INSO
11947-12
1st.Edition
2017
Identical with
ISO/IEC 23001-12:
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۱۹۴۷-۱۲
چاپ اول
۱۳۹۵

فنّاوری اطلاعات –
فنّاوری‌های سامانه‌های گروه متخصصین تصویر متحرک (MPEG) - قسمت۱۲: گونه‌های نمونه در قالب فایل رسانه بر پایه سازمان بین‌المللی استانداردسازی (ISO)

Information technology – MPEG systems technologies - Part 12: Sample Variants in the ISO base media file format

ICS: 35.040.40

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج - شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.gov.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.2592 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.gov.ir

Website: http://www.isiri.gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فنّاوری اطلاعات – فنّاوری سامانه‌های گروه متخصصین تصویر متحرک(MPEG) – قسمت۱۲: گونه‌های نمونه در قالب فایل رسانه بر پایه سازمان بین‌المللی استانداردسازی (ISO)»

رئیس:	**سمت و/یا محل اشتغال:**
رضائی، مهدی (دکتری مهندسی برق - مخابرات)	عضو هیئت علمی - دانشگاه سیستان و بلوچستان
دبیر:	
خزاعی، محمدرضا (کارشناسی ارشد مهندسی برق - مخابرات)	کارشناس فنّاوری اطلاعات - اداره کل استاندارد استان سیستان و بلوچستان
اعضا: (اسامی به ترتیب حروف الفبا)	
احمدی شکوه، جواد (دکتری مهندسی برق - مخابرات)	عضو هیئت علمی - دانشگاه سیستان و بلوچستان
خزاعی، علی‌اکبر (دکتری مهندسی برق - مخابرات)	عضو هیئت علمی - دانشگاه آزاد اسلامی واحد مشهد
صارمی‌فر، سرور (کارشناسی مهندسی برق - الکترونیک)	عضو مستقل
کشاورز، هنگامه (دکتری مهندسی برق - مخابرات)	عضو هیئت علمی - دانشگاه سیستان و بلوچستان
کلانتری، احسان (کارشناسی ارشد مهندسی شیمی)	کارشناس تدوین و آموزش - اداره کل استاندارد استان سیستان و بلوچستان
ماهرانی، مهدی (کارشناسی مهندسی برق - الکترونیک)	عضو مستقل
نظام، سید مهدی (کارشناسی ارشد مدیریت فنّاوری اطلاعات)	رئیس اداره فنّاوری اطلاعات - اداره کل استاندارد استان سیستان و بلوچستان
ویراستار:	
رثایی، حامد (کارشناسی مهندسی برق - قدرت)	کارشناس- دفتر تدوین استانداردهای ملی سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

پیش‌گفتار

استاندارد «فنّاوری اطلاعات – فنّاوری‌های سامانه‌های گروه متخصصین تصویر متحرک (MPEG) - قسمت۱۲: گونه‌های نمونه در قالب فایل رسانه بر پایه سازمان بین‌المللی استانداردسازی (ISO) » که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی/منطقه‌ای به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تهیه و تدوین شده، در چهارصد و هشتاد و نهمین اجلاسیه کمیتهٔ ملی استاندارد فنّاوری اطلاعات مورخ ۹۵/۱۲/۱۱ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم وخدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 23001-12, 2015: Information technology – MPEG systems technologies -Part 12: sample variants in the ISO base media file format

فنّاوری اطلاعات – فنّاوری‌های سامانه‌های گروه متخصصین تصویر متحرک (MPEG) – قسمت۱۲: گونه‌های نمونه در قالب فایل رسانه بر پایه سازمان بین‌المللی استانداردسازی (ISO)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و تعریف حمل جایگزین نمونه[1] در قالب فایل رسانه بر پایه سازمان بین‌المللی استانداردسازی (ISO) می‌باشد (ISO/IEC 14496-12).

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده‌شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود. درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده‌شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است .استفاده از مراجع الزامی زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 14496–12: 2015, Information technology - Coding of audio-visual objects - Part 12: ISO Base media file format

یادآوری ۱- استاندارد ملی ایران شماره ۱۲-۱۴۴۹۶: ۱۳۸۹، فنّاوری اطلاعات - کدگذاری شی‌های صوتی-تصویری - قسمت ۱۲ : قالب فایل رسانه‌ای بر پایه سازمان بین‌المللی استاندارد (ISO) با استفاده از استاندارد ISO/IEC 14496–12:2008 تدوین شده است.

یادآوری ۲- استاندارد ISO/IEC 14496-12 از نظر فنی، معادل استاندارد ISO/IEC 15444-12 می‌باشد.

2-2 ISO/IEC 23001-7:2015, Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files

یادآوری- استاندارد ملی ایران شماره ۷-۱۱۹۴۷: ۱۳۹۲، فن آوری اطلاعات - فن آوری سامانه MPEG- قسمت ۷: رمز گذاری عمومی در فایل‌های قالب فایل رسانه‌ای بر پایه سازمان بین المللی استانداردسازی (ISO) با استفاده از استاندارد ISO/IEC 23001-7:2012 تدوین شده است.

1- Carriage of sample variants

۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

۳-۱-۱

رمزنگاری‌شده مضاعف

double encrypted

داده گستره بایت[1] جایگزینِ نمونه که اولین مرتبه با یک کلید رسانه (به عنوان بخشی از رمزنگاری[2] جایگزین نمونه کامل) و سپس در مرتبه دوم با یک کلید گستره بایت جایگزین، رمزنگاری می‌شود.

یادآوری- جزئیات در زیربند ۶-۱ شرح داده شده است.

۳-۱-۲

کلید رسانه

media key

کلید رمزنگاری مربوط به یک یا تعداد بیشتری نمونه رسانه[3] است.

۳-۱-۳

شناسانه کلید (KID) رسانه

media KID

شناسانه کلید رمزنگاری مربوط به یک یا تعداد بیشتری نمونه رسانه است.

۳-۱-۴

جایگزینِ نمونه

sample variant

نمونه رسانه همگذاری‌شده[4] که جایگزین یک نمونه اصلی[5] می‌شود.

۳-۱-۵

گستره بایتِ جایگزین

variant byte range

محل دنباله[6] ای از بایت ها که ممکن است قسمتی از یک جایگزینِ نمونه را تشکیل دهد.

1- Byte range data
2- Encryption
3- Media samples
4- Assembled
5- Original sample
6- Sequence

۳-۱-۶

سازنده جایگزین

variant constructor

فراداده[1] جایگزینِ نمونه که توضیح می‌دهد چگونه یک جایگزینِ نمونه مجزا، همگذاری می‌شود.

۳-۱-۷

داده رسانه جایگزین

variant media data

داده رسانه که برای ساخت یک جایگزین نمونه به کار می‌رود، که بعضی از آن ها ممکن است از داده رسانه اصلی ناشی شوند.

۳-۱-۸

پردازنده جایگزین

variant processor

پودمان منطقی[2] که مراحل پردازش برای پیاده‌سازی فرآیند همگذاری جایگزین‌های نمونه را انجام می‌دهد.

۳-۲ کوته‌نوشت‌ها

CENC	Common ENCryption [a]	رمزنگاری عمومی
DRM	Digital Rights Management	مدیریت حقوق دیجیتالی
ISOBMFF	ISO Base Media File Format [b]	قالب فایل رسانه بر پایه ISO
IV	Initialization Vector	بردار مقداردهی اولیه
KID	Key Identifier	شناسانه کلید
a مشخص‌شده در استاندارد بین‌المللی ISO/IEC 23001-7:2015 b مشخص‌شده در استاندارد بین‌المللی ISO/IEC 14496-12:2015		

۴ مرور کلی (آگاهی‌دهنده)

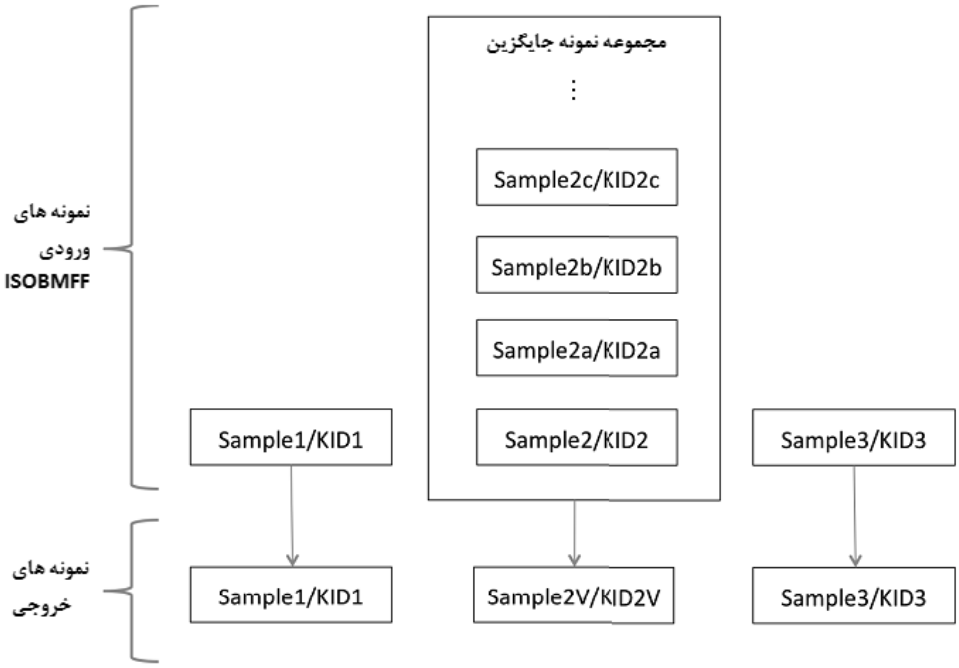
این استاندارد چارچوبی برای حمل جایگزین‌های نمونه در ISOBMFF تعریف می‌کند. جایگزین‌های نمونه به‌طور معمول برای فراهم کردن اطلاعات قانونی[3] در داده نمونه نونمایی شده[4] که به عنوان مثال می‌تواند شناسایی کارخواه[5] DRM باشد، به کار می‌روند. این چارچوب جایگزین در سازگاری[1] کامل با ISOBMFF و و CENC، و سازگار[2] با سامانه علامت‌گذاری[3] قانونی بخصوصی که به کار رفته در نظر گرفته شده است.

1- Metadadta
2- Logical module
3- Forensic information
4- Rendered sample data
5- Client

چارچوبِ جایگزین نمونه از سه ساختار هسته برای تعریف و حملِ داده جایگزین نمونه در ISOBMFF استفاده می‌کند: سازنده‌های جایگزین، گستره‌های بایتِ جایگزین، و نمونه‌های جایگزین.

یادآوری– مدل پردازش جایگزین که در بند ۹ توصیف شده، می‌تواند به معرفی مفاهیم کمک کند.

شکل ۱ فرانامه‌ای را نشان می‌دهد که در آن یک نمونه (نمونه۲) دارای تعدادی جایگزین نمونه است. شکل ۱، سه نمونه را در یک ردیف از چپ به راست نشان می‌دهد که نمونه وسطی آن‌ها دارای جایگزین‌هایی است. سطر بالایی نمایشی مفهومی از آنچه که به وسیله استاندارد ISOBMFF کدگذاری شده است می‌باشد و سطر پایین خروجی بعد از پردازش جایگزین نمونه است. دسترسی به نمونه‌ها، همان‌طور که در سطر بالایی از شکل ۱ نمایش داده شده، در اختیار KIDها است. برای جایگزین‌های نمونه، سلسله مراتبی از KIDها برای تأمین دسترسی به داده به کار می‌رود، که در آن KIDهای سطح بالاتر دسترسی به فراداده‌ی جایگزین نمونه و KIDهای سطح پایین‌تر دسترسی به داده رسانه را فراهم می‌کنند.



شکل ۱ – ساختار جایگزین نمونه

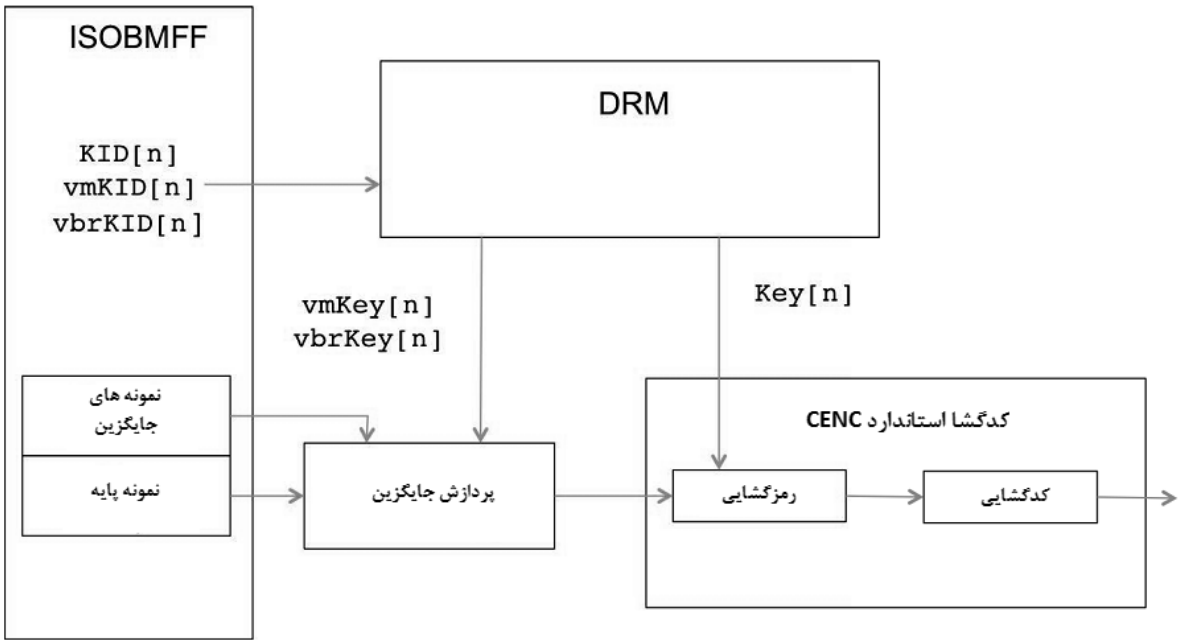
نقطه واپایش[4] برای استفاده از چارچوب پیشنهاد شده، منتشرکننده محتوا[5] است:

1- Compatible
2- Agnostic
در یک سامانه IT ، agnosticism اشاره به هر آن چه دارد که جهت سازگاری با بیشتر سامانه‌های رایج طراحی شده است.
3- Marking system
4- Control point
5- Content publisher

- منتشرکننده محتوا، داده جایگزین نمونه فشرده و رمزنگاری شده را به فایل ISOBMFF کدگذاری کرده و تضمین می‌کند که هر مجموعه از داده جایگزین نمونه برای یک زمان نمونه[1] مفروض توسط کلیدی متفاوت رمزنگاری شده و توسط KID متفاوتی نشانک‌دهی شده[2] باشد.
- منتشرکننده محتوا با DRM همکاری خواهد کرد تا نشر[3] کلیدها/ شناسانه‌کلیدها را مدیریت کنند به گونه‌ای که مسیر بازپخش[4] (داده نمونه واقعی که در طول بازپخش استفاده شده) کنترل می‌شود و پخش‌کننده صرفاً قادر به رمزگشایی و نونمایی داده‌ای است که برای نونمایی کردنش مجاز می‌باشد.

مدل کدگشا[5] برای پردازش فایل در شکل ۲ نشان داده شده است. آنچه که برای فرآیند کدگشایی کردنِ جایگزین نمونه مهم و بحرانی است، عبارت است از کنترل بر اینکه آیا و چگونه جایگزین‌های نمونه پردازش شده‌اند.

یادآوری– مراحل رمزگشایی و کدگشایی همان عملیات استانداردی هستند که برای هر کدگشای قادر به CENC صادق می‌باشد.



شکل ۲ – مدل کدگشای جایگزین

با اجرای عملیات در حوزه رمزنگاری/ فشرده‌سازی ، عملیات پیوند باند پایه امن[1]، (به عنوان مثال اختصاصی‌شده[2]، مسیرهای ویدئو امن[3]) محفوظ مانده و به طور کامل سازگار با CENC در نظر گرفته می‌شود.

1- Sample time
2- Signaled
3- Release
4- Playback path
5- Decoder

۵ سازنده‌های جایگزین

۵-۱ کلیات

یک سازنده جایگزین نمونه مشخص می‌کند که کدام بایت‌ها برای همگذاری یک جایگزین نمونه استفاده شده است. ممکن است برای یک نمونه ISOBMFF مفروض، یک یا تعداد بیشتری سازنده جایگزین نمونه مشخص شده باشد.

پردازنده جایگزین در صورت دسترسی داشتن به یک سازنده جایگزین ممکن است از آن استفاده کند. علاوه‌بر این با وجود سازنده جایگزین «دسترسی»، شامل دسترسیِ رمزنگاشتی[۴] نیز می‌باشد. یک سازنده جایگزین نمونه، داده‌ای که برای همگذاری یک جایگزین نمونه به کار رفته، و نیز KID رسانه مرتبط با آن و بردار مقداردهی اولیه برای رمزگشایی جایگزین نمونه را تعیین می‌کند.

۵-۲ دسترسی به سازنده‌های جایگزین نمونه

چنانچه به کدگشا اجازه دسترسی به کلید رسانه[۵] برای نمونه تعیین‌شده توسط شیار رسانه[۶] ISOBMFF داده شود، پردازش جایگزین برای این نمونه رخ نخواهد داد. اگر کدگشا دسترسی به کلید رسانه اصلی که توسط شیار رسانهISOBMFF تعیین شده نداشته باشد، به پردازنده جایگزین اجازه دسترسی به یک سازنده جایگزین مرتبط با نمونه داده خواهد شد.

کلید/ شناسانه‌کلید مرتبط با سازنده جایگزین، دسترسی به یک سازنده جایگزین بخصوص را کنترل می‌کند و بنابراین تابعی از مجموعه جفت مقادیر کلید/ شناسانه‌کلید است که توسط DRM در دسترس پردازنده جایگزین قرار می گیرد. بهتر است به ازای هر نمونه فقط یک سازنده جایگزین در دسترس پردازنده جایگزین قرار بگیرد. اگر به پردازنده جایگزین امکان دسترسی به یک سازنده جایگزین داده شود، باید به کدگشا نیز دسترسی به کلید رسانه مرتبط با KID رسانه که در سازنده جایگزین معین شده، داده شود.

اگر پردازنده جایگزین دسترسی به بیش از یک کلید/ شناسانه‌کلید مرتبط با سازنده جایگزین برای یک نمونه مفروض داشته باشد، اولین سازنده جایگزینی را که به ترتیب کدگذاری به آن دسترسی دارد مورد استفاده قرار می‌دهد. پردازنده جایگزین فقط از یک سازنده جایگزین برای همگذاری یک جایگزین نمونه استفاده می‌کند.

1- Secure baseband link operation
2- Dedicated
3- Secure video pathways
4- Cryptographic access
5- Media Key
6- Media track

۵-۳ رمزنگاری سازنده‌های جایگزین

هر سازنده جایگزین باید با یک «کلید سازنده جایگزین»[1] رمزنگاری شود.

از آنجایی که پردازنده جایگزین صرفاً با کلیدهای سازنده مربوط به سازنده جایگزینی که قرار است توسط آن پردازنده جایگزین بخصوص مورد استفاده قرار بگیرند، مجهز شده است، سازنده‌های جایگزین دیگری که توسط آن پردازنده جایگزین مورد استفاده قرار نمی‌گیرد، از لحاظ نفوذ امنیتی[2] تحت تأثیر پردازنده واقع نمی‌شوند.

۶ گستره‌های بایت جایگزین

۶-۱ کلیات

هر سازنده جایگزین، دنباله‌ای از یک یا تعداد بیشتر از گستره بایتِ جایگزین را معین می‌کند. هر گستره بایتِ جایگزین، محل دنباله‌ای از بایت‌هایی را تعیین می‌کند که ممکن است بایت‌های موجود در یک جایگزین نمونه را تشکیل دهند. گستره‌های بایتِ جایگزین می‌توانند شامل داده‌های بی‌استفاده نیز باشند.

دنباله گستره‌های بایتِ جایگزین که در یک سازنده جایگزین تعریف شده‌اند، در قالب یک یا تعداد بیشتری گروه‌های گستره بایتِ جایگزین با یکدیگر گروه‌بندی می‌شوند. هر گروه گستره بایتِ جایگزین باید تعداد یک یا بیشتری از گستره‌های بایت جایگزین را مشخص کنند. یک گستره بایتِ جایگزین مجزا درون یک گروه گستره بایتِ جایگزین:

- ممکن است به بایت‌های داده موجود در یک جایگزین نمونه که در دسترس پردازنده‌های جایگزین بخصوصی است، ارجاع دهد («گستره بایت جایگزین حقیقی»).
- ممکن است به بایت‌هایی از داده ارجاع دهد که در دسترس هیچ پردازنده جایگزینی قرار داده نشده‌اند («گستره بایت جایگزین جعلی»).

یک «گستره بایت جایگزین جعلی» را می‌توان جهت پنهان کردن مقدار واقعی «گستره بایت جایگزین حقیقی» که درون یک سازنده جایگزین تعریف شده، به کار برد. پردازنده جایگزین از تمام گستره‌های بایتِ جایگزین که به آن‌ها دسترسی دارد استفاده می‌کند. این «دسترسی» به گستره بایت جایگزین ، شامل دسترسیِ رمزنگاشتی نیز می‌باشد.

از آنجایی که داده‌های مربوط به جایگزین‌های نمونه توسط سازنده‌های جایگزین مختلف مورد ارجاع قرار می‌گیرند، می‌توان آن‌ها را به صورت غیرهمجوار[3] ذخیره نمود. داده مربوط به یک جایگزین نمونه بخصوص را

1- Variant Constructor key
2- Security compromise
3- Non-contiguously

می‌توان توسط یک دنباله از دو یا تعداد بیشتری از گستره‌های بایت جایگزین و به صورت غیرهمجوار ذخیره نمود.

۶-۲ دسترسی به گستره‌های بایت جایگزین

اگر یک گستره بایت جایگزین درون یک گروه گستره بایت جایگزین نشانک دهد که داده اشاره شده توسط گستره بایتِ جایگزین، رمزنگاری نشده است (و پردازنده جایگزین به سازنده جایگزین دسترسی داشته باشد)، در این صورت پردازنده جایگزین به گستره بایت جایگزین و بایت‌های رمزنگاری نشده مرتبط با آن دسترسی دارد.

اگر یک گستره بایتِ جایگزین موجود درون یک گروهِ گستره بایت جایگزین نشانک دهد که داده اشاره شده توسط گستره بایت جایگزین، رمزنگاری شده است، آنگاه دسترسی به گستره بایت جایگزین و بایت‌های مرتبط با آن یا توسط کلید/ شناسانه‌کلید مربوط به هر گستره بایت جایگزین کنترل می‌شود یا چنانچه هیچ کلید گستره بایتِ جایگزینی برای یک گروه بخصوص از گستره بایتِ جایگزین تعریف نشده باشد، با کلید رسانه تعریف شده توسط سازنده جایگزین کنترل می‌شود و چنانچه یکی تعریف شده باشد آنگاه این کنترل توسط کلید گستره بایت جایگزین صورت می‌پذیرد. بنابراین دسترسی به یک گستره بایت جایگزین و داده‌های مرتبط با آن که توسط گستره بایت جایگزین مورد اشاره قرار می‌گیرد، تابعی از یک مجموعه جفت مقادیر کلید/ شناسانه‌کلید می‌باشد که توسط DRM در دسترس پردازنده جایگزین قرار گرفته است. توصیه می‌شود تنها یک گستره بایت جایگزین درون یک گروه گستره بایت جایگزین در دسترس پردازنده جایگزین قرار بگیرد.

اگر پردازنده جایگزین برای یک نمونه مفروض به بیش از یک کلید/ شناسانه‌کلید مرتبط با گستره‌های بایت جایگزین موجود در همان گروه گستره بایتِ جایگزین دسترسی داشته باشد، آنگاه پردازنده از اولین گستره بایت جایگزین که به ترتیب کدگذاری داده به آن دسترسی دارد استفاده می‌کند. پردازنده جایگزین حداکثر از یک گستره بایت جایگزین موجود در یک گروه گستره بایت جایگزین برای همگذاری یک جایگزین نمونه استفاده می‌کند.

گستره‌های بایت جایگزین را می‌توان به صورت کارآمد برای کدگذاری صرفاً تفاضل‌ها (معمولاً کوچک) در جایگزین‌های نمونه برای یک زمان ارائه[1] مفروض بدون تکرار داده‌های غیرتفاضلی[2] یا بدون اینکه تفاضل‌های جایگزین نمونه در معرض پردازنده جایگزین قرار گیرد، به کار برد. این امر توسط رمزنگاری مضاعف، که در آن داده تفاضلی ابتدا توسط کلید رسانه رمزنگاری شده و سپس توسط کلید گستره بایت جایگزین رمزنگاری می‌گردد، صورت می‌پذیرد. پردازنده جایگزین جهت رمزگشایی چنین داده تفاضلی نیاز به دسترسی به کلید گستره بایت جایگزین دارد، از این رو دسترسی به داده تفاضلی را می‌توان از طریق کلید گستره بایت

1- Presentation time
2- Non-difference data

جایگزین کنترل کرد. این امر استفاده مجدد از داده مشترک[1] را امکان‌پذیر ساخته و سازگاری جایگزین نمونه با CENC را حفظ می‌کند، که مستلزم این است تنها یک کلید رسانه به یک نمونه مفروض اعمال شود. اگر گستره‌های بایت جایگزین این قابلیت را فراهم نکرده باشند، آنگاه لازم خواهد بود که تمام داده‌ها، شامل داده‌های تفاضلی و غیرتفاضلی، برای هر جایگزین نمونه تکرار شود تا از داده تفاضلی با یک کلید متفاوت حفاظت شود؛ این عملی کم بازده است.

۶-۳ رمزنگاری اطلاعات گستره بایت جایگزین

تعاریف گستره بایت جایگزین به صورت مجزا رمزنگاری نمی‌شوند (آنها به عنوان جزئی از سازنده جایگزین رمزنگاری می‌شوند).

۷ جایگزین‌های نمونه

۷-۱ کلیات

داده‌ای که برای نونمایی یک نمونه استفاده می‌شود توسط یک سازنده جایگزین (اگر پردازنده جایگزین دسترسی به سازنده جایگزین مربوط به نمونه را داشته باشد؛ مطابق با زیربند ۸-۳-۳) یا به وسیله داده رسانه که توسط ISOBMFF تعریف شده است، تعیین می‌شود. هنگامی که از سازنده‌های جایگزین استفاده می‌شود، داده واقعی[2] که برای بازسازی نمونه به کار می‌رود از طریق همگذاری به دست می‌آید و داده بایت که به وسیله گستره‌های بایت جایگزین مورد اشاره قرار می‌گیرد، به ترتیب ظاهر شدن در سازنده جایگزین در دسترس پردازنده جایگزین قرار می‌گیرد (مطابق با بند ۶ این استاندارد) و این ساختار نهایی یک نمونه رمزنگاری شده معتبر برای سامانه رمزنگاری نهفته نشانک‌دهی‌شده[3] را نتیجه می‌دهد؛ این نمونه به دست آمده یک جایگزین نمونه خوانده می‌شود.

۷-۲ دسترسی به جایگزین‌های نمونه

به محض این که جایگزین نمونه از گستره‌های بایت جایگزین همگذاری شد، دسترسی به داده نمونه توسط کلید رسانه معین شده در سازنده جایگزین کنترل می‌شود و بنابراین تابعی از مجموعه جفت مقادیر کلید/ شناسانه‌کلید که توسط DRM در دسترس پردازنده جایگزین قرار می‌گیرد، می‌باشد.

1- Common data
2- Actual data
3- Signalled underlying encryption system

۷-۳ رمزنگاری جایگزین‌های نمونه

جایگزین‌های نمونه باید همواره طبق نشانک‌دهیِ طرح[1] مربوط به شیار رسانه مرتبط رمزنگاری شوند. گستره‌های بایت جایگزین یک جایگزین نمونه ممکن است رمزنگاری نشده باشند، یا ممکن است با یک کلید رسانه رمزنگاری شده باشند. کلید رسانه با یک یا تعداد بیشتری نمونه مرتبط شده است.

هنگامی که بایت‌های موجود در جایگزین نمونه توسط یک کلید رسانه رمزنگاری شده‌اند، یک یا تعداد بیشتری از گستره‌های بایتِ داده رسانه جایگزین رمزنگاری‌شده، ممکن است مجدداً طبق نشانک‌دهیِ رمزنگاری عمومی با یک «کلید گستره بایت جایگزین» رمزنگاری شوند؛ جزئیات در زیربند ۸-۳-۴ شرح داده شده است.

از آنجایی‌که یک پردازنده جایگزین، تنها با کلیدهای گستره بایت جایگزین مربوط به داده رسانه جایگزین و رمزنگاری شده مضاعف که قرار است توسط آن پردازنده جایگزین بخصوص مورد استفاده قرار گیرند، تجهیز شده‌اند، داده‌های رسانه جایگزین رمزنگاری‌شده مضاعف که توسط آن پردازنده جایگزین به کار نمی‌روند در معرض کشف آن پردازنده جایگزین قرار نمی‌گیرند.

۸ ذخیره‌سازی ISO

۸-۱ کلیات

داده جایگزین در یک شیار فراداده ISOBMFF (شیار جایگزین) ذخیره می‌شود. یک شیار رسانه ISOBMFF (شیار رسانه) یا یک شیار جایگزین ممکن است که با یک یا تعداد بیشتری شیارهای جایگزین، همان‌طور که در زیربند ۸-۲-۲ تعریف شده، وابسته باشد.

- با برقرار شدن یک وابستگی[2] بین یک شیار رسانه و یک شیار جایگزین، هر زمان که یک کدگشا دسترسی به کلید/ شناسانه‌کلید تعریف شده برای یک نمونه در شیار رسانه نداشته باشد، پردازش جایگزین نمونه رخ خواهد داد، همان طور که در زیربند ۵-۲ شرح داده شده است.
- هنگامی که ارتباطی از طریق یک شیار جایگزین (شیار جایگزین اصلی) با شیار جایگزین دیگری (که آن را دیگر شیار جایگزین می‌نامیم) برقرار می‌شود، داده جایگزین موجود در دیگر شیار جایگزین را می‌توان توسط شیار جایگزین اصلی مورد استفاده قرار داد.
- نمونه‌های درون شیارهای وابسته در صورتی که زمان-موازی[3] باشند، با هم وابسته هستند، همان‌طور که در زیربند ۸-۳-۵ معین شده است.

1- Scheme signalling
2- Association
3- Time-parallel

۸-۲ شیارهای جایگزین

۸-۲-۱ تعریف

داده جایگزین باید در یک شیار فراداده ISOBMFF که از قیود زیر پیروی می‌کند، ذخیره شود:

الف- شیار باید از **handler_type** برابر با '**meta**' در جعبه اداره‌کننده مرجع[1] ('**hdlr**') برای هر ISOBMFF استفاده کند؛ به بند ۱۲ مراجعه شود.

ب- شیار باید از ورودی نمونه[2] **VariantMetaDataSampleEntry()** همانطور که در زیربند ۸-۲-۳ معین شده، استفاده کند.

پ- داده جایگزین به عنوان نمونه‌ها طبق زیربند ۸-۳ در شیار ذخیره شود.

ت- شیار باید از همان زمان پایه[3] یکسان متناظر با ویدئو، صدا یا دیگر شیارهای جایگزین استفاده کند.

۸-۲-۲ وابستگی

شیارهای ISOBMFF ممکن است به یکی از شیوه‌های زیر با شیارهای جایگزین وابسته شوند:

- زمینه تعریف‌شده بیرونی[4]
- در شیار منبع (به عنوان مثال در شیار رسانه اصلی) و با استفاده از جعبه نوع مرجع شیار[5] موجود در جعبه مرجع شیار[6] ('**tref**') از جعبه شیار[7] ('**trak**') که این جعبه شیار یک **reference_type** برابر با '**cvar**' دارد و یک یا تعداد بیشتر **track_IDs** که هر کدام متناظر هستند با یک **track_ID** از یک شیار جایگزین که قرار است در همان فایل به آن‌ها ارجاع شود.

ملزومات اضافی زیر به **track_IDs** موجود در یک جعبه نوع مرجع شیار با **reference_type** برابر با '**cvar**' اعمال می‌شود:

الف- **track_ID** ممکن است مقداری داشته باشد که با **track_ID** ای از یک شیار در همان فایل مطابقت نداشته باشد. این مشخصات چگونگی محل‌یابی[8] فایلِ ارجاع‌شده و حاوی چنین شیاری، را تعیین نمی‌کنند.

1- Handler Reference Box
2- Sample entry
3- Timebase
4- Externally defined context
5- Track reference type box
6- Track reference box
7- Track box
8- Locate

ب- اگر **track_ID** با یک **track_ID** از یک شیار در همان فایل مطابقت داشته باشد، شیار باید یک شیارِ جایگزین باشد که از زیربند ۸-۲-۱ پیروی می‌کند.

مرجع‌های شیار جایگزین[1] که برای یک شیار رسانه تعریف شده‌اند، باید به ترتیب جستجوی سازنده جایگزین تعریف شوند. پردازنده جایگزین ، به هنگام جستجو برای یک سازنده جایگزین قابل دسترس، شیارهای جایگزین را بر طبق همین ترتیب پردازش خواهد کرد.

۸-۲-۳ ورودی نمونه فراداده جایگزین[2]

۸-۲-۳-۱ قاعده نحوی

```
class VariantMetaDataSampleEntry() extends MetaDataSampleEntry
('cvar') {
     unsigned int(32)    variant_constructor_scheme_type;
     unsigned int(32)    variant_constructor_scheme_version;
     unsigned int(32)    media_track_scheme_type;
     unsigned int(32)    media_track_scheme_version;
     unsigned int(32)    IV_Size;
     unsigned int(32)    variant_byte_range_scheme_type;
     unsigned int(32)    variant_byte_range_scheme_version;
}
```

۸-۲-۳-۲ ساختار معنایی

- **variant_constructor_scheme_type** : باید با یک کد چهار نویسه‌ای[3] که طرح حفاظت حفاظت اعمال‌شده به سازنده‌های جایگزین موجود در شیار را تعیین می‌کند تنظیم شود، به زیربند ۸-۳-۴ مراجعه شود.

- **variant_constructor_scheme_version** : باید با نسخه طرح حفاظت اعمال شده به سازنده های جایگزین موجود در شیار تنظیم شود، به زیربند ۸-۳-۴ مراجعه شود.

- **media_track_scheme_type** : باید با یک کد چهار نویسه‌ای که طرح حفاظت اعمال‌شده به شیار رسانه وابسته را تعیین می‌کند تنظیم شود، همان‌گونه که برای فیلد **schema_type** در شیار رسانه وابسته توسط زیربند ۸-۱۲-۵-۳ استاندارد ISOBMFF مشخص شده است.

1- Variant track references
2- Variant Metadata Sample Entry
3- Character

- **media_track_scheme_version** : باید با نسخه طرح حفاظت اعمال‌شده به شیار رسانه وابسته تنظیم شود، همان گونه که برای فیلد **scheme_version** در شیار رسانه وابسته توسط زیربند ۸-۱۲-۵-۳ استاندارد ISOBMFF مشخص شده است.

- **IV_Size** : باید اندازه IV بر حسب بایت که به شیار جایگزین اعمال می‌شود را نشانک‌دهی کند (همان‌گونه که در فهرست سازنده جایگزین و ساختارهای سازنده جایگزین به کار رفته است). IV_Size باید با IV_Size شیار رسانه وابسته، همخوانی داشته باشد.

- **variant_byte_range_scheme_type** : باید با کد چهار نویسه‌ای تنظیم شود که طرح حفاظت اعمال‌شده به رمزنگاری مضاعفِ بایت‌هایی که توسط گستره بایت جایگزین مورد اشاره قرار می‌گیرند را تعیین می‌کند؛ به زیربند ۸-۳-۴ مراجعه شود.

- **variant_byte_range_scheme_version** : باید با نسخه طرح حفاظت اعمال‌شده به رمزنگاری مضاعفِ بایت‌هایی که توسط گستره‌های بایت جایگزین مورد اشاره قرار می‌گیرند تنظیم شود؛ به زیربند ۸-۳-۴ مراجعه شود.

۸-۳ داده نمونه

۸-۳-۱ داده جایگزین

۸-۳-۱-۱ تعریف

یک نمونه در یک شیار جایگزین یا خالی است (اندازه صفر) یا برابر با یک ساختار **VariantData()**.

۸-۳-۱-۲ قاعده نحوی

```
aligned(8) class VariantData
{
     VariantConstructorList()     variant_list;
     VariantConstructor()[]       variant_constructors;
     unsigned int(8)[]            variant_pool;
}
```

۸-۳-۱-۳ ساختار معنایی

- **variant_list** : فهرست سازنده جایگزین همان گونه که در ۸-۳-۲ تعریف شده است.

- **variant_constructor** : آرایه سازنده‌های جایگزین که توسط فهرست سازنده جایگزین به آن اشاره می‌شود.

- **variant_pool** : انباره‌ای[1] از بایت‌های جایگزین که سازنده جایگزین ممکن است به آنها اشاره کند.

۸-۳-۲ فهرست سازنده جایگزین

۸-۳-۲-۱ تعریف

ساختار **VariantConstructorList()** اطلاعات ویژه نمونه درباره محل سازنده‌های جایگزین بالقوه[2] را برای جایگزین‌های نمونه مشخص می‌کند.

هر تعریف نمونه در یک شیار جایگزین ممکن است یک یا چند ورودی محل سازنده جایگزین[3] در **VariantConstructorList()** داشته باشد. همان‌طور که در زیربند ۵-۲ لازم بود، فقط یک ورودی محل سازنده جایگزین مجزا در طول بازپخشِ یک نمونه مفروض به کار می‌رود و پردازنده جایگزین از اولین سازنده جایگزینی که به ترتیب تعریف شده در ساختار **VariantConstructorList()** به آن دسترسی دارد استفاده می‌کند.

ورودی‌های مجزا در **VariantConstructorList()** :

- ممکن است به یک **VariantConstructor()** برای تعریف نمونه‌ای که در طول فرامانه‌های بازپخش بخصوص به کار می‌رود اشاره کنند («سازنده‌های جایگزین حقیقی»)؛ یا
- ممکن است به بایت‌هایی که در دسترس هیچ پردازنده جایگزین دیگری قرار داده نشده‌اند، اشاره کنند («سازنده جایگزین جعلی»).

یادآوری- بدون دسترسی به کلید رمزگشایی اشاره شده توسط vcKID، سازنده‌های جایگزین جعلی و سازنده‌های جایگزین حقیقی غیر قابل تشخیص هستند. سازنده‌های جایگزین جعلی را می‌توان برای پنهان کردن تعداد سازنده‌های جایگزین حقیقی که در آرایه **variant_constructors** تعریف شده‌اند به‌کار برد.

۸-۳-۲-۲ قاعده نحوی

```
aligned(8) class VariantConstructorList
{
      unsigned int(32)                    size;
      unsigned int(8)                variant_constructors_count;
      for( i=1 ; i<= variant_constructors_count; i++) {
            unsigned int(8)[16]           vcKID;
            unsigned int(8*IV_Size)       vcIV;
            unsigned int(32)              variant_constructor_offset;
            unsigned int(32)              variant_constructor_size;
      }
      unsigned int(8)[]                   padding;
}
```

1- Pool
2- Location of potential variant constructors
3- Variant constructor location entries

۸-۳-۲-۳ ساختار معنایی

- **Size** : باید با اندازه **VariantConstructorList()** برحسب بایت تنظیم شود.
- **variant_constructors_count** : باید با تعداد ورودی های سازنده جایگزین در آرایه سازنده های موجود در **VariantData()** تنظیم شود.
- **vcKID** : «KID سازنده جایگزین». این KID باید ID کلید فراداده سازنده جایگزینی را که برای رمزگشایی سازنده جایگزین رمزنگاری‌شده به کار رفته است، مشخص کند.
- **vcIV** : «بردار مقداردهی اولیه سازنده جایگزین». این فیلد باید حاوی بردار مقداردهی اولیه که برای رمزگشایی سازنده جایگزین رمزنگاری شده به‌کار می‌رود باشد.
- **variant_constructor_offset** : دورافت[1] بایت از **VariantConstructor()** متناظر. این دورافت نسبت به شروع **VariantData()** است.
- **variant_constructor_size** : طول **VariantConstructor()** برحسب بایت. ترکیب **variant_constructor_offset** و **variant_constructor_size** محل و اندازه **VariantConstructor()** را نشان می دهد. گستره بایت تعریف شده توسط **variant_constructor_offset** و **variant_constructor_size** باید صرفاً به بایت‌های درون **variant_constructors array** موجود در **VariantData()** اشاره کنند و نه هیچ بایت دیگری.
- **padding**: آرایه بایت[2] ممکن است شامل هر داده‌ای باشد و برای افزایش اندازه **VariantConstructorList()** به کار رود.

یادآوری- این لایی‌گذاری[3] را می‌توان برای نامشخص کردن اندازه **VariantConstructorList()** در صورتی که رمزنگاری شده باشد به کار برد.

1- Offset
2- Byte array
3- Padding

۸-۳-۳ سازنده جایگزین

۸-۳-۳-۱ قاعده نحوی

```
aligned(8) class VariantConstructor
{
      unsigned int(8)[16]                KID;
      unsigned int(8*IV_Size)            IV;
      unsigned int(32)                       variant_byte_ranges_count;
      for( i=1; i<= variant_byte_ranges_count; i++ )
      {
            unsigned int(8)              variant_byte_range_flgs;
            if( variant_byte_range_flgs & 0x02 )
            {
                  unsigned int(8)[16]    vbrKID;
                  unsigned int(8*IV_Size)    vbrIV;
                  }
                  if( variant_byte_range_flgs & 0x08 ) {
                  unsigned int(8)        variant_track_reference index;
                  }
                  signed int(8)              relative_sample_number;
                  unsigned int(32)       variant_byte_range_offset;
                  if( variant_byte_range_flgs & 0x06 != 0x02 ) {
                  unsigned int(32)       variant_byte_range_size;
                  }
      }
      unsigned int(8) []                 padding;
}
```

۸-۳-۳-۲ ساختار معنایی

KID : KID رسانه. این KID باید ID کلید رسانه‌ای را مشخص کند که از آن برای رمزگشایی داده جایگزین نمونه رمزنگاری شده بعد از بازهمگذاری[1] گستره‌های بایت جایگزین کاربردی[2] استفاده می‌شود. رمزگشایی بر طبق طرح حفاظت نشانک‌دهی‌شده در شیار رسانه وابسته رخ می‌دهد.

IV : بردار مقداردهی اولیه که باید برای رمزگشایی داده رسانه جایگزین رمزنگاری شده بعد از همگذاری دوباره گستره‌های بایت جایگزین کاربردی مطابقِ طرح حفاظت نشانک‌دهی‌شده در شیار رسانه وابسته به کار می‌رود.

variant_byte_ranges_count : باید با مقداری برابر با تعداد گستره‌های بایت جایگزین تعیین‌شده برای این سازنده جایگزین تنظیم شود. جزئیات در بند ۶ شرح داده شده است.

1- Re-assembly
2- Applicable

variant_byte_range_flags : باید به شرح زیر تنظیم شود:

0x01 رمزنگاری‌شده[1]

هنگامی که نشانده شود، داده جایگزین نمونه که توسط گستره بایت جایگزین مورد اشاره قرار گرفته باید با کلید رسانه رمزنگاری شود.

0x02 رمزنگاری-مضاعف[2]

هنگامی که نشانده شود، داده جایگزین نمونه که توسط گستره بایت جایگزین مورد اشاره قرار گرفته باید به وسیله یک کلید گستره بایت جایگزین، رمزنگاری مضاعف شود. چنانچه **variant_byte_range_flags** بدین صورت نشانک‌دهی شده باشد که داده جایگزین نمونه که توسط گستره بایتِ جایگزین مورد اشاره قرار گرفته، رمزنگاری نشده است، معنایی برای آن تعریف نشده است.

0x04 شروع-گروه[3]

هنگامی‌که نشانده شود، گستره بایت جایگزین باید شروع یک گروه گستره بایت جایگزین باشد و بدین طریق نشانگری[4] را برای گروه‌های گستره بایت جایگزین درون **VariantConstructor()** فراهم کند. همانطور که در بند ۶ ذکر شد، گستره‌های بایت جایگزین که در **VariantConstructor()** تعریف شده‌اند، به یک یا تعداد بیشتری گروه-های گستره بایت جایگزین گروه‌بندی می‌شوند، و از هر گروه گستره بایت جایگزین، یک گستره بایت جایگزین توسط پردازنده جایگزین به کار می‌رود. در نتیجه این امر مستلزم این است که حتی اگر تنها یک گستره بایت جایگزین در **VariantConstructor()** تعریف شده باشد، یا اگر تنها یک گستره بایت جایگزین درون یک گروه گستره بایت جایگزین وجود داشته باشد (بدین معنی که گستره‌های بایت جایگزینِ دیگر برای یک گستره بایت جایگزین بخصوص مربوط به داده رسانه جایگزین وجود نداشته باشند)، شروع گروه گستره بایت جایگزین با این تک[5] گستره بایت جایگزین نشانک‌دهی شود. نظیر زیربند ۶-۲، اگر بیش از یک گستره بایت جایگزین در یک گروه گستره بایت جایگزین منفرد حضور داشته باشد، هر کدام به ترتیب رمزنگاری مضاعف شده-اند تا دسترسی پردازنده جایگزین به یک گستره بایت درون گروه گستره بایت را محدود کنند.

1- Encrypted
2- Double-enc
3- Group-start
4- Marker
5- Singular

یادآوری- یک پردازنده جایگزین از این پرچم برای تصمیم گرفتن در مورد وقوع خطای داده استفاده می‌کند – اگر هیچ گستره بایت جایگزین در یک گروه گستره بایت جایگزین تشخیص داده نشود، یک خطا رخ داده است.

0x08 منبع-داده[1]

هنگامی که با مقدار 0 تنظیم شود، باید منبع داده برای این گستره، شیار رسانه اصلی باشد.

هنگامی که با مقدار 1 تنظیم شود، **variant_track_reference_index** به شیار جایگزینی که باید منبع داده باشد، اشاره می‌کند.

vbrKID : «KID گستره بایت جایگزین». این KID باید ID کلید گستره بایت جایگزین که برای رمزگشایی داده رسانه جایگزین رمزنگاری شده مضاعف به کار رفته را مشخص کند.

vbrIV : «بردار مقداردهی اولیه گستره بایت جایگزین». این فیلد باید حاوی بردار مقداردهی اولیه که برای رمزگشایی داده رسانه جایگزین رمزنگاری شده مضاعف به کار رفته، باشد.

variant_track_reference_index : این شاخص[2] یا باید برای مراجع شیار از این شیار نمونه جایگزین تا شیار جایگزین دیگر که حاوی داده جایگزینی است برابر 1 باشد (بر حسب ترتیب تعریف مرجع؛ مطابق با زیربند ۸-۲-۲) یا این مقدار برابر با 0 بوده که در این صورت داده از همین شیار جایگزین حاضر استخراج می‌شود.

relative_sample_number : با یافتن منبع داده شیار (پرچم data-source و فیلد **variant_track_reference_index** را در بالا ببینید)، این فیلد به شرح زیر تعیین می‌کند که کدام منبع داده نمونه باید برای گستره بایت جایگزین استفاده گردد : هنگامی که با 0 تنظیم شود، data-source نمونه، نمونه مرتبط زمان-موازی[3] در زیربند ۸-۳-۵ است؛ هنگامی که با یک مقدار منفی تنظیم شود، نمونه قبلی N اُم به کار می‌رود؛ هنگامی که با یک مقدار مثبت تنظیم شود، نمونه بعدی N اُم به کار می رود.

variant_byte_range_offset : دوراُفتِ بایت از شروع نمونه ارجاع شده (نمونه اصلی در شیار رسانه، **VariantData()** که حاوی این سازنده جایگزین است، یا **VariantData()** در یک شیار جایگزین ارجاع شده، وابسته به پرچم **data-source** و **variant_track_reference_index**) تا ابتدای داده مربوط به این گستره بایت جایگزین.

1- Data-source
2- Index
3-Time-parallel associated sample

variant_byte_range_size : اندازه گستره بایت جایگزین برحسب بایت. ترکیب **variant_byte_range_offset** و **variant_byte_range_size** گستره بایت مربوط به گستره بایت جایگزین در نمونه مورد اشاره را مشخص می‌کند. گستره بایت جایگزین معین شده توسط **variant_byte_range_offset** و **variant_byte_range_size** باید صرفاً به بایت‌های درون نمونه ارجاع شده و نه هیچ بایت دیگری، اشاره کند. اگر بیش از یک گستره بایت جایگزین در یک گروه گستره بایت جایگزین باشد، این فیلد تنها برای اولین گستره بایت جایگزین وجود خواهد داشت چرا که اندازه گستره‌های بایت جایگزین موجود در یک گروه گستره بایت جایگزین یکی می‌باشد.

padding : آرایه بایت ممکن است که حاوی هر داده‌ای باشد و از آن برای افزایش اندازه سازنده جایگزین استفاده شود.

یادآوری- از آنجایی که این لایی‌گذاری رمزنگاری شده است می‌توان آن را برای مبهم کردن اندازه واقعی سازنده جایگزین به کار برد.

۸-۳-۴ رمزنگاری

همان‌طور که در زیربند ۵-۳ تعریف شد، سازنده‌های جایگزین همواره رمزنگاری شده هستند، و در زیربند ۸-۲-۳ ذکر شد، طرح حفاظت در **VariantMetaDataSampleEntry()** نشانک‌دهی می‌شود. باید از یکی از حالت‌های رمزنگاری CENC به شرح زیر برای رمزنگاری سازنده‌های جایگزین استفاده گردد:

- رمزنگاری نمونه کامل AES-CTR: با یک مقدار کد چهار نویسه‌ایی '**cvar**' و یک مقدار **scheme_version** برابر با 0x00010000 (نسخه اصلی 1 و نسخه فرعی 0) در **VariantMetaDataSampleEntry()** نشانک‌دهی می‌شود، به زیربند ۸-۲- ۳ مراجعه شود.
- رمزنگاری نمونه کامل AES-CBC-128: با استفاده از مقدار کد چهار نویسه‌ای مربوط به فیلد **scheme_type** و برابر با '**cval**' و مقدار فیلد **scheme_version** برابر با 0x00010000 (نسخه اصلی 1 و نسخه فرعی 0) در **VariantMetaDataSampleEntry()** نشانک‌دهی می‌شود، به زیربند ۸-۲- ۳ مراجعه شود.

همان‌طور که در زیربند ۷-۳ تعریف شد، جایگزین‌های نمونه که از گستره‌های بایت جایگزین تعیین شده در یک سازنده جایگزین همگذاری شده‌اند، برحسب نشانک‌دهی طرح مربوط به شیار رسانه وابسته رمزنگاری می‌شوند. مطابق با زیربند ۸-۲-۳ ، این طرح در **VariantMetaDataSampleEntry()** نیز نشانک‌دهی شده است.

همان‌طور که در زیربند ۷-۳ تعریف شد، بایت‌هایی که توسط یک گستره بایت جایگزین مورد اشاره قرار می‌گیرند، ممکن است توسط یک «کلید گستره بایت جایگزین» رمزنگاری مضاعف شده باشند. در زیربند ۸-۲-۳، طرح رمزنگاری مضاعف در **VariantMetaDataSampleEntry()** نشانک‌دهی شده است.

برای رمزنگاریِ داده بایت در یک شیار جایگزین باید یکی از حالت‌های رمزنگاری CENC زیر مورد استفاده قرار گیرد:

- رمزنگاری نمونه کامل AES-CTR: با یک مقدار کد چهار نویسه‌ای '**cvar**' و یک مقدار **scheme_version** برابر با 0x00010000 (نسخه اصلی 1 و نسخه فرعی 0) در **VariantMetaDataSampleEntry()** نشانک دهی می‌شود، به زیربند ۸-۲- ۳ مراجعه شود.
- رمزنگاری نمونه کامل AES-CBC-128: با استفاده از مقدار کد چهار نویسه‌ای مربوط به فیلد **scheme_type** و برابر با '**cva1**' و مقدار فیلد **scheme_version** برابر با 0x00010000 (نسخه اصلی 1 و نسخه فرعی 0) در **VariantMetaDataSampleEntry()** نشانک‌دهی می‌شود، به زیربند ۸-۲- ۳ مراجعه شود.

بایت‌هایی که توسط یک گستره بایت جایگزین مورد اشاره قرار می‌گیرند، باید به منزله یک نمونه منفرد و برای اهداف اِعمال یکی از این حالت‌های رمزنگاری CENC تلقی شوند.

۸-۳-۵ وابستگی

نمونه‌ها به شرح زیر به هم وابسته می‌شوند:

الف- نمونه‌ای در یک شیار رسانه باید با یک نمونه در شیار جایگزینی که توسط شیار رسانه به آن اشاره شده است وابسته گردد در صورتی که نمونه‌ها زمان-موازی باشند.

ب- یک نمونه در یک شیار جایگزین باید با نمونه ای در دیگر شیار جایگزین دیگر که توسط شیار جایگزین به آن اشاره شده، وابسته گردد در صورتی که نمونه ها زمان-موازی باشند.

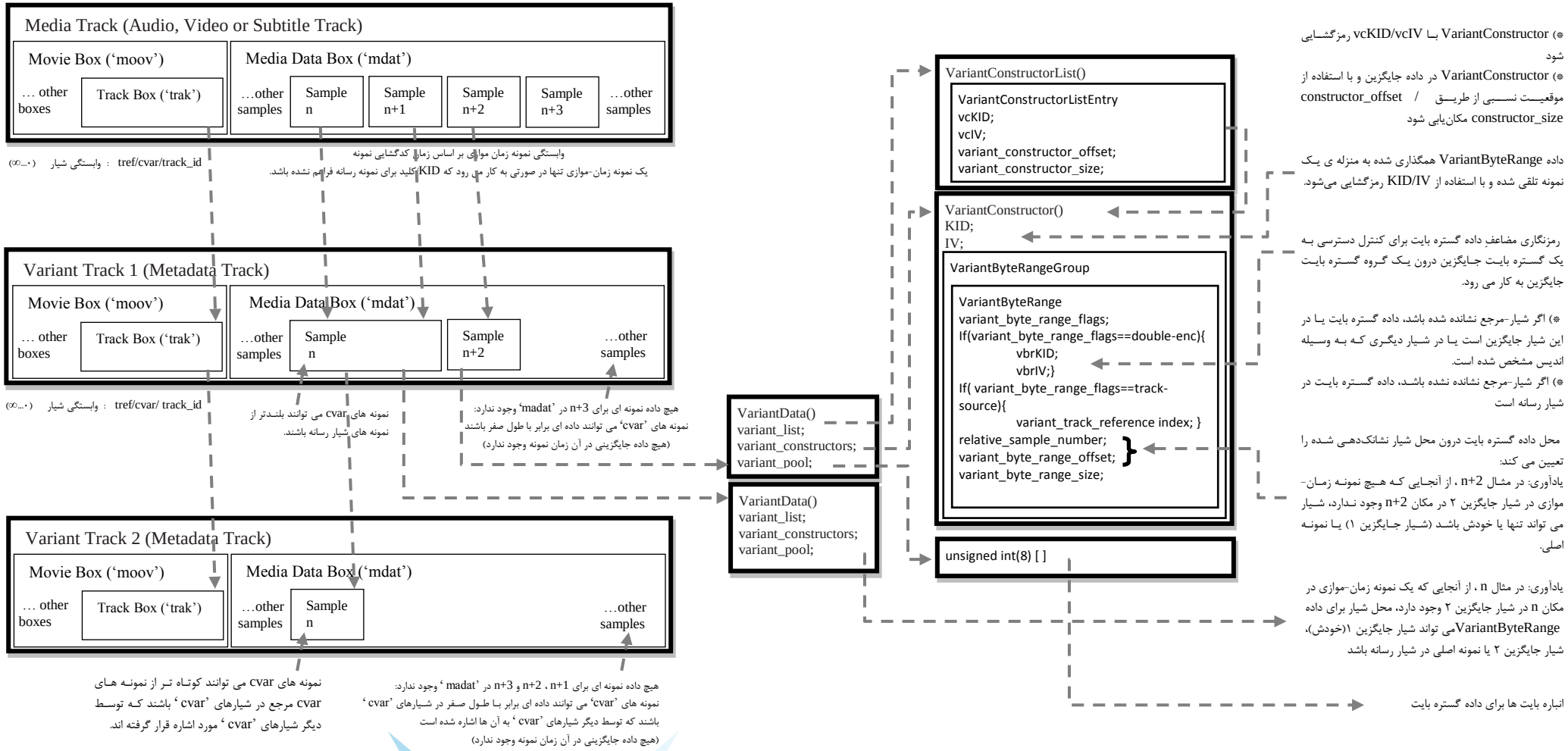
پ- نمونه‌ها به شرح زیر زمان-موازی در نظر گرفته می‌شوند: اگر To زمان کدگشایی نمونه در شیار اصلی باشد، آنگاه نمونه زمان-موازی در یک شیار مورد اشاره، همان نمونه‌ای در آن شیار است که زمان کدگشایی برابر با Tv و مدت[1] D دارد به طوری که Tv<=To<(Tv+D) .

یادآوری۱ – در زمان کدگشایی رسانه، پیش از هر نوع ملاحظات مربوط به فهرست‌های ویرایش[2] یا دورافت ترکیب[3]، نمونه رخ می‌دهد.

1- Duration
2- Edit lists
3- Composition offset

یادآوری۲- در صورتی که هیچ داده جایگزینی در یک زمانِ نمونه بخصوص برای فراهم کردن وجود نداشته باشد، آن نمونه در شیار جایگزین می‌تواند اندازه داده‌ای برابر با صفر داشته باشد.

مثالی از شیار رسانه و ارجاع شیار جایگزین در شکل ۳ نشان داده شده است.



شکل ۳ – شیار رسانه و شیار جایگزین ارجاع دهنده

۹ مدل پردازنده جایگزین و مثال (آگاهی‌دهنده)

۹-۱ مدل پردازنده جایگزین

از نونمایی کردن یک نمونه انتظار می‌رود که رفتار قابل مشاهده تعریف شده توسط مدل زیر را برآورده کند:

الف- منبع داده برای هر نمونه به شرح زیر ارزیابی می‌شود:

۱- اگر کدگشا به نمونه موجود در شیار رسانه دسترسی داشته باشد، کدگشا برای نونمایی کردن نمونه نظیر زیربند ۵-۲ پیش می‌رود.

۲- اگر کدگشا به نمونه موجود در شیار رسانه دسترسی نداشته باشد، پردازنده جایگزین همان طور که در زیربند ۵-۲ مشخص شد، تعیین می‌کند که کدام سازنده جایگزین، منبع داده برای نمونه است. پردازنده جایگزین یک سازنده جایگزین قابل دسترسی را به شرح زیر جستجو می‌کند:

i. پردازنده جایگزین هر شیار جایگزین اشاره‌شده توسط شیار رسانه را به ترتیب تعریف مرجع جستجو خواهد کرد، به عنوان مثال به ترتیب مرجع های شیار در جعبه مرجع شیار (‘**tref**’). برای اطلاعات بیشتر به زیربند ۸-۲-۲ مراجعه شود.

ii. در هر شیار جایگزین جستجو شده، پردازنده جایگزین مشخص میکند که آیا داده جایگزین برای نمونه زمان-موازی در شیار جایگزین وجود دارد یا نه. اگر داده جایگزین وجود داشته باشد، پردازنده جایگزین در نمونه زمان-موازی موجود در شیار جایگزین دنبال **VariantConstructorList()** می‌گردد.

iii. پردازنده جایگزین به جستجو ادامه خواهد داد تا زمانی که یک KID سازنده جایگزین (‘**vcKID**’) موجود در یک **VariantConstructorList()** را که با یک کلید/ شناسانه‌کلید مطابق است و پردازنده جایگزین به آن دسترسی دارد پیدا کند.

ب- با استفاده از کلید سازنده جایگزین و بردار مقداردهی اولیه که برای سازنده جایگزین توسط پردازنده جایگزین انتخاب و در **VariantConstructorList()** تعریف شده اند، پردازنده جایگزین ساختار **VariantConstructor()** تعریف شده در زیربند ۸-۳-۳ را رمزگشایی می‌کند.

پ- پردازنده جایگزین به صورت پی‌درپی هر گستره بایت جایگزین در دنباله‌ای از گستره‌های بایت جایگزین را که در سازنده جایگزینِ رمزگشایی شده، تعریف شده‌اند، پردازش می‌کند و به شرح زیر داده رسانه جایگزین را برای نمونه همگذاری می‌کند:

۱- اگرگستره بایت جایگزین مطابق تعریف **variant_byte_range_flgs** در زیربند ۸-۳-۳-۲ نشانک‌دهی شده باشد که رمزنگاری نشده باشد، گستره بایت مستقیماً در همگذاری جایگزین قرار داده می‌شود و به عنوان رمزنگاری نشده شناسایی می‌شود.

۲- اگر گستره بایت جایگزین مطابق تعریف **variant_byte_range_flgs** در زیربند ۸-۳-۳-۲ نشانک‌دهی شده باشد که رمزنگاری شده باشد:

i. اگر داده گستره بایت جایگزین با کلید رسانه براساس تعریف **variant_byte_range_flgs** در زیربند ۸-۳-۳-۲ به صورت رمزنگاری شده ی منفرد نشانک دهی شود، مستقیماً در همگذاری جایگزین قرار داده می شود و به صورت رمزنگاری شده شناسایی می گردد.

ii. اگر رسانه گستره بایت جایگزین مطابق تعریف **variant_byte_range_flgs** در زیربند ۲-۳-۳-۸ به صورت رمزنگاری مضاعف نشانک‌دهی شده باشد:

I. اگر KID گستره بایت جایگزین(‘**vbrKID**’) که توسط گستره بایت جایگزین تعریف شده در دسترس پردازنده جایگزین باشد، داده گستره بایت جایگزین که توسط گستره بایت جایگزین بدان اشاره شده، با استفاده از کلید گستره بایت جایگزین اشاره شده توسط KID گستره بایت جایگزین(‘**vbrKID**’) و نیز بردار مقداردهی اولیه اشاره شده توسط IV گستره بایت جایگزین(‘**vbrIV**’) رمزگشایی می شود. این عملیات منجر به داده رمزنگاری منفرد می شود که در همگذاری نمونه قرار داده شده و به صورت رمزنگاری شده شناسایی می شود.

II. اگر KID گستره بایت جایگزین(‘**vbrKID**’) که توسط گستره بایت جایگزین تعریف شده، در دسترس پردازنده جایگزین نباشد، از گستره بایت جایگزین پرش[1] می شود.

ت- داده رسانه جایگزین همگذاری شده با استفاده از کلید رسانه توسط فراداده جایگزین تعریف شده (همان طور که توسط فیلد KID در فراداده جایگزین به آن رجوع و در زیربند ۸-۳-۲-۳ تعریف شده است) طبق CENC رمزگشایی می‌شود.

۹-۲ مثال

فرض کنید یک سازنده جایگزین از سه گروه گستره بایت تشکیل شده است:

- اولین گروه گستره بایت دارای یک گستره بایت جایگزین با نام S1 می باشد که رمزنگاری نشده است.
- دومین گروه گستره بایت دارای یک گستره بایت جایگزین با نام S2 می باشد که رمزنگاری شده است.
- سومین گروه گستره بایت دارای دو گستره بایت جایگزین با نام های S3 و S4 می‌باشد که هر کدام رمزنگاری شده می باشند.

در زمان رمزنگاری:

- داده جایگزین نمونه وابسته با گستره بایت جایگزین با نام S1 ، رمزنگاری نمی‌شود و حاصل آن داده جایگزین نمونه رمزنگاری نشده با نام D1 می شود.

1 _ Skip

- داده جایگزین نمونه وابسته با گستره بایت جایگزین{S2, S3,S4} هر کدام با کلیدهای رسانه K1 (KID KID1) رمزنگاری شده اند، حاصل آن ها داده جایگزین نمونه رمزنگاری شده با نام {D2*, D3*, D4*} می شود.
- داده جایگزین نمونه رمزنگاری شده D3 بعداً توسط کلید گستره بایت جایگزین با نام K3 (KID KID3) رمزنگاری می‌شود و داده جایگزین نمونه رمزنگاری شده D4 نیز توسط کلید گستره بایت جایگزین با نام K4 (KID KID4) رمزنگاری می‌شود، حاصل آن ها داده رسانه رمزنگاری شده مضاعف با نام D3** و D4** می‌شود.

سازنده جایگزین حاصل چهار گستره بایت جایگزین خواهد داشت و به صورت [| S1 | S2 | S3 S4] سازمان می‌یابد که در آن نماد "|" به شروع یک گروه گستره بایت اشاره می‌کند. داده رسانه نهفته[1] به صورت {D1, D2*, D3**, D4**} ذخیره می‌شود.

اگر پردازنده جایگزین صرفاً به KID1 و KID3 دسترسی داشته باشد، اعمال زیر را انجام می‌دهد:

الف- S1 را پردازش می‌کند و نهایتاً بعد از اینکه رمزنگاری نبودنش محقق شد، D1 را به همگذاری نمونه اضافه می‌کند و آن را به عنوان رمزنگاری نشده شناسایی می‌کند (مطابق با مورد ۱ بخش پ زیربند ۹-۱).

ب- S2 را پردازش می‌کند، KID1 را تطبیق می‌دهد و نهایتاً D2* به همگذاری نمونه اضافه می‌کند و آن را به عنوان رمزنگاری شده شناسایی می‌کند (مطابق با مورد ۲-i بخش پ زیربند ۹-۱).

پ- S3 را پردازش می‌کند، KID3 را تطبیق می‌دهد و نهایتاً D3** را با استفاده از K3 رمزگشایی می‌کند، سپس D3* حاصل را به همگذاری نمونه اضافه می‌کند و آن را به عنوان رمزنگاری شده شناسایی می‌کند (مطابق با مورد ۲-I-ii بخش پ زیربند ۹-۱).

ت- S4 را پردازش می‌کند، KID4 را تشخیص نمی‌دهد و نهایتاً از D4** پرش می‌کند (مطابق با مورد ۲-II-ii بخش پ زیربند ۹-۱).

ث- نمونه همگذاری [D1 D2* D3*] را با پرش از D1 و استفاده از کلید رسانه K1 برای رمزگشایی D2* و D3* را رمزگشایی می‌کند، جایگزین نمونه رمزنگاری نشده را نتیجه می‌دهد [M1 M2 M3] (مطابق بخش ت زیربند ۹-۱).

1- Underlying media data