xác thực khả năng co giãn của dòng mã JPEG 2000

B.9.1 Dịch vụ bảo mật

Mục này cung cấp một cơ chế nhận thực cho dòng mã JPEG 2000. Nó cho phép người sử dụng xác minh tính xác thực và tính toàn vẹn của các ảnh phụ khác nhau với chữ ký số đơn.

B.9.2 Ứng dụng đặc thù

Các lĩnh vực ứng dụng đặc thù như chính phủ, tài chính, y tế, luật, khách hang thường yêu cầu xác thực nội dung nhận được. Theo đó, một cơ chế xác thực mở rộng để xác thực tài liệu được yêu cầu trong công tác phân tán nội dung.

B.9.3 Động cơ

Trong các ứng dụng đang công bố cho bên thứ ba, nhà sản xuất ảnh tạo ra một dòng mã và chữ ký. Sau đó, nhà sản xuất phân phối dòng mã này và chữ ký tới bên thứ ba. Người sử dụng co thể yêu cầu bên thứ ba một dòng mã đượcchuyển mã do việc giới hạn tài nguyên (như băng thông, điện toán). Bên thứ ba sẽ phân phát tới người sử dụng dữ liệu ảnh phụ cũng như bằng chứng xác thực của nó.

B.9.4 Tổng quan kỹ thuật

Lược đồ này cung cấp cơ chế xác thực linh hoạt cho các dòng mã JPEG 2000. Bao gồm ba mô-đun: tạo chữ ký, chuyển mã, xác minh. Công nghệ cơ bản này là cây Merkle, cây này tổ chức các gói JPEG 2000.

B.9.4.1 Mô-đun tạo chữ ký

Mô đun nàytạo ra chữ ký ở đầu vào dòng mã JPEG 2000 theo lược đồ chữ ký số được ưu tiên. Dòng mã này được bảo vệ bằng cách chèn mã đánh dấu SEC vào dòng mã nguyên bản. Cụ thể, bên cung cấp:

– Đọc dòng mã JPEG2000.

– Xây dựng cây băm để tạo ra giá trị gốc. Giá trị này của mỗi nút lá là giá trị băm của gói. Giá trị của mỗi nút bên trong là giá trị băm của các nút con của nó. Cấu trúc cây này tương tự với thứ tự tiến trình của một dòng mã.

– Ký giá trị gốc của cây giá trị băm với một khóa riêng dựa trên thuật toán chữ ký số.

– Tạo các tham số SEC. Chèn các tham số này vào đoạn SEC để tạo ra một dòng mã

B.9.4.2 Mô đun chuyển mã

Mô đun này tạo ra các SIT (Subsidiary Integrity Tokens) và dòng mã đã chuyển mã dựa trên độ phân giải, lớp, phần tử và vùng được yêu cầu. SEC của dòng mã mới này bao gồm các SIT và một vài tham số khác. Cụ thể, bên cung cấp và/hoặc proxy:

– Đọc các gói đã bị loại bỏ, các gói này không có trong dòng mã được chuyển mã.

– Xây dựng các nhánh giá trị băm với cá gói bị xóa bỏ.

– Chèn giá trị gốc của mỗi nhánh cây vào đoạn SEC.

Dòng mã được chuyển mã này bao gồm đoạn SEC được cập nhật và dòng mã ngoại trừ các gói bị xóa bỏ.

B.9.4.3 Mô đun xác minh

Mô-đun xác minh kiểm tra tính xác thực của dòng mã được bảo vệ. Theo lược đồ chữ ký số được ưu tiên, bộ xác minh lấy khóa công khai, sau đó thực hiện:

– Đọc dòng mã nhận được

– Xây dựng cây giá trị băm với các gói nhận được và các đầu đề dòng mã từ dưới lên trên. Nếu một số gói bị xóa bỏ, thay thế nhánh cây với một SIT tương ứng. Cứ như thế cho đến khigiá trị gốc được thiết lập.

– Kiểm tra giá trị gốc so với chữ ký số trong đoạn SEC dựa trên hệ thống chữ ký số cụ thể. Nếu phù hợp, dòng mã được chấp nhận; nếu không phù hợp thì loại bỏ gói vừa nhận được.

B.9.5 Cú pháp dòng mã

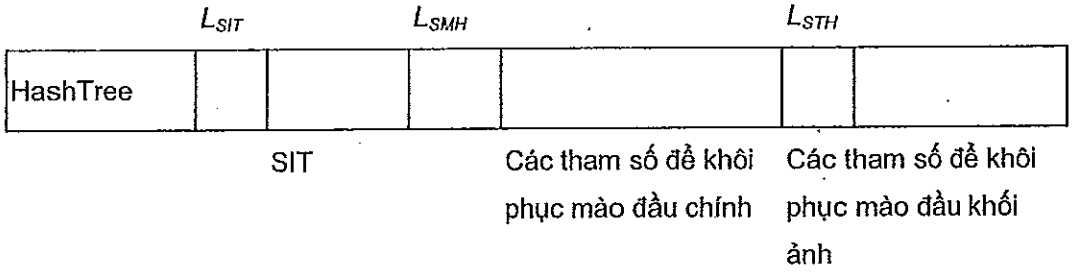
Cấu trúc SEC được đưa ra trong Bảng B.24

Bảng B.24 – Cú pháp công cụ không chính tắc

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

Tham số		Kích thước	Giá trị	Ngữ nghĩa
t		8 (RBAS)	1	Công cụ bảo vệ cơ quan đăng ký
i		8 (RBAS)	*Giá trị mẫu*	Định danh thực thể công cụ
ID_{RA}	$ID_{RA,Id}$	32	*Giá trị ID*	Định danh đã được đăng ký
	$ID_{RA,nsl}$	8 (RBAS)	21	Độ dài của $ID_{RA,ns}$ tính theo bytes
	$ID_{RA,ns}$	168	*Không gian tên*	Không gian tên của RA với công cụ đã được đăng ký
L_{ZOI}		16	$[0 ... 2^{16} – 1]$	Chiều dài các tham số đối với ZOI
ZOI_{ID}		Thay đổi	Giá trị ZOI	Tham số của miền
L_{ID}		16	$[19 ... 2^{16} – 1]$	Chiều dài các tham số
ID_T		8	2	Định danh lớp mẫu xác thực
T		Thay đổi	*Các giá trị mẫu xác thực*	Xác thực/mẫu MAC
TP_{ID}		Thay đổi	Xem Bảng B.25	tham số bảo mật

Bảng B.25 – các tham số bảo mật



Tham số	Kích thước (Bit)	Giá trị	Ý nghĩa

Cây giá trị băm	8	0 ... (2^8 – 1)	Thứ tự cây giá trị băm. Nó có thể khác với thứ tự tiến trình dòng mã. Thực hiện dò, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL khác: được dự trữ
L_{SIT}	16	0 ... (2^{16} – 1)	Số lượng SIT
SIT	Thay đổi: L_{hash}*L_{SIT}	NaN	thẻ xác thực toàn vẹn bổ sung
L_{SMH}	16	0 ... (2^{16} – 1)	chiều dài SMH
SMH	Thay đổi		Các tham số khôi phục mào đầu chính
L_{STH}	16	0 ... (2^{16} – 1)	Chiều dài cho STH
STH	Thay đổi		Các tham số cho việc khôi phục mào đầu khối ảnh
a) cho việc xác thực Keyed-MAC, khóa (xác minh) cần phải được phân phối tách biệt. b) NaN: không phải là số. c) L_{hash} là kích thước giá trị băm, ví dụ 160 đối với SHA-1.			

B.9.6 Kết luận

Công nghệ này cung cấp cơ chế xác thực linh hoạt cho dòng mã JPEG 2000. Nó có thuộc tính "ký một lần, xác minh nhiều cách". Cụ thể, sau khi một dòng mã JPEG 2000 được ký, các dòng mã khác nhau được chuyển mã từ dòng mã nguyên mẫu có thể được xác minh tin cậy với chỉ nhà sản xuất. Thuộc tính này kết nối chức năng "nén một lần, giải nén nhiều cách". Nó trái ngược với phương pháp xác thực ảnh truyền thống, phương pháp này cho phép một chữ ký xác thực chỉ một ảnh.

B.10 Độ tin cậy dữ liệu JPEG 2000 và hệ thống giám sát truy nhập dựa trên phân tách và thu hút dữ liệu

Hệ thống được mô tả trong mục này dựa trên sự phân tách, thông qua môt tiến trình gọi là Phân tách dữ liệu và thu hút dữ liệu, một tệp JPEG2000 nguyên bản ra hai tệp mới tương ứng gọi là

Lured_jp2file, chúng chuyển tải nội dung được bảo vệ và Control_file chứa thông tin cần thiết để truy nhập tới thông tin được bảo vệ. Chỉ việc kết hợp thời gian thực của hai tệp nàynhờ tiến trình Live – Composing, cho phép tái thiết lại tệp JPEG 2000 nguyên bản ban đầu. Live_Composing được quản lý bởi các quy tắc giám sát truy nhập và quản lý quyền. với hệ thống này dữ liệu JPEG 2000 và việc giám sát truy nhập linh hoạt và tin cậy hơn do hết ít thời gian và chi phí thấp.

B.10.1 Mô tả hoạt động

B.10.1.1 thực hiện dịch vụ bảo mật

– Tính tin cậy: Lured_jp2file chứa nội dung được bảo vệ. Chỉ bằng cách giải mã một Lured_jp2file đơn, nội dung đã cung cấp được xáo trộn, do đó ngăn ngừa một truy nhập tới nội dung nguyên bản ban đầu.

– Giám sát truy nhập: hệ thống này có thể được sử dụng để giám sát truy nhập đối với nội dung ảnh: một vài người sử dụng chia sẻ cùng một Lured_jp2file nhưng sở hữu các quyền truy nhập khác nhau vì thế sẽ không được phép truy nhập tới các phần giống nhau của nội dung này.

Chú ý về bảo vệ IPR: bằng cách liên kết truy nhập nội dung với xác thực và quản lý quyền, giám sát hiệu quả và theo dõi việc phát quảng bá và sử dụng nội dung được bảo vệ có thể được đảm bảo theo ý muốn của chủ sở hữu nội dung và quền của họ, có thể là sự kết hợp hệ thống này với đánh thủy vân hoặc dấu vân tay.

B.10.1.2 Các ứng dụng đặc thù

Một trong những ý tưởng chính của hệ thống này là tách tệp JPEG 2000 nguyên bản ban đầu thành hai tệp, tệp đầu tiên (Lured_jp2file) chỉ chứa 99% dữ liệu gốc và 1% dữ liệu giả gọi là mồi và có thể phân phối, phát quảng bá, trao đổi tự do hoặc sao chép thông qua bất kỳ loại mạng hoặc phương tiện truyền thông nào; tệp thứ hai (control_file) chứa 1% dữ liệu nguyên bản cộng với một số thông tin, cả hai loại dữ liệu này đều cần thiết để truy nhập tới các nội dung được bảo vệ trong Lured_lp2file.

Một ý tưởng quan trọng khác là để liên kết truy nhập này tới nội dung được bảo vệ trong Lured_jp2file với một định danh và các bước quản lý quyền và kết quả của ý tưởng là kích hoạt trực tuyến thông tin cần thiết sử dụng để khôi phục thời gian thực chỉ với thông tin không xáo trộn.

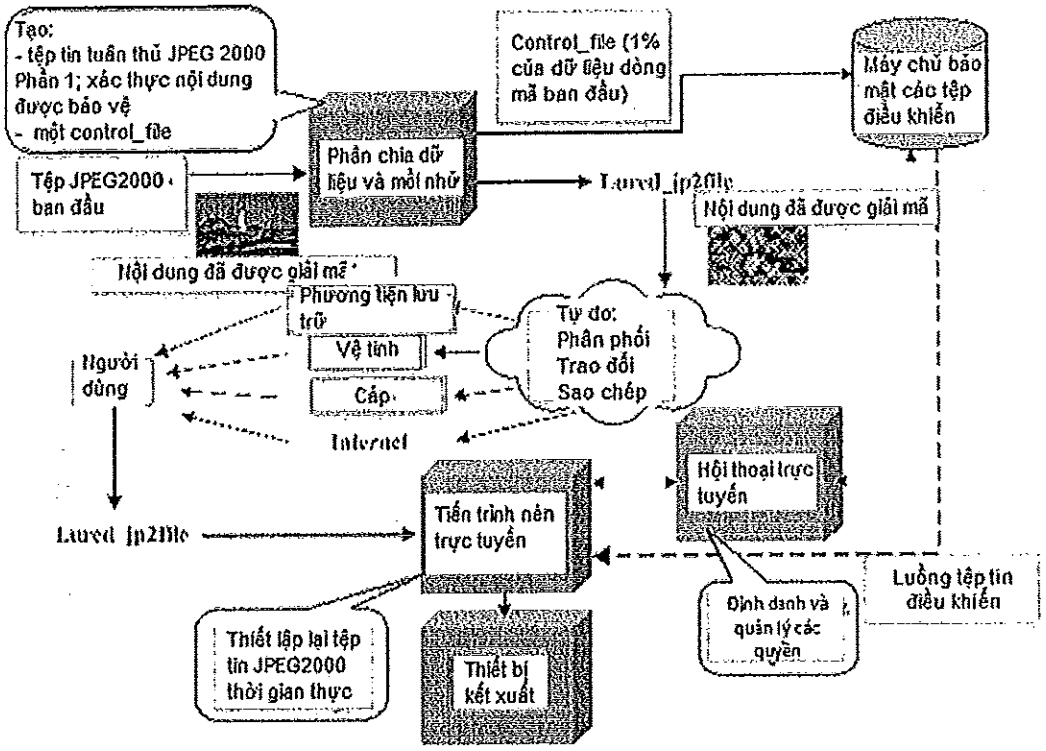
Cuối cùng, sử dụng theo dõi và báo cáo được cho phép thông qua số đo thống kê từ lịch sử control_file của máy chủđược bảo mật.

B.10.1.3 Người sử dụng tiềm năng, mô hình thực hiện và các động cơ

Những người sử dụng tiềm năng của hệ thống được mô tả này là các bộ phận tạo nội dung, chủ sở hữu và bên cung cấp nội dung vì hệ thống này đảm bảo các nội dung đó được bảo vệ và vận chuyển trong Lured_jp2file, chỉ người sử dụng được cho phép và được xác thực mới có thể truy nhập vào các nội dung nguyên bản ban đầu. Phải chú ý rằng chỉ 99% nội dung nguyên bản ban đầu được cung cấp một cách tùy thích, trong khi đó 1% cần phải truy nhập tới nội dung nguyên bản ban đầu sẽ được phân phối chỉ sau khi xác thức và các giao thức quản lý quyền được kiểm tra.

B.10.2 tổng quan kỹ thuật

Hình B.9 Tổng quan hệ thống



Hình B.9 – Tổng quan công nghệ

Tệp JPEG 2000 đầu vào được chia thành hai tệp nhờ hoạt động được gọi là "chia và thu hút dữ liệu". Hai tệp mới này: Lured_ip2file chứa nội dung được bảo vệ(nội dung JPSEC) và Control_File.

Thông qua thủ tục "chia và thu hút dữ liệu", một số phần của tệp JPEG 2000 ban đầu được trích xuất và thay thế bởi Lures. Lered_ip2file chứa khoảng 99% nội dung tệp ban đầu trong khi 1% còn lại là dữ liệu giả và được gọi là lures, ví dụ dữ liệu không có bất kỳ ưu tiên liên kết với dữ liệu nguyên bản. Không giống với mã cổ điển, tiến trình thu hút không phải là một cơ sở quan trọng. Lured_ip2file có thể được phân phối, trao đổi hoặc sao chép tự do bởi bất kỳ người dung nào. Control_file chứa 1% dữ liệu nguyên bản được trích xuất từ tệp nguyên bản. Nó được lưu trong *máy chủ bảo mật chứa các tệp giám sát.*

Khi Lured_ip2file được giải mã bởi bất kỳ một bộ giải mã JPEG 2000 phần 1, nội dung này có vẻ như bị xáo trộn. Chỉ có một cách để truy nhập tới nội dung nguyên bản là khôi phục dữ liệu nguyên bản đã bị trích xuất nhờ Control_File. Thiết bị Live_Composing kết nối tới máy chủ bảo mật của các tệp giám sát thông qua giao thức Live_Dialog và một định danh và giao thức quản lý quyền xuất hiện:

– nếu người sử dụng sở hữu các quyền này và đồng ý các điều kiện truy nhập nội dung (ví dụ, thanh toán hoặc đăng ký) dữ liệu đã trích xuất được thu hồi lại từ Control_file và tệp JPEG 2000 nguyên bản được khôi phục theo thời gian thực. Tuy nhiên, theo quyền người dung, tái xây dựng lại

tệp JPEG 2000 có thể phân tách (ví dụ, chỉ cho phép truy nhập tới khối ảnh cụ thể và/hoặc thành phần màu và/hoặc độ phân giải và/hoặc ranh giới và/hoặc các lớp chất lượng) hoặc là toàn bộ.

– nếu người sử dụng không sở hữu các quyền hoặc không chấp nhận các điều kiện, chỉ nội dung đã xáo trộn được hiển thị.

Các đặc điểm chính của hệ thống:

– Chia tệp JPEG nguyên bản ban đầu thành hai tệp, tệp thứ nhất chứa nội dung JPEG 2000 được bảo vệ với 99% dữ liệu nguyên bản cộng với 1% dữ liệu giả gọi là Lures (Lured_jp2file), tệp thứ hai lưu 1% dữ liệu nguyên bản cần thiết để tái thiết lại nội dung JPEG 2000 ban đầu;

– Xáo trộn trực quan các nội dung;

– Tuân thủ và bảo toàn kích thước tệpJPEG 2000 Phần 1;

– Tỷ lệ bit thấp và chi phí hệ thống bảo vệ thấp

Hệ thống này có thể được sử dụng với bất kỳ môi trường và/hoặc hệ điều hành nào. Không yêu cầu một phần cứng hay phần mềm cụ thể nào.

Tiến trình thu hút sẽ chèn mã đánh dấu SEC sau đây vào Lured_jp2file.

Bảng B.26 – Các giá trị tham số cho công cụ này

Tham số		Kích thước (bit)	Giá trị (số thứ tự)	Ý nghĩa suy ra
SEC		16	0xFF65	Mã đánh dấu SEC
L_{SEC}		16	0xXXXX	Chiều dài của đoạn mã đánh dấu SEC
Z_{SEC}		8	1 ... 255	Chỉ số của đoạn mã đánh dấu
P_{SEC} (if Z_{SEC} = 1)	F_{INSEC}	1	0	INSEC không được sử dụng
	$F_{multiSEC}$	1	0	Một đoạn mã đánh dấu SEC được sử dụng
	F_{J2K}	2	1	Dòng JPSEC phù hợp với JPEG 2000 phần 1
	F_{TRLCP}	1	0	Sử dụng gán thẻ TRLCP không được định nghĩa trong trường này.
	N_{tools}	7	1	Một công cụ bảo mật được sử dụng trong dòng mã này

	I_{max}			7	1	Maximum tool instance index value used
	Padding			5	0	Padding
Tool[(0)]	t			8 (RBAS)	1	Công cụ bảo vệ không chính tắc
	i			8 (RBAS)	0	Tool instance index
	ID_{RA}	$ID_{RA,Id}$		32	ID	RA được sử dụng để phân phát số ID
		$ID_{RA,nsl}$		8 (RBAS)	21	Chiều dài của $ID_{RA,ns}$ là 21 byte
		$ID_{RA,ns}$		168	*Không gian tên*	Không gian tên của RA với công cụ này được đăng ký.
	L_{ZOI}			16	*Length value*	Độ dài L_{ZOI} + ZOI
	ZOI	NZ_{ZOI}		8	0...254	Số miền
		$Zone^0$	DC_{ZOI}	1	0	Đoạn căn chỉnh byte không tuân theo
				1	1	Đối tượng không lớp mô tả liên quan đến ảnh
				6	000010	Các chỉ số gói được quy định
			$Pzoi^{0,0}$ Mzoi	1	0	Đoạn căn chỉnh byte không tuân theo
				1	0	Các miền quy định chịu ảnh hưởng của phương pháp bảo vệ này
				1	1	Nhiều phần tử được quy định
				2	10	Index mode
				2	xx	Izoi sử dụng 8- hoặc 16- hoặc 32-bit
				1	0	Izoi được mô tả theo một hướng
			Nzoi	8	Thay đổi	2 ... 255 (số các chỉ số gói)

				Izoi[i]	xxx Nzoi	Thay đổi	Chỉ số gói
	L_{PID}				16	0 ... (2^{16} – 1)	Chiều dài L_{PID} + P_{ID} (byte)
	P_{ID}				Thay đổi	Thay đổi	Control_File ID, URL của máy chủ Control_File...; Cú pháp đầy đủ được cung cấp bởi RA

Các công cụ cần thiết để thực hiện các tiến trình nén trực tiếp và/hoặc thu hút và chia dữ liệu có thể được cung cấp thông qua một kết nối tới cơ quan đăng ký và tải về từ nó.

B.11 Chuyển mã bảo mật và tạo dòng phân cấp bảo mật

B.11.1 Tổng quan và động cơ thúc đẩy

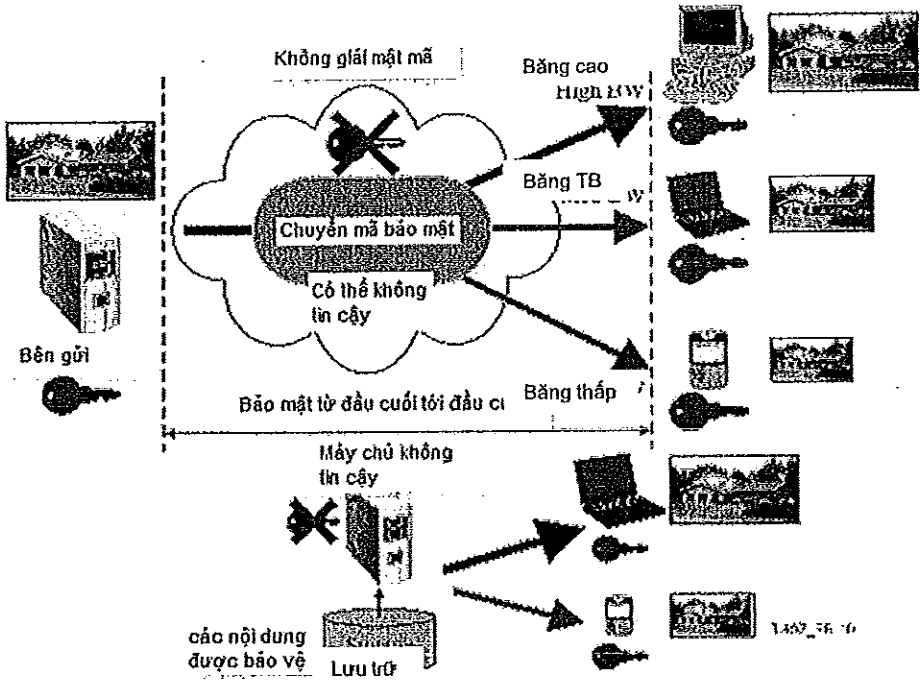
Mục này mô tả một phương pháp để cung cấp các dịch vụ bảo vệ tin cậy và xác thực các dòng mã theo cách:

1) Cho phép một thực thể (có khả năng là không bảo mật) chuyển mã bảo mật hoặc tương thích với JPSEC bảo vệ các dòng mà không yêu cầu thực thể đó mở khóa bảo vệ hoặc giải mã nội dung; và

2) Cho phép một khách xác nhận hoạt động chuyển mã được thực hiện theo cách hợp lệ và cho phép.

Việc chuyển mã thường yêu cầu tương thích với nội dung đã được mã hóa theo JPEG 2000 cho các khách hàng với tính đa dạng của thiết bị (như màn hình hiển thị nhỏ hoặc tốc độ kết nối mạng thấp) và đối với các điều kiện mạng thời gian thay đổi. JPEC 2000 đặc biệt phù hợp với các ứng dụng chuyển mã nhờ phân cấp vốn có của nó. Tuy nhiên, nếu không cẩn thận khi bảo vệ các dòng mã JPEG, thuộc tính mở rộng có thể mất. Ví dụ, nó xảy ra khi toàn bộ dòng mã được mã hóa như một tệp đơn. Trong trường hợp này, chỉ có một cách để chuyển mã dòng mã được bảo vệ là thực hiện mã hóa và sau đó chuyển mã hoặc thích ứng dòng giải mã.

JPEC được thiết kế để đảm bảo việc chuyển mã của nội dung được bảo vệ JPSEC, nơi việc chuyển mã bảo mật được xác định như là việc chuyển mã không được bảo vệ (việc giải mã) nội dung. Đạt được tính năng này



Hình B.10 – JPSEC cho phép bảo mật đầu cuối –đầu cuối và chuyển mã bảo mật giữa mạng

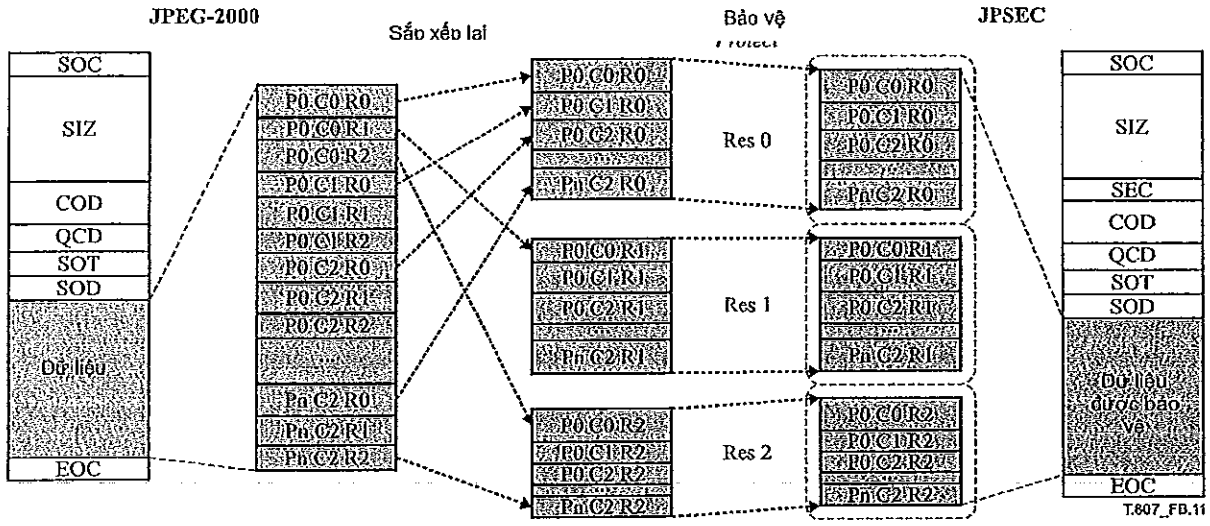
B.11.2 Mô tả hoạt động và ví dụ sử dụng

Trong ví dụ này, dòng mã JPEG 2000 ban đầu theo thứ tự RLCP và với mục tiêu bảo vệ dòng mã bằng cách mật mãhóa và xác thực trong khi cho phép chuyển mã bảo mật nhờ những nỗ lực trên dòng mã được bảo vệ. Do dòng mã ban đầu sử dụng thứ tự RLCP nên mỗi thành phần phân giải được tái diễn bởi một đoạn dữ liệu liền kề. Việc mật mã hóa có thể được thực hiện trên từng đoạn của ba đoạn liền kề. Mào đầu JPSEC quy định ba miền ảnh hưởng mô tả thành phần phân giải, đoạn dòng mã, và mẫu mã hóa được sử dụng cho mỗi đoạn. Xác thực cũng được thực hiện trên từng đoạn của ba đoạn dữ liệu, hoặc là trước hoặc là sau mật mã hóa phụ thuộc vào chức năng mong muốn. Điều này cũng được quy định trong đầu đề SEC sử dụng mẫu xác thực.

Để thực hiện chuyển mã bảo mật trên dòng mã JPSEC, Bộ chuyển mã đọc và phân tích các mào đầu, định danh các vị trí của các đoạn độ nét, và sau đó giữ lại hoặc loại bỏ các đoạn/độ phân giải dữ liệu thích hợp. Chú ý rằng hoạt động chuyển mã này tương ứng với hoạt động phân tích đơn giản và nó không yêu cầu thôi bảo vệ dữ liệu này. Xác thực được thực hiện bằng cách xác thực dữ liệu chuyển mã nhận được với các giá trị MAC, các giá trị này được thay thế trong mào đầu SEC trong suốt tiến trình bảo vệ JPSEC.

Trong ví dụ thứ hai, mục tiêu đưa ra là tiếp tục bảo vệ dòng mã trong khi vẫn cho phép chuyển mã bởi độ phân giải; tuy nhiên, ví dụ này có phần phức tạp hơn vì dòng mã JPEG 2000 gốc theo thứ tự PCRL chứ ko phải là RLCP, do đó các đoạn dữ liệu tương ứng với ba thành phần phân giải không liền kề trong dòng mã gốc ban đầu. JPSEC cho phép mục tiêu chuyển mã hoặc mở rộng bảo mật bằng độ phân giải đạt được theo một số cách. Có một phương pháp là mã hóa các gói riêng biệt trong khi tách

bỏ mào đầu gói không mã hóa. Điều này giữ lại mức mở rộng cao nhất trong dòng nhưng cũng yêu cầu hoạt động chuyển mã bảo mật phức tạp do bộ chuyển đổi phải phân tích dòng JPSEC ở mức gói. Một giới hạn khác là các kết quả của hoạt động chuyển mã bảo mật đơn giản là để sắp xếp lại dữ liệu, vì thế các thành phần phân giải tiếp tục ở trong các đoạn liên kề, độ dịch của các đoạn này được báo hiệu trong mào đầu SEC. Điều này có thể đạt được theo cách phù hợp bằng cách sắp xếp lại các gói JPEG 2000 từ thứ tự PCRL cho đến RLCP và báo hiệu thứ tự tiến trình mới trong đoạn mã đánh dấu COD hoặc với thay đổi thứ tự tiến trình (POC) đoạn mã đánh dấu. Kết quả sắp xếp lại dữ liệu và việc chuyển đổi bảo vệ được đưa ra trong hình B.11. Một lần nữa mào đầu SEC chính chứa các tham số ZOI mô tả ảnh liên quan tương ứng và các tham số dòng bit – liên quan được kết hợp với mỗi một đoạn dữ liệu.



Hình B.11 – Ví dụ của việc tạo lập một dòng mã JPSEC

B.11.3 Cú pháp dòng mã

Cú pháp dòng mã JPSEC có thể được sử dụng để tạo dòng có khả năng co giãn bảo mật và hệ thống chuyển mã bảo mật với công cụ bảo vệ mẫu. Đặc biệt, Miền ảnh hương (ZOI) có thể được sử dụng với mẫu mã hóa, vùng xử lý, và Độ chi tiết để định nghĩa một cách đầy đủ tiến trình giải mã, tiến trình này cho phép khách hàng JPSEC có thể sử dụng để giải mã dòng mã. Ngoài ra, các tham số ZOI cho biết thông tin mà các Nút chuyển mã có thể sử dụng để thực hiện chuyển mã bảo mật.

ZOI quy định ba miền, mỗi một miền cho một độ phân giải, và khoảng byte được kết hợp với các bit được mật mã hóa cho mỗi miền. Cú pháp báo hiệu cho mẫu bảo vệ giải mật mã, miền xử lý và Độ chi tiết được đưa ra trong Bảng B.27. Phương pháp giải mã này được báo hiệu với mẫu bảo vệ giải mã. Trong trường hợp này, nó quy định việc mã hóa AES trong chế độ CTR, và kích thước khối và độ dài khóa. Ngoài ra, Miền xử lý này và độ chi tiết quy định cách thực hiện giải mã. Nó báo hiệu cho biết miền xử lý là bản thân dòng bit và các mào đầu gói và thân gói được mã hóa. Các phương pháp giải mã khác có thể được quy định bằng cách thay đổi miền tiến trình và độ chi tiết. Ví dụ, Độ chi tiết của việc mã hóa có thể ở trên các gói riêng biệt hoặc chỉ trên thân các gói. Hơn nữa, phương pháp xác

thực được quy định với cùng một ZOI như trên nhưng với mẫu xác thực như sau. Cú pháp cho mẫu xác thực này được đưa ra trong Bảng B.28 để sử dụng HMAC với SHA-1 để xác thực. Tuy nhiên, các mật mã JPSEC và MAC khác cũng có thể được sử dụng. Thêm vào đó, giải pháp được đề xuất có thể được sử dụng với chữ ký số, giám sát truy nhập và các công cụ quản lý khóa khác. Ngoài ra, méo có thể kết hợp với mỗi gói (hoặc các miền khác của dữ liệu) sử dụng trường méo này (xem 5.7.3.2) để cho phép tốc độ méo (R-D) tối ưu việc tạo dòng bảo mật và chuyển đổi mã bảo mật.

Bảng B.27 – Các giá trị tham số đối với công cụ bảo vệ mẫu, miền xử lý và độ chi tiết

Tham số			Kích thước (bits)	Giá trị (số thứ tự)	Ý nghĩa
T_{decry}	ME_{decry}		8	0	Cờ mô phỏng mã đánh dấu là NULL
	CT_{decry}		16	1	Mã hóa AES
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	CTR và không có đệm
		P_{bc}	2	0	Đệm không được sử dụng cho chế độ CRT
		SIZ_{bc}	8	128	Kích thước khối là 128 bit
		KT_{bc}	thay đổi	*mẫu khóa*	Mẫu thông tin khóa
PD			1	0_b	Đoạn căn chỉnh byte (BAS) không tuân theo
			1	0_b	Không phải trong phạm vi điểm ảnh
			1	0_b	Không phải trong miền hệ số song con
			1	0_b	Không phải trong miền hệ số song con được lượng tử hóa
			1	1_b	Xử lý trong miền dòng mã
			3	000_b	Không được sử dụng
G		PO	16	$0\ 0000\ 0101\ 0011\ 100_b$	Thứ tự tiến trình là TRLCP

	GL	8	$0000\ 1001_b$	Độ chi tiết là toàn bộ miền được định danh bởi ZOI
V	N_V	16	1	Một giá trị được quy định
	Sv	8	16	Kích thước là 16 byte
	VL	128	*Nonce value*	Giá trị đếm cho chế độ CTR

Bảng B.28 – Giá trị tham số cho công cụ bảo vệ mẫu xác thực

Tham số			**kích thước (bit)**	**Giá trị**	**Ý nghĩa suy ra**
T_{auth}	M_{auth}		8	0	MAC dựa vào hàm băm
	P_{auth}	M_{HMAC}	8	1	HMAC
		H_{HMAC}	8	1	ID băm là SHA-1
		KT_{HMAC}	Thay đổi	*Giá trị khóa*	Xem mẫu khóa
		SIZ_{HMAC}	16	80	Kích thước MAC size 80 bit (được cắt từ 160) Kích thước MAC là 80 bit (cắt từ 160)

B.11.4 Kết luận

Mục này mô tả việc tạo dòng phân cấp bảo mật và chuyển đổi mã bảo mật với JPSEC, nó cho phép các thuộc tính có vẻ đối lập nhưviệc bảo mật đầu cuối đến đầu cuối với việc chuyển đổi mã bảo mật ở các nút giữa mạng. Nó cho phép dòng mã JPSEC được chuyển mã mà không yêu cầu giải mã. Ngoài ra, phương pháp này cung cấp việc xác thực việc chuyển đổi mã chỉ được thực hiện theo cách hợp lệ và được cho phép, và không có sự thay đổi chủ ý hoặc độc hại từ một lỗi hoặc từ kẻ tấn công. Nó cho phép một máy chủ (có khả năng là không bảo mật) hoặc nút giữa mạng ví dụ như proxy để thực hiện chuyển mã bảo mật trong khi vẫn cho phép một khách hàng JPSEC xác thực nội dụng đã nhận được chuyển mã theo cách hợp lệ và cho phép.

Phụ lục C

(Quy định)

Khả năng tương tác

C.1 Phần 1

Số phương pháp bảo vệ có thể được áp dụng cho dòng mã JPEG 2000 để tạo ra các dòng mã JPEG mà vẫn tuân thủ nghiêm chỉnh JPEG 2000 phần 1. Chúng ta sử dụng thuật ngữ "Tuân thủ phần 1" để đề cập đến các dòng mã JPSEC mà được quy định nghiêm ngặt cho người lập trình JPEG 2000 phần 1 bao gồm cả những người không có khái niệm về JPSEC.

Người lập trình JPEG 2000 phần 1 sẽ bỏ qua mã đánh dấu các đoạn mã đánh dấu không được công nhận. Công cụ JPSEC chẳng hạn như công cụ JPSEC quy định để xác thực chèn các giá trị mã xác thực bản tin, các giá trị này được tính toán từ dữ liệu JPEG 2000 vào đoạn mã đánh dấu SEC cùng với các tham số mô tả các phương pháp xác thực đặc biệt mà người sử dụng JPSEC sử dụng. Những tham số này và các giá trị cho khách hang JPSEC cách xác minh dòng mã nhận được là đúng. Chú ý công cụ xác thực JPSEC không thao tác dữ liệu JPEG 2000. Vì vậy, một bộ giải mã JPEG 2000 phần 1 nhận được dòng mã JPSEC này sẽ bắt đầu giải mã dòng JPSEC, sau đó nó sẽ bỏ qua đoạn mã đánh dấu SEC, và tiếp tục để giải mã dòng JPSEC như thể nó là một dòng JPEG 2000 phần 1. Công cụ chính tắc JPSEC cho việc xác thực chia sẻ những đặc điểm này và do đó cũng kết quả cũng tuân thủ dòng mã trong Phần 1.

JPSEC cho phép mật mã hóa và giải mã được thực hiện trên JPEG 2000 và các dòng mã JPSEC. Khi mật mã hóa được sử dụng, dữ liệu JPEG 2000 tất nhiên thay đổi. Nói đúng ra, Tuân thủ phần 1 không phù hợp với dòng mã được mật mã hóa vì nó rất có thể sẽ làm cho bộ giải mã phần 1 JPEG 2000 xem giá trị không hợp lý. Một trong những cách có thể khắc phục hoặc ít nhất là giảm nhẹ vấn đề này là sử dụng các khả năng kháng lỗi của JPEG 2000. Với đàn hồi lỗicó thể có dòng mã JPSEC được mật mã, các dòng mã này có một số khả năngđược định nghĩa cho bộ giải mã JPEG 2000 phần 1.

JPSEC có trường tham số P_{sec} chứa các tham số bảo mật cho toàn bộ dòng mã. Nó bao gồm một cờ F_{J2K}, cờ này có thể được thiết lập là 1 để chỉ ra rằng một dòng mã JPSEC có khả năng giải mã bởi bộ giải mã JPEG 2000 phần 1. Một bộ tạo JPSEC có thể thiết lập tham số này vì nó áp dụng các công cụ JPSEC cho các dòng mã JPEG 200. Một vấn đề đã được đề cập là một bộ tạo JPSEC có thể chấp nhận một dòng mã JPSEC được bảo vệ như đầu vào. Nếu một bộ tạo JPSEC nhận được một dòng mã JPSEC đầu vào, dòng mã đó có cờ F_{J2K} thiết lập chỉ thị Tuân thủ phần 1 và sau đó áp dụng công cụ JPSEC không tuân thủ phần 1, nó phải đặt cờ FJ2K là 0.

Đối với các dòng JPSEC không tuân thủ phần 1 được khuyến nghị sử dụng mở rộng tệp .jp2s để cho biết bộ giải mã JPEG 2000 phần 1 không thể giải mã được dòng mã được bảo vệ.

C.2 Phần 2

Phiên bản JPEG 2000 phần 2 sửa đổi lần 2 mở rộng đoạn mã đánh dấu (CAP) cho biết JPSEC được sử dụng. Cụ thể, phần 2 sử dụng tham số R_{siz} để cho biết sự hiện diện của một đoạn mã đánh dấu CAP, có chứa một tham số C_{cap} , tham số đó có thể được sử dụng để báo hiệu phần JPEG 2000 nào được sử dụng trong dòng mã này. Sử dụngJPEG 2000 phần 8 (JPSEC) được báo hiệu bằng cách thiết lập bit thích hợp trong Ccap.

Vì vậy, bộ tạo JPSEC có thể thiết lập tham số R_{siz} để cho biết sự hiện diện của một đoạn mã đánh dấu CAP. Có thể chèn hoặc chỉnh sửa đoạn mã đánh dấu CAP để thiết lập các tham số C_{cap} báo hiệu phần 8 được sử dụng.

C.3 JPIP

C.3.1 Mối quan hệ giữa JPIP và JPSEC

JPIP quy định giao thức bao gồm một loạt các tương tác có cấu trúc giữa một người dùng và máy chủ theo cách những siêu dữ liệu tập tin ảnh, cấu trúc và một phần hoặc toàn bộ dòng mã có thể được trao đổi hiệu quả trong thông tin và truyền thông.

JPIP có thể được thiết kế thông qua các phần mở rộng khác nhau tới định dạng tập tin JPEG 2000, như được định nghĩa trong ITU-T Rec. T.801 | ISO/IEC 15444-2, ITU-T Rec. T.802 | ISO/IEC 15444-3 và ITU-T Rec. T.805 | ISO/IEC 15444-6. Tuy nhiên, để đạt được một mức độ tương tác đơn giản mà cho phép các phần của một tập tin JPEG 2000 đơn hoặc dòng mã được truyền, các khả năng khác không bắt buộc.

Những quy định cho phần mở rộng của giao thức JPIP nhằm hỗ trợ các tiêu chuẩn JPEG 2000 hiện hành ITU - T Rec. T.802 | ISO/IEC 15444-3, JPEG 2000 động, và ITU-T Rec. T.805 | ISO/IEC 15444-6, và các phần khác của JPEG 2000 sẽ được công bố trong tương lai (hiện tại là JP3D, JPSEC, và JPWL).

JPSEC cung cấp dịch vụ bảo mật cho ảnh JPEG 2000. Cú pháp JPSEC hỗ trợ hai loại mã đánh dấu: SEC và INSEC. Một hoặc nhiều hơn các mã đánh dấu SEC xuất hiện trong mào đầu chính của dòng bit JPSEC. Nói cách khác, JPSEC sử dụng một dòng mã JPEG 2000, hiệu chỉnh mào đầu chính JPEG 2000 để tạo thành một "mào đầu chính" JPSEC mới, và hiệu chỉnh dòng mã JPEG 2000 tương ứng để tạo thành một dòng mã được bảo vệ mới phù hợp. Các mã đánh dấu INSEC có thể xuất hiện một cách tùy chọn trong phần "dữ liệu" của dòng dữ liệu. Nó quy định một số tham số "kích thước nhỏ hơn" hoặc "vùng cục bộ" so với mã đánh dấu SEC và có thể được sử dụng bổ sung cho mã đánh dấu SEC.

Theo quan sát cho thấy JPIP vượt ra ngoài tầng giao vận, trong khi JPSEC ở lớp ứng dụng. Theo đó, JPIP cung cấp dịch vụ vận chuyển tới JPSEC. Tức là JPIP cung cấp các công cụ phân phối thông tin ảnh hiệu quả, bao gồm mào đầu chính (Tất cả các mã đánh dấu) và các dòng mã, giữa máy chủ và người dùng. Mục này này xem xét cách thức sử dụng JPIP để truyền tải nội dung JPSEC.

C.3.2 Các vấn đề cụ thể về khả năng tương tác giữa JPIP và JPSEC

Mục này mô tả những vấn đề mà một bên gửi và bên nhận JPIP phải xem xét để truyền tải nội dung JPSEC.

Trong A.3.5 "thùng dữ liệu mào đầu chính" của ITU-T Rec. T.808 | ISO/IEC 15444-9, cả hai loại phương tiện truyền thông dòng JPP và dòng JPT sử dụng thùng dữ liệu mào đầu chính. Thùng dữ liệu này bao gồm một danh sách liên tiếp tất cả các đoạn mã đánh dấu và mã đánh dấu trong mào đầu chính, bắt đầu từ điểm mã đánh dấu SOC. Nó không chứa các mã đánh dấu SOT, SOD hay EOC. Tuy nhiên, các mào đầu chính của JPEG 2000 không bao gồm mã đánh dấu SEC và phân đoạn của nó. Kết quả là, A.3.5 của JPIP FCD 2.0 không quy định hỗ trợ đối với đoạn mã đánh dấu SEC được quy định trong JPSEC. Do đó, bên gửi và bên nhận JPIP phải được hiệu chỉnh để công nhận các đoạn mã đánh dấu SEC mã đánh dấu xuất hiện trong mào đầu chính của một dòng mãJPSEC.

A.3.2 "Phân khu các thùng dữ liệu" của ITU-T Rec. T.808 | ISO/IEC 15444-9 mô tả hỗ trợ của nó cho dữ liệu phân khu. Tuy nhiên, A.3.2 của JPIP FCD 2.0 không quy định hỗ trợ mã đánh dấu INSEC và đoạn mã đánh dấu được quy định trong JPSEC. Do đó, bên gửi và bên nhận JPIP phải có sự hiệu chỉnh để nhận ra các đoạn mã đánh dấu INSEC xuất hiện trong dữ liệu dòng mã JPSEC.

Trong A.3.3 "Thùng dữ liệu mào đầu khối ảnh" của tiêu chuẩn ITU-T Rec. T.808 | ISO/IEC 15444-9, thùng dữ liệu mào đầu khối ảnh chỉ xuất hiện trong kiểu phương tiện dòng JPP. Đối với thùng dữ liệu thuộc lớp này, bộ định danh trong lớp giữ chỉ số (bắt đầu từ 0) của khối ảnh mà thùng dữ liệu đề cập. Thùng dữ liệu này bao gồm điểm mã đánh dấu và đoạn mã đánh dấu cho khối ảnh n. Nó không chứa đoạn mã đánh dấu SOT. Các điểm mã đánh dấu SOD là tùy chọn. Thùng dữ liệu này có thể được hình thành từ một dòng mã hợp lệ, bằng cách ghép tất cả các đoạn mã đánh dấu trừ SOT và POC trong tất cả các mào đầu phần - khối ảnh đối với khối ảnh n.

Trong A.3.4 "Thùng dữ liệu khối ảnh" của tiêu chuẩn ITU-T Rec. T.808 | ISO/IEC 15444-9, thùng dữ liệu khối ảnh sẽ chỉ được sử dụng với các loại phương tiện truyền thông dòng JPT. Đối với dữ liệu-thùng thuộc lớp này, định danh trong lớp là chỉ số (bắt đầu từ 0) của khối ảnh mà thùng dữ liệu thuộc vào. Mỗi thùng dữ liệu khối ảnh tương ứng chuỗi byte được hình thành bằng cách ghép tất cả các phần của khối ảnh đó, để hoàn chỉnh với SOT, SOD của chúng và tất cả các đoạn mã đánh dấu có liên quan khác.

Như đã đề cập ở trên, A.3.4 và A.3.5 của ITU-T Rec. T.808 | ISO/IEC 15444-9 mô tả sự hỗ trợ để mào đầu phần khối ảnh và dữ liệu phần khối ảnh. Tuy nhiên, ITU-T Rec. T.808 | ISO/IEC 15444-9 không quy định nếu chúng hỗ trợ các đoạn mã đánh dấu SEC và đoạn mã đánh dấu INSEC. Do đó, bên gửi và bên nhận JPIP phải được hiệu chỉnh để nhận ra và vận chuyển các đoạn mã đánh dấu cùng với các dữ liệu được bảo vệ.

C.3.3 Tổng quan

Nói chung, JPSEC làm cho bản thân phù hợp để được vận chuyển bằng JPIP. Mã đánh dấu INSEC được sử dụng trong dòng mã để mô tả một số phần nhỏ dữ liệu quy định, dữ liệu này được bảo vệ bởi công cụ/các công cụ bảo mật. Nó làm cho JPSEC linh hoạt hơn. Để làm cho INSEC hữu ích hơn, các

lớp dịch vụ (có nghĩa là JPIP) sẽ cung cấp chất lượng dịch vụ hay việc bảo vệ tốt trên điểm mã đánh dấu INSEC và phân đoạn của nó. Để đạt được mục tiêu này, JPIP và JPSEC cần phải tìm ra một số vấn đề và đảm bảo tương tác giữa JPIP và JPSEC.

C.4 JPWL

JPEG 2000 hoặc JPWL không dây (ITU-T Rec. T.810 | ISO/IEC 15444-11) mở rộng các thuộc tính của JPEG 2000 để đạt được hiệu quả truyền dẫn ảnh JPEG 2000 qua một môi trường truyền dễ bị lỗi. Cụ thể hơn, JPWL định nghĩa một tập hợp các công cụ và phương pháp để bảo vệ dòng mã khỏi các lỗi truyền dẫn. Nó cũng xác định phương tiện để mô tả sự nhạy cảm của dòng mã với lỗi truyền, và để mô tả các vị trí trong dòng mã của lỗi dư truyền dư ra.

Đặc biệt JPWL giải quyết việc bảo vệ mào đầu ảnh, các mã sửa lỗi trước FEC, bảo vệ lỗi không đồng đều (UEP), mã hóa kết hợp nguồn - kênh, phân vùng và kỹ thuật đan xen dữ liệu, và mã số học chống lỗi. JPWL không được liên kết với một mạng hoặc giao thức vận chuyển cụ thể, nhưng cung cấp giải pháp chung để truyền ảnh JPEG 2000 trên mạng dễ bị lỗi.

Các chức năng chính của JPWL:

- bảo vệ dòng mã chống lại lỗi truyền;
- mô tả độ nhạy của các phần khác nhau của dòng mã với lỗi truyền;
- mô tả các vị trí của lỗi dư trong dòng mã.

JPWL định nghĩa bốn đoạn mã đánh dấu: Khả năng bảo vệ lỗi (EPC), Khối bảo vệ lỗi (EPB), Bộ mô tả nhạy lỗi (ESD) và Bộ mô tả lỗi dư (RED).

Đoạn mã đánh dấu EPC cho biết những công cụ qui định và không quy định của JPWL được sử dụng trong dòng mã. Cụ thể hơn, EPC báo hiệu liệu ba đoạn mã đánh dấu khác có tính quy định được xác định bởi JPWL, cụ thể là mô tả độ nhạy lỗi (ESD), mô tả lỗi dư (RED) và khối bảo vệ lỗi (EPB) có mặt trong dòng mã không. Hơn nữa, EPC báo hiệu việc sử dụng các công cụ không quy định mà trước đây đã được đăng ký với JPWL RA. EPC là bắt buộc trong một dòng mã JPWL.

Chức năng chính của EPB là để bảo vệ mào đầu chính và mào đầu phần khối ảnh. Tuy nhiên, nó cũng có thể được sử dụng để bảo vệ phần còn lại của dòng mã. Đoạn mã đánh dấu EPB chứa thông tin về tham số bảo vệ lỗi và dữ liệu dư được sử dụng để bảo vệ dòng mã khỏi các lỗi.

Đoạn mã đánh dấu ESD chứa thông tin về sự nhạy cảm của dòng mã với lỗi. Thông tin này có thể được khai thác khi áp dụng một kỹ thuật bảo vệ lỗi không đồng đều (UEP). Một cách thẳng thắn, mã hóa mạnh hơn được sử dụng để bảo vệ phần nhạy với lỗi nhất của dòng mã. Thông tin này cũng có thể được sử dụng cho việc truyền lại có chọn lọc. Cuối cùng, thông tin được mang trong ESD cũng có thể được sử dụng cho các ứng dụng không phải JPWL chẳng hạn như chuyển mã hiệu quả hoặc việc tìm nạp trước thông minh.

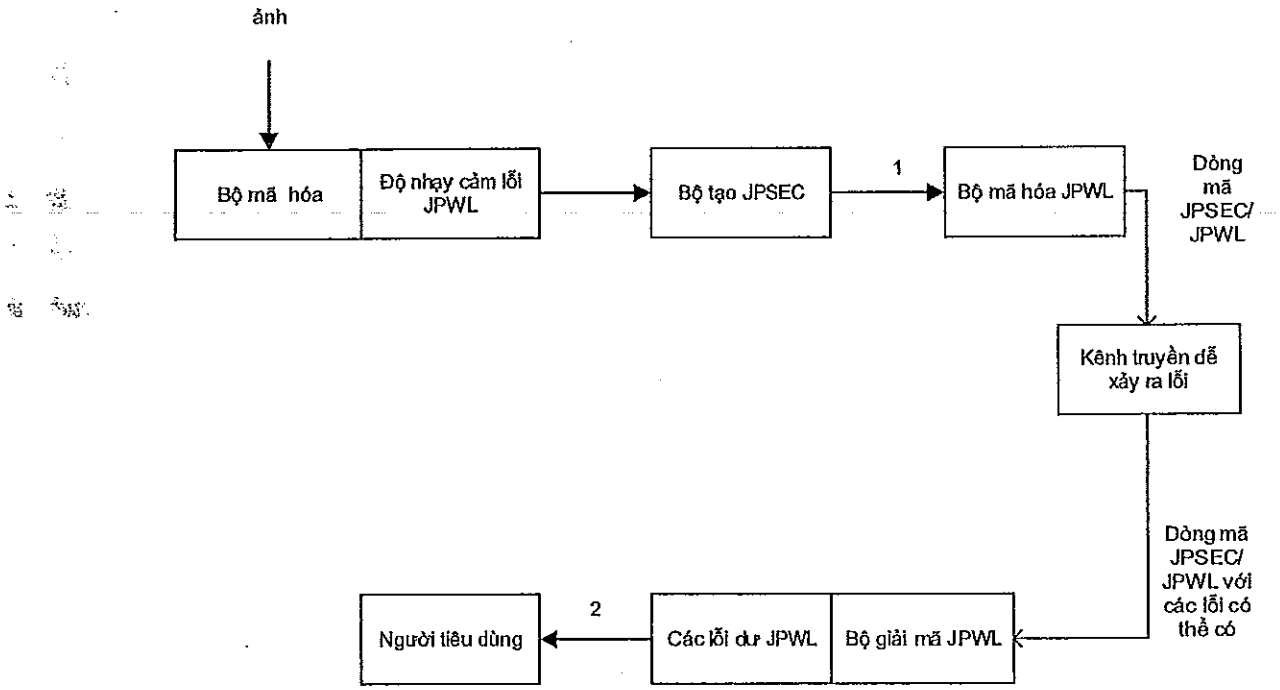
Các đoạn mã đánh dấu RED báo hiệu sự xuất hiện của các lỗi dư trong dòng mã. Thật vậy, một bộ giải mã JPWL có thể thất bại trong việc sửa lỗi tất cả các lỗi trong một dòng mã. RED cho phép báo hiệu vị trí các lỗi dư. Thông tin này sau đó có thể được khai thác bởi một bộ giải mã JPEG 2000 để đối phó với các lỗi tốt hơn. Ví dụ, các bộ giải mã có thể yêu cầu truyền lại, che giấu các lỗi hoặc loại bỏ các thông tin bị hỏng.

C.4.1 Mối quan hệ chung giữa JPWL và JPSEC

Yêu cầu phải có sự kết hợp giữa JPWL và JPSEC khi truyền dẫn các ảnh JPEG 2000 qua một kênh không dây dễ bị lỗi và yêu cầu bảo mật

Ở phía bên phát, Độ nhạy lỗi của JPWL thường được tạo ra trong quá trình mã hóa JPEG 2000. Sau đó công cụ JPSEC được áp dụng cho dòng mã để bảo mật. Cuối cùng công cụ mã hóa JPWL được sử dụng đảm bảo cho dòng mã bảo mật hơn trước các lỗi truyền.

Ở phía bên nhận, công cụ giải mã JPWL được áp dụng đầu tiên để sửa lỗi truyền dẫn. Trong bước này, JPWL cũng có thể tạo ra thông tin lỗi dư. Cuối cùng, công cụ JPSEC được áp dụng để thực hiện các dịch vụ bảo mật đã lựa chọn.



Hình C.1 – Kết hợp JPWL và JPSEC

C.4.2 Các vấn đề cụ thể trong tương thích giữa JPWL và JPSEC

Một số vấn đề cần phải được xem xét cho khả năng tương tác giữa JPWL và JPSEC, chi tiết như sau:

1) khả năng bảo vệ lỗi JPWL (EPC): sự hiện diện của đoạn mã đánh dấu này sẽ ảnh hưởng đến các khoảng byte. CHÚ THÍCH rằng đoạn mã đánh dấu này là bắt buộc trong một dòng mã JPWL.

2) Khối bảo vệ lỗi (EPB) JPWL: đoạn mã đánh dấu này thường được bổ sung vào như là bước cuối cùng của bộ phát và loại bỏ như là bước đầu tiên tại bên nhận. Về nguyên tắc, nó không ảnh hưởng đến JPSEC.

3) Bộ miêu tả độ nhạy lỗi (ESD) JPWL: đoạn mã đánh dấu này thường được thêm vào trong giai đoạn mã hóa 2000 JPEG phần 1, trong trường hợp nó sẽ được trong suốt đối với các hoạt động JPSEC tiếp theo. Tuy nhiên, JPSEC có thể gây bất lợi đối với việc sử dụng ESD trong JPWL. Đặc biệt, JPSEC không nên thay đổi các khoảng byte bất cứ khi nào ESD sử dụng khoảng byte. Ngoài ra, các hoạt động JPSEC không ảnh hưởng đến giá trị méo; Nếu không, thông tin được mang bởi ESD trở thành không phù hợp. Trong trường hợp sau, bộ tạo JPSEC có thể lựa chọn loại bỏ các đoạn mã đánh dấu ESD.

4) Bộ mô tả lỗi dư (RED) JPWL: đoạn mã đánh dấu này có thể được chèn sau khi giả mã JPWL. Do đó nó có thể ảnh hưởng đến các khoảng byte JPSEC. Nó cũng có thể ảnh hưởng đến JPSEC xác thực kỹ thuật. Trong trường hợp một codestream bị hỏng, thông tin màu đỏ có thể hữu ích cho người tiêu dùng JPSEC để một cách thích hợp có thể xử lý nó.

5) JPSEC SEC: Sự hiện diện của đoạn mã đánh dấu này sẽ ảnh hưởng đến các khoảng byte. Chú ý rằng đoạn mã đánh dấu này là bắt buộc trong một dòng mã JPSEC.

Trong trường hợp khi không có không có lỗi dư, bộ mã hóa và bộ giải mã JPWL lý tưởng xem là trong suốt. Nói cách khác, trong trường hợp này, các dòng tại các điểm 1 và 2 trong hình ở trên nên được xác định nghiêm ngặt.

Khuyến nghị rằng khi được sử dụng kết hợp với JPWL, JPSEC nên sử dụng các khoảng byte bắt đầu sau mã đánh dấu SOD để giảm thiểu các vấn đề với các byte. Ngoài ra, hạn chế sự hiện diện của đoạn mã đánh dấu JPWL trong mào đầu chính và tránh sự hiện diện của nó trong các mào đầu phần khối ảnh

Phụ lục D

(Tham khảo)

Tuyên bố về bằng sáng chế

Tổ chức tiêu chuẩn quốc tế (ISO) và Ủy ban Kỹ thuật Điện Quốc tế (IEC) hướng chú ý đến một thực tế rằng đây là tuyên bố về việc tuân thủ một phần của tiêu chuẩn ISO / IEC 15444 có thể liên quan đến việc sử dụng các bằng sáng chế.

ISO và IEC sẽ không liên quan đến các chứng cứ, tính hiệu lực và phạm vi của các bản quyền sáng chế.

Chủ sở hữu các bản quyền sáng chế đã đảm bảo với tiêu chuẩn ISO và IEC rằng họ sẵn sàng đàm phán cấp giấy phép theo các điều khoản hợp lý và không phân biệt đối xử và điều kiện với các ứng viên trên khắp thế giới. Về mặt này, các báo cáo của những người nắm giữ các bằng sáng chế phải được đăng ký với ISO và IEC. Thông tin có thể thu được từ các công ty được liệt kê dưới đây.

Sự chú ý đưa ra khả năng rằng một số các yếu tố này là một phần của tiêu chuẩn ISO / IEC 15444 có thể là đối tượng của quyền sáng chế khác với những xác định trong phụ lục này. ISO và IEC sẽ không chịu trách nhiệm xác định bất kỳ hoặc tất cả các quyền bằng sáng chế như vậy.

Bảng D.1 - Danh sách tuyên bố

STT	Cơ quan tuyên bố
1	Canon Inc
2	Đại học Columbia
3	Giám sát EMITALL
4	HP
5	Viện nghiên cứu Infocomm
6	MediaLive
7	Viện công nghệ New Jersey

Phụ lục E

(Quy định)

An toàn định dạng tập tin

E.1 Phạm vi

Phụ lục này quy định các định dạng tập tin JPSEC bắt nguồn từ định dạng tập tin cơ sở ISO và sửa đổi sang định dạng tập tin họ JPEG (bao gồm JP2, JPX và JPM) để bảo vệ và thích ứng bảo mật của ảnh mở rộng, đó là có thể mã hóa và / hoặc chứng thực của các chủ sở hữu. Các ảnh có thể là một trong hai ảnh tĩnh hoặc ảnh sắp xếp theo trình tự thời gian. Đặc biệt, phụ lục này cung cấp chức năng để làm những việc sau:

– Để lưu trữ dữ liệu truyền thông được mã hóa tương ứng với mức độ phân cấp khác nhau. Dòng sơ cấp (ES) được sử dụng cho mục đích này. Có ba loại ES: ES tự chứa, ES phân cấp và ES có khả năng giải mã.

– Để xác định vùng bộ nhớ lưu thông tin mô tả đặc điểm của dữ liệu truyền thông mã hóa được lưu trữ trong ES. Ví dụ, vùng bộ nhớ có thể cho biết mức độ phân cấp (độ phân giải, lớp, vùng, vv) và các gợi ý tỷ lệ làm méo của các dữ liệu truyền thông được mã hóa để tạo điều kiện thích ứng dễ dàng và bảo mật.

– Để xác định các khung định dạng tập tin mới cho các công cụ và tham số bảo vệ tín hiệu được áp dụng cho dữ liệu truyền thông hoặc siêu dữ liệu. Các công cụ bảo vệ có thể áp dụng cho ảnh JPEG2000 tĩnh hoặc sắp xếp theo thứ tự thời gian.

– Các công cụ bảo vệ trong bản sửa đổi này có thể được áp dụng cho các định dạng tập tin họ JPEG bao gồm JP2, JPX và JPM, các định dạng tập tin theo chuẩn ISO như MJ2 cho JPEG động.

E.2 Giới thiệu

E.2.1 Bảo vệ bảo mật mức định dạng tập tin

Phụ lục này mô tả định dạng tập tin JPSEC bắt nguồn từ định dạng tập tin ISO và sửa đổi thành định dạng tập tin họ JPEG, để bổ sung bảo vệ an ninh cho ảnh JPEG 2000 ở mức định dạng tập tin. Bảo vệ áp dụng ở mức định dạng tập tin có thể phân thành hai loại: bảo vệ dựa trên đối tượng và bảo vệ dựa trên mẫu. Cả hai cấu trúc được xác định mởi định dạng tập tin ISO. Bảo vệ dựa trên đối tượng được thiết kế để bảo vệ tất cả các byte (gồm dữ liệu truyền thông mã hóa và siêu dữ liệu) trong khi bảo vệ dựa trên mẫu được thiết kế để bảo vệ dữ liệu truyền thông sắp xếp theo thứ tự thời gian bao gồm ảnh JPEG 2000.

Khi các công cụ bảo mật áp dụng thay đổi độ dài dữ liệu, nó sẽ cập nhật tất cả các con trỏ và trường độ dài trong tất cả các khung, để đảm bảo phân tích chính xác bởi đầu đọc.

E.2.2 Bảo vệ dựa trên đối tượng

Phụ lục này mô tả hai cơ chế bảo vệ dựa trên đối tượng đối với định dạng tập tin ISO, bằng cách tận dụng cú pháp và các cấu trúc trong chuẩn JPSEC. Cụ thể, nó mô tả các cơ chế gải mã và xác thực. Mỗi đối tượng trong ItemLocationBox được bảo vệ bởi một hoặc nhiều cơ chế bảo vệ nằm trong ItemProtectionBox. Khi nhiều cơ chế được sử dụng (hay kết hợp tuần tự với nhau), thứ tự mà chúng được áp dụng có thể trở nên quan trọng và vì vậy cần phải được chỉ rõ. Phụ lục này cũng quy định cụ thể các hoạt động đó được kết hợp tuần tự như thế nào. Ngoài ra, ItemDesscriptionBox và ItemCorrespondingBox cũng được bổ sung vào định dạng tập tin ISO để cho phép các tiện ích xử lý linh hoạt được cung cấp bởi JPSEC. Cụ thể, ItemDescriptionBox cho phép siêu dữ liệu phụ thuộc dữ liệu (như độ phân giải, lớp chất lượng, vùng không gian và thành phần không gian màu sắc) được liên kết với các phần khác nhau của tập tin. Các mô tả này có thể được cung cấp bất kể loại bảo vệ nào được sử dụng. Khi được sử dụng với ảnh mã hóa phân cấp, điều này cho phép tập tin có thể được thu nhỏ lại hoặc chuyển mã mà không cần phân tích hoặc giải mã các dữ liệu truyền thông. Trong trường hợp bảo vệ được sử dụng, điều này sử dụng được lợi ích của cho phép chuyển mã mà không cần giải mã.

E.2.3 Bảo vệ dựa trên mẫu của phương tiện phân cấp

Đối với hình ảnh thời gian sắp xếp trình tự, phụ lục này thêm các cú pháp để tạo điều kiện cho phân cấp tại mức định dạng tập tin, bao gồm cả dòng sơ cấp (ES) soạn thảo phân cấp, ES soạn thảo có khả năng giải mã, cấu trúc con trỏ, cấu trúc ngăn chứa và cấu trúc dữ liệu byte. Những hình ảnh được mã hóa phân cấp có thể được chia (hoặc vật lý hoặc ảo) thành dòng sơ cấp tại mức phân cấp khác nhau, như vậy bộ chuyển đổi / chuyển mã có thể "làm mỏng" dữ liệu phương tiện với độ phức tạp thấp.

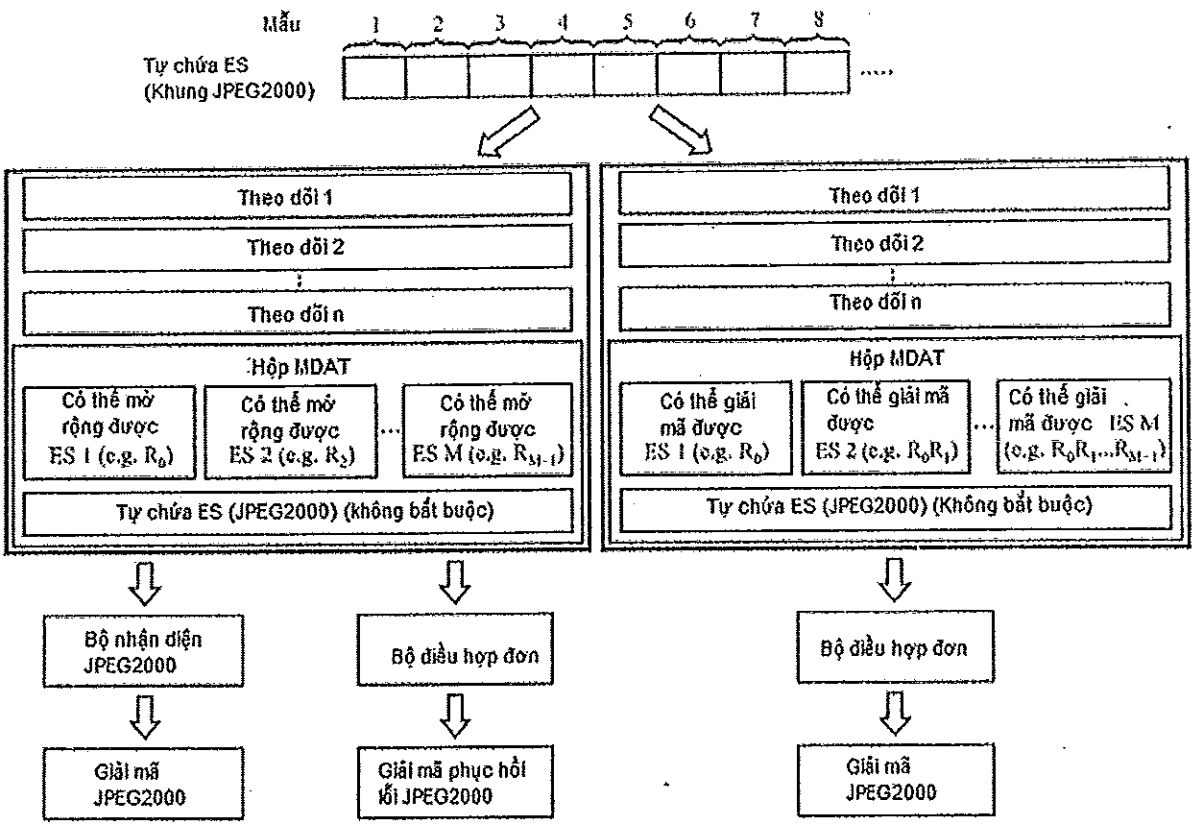
Hình E.1 đưa ra một cái nhìn tổng quan về định dạng tập tin theo quy định của phụ lục này và cũng cho thấy làm thế nào FF quy định được sử dụng để thích ứng với dữ liệu phương tiện.

Với một chuỗi các ảnh JPEG 2000 cho trước (còn gọi là ES tự chứa: Self-contained ES), có hai phương pháp tiếp cận để xây dựng định dạng tập tin. Trong cách tiếp cận đầu tiên, khung MDAT chứa một hoặc nhiều ES soạn thảo phân cấp (Scalable Composed ES), mỗi ES này tương ứng với một mức phân cấp của dữ liệu phương tiện, ví dụ như, một độ phân giải hoặc lớp. ES soạn thảo phân cấp phải được lưu trữ trong khung MDAT cùng vị trí với định dạng tập tin. ES tự chứa có thể được đặt trong khung MDAT trong cùng một tập tin hoặc đặt trong một tập tin khác có định dạng không được xác định trong tiêu chuẩn này. ES soạn thảo phân cấp không có khả năng tự giải mã, nó cần phải được kết hợp với ES soạn thảo phân cấp khác để tạo ra ảnh JPEG 2000 có khả năng giải mã hoàn toàn. Trong phương pháp thứ hai, khung MDAT chứa một hoặc nhiều ES soạn thảo có khả năng giải mã và mỗi ES tự tạo thành ảnh JPEG 2000 có khả năng giải mã hoàn toàn. Tương tự như vậy, các ES soạn thảo có khả năng giải mã phải được lưu trữ trong khung MDAT cùng vị trí với định dạng tập tin và ES tự chứa được lưu trữ trong khung MDAT cùng một tập tin hoặc trong một tập tin khác có định dạng không được xác định trong tiêu chuẩn này.

Mỗi ES soạn thảo phân cấp hoặc ES soạn thảo có khả năng giải mã phải được mô tả bởi ít nhất một rãnh từ. Các đặc tính của ES (như độ phân giải, lớp, và khu vực) được ghi trong SampleEntryBox bên trong mỗi rãnh từ.

Để tạo ra một dòng mã JPEG 2000 có khả năng giải mã hoàn toàn từ các ES soạn thảo phân cấp, một bộ thích ứng nhận biết JPEG 2000 phải có khả năng tự động tạo ra các mào đầu ảnh (dựa trên số lượng độ phân giải, các lớp và khu vực trong dòng mã thích ứng), để chèn gói rỗng hoặc để chèn các mã đánh dấu POC cần thiết để tạo ra dòng mã có khả năng giải mã bởi mọi bộ giải mã chuẩn. Tuy nhiên, nếu một bộ chuyển đổi đơn giản được sử dụng, thì dòng mã sinh ra này có thể có mào đầu ảnh không phù hợp và có gói tin bị mất, mà đòi hỏi một bộ giải mã định dạng thích ứng JPEG 2000.

Khi một ES soạn thảo có khả năng giải mã tự giải mã thì một bộ thích ứng đơn giản đủ để tạo ra ảnh JPEG 2000 được tuân thủ hoàn toàn



Hình E.1 – Sơ đồ hệ thống cho phương tiện mở rộng được sắp xếp theo trình tự thời gian

Mỗi dòng cơ bản được mô tả bởi ít nhất một rãnh từ phương tiện và các đặc tính của nó được mô tả trong SampleDescriptionEntry hoặc SampleGroupEntryBox bên trong rãnh từ. Có thể là một dòng cơ bản được mô tả bởi nhiều rãnh từ, mỗi rãnh từ có thể mô tả các khía cạnh khác nhau của dòng cơ bản.

Việc bảo vệ dựa trên mẫu có thể được áp dụng cho tất cả các mẫu hoặc một nhóm các mẫu trong một ES soạn thảo phân cấp hoặc ES soạn thảo có khả năng giải mã. Nếu bảo vệ được áp dụng cho tất cả các mẫu, một ProtectionSchemeInfoBox báo hiệu các tham số của công cụ bảo vệ được thêm vào SampleDescriptionBox, sau đó được đóng gói như mô tả trong E.5.2. Ngoài ra, nếu bảo vệ được áp dụng cho một nhóm các mẫu, một ProtectionSchemeInfoBox được thêm vào SampleGroupEntryBox, sau đó được đóng gói như mô tả trong E.5.4.

E.3 Mở rộng định dạng tệp đa phương tiện dựa trên chuẩn ISO

E.3.1 Tổng quan

Mục này tổng hợp lại những mở rộng kỹ thuật (kiểu khung bổ sung) vào định dạng tệp phương tiện dựa trên tiêu chuẩn ISO, những kỹ thuật này được sử dụng cho việc bảo vệ, việc thích nghi, hoặc việc thích nghi bảo mật của các ảnh được mã hóa co giãn. Tuy nhiên những kiểu box bổ sung có thể được sử dụng cho những mục đích khác. Cụ thể, mục này định nghĩa ProtectionSchemeInfoBox cho công cụ mật mã hóa và công cụ nhận thực, ItemDescriptionBox, ScalableSampleDescriptionEntry,

ScalableSampleGroupEntry, và Generic Protected Box. Tất cả các khung khác được định nghĩa trong ISO/IEC 15444-12 vẫn được sử dụng.

E.3.2 Gắn dòng mã JPSEC vào định dạng tập tin điều khiển ISO

Dòng mã JPSEC có thể được coi như là tải tin trong khung 'mdat' của định dạng tệp cơ bản của ISO. Trong Khung Mô tả mẫu ('stsd'), 'codingname' của bản ghi mẫu tương ứng được định nghĩa là 'jpsc', là một định danh đăng ký cho bộ giải mã JPSEC. Trong trường hợp này, dịch vụ bảo mật được cung JPSEC cung cấp cho dòng mã.

E.3.3 Nhãn hiệu định dạng tệp được bảo vệ

Các tệp hợp lệ trong tiêu chuẩn này có thể sử dụng 'ffsc' như một tên hiệu chính trong Khung tương thích kiểu tệp.

Các tệp hợp lệ trong tiêu chuẩn này chứa thông tin nhật thực hoặc bảo vệ có thể sử dụng 'ffsc' như một tên hiệu chính trong Khung tương thích kiểu tệp (File Type Compatibility Box).

Sử dụng tiêu chuẩn này phù hợp với tệp JP2, JPX, MJ2 và JPM. Cụ thể sử dụng tiêu chuẩn này thì tên tệp lớn không thay đổi nhưng các khung thêm vào thì sử dụng tên hiệu 'ffsc' là thích hợp.

Do đó các tên hiệu bao gồm 'isom' , 'iso2', 'jp2\040, 'jpx\040' và 'jpm\040' phải phù hợp.

Tên hiệu 'ffsc' cho biết việc sử dụng các khung mới và công cụ mới tương ứng với các phương pháp bảo vệ trong JPSEC.

Một tệp được bảo vệ cho đến mức mà một ứng dụng dự kiến để xử lý JP2, JPX, JPM hoặc nội dung kiểu tệp khác sẽ không được thực hiện nếu không sử dụng các công cụ bảo vệ, có thể sử dụng tên hiệu chính 'ffsc' như kiểu tệp; như một tệp bảo vệ không sử dụng tên hiệu lớn khi mà không còn phù hợp.

E.3.4 Tổng quan các khung được sử dụng

Định dạng tập tin đa phương tiện ISO xác định hai cấu trúc để mô tả một trình diễn: cấu trúc logic và cấu trúc tuần tự phương tiện. Cấu trúc logic sử dụng ItemLocationBox ('iloc') để mô tả một phần tử ở chế độ khoảng byte hoặc chuỗi các khoảng byte đối với một tệp cụ thể, hoặc là tệp cục bộ hoặc tệp từ xa. Cấu trúc tuần tự đa phương tiện sử dụng SampleGroupDescriptionBox ('spgd') hoặc SampleDescriptionBox ('stsd') để mô tả các mẫu, có thể là một khung của video hoặc chuỗi liên tiếp các khung video, hoặc một đoạn âm thanh được nén liên tục.

Theo đó, bảo vệ ở mức độ định dạng tập tin truyền thông ISO cơ sở được phân loại thành bảo vệ dựa trên phần tử và bảo vệ mẫu, như mô tả trong E.5.2 và E.5.4 tương ứng.

Một số khung được sử dụng trong ISO/IEC 15444-12 thì sẽ được đánh dấu là "đã có" trong Bảng E.1. Các khung được định nghĩa trong tiêu chuẩn này được liệt kê là "mới". Các định nghĩa của những khung này tùy thuộc vào định nghĩa khung và "khung đầy đủ" trong ISO/IEC 15444-12, và được nhắc lại trong E.7.

Bảng E.1 – Liệt kê các khung

Tên khung						Trạng thái	Nhận xét
meta						Đã có	Siêu dữ liệu
	iloc					Đã có	Vị trí phần tử
	iproc					Đã có	Sự bảo vệ Phần tử
		sinf				Đã có	Khung thông tin lược đồ bảo vệ
			frma			Đã có	Khung định dạng đầu tiên
			schm			Đã có	Khung kiểu lược đồ
			schi			Đã có	Khung thông tin lược đồ
				gran		Mới	Khung có độ chi tiết
				vall		Mới	Khung danh sách giá trị
				bcip		Mới	Khung mật mã hóa khối
					keyt	Mới	Khung mẫu khóa
				scip		Mới	Khung mật mã hóa dòng
					keyt	Mới	Khung mẫu khóa
				auth		Mới	Khung xác thực
					keyt	Mới	Khung mẫu khóa
	iinf					Đã có	Khung thông tin phần tử
	ides					Mới	Khung mô tả phần tử
		dest				Mới	Khung kiểu mô tả
		desd				Mới	Khung dữ liệu mô tả
		vide				Mới	Bản ghi mô tả phần tử trực quan
		j2ke				Mới	Bản ghi mô tả phần tử JPEG 2000
	icor					Mới	Khung tương ứng với phần tử

Bảng E.1 – Liệt kê các khung

Tên khung						Trạng thái	Nhận xét
...	...	...	...	...	...	...	...
stbl						Đã có	Khung bảng mẫu
	stsd					Đã có	Khung mô tả mẫu
		ScalableSampleDescriptionEntry				Mới	Bản ghi mô tả mẫu co giãn
	sbgp					Đã có	Mẫu để nhóm khung
	sgpd					Đã có	Khung nhóm các mẫu
		ScalableSampleGroupEntry				Mới	Bản ghi nhóm mẫu co giãn
gprt						Mới	Khung được bảo vệ

E.3.5 Lược đồ giải mật mã

Lược độ bảo vệ giải mật mã được định ra trong SchemeTypeBox như sau:

scheme_type="decr"

scheme_version=0

scheme_uri=null

với lược đồ bảo vệ giải mật mã, cấu trúc của SchemeInfoBox như sau:

```
aligned(8) class GranularityBox extends Box('gran') {
unsigned int(8) granularity;
}
```

Ngữ nghĩa:

Granularity được sử dụng cho việc bảo vệ phần tử. Với việc bảo vệ này, 0 cho biết đơn vị xử lý là toàn bộ phần tử và 1 cho biết đơn vị xử lý chỉ là một mức độ nào đó trong một phần tử. Với kiểu bảo vệ mẫu, 0 cho biết đơn vị xử lý là tất cả các mẫu trong một rãnh ghi hoặc của một nhóm mẫu và 1 cho biết đơn vị xử lý là một mẫu

```
aligned(8) class ValueListBox extends Box('vall') {
    unsigned int(8) value_size;
```

```
    unsigned int(16) value_count;
    unsigned int(16) count [value_count];
    unsigned char (value_size) value[value_count];
}
```

Ngữ nghĩa:

value_size là kích thước theo byte của mỗi giá trị trong mảng

value_count là số cặp (count, value) trong mảng, với kiểu bảo vệ phần tử, các cặp (count, value) được sử dụng để ánh xạ mỗi giá trị với đơn vị xử lý count. Với kiểu bảo vệ mẫu, cặp (count, value) được sử dụng để ánh xạ mỗi giá trị với các mẫu count . ví dụ, value[0] tương ứng với mẫu hoặc đơn vị count[0], và value[1] tương ứng với mẫu hoặc đơn vị count[1]kế tiếp , và cứ như thế.

```
aligned(8) class KeyTemplateBox extends Box('keyt') {
    unsigned int(16) key_size;
    unsigned int(8) key_info;
    GranularityBox GL;          //optional
    ValueListBox   VL;
}
```

Ngữ nghĩa:

key_size là kích thước khóa theo đơn vị bít.

key_info cho biết ý nghĩa của các giá trị trong ValueListBox. 1 nghĩa là các giá trị là chứng thư X.509; 2 nghĩa là các giá trị là URI cho chứng thư hoặc khóa bí mật.

GL là GranularityBox.

VL là ValueListBox, chứa danh sách các giá trị, ý nghĩa của các giá trị đó được định nghĩa bởi trường key_info.

```
aligned(8) class BlockCipherBox extends Box('bcip') {
unsigned int(16) cipher_id;
bit (6) cipher_mode;
bit (2) padding_mode;
unsigned int(8) block_size;
KeyTemplateBox KT;
```

}

Ngữ nghĩa:

cipher_id định danh thuật toán mã hóa khối nào được sử dụng để bảo vệ. Các giá trị được định nghĩatr ong Bảng 25.

cipher_mode có thể là ECB, CBC, CFB, OFB hoặc CTR. Các giá trị được định nghĩa trong Bảng 29.

padding_mode là ciphertext lấy cắp hoặc PKCS#7-đệm. Các giá trị được định nghĩa trong Bảng 30.

block_size là kích thước khối hoặc mật mã khối.

KT là KeyTemplateBox, giữ tất cả thông tin khóa được sử dụng bởi mật mã khối đó.

aligned(8) class StreamCipherBox extends Box('scip') {

unsigned int(8) cipher_type;

unsigned int(16) cipher_id;

KeyTemplateBox KT;

}

Ngữ nghĩa:

cipher_type cho biết kiểu mật mã được sử dụng. Có giá trị cipher_type = STRE đối với mật mã dòng hoặc cipher_type = ASYM đối với mật mã không đối xứng.

cipher_id cho biết thuật toán mật mã dòng được sử dụng để bảo vệ. Nếu cipher_type = STRE, xem Bảng 26; nếu cipher_type = ASYM, xem bảng 27.

KT là KeyTemplateBox, giữ tất cả thông tin khóa được sử dụng bởi mật mã dòng đó.

aligned(8) class SchemeInfomationBox extends Box('schi', cipher_id) {

unsigned int(8) MetaOrMedia;

unsigned int(8) HeaderProtected;

BlockCipherBox(); orStreamCipherBox();

GranularityBox GL;

ValueListBox VL;

}

Ngữ nghĩa:

MetaOrMedia là để cho biết liệu đoạn dữ liệu bảo vệ tương ứng với đoạn dữ liệu đa phương tiện hay các khung siêu dữ liệu. (0 đối với dữ liệu đa phương tiện và 1 là cho khung siêu dữ liệu).

HeaderProtected là để cho biết kiệu việc bảo vệ được áp dụng chỉ cho một phần khung (giá trị 0) hay áp dụng cho toàn bộ khung bao gồm cả mào đầu của nó (giá trị 1).

SchemeInformationBox có thể chứa một BlockCipherBox, hoặc StreamCipherBox, chúng là các ngăn chứa đối với các tham số của thuật toán mật mã hóa. Những khung này có thể chỉ chứa các giá trị cipher_id.

GL là GranularityBox, giữ thông tin về đơn vị xử lý. Trường này được tối ưu cho bảo vệ mẫu và được yêu cầu cho bảo vệ phần tử.

VL là ValueListBox. Đối với mật mã khối, khung có thể trống. Với mật mã dòng, khung chứa tất cả các véc tơ ban đầu.

E.3.6 Lược đồ xác thực

Lược đồ bảo vệ nhật thực được xác định bởi SchemeTypeBox như sau:

scheme_type="auth"

scheme_version=0

scheme_uri=null

Đối với lược đồ này, cấu trúc của SchemeInfoBox được định nghĩa như sau:

```
aligned(8) class AuthBox extends Box('Auth') {
    unsigned int(8) auth_type; //hash, cipher, or signature
    unsigned int(8) method_id;
    unsigned int(8) hash_id;
    unsigned int(16) MAC_size;
    KeyTemplateBox KT;
}
```

Ngữ nghĩa:

auth_type cho biết kiểu nhận thực, bao gồm nhật thực dựa trên hàm băm (HASH), nhật thực dựa trên mật mã(CIPH) và nhật thực dựa trên chữ ký số(SIGN).

method_id cho biết phương pháp nhật thực. 1 cho biết HMAC. Nếu auth_type = HASH, xem Bảng 36; nếu auth_type = CIPH, xem Bảng 39; nếu auth_type = SIGN, xem Bảng 41.

hash_id cho biết hàm băm được sử dụng. Nếu auth_type = HASH hoặc SIGN, xem bảng 37; nếu auth_type = CIPH, xem Bảng 25.

MAC_size là kích thước của MAC (nếu auth_type = HASH hoặc CIPH) hoặc chữ ký số (nếu auth_type = SIGN) theo đơn vị bít.

KT là KeyTemplateBox, giữ tất cả thông tin khóa để nhật thực.

```
aligned(8) class SchemeInfoBox extends Box('schi', auth_method) {
    unsigned char (8) auth_method;
    AuthBox authBox;
GranularityBox GL;          //optional
ValueListBox VL;
}
```

Ngữ nghĩa:

auth_method cho biết phương pháp nhật thực được sử dụng. 0 là phương pháp dựa trên hàm băm MAC; 1 là phương pháp dựa trên mật mã MAC; 2 là phương pháp chữ ký số. Tùy thuộc vào auth_method, khung này có thể chứa hoặc là HashAuthBox, CipherAuthBox, hoặc SignatureAuthBox.

GL là GranularityBox. Trường này là tùy chọn cho bảo vệ mẫu và bắt buộc đối với bảo vệ phần tử.

VL là ValueListBox, giữ tất cả MAC hoặc chữ ký số.

E.3.7 Khung ItemDescription

Trong Khung vị trí đối tượng (Item Location Box), tất cả các đối tượng được quy định là ở chế độ khoảng byte(sử dụng dịch hoặc chiều dài). Khung 'iloc' không chứa thông tin liên quan nội dung về các khoảng byte quy định, khoảng được yêu cầu bởi một số phương pháp bảo vệ. Ví dụ, nếu phương pháp chuyển mã bảo mật muốn loại bỏ các lớp ít quan trọng hoặc độ phân giải, thì phải biết khoảng byte nào tương ứng với lớp hoặc độ phân giải nào loại bỏ.

Như vậy, mục này định nghĩa hai khung mới để đảm bảo xử lý liên quan đến nội dung ở mức định dạng tệp: Khung mô tả đối tượng ('ides') và Khung tương ứng đối tượng(Item Correspondence Box) ('icor'). Khung 'ides' quy định thông tin liên quan nội dung như lớp, độ phần giải (đối với các nội dung ảnh, thời gian (nội dung âm thanh). Khung 'icor' liên kết với thông tin liên quan nội dung với các đối tượng trong khung 'iloc' theo kiểu liên kết như khung 'innf' liên kết khung 'iloc' với khung 'ipro'.

Khung mô tả đối tượng ('ides') được định nghĩa như sau:

```
aligned(8) class ItemDescriptionBox extends Box('ides') {
    unsigned int(32) entry_count;
    for(i=0; i < entry_count; i++) {
```

```
        DescriptionTypeBox desType;
        unsigned int(32) item_ID;
        DescriptionDataBox desData;
    }
}
```

Ngữ nghĩa:

entry_count là số bản ghi trong ItemDescriptionBox.

item_ID tham chiếu đến đối tượng trong ItemLocationBox. Nếu trường này là 0 thì item_ID sẽ được quy định bởi CorrespondenceBox.

```
Aligned(8) class DescriptionTypeBox extends Box('dest') {
    Unsigned int(32) description_type;
    Unsigned int(32) description_version;
    Unsigned int(8) description_uri[];
}
```

Ngữ nghĩa:

description_type là mã 4CC xác định lược đồ mô tả.

description_version là phiên bản mô tả.

description_uri cho phép tùy chọn dẫn người sử dụng đến một trang web nếu họ không có định nghĩa mô tả được cài đặt trên hệ thống của họ. Đó là một URI tuyệt đối được hình thành như một chuỗi kết cuối bởi null trong các ký tự UTF-8.

```
Aligned(8) class DescriptionDataBox extends Box('desd') {
    Box description_specific_data [];
}
```

Ngữ nghĩa:

Nếu description_type = 'vide', Thì đây là VisualItemDescriptionEntry; nếu description_type = 'j2ke', thì đây là J2KItemDescriptionEntry; đối với bất kỳ giá trị khác của description_type, cú pháp của môt tả này có thể tìm ở description_uri.

VisualItemDescriptionEntry được định nghĩa như sau:

```
aligned(8) Class VisualItemDescriptionEntry extends Box('vide') {
```

```
    unsigned int(16) layer_start;
    unsigned int(16) layer_count;
    unsigned int(16) res_start;
    unsigned int(16) res_count;
    unsigned int(16) horizontal_offset;
    unsigned int(16) horizontal_length;
    unsigned int(16) vertical_offset;
    unsigned int(16) vertical_length;
    unsigned int(16) color_space;
    unsigned int(16) time_start;
    unsigned int(16) time_length;
}
```

Ngữ nghĩa:

layer_start và layer_count cùng quy định khoảng các lớp. Khi layer_start bằng 2^{16}–1, khoảng lớp này sẽ bắt đầu từ lớp 0; khi layer_count bằng 2^{16}–1, khoảng lớp sẽ kết thúc ở lớp sau cùng. Khi cả layer_start và layer_count bằng 2^{16}–1, khoảng lớp sẽ bao gồm tất cả các lớp.

res_start và res_count cùng quy định khoảng các độ phân giải. Thì nó có ý nghĩa giống với layer_start và layer_count khi các giá trị của chúng bằng 2^{16}–1.

horizontal_offset, horizontal_length, vertical_offset và vertical_length cùng quy định miền không gian. Thì nó có ý nghĩa như layer_start và layer_count khi các giá trị của chúng bằng 2^{16}–1.

color_space quy định không gian màu. 0: không gian màu đỏ; 1: không gian màu xanh lá; 2: không gian xanh sẫm.

Liên đoạn này được áp dụng cho các khỏng lớp, khoảng độ phân giải, các vùng và không gian màu để lấy được phần của ảnh, video quy định bởi VisualItemDescriptionEntry.

The intersection is applied to the layer ranges, resolution ranges, areas and color space to get the portion of the image/video specified by the VisualItemDescriptionEntry.

J2KItemDescriptionEntry được định nghĩa như sau:

```
aligned(8) class J2KItemDescriptionEntry extends Box('j2ke') {
    VisualItemDescriptionEntry visualDesEntry; //optional
    unsigned int(16) tile_start;
    unsigned int(16) tile_count;
```

```
    unsigned int(16) precinct_start;
    unsigned int(16) precinct_count;
    unsigned int(16) j2k_packet_start;
    unsigned int(16) j2k_packet_count;
}
```

Ngữ nghĩa:

visualDesEntry quy định các thuộc tính quy định ảnh/video. Và trường này là tùy chọn.

tile_start và tile_count quy định các khối ảnh.

precinct_start và precinct_count quy định các phân khu.

j2k_packet_start và j2k_packet_count quy định các gói được định nghĩa theo JPEG2000.

Tương tự với VisualItemDescriptionEntry, liên đoạn này được áp dụng cho các khối ảnh, các phân khu và các gói JPEG2000 để có được các phần của dòng mã JPEG2000 quy định bởi J2KItemDescriptionEntry

ItemCorrespondenceBox ('icor') được định nghĩa như sau:

```
aligned(8) class ItemCorrespondenceEntry extends Box('icor') {
    unsigned int(16) item_ID;
    unsigned int(16) desc_ID;
}
```

Ngữ nghĩa:

item_ID chỉ ra một đối tượng trong ItemLocationBox.

desc_ID chỉ ra một bản ghi mô tả trong ItemDescriptionBox.

E.3.8 Khung ScalableSampleDescriptionEntry

ScalableSampleDescriptionEntry được sử dụng để mô tả đặc điểm kết hợp với ES có khả năng co giãn gồm ES hoặc ES có thể giải mã được, giống như các mức phân giải, chất lượng lớp, miền cắt. Đối với ES có khả năng co giãn, res và layer cho biết dữ liệu phương tiện của độ phân giải và lớp cụ thể, còn đối với ES có khả năng giải mã được thì chúng cho biết độ phân giải lớn nhất hoặc lớp chất lượng cao nhất.

Khi các mẫu phương tiện truyền thông được bảo vệ bởi công cụ bảo vệ, ScalableSampleDescriptionEntry được đóng gói như sau:

Mã bốn ký tự (four-character-code) của ScalableSampleDescriptionEntry được thay thế với một mã bốn ký tự khác cho biết việc đóng gói bảo vệ, nó chỉ thay đổi kiểu phương tiện như định nghĩa sau:

- Encv: cho biết các mẫu video được mật mã và không bảo vệ phải được áp dụng để có được dữ liệu phương tiện có ý nghĩa.
- Autv: cho biết mẫu video được nhận thực và dữ liệu phương tiện có thể vẫn có ý nghĩa trước khi không bảo vệ.
- Enct: cho biết mẫu bản tin được mật mã hóa.
- Autt: cho biết các mẫu bản tin được nhận thực.
- Encs: cho biết các mẫu hệ thống được mật mã hóa.
- Auts: cho biết các mẫu hệ thống được nhận thực.

ProtectionSchemeInfoBox được thêm vào ScalableSampleDescriptionEntry, để lại tất cả các khung khác không bị hiệu chỉnh.

Kiểu bản ghi mẫu đầu tiên được lưu trong OriginalFormatBox cùng với ProtectionSchemeInfoBox.

```
Class     ScalableSampleDescriptionEntry(codingname)extends    VisualSampleEntry(codingname) {
    Unsigned int(8)      res;
    Unsigned int(8)      layer;
    Unsigned int(32)          cropped_width, cropped_height;
    If(cropped_width > 0 && cropped_height > 0) {
        Unsigned int(32)      startx;
        Unsigned int(32)      starty;
    }
    ProtectionSchemeInfoBox protectionSchemes[]; //optional
}
```

Ngữ nghĩa:

codingname là "sces" nếu rãnh in này tham chiếu đến ES có khả năng co giãn và "dces" nếu rãnh in này tham chiếu tới ES có khả năng giải mã.

res là độ phân giải của các mẫu được quy định. Một giá trị là -1 cho biết tất cả các mức phân giải.

layer là lớp chất lượng của các mẫu được mô tả. Một giá trị là -1 cho biết tất cả các lớp chất lượng.

cropped_width là chiều rộng của miền cắt.

cropped_height là chiều cao của miền cắt.

startx & starty cho biết vị trí của góc trái trên cùng của miền cắt. Nếu hoặc cropped_width hoặc cropped_height là 0, thì startx và starty sẽ không xuất hiện

protectionSchemes là danh sách ProtectionSchemeInfoBoxes cho biết các công cụ bảo vệ được áp dụng cho các mẫu được mô tả. Tiến trình không bảo vệ (un-protection) phải theo thứ tự mà chúng xuất hiện trong danh sách.

E.3.9 Khung ScalableSampleGroupEntry

Một rãnh in có thể được tạo ra từ các mẫu với các ký tự khác nhau và được bảo vệ bởi các công cụ bảo vệ khác nhau hoặc với các tham số khác nhau. Khung ScalableSampleGroupEntry được sử dụng để báo hiệu việc nhóm các mẫu cơ bản. Ví dụ, nếu một rãnh in có 1000 mẫu, 500 mẫu đầu tiên được mật mã với khóa 1 và 500 mẫu thứ hai được mật mã với khóa 2, khung SampleGroupDescription chứa hai khung ScalableSampleGroupEntry: khung thứ nhất mô tả 500 mẫu đầu và khung thứ hai mô tả 500 mẫu thứ hai.

Khi các mẫu phương tiện được bảo vệ bởi công cụ bảo vệ, ScalableSampleGroupEntry được đóng gói như ScalableSampleDescriptionEntry trong E.3.8.

```
Class    ScalableSampleGroupEntry(type)    extends VisualSampleGroupEntry(type) {
    unsigned int(8)        res;
    unsigned int(8)        layer;
    unsigned int(32)            cropped_width, cropped_height;
    If(cropped_width > 0 && cropped_height > 0) {
        unsigned int(32)            startx;
        unsigned int(32)            starty;
    }
    ProtectionSchemeInfoBox protectionSchemes[]; //optional
}
```

Ngữ nghĩa:

type cho biết kiểu nhóm. Nếu nhóm dựa trên một công cụ bảo vệ khác được áp dụng cho mẫu này thì kiểu "prot"; nếu nhóm dựa trên các ký tự phương tiện khác (như lớp hoặc độ phân giả) thì kiểu "attr".

res là độ phân giải của mẫu được mô tả. Một giá trị –1 cho biết tất cả các mức phân giải.

layer là lớp chất lượng của các mẫu được mô tả. Một giá trị là –1 cho biết tất cả các lớp chất lượng.

cropped_width là chiều rộng của miền cắt.

cropped_height là chiều cao của miền cắt.

startx & starty cho biết vị trí của góc trên cùng bên trái của miền cắt. Nếu cropped_width hoặc cropped_height là không, thì startx và starty sẽ không xuất hiện.

protectionSchemes là danh sách ProtectionSchemeInfoBoxes cho biết các công cụ bảo vệ được áp dụng cho các mẫu được mô tả. Tiến trình không bảo vệ phải theo thứ tự mà chúng xuất hiện trong danh sách.

E.3.10 Khung bảo vệ chung

E.3.10.1 Định nghĩa

Kiểu khung: 'gprt'

Ngăn chứa: tệp hoặc bất kỳ khung ngăn chứa nào

Bắt buộc: Có, nếu sử dụng sai sẽ ngăn chặn việc phân tích tệp

Số lượng: bất kỳ số nào

Khung JProtected được sử dụng khi lược đồ bảo vệ được áp dụng cho một khung và sử dụng lược đồ bảo vệ để ngăn ngừa việc phân tích khung. Ví dụ, nếu các nội dung của một khung lớn được mật mã hóa, bao gồm chiều dài khung và kiểu khung, khung đó không thể phân tách được nữa, và không đáp ứng định nghĩa đầu tiên cho khung. Trong trường hợp này, Khung JProtected có thể đặt trong tệp sao cho tệp đó không tiếp tục được phân tách chính xác và dữ liệu mật mã được đặt trong khung JProtected.

Thông dịch nội dung của thành phần data[] của khung sẽ được thực hiện nhờ sử dụng ItemLocationBox.

Sau khi tất cả các phương pháp bảo vệ hoạt động từ ItemInformationBox, nội dung này có thể được tổ chức lại thành các khung ban đầu. Các byte đầu tiên size[0] của mảng data[] không được bảo vệ sẽ đặt trong khung type[0], và các byte size[i] tiếp theo được đặt trong một khung type[i] và cứ tiếp tục như thế. Chú ý, khi size_flag là 0, kích thước của khung đầu tiên không được biết và khi type_flag là 0, thì kiểu khung ban đầu không được biết. Điều này ngăn ngừa tấn công thuần văn bản. Khi cả size_flag và type_flag là 0, total_size cung cấp kích thước tổng của nội dung được bảo vệ.

Nếu số bản ghi là 0, hoặc nếu không có dữ liệu dư lại thhì dữ liệu đó sẽ có định dạng khung phù hợp với mã kiểu và mã kích thước, tức là dữ liệu không được bảo vệ chứa các kiểu và các kích thước.

Nếu bất kỳ một khung ở phần 1 bắt buộc được mã hóa, thì "jp2" sẽ được gỡ khỏi danh sách ở trong khung kiểu tệp.

If any part-1 mandatory box is encrypted, the "jp2" brand should be removed from the compatible list in file type box.

E.3.10.2 Cú pháp

```
aligned(8) class JProtectedBox extends Box('gprt') {
    bit(1) type_flag;
    bit(1) size_flag;
```

```
        bit(1) location_flag;
        unsigned int(5) reserved; // for ISO use
        if(size_flag == 1 || type_flag == 1 || location_flag == 1) {
            unsigned int(32) entry_count;
            if(location_flag == 1)
                unsigned int(8) offset_size;
            for(i=0; i<entry_count; i++) {
                if(size_flag == 1)
                    unsigned int(32) size;
                if(type_flag == 1)
                    unsigned int(32) type = boxtype;
                if(size_flag == 1 && size == 1)
                    unsigned int(64) large_size;
                if(location_flag == 1)
                    unsigned int(offset_size*8) offset;
            }
        }
        else {
            Unsigned int(32) total_size;
            if(total_size == 1)
                unsigned int(64) large_total_size;
    }
        unsigned int(8) data[];
    }
```

E.3.10.3 Ngữ nghĩa

size_flag cho biết giá trị kích thước có xuất hiện hay không. Giá trị 1 có nghĩa là có xuất hiện, 0 là không xuất hiện

type_flag cho biết kiểu khung có xuất hiện hay không. Giá trị là 1 tức là có xuất hiện, 0 tức là không xuất hiện

location_flag cho biết vị trí có xuất hiện hay không. Giá trị 1 có nghĩa là có xuất hiện, 0 có nghĩa là không xuất hiện.

entry_count cho biết số bản ghi trong Khung bảo vệ chung chung.

offset_size là chiều dài của offset theo đơn vị byte.

Mỗi bản ghi size là kích thước của khung được thay thế bởi Khung mô tả chung chung.

Mỗi bản ghi type là kiểu ban đầu của khung được thay thế bởi Khung bảo vệ chung chung.

Mỗi bản ghi offset là độ lệch của khung đã được thay thế bởi Khung mô tả chung chung.

total_size là kích thước tổng của các bản ghi trong Khung mô tả chung chung.

data[] là mảng các byte đến điểm cuối của khung, nó có thể được tham chiếu bởi ItemLocationBox và do đó được bảo vệ bởi một phương pháp được định nghĩa trong ItemProtectionBox.

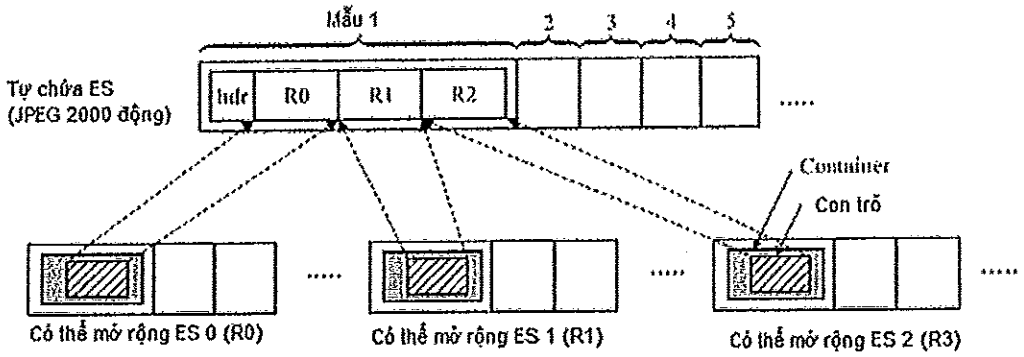
E.4 Định nghĩa mẫu và dòng cơ bản

E.4.1 Tổng quan

Mục này định nghĩa cấu trúc của dòng cơ bản (ES)

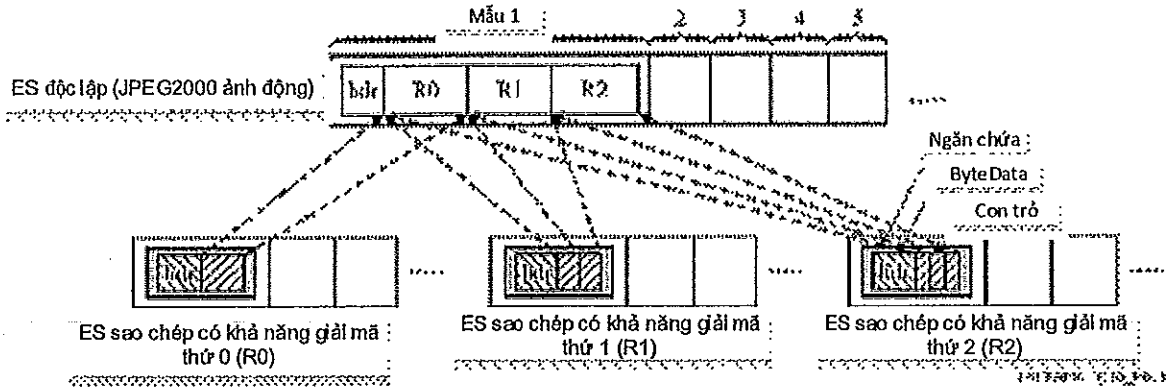
Dòng cơ bản chứa dữ liệu phương tiện, cấu trúc ByteData, cấu trúc ngăn chứa, cấu trúc con trỏ, hoặc là tổng hợp các thành phần đã nêu. Có hai loại dòng cơ bản: Loại thứ nhất được gọi là ES tự chứa, dòng này không có ngăn chứa, con trỏ hoặc cấu trúc ByteData. Định dạng của ES tự chứa không được định nghĩa trong tiêu chuẩn này, và ES đó có thể là bất kỳ định dạng phương tiện nào như chuỗi ảnh JPEG động. Loại thứ hai là ES sao chép (*composed ES),* dữ liệu phương tiện được sao chép từ các dòng cơ bản khác. ES sao chép có thể hoặc là sao chép dữ liệu từ rãnh ghi hoặc dữ liệu chuẩn trong các rãnh ghi khác. Khi phân đoạn dữ liệu phương tiện được sao chép từ các rãnh ghi khác thì đoạn này phải đóng gói theo cấu trúc ByteData; cấu trúc con trỏ được sử dụng để tham chiếu tới các phân đoạn dữ liệu phương tiện trong các dòng cơ bản khác. Khi một mẫu trong ES sao chép có nhiều hơn một cấu trúc, thì cấu trúc ngăn chứa phải được sử dụng để đóng gói tất cả các cấu trúc thuộc về mẫu đó.

Hình E.2 minh họa quan hệ giữa ES tự chứa và ES soạn thảo phân cấp. Trong ES soạn thảo phân cấp, mỗi mẫu được đóng gói bởi một cấu trúc ngăn chứa, tại đó con trỏ tham chiếu tới các phân đoạn dữ liệu mong muốn trong ES tự chứa. Chú ý rằng ES soạn thảo phân cấp không chứa bất kỳ một mào đầu nào, bộ tương thích phải tự động tạo ra mào đầu để dòng mã có khả năng giải mã bằng bộ giải mã thông thường. Hơn nữa, mỗi ES soạn thảo phân cấp không thể tự nó tạo thành một dòng mã hoàn chỉnh nhưng nhiều ES như vậy thì có thể tạo thành dòng mã hoàn chỉnh và có khả năng giải mã được. Ví dụ, trong Hình E.2, bộ tương thích phải kết hợp ES soạn thảo phân cấp 0 và 1 để tạp ra một khung JPEG2000 ở độ phân giải 1.



Hình E.2 – ES tự chứa và ES soạn thảo phân cấp

Hình 3 minh họa mối quan hệ giữa ES tự chứa và ES sao chép có khả năng giải mã. Trong ES sao chép có khả năng giải mã, một mẫu được đóng gói bởi một ngăn chứa, bao gồm cấu trúc dữ liệu (với thông tin mào đầu), và một hoặc nhiều cấu trúc con trỏ tham chiếu tới các phân đoạn dữ liệu trong ES tự chứa.



Hình E.3 – ES tự chứa và ES sao chép có khả năng giải mã

E.4.2 Cấu trúc trong dòng mã

Mục này định nghĩa cấu trúc bên trong dòng mã được sử dụng trong ES soạn thảo phân cấp và ES sao chép có khả năng giải mã. ES sao chép có thể có phương tiện truyền thông từ các dòng cơ bản khác hoặc nhờ sao chép hoặc tham chiếu. Cấu trúc ByteData được sử dụng để chứa dữ liệu phương tiện nhờ sao chép và cấu trúc con trỏ được sử dụng để chứa dữ liệu phương tiện nhờ tham chiếu. Ngoài ra, mỗi mẫu được đóng gói bởi cấu trúc ngăn chứa, cấu trúc này có thể chứa một hoặc nhiều ByteData hoặc cấu trúc con trỏ.

```
class aligned(8) DataUnit(type) {
    unsigned int(32) type;
    unsigned int(32) size;
    unsigned int(32) RDHints;
}
```

```
class ByteData (type='bdat') extends DataUnit {
        unsigned int(8) data[];
}
class container (type='cont') extends DataUnit {
        DataUnit(type) units[];
}
class Pointer(type='poin') extends DataUnit {
        unsigned int(8) track_ref_index;
        unsigned int(8) segment_count;
        for(int i=0; i<segment_count; i++) {
                unsigned int(32) offset;
                unsigned int(32) length;
        }
}
```

Ngữ nghĩa:

type cho biết loại cấu trúc dữ liệu, như "ByteData", "ngăn chứa" và "con trỏ".

size là kích thước của cấu trúc này, bao gồm chính nó và dữ liệu tiếp theo trong cấu trúc này.

RDHints cho biết độ quan trọng tương đối hoặc tuyệt đối của dữ liệu phương tiện mà đối tượng này chứa hoặc tham chiếu. Ví dụ, RDHints có thể là một giá trị tăng của méo, méo phương tiện sẽ tăng nếu dữ liệu phương tiện bị mất hoặc dữ liệu đó được xem là rất quan trọng.

data[] là mảng các byte chứa dữ liệu phương tiện theo định dạng ban đầu của dữ liệu đó. Bản sửa đổi này không quy định định dạng của dữ liệu phương tiện.

units[] là danh sách các đối tượng trong một ngăn chứa mục tiêu. Đối tượng có thể là ByteData hoặc con trỏ, nhưng không phải là một ngăn chứa khác.

track_ref_index quy định chỉ số của rãnh ghi mà con trỏ này chỉ tới.

segment_count là số cặp "độ dịch" và "chiều dài"

offset là độ lệch của byte đầu tiên trong phạm vi mẫu tham chiếu để sao chép.

length là số byte của đoạn dữ liệu

E.5 Bảo vệ ở mức định dạng tệp

E.5.1 Tổng quan

Mục này mô tả cách thức mà dữ liệu phương tiện được bảo vệ nhờ sử dụng các lược đồ bảo vệ (tức là việc nhận thực và mô tả) và bảo vệ này được báo hiệu bảo vệ nhờ sử dụng các khung được định nghĩa trong E..3.4 và E.3.5.

Khi các công cụ bảo mật được áp dụng thay đổi độ dài dữ liệu, công cụ đó sẽ cập nhật tất cả các con trỏ và các trường chiều dài trong tất cả các khung để đảm bảo bộ đọc phân tích chính xác.

E.5.2 Bảo vệ dựa trên đối tượng cho định dạng tập tin họ JPEG và định dạng tệp cơ sở ISO

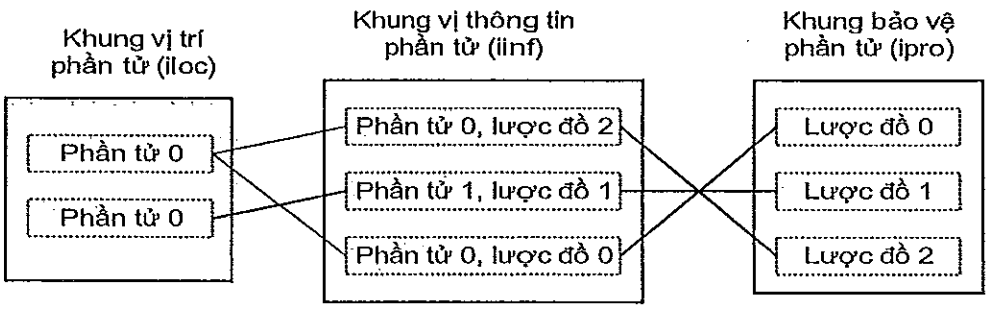
Phục lục này định nghĩa hai kiểu ProtectionSchemeInfoBox: nhận thực và mật mã hóa. Hai lược đồ bảo vệ này bảo vệ phương tiện co giãn mà không làm mất tính co giãn của nó.

This annex defines two types of ProtectionSchemeInfoBox: authentication and decryption. The two protection schemes protect the scalable media without loss of scalability.

Mỗi trường hợp sử dụng các tham số (MAC, IV, các khóa...) được ProtectionSchemeInfoBox đặt bên trong ItemProtectionBox mô tả. Mặt khác, ItemProtectionBox chứa danh sách các đối tượng và mỗi phần tử trỏ đến một hoặc nhiều hơn một phân đoạn dữ liệu phương tiện liên tiếp. ItemProtectionBox duy trì một bảng kết nối giữa các đối tượng bên trong ItemProtectionBox và lược đồ bảo vệ trong ItemProtectionBox. Hình E.4 là một ví dụ, trong đó có hai đối tượng và ba lược đồ bảo vệ: Đối tượng 0 được bảo vệ bởi lược đồ 1 và lược đồ 2; Đối tượng 1 được bảo vệ bởi lược đồ 1.

Như minh họa trong Hình E.4, đối tượng đó có thể được áp dụng với nhiều lược đồ bảo vệ, ví dụ đối tượng 0. Ngoài ra, đối tượng này có thể xếp chồng cùng với các đối tượng khác và các miền bị xếp chồng này có thể được áp dụng với nhiều lược đồ bảo vệ. Vì thế, quy định thứ tự tiến trình giữa các lược đồ bảo vệ là rất quan trọng. Định dạng tệp 'ffsc' yêu cầu tệp này phải không được bảo vệ (un-protected) ở vị trí đó vì các lược đồ này xuất hiện trong khung 'iinf'. Ví dụ lược đồ đầu tiên xuất hiện trong khung 'iinf' được áp dụng cho tệp đầu tiên và lược đồ sau cùng xuất hiện trong khung 'iinf' sẽ áp dụng cho tệp sau cùng. Trong ví dụ này, lược đồ 2 với đối tượng 0, lược đồ 1 với đối tượng 1, lược đồ 0 với đối tượng 0.

CHÚ THÍCH: thứ tự bảo vệ (với nhiều công cụ bảo vệ) phải chính xác, ngược lại với thứ tự không bảo vệ, tức là lược đồ đầu tiên xuất hiện trong khung 'iinf' là công cụ sau cùng được áp dụng và lược đồ sau cùng xuất hiện trong khung 'iinf' là công cụ đầu tiên được áp dụng.



Hình E.4 – Mối quan hệ giữa iloc, iinf và ipro

E.5.3 Các yêu cầu khác đối với bảo vệ đối tượng cho các định dạng tập tin họ JPEG

Các tệp JP2, JPX và JPM không dựa trên định dạng tệp cơ bản của ISO nhưng có một vài khung chung như Khung Kiểu Tệp. Để sử dụng bảo vệ đối tượng trong tiêu chuẩn này, những định dạng tệp này sẽ kết hợp bảo vệ bằng cách bổ sung 'meta', 'hdlr', 'ipro', 'iloc', và 'iinf' từ ISO/IEC 15444-12:2005, bổ sung vào các khung mới được định nghĩa trong phần bổ sung này.

Việc hoạt động của bảo vệ giống với định dạng tệp ISO cơ bản. Tuy nhiên, các dòng mã có định dạng tệp trong họ JPEG có thể xuất hiện trong các khung dòng mã liên lục bổ sung cho các khung Dữ liệu phương tiện ('mdat').

E.5.4 Bảo vệ mẫu

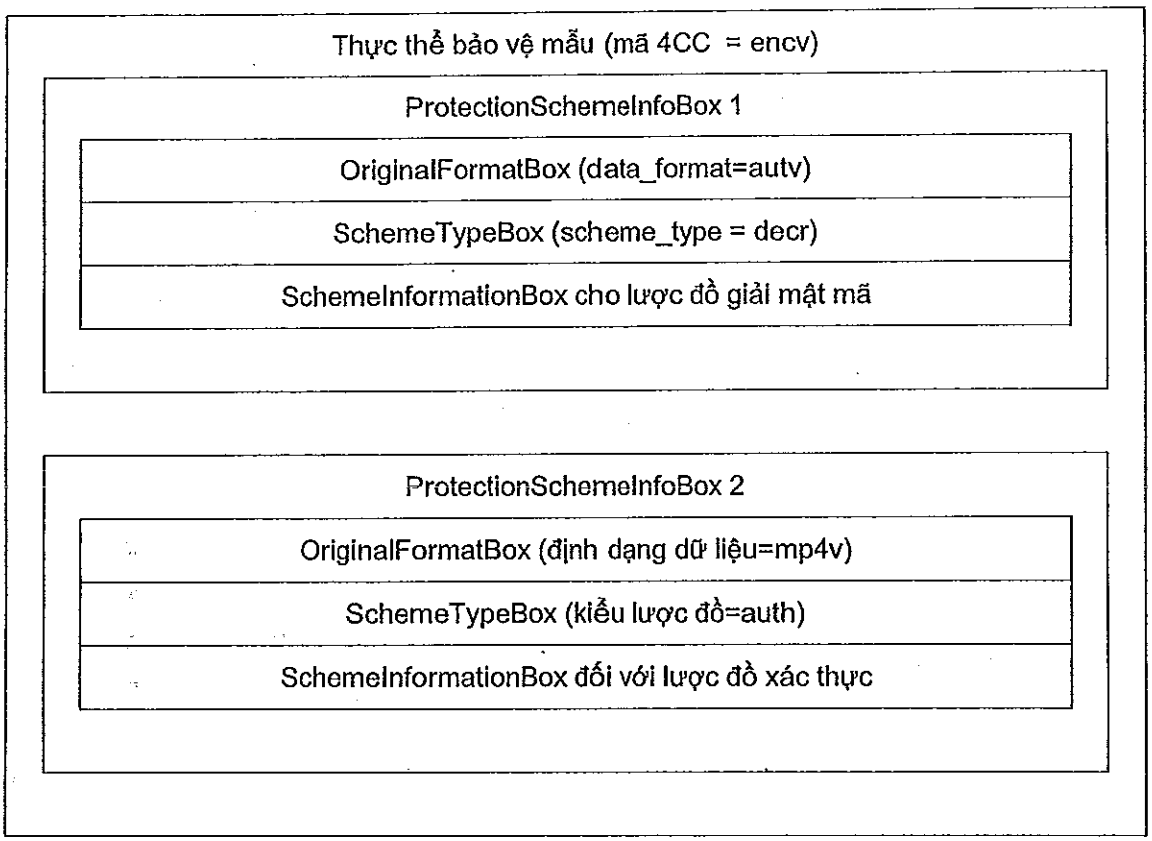
Khi lược độ bảo vệ được áp dụng cho mẫu cơ bản thì được báo hiệu bởi ProtectionSchemeInfoBox trong hoặc là ScalableSampleDescriptionEntry hoặc là ScalableSampleGroupEntry. Khi ProtectionSchemeInfoBox được đặt trong ScalableSampleDescriptionEntry thì bảo vệ này được áp dụng cho tất cả các mẫu trong rãnh ghi đó; khi ProtectionSchemeInfoBox đặt trong ScalableSampleGroupEntry thì bảo vệ chỉ được áp dụng cho các mẫu trong nhóm mẫu đó.

Khi các mẫu được áp dụng với nhiều lược đồ bảo vệ, thì ScalableSampleDescriptionEntry hoặc ScalableSampleGroupEntry chứa nhiều ProtectionSchemeInfoBoxes. Theo tên hiệu tệp 'ffsc', các mẫu phải không được bảo vệ (un-protected) ở vị trí tương ứng với ProtectionSchemeInfoBoxes được xác định.

Hình E.5 đưa ra ví dụ về một thực thể mô tả mẫu "mp4v" được bảo vệ với một nhật thực theo sau mật mã hóa. Chú ý rằng có hai ProtectionSchemeInfoBoxe trong thực thể này: một cho lược đồ mật mã và một cho lược đồ nhật thực. Để không bảo vệ mẫu, bộ đọc tệp phải áp dụng lược độ mật mã hóa đi sau lược đồ nhật thực, thứ tự đó là thứ tự xuất hiện trong thực thể mẫu này.

Khi bảo vệ mẫu được áp dụng cho ES sao chép thì nó được áp dụng cho dữ liệu phương tiện mà ngăn chứa, ByteData chứa hoặc con trỏ trỏ tới. Ví dụ để mật mã một mẫu trong ES sao chép, thì mẫu đó phải được gói bởi một ngăn chứa, tiến trình bảo vệ sẽ chỉ mật mã dữ liệu phương tiện của nó, cấu trúc khung của ngăn chứa không được mật mã.

Bảo vệ mẫu có thể được áp dụng cho tất cả các mẫu trong rãnh ghi hoặc nhóm các mẫu như một thể thống nhất (khi GL=0 trong SchemeInformationBox) hoặc tách biệt cho mỗi mẫu (khi GL=1 trong SchemeInformationBox). Thông thường, danh sách giá trị chỉ có MAC hoặc IV, và trong các trường hợp sau, Danh sách giá trị có một MAC hoặc IV cho mỗi mẫu.



Hình E.5 – Ví dụ về thực thể mô tả mẫu được bảo vệ bởi lược đồ xác thực theo lược đồ mô tả

Thư mục tài liệu tham khảo

[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.