استاندارد ملی ایران

۱۱۹۴۷-۷

چاپ اول

اسفند ۱۳۹۲

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

INSO
11947-7
1st. Edition
Feb.2014

فن‌آوری اطلاعات – فن‌آوری‌های سامانه MPEG– قسمت ۷: رمزگذاری عمومی در فایل‌های قالب فایل رسانه‌ای بر پایه سازمان بین المللی استانداردسازی (ISO)

Information technology - MPEG systems technologies- Part 7: Common encryption in ISO base media file format files

ICS:35.040

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5]در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی یکاها ، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

" فن‌آوری اطلاعات – فن‌آوری‌های سامانه MPEG-

قسمت ۷: رمزگذاری عمومی در فایل‌های قالب فایل رسانه‌ای بر پایه سازمان بین‌المللی استانداردسازی (ISO)"

رئیس:	**سمت و/یا نمایندگی**
بدلی افشرد، بابک (فوق لیسانس مهندسی کامپیوتر)	اداره کل استاندارد و تحقیقات صنعتی آذربایجان‌شرقی

دبیر:

خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا

اعضاء: (اسامی به ترتیب حروف الفبا)

اصل‌زاد، محمدعلی (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
اکبری سروری, شبنم (لیسانس مهندسی کامپیوتر)	شرکت پگاسوس
بدلی افشرد، محمدرضا (فوق لیسانس مهندسی برق)	نیروگاه حرارتی تبریز
تفسیری, حامد (لیسانس مهندسی کامپیوتر)	شرکت پگاسوس
خوشقدم، سهیلا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکا پژوه
عظیمی حسینی، سارا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه

فهرست مندرجات

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات – فن‌آوری‌های سامانه MPEG- قسمت ۷: رمزگـذاری عمـومی در فایـل‌هـای قالب فایل رسانه‌ای بر پایه سازمان بین المللی استانداردسازی (ISO)" که پیش‌نویس آن در کمیسـیون‌هـای مربوط توسط شرکت ریزفناوران آرکا پژوه تهیه و تدوین شده و در دویست و هفتاد و هفتمین اجلاس کمیته ملی استاندارد رایانه تاریخ ۹۱/۱۲/۲۴ مورد تصویب قرارگرفته‌است، اینک به استناد بنـد یـک مـاده ۳ قـانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوّب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملـی ایـران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحوّلات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علـوم و خـدمات، استاندارد های ملی ایران در موقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه‌شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیر است :

ISO/IEC 23001-7:2012, Information technology - MPEG systems technologies
Part 7: Common encryption in ISO base media file format files

فن‌آوری اطلاعات – فن‌آوری‌های سامانه MPEG–
قسمت ۷: رمزگذاری عمومی در فایل‌های قالب فایل رسانه‌ای بر پایه سازمان بین‌المللی استانداردسازی (ISO)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین قالب عمومی رمزگذاری برای استفاده در هر قالب فایل بر اساس استاندارد ISO/IEC 14496-12، قالب فایل رسانه مبنی بر سازمان بین‌المللی استانداردسازی (ISO) است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی به آن‌ها ارجاع داده شده است. بدین‌ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شود.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن مورد نظر است.

استفاده از مراجع زیر برای کاربرد استاندارد الزامی است:

۲-۱ مجموعه استانداردهای ملی ایران-ایزو شماره ۱۴۴۹۶: سال ۱۳۸۸، فناوری اطلاعات- کدگذاری شی‌های صوتی-تصویری قسمت ۱۰: کدگذاری ویدیویی پیشرفته

۲-۲ مجموعه استانداردهای ملی ایران-ایزو شماره ۱۴۴۹۶: سال ۱۳۸۹، فناوری اطلاعات کدگذاری شی‌های صوتی-تصویری قسمت ۱۲: قالب فایل رسانه‌ای برپایه سازمان بین المللی استانداردسازی (ISO)

۲-۳ مجموعه استانداردهای ملی ایران-ایزو شماره ۱۴۴۹۶: سال ۱۳۸۹، فناوری اطلاعات کدگذاری شی‌های صوتی-تصویری قسمت ۱۵: قالب فایل کدگذاری ویدئویی پیشرفته (AVC)

2-4 Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS-197, http://www.nist.gov/

2-5 Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A, http://www.nist.gov/

۳ اصطلاحات و تعاریف و اختصارات

۳-۱ تعاریف و اصطلاحات

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱-۱

فایل رسانه مبنی بر سازمان بین‌المللی استانداردسازی (ISO)[1]

نام یک فایل منطبق با قالب فایل شرح داده شده در استاندارد ایران-ایزو شماره ۱۲-۱۴۴۹۶ که در آن فن‌آوری‌های این استاندارد می‌توانند استفاده شوند.

یادآوری- به بند ۳-۱-۸ استاندارد ایران-ایزو ۱۲-۱۴۴۹۶ مراجعه کنید.

۳-۱-۲

یادآوری- گروه افزاره رسانه‌ای از دو بخش تشکیل شده است: گروه افزاره خدمات شاخص محتوا و گروه افزاره چندپخشی صوتی/ تصویری.

۳-۲ اختصارات

AES Advanced Encryption Standard

استاندارد رمزگذاری پیشرفته مشخص شده در انتشار ۱۹۷ استانداردهای فدرال پردازش اطلاعات

AES-CTR AES Counter Mode

حالت شمارنده AES مشخص شده در نظریه روش‌های عمل رمز نگاری بلوک،NIST، انتشار 800-38A ویژه NIST

AVC Advanced Video Compression

فشرده سازی پیشرفته ویدیویی مشخص شده در استاندارد ایران-ایزو ۱۰-۱۴۴۹۶

ISOAVC An ISO Base Media File containing AVC media tracks

NAL Network Abstraction Layer لایه انتزاعی شبکه مشخص شده در استاندارد ایران-ایزو ۱۰-۱۴۴۹۶

۴ علامت‌گذاری طرح

علامت‌گذاری طرح باید مطابق با استاندارد ایران-ایزو ۱۲-۱۴۴۹۶باشد. همان‌طور که در استاندارد ایران-ایزو ۱۰-۱۴۴۹۶تعریف شده، رکورد نمونه تبدیل می‌شود و یک طرح حفاظت جعبه اطلاعات[2] ('sinf') به رکورد نمونه استاندارد در جعبه شرح نمونه اضافه می‌شود تا نشان دهد که جریان رمزگذاری شده است. طرح حفاظت جعبه اطلاعات باید شامل یک جعبه نوع طرح ('schm') باشد تا طرح قابل شناسایی باشد. جعبه نوع طرح، محدودیت‌های اضافی زیر را دارد:

در فیلد نوع-طرح، مقدار 'cenc' قرار داده می‌شود (رمزگذاری عمومی)

در فیلد نسخه طرح، مقدار 0x00010000 قرار داده می‌شود (نسخه اصلی ۱، نسخه فرعی ۰)

طرح حفاظت جعبه اطلاعات باید شامل جعبه اطلاعات طرح ('schi') باشد. جعبه اطلاعات طرح دارای محدودیت اضافی زیر است.

- طرح جعبه اطلاعات باید شامل یک جعبه رمزگذاری شیار ('tenc') باشد که بیان کننده پارامترهای رمزگذاری برای track است.

1- ISO Base Media File

2- Protection Scheme Information Box

۵ بررسی رمزگذاری فرا داده

رمزگذاری فرا داده تعریف شده توسط طرح رمزگذاری عمومی 'cenc' می‌تواند به‌صورت زیر گروه‌بندی شود:

الف- داده خاص سامانه حفاظت شده- این داده برای طرح رمزگذاری عمومی 'cenc' مبهم است و برای سامانه‌های حفاظت شده، مکانی می‌دهد تا داده خود را با استفاده از مکانیزم عمومی ذخیره کنند. این داده درون متغیر ProtectionSystemSpecificHeaderBox که در بند ۸-۱ شرح داده شده‌است، موجود است.

ب- اطلاعات رمزگذاری عمومی برای یک شیار[1] رسانه- شامل مقادیر پیش فرض برای شناسه کلیدی (KID)[2]، اندازه بردار اولیه و پرچم رمزگذاری می‌باشد. این داده در جعبه رمزگذاری شیار شرح داده شده در بند ۸-۲ موجود است.

پ- اطلاعات رمزگذاری عمومی برای گروه‌هایی از نمونه‌های رسانه- شامل بازنویسی پیش‌فرض‌های سطح شیار برای شناسه کلید، اندازه بردار اولیه و پرچم رمزگذاری می‌باشد. این امر به گروه‌های نمونه‌های داخل شیار اجازه می‌دهد تا از کلیدهای متفاوت، ترکیبی از محتوای واضح و رمزگذاری شده و غیره استفاده کنند. این داده در تابع ((SampleGroupDescriptionBox('sgpd موجود است که توسط تابع ((SampleToGroupBox('sbgp ارجاع داده می‌شود. برای جزئیات بیشتر، بند ۶ را مشاهده کنید.

ت- اطلاعات رمزگذاری برای نمونه‌های خاص رسانه- که شامل بردارهایی با مقادیر اولیه و در صورت لزوم داده رمزگذاری نمونه فرعی می‌باشد. این داده، اطلاعات کمکی نمونه است که با استفاده از توابع SampleAuxiliaryInformationSizesBox (‘saiz’) و SampleAuxiliaryInformationOffsetsBox ('saio') مراجعه شده است. برای جزئیات بیشتر بند ۷ را مشاهده کنید.

۶ پارامترهای رمزگذاری به اشتراک گذاشته شده توسط گروه‌های نمونه‌ها

هر نمونه در یک شیار محافظت شده، باید با یک پرچم IsEncrypted، IV-Size و KID همراه باشد. این امر می‌تواند به‌وسیله الف) متکی شدن بر مقادیر پیش فرض در TrackEncryptionBox (جعبه رمزگذاری شیار) (بند ۸-۲ را مشاهده کنید) یا ب) تعیین پارامترها توسط گروه نمونه، یا پ) استفاده از ترکیب این دو روش، انجام شود.

هنگام تعیین پارامترها توسط گروه نمونه، تابع (SampleToGroupBox) در جدول نمونه یا قطعه شیار مشخص می‌کند که کدام نمونه‌ها، کدام شرح گروه از تابع SampleGroupDescriptionBox را استفاده می‌کنند. قالب شرح گروه نمونه مبتنی بر نوع کنترل کننده برای شیار است.

شیارهای با نوع کنترل کننده 'vide' باید از ساختار شرح گروه نمونه CenceSampleEncryptionInformationVideoGroupEntry استفاده کنند که دارای گرامر زیر است:

```
aligned(8) class CencSampleEncryptionInformationVideoGroupEntry
      extends VisualSampleGroupEntry( ‘seig’ )
{
     unsigned int(24) IsEncrypted;
     unsigned int(8) IV_size;
```

1- Track

2- Key identifier

```
    unsigned int(8)[16] KID;
}
```

به‌طور مشابه شیارهای با نوع کنترل کننده 'soun' باید از ساختار شرح گروه نمونه CencSampleEncryptionInformationAudioGroupEntry استفاده کنند که دارای گرامر زیر است:

```
aligned(8) class CencSampleEncryptionInformationAudioGroupEntry
           extends AudioSampleGroupEntry( 'seig' )
{
           unsigned int(24) IsEncrypted;
           unsigned int(8) IV_size;
           unsigned int(8)[16] KID;
}
```

یادآوری- در صورتی‌که محافظت از انواع دیگر رسانه مورد نیاز باشد، باید گروه‌هایی با ساختار یکسان تعریف شوند.

این ساختارها به‌صورت زیر از معنای مشترکی برای فیلدهای خود استفاده می‌کنند:

IsEncrypted، پرچمی است که حالت رمزگذاری نمونه‌ها در گروه نمونه را نشان می‌دهد. برای جزئیات بیشتر فیلد IsEncrypted در بند ۹-۲ را مشاهده کنید.

فیلد IV_size، برای نمونه‌های در گروه نمونه، اندازه بردار اولیه بر حسب بایت است. برای جزئیات بیشتر فیلد IV_size در بند ۹-۲ را مشاهده کنید.

فیلد KID، شناسه کلید استفاده شده برای نمونه‌ها در گروه نمونه است. برای جزئیات بیشتر فیلد KID در بند ۹-۲ را مشاهده کنید.

به منظور تسهیل اضافه کردن فیلدهای اختیاری بعدی، سرویس گیرنده‌ها باید بایت‌های اضافی بعد از فیلدهای تعریف شده در ساختارهای مدخل گروه CencSampleEncryption را نادیده بگیرند.

۷ اطلاعات کمکی نمونه رمزگذاری عمومی

هر نمونه رمزگذاری شده در یک شیار محافظت شده باید یک بردار اولیه همراه با آن داشته باشد. به‌علاوه هر نمونه رمزگذاری شده در شیارهای ویدیو AVC محافظت شده باید مطابق با استانداردهای ایران-ایزو ۱۰-۱۴۴۹۶ و ۱۵-۱۴۴۹۶ باشند و باید طرح رمزگذاری نمونه فرعی مشخص شده در بند ۹-۶-۲ که نیازمند داده رمزگذاری نمونه فرعی است را استفاده کنند. هم بردارهای اولیه و هم داده رمزگذاری نمونه فرعی به عنوان اطلاعات کمکی با aux_info_type برابر 'cenc' و aux_info_type_parameter برابر صفر، ارائه می‌شوند. برای شیارهای محافظت شده با استفاده از طرح 'cenc'، مقدار پیش فرض برای aux_info_type برابر'cenc' است و مقدار پیش فرض برای aux_info_type_parameter برابر صفر است بنابراین محتوا می‌تواند با حذف این فیلدهای اختیاری ایجاد شود. ذخیره سازی اطلاعات کمکی نمونه برای نمونه‌های با این نوع باید به این صورت باشد:

```
aligned(8) class CencSampleAuxiliaryDataFormat
{
        unsigned int(IV_size*8) InitializationVector;
        if  ( sample_info_size > IV_size )
         {
             unsigned int(16) subsample_count;
             {
```

```
            unsigned int(16) BytesOfClearData;
             {
                 unsigned int(32) BytesOfEncryptedData;
                 unsigned int(32) BytesOfEncryptedData;
              }  [ subsample_count ]
        }
    }
```

که در آن:

InitializationVector مقدار اولیه بردار برای نمونه است. برای جزئیات بیشتر InitializationVector را در بند ۹-۲ مشاهده کنید.

Subsample_count، تعداد نمونه‌های فرعی برای این نمونه است. برای جزئیات بیشتر subsample_count در بند ۹-۲ را مشاهده کنید.

BytesOfClearData، تعداد بایت‌های داده واضح در این نمونه فرعی است. برای جزئیات بیشتر ByteOfClearData در بند ۹-۲ را مشاهده کنید.

BytesOfEncryptedData، تعداد بایت‌های داده رمزگذاری شده در این نمونه فرعی است. برای جزئیات بیشتر BytesOfEncryptedData در بند ۹-۲ را مشاهده کنید.

اگر رمزگذاری نمونه فرعی استفاده نشود، (Sample_info_size برابر IV-size است) در آن‌صورت کل نمونه رمزگذاری می‌شود. (برای جزئیات بیشتر، بند ۹-۵ را مشاهده کنید). در این حالت تمامی اطلاعات کمکی اندازه یکسانی خواهند داشت و از این رو default_sample_info_size از SampleAuxiliaryInformationSizesbox برابر با IV_size از بردارهای مقدار دهی اولیه خواهد بود.

توجه داشته باشید، حتی اگر رمزگذاری نمونه فرعی استفاده شود، ممکن است اندازه اطلاعات کمکی نمونه برای تمامی نمونه‌ها یکسان باشد (در صورتی‌که همه نمونه‌ها تعداد نمونه‌های فرعی یکسانی داشته باشند) و default_sample_info_size استفاده شود.

۸ تعاریف جعبه

۸-۱ جعبه سرآیند خاص سامانه حفاظت شده

۸-۱-۱ تعریف

نوع جعبه: 'pssh'

محتویات: فیلم ('moov') یا قطعه فیلم ('moof')

الزامی: خیر

مقدار: صفر یا بیشتر

این جعبه حاوی اطلاعات مورد نیاز توسط یک سامانه حفاظت محتوا به‌منظور پخش محتوا است. قالب داده به وسیله سامانه مشخص شده توسط 'pssh' پارامتر SystemID مشخص شده است و برای اهداف این مشخصه، مبهم در نظر گرفته شده است.

داده محصور شده در فیلد داده می‌تواند توسط سامانه حفاظت محتوای شناسایی شده، خوانده شود تا رمزگشایی کلید و رمزگشایی داده رسانه امکان‌پذیر باشد. برای سامانه‌های مبنی بر مجوز/حقوق، اطلاعات سرآیند می‌تواند شامل داده‌هایی مانند URL سرویس دهنده‌های مجوز یا صادرکنندگان حقوق استفاده‌شده، مجوزها/ حقوق ادغام شده، و/یا دیگر سامانه حفاظت فراداده خاص باشد.

یک فایل واحد ممکن است توسط کلیدهای چندگانه و سامانه‌های مدیریت حقوق دیجیتال (DRM) با دارا بودن جعبه سرآیند خاص برای هر سامانه پشتیبانی شده، قابل پخش باشد. خواننده‌هایی[1] که چنین ارائه-هایی را پردازش می‌کنند، باید فیلد SystemID در این جعبه را با شناسه یا شناسه‌های SystemID سامانه یا سامانه‌های DRMای که پشتیبانی می‌کنند، تطبیق دهند و جعبه‌های سرآیند خاص سامانه حفاظت مطابق را برای بازیابی اطلاعات خاص سامانه حفاظتی که توسط آن سامانه DRM تفسیر یا ایجاد شده، انتخاب کنند.

۸-۱-۲ گرامر[2]

```
aligned(8) class ProtectionSystemSpecificHeaderBox extends
FullBox('pssh', version=0, flags=0)
{
            unsigned int(8)[16]                 SystemID;
            unsigned int(32)                     DataSize;
            unsigned int(8)[DataSize]       Data;
 }
```

۸-۱-۳ معانی

SystemID یک شناسه منحصربه‌فرد کاربر (UUID)[3] را مشخص می‌کند که به‌صورت منحصربه‌فرد سامانه حفاظت محتوایی که این سرآیند متعلق به آن است را شناسایی می‌کند.

متغیر DataSize، اندازه عضو داده را بر حسب بایت مشخص می‌کند.

متغیر Data، داده خاص سامانه حفاظت محتوا را نگه می‌دارد.

۸-۲ جعبه رمزگذاری شیار

۸-۲-۱ تعریف

نوع جعبه: 'tenc'

محتویات: جعبه اطلاعات طرح ('schi')

الزامی: خیر (برای شیارهای رمزگذاری شده، بله)

مقدار: صفر یا یک

TrackEncryptionBox شامل مقادیر پیش فرض برای پرچم IsEncrypted، IV_size و KID برای کل شیار است. این مقادیر به‌عنوان پارامترهای رمزگذاری برای نمونه‌های این شیار استفاده می‌شوند، مگر این‌که توسط شرح گروه نمونه مربوط، به گروهی از نمونه‌ها بازنویسی شوند. برای فایل‌های با تنها یک کلید در هر

1- readers
3- syntax
4- Unique User Identifier

شیار، این جعبه اجازه می‌دهد که پارامترهای پایه رمزگذاری بجای این‌که در هر نمونه تکرار شوند در هر شیار یک‌بار تعیین شوند.

۸-۲-۲ گرامر

```
aligned(8) class TrackEncryptionBox extends FullBox('tenc',
version=0, flags=0)
{
   unsigned int(24)            default_IsEncrypted;
   unsigned int(8)             default_IV_size;
   unsigned int(8)[16]         default_KID;
}
```

۸-۲-۳ معانی[1]

default_IsEncrypted، پرچم رمزگذاری است که حالت رمزگذاری پیش فرض نمونه‌ها در شیار را نشان می‌دهد. برای جزئیات بیشتر، IsEncrypted در بند ۹-۲ را مشاهده کنید. default_IV_size، اندازه پیش فرض بردار اولیه بر حسب بایت می‌باشد. برای جزئیات بیشتر، IV_size در بند ۹-۲را مشاهده کنید.
default_KID، شناسه پیش فرض کلید استفاده شده برای نمونه‌های در این شیار می‌باشد. برای جزئیات بیشتر، KID در بند ۹-۲ را مشاهده کنید.

۹ رمزگذاری داده رسانه

۹-۱ طرح‌های رمزگذاری

داده رسانه با استفاده از طرح حفاظت 'cenc' باید استاندارد رمزگذاری پیشرفته، انتشار ۱۹۷ استانداردهای فدرال پردازش اطلاعات را استفاده کند. FIPS-197 توسط موسسه ملی استانداردها و فناوری (NIST) با استفاده از کلیدهای ۱۲۸ بیتی در روش شمارنده (AES_CTR)، همان‌طور که در نظریه روش‌های عمل رمزنگاری بلوک، NIST، انتشار NIST 800-38A، مشخص شده، انتشار شده است. طرح، دو قالب اصلی برای رمزگذاری جریان تعریف می‌کند، رمزگذاری نمونه کامل و رمزگذاری نمونه فرعی. در رمزگذاری نمونه کامل، کل نمونه به‌عنوان یک واحد رمزگذاری منفرد، رمزگذاری می‌شود، در حالی‌که در رمزگذاری نمونه فرعی، نمونه به واحدهای کوچکتری شکسته می‌شود که هر یک شامل یک ناحیه واضح و یک ناحیه رمزگذاری شده هستند. شیارهای ویدیو AVC رمزگذاری شده باید از طرح رمزگذاری نمونه فرعی مشخص شده در بند ۹-۶-۲ پیروی کنند که آن یک طرح رمزگذاری مبنی بر واحد NAL تعریف می‌کند تا دسترسی به واحدهای NAL و سرآیندهای واحد NAL رمزگذاری نشده در یک جریان AVC رمزگذاری شده را اجازه دهد. تمامی انواع دیگر شیارها باید از طرح مشخص شده در بند ۹-۵ که یک طرح ساده رمزگذاری مبنی بر نمونه تعریف می‌کند، پیروی کنند.

۹-۲ معانی فیلد

1-Semantics

در گروه‌های نمونه و اطلاعات کمکی نمونه استفاده شده توسط طرح رمزگذاری عمومی، فیلدها دارای معانی زیر هستند:

شناسه IsEncrypted، شناسه حالت رمزگذاری نمونه‌ها در شیار یا گروه نمونه‌ها است. این پرچم می‌تواند مقادیر زیر را داشته باشد:

0x0: رمزگذاری نشده؛

0x1: رمزگذاری شده با استفاده از AES، ۱۲۸ بیتی در حالت CTR؛

0x000002-0xFFFFFF: رزرو شده؛

IV_size، اندازه فیلد بردار اولیه بر حسب بایت است. مقدار پشتیبانی شده عبارتند از:

مقدار ۰- اگر IsEncrypted، 0x0 باشد. (رمزگذاری نشده)

مقدار ۸- بردارهای اولیه ۶۴ بیتی را مشخص می‌کند.

مقدار ۱۶- بردارهای اولیه ۱۲۸ بیتی را مشخص می‌کند.

KID شناسه کلیدی است که به‌صورت منحصربه‌فرد کلید مورد نیاز برای رمز گشایی نمونه‌های مربوطه را شناسایی می‌کند. این، شناسایی چندین کلید رمزگذاری برای هر فایل یا شیار را اجازه می‌دهد. نمونه‌های رمزگذاری نشده در یک شیار رمزگذاری شده باید با داشتن یک IsEncrypted برابر 0x0، یک IV_size برابر 0x0 و یک مقدار KID برابر 0x0، شناسایی شوند.

InitializationVector، بردار اولیه (IV) مورد نیاز برای رمز گشایی یک نمونه را مشخص می‌کند. برای IsEncrypted با مقدار 0x0، هیچ بردار اولیه‌ای مورد نیاز نیست و باید اطلاعات کمکی اندازه صفر داشته باشند به عبارت دیگر وجود نداشته باشند.

برای پرچم IsEncrypted با مقدار 0x1 (AES-CTR)، اگر مقدار فیلد IV_size، ۱۶ باشد، در آن صورت Initialization Vector، کل مقدار IV ،۱۲۸بیتی استفاده شده به‌عنوان مقدار شمارنده را مشخص می‌کند. اگر فیلد IV_size دارای مقدار ۸ باشد، در آن صورت مقدارش به بایت‌های ۰ تا ۷ مقدار شمارنده کپی می‌شود و بایت‌های ۸ تا ۱۵ مقدار شمارنده صفر می‌شوند. زمانی‌که پرچم IsEncrypted برابر 0x1 است (AES-CTR)، فیلد IV_size نباید صفر باشد.

برای پرچم IsEncrypted با مقدار 0x1 (AES-CTR) باید مقادیر شمارنده برای هر KID منحصربه‌فرد باشد. اگر یک IV_size با مقدار ۸ استفاده شود، در آن صورت مقادیر InitializationVector برای یک KID داده شده، باید برای هر نمونه در تمامی شیارها منحصربه‌فرد باشند و طول نمونه‌ها باید کمتر از $۲^{۶۴}$ بلوک باشند. اگر یک IV_size با مقدار ۱۶ استفاده شود در آن صورت باید بردارهای اولیه تفاوت‌های عددی به اندازه کافی بزرگ داشته باشند تا از تکرار مقادیر شمارنده برای هر بلوک رمزگذاری شده با استفاده از KID یکسان، جلوگیری کنند.

Subsample-count، تعداد مدخل‌های رمزگذاری نمونه فرعی موجود برای این نمونه را مشخص می‌کند. در صورتی‌که این فیلد موجود باشد، باید بزرگتر از صفر باشد.

BytesOfClearData تعداد بایت‌های داده واضح در ابتدای این مدخل رمزگذاری شده نمونه فرعی را مشخص می‌کند.

یادآوری- اگر هیچ بایت واضحی برای این مدخل وجود نداشته باشد، این مقدار ممکن است صفر باشد.

BytesOfEncryptedData، تعداد بایت‌های رمزگذاری شده بعد از داده واضح را مشخص می‌کند.

یادآوری- اگر بایت رمزگذاری شده‌ای برای این مدخل وجود نداشته باشد، این مقدار می‌تواند صفر باشد.

مدخل‌های رمزگذاری نمونه فرعی هم در BytesOfClearData و هم در BytesOfEncryptedData نباید شامل یک مدخل با مقدار صفر باشد مگر این‌که طول نمونه، صفر بایت باشد. برای یک نمونه، طول کل BytesOfClearData و BytesOfEncryptedData باید برابر طول نمونه باشد. علاوه بر این، توصیه شده که مدخل‌های رمزگذاری نمونه فرعی تا حد امکان به‌صورت فشرده نشان داده شوند. به‌عنوان مثال بجای دو مدخل با {۰ رمزگذاری شده , ۱۵ واضح}،{۵۰۰ رمزگذاری شده,۱۷ واضح} از یک مدخل {۵۰۰رمزگذاری شده,۳۲ واضح} استفاده می‌شود.

۹-۳ بردارهای اولیه

مقادیر بردار اولیه(IV) برای هر نمونه، در اطلاعات کمکی نمونه مربوط به نمونه‌های رمزگذاری شده قرار گرفته‌اند. برای جزئیات این‌که بردارهای اولیه چگونه تشکیل شده و ذخیره می‌شوند، بند ۹-۲ را مشاهده کنید.

توصیه شده، کاربردهای اعمال کننده رمزگذاری، بردار اولیه برای اولین نمونه در شیار را به‌صورت تصادفی با استفاده از یک مولد عدد تصادفی به‌صورت پنهانی صوتی، تولید کنند.

- برای IV_sizeهای ۶۴ بیتی (۸ بایتی)، بردارهای اولیه برای نمونه‌های بعدی می‌توانند با افزایش بردار اولیه نمونه قبلی ایجاد شوند. با استفاده از یک مقدار شروع تصادفی، آنتروپی را به مقادیر بردار اولیه معرفی می‌کند و با افزایش برای هر نمونه پردازش شده، تضمین می‌کند که هر مقدار IV منحصربه‌فرد است. در صورتی‌که موقعیت شروع تصادفی نزدیک به مقدار حداکثر باشد، بردار اولیه ۶۴ بیتی باید اجازه داشته باشد تا از مقدار حداکثر (0xFFFFFFFFFFFFFFFF) به مقدار حداقل (0x0) نوسان کند.

- برای IV_sizeهای ۱۲۸ بیتی (۱۶ بایتی)، بردارهای اولیه برای نمونه‌های بعدی باید با اضافه کردن تعداد بلوک نمونه قبلی به بردار اولیه نمونه قبلی، ایجاد شوند. با استفاده از یک مقدار تصادفی شروع، بی‌نظمی را به مقادیر اولیه معرفی می‌کند و با افزایش توسط تعداد بلوک نمونه قبلی، تضمین می‌کند که هر مقدار IV منحصربه‌فرد است. با وجود این‌که، بخش شمارنده بلوک از شمارنده (بایت‌های ۸ تا ۱۵) همان‌طور که در بند ۹-۴ شرح داده شد، توسط گیرنده به عنوان یک عدد ۶۴ بیتی بدون علامت تلقی می‌شود، توصیه می‌شود بردار اولیه هنگام محاسبه بردار اولیه بعدی از قبلی به‌عنوان یک عدد ۱۲۸ بیتی تلقی شود.

۹-۴ عمل شمارنده

حالت AES-CTR، یک رمزنگاری بلوک است که می‌تواند داده با طول اختیاری را بدون نیاز به لایه گذاری، رمزگذاری کند. این عمل توسط رمزگذاری یک بلوک شمارنده با الگوریتم AES عمل می‌کند و سپس برای رمزگذاری یا رمزگشایی، خروجی AES را با داده، XOR می‌کند.

بلوک شمارنده استفاده شده به‌صورت طرح داده شده در بند ۹-۲ ایجاد می‌شود. از ۱۶ بایت بلوک شمارنده، بایت‌های ۸ تا ۱۵ (به عبارت دیگر بایت‌های کم اهمیت) مانند یک عدد صحیح ۶۴ بیتی بدون علامت استفاده می‌شوند که برای هر بلوک بعدی داده نمونه پردازش شده، یک واحد افزایش می‌یابد و به‌ترتیب بایت در شبکه نگهداری می‌شود. توجه داشته باشید که اگر این عدد صحیح، در حالتی که یک IV_size ، ۱۲۸ بیتی(۱۶ بایتی) استفاده می‌شود، به مقدار حداکثر (0xFFFFFFFFFFFFFFFF) برسد، با افزایش آن شمارنده بلوک مجددا به صفر تنظیم می‌شود بدون این‌که به ۶۴ بیت دیگر شمارنده (بایت‌های صفر تا ۷) تاثیر بگذارد.

۹-۵ رمزگذاری نمونه کامل

در رمزگذاری نمونه کامل، کل نمونه رمزگذاری می‌شود. شکل ۱ رمزگذاری مبنی بر نمونه را با استفاده از روش AES-CTR نشان می‌دهد.

شکل ۱- رمزگذاری مبنی بر نمونه برای AES-CTR

توجه داشته باشید که روش AES-CTR یک روش رمزنگاری بلوک است که مانند رمزنگاری جریان عمل می‌کند. بلوک‌ها نشان داده شده‌اند تا بلوک‌های رمزنگاری شده استفاده شده در تولید رمزنگاری جریان را نشان دهند (دلیل این‌که تنها بخشی از بلوک ۷ به‌عنوان بلوک مورد استفاده ، نشان داده شده، این است که بایت‌های استفاده نشده جریان در طول پردازش رمزنگاری حذف می‌شوند.)

۹-۶ رمزنگاری نمونه فرعی[1]

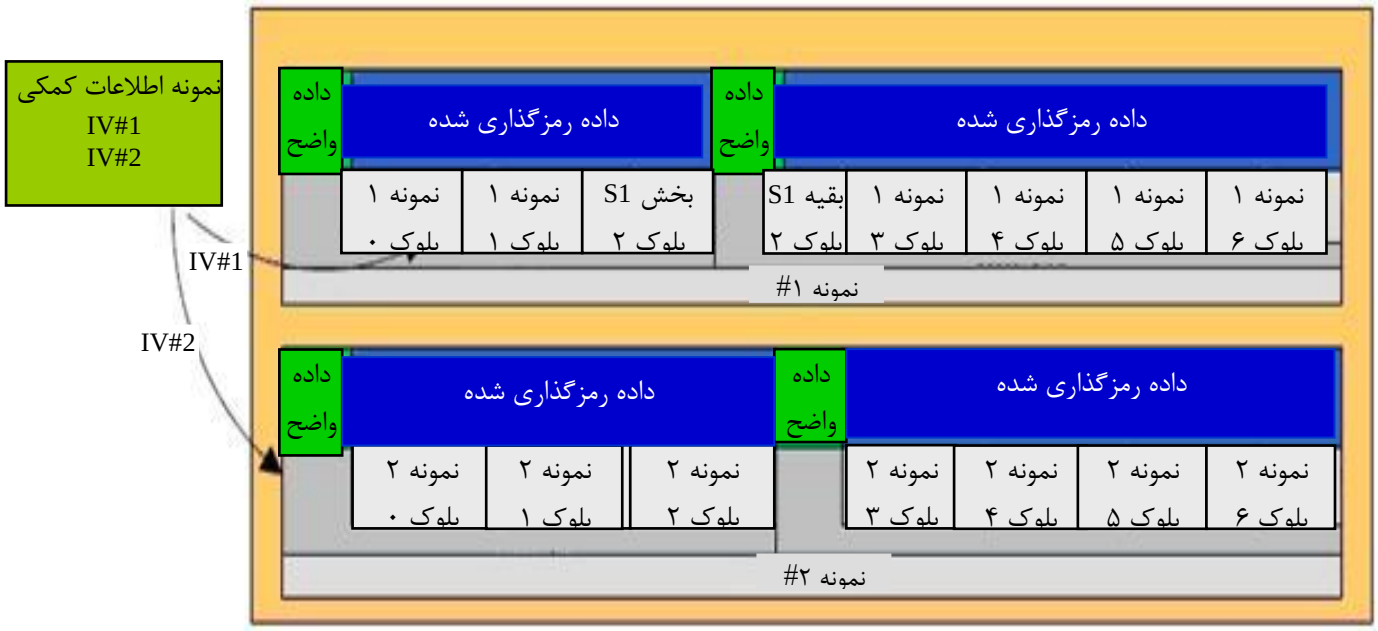
۹-۶-۱ تعریف

1- Sub instance

در رمزنگاری نمونه فرعی، نمونه به یک یا چند نمونه فرعی تقسیم می‌شود. هر نمونه فرعی می‌تواند دارای یک بخش رمزنگاری نشده و به دنبال آن یک بخش رمزنگاری شده باشد. مجموع طول تمامی نمونه فرعی-هایی (جمع بایت‌های واضح و بایت‌های داده رمزنگاری شده برای هر نمونه فرعی) که نمونه را می‌سازند، باید برابر با اندازه خود نمونه باشند.

نواحی رمزگذاری شده یک نمونه، به‌طور منطقی به‌عنوان یک بلوک پیوسته تلقی می‌شوند، با وجود این‌که آن‌ها توسط نواحی داده واضح شکسته می‌شوند. به‌عبارت دیگر شمارنده بلوک به‌صورت اختیاری مابین واحدهای NAL، افزایش نمی‌یابد.

شکل ۲ رمزگذاری مبنی بر نمونه فرعی با استفاده از AES-CTR را نشان می‌دهد.



شکل۲- طرح رمزگذاری مبنی بر زیر نمونه برای AES-CTR با IV های نشان داده شده

توجه داشته باشید که روش AES-CTR یک روش رمزنگاری بلوک است که مانند رمزنگاری جریان عمل می‌کند. بلوک‌ها نشان داده شده‌اند تا بلوک‌های اساسی استفاده شده در تولید رمزنگاری جریان را نمایش دهند. دلیل این‌که بلوک ۶ هم در نمونه ۱# و هم در نمونه ۲# به‌صورت بلوک ۱۶ بایتی کامل نشان داده نشده است، این است که بایت‌های استفاده نشده رمزنگاری جریان در طول پردازش رمزنگاری حذف می‌شوند. هم‌چنین توجه کنید که بلوک ۲# برای رمزنگاری انتهای اولین نمونه فرعی و آغاز نمونه فرعی دوم استفاده می‌شود.

۹-۶-۲ رمزنگاری شیارهای AVC

شیارهای AVC رمزنگاری شده، باید از رمزنگاری نمونه فرعی مشخص شده در بندهای زیر استفاده کنند:

۹-۶-۲-۱ ساختار شیارهای ویدئو AVC

AVC، ساختمان بلوک‌های جریان اولیه AVC را مشخص می‌کند تا واحدهای لایه انتزاعی شبکه (NAL) باشند. این واحدها می‌توانند برای ساختن جریان‌های اولیه AVC برای انواع کاربردهای متنوع استفاده شوند.

برای تعریف این‌که چگونه داده جریان اولیه AVC در یک نگهدارنده قالب فایل رسانه مبنی بر ISO قرار داده می‌شود، باید استاندارد ایران-ایزو ۱۰-۱۴۴۹۶ استفاده شود. در طرح ISO AVC، نمونه‌های سطح نگهدارنده از چندین واحد NAL تشکیل شده‌اند که هر یک توسط فیلد طول، که طول NAL را نشان می‌دهد جدا می‌شوند. شکل ۳ یک نمونه ویدیو AVC توزیع شده روی چندین واحد NAL را نشان می‌دهد.

شکل ۳- نمونه ویدئو AVC توزیع شده روی چندین واحد NAL

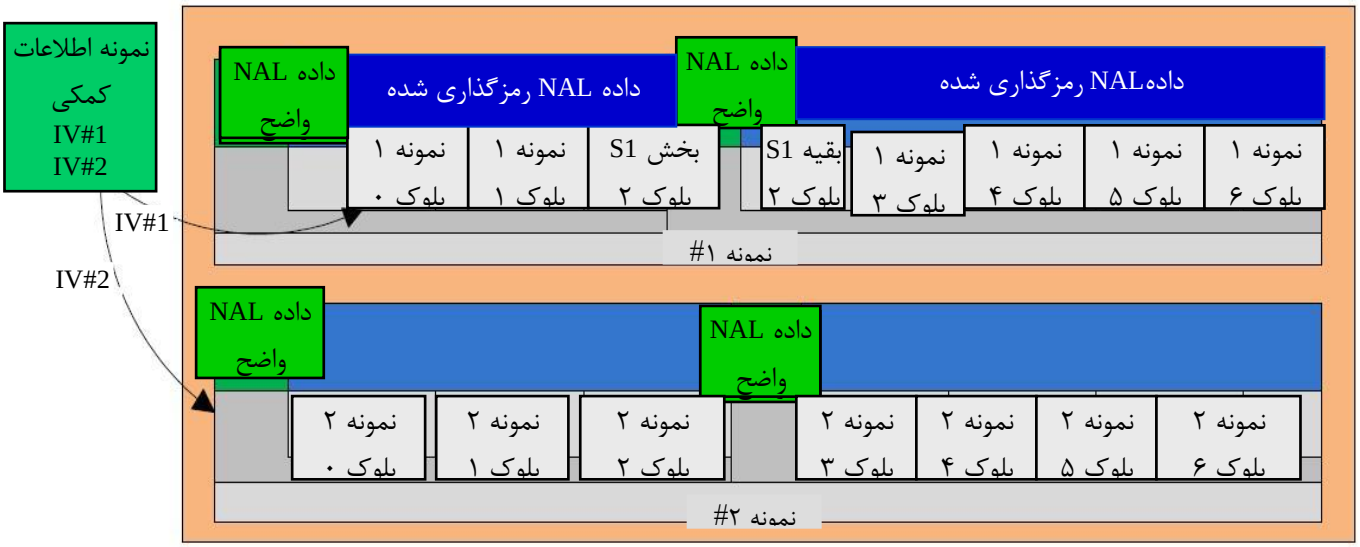
تمامی رمزگشاها به‌منظور سر و کار داشتن با جریان‌های قالبندی ISOAVC، طراحی نشده‌اند. برخی از رمزگشاها برای مدیریت کردن قالب متفاوتی از جریان اولیه AVC طراحی شده‌اند: به‌عنوان مثال، پیوست ب از استاندارد ایران-ایزو ۱۰-۱۴۴۹۶. علاوه بر این ممکن است لازم باشد که جریان اولیه به‌منظور انتقال داده با استفاده از یک پروتکل شبکه مانند RTP که واحدهای NAL را بسته‌بندی می‌کند، مجدداً قالبندی شود. رمزگذاری نمونه کامل از قالب‌بندی مجدد جریان بدون این‌که ابتدا نمونه‌ها برای دسترسی به واحدهای NAL یا سرآیندهای خود رمز گشایی شوند، جلوگیری می‌کند.

جریان بیتی ذخیره شده می‌تواند با اضافه کردن کدهای شروع و واحدهای PPS/SPS NAL به‌عنوان سرآیندهای دنباله، به قالب جریان بایت پیوست ب، تبدیل شود. برای امکان‌پذیر کردن قالب‌بندی مجدد جریان قبل از رمز گشایی، لازم است که حداقل فیلد طول NAL و فیلد nal_unit_type (اولین بایت بعد از طول) از هر واحد NAL رمزگذاری نشده باشند. به‌علاوه باید توجه شود که:

- فیلد طول، فیلد طول متغیر است که می‌تواند ۱، ۲ یا ۴ بایت باشد و برای هر شیار در مدخل نمونه به‌عنوان فیلد LenghSizeMinusOne در AVCDecoderConfigurationRecord مشخص شود.
- در هر نمونه چندین واحد NAL وجود دارد که ملزم به چندین قطعه داده واضح و رمزگذاری شده در هر نمونه است.

۹-۶-۲-۲ رمزگذاری نمونه فرعی اعمال شده در AVC

برای نمونه‌های AVC، هر واحد NAL باید به‌عنوان یک نمونه فرعی تلقی شود. علاوه برآن مقدار BytesOfClearData برای هر نمونه، باید به اندازه کافی بزرگ باشد تا حداقل، بخش سرآیند هر واحد NAL (به‌ویژه فیلد طول NAL و فیلد nal_unit_type) در آن جا شود. شکل ۴ رمزگذاری نمونه فرعی اعمال شده به AVC با استفاده از AES-CTR را نشان می‌دهد. شکل AVهای استفاده شده، نواحی داده واضح، نواحی داده رمزگذاری شده، همچنین واحد NAL و مرزهای نمونه را شرح می‌دهد.



شکل ۴- رمزگذاری زیر نمونه ی اعمال شده به AVC با استفاده از AES-CTR

توجه داشته باشید که روش AES-CTR یک روش رمزنگاری بلوک است که مانند رمزنگاری جریان عمل می‌کند. بلوک‌ها نشان داده شده‌اند تا بلوک‌های اساسی استفاده شده در تولید رمزنگاری جریان را نمایش دهند. دلیل این‌که بلوک ۶ هم در نمونه ۱# و هم در نمونه ۲# به‌صورت بلوک ۱۶ بایتی کامل نشان داده نشده است، این است که بایت‌های استفاده نشده رمزنگاری جریان در طول فرآیند رمزگذاری حذف می‌شوند. همچنین توجه داشته باشید که بلوک ۲ از نمونه ۱# برای رمزگذاری انتهای اولین NAL و ابتدای NAL دوم استفاده شده است.