# مخفی‌سازی اطلاعات مبتنی بر جاسازی ماتریسی و بردار حرکت در استاندارد HEVC

یعقوب صابری[۱]، کارشناس ارشد؛ محمدرضا رمضان‌پور[۲]، استادیار؛ ریحانه خورسند[۳]، استادیار

۱-گروه مهندسی کامپیوتر - واحد مبارکه - دانشگاه آزاد اسلامی - مبارکه - اصفهان - ایران - yaghoubsaberi880@gmail.com
۲-گروه مهندسی کامپیوتر - واحد مبارکه - دانشگاه آزاد اسلامی - مبارکه - اصفهان - ایران - ramezanpour@mau.ac.ir
۳-گروه مهندسی کامپیوتر - واحد دولت آباد - دانشگاه آزاد اسلامی - اصفهان - ایران - r.khorsand@iauda.ac.ir

**چکیده:** با رشد سریع اطلاعات، امنیت آن نیز از جمله موضوعاتی است که توجه زیادی به خود جلب کرده است. مخفی‌سازی اطلاعات یک روش مناسب برای تضمین امنیت اطلاعات مهم بر روی اینترنت است. استاندارد HEVC آخرین استاندارد فشرده‌سازی ویدئو تاکنون است که می‌توان از آن، جهت حمل اطلاعات مخفی استفاده کرد. در این مقاله روشی جدید به‌منظور مخفی‌سازی اطلاعات در ویدئوهای فشرده شده با استاندارد HEVC ارائه شده است. در روش پیشنهادی از بردارهای حرکت بلوک‌های پیشگویی بین‌قابی به عنوان حمل‌کننده‌ی اطلاعات استفاده شده است. مجموعه‌ای از بردارهای حرکت یک بلوک کدکننده در استاندارد HEVC جهت حمل رشته‌ای از بیت‌های مخفی انتخاب شده است و تنها یک مؤلفه از آن مجموعه به میزان یک واحد افزایش یا کاهش می‌یابد که باعث می‌شود نسبت پیک سیگنال به نویز تغییر چندانی نداشته باشد و نرخ بیت، بعد از جاسازی افزایش چندانی نشان ندهد. نتایج آزمایش‌ها نشان می‌دهد که میانگین نسبت سیگنال به نویز ۰/۲۱ دسی‌بل کاهش و نرخ بیت به طور میانگین ۰/۷۶ درصد افزایش یافته است. مقایسه‌ی روش پیشنهادی با سایر روش‌هایی که اخیراً ارائه شده‌اند برتری روش پیشنهادی را نشان می‌دهد.

**واژه‌های کلیدی:** مخفی‌سازی اطلاعات، بردار حرکت، استاندارد HEVC، پیشگویی بین‌قابی.

# Information Hiding Based on Matrix Embedding and Motion Vector in the HEVC Standard

Y. Saberi[1], MSc; M. R. Ramezanpour[2], Assistant Professor; R. Khorsand[3], Assistant Professor

1- Department of Computer Engineering, Mobarakeh branch, Islamic Azad University, Mobarakeh, Isfahan, Iran, Email: yaghoubsaberi880@gmail.com
2- Department of Computer Engineering, Mobarakeh branch, Islamic Azad University, Mobarakeh, Isfahan, Iran, Email: ramezanpour@mau.ac.ir
3- Department of Computer Engineering, Dolatabad branch, Islamic Azad University, Isfahan, Iran, Email: r.khorsand@iauda.ac.ir

**Abstract:** With the rapid development of information, the security of information has gained more and more attention. Information hiding is a useful method to protect secret data through the internet. The High Efficiency Video coding (HEVC) standard is the latest video compression standard ever which can be used to carry hidden data. This paper presents a new method for hiding data in compressed videos using the HEVC standard. In the proposed method, the motion vectors of the inter prediction are used as data carriers. A set of motion vectors of an prediction unit in the HEVC standard is selected to carry a string of hidden data and only a component of that set increases or decreases by one unit, which does not change the peak signal-to-noise ratio (PSNR) significantly, and bit rate does not increase significantly after embedding of hidden data. The results of the experiments demonstrate that the average signal-to-noise ratio decreased by 0.21 decibel and the bit rate increased by an average of 0.76%. Comparison of the proposed method with other recently suggested methods indicates the superiority of the proposed method.

**Keywords:** Information hiding, Motion vector, HEVC standard, Inter prediction.

تاریخ ارسال مقاله: ۱۳۹۸/۰۱/۰۹
تاریخ اصلاح مقاله: ۱۳۹۸/۰۹/۰۹
تاریخ پذیرش مقاله: ۱۳۹۸/۰۹/۱۰
نام نویسنده مسئول: محمدرضا رمضان‌پور
نشانی نویسنده مسئول: ایران - اصفهان - مبارکه - بلوار معلم - میدان فردوسی - بلوار شهید نصوحی - دانشگاه آزاد اسلامی واحد مبارکه - دانشکده فنی و مهندسی - گروه مهندسی کامپیوتر.

## ۱- مقدمه

با پیشرفت روزافزون علوم کامپیوتر و فنّاوری ارتباطات و گسترش شبکه‌های کامپیوتری و افزایش کاربرد سیستم‌های چندرسانه‌ای طی سال‌های اخیر، موضوع «مخفی سازی اطلاعات» در رسانه‌های دیجیتالی بیش از پیش مورد توجه محققان و پژوهشگران قرار گرفته است. امروزه اینترنت به عنوان محیطی ساده و سریع جهت تبادل و به اشتراک گذاشتن اطلاعات و ارسال انواع محصولات دیجیتالی از قبیل فایل‌های متنی، صوتی، تصویری و فیلم، در بین اقشار مختلف جامعه جهانی شناخته شده و موجب رشد بیشتر تولید این محصولات توسط افراد و شرکت‌های فعال در این زمینه‌ها گردیده است. بنابراین لزوم استفاده از روش‌هایی امن جهت برقراری ارتباطات مخفی در سطح شبکه‌های کامپیوتری و اینترنتی بسیار محسوس‌تر شده است [۱]. مخفی کردن اطلاعات به دو روش قابل انجام است، پنهان‌سازی[۱] و نهان‌نگاری. در پنهان‌سازی، اطلاعات غیرقابل رویت بوده به‌طوری‌که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند در حالی‌که در نهان‌نگاری، پیام می‌تواند هم قابل رویت و هم غیرقابل رویت باشد. در نهان‌نگاری تصاویر دیجیتال، اطلاعات دیجیتال تحت عنوان اطلاعات نهان‌نگار در یک تصویر میزبان جاسازی می‌شود و تصویر نهان‌نگاری شده ارسال می‌گردد. در گیرنده پس از دریافت تصویر نهان‌نگاری شده، اطلاعات نهان‌نگار را از آن استخراج می‌کنند.

تقسیم‌بندی‌های مختلفی برای الگوریتم‌های مخفی‌سازی اطلاعات وجود دارد. این الگوریتم‌ها از لحاظ حوزه‌ی عملکرد به دو دسته کلی، الگوریتم‌های حوزه مکان و الگوریتم‌های حوزه تبدیل تقسیم می‌شوند. الگوریتم‌های حوزه مکان به طور مستقیم پنهان نگاری را روی مقادیر پیکسل‌های تصویر میزبان انجام می‌دهند، در حالی که الگوریتم‌های حوزه تبدیل، ابتدا تصویر میزبان را با استفاده از تبدیل‌هایی مانند DCT[۲] و DWT[۳] به حوزه تبدیل انتقال می‌دهند، در آنجا عمل درج اطلاعات محرمانه را انجام داده و دوباره به حوزه مکان برمی‌گردانند. مزیت عمده‌ی روش‌های حوزه مکان، داشتن پیچیدگی زمانی و محاسباتی پایین، سرعت اجرای بالا و سادگی نسبی در پیاده‌سازی آن-هاست [۲]. به‌علاوه روش‌های حوزه مکان را می‌توان برای انواع گوناگونی از تصاویر دیجیتالی به‌کار برد. در مقابل این روش‌ها، روش‌های حوزه تبدیل قرار دارند که مقاومت زیادی در مقابل حملات تحلیل پنهان‌شکنی و پردازش‌های رایج از خود نشان می‌دهند [۳]. این روش‌ها، به دلیل انتقال تصویر به حوزه تبدیل و بازگرداندن دوباره آن به حوزه مکان با استفاده از تبدیل وارون، دارای پیچیدگی زمانی و محاسباتی بالا هستند [۴].

یکی از مهم‌ترین کاربردهای مخفی‌سازی اطلاعات، در ویدئوها است. از آنجایی که ویدئوها معمولاً به منظور ذخیره‌سازی فشرده می‌شوند، می‌توان اطلاعات مخفی را قبل یا بعد از فشرده‌سازی به ویدئو اضافه کرد. در صورتی که قبل از فشرده‌سازی، اطلاعات مخفی در ویدئو جاسازی شود ممکن است داده‌ها در هنگام فشرده‌سازی از بین بروند. روش دیگر جاسازی داده‌ها در حین فشرده‌سازی و یا بعد از فشرده‌سازی است که مشکل روش قبل را ندارد. آخرین استاندارد فشرده‌سازی ویدئو، HEVC[۴] است که در سال ۲۰۱۳ معرفی شد [۵]. به همین منظور در این مقاله به بررسی روش‌های مخفی‌سازی اطلاعات در ویدئو پرداخته می‌شود که با استاندارد HEVC فشرده شده‌اند. روش پیشنهادی نیز از ویژگی‌های استاندارد HEVC استفاده می‌نماید تا اطلاعات را در ویدئوهای فشرده شده در استاندارد HEVC مخفی نماید. کارهای مختلفی در زمینه‌ی مخفی‌سازی اطلاعات در استاندارد HEVC انجام گرفته است.

لانگ و همکاران[۶] از ضرایب باقیمانده بعد از پیشگویی در استاندارد HEVC جهت مخفی کردن اطلاعات استفاده کرده‌اند. در استاندارد HEVC به همراه بردارهای حرکت، ماتریس جبران حرکت که شامل اختلاف تصویر پیش‌گویی با تصویر اصلی است ذخیره می‌گردد. آن‌ها از ضرایب غیر صفر ماتریس جبران حرکت (ضرایب باقیمانده) استفاده کرده تا اطلاعات را در آن‌ها ذخیره نمایند. برای افزایش امنیت ابتدا ویدئو و پیام مخفی رمز شده، سپس اطلاعات مخفی در ضرایب غیر صفر ماتریس جبران حرکت جاسازی می‌گردد.

سواتی و همکاران[۷] از بلوک‌های تبدیل در استاندارد HEVC جهت مخفی‌سازی اطلاعات استفاده کرده‌اند. بلوک تبدیل نتایج حاصل از تبدیل DCT روی ماتریس جبران حرکت را شامل می‌شود. اندازه‌ی بلوک‌های تبدیل از ۴×۴ تا ۳۲×۳۲ می‌تواند متغیر باشد. آن‌ها از بیت‌های کم ارزش‌تر ضرایب بلوک تبدیل، جهت مخفی سازی اطلاعات استفاده کرده‌اند.

یانگ و همکاران [۵] روش مبتنی بر حالت‌های تقسیم شدن بلوک‌های پیشگویی در استاندارد HEVC جهت مخفی‌سازی اطلاعات ارائه داده‌اند. روش آن‌ها شامل دو مرحله می‌باشد. در مرحله‌ی اول حالت‌های تقسیم شدن بلوک‌های پیشگویی توسط استاندارد HEVC ثبت می‌شود سپس در مرحله بعد، هر حالت با توجه به بیت‌های مخفی به یک گروه اختصاص می‌یابد و بر اساس ویژگی آن گروه حالت تقسیم شدن، اصلاح می‌گردد.

لی و همکاران [۸] از بردار حرکت مبتنی بر اصلاح هیستوگرام استفاده کرده است. ابتدا بردار حرکت بر اساس مقدار مولفه‌ها به یکی از ۱۷ مجموعه از پیش تعریف‌شده تعلق می‌گیرد سپس بر اساس مجموعه‌ای که بردار حرکت به آن تعلق دارد مقادیر بردار حرکت اصلاح می‌گردد. عیب این روش کاهش چشمگیر کیفیت ویدئو پس از جاسازی اطلاعات مخفی می‌باشد.

کونیار و همکاران [۹] از ضرائب تبدیل DST در استاندارد HEVC جهت مخفی‌سازی اطلاعات استفاده کرده‌اند. روش پیشنهادی آن‌ها مبتنی بر روش جاسازی ماتریسی در پیشگویی درون‌قابی است. از آنجایی‌که روش پیشنهادی از پیشگویی درون‌قابی استفاده می‌نماید در نتیجه از انتشار خطا در فریم‌های بعدی جلوگیری می‌نماید.

ژو [۱۰] از اصلاح ضرائب تبدیلDCT، اختلاف بردارهای حرکت در پیشگویی بین‌قابی و مدهای پیشگویی درون‌قابی به طور همزمان جهت مخفی‌سازی اطلاعات استفاده کرده‌اند. آن‌ها نشان داده‌اند که روش پیشنهادی تاثیر کمتری در کاهش کیفیت ویدئوهای حامل دارد. آن‌ها برای این کار، ساختار رشته‌بیت به‌دست آمده توسط استاندارد HEVC را تغییر داده‌اند که از معایب این کار می‌توان برشمرد.

جی و ژو [۱۱] نیز از بلوک‌های تبدیل در استاندارد HEVC استفاده کرده‌اند، با این تفاوت که اندازه‌ی بلوک‌های تبدیل را ۸×۸ در نظر گرفته‌اند. ضرایبی که نزدیک به فرکانس میانی هستند را، به عنوان حمل‌کننده‌ی اطلاعات مخفی در نظر گرفته‌اند.

چانگ و همکاران [۱۲] روشی برای مخفی سازی اطلاعات در فریم‌هایی که به صورت درون‌قابی در استاندارد HEVC کد شده‌اند ارائه داده‌اند. آن‌ها در این روش، محدودیت انتشار خطا در بلوک‌های همسایه را اعمال کرده‌اند. در روش پیشنهاد شده، ویژگی‌های سیگنال DCT/DST را آنالیز کرده‌اند تا سیگنال‌هایی را پیدا کنند که در انتشار خطا به بلوک‌های مجاور یا فریم‌های مجاور نقش نداشته باشند. آن‌ها همچنین یک روش بهبود کیفیت تصویر ارائه داده‌اند تا تأثیر تغییرات فریم‌های درون قابی را روی پیشگوی بین‌قابی کم کنند. آن‌ها روش خود را با دو طرح ارائه شده برای استاندارد H.264/AVC[۵] مقایسه کرده‌اند و نتایج آن‌ها بهبود نسبت به دو طرح دیگر را نشان می‌دهد.

وانگ و همکاران [۱۳] از مدهای پیشگویی درون قابی برای مخفی سازی اطلاعات استفاده کرده‌اند. آن‌ها بهترین مدهای پیشگویی بلوک‌های ۴×۴ را انتخاب کرده و اختلاف زاویه بین دو مد بلوک پشت سر هم را به دست می‌آورند. سپس با توجه به رشته اطلاعات مخفی، مدهای پیشگویی را اصلاح می‌نماید. روش آن‌ها فقط زمانی مفید است که ویدئوها به صورت درون قابی کد شوند.

تعدای از مقالات از پیشگویی درون قابی جهت مخفی‌سازی اطلاعات استفاده کرده‌اند. اگر چه پیاده‌سازی‌های متفاوتی دارند ولی این روش‌ها اطلاعات را با اصلاح مدهای پیشگویی درون‌قابی مخفی می‌نمایند. در این روش‌ها اطلاعات فقط می‌تواند در فریم‌هایی که به‌صورت درون‌قابی کد شده‌اند جاسازی شود. از آنجایی‌که بخش کمی از فریم‌ها در یک ویدئو به صورت درون‌قابی کد می شوند ظرفیت جاسازی این روش‌ها محدود است. تعدادی دیگر از مقالات از اصلاح بردار حرکت در پیشگویی بین‌قابی جهت مخفی‌سازی اطلاعات استفاده کرده‌اند. از آنجایی‌که در پیشگویی بین‌قابی علاوه بر بردار حرکت از یک ماتریس جبران ساز استفاده می‌گردد روش‌هایی که از بردار حرکت استفاده می‌نمایند تاثیر کمتری در از بین بردن کیفیت ویدئو خواهند داشت. از سوی دیگر، فریم‌هایی که به‌صورت بین‌قابی کد می‌شوند سهم بیشتری نسبت به فریم‌هایی دارند که به‌صورت درون قابی کد می‌شوند. در نتیجه روش‌هایی که از اصلاح بردار حرکت در پیشگویی بین‌قابی استفاده می‌نمایند ظرفیت جاسازی بیشتری خواهند داشت.

روش پیشنهادی در این مقاله نیز مشابه با مقاله یانگ و لی [۱۴] از بردارهای حرکت جهت مخفی‌سازی اطلاعات استفاده کرده‌اند با این تفاوت که به منظور افزایش ظرفیت جاسازی، روش مخفی‌سازی بهبود داده شده است. در روش پیشنهاد شده توسط یانگ و لی [۱۴]، تعدادی از بردارهای حرکت در یک بلوک انتخاب شده و روش مخفی سازی EMD روی بردارهای حرکت اعمال می‌شود در حالی‌که در روش پیشنهادی نیز از بردارهای حرکت جهت مخفی‌سازی استفاده خواهد شد اما به‌جای الگوریتم EMD از روش جدیدتری استفاده شده است تا ظرفیت جاسازی بیت‌های مخفی افزایش یابد. در روش پیشنهادی، به منظور جاسازی L بیت از اطلاعات مخفی، تنها یکی از مؤلفه‌های بردار حرکت به میزان یک واحد کاهش یا افزایش خواهد یافت. علاوه بر این، از یک کلید برای جاسازی و استخراج پیام مخفی استفاده می‌شود و تنها با استفاده از Nتا از کوچک‌ترین بلوک‌های پیشگویی به عنوان میزبان، کار جاسازی انجام می‌شود که N تعداد بلوک‌های پیشگویی است. همچنین، با استفاده از ویژگی‌های محتوای HEVC و قابلیت جاسازی داده در فرایند فشرده‌سازی جریان‌های ویدئوی HEVC، احتمال حمله امنیتی به حداقل می‌رسد. در مقایسه با روش‌های دیگر، روش پیشنهادی می‌تواند بعد از جاسازی داده‌ها در ویدئوهای HEVC ظرفیت جاسازی بالاتری با حفظ کیفیت و امنیت را حاصل کند.

ادامه‌ی بخش‌های این مقاله به شرح زیر است: در بخش ۲، دانش پیش زمینه شامل مروری بر استاندارد HEVC تا حدی که بقیه‌ی قسمت‌ها قابل فهم باشند شرح داده می‌شود. روش پیشنهادی که شامل نحوه‌ی ساخت بردار حمل کننده و نحوه‌ی جاسازی و استخراج داده‌ها است در بخش ۳ بیان می‌شود. در بخش ۴ به معرفی پارامترهای اندازه گیری و تحلیل نتایج و مقایسه‌ی روش پیشنهادی با روش‌های اخیری که در این زمینه ارائه شده، پرداخته می‌شود. در نهایت، نتیجه گیری در بخش ۵ ارائه خواهد شد.

## ۲- دانش پیش زمینه

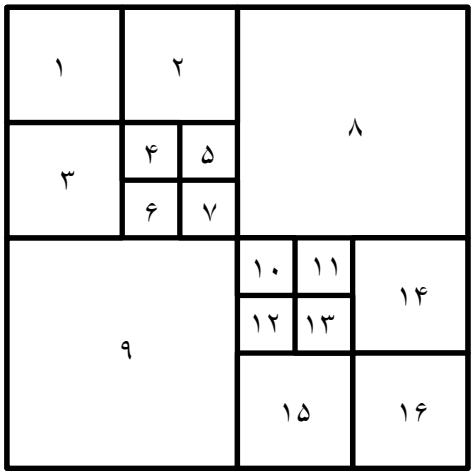
برای درک بهتر روش پیشنهادی، به مروری کوتاه بر استاندارد فشرده‌سازی HEVC و انواع پیشگویی‌های مورد استفاده در آن پرداخته می‌شود؛ توضیحات بیشتر در مراجع [۱۵-۱۷] بیان شده است.

### ۲-۱- استاندارد فشرده‌سازی HECV

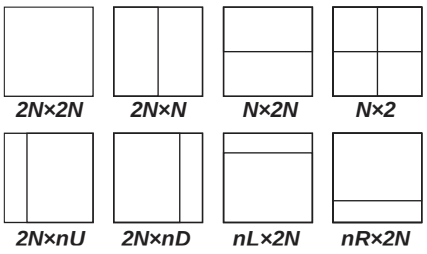
کدگذاری ویدئویی با کارایی بالا (HEVC)، آخرین استاندارد فشرده‌سازی ویدئو است. در استاندارد HEVC هر تصویر به بلوک‌های ۶۴×۶۴ پیکسل به نام CTU[۶] تقسیم می‌شود، سپس این CTU ها به واحدهایی به نام واحد کد کننده CU[۷] در یک ساختار بازگشتی درخت چهارتایی شکسته می‌شود به طوری که CTU به عنوان ریشه‌ی این درخت شناخته می‌شود و هر واحد کد کننده شامل یک بلوک لوما و دو بلوک کروما است و اندازه‌ی آن می‌تواند به صورت $2^n \times 2^n$ باشد که n یک عدد صحیح از مقدار ۳ تا ۶ است [۱۵]. هر بلوک کد کننده،

ناحیه‌ای از تصویر را مشخص می‌کند که حالت پیشگویی آن‌ها یکسان است. شکل۱ نحوه‌ی تقسیم شدن یک CTU را به واحدهای کد کننده با اندازه‌ی ۶۴×۶۴ تا ۸×۸ را نشان می‌دهد. اعداد نوشته شده در هر بلوک نشان دهنده‌ی ترتیب کد شدن هر بلوک است.

هر بلوک کد کننده می‌تواند شامل یک یا چند بلوک پیشگویی PU[۸] باشد. در پیشگویی بین قابی اندازه‌ی بلوک پیشگویی می‌تواند ضریبی از بلوک کد کننده باشد که در این حالت بلوک کد کننده می‌تواند به ۸ حالت مختلف شکسته شود که اندازه‌های مختلف آن در شکل ۲ نشان داده شده است.




**شکل ۱: یک مثال از نحوه‌ی تقسیم شدن یک CTU به بلوک‌های کد کننده.**




**شکل ۲: هشت حالت برای تقسیم بندی CU به PU ها**

در پیشگویی بین‌قابی استاندارد HEVC برای حذف افزونگی زمانی، از روش تخمین حرکت و جبران استفاده شده است. برای تخمین حرکت در استاندارد HEVC ابتدا تصویر به بلوک‌های پیشگویی شکسته می‌شود، سپس به دنبال بهترین مکان این بلوک در یک محدوده‌ی خاص از فریم قبلی می‌گردد و بهترین جایی که این بلوک با فریم قبلی مطابقت کند را یافته و میزان این تغییر حرکت را با بردار حرکت نمایش می‌دهد. پس هر بلوک پیشگویی دارای یک بردار حرکت است که میزان جابه‌جایی آن بلوک را نسبت به فریم قبلی نشان می‌دهد و شامل دو مقدار y و x است که x میزان اختلاف حرکت در جهت محورافقی و y میزان اختلاف حرکت در جهت محور عمودی را نشان می‌دهد. در بخش بعد روش پیشنهادی با جزئیات آن بیان خواهد شد.

## ۳- روش پیشنهادی

در پیشگویی بین‌قابی، هر بلوک پیشگویی دارای یک بردار حرکت است که میزان جابجایی آن بلوک را نسبت به بلوک هم مکان در فریم مرجع نشان می‌دهد. در روش پیشنهادی از این بردارهای حرکت به عنوان حمل کننده اطلاعات مخفی استفاده می‌شود. برای افزایش امنیت در روش پیشنهادی تنها بخشی از بلوک‌ها انتخاب شده و از بردارهای حرکت آن‌ها به عنوان حمل کننده اطلاعات مخفی استفاده می‌شود. همچنین در روش پیشنهادی، طرح پیشنهاد شده توسط فن و همکاران [۱۸]، جهت مخفی سازی اطلاعات در بردارهای حرکت بهبود داده می‌شود تا ظرفیت جاسازی بیت‌های مخفی افزایش یابد. دلیل انتخاب این الگوریتم، ساده بودن و ظرفیت جاسازی بالاتر نسبت به سایر الگوریتم‌ها است. جزئیات روش پیشنهادی در ادامه بیان خواهد شد.

### ۳-۱- ساخت بردار حمل کننده

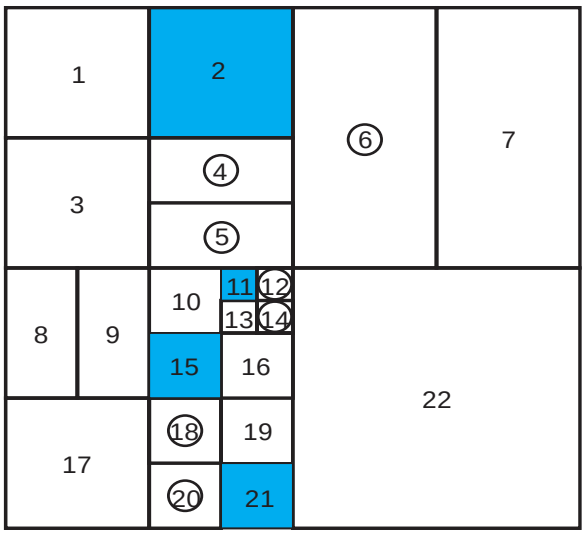
در روش پیشنهادی، بلوک پایه جهت جاسازی اطلاعات، یک CTU است که بلوک پایه استاندارد HEVC برای پیشگویی نیز هست. برای افزایش امنیت از تمام CTU ها جهت جاسازی استفاده نمی‌شود. برای هر CTU یک عدد تصادفی r توسط تابع G تولید می‌گردد که این عدد احتمال انتخاب شدن آن CTU را به عنوان حمل کننده نشان می‌دهد. پارامتری به نام e تنظیم شرط انتخاب است که عددی بین صفر و یک است. برای مثال اگر e برابر با ۰/۵ باشد یعنی به احتمال ۵۰ درصد هر CTU به عنوان حمل کننده انتخاب نخواهد شد و اگر r کمتر از e باشد، CTU به عنوان حمل کننده انتخاب می‌گردد. به منظور جاسازی و استخراج اطلاعات مخفی به طور صحیح، تولید کننده عدد تصادفی یعنی G باید با مقدار کلید مشترک در گیرنده و فرستنده بارگذاری شود. این کلید مشترک به عنوان کلید رمز k بین فرستنده و گیرنده تبادل خواهد شد. اگر یک CTU به عنوان حمل‌کننده انتخاب گردید، تعداد بلوک‌های پیشگویی داخل یک CTU جهت ساخت بردار حمل کننده از رابطه‌ی ۱ به دست می‌آید:

$$N = (r \times 100) \bmod u \qquad (۱)$$

در اینجا $r$ عددی تصادفی است که احتمال انتخاب یک بلوک CTU را نشان می‌دهد، $u$ ماکزیمم تعداد بلوک‌های پیشگویی در یک CTU است و $N$ تعداد بلوک‌های پیشگویی برای ساخت بردار حمل کننده را نشان خواهد داد که برای هر بلوک متفاوت و به صورت تصادفی است، در نتیجه باعث افزایش امنیت روش پیشنهادی خواهد شد. در مرحله بعد تعداد بلوک‌های پیشگویی در CTU که دارای بردار حرکت می‌باشند شمارش می‌شود. در صورتی که تعداد آن‌ها از N بیشتر باشد آن CTU به عنوان حمل‌کننده انتخاب می‌گردد، در غیر این صورت CTU شرط حمل اطلاعات را نخواهد داشت. به دلیل آنکه بردارهای حرکت بلوک‌های انتخابی جهت حمل اطلاعات تغییراتی خواهند داشت، پس هر چه اندازه‌ی بلوک‌ها کوچک‌تر باشند اعوجاج

تصویر کمتر خواهد شد، در نتیجه Nتا از بلوک‌های پیشگویی که دارای کوچک‌ترین اندازه است جهت ساخت بردار حمل‌کننده انتخاب خواهند شد. بردار حمل‌کننده با استفاده از N بلوک‌های پیشگویی به صورت $C=(c_1,c_2,\ldots,c_{2N})$ ساخته می‌شود که $(c_{2i-1}, c_{2N})$ بردار حرکت بلوک پیشگویی i ام است که $c_{2i-1}$ میزان جابجایی در جهت محور x و $c_{2i}$ میزان جابجایی در جهت محور y است. در روش پیشنهادی حداکثر یک مؤلفه از بردار حمل‌کننده به میزان یک واحد افزایش یا کاهش خواهد داشت.

شکل ۳ مثالی از یک CTU را نشان می‌دهد که به عنوان حمل‌کننده انتخاب شده است. بلوک‌های پیشگویی با شماره‌هایی که در شکل ، دایره دور آن رسم گردیده است، بلوک‌هایی هستند که بردار حرکت آن‌ها (0,0) است و مد آن‌ها پرش یا ادغام انتخاب شده است، یعنی این بلوک‌ها دارای بردار حرکت نیستند و نمی‌توان برای ساخت بردار حمل از آنها استفاده کرد. با فرض انتخاب N= 4، باید ۴ بلوک پیشگویی با کوچک‌ترین اندازه که دارای بردار حرکت هستند، جهت ساخت بردار حمل‌کننده انتخاب شوند. بلوک‌های پیشگویی انتخاب شده با اعداد ۲، ۱۱، ۱۵ و ۲۱ مشخص شده‌اند. در شکل ۳ بلوک‌های پیشگویی با سایه به عنوان حامل انتخاب شده‌اند. از بردارهای حرکت این ۴ بلوک پیشگویی جهت ساخت بردار حمل کننده استفاده خواهد شد.




**شکل ۳: تقسیم یک CTU و انتخاب بلوک‌های پیشگویی به عنوان حامل. بلوک‌های پیشگویی که با کادر پر رنگ نشان داده شده اند از حالت پرش یا ادغام استفاده می‌کنند.**

بردار حرکت بلوک پیشگویی i ام با $d_i$ نشان داده می‌شود که هر بردار شامل دو مؤلفه‌ی h و v خواهد بود. h میزان جابجایی در جهت محور افقی و v میزان جابجایی در جهت محور عمودی را نشان می‌دهد. اگر بردارهای حرکت چهار بلوک پیشگویی انتخاب شده را با $d_1=(h_1, v_1)$، $d_2=(h_2, v_2)$ ، $d_3=(h_3, v_3)$ و $d_4=(h_4, v_4)$ نشان دهیم بردار حمل‌کننده به صورت $C=(h_1, v_1, h_2, v_2, h_3, v_3, h_4, v_4)$ خواهد بود که می‌توان آن را به صورت $C=(c_1, c_2, \ldots, c_8)$ بازنویسی کرد.

### ۳-۲- نحوه‌ی جاسازی اطلاعات در بردار حمل‌کننده

در روش پیشنهادی حداکثر یک مؤلفه از بردار حرکت به میزان یک واحد کم یا زیاد خواهد شد. قبل از جاسازی، اطلاعات به صورت عکس، متن و یا قالب‌های دیگر است که باید به صورت عدد باینری در آیند تا اطلاعات رمز شده به صورت رشته بیت استفاده شوند. برای هر CTU یک رشته بیت به طول L انتخاب می‌شود تا در آن CTU جاسازی شود که L از رابطه ۲ به دست می‌آید:

$$L=\lfloor \log_2(2N+1) \rfloor+1 \qquad (۲)$$

اگر رشته‌ی انتخابی s باشد $s=(s_L, s_{L-1}, \ldots, s_2, s_1)$ آنگاه مقدار دسیمال رشته بیت انتخابی از رابطه ۳ قابل محاسبه است:

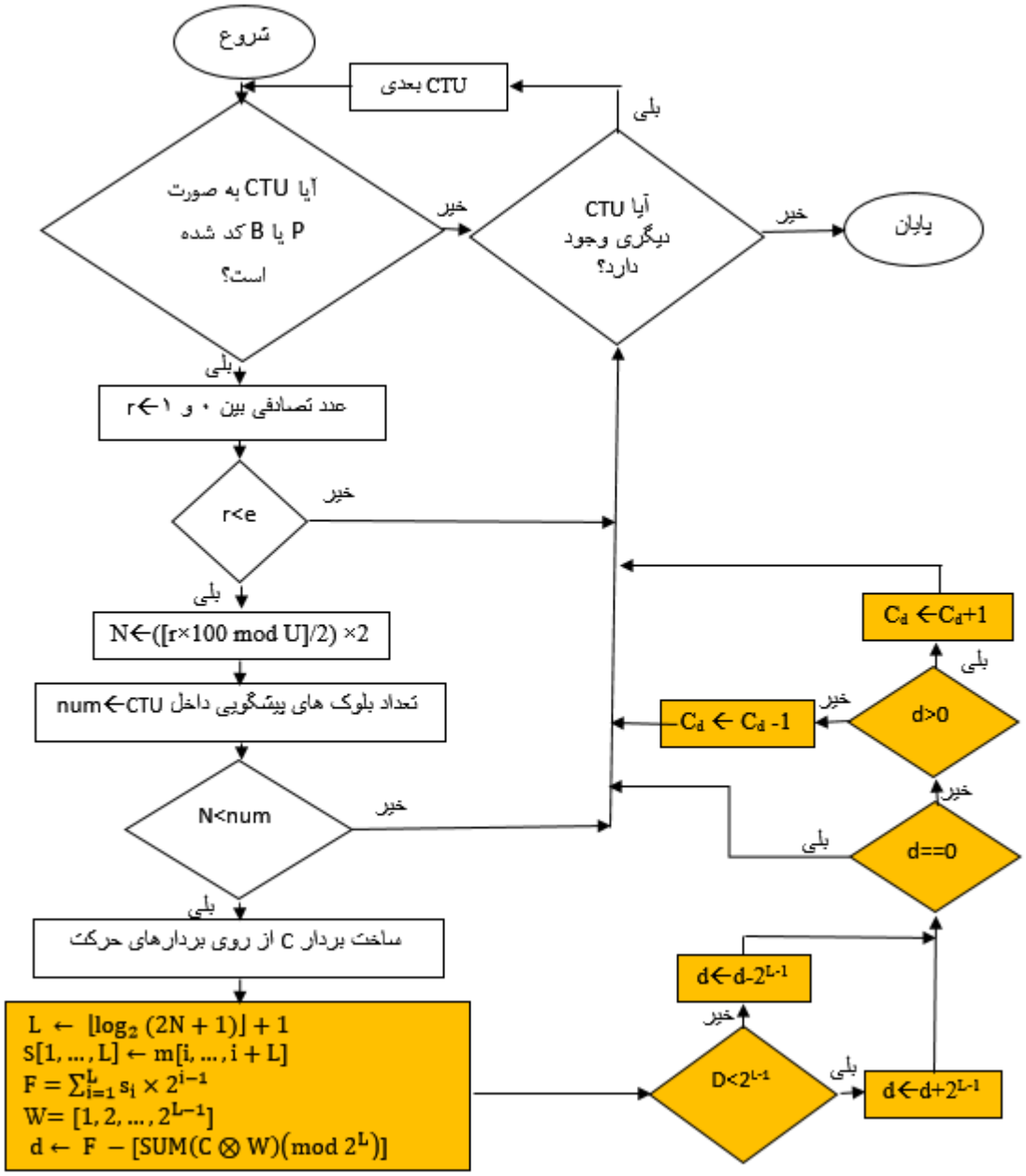
$$F=\sum_{i=1}^{L} S_i \times 2^{i-1} \qquad (۳)$$

در مرحله‌ی بعد یک ماتریس سطری که w نامیده می‌شود با اندازه ی $1\times 2^{L-1}$ استفاده می‌شود که هر یک از مقادیر یک تا $2^{L-1}$ حداقل یک‌بار در آن وجود دارد. در مرحله‌ی بعد، از رابطه‌ی ۴ مقدار d محاسبه می‌گردد:

$$d=F-\left[ SUM(c_i \otimes w) \bmod 2^L \right] \qquad (۴)$$

که در این رابطه $\otimes$ نشانه‌ی ضرب درایه به درایه در دو بردار است. همچنین *SUM* بیانگر جمع تمامی درایه‌های بردار با یکدیگر و mod به معنای محاسبه‌ی باقیمانده‌ی عدد به دست آمده بر $2^L$ است. اکنون، بر اساس مقدار d به دست آمده محل اصلاح درایه‌ی مورد نظر در بردار C تغییر داده می‌شود. در صورتی که d= 0 بود هیچ یک از درایه‌های بردار حمل‌کننده نیاز به اصلاح ندارند و فرآیند جاسازی اطلاعات، در آن CTU به پایان می‌رسد، در غیر این صورت درایه‌ی d ام با توجه به علامت d یک واحد کاهش یا یک واحد افزایش می‌یابد یعنی در صورتی که علامت عدد d منفی باشد درایه‌ی d ام یک واحد کاهش و در غیر این صورت، یک واحد افزایش می‌یابد. شکل شکل ۴ فلوچارت روش پیشنهادی را نشان می‌دهد. بلوک‌هایی که به‌صورت رنگی می‌باشند تفاوت بین روش یانگ و لی [۱۱] با روش پیشنهادی را نشان می‌دهد در حالی‌که ظرفیت جاسازی بیت‌های مخفی افزایش یافته است. مقدار K به عنوان کلید رمز است که بین فرستنده و گیرنده توزیع شده است. تابع G تولید کننده‌ی عدد تصادفی است و پارامتر e احتمالی است که برای انتخاب شدن یا نشدن یک CTU تنظیم می‌گردد. در استاندارد HEVC، CTUها به صورت درون‌قابی یا بین‌قابی کد می‌شوند. به دلیل اینکه از بردارهای حرکت جهت حمل اطلاعات استفاده می‌نماییم، پس CTUهایی که به صورت بین‌قابی کد شده‌اند باید انتخاب گردند. سپس مقدار r که یک عدد تصادفی است تعیین می‌نماید که آیا CTU برای مخفی سازی اطلاعات انتخاب گردد یا نه. در صورتی که مقدار r از e که توسط کاربر تنظیم می‌شود کمتر باشد، شانس انتخاب شدن برای حمل اطلاعات مخفی را خواهد داشت. برای افزایش امنیت مجدداً تعداد بلوک‌های پیشگویی داخل CTU

شمارش می‌گردد، در صورتی که از N بزرگ‌تر باشد جهت حمل اطلاعات انتخاب شده در غیر این صورت به سراغ CTU بعدی می‌رود. بعد از انتخاب CTU به عنوان حمل‌کننده‌ی اطلاعات مخفی، Nتا از کوچک‌ترین بلوک‌های پیشگویی که دارای بردار حرکت هستند، انتخاب شده و بردار حمل کننده از روی بردارهای حرکت آن بلوک‌ها ساخته می‌شوند. سپس L بیت از اطلاعات مخفی در این بردار حمل خواهد شد. برای این کار L بیت از رشته اطلاعات مخفی را جدا کرده و مقدار دسیمال آن را F می‌نامیم. بردار وزن W با اندازه‌ی $1\times2^{L-1}$ که شامل اعداد ۱ تا $2^{L-1}$ است، ساخته می‌شود. مقدار d از رابطه‌ی ۴ محاسبه گردیده و مقدار آن را در بازه‌ی $[-2^{L-1},2^{L-1}]$ تنظیم می‌نماییم. در صورتی که مقدار d برابر صفر باشد عملیات مخفی‌سازی به پایان رسیده و به سراغ CTU بعدی می‌رویم. در غیر این صورت درایه‌ی d ام بردار C انتخاب شده و با توجه به علامت مقدار d از درایه‌ی d ام یک واحد کاهش و یا یک واحد افزایش خواهد یافت. مزیت این روش این است که فقط یک درایه از بردار C یک واحد تغییر خواهد کرد.




**شکل ۴: فلوچارت روش پیشنهادی جهت جاسازی اطلاعات مخفی**

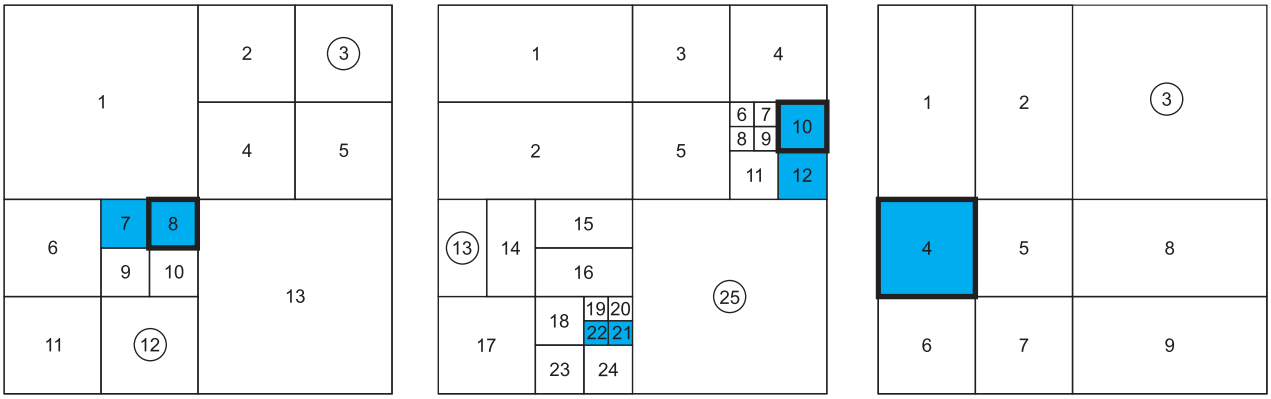
در ادامه برای فهم بهتر روش پیشنهادی مثالی ارائه می‌شود. شکل ۵، سه CTU را نشان می‌دهد که با استاندارد HEVC کد شده است. بلوک‌های پرش و ادغام با شماره‌ی دایره‌دار نشان داده شده‌اند. در این مثال رشته اطلاعات مخفی، 101100011 می‌باشد و مقدار N = 1, 4, 2 در نظر گرفته می‌شود بنابراین تمام ۹ بیت رشته اطلاعات مخفی در سه CTU جاسازی می‌شود که حاصل کد کردن در شکل ۵ با جزئیات نشان داده شده است. به عنوان مثال، در حالت (ب) که مقدار N = 4 است، ۴ بلوک با اندازه‌ی کوچک‌تر جهت ساخت بردار حمل کننده

انتخاب شده و بردارهای حرکت آن‌ها به ترتیب $d_1$= (-1, -2)، $d_2$= (30, 16)، $d_3$= (1, 2) و $d_4$= (11, 19) است؛ در نتیجه بردار حمل کننده برابر است با: C= (-1, -2, 30, 16, 1, 2, 11, 19) است. رشته اطلاعات مخفی به طول ۴ بیت که در این CTU قرار است جاسازی شود، برابر است با "1100"، در نتیجه با استفاده از رابطه ۴ مقدار d عبارت است از:

$$d = F\text{-}[SUM\ (c_i \otimes w)\ mod\ 2^L] = 12\text{-}[SUM\ ((-1, -2, 30, 16, 1, 2, 11, 19) \otimes (1, 2, 3, 4, 5, 6, 7, 8))\ mod\ 2^4] =$$

$$12\text{-}[((-1\times1)+(-2\times2)+(30\times3)+(16\times4)+(1\times5)+(2\times6)+(11\times7)+(19\times8))\ mod\ 2^4] = 12-11=1$$

درایه dام در بردار حمل کننده، باید یک واحد تغییر کند، چون d>0 است؛ درایه‌ی اول یک واحد افزایش خواهد یافت. بردار حمل کننده بعد از اصلاح و جاسازی اطلاعات به صورت C'= (0, -2, 30, 16, 1, 2, 11, 19) خواهد بود.




| ردیف | N | Z | $d_i$ | C | m | L | S | F | d | T | $\bar{C}$ | $\bar{d}_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| الف | 1 | 4 | $d_1$ = (2,3) | C = (2,3) | 101100011 | 2 | 10 | 2 | 2 | 4 | (2,4) | $d_1$ = (2,4) |
| ب | 4 | 10, 12, 21,22 | $d_2$ = (-1,-2)<br>$d_3$ = (30,16)<br>$d_4$ = (1,2)<br>$d_5$ = (11,19) | C = (-1,-2,30,16,1,2,11,19) | 101100011 | 4 | 1100 | 12 | 1 | 10 | (0,-2,30,16,1,2,11,19) | $d_2$ = (0,-2)<br>$d_3$ = (30,16)<br>$d_4$ = (1,2)<br>$d_5$ = (11,19) |
| ج | 2 | 7,8 | $d_6$ = (10,20)<br>d7 = (-4,-8) | C = (10,20,-4,-8) | 101100011 | 3 | 011 | 3 | -3 | 8 | (10,20,-5,-8) | $d_6$ = (10,20)<br>$d_7$ = (-5,-8) |

**توصیف نمادهای استفاده‌شده**

| توضیحات | علامت |
|---|---|
| تعداد بلوک‌های پیشگویی برای ساخت بردار حمل کننده | N |
| رشته اطلاعات مخفی اصلی | m |
| بردار حرکت بلوک i ام قبل از جاسازی اطلاعات | $d_i$ |
| بردار حمل کننده قبل از جاسازی | C |
| تعداد بیت‌های قابل مخفی‌سازی در آن CTU | L |
| زیر رشته اطلاعات مخفی جهت جاسازی در CTU | S |
| مقدار دسیمال زیر رشته اطلاعات مخفی | F |
| شماره‌ی درایه‌ای که در بردار حمل کننده باید تغییر کند | d |
| بردار حمل کننده بعد از جاسازی | $\bar{C}$ |
| بردار پیشگویی بلوک i ام بعد از جاسازی اطلاعات | $\bar{d}_i$ |
| شماره‌ی بلوک‌های کاندید | Z |
| شماره‌ی بلوک حمل کننده | T |

**شکل ۵: مثالی از جاسازی اطلاعات در بردارهای حرکت با استفاده از روش پیشنهادی. (الف) N = 2 (ب) N =8 (ج) N =4**

### ۳-۳- بازیابی اطلاعات جاسازی شده

برای بازیابی اطلاعات جاسازی شده، ابتدا نیاز است تا بررسی شود که آیا در CTU اطلاعات، جاسازی شده است یا نه. برای بازیابی نیز از تابع Gبرای تولید عدد تصادفی r استفاده می‌گردد که این تابع از کلید رمز Kبه عنوان کلید مشترک بین فرستنده و گیرنده استفاده می‌نماید تا عدد r یکسان با مبدأ تولید نماید. در صورتی که r از مقدار e کوچک‌تر بود در نتیجه آن CTU شامل اطلاعات جاسازی شده است.

با توجه به مقدار r پارامتر N از رابطه‌ی ۱ محاسبه شده و Nتا از کوچک‌ترین بلوک‌های پیشگویی که دارای بردار حرکت است (به جز حالت ادغام و پرش) انتخاب شده تا بردار $C'=(c_1,c_2,\ldots,c_{2N})$ را تشکیل دهند، سپس مقدار S از رابطه‌ی ۵ محاسبه می‌گردد:

$$S = SUM(c' \otimes w) \bmod 2^L \qquad (۵)$$

در اینجا S مقدار دسیمال رشته‌ی جاسازی شده است و می‌توان آن را به یک عدد باینری به طول L تبدیل کرد. بعد از استخراج تمام اطلاعات جاسازی شده در CTU ها می‌توان با اتصال این رشته‌ها، کل اطلاعات جاسازی شده را بازیابی نمود.

برای روشن‌تر شدن مطلب یک مثال از بازیابی اطلاعات جاسازی شده ارائه می‌شود. شرایط همانند مثال بیان شده در شکل ۵ در نظر گرفته شده است. ابتدا با توجه به مقدار N، تعداد بلوک‌های پیشگویی برای ساخت بردار C' انتخاب می‌گردد. در مورد شکل ۵ (ب) مقدار N = 4 است، در نتیجه ۴ تا از کوچک‌ترین بلوک‌های پیشگویی انتخاب گردیده و بردار حمل کننده‌ی C'= (0, -2, 30, 16, 1, 2, 11, 19) به دست می‌آید. با جایگذاری مقدار N = 4 مقدار L برابر ۴ به دست می‌آید. در نتیجه مقدار S = (0×1)+ (-2×2)+ (30×3)+ (16×4)+ (1×5)+ (2×6)+ (11×8)+ (19×8) = 396 mod $2^4$ = 12 از رابطه‌ی ۵ به‌دست می‌آید که اگر آن را به عدد باینری به طول L تبدیل نماییم، رشته‌ی "1100" که در واقع همان عدد مخفی است، به دست می‌آید. بعد از بازیابی و کنار هم قرار دادن اطلاعات جاسازی شده در هر سه CTUمی‌توان کل اطلاعات جاسازی شده را به صورت "111100011" به دست آورد.

## ۴- پیاده سازی و تحلیل نتایج

در این بخش، روش پیشنهادی با ویدئوهای مختلف ارزیابی می‌شود. هدف از این کار محاسبه‌ی کارایی روش پیشنهادی در استاندارد فشرده‌سازی HEVC است.

### ۴-۱- شرایط آزمایش

تمامی آزمایش‌ها روی آخرین نسخه‌ی نرم افزار مرجع HEVC، یعنی HM 16.20 انجام شده است [۱۹]. ساختار رمزگذار Encoder-low-delay جهت پیشگویی بین قابی استفاده شده است که تنظیمات آن طبق شرایط مشترک در [۲۰] انجام شده است. برای کد کردن از ۱۰ ویدئوی مختلف با رزولوشن‌های متفاوت که هر یک دارای بافت‌های متفاوتی می‌باشند استفاده شده است. ۱۰۰ فریم اول از هر ویدئو برای کد کردن در نظر گرفته شد و سه بار هر ویدئو با سه پارامتر چندی شدن مختلف ۱۶، ۲۲ و ۲۸ کد شده و روش پیشنهادی با آن‌ها ارزیابی شده است.

### ۴-۲- پارامترهای مورد ارزیابی

جهت ارزیابی روش پیشنهادی از چهار پارامتر استفاده شده است که در ادامه هر یک شرح داده می‌شود:

**ظرفیت جاسازی:** این پارامتر متوسط بیت‌های جاسازی شده در هر فریم را نشان می‌دهد که از رابطه‌ی ۶ به دست می‌آید.

$$R = \frac{r}{N} \qquad (۶)$$

در رابطه فوق r تعداد کل بیت‌های جاسازی شده و N تعداد کل فریم‌ها است.

**جدول ۱: ظرفیت جاسازی روش پیشنهادی**

| ویدئو | QP | R (bit/frame) |
|---|---|---|
| Basketballpass ۴۱۶×۲۴۰ | ۱۶ | ۱۲۴ |
| | ۲۲ | ۹۴ |
| | ۲۸ | ۵۲ |
| BQsquare ۴۱۶×۲۴۰ | ۱۶ | ۱۷۲ |
| | ۲۲ | ۲۲۴ |
| | ۲۸ | ۱۸۸ |
| RaseHorses ۸۳۲×۴۸۰ | ۱۶ | ۲۸۴ |
| | ۲۲ | ۱۷۴ |
| | ۲۸ | ۱۰۸ |
| PartyScene ۸۳۲×۴۸۰ | ۱۶ | ۱۹۶ |
| | ۲۲ | ۱۳۲ |
| | ۲۸ | ۵۶ |
| BQMall ۸۳۲×۴۸۰ | ۱۶ | ۲۴۲ |
| | ۲۲ | ۱۷۸ |
| | ۲۸ | ۸۴ |
| Fourpeople ۱۲۸۰×۷۲۰ | ۱۶ | ۵۵۴ |
| | ۲۲ | ۵۸۲ |
| | ۲۸ | ۳۲۶ |
| Kimono ۱۹۲۰×۱۰۸۰ | ۱۶ | ۱۳۳۸ |
| | ۲۲ | ۱۰۰۸ |
| | ۲۸ | ۷۴۴ |
| BasketballDrive ۱۹۲۰×۱۰۸۰ | ۱۶ | ۱۱۳۲ |
| | ۲۲ | ۹۴۰ |
| | ۲۸ | ۴۲۸ |
| Peopleonstreet ۲۵۶۰×۱۶۰۰ | ۱۶ | ۲۸۲۴ |
| | ۲۲ | ۲۱۴۸ |
| | ۲۸ | ۱۴۹۸ |
| Traffic ۲۵۶۰×۱۶۰۰ | ۱۶ | ۱۹۵۲ |
| | ۲۲ | ۲۸۸۶ |
| | ۲۸ | ۲۱۵۲ |
| میانگین | --- | ۷۶۲ |

**نرخ بیت:** این پارامتر میزان افزایش یا کاهش نرخ بیت ویدئوی کد شده در استاندارد HEVC در حالتی که حامل اطلاعات مخفی است، نسبت به حالتی که حامل اطلاعات مخفی نیست را نشان می‌دهد. میزان افزایش نرخ بیت از رابطه‌ی **Error! Reference source not found.**۷ قابل محاسبه است [۵].

$$BRI = \frac{BR - BR'}{BR} \times 100 \qquad (۷)$$

در آن BR نرخ بیت کل ویدئو در حالتی که حامل اطلاعات مخفی نیست و 'BR نرخ بیت کل ویدئو در حالتی که اطلاعات در ویدئو مخفی شده است می‌باشد.

**PSNR**: برای بررسی تأثیر روش پیشنهادی بر کیفیت تصویر حامل اطلاعات مخفی از معیار PSNR استفاده می‌گردد. این معیار برحسب دسی‌بل است و از رابطه‌ی ۸ محاسبه می‌شود [۲۱]:

$$PSNR = 10\log_2\left(\frac{255^2}{MSE}\right) \qquad (۸)$$

که در آن MSE[۹] مجموع مربعات اختلاف بین تصویر حامل اطلاعات و تصویر پوششی است و از رابطه‌ی ۹ به دست می‌آید:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(S[i][j] - C[i][j])^2 \qquad (۹)$$

که در آن i و j مختصات تصویر، M و N ابعاد تصویر و S و C به ترتیب تصاویر پوششی و حامل هستند. هر چه اختلاف بین تصویر اصلی و تصویر پوششی کمتر باشد MSE کاهش یافته و PSNR افزایش می‌یابد، در نتیجه هر چه مقدار PSNR بیشتر باشد، یعنی اعوجاج تصویر کمتر و کیفیت تصویر بهتر است.

**جدول ۲: مقایسه کیفیت و معیار تشابه ویدئوها قبل و بعد از جاسازی اطلاعات با روش پیشنهادی**

| ویدئو | QP | بدون جاسازی اطلاعات | | با جاسازی اطلاعات | |
|---|---|---|---|---|---|
| | | PSNR | MSSIM | PSNR | MSSIM |
| Basketballpass ۴۱۶×۲۴۰ | ۱۶ | ۴۷٫۲۱ | ۰٫۹۹۰۷ | ۴۷٫۱۷ | ۰٫۹۸۹۲ |
| | ۲۲ | ۴۳٫۶۶ | ۰٫۹۷۵۸ | ۴۳٫۶ | ۰٫۹۷۴۳ |
| | ۲۸ | ۳۹٫۹۱ | ۰٫۹۴۱۳ | ۳۹٫۸۷ | ۰٫۹۳۹۹ |
| BQsquare ۴۱۶×۲۴۰ | ۱۶ | ۴۵٫۰۷ | ۰٫۹۸۶۳ | ۴۵٫۰۱ | ۰٫۹۸۴۷ |
| | ۲۲ | ۴۲٫۳۹ | ۰٫۹۵۱۲ | ۴۲٫۳۷ | ۰٫۹۴۹۹ |
| | ۲۸ | ۳۸٫۳۵ | ۰٫۹۳۷۷ | ۳۴٫۲۵ | ۰٫۹۳۶۱ |
| RaseHorses ۸۳۲×۴۸۰ | ۱۶ | ۴۵٫۱۷ | ۰٫۹۹۲۱ | ۴۵٫۱۱ | ۰٫۹۹۰۷ |
| | ۲۲ | ۴۲٫۰۶ | ۰٫۹۷۶۲ | ۴۲٫۰۴ | ۰٫۹۷۴۹ |
| | ۲۸ | ۳۸٫۶۲ | ۰٫۹۲۴۷ | ۳۸٫۵۶ | ۰٫۹۲۳۲ |
| PartyScene ۸۳۲×۴۸۰ | ۱۶ | ۴۴٫۳۷ | ۰٫۹۸۸۴ | ۴۴٫۳۳ | ۰٫۹۸۷ |
| | ۲۲ | ۴۰٫۸۲ | ۰٫۹۷۱۶ | ۴۰٫۷۸ | ۰٫۹۷۰۲ |
| | ۲۸ | ۳۷٫۶۵ | ۰٫۹۳۴۹ | ۳۷٫۶۱ | ۰٫۹۳۳۴ |
| BQMall ۸۳۲×۴۸۰ | ۱۶ | ۴۵٫۳۳ | ۰٫۹۸۳۱ | ۴۵٫۲۹ | ۰٫۹۸۱۶ |
| | ۲۲ | ۴۳٫۷۴ | ۰٫۹۷۲ | ۴۳٫۷۲ | ۰٫۹۷۰۶ |
| | ۲۸ | ۴۰٫۱۸ | ۰٫۹۶۱۳ | ۴۰٫۱ | ۰٫۹۵۹۷ |
| Fourpeople ۱۲۸۰×۷۲۰ | ۱۶ | ۴۶٫۱۵ | ۰٫۹۸۷۳ | ۴۶٫۱۱ | ۰٫۹۸۵۹ |
| | ۲۲ | ۴۳٫۶۷ | ۰٫۹۶۴۵ | ۴۳٫۶۵ | ۰٫۹۶۳۲ |
| | ۲۸ | ۴۰٫۵۵ | ۰٫۹۵۰۴ | ۴۰٫۵۱ | ۰٫۹۴۸۹ |
| Kimono ۱۹۲۰×۱۰۸۰ | ۱۶ | ۴۵٫۳۸ | ۰٫۹۷۴۶ | ۴۵٫۳ | ۰٫۹۷۲۹ |
| | ۲۲ | ۴۳٫۲ | ۰٫۹۶۳۸ | ۴۳٫۱۴ | ۰٫۹۶۱۸ |
| | ۲۸ | ۴۱٫۱۹ | ۰٫۹۴۷۲ | ۴۱٫۱۳ | ۰٫۹۴۵۶ |
| BasketballDrive ۱۹۲۰×۱۰۸۰ | ۱۶ | ۴۵٫۳۲ | ۰٫۹۷۴۳ | ۴۵٫۲۸ | ۰٫۹۷۲۸ |
| | ۲۲ | ۴۳٫۸۳ | ۰٫۹۳۸۵ | ۴۳٫۷۳ | ۰٫۹۳۶۵ |
| | ۲۸ | ۴۲٫۱۶ | ۰٫۹۱۵۶ | ۴۲٫۱ | ۰٫۹۱۴ |
| Peopleonstreet ۲۵۶۰×۱۶۰۰ | ۱۶ | ۴۶٫۹۲ | ۰٫۹۹۰۳ | ۴۶٫۸۴ | ۰٫۹۸۸۵ |
| | ۲۲ | ۴۴٫۶۱ | ۰٫۹۷۸۶ | ۴۴٫۵۷ | ۰٫۹۷۷ |
| | ۲۸ | ۴۲٫۲۴ | ۰٫۹۴۵۳ | ۴۲٫۱۸ | ۰٫۹۴۳۴ |
| Traffic ۲۵۶۰×۱۶۰۰ | ۱۶ | ۴۴٫۴۱ | ۰٫۹۸۹۱ | ۴۴٫۳۵ | ۰٫۹۸۷۵ |
| | ۲۲ | ۴۱٫۴۹ | ۰٫۹۷۸۸ | ۴۱٫۴۱ | ۰٫۹۷۶۹ |
| | ۲۸ | ۳۹٫۱۴ | ۰٫۹۵۱۱ | ۳۹٫۰۴ | ۰٫۹۴۹ |
| میانگین | --- | ۴۲٫۸۳ | ۰٫۹۶۴۶ | ۴۲٫۶۱ | ۰٫۹۶۲۹ |

**SSIM**[۱۰]: به منظور ارزیابی تشابه بین تصویر پوشش و تصویر حامل از SSIM استفاده می‌شود که از رابطه‌ی ۱۰ به دست می‌آید [۲۲]:

$$SSIM(S,C)=\frac{(2\mu_s\mu_c+C_1)(2\delta_{s,c}+C_2)}{(\mu_s^2+\mu_c^2+C_1)(\delta_s^2+\delta_c^2+C_2)} \qquad (۱۰)$$

که در اینجا $\mu_i$ متوسط شدت پیکسل‌های بلوک i ام، $\delta_i$ انحراف معیار شدت پیکسل‌های بلوک i و $\delta_{s,c}$، کوواریانس بین دو بلوک s و c است. همچنین $C_1$ و $C_2$ ثابت‌های پایداری می‌باشند. متوسط معیار SSIM برای کل ویدئو با MSSIM[۱۱] نشان داده می‌شود و از رابطه‌ی ۱۱ به دست می‌آید.

$$MSSIM(S,C)=\frac{1}{N}\sum_{K=1}^{N}SSIM(S_K,C_K) \qquad (۱۱)$$

که این رابطه $S_K$ و$C_K$ به ترتیب فریم $K$ ام از ویدئو است و $N$ تعداد کل فریم‌ها است. هر چه این شاخص به یک نزدیک‌تر باشد، شباهت بین دو تصویر بیشتر است.

### ۴-۳- تحلیل نتایج آزمایش‌ها

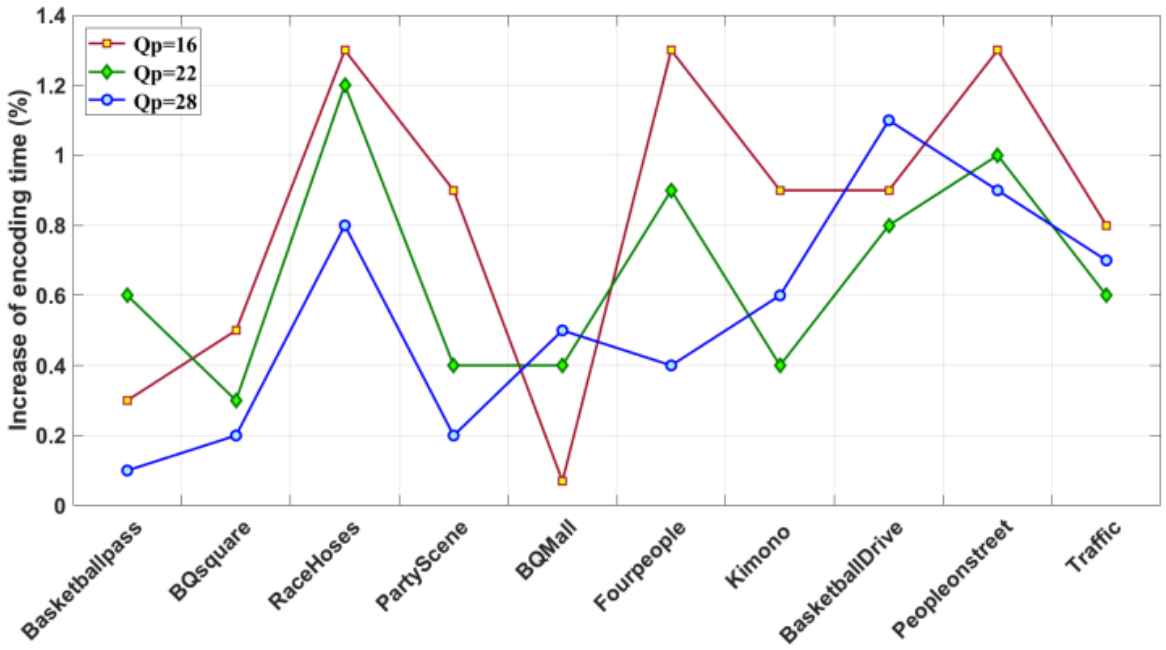
ظرفیت جاسازی داده برای هر فریم در جدول ۱ نشان داده شده است. همان‌طور که مشاهده می‌شود، ماکزیمم ظرفیت جاسازی ۲۸۸۶ بیت در هر فریم است. به دلیل آنکه ویدئوهای مختلف دارای رزولوشن مختلف و بافت متفاوت می‌باشند تعداد بلوک‌های پیشگویی در هر فریم متفاوت است در نتیجه ظرفیت جاسازی در هر فریم متفاوت خواهد بود. جدول ۲، PSNR و MSSIM تصویر حامل و تصویر پوششی را قبل و بعد از جاسازی اطلاعات، نشان می‌دهد. این معیارها برای مقادیر مختلف پارامتر چندی شدن اندازه گیری شده است. همان‌طور که در جدول ۲ نشان داده شده است تغییرات PSNR و MSSIM ویدئوها در حالتی که اطلاعات در آن جاسازی شده، تغییرات کمی دارد و میانگین کاهش در SSIM برابر ۰،۱۷ و در PSNR برابر ۰،۲۱ دسی‌بل است.

**جدول ۳: نسبت افزایش نرخ بیت ویدئوهای مختلف با پارامتر چندی شدن متفاوت**

| ویدئو | QP | بدون جاسازی اطلاعات (بایت) | با جاسازی اطلاعات (بایت) | BRI (%) |
|---|---|---|---|---|
| Basketballpass ۴۱۶×۲۴۰ | ۱۶ | ۶۱۰۷۸۵ | ۶۱۴۴۵۰ | ۰٫۶ |
| | ۲۲ | ۳۶۰۰۴۳ | ۳۶۱۱۲۳ | ۰٫۳ |
| | ۲۸ | ۱۳۰۷۱۲ | ۱۳۰۳۲۰ | -۰٫۳ |
| BQsquare ۴۱۶×۲۴۰ | ۱۶ | ۱۱۵۵۴۱۳ | ۱۱۴۸۴۸۱ | -۰٫۶ |
| | ۲۲ | ۴۵۴۷۸۲ | ۴۵۶۱۴۶ | ۰٫۳ |
| | ۲۸ | ۱۴۲۸۰۶ | ۱۴۳۶۶۳ | ۰٫۶ |
| RaseHorses ۸۳۲×۴۸۰ | ۱۶ | ۱۴۰۳۴۳۹ | ۱۴۳۲۹۱۱ | ۲٫۱ |
| | ۲۲ | ۶۴۹۷۰۷ | ۶۵۵۵۵۴ | ۰٫۹ |
| | ۲۸ | ۲۶۵۵۳۴ | ۲۷۰۳۱۴ | ۱٫۸ |
| PartyScene ۸۳۲×۴۸۰ | ۱۶ | ۶۲۷۹۴۹۲ | ۶۳۳۶۰۰۷ | ۰٫۹ |
| | ۲۲ | ۲۵۷۰۸۲۷ | ۲۵۹۳۹۶۴ | ۰٫۹ |
| | ۲۸ | ۹۷۸۳۳۶ | ۹۷۲۴۶۶ | -۰٫۶ |
| BQMall ۸۳۲×۴۸۰ | ۱۶ | ۳۹۵۳۸۲۹ | ۳۹۸۹۴۱۳ | ۰٫۹ |
| | ۲۲ | ۱۲۳۱۹۹۴ | ۱۲۴۶۷۷۸ | ۱٫۲ |
| | ۲۸ | ۴۸۱۴۵۸ | ۴۸۷۲۳۵ | ۱٫۲ |
| Fourpeople ۱۲۸۰×۷۲۰ | ۱۶ | ۸۷۳۲۹۵۲ | ۸۷۵۹۱۵۱ | ۰٫۳ |
| | ۲۲ | ۳۸۹۴۵۱۲ | ۳۹۲۹۵۶۳ | ۰٫۹ |
| | ۲۸ | ۱۰۷۳۱۹۷ | ۱۰۶۹۹۷۷ | -۰٫۳ |
| Kimono ۱۹۲۰×۱۰۸۰ | ۱۶ | ۱۱۴۲۳۲۲۱ | ۱۱۶۲۸۸۳۹ | ۱٫۸ |
| | ۲۲ | ۳۴۶۰۵۶۲ | ۳۴۹۱۷۰۷ | ۰٫۹ |
| | ۲۸ | ۱۴۷۶۲۸۱ | ۱۴۹۳۹۹۶ | ۱٫۲ |
| BasketballDrive ۱۹۲۰×۱۰۸۰ | ۱۶ | ۲۶۸۷۶۲۶۲ | ۲۶۴۷۳۱۱۸ | -۱٫۵ |
| | ۲۲ | ۴۸۹۳۷۳۰ | ۴۸۴۹۶۸۶ | -۰٫۹ |
| | ۲۸ | ۱۴۵۳۲۱۹ | ۱۴۵۷۵۷۹ | ۰٫۳ |
| Peopleonstreet ۲۵۶۰×۱۶۰۰ | ۱۶ | ۴۰۸۹۲۵۹۴ | ۴۱۹۹۶۶۹۴ | ۲٫۷ |
| | ۲۲ | ۱۵۷۴۲۲۸۶ | ۱۵۹۳۱۱۹۳ | ۱٫۲ |
| | ۲۸ | ۶۲۰۳۷۷۱ | ۶۳۱۵۴۳۹ | ۱٫۸ |
| Traffic ۲۵۶۰×۱۶۰۰ | ۱۶ | ۲۱۶۴۹۷۰۳ | ۲۱۸۴۴۵۵۰ | ۰٫۹ |
| | ۲۲ | ۵۹۷۰۶۱۱ | ۶۰۶۰۱۷۰ | ۱٫۵ |
| | ۲۸ | ۱۷۴۹۰۸۳ | ۱۷۷۵۳۱۹ | ۱٫۵ |
| میانگین | --- | --- | --- | ۰.۷۶ |

نسبت افزایش نرخ بیت ویدئوهای مختلف با پارامتر چندی شدن متفاوت در جدول ۳ نشان داده شده است. علامت‌های مثبت و منفی در جدول ۳ نشان دهنده افزایش یا کاهش در پارامتر مورد اندازه‌گیری است. از آنجایی که در روش پیشنهادی فقط اندازه‌ی یکی از مؤلفه‌های بردار حرکت ممکن است یک واحد کاهش یا افزایش داشته باشد، در نتیجه ممکن است نرخ بیت افزایش یا کاهش یابد

شکل ۶ نتایج نسبت افزایش زمان کد کردن بین روش پیشنهادی برای ویدئوهای مختلف به ازای پارامتر چندی‌شدن مختلف را نشان می‌دهد. همان‌طور که در شکل ۶ مشاهده می‌شود، اختلاف بین زمان کد کردن در استاندارد HEVC در حالت عادی که اطلاعات در آن جاسازی نشود با حالتی که اطلاعات در آن فریم با روش پیشنهاد جاسازی شود خیلی کم است؛ بنابراین تأثیر پیچیدگی زمانی آن ناچیز است و این یعنی روش پیشنهادی دارای کارایی بالایی است در حالی که محاسبات خیلی کمی را به سیستم تحمیل می‌کند.




**شکل ۶: میزان افزایش زمان کد کردن ویدئوهای مختلف در حالت جاسازی داده**

**جدول ۴: مقایسه روش پیشنهادی با کارهای مشابه در استاندارد HEVC**

| روش | نوع پیشگویی | عنصر انتخاب شده برای جاسازی اطلاعات | افزایش نرخ بیت | کاهش PSNR | ظرفیت جاسازی | F |
|---|---|---|---|---|---|---|
| Yang [5] | بین قابی | بلوکهای پیشگویی | ٪۶ | ۰٫۰۸ | ۱۶۱۵ | ۳۳۶۵ |
| Long [6] | بین قابی | علامت ضرایب باقی مانده بلوک تبدیل | ٪۲٫۲۵ | ۷٫۵۳ | ۵۷۹۳۸ | ۳۴۱۹ |
| Gui [11] | بین قابی | ضرایب باقی مانده‌ی بلوک تبدیل | ٪۱٫۲ | ۱٫۱۳ | ۵۲۷۹ | ۳۸۹۳ |
| Yang [14] | بین قابی | بردارهای حرکت | ٪۰٫۵۴ | ۰٫۴۱ | ۶۹۴ | ۳۱۳۴ |
| روش پیشنهادی | بین قابی | بردارهای حرکت | ٪۰٫۷۶ | ۰٫۲۱ | ۷۶۲ | ۴۵۷۷ |

جدول ۴ مقایسه بین روش پیشنهادی با روش‌هایی که اخیراً برای ویدئوهای فشرده شده پیشنهاد شده‌اند و همچنین از پیشگویی بین-قابی استفاده کرده‌اند را نشان می‌دهد. با توجه به این که روش‌های مختلف، ظرفیت جاسازی مختلفی به ازاء نرخ بیت و PSNR متفاوت گزارش کرده‌اند، مقایسه بین آنها عادلانه نیست. جهت مقایسه‌ی عادلانه از رابطه‌ی ۱۲ استفاده می‌شود تا نسبت جاسازی اطلاعات مخفی به افزایش نرخ بیت و کاهش PSNR به دست آید.

$$F = \frac{R}{d_{PSNR} \times BRI} \qquad (۱۲)$$

در رابطه‌ی فوق R ظرفیت جاسازی در هر فریم، $d_{PSNR}$ میزان کاهش PSNR و BRI میزان افزایش نرخ بیت را نشان می‌دهد. پارامتر F با ظرفیت جاسازی رابطه‌ی مستقیم و با افزایش نرخ بیت و کاهش PSNR رابطه‌ی عکس دارد. به عبارت دیگر هر چه نرخ بیت بعد از جاسازی اطلاعات، افزایش بیشتری داشته باشد مقدار F کاهش خواهد یافت و هر چه PSNR افزایش بیشتری داشته باشد نیز مقدار F کاهش خواهد یافت. مقادیر گزارش شده در جدول ۴ در همه‌ی روش‌ها به ازاء ۱۰۰ فریم از ویدئوهای یکسان است که در استاندارد HEVC کد شده-اند. همان طور که مشاهده می‌شود مقدار F روش پیشنهادی نسبت به چهار روش دیگر بیشتر است، که برتری روش پیشنهادی را نشان می-دهد. همچنین مقایسه روش پیشنهادی با مرجع [۱۴] نشان می‌دهد که علاوه بر اینکه ظرفیت جاسازی بیت‌های مخفی نسبت به مرجع [۱۴] بیشتر شده است کیفیت تصویر، کاهش کمتری داشته است که برتری روش پیشنهادی را نشان می‌دهد.

## ۵- نتیجه گیری

در این مقاله یک روش جدید برای مخفی‌سازی اطلاعات در ویدئوهایی که با استاندارد HEVC کد شده‌اند، ارائه شد. در روش پیشنهادی از بردارهای حرکت بلوک‌های پیشگویی بین‌قابی که برای کد کردن ویدئو در استاندارد HEVC تولید می‌شوند، جهت حمل اطلاعات مخفی استفاده شد. مزیت روش پیشنهادی در این است که حداکثر یکی از مؤلفه‌های بردار حرکت در یک CTU به اندازه‌ی یک واحد کاهش یا افزایش می‌یابد که تأثیر کمی روی کیفیت تصاویر حامل می‌گذارد. نتایج آزمایش‌ها نشان می‌دهد که روش پیشنهادی دارای نرخ جاسازی خوبی است در حالی که نرخ بیت افزایش چندانی نداشته و حتی ممکن است نرخ بیت کاهش نیز داشته باشد. مقایسه با کارهای اخیر نشان می‌دهد که روش پیشنهادی کمترین تأثیر را روی کارایی فشرده‌سازی استاندارد HEVC و کاربردهای بی‌درنگ دارد.

## مراجع


[1] P. Bo and Y. Jie, "A Reversible Information Hiding Method Based on HEVC," *IFAC-PapersOnLine*, vol. 51, pp. 238-243, 2018/01/01/ 2018.

[2] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Computers & Electrical Engineering*, vol. 70, pp. 380-399, 2018/08/01/ 2018.

[3] M. Khairullah, "A novel steganography method using transliteration of Bengali text," *Journal of King Saud University - Computer and Information Sciences*, 2018/02/17/ 2018.

[4] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing*, vol. 148, pp. 41-47, 2018/07/01/ 2018.

[5] Yang, Yiyuan, Zhaohong Li, Wenchao Xie, and Zhenzhen Zhang. "High capacity and multilevel information hiding algorithm based on pu partition modes for HEVC videos." Multimedia Tools and Applications, vol. 78, no. 7,pp. 8423-8446, 2019.

[6] M. Long, F. Peng, and H.-y. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, pp. 171-182, 2018.

[7] S. Swati, K. Hayat, and Z. Shahid, "A watermarking scheme for high efficiency video coding (HEVC)," *PloS one*, vol. 9, p. e105613, 2014.

[8] Li, Dong, Yingnan Zhang, Xinchao Li, Ke Niu, Xiaoyuan Yang, and YuJuan Sun. "Two-dimensional histogram modification based reversible data hiding using motion vector for H. 264." Multimedia Tools and Applications, vol. 78, no. 7, pp.8167-8181, 2019.

[9] Konyar, Mehmet Zeki, Orhan Akbulut, and Sıtkı Öztürk. "Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC." Signal, Image and Video Processing, pp.1-9, 2020.

[10] Xu, Dawen. "Commutative Encryption and data hiding in HEVC Video Compression." IEEE Access 7, pp. 66028-66041, 2019.

[11] F. Gui and H. Xue, "A Reversible Data Hiding Scheme for HEVC," in *Computational Intelligence and Design (ISCID), 2017 10th International Symposium on*, 2017, pp. 34-37.

[12] P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, "A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames," *Journal of Visual Communication and Image Representation*, vol. 25, pp. 239-253, 2014.

[13] J. Wang, R. Wang, W. Li, D. Xu, and M. Huang, "A high-capacity information hiding algorithm for HEVC based on intra prediction mode," *J. Comput. Inform. Syst*, vol. 10, pp. 8933-8943, 2014.

[14] Yang, Jie, and Songbin Li. "An efficient information hiding method based on motion vector space encoding for HEVC." Multimedia Tools and Applications, vol. 77, no. 10, pp. 11979-12001, 2018.

[15] Dorfeshan, Navid, and Mohammadreza Ramezanpour. "Compressed Domain Scene Change Detection Based on Transform Units Distribution in High Efficiency Video Coding Standard." Journal of Computer & Robotics, vol. 11, no. 2, pp. 41-48, 2018.

[16] Heidari, Behnam, and Mohammadreza Ramezanpour. "Reduction of intra-coding time for HEVC based on temporary direction map." Journal of Real-Time Image Processing, pp. 1-13, 2019.

[17] Najafabadi, Narjes, and Mohammadreza Ramezanpour. "Mass center direction-based decision method for intraprediction in HEVC standard." Journal of Real-Time Image Processing, pp. 1-16, 2019.

[18] Fan, Li, Tiegang Gao, Qunting Yang, and Yanjun Cao. "An extended matrix encoding algorithm for steganography of high embedding efficiency." Computers & Electrical Engineering, vol. 37, no. 6, pp. 973-981, 2011.

[19] J.-V. HEVC. (2018). *High Efficiency Video Coding (HEVC)*. Available Online at: https://hevc.hhi.fraunhofer.de/trac/hevc/browser/tags/HM-16.18

[20] F. Bossen, "Common test conditions and software reference configurations," *JCTVC-L1100*, vol. 12, 2013.

[21] S. Sharda and S. Budhiraja, "Image steganography: A review," *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, vol. 3, pp. 707-710, 2013.

[22] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, pp. 600-612, 2004.


## زیرنویس‌ها

[1] Steganography

[2] Discrete Cosine Transform

[3] Discretei Wavelet Transform

[4] High Efficiency Video Coding

[5] Advanced Video Coding
[6] Coding Tree Unit (CTU)
[7] Coding Unit (CU)
[8] Prediction Unit (PU)
[9] Mean Squared Error
[10] Structural Similarity
[11] Middle Structural Similarity