

نهان نگاری ویدیوی خام مبتنی بر آشکارسازی مناسب با مصالحه بین پارامترهای

شفافیت، مقاومت و ظرفیت

رضا اصفهانی^۱، زین العابدین نوروژی^{۲*}، محمدعلی اخایی^۳

۱- استادیار و ۲- دانشیار، دانشگاه جامع امام حسین (ع)، ۳- استادیار، دانشگاه تهران

(دریافت: ۹۷/۹/۱۴، پذیرش: ۹۸/۳/۲۸)

چکیده

یکی از ضعف‌های عمده الگوریتم‌های نهان نگاری، عدم تخمین مناسب در سمت گیرنده از داده‌ها در آشکارسازی می‌باشد. آشکارسازی مناسب در الگوریتم نهان نگاری، با مصالحه سه پارامتر شفافیت، مقاومت، ظرفیت ارتباط مستقیم دارد. الگوریتم پیشنهادی، مصالحه مناسبی بین این سه پارامتر ایجاد می‌کند که با توجه به این موضوع، در این مقاله برای حفظ شفافیت، از درج اطلاعات به شیوه طیف‌گسترده در ضرایب فرکانس میانی موجک استفاده شده است. با به دست آوردن پارامتر ضریب قدرت مناسب درج اطلاعات (α)، از کاهش مقاومت جلوگیری شده است. سنجش مناسب بودن α نیز توسط نرخ بیت خطا ارزیابی شده است. دو مرحله تنظیم ظرفیت مناسب در یک پوشانه و پوشش کامل درج داده‌های محرمانه، دو مرحله‌ی پیشنهادی است که مربوط به پارامتر ظرفیت می‌باشد. در مرحله اول، ظرفیت مناسب به معنی مصالحه مناسب پارامتر ظرفیت با پارامتر شفافیت است، یعنی نهان نگاری دارای مقادیر مناسب پارامترهای SSIM و PSNR باشد. اگر از پوشانه با آنتروپی پایین استفاده گردد، نتیجه آن ظرفیت پایین ولی مقاومت بالا است. در این وضعیت نرخ بیت خطا کاهش یافته و این به معنی نزدیک شدن به مقدار مناسب α و به عبارتی مقاومت مناسب است. برای جلوگیری از کاهش ظرفیت و برای پوشش کامل درج داده‌های محرمانه، استفاده از فریم‌های ویدیوی خام پیشنهاد شده است. امکان دارد داده‌های محرمانه دارای حجم بالایی باشند و یک پوشانه کافی نباشد و نیاز به بانک پوشانه خواهد بود. از آنجا که ممکن است تهیه بانک تصاویر دارای خواص آماری مناسب نزدیک به هم، کاری مشکل و زمان‌بر باشد، از فریم‌های ویدیوی خام استفاده شده است.

کلمات کلیدی: طیف گسترده، آشکارسازی مناسب، ضرایب فرکانس میانی تبدیل موجک، مقاومت، نرخ خطای بیت

۱. مقدمه

مقاله استفاده از نهان نگاری به روش طیف‌گسترده ضریب در ضرایب فرکانس میانی تبدیل موجک است. در دو مقاله [۲-۳] نهان نگاری در حوزه DWT است و پارامتر مقاومت بیشتر مورد نظر است. در مقاله [۴] مبتنی بر DWT و تجزیه مقدار منفرد^۲ نهان نگاری صورت گرفته است. مقاله [۵] یک نوع بهبود یافته از حوزه DWT را معرفی کرده است. در مرجع [۶] براساس طراحی یک مدل بصری رنگی است و پارامترهای مقاومت، شفافیت و ظرفیت دارای مصالحه مناسبی هستند. در مقاله [۷] نیز براساس DWT بوده و از شفافیت و مقاومت مناسبی برخوردار است که با هم مصالحه به نسبت خوبی را فراهم نموده‌اند.

نهان نگاری در ضرایب فرکانس میانی تبدیل موجک سبب شفافیت روش خواهد شد، ولی به دلیل حساسیت ضرایب فرکانس میانی، الگوریتم قادر به برخورداری از مقاومت بالا نیست. در کانالی مانند اسکایپ که کد کانال را نداریم و نرخ پایین مطرح است دیگر نمی‌توان از روش‌هایی هم چون LSB

نهان نگاری در فریم ویدیوی یکی از راه‌حل‌های موثر برای مقابله با بسیاری از مسائل هم‌چون مخفی کردن اطلاعات بدون ایجاد حساسیت است، به طوری که همواره بین سه ویژگی مهم مقاومت^۱، غیرقابل مشاهده بودن و ظرفیت نوعی مصالحه برقرار گردد. آشکارسازی مناسب، تخمین مناسب داده‌های محرمانه از سیگنال دریافتی در گیرنده است. در واقع سیگنال نهان نگاری شده از کانال نویزی عبور کرده و با حفظ شفافیت، مقاومت و ظرفیت مناسب، به مقصد می‌رسد. مقاله [۱] یک آشکارساز مناسب در حوزه LSB است. مهم‌ترین ویژگی‌های یک نهان نگاری معتبر، ایجاد ظرفیت مناسب جهت درج اطلاعات محرمانه، نامحسوس بودن نهان نگاره، مقاومت آن در مقابل حمله‌های مختلف و حفظ شفافیت^۲ می‌باشد. ایده اصلی در این

*نویسنده پاسخگو: znorozi@ihu.ac.ir

1- Robustness
2- Transparency

3- Singular Value Decomposition (SVD)

احتمال خطا و ظرفیت به سادگی روش جمعی نیست و دیگر نمی‌توان از روابط تئوری اطلاعات و مخبرات بهره برد و نیاز به طراحی آشکارسازی مناسب دارد. در روش ضربی هرچه تبدیل مورد نظر سیگنال پوشانه را به صورت تنک‌تر^۲ نمایش دهد، عملکرد روش نهان‌نگاری در آن حوزه بهتر می‌گردد [۱۶]. در این مقاله حالت نیمه‌کور استفاده از اطلاعاتی مانند میانگین و واریانس پوشانه در گیرنده (بخش استخراج اطلاعات) در نظر گرفته و در تبدیل موجک از فیلتر هار^۳ استفاده شده است. از مهم‌ترین خواص تبدیل موجک به موارد زیر اشاره می‌کنیم:

۱. تبدیل موجک نسبت به تبدیل DCT به سیستم بینایی انسان نزدیک‌تر است و تغییرات حاصل از نویز و فشرده‌سازی در آن کم‌تر به چشم می‌آید. اعوجاج‌های ناشی از بلوکی کردن در تبدیل DCT، در تبدیل موجک کم‌تر به وجود می‌آید. تبدیل موجک توصیف چند رزولوشنی^۴ سیگنال است و کدگشایی^۵ به صورت سلسله مراتبی از یک رزولوشن پایین‌تر به رزولوشن بالاتر انجام می‌گیرد.

۲. این تبدیل مدل بینایی بهتری را در اختیار قرار می‌دهد و نسبت به تبدیل DCT، تبدیل دقیق‌تری به منظور پردازش زیرباندها، به صورت مستقل است.

۳. تبدیل موجک دارای ساختار شناخته شده‌ای به نام نمایش مکان-مقیاس است. در این ساختار بخش‌های فرکانس پایین تصویر در زیرباند تقریب LL و بخش‌های فرکانس میانی در زیرباندهای جزییات HL و LH نمایان می‌گردند. لبه‌های تیز تصویر که دارای مولفه‌های فرکانس میانی قوی هستند، در زیرباندهای جزییات به چشم می‌خورند.

به طور کلی نهان‌سازی اطلاعات در ضرایب زیرباند تقریب LL در برابر حملات مقاوم‌تر است، اما در این حالت میزان کاهش کیفیت تصویر زیاد است. نهان‌سازی در باند HH موجک از نظر سیستم بینایی انسان قابل درک نیست، اما در برابر حملات آسیب‌پذیر است. نهان‌سازی در زیرباندهای HL و LH مصالحه‌ای بین کیفیت و آسیب‌پذیری است. روش‌های جایگزینی در دامنه موجک به اندازه روش‌های حوزه DCT مورد بررسی و تحلیل قرار نگرفته‌اند.

در این مقاله از شباهت بیشینه (ML) برای آشکارسازی مناسب بهره‌برداری شده است. تخمین شباهت بیشینه (MLE) روشی برای محاسبه و تخمین پارامترهای یک مدل آماری است،

بهره برد، بلکه استفاده از طیف‌گسترده مناسب‌تر است. در مقاله [۸] بر موضوع طیف‌گسترده پرداخته ولی در این تحقیق، نشان‌گذاری مورد بحث قرار گرفته است. در مرجع [۹] یک آشکارساز محلی به روش ضربی به کمک مدل بینایی انسان در ضرایب حوزه موجک طراحی و بررسی شده است. این مقاله بیش‌تر به مقوله نشان‌گذاری پرداخته است. مقاله [۱۰] بیش‌تر بر روی تحلیل نهان‌نگاری طیف‌گسترده با توجه به میزان روشنایی پنجره‌ها (اندازه ماتریس‌ها) برای هر تصویر متمرکز شده است.

در ادامه کلاس‌بندی مقاله به شرح زیر است. در بخش دوم اولیه‌های مورد نیاز که در مقاله از آن استفاده شده، ارائه گردیده است. راه‌کار پیشنهادی برای نهان‌نگاری با آشکارسازی مناسب با توجه به سه پارامتر اصلی شفافیت، مقاومت و ظرفیت در بخش سوم ارائه شده است و بخش چهارم به نتایج شبیه‌سازی‌ها پرداخته‌ایم.

۲. اولیه‌های مورد نیاز

توانایی روش نهان‌نگاری به روش طیف‌گسترده تصاویر^۱ (SSIS) در تحمل تداخلات ناخواسته بسیار بالا است. در این مقاله برای گسترش طیف سیگنال پیام در پوشانه، از روش گسترش هر بیت در پنجره‌های مشخص شده که دارای خواص آماری مناسبی از نظر همبستگی متقابل پایین هستند، استفاده شده است. روش نهان‌نگاری طیف‌گسترده تصاویر ترکیب چند تکنیک مختلف همانند کدگذار خطا، بازیابی تصویر و ارتباط طیف‌گسترده می‌باشد [۱۱]. این روش دارای محاسبات پیچیده‌ای است که با طراحی آشکارسازی مناسب می‌توان عملکرد سیستم را به صورت ریاضی تحلیل کرد. اگرچه نسخه‌های متفاوتی برای درج در نهان‌نگاری روش طیف‌گسترده ارائه شده است و اساس این مقاله بخشی از مدل اصلی در مقاله [۱۲]، مورد نظر بوده است. نهان‌نگاری در این روش به دو صورت جمعی [۱۳] و ضربی قابل انجام است. روش ضربی مبتنی بر مدل بوده و با ویژگی‌های بینایی و شنیداری انسان کاملاً منطبق است [۱۴-۱۵]. همین عامل سبب موفقیت این الگوریتم نسبت به روش‌های جمعی شده است. در نهان‌نگاری ضربی دو حالت آشکارسازی کور و نیمه‌کور وجود دارند که در روش پیشنهادی از حالت نیمه‌کور بهره برده‌ایم. همان‌طور که در جدول (۱) بخش نتایج تجربی قابل مشاهده است، روش ضربی در مقایسه با روش جمعی در حوزه مکان دارای درصد آشکارسازی کم‌تری است زیرا مناسب‌سازی پارامتر ضریب قدرت درج اطلاعات و یا به دست آوردن روابط

2- Sparse

3- Haar

4- Approximation Subband

5- Decode

6- Maximum Likelihood

7- Maximum Likelihood Estimation

1- Spread Spectrum Image Steganography (SSIS)

نویز و سایر عوامل مزاحم، سبب به‌اشتباه انداختن گیرنده در تشخیص بیت می‌شوند و به‌طور کلی میزان سلامت سامانه مخابراتی را می‌توان در انتقال با کم‌ترین اشتباه در مقصد سنجید، به‌همین منظور تعداد نسبی بیت‌های استخراج شده اشتباه، تعیین‌کننده نرخ خطای بیت (BER) است. در این مقاله از BER برای ارزیابی آشکارسازی بهره‌گرفته شده است.

۳. روش پیشنهادی

در روش پیشنهادی راه‌کاری برای نهان‌نگاری تصویر در حوزه تبدیل ارائه شده است، به‌طوری‌که دارای آشکارسازی مناسب در گیرنده بوده و علاوه بر بالا بودن مقاومت و امنیت این روش در برابر حملات، ظرفیت سیگنال پوشانه نیز پاسخ‌گوی حجم داده‌های محرمانه جهت جاسازی پیام می‌باشد. در بسیاری از پژوهش‌ها برای افزایش مقاومت روش، از نهان‌نگاری در اطلاعات فرکانس پایین سیگنال استفاده می‌شود. اگرچه چنین سیستمی از نقطه نظر مقاومت عملکرد مناسبی خواهد داشت، ولی از نظر امنیت و شفافیت بسیار آسیب‌پذیر خواهد بود [۱۷-۱۸]. راه‌کاری که در این مقاله پیشنهاد می‌شود، استفاده از ضرایب فرکانس مینای تبدیل گسسته مویک برای ایجاد شفافیت مناسب استفاده شده است. روش تبدیل مویک یکی از روش‌های حوزه تبدیل است که در مقالات از آن استفاده می‌شود. در مقاله [۱۹] یک روش نهان‌نگاری بر مبنای تبدیل مویک است، که براساس الگوریتم ژنتیک در حوزه تبدیل مویک کار شده است و ظرفیت بالا در آن مورد نظر است. نهان‌نگاری بر اساس تبدیل مویک یکی از مواردی است که باب پژوهشی آن باز است و تقریباً هر ساله مقالاتی مانند [۲۰] در این حوزه انتشار می‌یابند که برای افزایش مقاومت، از نهان‌نگاری در اطلاعات فرکانس پایین سیگنال استفاده می‌شود. اگرچه چنین سیستمی از نقطه نظر مقاومت عملکرد مناسبی خواهد داشت، ولی از نظر امنیت و شفافیت بسیار آسیب‌پذیر خواهد بود. عموماً بیش‌تر انرژی تصویر در زیرباند‌هایی با فرکانس پایین LLX متمرکز شده است، بنابراین درج نهان‌نگاره در این زیرباند، مقاومت را به‌طور قابل ملاحظه‌ای افزایش خواهد داد ولی در واقع از کیفیت تصویر می‌کاهد، لذا درج نهان‌نگاری در زیرباند‌هایی با فرکانس مینای کیفیت را کاهش نمی‌دهد ولی از مقاومت خوبی برخوردار نیست. به‌همین علت در این مقاله درج نهان‌نگاری در زیرباند‌هایی با فرکانس مینای پیشنهاد می‌شود. در روش پیشنهادی برای ارتقاء شفافیت نهان‌نگاری از ضرایب فرکانس مینای مبتنی بر طیف‌گسترده ضربی استفاده شده است که توان نهان‌نگاره متناسب با توان

که واریانس و میانگین را مجهول در نظر می‌گیرد، آن‌گاه مقادیری را به آن‌ها نسبت می‌دهد که با توجه به اطلاعات موجود محتمل‌ترین حالت باشد. اصول کار به‌شرح زیر است: فرض کنیم n مشاهده x_1, x_2, \dots, x_n وجود داشته باشد که مستقل از هم و دارای توزیع احتمال نامشخص f_0 باشند. به‌طور محتمل متعلق به یک خانواده مشخص از توزیع‌های نرمال مانند $\{f(0|\theta), \theta \in \Theta\}$ می‌باشد که مدل پارامتری نامیده می‌شود، بنابراین، $f(0|\theta) = f_0$ می‌باشد و $\Theta = \{\theta_0, \theta_1, \dots, \theta_q\}$ متغیر ثابت و ناشناخته است که باید تخمین زده شود. مقدار θ_0 نامعلوم است و به‌عنوان مقدار صحیح پارامتر در نظر گرفته می‌شود. حال می‌خواهیم تخمین‌گری چون $\hat{\theta}$ بیابیم که تا حد امکان به‌مقدار صحیح یعنی θ_0 نزدیک باشد. هم x_i ‌ها و هم پارامتر θ هر دو می‌توانند بردار باشند. برای استفاده از روش شباهت بیشینه ابتدا باید تابع چگالی توام را برای همه‌ی مشاهدات مشخص کنیم. برای حالتی که توزیع‌ها مستقل و یکنواخت باشند، تابع چگالی توام به‌صورت زیر است:

$$f(x_1, x_2, \dots, x_n | \theta) = f(x_1 | \theta) \cdot f(x_2 | \theta) \dots f(x_n | \theta) \quad (1)$$

در نگاه دیگر، می‌توان گفت مشاهدات x_1, x_2, \dots, x_n پارامترهای ثابت و θ پارامتر متغیر این تابع است و از این منظر این تابع توزیع، تابع شباهت نامیده می‌شود. در عمل راحت‌تر است که از رابطه زیر استفاده شود.

$$L(\theta | x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n | \theta) = \prod_{i=1}^n f(x_i | \theta) \quad (2)$$

که لگاریتم شباهت نامیده می‌شود و نمونه‌ی ترازشده آن معادله (۳) است، که میانگین شباهت لگاریتمی نامیده می‌شود.

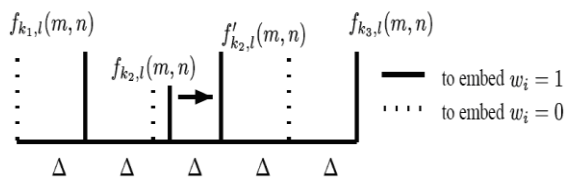
$$\ln L(\theta | x_1, x_2, \dots, x_n) = \sum_{i=1}^n \ln f(x_i | \theta), \quad \hat{\ell} = \frac{1}{n} \ln L \quad (3)$$

در واقع $\hat{\ell}$ مقدار لگاریتم شباهت انتظاری یک مشاهده‌ی منفرد را در مدل بیان می‌کند. روش شباهت بیشینه، عبارت θ_0 را با یافتن مقداری از θ که $\hat{\ell}(\theta | x)$ را بیشینه کند، تخمین می‌زند. برای بسیاری از مدل‌ها می‌توان MLE را به‌صورت تابعی صریح از داده‌های مشاهده شده x_1, x_2, \dots, x_n پیدا کرد. اما در بسیاری از مسایل پیدا کردن یک فرم بسته برای تابع شباهت ممکن نیست و باید از روش‌های عددی برای یافتن MLE استفاده کرد. ویژگی‌های MLE را می‌توان این‌طور بیان کرد که شباهت بیشینه یک تخمین‌گر، اکسترم بنا شده بر تابع هدف زیر است.

$$\hat{\ell}(\theta | x) = \frac{1}{n} \sum_{i=1}^n \ln f(x_i | \theta) \quad (4)$$

و مشابه نمونه‌ای آن شباهت لگاریتمی میانگین عبارت $\ell(\theta) = E[\ln f(x_i | \theta)]$ می‌باشد. در سیستم‌های دیجیتال اثر

قرار دادن اطلاعات نهان استفاده نموده که مبتنی بر کوانتیزاسیون است. در این تکنیک بازه اعداد حقیقی به تعدادی نقطه با فاصله Δ تقسیم می‌شود و ضرایب دامنه موجک به نزدیک‌ترین نقطه بازسازی^۱ (نقاط تعیین شده برای کوانتیزاسیون) جهت درج بیت موردنظر از اطلاعات نهان کوانتیزه می‌گردد. پارامتر Δ وظیفه‌ی تنظیم اندازه‌ی گام کوانتیزاسیون را بر عهده دارد شکل (۲). بالا بردن این پارامتر باعث بیش‌تر شدن مقاومت اطلاعات نهان و در ازای آن افزایش میزان تخریب تصویر می‌گردد.



شکل (۲): روش کوانتیزاسیون استفاده شده در روش‌های نهان‌نگاری [۲۱].

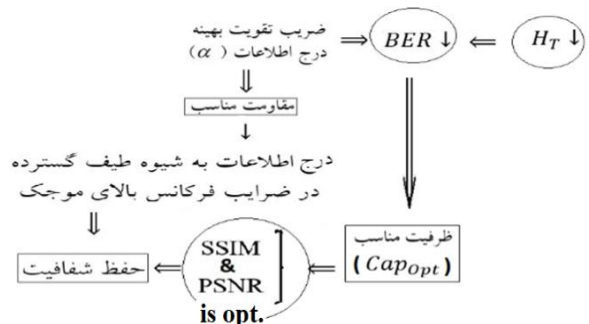
در قسمت درج، الگوریتم نهان‌نگاری به این‌صورت عمل می‌شود که سیگنال پوشانه به بلوک‌های غیرهمپوشان (بلوک‌هایی که دارای پیکسل مشترک نباشند) با طول N تقسیم می‌شود. سپس اطلاعات نهان با وزن‌دهی دامنه هر بلوک به شکل $x_i' = \frac{1}{\alpha} \times x$ (برای درج بیت صفر) یا $x_i' = \alpha \times x$ (برای درج بیت یک) درج خواهد شد. مقدار α (ضریب قدرت درج اطلاعات) باید به شکل $\alpha = 1 + \varepsilon$ باشد. مقادیر بزرگ‌تر α منجر به مقاومت بالاتر شده ولی کیفیت سیگنال نهان‌نگاری شده را پایین می‌آورند. استخراج آن در حالت نیمه کور (با داشتن بعضی ویژگی‌ها از سیگنال پاک) و یا کور (بدون داشتن بعضی ویژگی‌ها از سیگنال پاک) به شکل آشکارساز مناسب با شیوه‌هایی مانند ML به شکل رابطه (۵) قابل تخمین است.

$$P(y_1, y_2, \dots, y_N | 1) \geq \frac{1}{0} P(y_1, y_2, \dots, y_N | 0) \quad (5)$$

که در آن، $y = \alpha \cdot w + n$ ضرایب دریافتی حاوی بیت یک یا بیت صفر است. α ضریب قدرت موجک و n نویز گوسی سفید با میانگین صفر می‌باشد.

$$\begin{aligned} y_{11} &= \alpha w_1 + n_1 \rightarrow y_{11} \sim (\alpha \mu, \sigma_{y_{11}}^2) \\ y_{10} &= \alpha^{-1} w_1 + n_1 \rightarrow y_{10} \sim N(\alpha^{-1} \mu, \sigma_{y_{10}}^2) \\ \sigma_{y_{11}}^2 &= \alpha^2 \sigma^2 + \sigma_n^2 \\ \sigma_{y_{10}}^2 &= \alpha^{-2} \sigma^2 + \sigma_n^2 \end{aligned} \quad (6)$$

سیگنال تغییر خواهد کرد که این موضوع باعث کاهش مقاومت می‌شود. برای بهبود عملکرد مقاومت، در بسیاری از پژوهش‌ها از الگوریتم ML برای آشکارسازی داده استفاده شده است. راه‌کار اصلی پیشنهادی در این روش، نوآوری در ارائه الگوریتم آشکارسازی است که بتواند با کاهش خطای آشکارسازی نهان‌نگاره، مقاومت روش را افزایش دهد. برای استفاده از گیرنده مبتنی بر روش ML، مهم‌ترین بخش، مدل‌سازی ضرایب مورد نظر از سیگنال پوشانه می‌باشد. برای حفظ ظرفیت مناسب نیز استفاده از تصاویر پوشانه با آنتروپی پایین مطرح شده، ولی با توجه به این که ممکن است، داده‌های محرمانه دارای حجم بالایی باشند، و یک پوشانه تصویر کافی نباشد، استفاده از فریم‌های ویدئو برای پوشش کامل درج داده‌های محرمانه مطرح شده است شکل (۱).

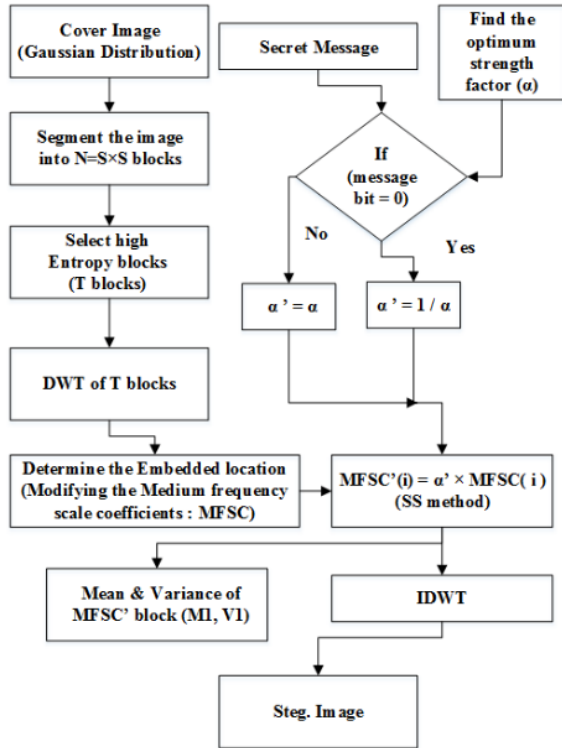


شکل (۱): ارتباط بین سه پارامتر شفافیت، مقاومت و ظرفیت در روش پیشنهادی.

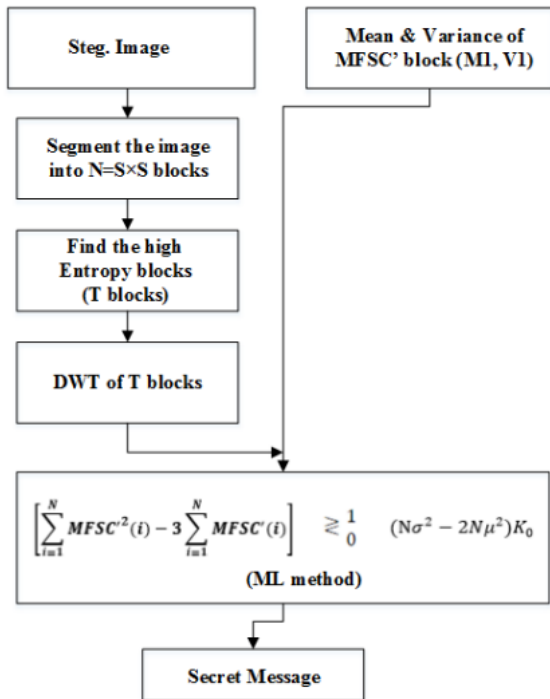
۳-۱. نهان‌نگاری نیمه‌کور با شفافیت مناسب و درج در ضرایب فرکانس میانی تبدیل موجک تصویر

در بین روش‌های نهان‌نگاری در حوزه تبدیل، روش‌های نهان‌نگاری در حوزه تبدیل موجک گسسته به علت خواص نظیر محلی‌سازی مکان-فرکانس، نمایش مالتی رزولوشن و پیچیدگی خطی محاسبات کارآمدتر هستند. این نوع از الگوریتم‌ها باند پایین را به‌عنوان نقاط مهم ادراکی برای قرار دادن اطلاعات نهان انتخاب می‌کنند و عموماً الگوریتم‌هایی با مقاومت بالا هستند و اکثراً بر اساس شیوه‌های مبتنی بر روش طیف‌گسترده عمل می‌کنند تا حداقل تغییر را در ضرایب این زیرباند موجب شوند، چون تغییر در ضرایب این زیرباند به‌شدت بر کیفیت تصویر تاثیر می‌گذارد. در این روش‌ها عموماً اطلاعات نهان را روی نویز قرار می‌دهند. اشکال اساسی در این روش‌ها عبارت است از این‌که ایجاد هرگونه اعوجاجی، اطلاعات نهان، حذف شده و به‌شدت کیفیت تصویر کاهش می‌یابند. ولی در روش پیشنهادی که به صورت عمومی از لبه‌ها (مناطق) از تصویر که تغییرات سطح خاکستری زیاد است) برای مخفی کردن اطلاعات نهان استفاده می‌کند، الگوریتمی است که از زیرباندهای با فرکانس میانی برای

در شکل (۳-الف) چگونگی ساختار عملیات جاسازی پیام و همچنین چگونگی ساختار عملیات استخراج داده در شکل (۳-ب) نشان داده شده است.



الف) ساختار جاسازی داده



ب) ساختار استخراج داده

شکل (۳): نهان نگاری در تصویر به شیوه موجک دوبعدی با سه سطح و فیلتر موجک هر

واریانس نویز σ_n^2 به شکل زیر تخمین زده می شود و اگر انحراف معیار نویز در سیگنال تصویر σ^2 باشد، این مقدار به کمک ضرایب جزئی تبدیل موجک (HH_1) به وسیله تخمین گر مقاوم میانه طبق مرجع [۲۲] قابل تخمین زدن است:

$$\sigma_{approx} = \frac{Median(|Y_i|)}{0.6745}; Y_i \in subband HH_1 \quad (7)$$

$$\|L\| \sigma_{approx} \rightarrow \|L\| = \sqrt{\sum_l \sum_k L^2(l,k)}$$

که در آن، L تقریب باند گسسته ضربه پاسخ است. با توجه به این که ضرایب تبدیل موجک در هر مرحله تجزیه، زیر نمونه می شوند، این ضرایب در مدل iid^۱ در نظر گرفته شده اند. در نتیجه توزیع این ضرایب در یک بلوک مشخص با N ضریب (y_1, y_2, \dots, y_N) بعد از درج بیت یک و بیت صفر طبق رابطه (۸) می باشد:

$$P(y_1, y_2, \dots, y_n | 1) = \prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y1}^2}} e^{\beta_1} \quad (8)$$

$$P(y_1, y_2, \dots, y_n | 0) = \prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y0}^2}} e^{\beta_0}$$

که در آن، $\beta_0 = \frac{(y_i - \alpha\mu)^2}{2\sigma_{y0}^2}$ و $\beta_1 = \frac{(y_i - \alpha\mu)^2}{2\sigma_{y1}^2}$ می باشند. با توجه به رابطه (۳)، آشکارساز مناسب با شیوه ML به شکل رابطه زیر تخمین زده می شود:

- اگر $\prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y1}^2}} e^{\beta_1} > \prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y0}^2}} e^{\beta_0}$ جایگذاری می شود.
- اگر $\prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y1}^2}} e^{\beta_1} < \prod_{i=1}^N \frac{1}{\sqrt{2\pi\sigma_{y0}^2}} e^{\beta_0}$ جایگذاری می شود.

بعد از لگاریتم گیری طرفین، ساده سازی رابطه و فرض $\alpha = 1$ می توان بیان کرد که آشکارسازی مناسب در محیط های با نویز کم و $\alpha = 1$ طبق رابطه زیر محاسبه خواهد شد:

- اگر $\sum_{i=1}^N MFSC'^2(i) - 3 \sum_{i=1}^N MFSC(i) > (N\sigma^2 - 2N\mu^2)K_0$ یک جایگذاری می شود.
- اگر $\sum_{i=1}^N MFSC'^2(i) - 3 \sum_{i=1}^N MFSC(i) < (N\sigma^2 - 2N\mu^2)K_0$ صفر جایگذاری می شود.

است. طبق تعریف بهبودیافته کشین، الگوی جایگذاری امن است اگر آنتروپی نسبی میان P_C و P_S برابر با ε -امنیت^۵ باشد یعنی $H(P_C | P_S) = \varepsilon_{Secure}$. با توجه به [۳۲] اگر نهان‌نگاری امن کامل باشد، پارامترهای SSIM و PSNR دارای مقادیر مناسب و خوبی هستند که به معنی شفافیت مناسب است. شفافیت مناسب هم با توجه به یک مقدار درج داده‌های محرمانه رخ داده که ما در این مقاله ظرفیت مناسب (Cap_{opt}) نامیده‌ایم. پس طبق رابطه (۱۳)، اگر آنتروپی نسبی به سمت صفر میل کند (مقدار ε)، ظرفیت مناسب را خواهیم داشت.

$$H(P_C | P_S) = \sum_{I \in Cover} P_C(I) \log \frac{P_C(I)}{P_S(I)} \quad (13)$$

$$\therefore \{H(P_C | P_S) \rightarrow 0\}$$

$$\Rightarrow \{Cap_{opt} (Capacity \rightarrow Optimum)\}$$

هدف تحقیق [۲۰] تعیین ظرفیت نهان‌نگاری در تصاویر JPEG (بیش‌ترین میزان داده‌ای که به صورت غیرقابل تشخیص می‌تواند در یک تصویر JPEG جایگذاری شود) با در نظر گرفتن روش‌های نهان‌نگاری است. به علاوه با آزمایش الگوریتم‌های نهان‌نگاری منتخب، تاثیر المان‌ها و اصول طراحی بررسی می‌شود. به عنوان مثال می‌توان با مناسب‌سازی فشرده‌ساز JPEG، نهان‌نگاری با حداقل خرابی با استفاده از اطلاعات سمت فرستنده را داشت. نتایج آزمایشات نشان می‌دهد که متوسط ظرفیت نهان‌نگاری تصاویر JPEG سطح خاکستری با فاکتور کیفیت ۷۰۶ تقریباً ۰/۰۵ بیت در هر ضریب غیرصفر AC از ضرایب DCT است [۲۷]. در این مقاله مناسب‌بودن ظرفیت را از طریق مصالحه با شفافیت (پارامترهای SSIM و PSNR) مورد بررسی قرار داده‌ایم.

- تصاویر پوشانه با آنتروپی پایین: هرگاه درج ضرایب فرکانس میانی موجب به صورت طیف‌گسترده و با توجه به مقدار α صورت پذیرد، نتیجه آن افزایش مقاومت است. حال اگر آنتروپی آن از یک سطح آستانه‌ای پائین‌تر باشد که آن را با نماد ($H_T \downarrow$) نشان می‌دهیم، آن‌گاه BER در یکی از مقادیر پایین‌تر از سطح آستانه آنتروپی، کاهش یافته و در امتداد آن درصد آشکارسازی آن طبق رابطه (۱۴) افزایش می‌یابد، که آشکارسازی بالا را با نماد ($D \uparrow$) نشان می‌دهیم. طبق رابطه (۱۴) اگر ظرفیت مناسب وجود داشته باشد، آنگاه میزان آشکارسازی نیز بالا است.

$$H_T \downarrow \Rightarrow \{BER \downarrow \& D \uparrow\} \therefore Cap_{opt} \geq D \quad (14)$$

که H_T سطح آستانه بیشینه بی‌نظمی و D میزان آشکارسازی است. به طور کلی بیش‌ترین میزان آنتروپی برای یک متغیر

توابع هدف است. کم‌ترین مقدار λ در F_S رخ می‌دهد، جایی که بردار $F^* + \omega\lambda$ مرز پایینی اهداف را قطع می‌کند. مقدار مناسب α که معادل λ است، کمی بزرگ‌تر از 1 است. به عنوان مثال در نمودار مربوط به جدول (۳) نحوه به دست آوردن هدف نشان داده شده است. بازه وزن $f_D(\alpha)$ عددی بسیار کوچک‌تر از 1 است و بازه وزن $f_E(\alpha)$ که از جنس احتمال بوده از 0 تا 1 است با استفاده از این روش مقدار مناسب α را جهت جاسازی پایدار و نامحسوس در تصویر به دست آوردیم تا در برابر حملاتی مانند مقیاس، بُرش، فیلتر میانه، فیلتر گوسی و چرخش مقاومت داشته باشد. به عنوان مثال در جدول (۴) نتایج تجربی آن آمده است.

۳-۳. پوشش کامل درج داده‌های محرمانه

ظرفیت نهان‌نگاری میزان اطلاعاتی است که می‌توان از طریق الگوریتم نهان‌نگاری در تصاویر مورد نظر ذخیره کرد، طوری که این جایگذاری توسط روش‌های نهان‌کاوی قابل شناسایی نباشد. به عبارت دیگر ظرفیت نهان‌نگاری، ظرفیت قابل جایگذاری برای حداکثر میزان داده‌ای^۱ است که داده‌ها قابل شناسایی نباشند [۲۷]. ظرفیت نهان‌نگاری معیار اصلی مقایسه کارایی الگوریتم‌های مختلف نهان‌نگاری است. تاکنون روش‌هایی برای محاسبه ظرفیت نهان‌نگاری در [۲۸، ۲۹، ۳۰، ۳۱] ارائه شده است. در [۲۸] ظرفیت نهان‌نگاری از منظر روش‌های نهان‌کاوی تعریف شده است. به علت فقدان مدل‌های آماری دقیق برای تصاویر طبیعی، روش‌های نهان‌نگاری از دید مدل تئوری ضرایب DCT مورد بررسی قرار نگرفته‌اند [۲۷]. محققان معتقدند که برای به دست آوردن جواب قابل قبول، نیاز است تا برخی از عبارت‌های مدل آماری ساده‌تر شود (پیچیدگی محاسباتی آن‌ها کم‌تر گردد) که این امر باعث ایجاد نتیجه نامناسب می‌گردد [۱۸]. در [۲۶] به جای بررسی مدل تئوری، به آخرین روش‌های نهان‌کاوی توجه شده است. یک مدل مناسب برای تصاویر فرمت JPEG است و می‌توان امنیت روش‌های نهان‌نگاری را با توجه به مدل [۲۶] با ابعاد بزرگ ارزیابی نمود. در حقیقت [۲۷] این بحث را از نقطه نظر تعریف کشین^۲ از امنیت نهان‌نگاری، بررسی می‌کند. ویژگی‌های تصویر پوشانه، pdf^۳ تصاویر پوشانه را مدل می‌کند. امنیت سیستم نهان‌نگاری می‌تواند با فاصله KL^۴ میان توزیع آماری تصاویر بدون پیام P_C و تصاویر حاوی پیام P_S در فضای ویژگی ارزیابی شود. فاصله KL در رابطه (۱۳) آمده

- 1- Payload
- 2- Cachin
- 3- probability density function
- 4- Kullback-beibler

ظرفیت نهان‌نگاری یکسانی هستند. ۲) داده محرمانه اندازه مشخصی دارد. ۳) تعداد اشیاء پوشانه ثابت است و نهان‌کاو از این تعداد مطلع است.

به علاوه در [۳۳] بیان شده است که بهترین گزینه برای نهان‌نگار این است که داده محرمانه را به‌طور مساوی میان تصاویر پخش نماید. ما این رویکرد تئوری نهان‌نگاری دسته‌ای را «نهان‌نگاری دسته‌ای ایستا» می‌نامیم. همان‌طور که در [۳۴] نیز بررسی شده است برخی از این فرض‌ها به‌منظور ارائه یک چهارچوب تئوری مناسب برای موضوع جدید نهان‌نگاری دسته‌ای است. با این وجود ممکن است این فرض‌ها در موارد عملی، کاربردی نباشد. مثلاً اگر تعداد تصاویر کم باشد و ظرفیت کل تصاویر برای مخفی کردن داده محرمانه کافی نباشد، در هر تصویر بیش از حد جایگذاری می‌شود و در نتیجه از امنیت تصاویر حاوی پیام کاسته می‌شود. اگر تعداد تصاویر زیاد باشد با پخش مساوی داده میان تصاویر، امنیت تصاویر حاوی پیام بالا می‌رود، اما کانال ارتباطی بیشتر اشغال می‌شود. در [۳۴] روش نهان‌کاو دسته‌ای^۴ را برای تحلیل یک دسته تصویر و کشف این‌که آیا اصلاً در این دسته نهان‌نگاری صورت گرفته است یا نه تعریف نمود. در [۳۴] یک دسته تصویر شامل چند تصویر حاوی پیام و چند تصویر بدون پیام است. در [۳۵] نشان داده شده که ظرفیت نهان‌نگاری یک تصویر تحت شرایطی متناسب با جذر اندازه تصویر است و در نهان‌نگاری دسته‌ای برای تصاویر با ظرفیت نهان‌نگاری یکسان و در صورت برقراری شرایط مطرح شده در مقاله مذکور، ظرفیت نهان‌نگاری متناسب با جذر تعداد تصاویر است. ولی در این مقاله ظرفیت و میزان درج اطلاعات در هر فریم ویدیویی متفاوت در نظر گرفته شده است. در واقع در این قسمت، ظرفیت را با بانکی از تصاویر پوشش داده‌ایم و چون تهیه اختصاصی آن وقت‌گیر است از فریم‌های ویدیو استفاده شده است. فرمت ویدیوی خام AVI^۵ عرضه شده در نوامبر ۱۹۹۲ توسط مایکروسافت، به دلیل انعطاف‌پذیری در اغلب دستگاه‌ها قابل استفاده است. البته توسعه فرمت AVI در ۱۹۹۶ توسط گروه Matrix Open DML (AVI 2.0) و تلفیق موفقیت‌آمیز AVI و DIVX در سال ۲۰۰۵ توسط شرکت DIVX صورت گرفت. الگوریتم درج و استخراج، همانند شکل (۳-الف) و (۳-ب) است. البته همان‌طور که در شکل (۵) مشاهده می‌شود، مدیریت ظرفیت مطابق طول پیام به کمک شمارنده ز مدیریت شده است و با درج مقدار متغیر k در هر تصویر مشخص شده که درج در تصویر بعدی ادامه دارد. اگر $k=1$ باشد به معنی ادامه داشتن است و $k=0$ یعنی آخرین تصویر درج است.

تصادفی در توزیع یکنواخت، و کم‌ترین میزان آنتروپی در توزیعی با یک رویداد قطعی (یعنی با احتمال یک) رخ می‌دهد.

با توجه به ویژگی‌های کانال واقعی و همچنین با توجه به این‌که خراب‌شدن بیت‌ها یک پدیده تصادفی است، برای محاسبه احتمال نادرست‌بودن بیت‌های دریافتی در گیرنده، از تئوری احتمال بهره برده شده است [۳۱]. با رابطه (۱۵) احتمال نادرست‌بودن (آسیب‌دیده) یک بسته F بیتی به‌دست می‌آید.

$$P_f = 1 - (1 - BER)^F \quad (15)$$

و احتمال درست‌بودن بیت‌ها را می‌توان با رابطه (۱۶) محاسبه کرد.

$$P_f = (1 - BER)^F \quad (16)$$

با توجه به روابط (۱۵) و (۱۶) می‌توان به رابطه (۱۷) رسید.

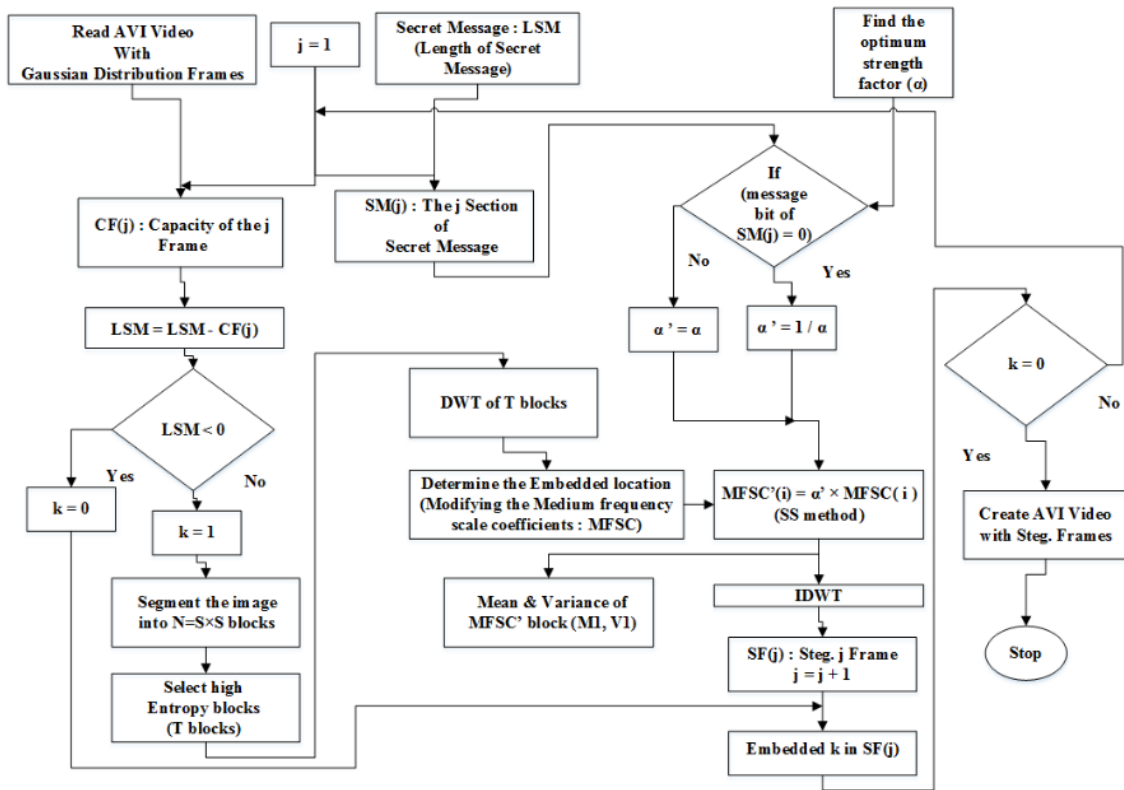
$$H_T = - \sum_{i=1}^n P_t(x_i) \log_2 P_t(x_i) \\ = - \sum_{i=1}^n (1 - BER_{x_i})^{F_{x_i}} \log_2 (1 - BER_{x_i})^{F_{x_i}} \quad (17) \\ \therefore H_T \downarrow \Rightarrow BER \downarrow$$

آزمایش‌های متعددی که نمونه آن در جداول ۵ و ۶ بخش نتایج تجربی مشخص شده، این موضوع را نشان می‌دهد.

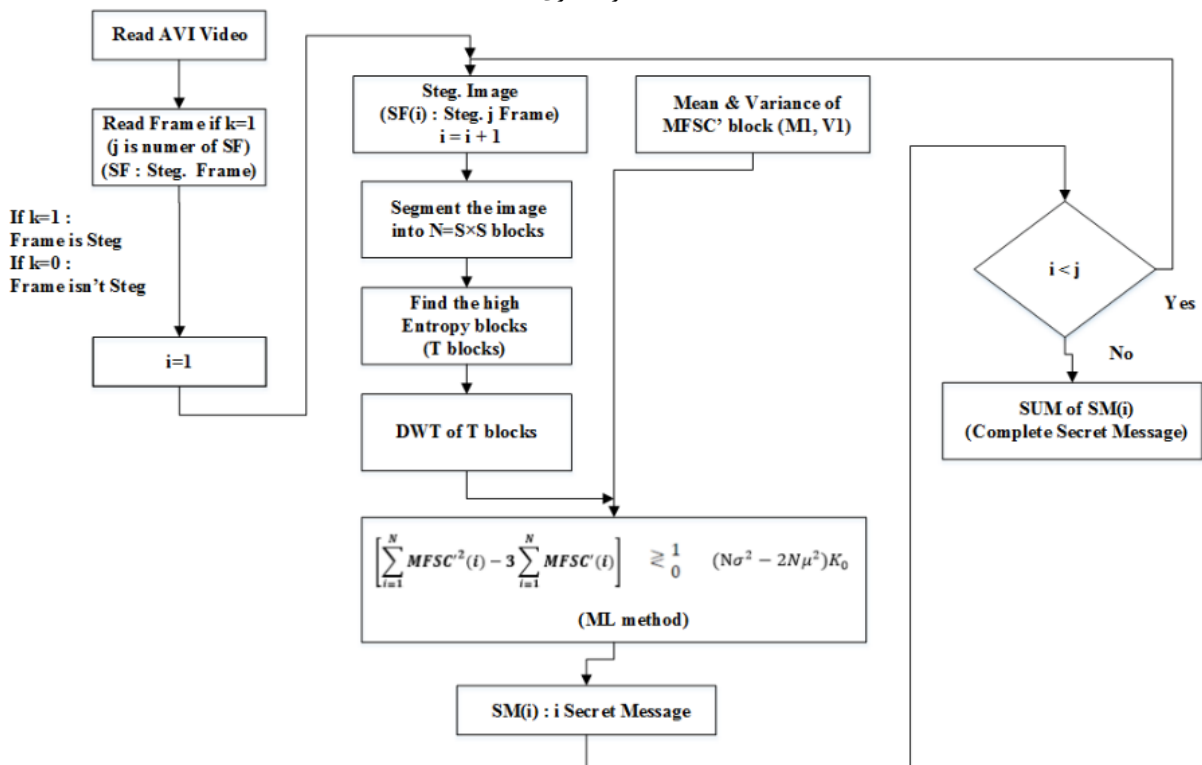
- فریم‌های ویدیوی خام: ممکن است اندازه ظرفیت مناسب، کوچک‌تر از کل داده محرمانه برای درج باشد، آن‌گاه می‌توان نهان‌نگاری دسته‌ای را مطرح کرد. نهان‌نگاری دسته‌ای مساله پنهان‌کردن و نهان‌کاو را به چندین شیء پوشانه تعمیم می‌دهد [۳۱]. کِر^۱ در [۳۱] ظرفیت نهان‌نگاری دسته‌ای را تعریف می‌کند و به‌صورت تئوری ثابت می‌کند که اندازه داده محرمانه می‌تواند با امنیت افزایش یابد اما نباید نرخ افزایش آن بیش‌تر از جذر تعداد تصاویر پوشانه باشد. در رویکرد نهان‌نگاری دسته‌ای، داده محرمانه در چندین شیء پوشانه پنهان می‌شود. اگر یک داده محرمانه با اندازه مشخصی را در نظر بگیریم، پنهان‌کردن آن در چندین تصویر، نرخ جایگذاری در هر تصویر را کم‌تر کرده و شناسایی تصاویر حاوی پیام را مشکل می‌کند. به علاوه فردریچ^۲ در [۲۷] تاکید نموده است که یک الگوریتم نهان‌نگاری قابل شناسایی است اگر نرخ جایگذاری بالاتر از آستانه‌ای (۰/۰۵) بیت در هر ضریب غیرصفر (DCT) باشد. بنابراین نرخ کم جایگذاری در نهان‌نگاری دسته‌ای قابل شناسایی بودن تصاویر حاوی پیام را کاهش می‌دهد. کِر در [۳۱] سه فرض ذیل را برای نهان‌نگاری دسته‌ای در نظر گرفته است: ۱) تمامی اشیاء پوشانه دارای

3- Static batch steganography
4- Pooled steganalysis approach
5- Audio Video Interleave

1- Ker
2- Fridrich



الف) ساختار جاسازی داده



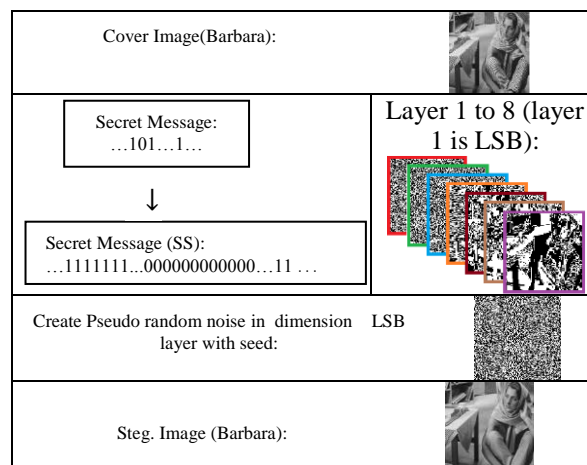
ب) ساختار استخراج داده

شکل (۵): نهان‌نگاری در فریم‌های ویدیوی خام

۴. نتایج تجربی

۴-۱. مقایسه روش ضربی و جمعی

در شکل (۶) مثال درج به شکلی ساده در حالت طیف گسترده آورده شده است. درج به روش های جمعی و ضربی صورت گرفته است.



شکل (۶): درج اطلاعات نهان نگاری به شیوه گسترش طیف سیگنال نهان در تصویر باربارا

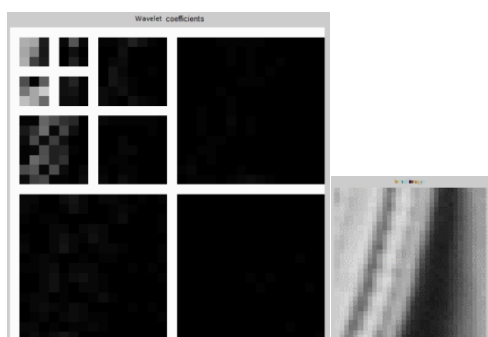
همان طور که در جدول (۱) بخش نتایج تجربی قابل مشاهده است، روش ضربی در مقایسه با روش جمعی در حوزه مکان دارای درصد آشکار سازی کمتری است زیرا متناسب سازی پارامتر، به دست آوردن روابط احتمال خطا و ظرفیت به سادگی روش جمعی نیست. در روش ضربی هر چه تبدیل مورد نظر سیگنال میزبان به صورت تنگ تر نمایش داده شود، عملکرد روش در آن حوزه بهتر می گردد. لذا استفاده از تبدیل های چنددقتی جدانشدنی مانند کانتورلت و ریچلت گسسته سبب افزایش چشم گیر عملکرد روش های ضربی برای تصاویر می گردد [۳۶].

جدول (۱): مقایسه نهان نگاری روش ضربی و جمعی در حوزه مکان

مشخصات پیام و نویز کانال	درصد آشکار سازی روش جمعی	درصد آشکار سازی روش ضربی
طول پیام ۱۰۰۰۰۰ بیت و نویز کانال ۰/۰۲	۹۸/۶۲	۳۰/۱۵۹
طول پیام ۱۰۰۰۰۰ بیت و نویز کانال ۰/۲	۸۰/۶۹۳	۲۸/۴۴۴
طول پیام ۱۰۰۰ بیت و نویز کانال ۰/۰۲	۷۲	۰

۴-۲. نتایج شفافیت

به عنوان مثال، تصویر باربارا دارای اندازه ۵۱۲×۵۱۲ است. با توجه به شکل (۳-الف) ساختار عملیات جاسازی و طبق شکل (۳-ب) ساختار عملیات استخراج داده به کمک موجک دوبعدی با سه سطح و فیلتر موجک هار و به شیوه طیف گسترده عمل نهان نگاری اطلاعات (شامل یک بردار ۲۰۰ بیتی) در ضرایب فرکانس میانی موجک بلوک های ۳۲×۳۲ از تصویر صورت می گیرد. شکل (۷-الف) اولین موجک بلوک ۳۲×۳۲ از تصویر است و شکل (۷-ب) ضرایب تبدیل موجک اولین موجک ۳۲×۳۲ از تصویر را نمایش می دهد.



الف) اولین موجک ۳۲×۳۲ ب) ضرایب تبدیل موجک



ج) تصویر بالا: اصلی؛ تصویر پائین: نهان نگاری شده

شکل (۷): نهان نگاری در تصویر Barbara به شیوه موجک دوبعدی با سه سطح و فیلتر موجک هار

جدول (۲)، مقایسه بین پارامتر شفافیت درج در ضرایب فرکانس میانی و ضرایب فرکانس پایین (LFSC^۱) را نشان می دهد.

جدول (۲): مقایسه شفافیت بین درج در MFSC و LFSC

$SSIM_{HFSC}$	$PSNR_{HFSC}$	$SSIM_{LFSC}$	$PSNR_{LFSC}$
۰/۹۹۲۴	۴۲/۱۷۳۴	۰/۹۸۰۱	۳۴/۱۵۱۶

^۱ Low Frequency Scale Coefficients

۳-۴. نتایج مقاومت

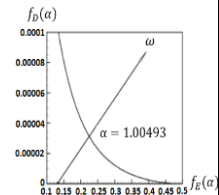
مطابق با جدول (۳) با انتخاب بردار وزن

$$(\omega_{f_D(\alpha)}, \omega_{f_E(\alpha)}) = [0/65, 0/45]$$

ما مقدار مناسب α را جهت جاسازی پایدار و نامحسوس در تصویر باربارا به دست آوردیم.

جدول (۳): محاسبه مقدار مناسب α به روش جمبیکی در تصویر باربارا

α	$f_D(\alpha)$	$f_E(\alpha)$
۱/۰۰۳	۰/۰۰۰۰۰۰۲۵	۰/۴۱۵
۰/۰۰۳۵	۰/۰۰۰۰۰۰۷۷	۰/۳۴۵
۰/۱۰۰۴	۰/۰۰۰۰۰۰۱۵	۰/۲۸۲
۱/۰۰۴۵	۰/۰۰۰۰۰۰۲۶	۰/۲۴
۱/۰۰۴۹۳ ۱	۰/۰۰۰۰۰۰۲۵	۰/۲۳
۱/۰۰۵	۰/۰۰۰۰۰۰۴۱	۰/۲
۱/۰۰۵۵	۰/۰۰۰۰۰۰۵۸	۰/۱۷۵
۱/۰۰۶	۰/۰۰۰۰۰۰۷۹	۰/۱۵
۱/۰۰۶۵	۰/۰۰۰۰۰۱۰۵	۰/۱۳۵



حال اگر در جدول قبل، در بلوک‌های دارای بیشینه بی‌نظمی، درج صورت گیرد، مقدار α کم‌تر شده و به عبارتی بهتر می‌شود. به‌عنوان مثال در حالت $\alpha = 1/0.493$ مقدار BER برابر با 0.1359 خواهد بود و در حالت $\alpha = 1/493$ مقدار BER برابر با 0.1494 خواهد بود. نتایج تست تخمین اطلاعات به‌شیوه ML در آشکارسازی مناسب با روش ضربی نیمه‌کور نهان‌نگاری در تصویر 32×32 باربارا با آنتروپی‌های مختلف در جدول (۶) آمده است.

جدول (۵): نتایج نهان‌نگاری بدون در نظر گرفتن بیشینه بی‌نظمی

بلوک‌ها

حمله مقیاس	
ضریب مقیاس	BER
۰/۹	۰/۱۲۰۱
۱/۱	۰/۱۷۶
۱/۴	۰/۱۹۳
۱/۷	۰/۲۲۳
۲	۰/۲۸۹
حمله بُرش	
بُردن	BER
۵٪	۰/۱۷۸
۱۰٪	۰/۲۰۱
۱۵٪	۰/۲۴۱
حمله فیلتر میانه	
فیلتر میانه	BER
۳×۳	۰/۱۸۵
۵×۵	۰/۲۷۴
حمله فیلتر گوسی	
فیلتر میانه	BER
۳×۳	۰/۱۸۹
۵×۵	۰/۲۷۸
۷×۷	۰/۲۸۹
حمله چرخش	
زاویه چرخش (درجه)	BER
۵	۰/۲۱۲
۲	۰/۲۱۱
۱	۰/۱۹۲
۰/۵	۰/۱۶۸
-۰/۵	۰/۱۷۲
-۱	۰/۱۹۸
-۲	۰/۲۱۱
-۵	۰/۲۳۴

جدول (۴) نتایج BER در برابر حملات مقیاس، بُرش، فیلتر میانه، فیلتر گوسی و چرخش در تصویر باربارا (در حالت مقدار مناسب α برابر با $1/0.493$) را نشان می‌دهند.

جدول (۴): نتایج BER در حملات مقیاس، بُرش، فیلتر میانه، فیلتر گوسی و فیلتر گوسی

α	PSNR	SSIM	BER
۱/۰۰۰۴۹۳	۳۴/۱۵۰۰	۰/۹۸۰۰	۰/۵۰۰۲
۱/۰۰۴۹۳	۳۴/۱۵۱۶	۰/۹۸۰۱	۰/۴۹۵۴
۱/۰۴۹۳	۳۴/۱۵۲۴	۰/۹۸۰۱	۰/۴۹۸۳
۱/۴۹۳	۳۴/۱۴۸۲	۰/۹۸۰۰	۰/۵۰۷۳

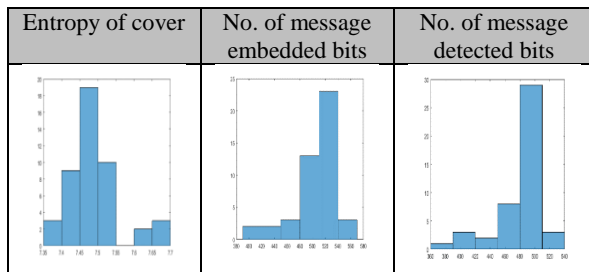
۴-۴. نتایج ظرفیت

تصاویر با ظرفیت مناسب: در جدول (۵) نتایج تست تخمین اطلاعات به‌شیوه ML در آشکارسازی مناسب روش ضربی نیمه‌کور نهان‌نگاری در تصویر 32×32 باربارا با آنتروپی کل تصویر $7/6418$ آورده شده‌است. درج در تمام بلوک‌های 32×32 بدون در نظر گرفتن بیشینه بی‌نظمی بلوک‌ها می‌باشد. طول پیام 4096 بیت است و درج در ضرایب فرکانس میانی موجب انجام شده‌است.

در یک تصویر جایگذاری شود آنگاه قابلیت شناسایی افزایش می‌یابد [۳۷]. همان‌طور که در جدول (۷) نشان داده‌شده با در نظر گرفتن سطح آستانه آنتروپی ۷/۵ موارد ذیل به‌دست آمده است:

- مناسب‌ترین ظرفیت (در حالت بیش‌ترین مقدار SSIM و PSNR به عبارتی شفافیت فریم) در فریم دارای پایین‌ترین آنتروپی (۷/۳۷۴۷۶۴) به‌دست آمده‌است.
- کم‌ترین BER (با در نظر گرفتن مقدار مناسب α و در نتیجه مقاومت فریم) و بیش‌ترین درصد آشکارسازی با نسبت ۹۶/۱٪ در فریم دارای آنتروپی نسبتاً پایین، ۷/۴۸۸۶۵۸ حاصل شده است.

جدول (۷): نتایج تست بروی فریم‌های ویدیوی خام



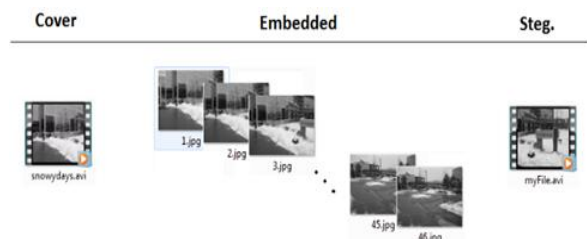
Frame No.	α Optimum	Entropy of Steg.	Bits of Message	Percent of Detected (Bits)	BER	PSNR	SSIM
۱	۱/۰۰۴۸۲۵	۷/۶۵۲۱۵۷	۴۳۴	۹۴/۴۷/(۴۱۰)	۰/۱۵۵۲۹۹	Min= ۳۹/۲۳۰۴۶	Min= ۰/۹۹۴۳۶۲
۲	۱/۰۰۴۸۲۱	۷/۶۵۱۴۳۳	Min=۴۱۱	۹۴/۱۶/(۳۸۷)	۰/۱۵۵۸۳۹۴	۴۲/۶۶۹۴	۰/۹۹۷۳۵۳
۳	۱/۰۰۴۷۴۹	۷/۶۵۶۲۵۴	۴۱۷	۹۳/۷۶/(۳۹۱)	۰/۱۶۳۳۵۰	43.5623 ۴۲/۵۶۲۳	۰/۹۹۷۷۵۵
۴	۱/۰۰۴۷۴۱	۷/۶۴۲۱۵۶	۴۵۲	Min= ۹۳/۵۸/(۴۳۳) Max= ۰/۱۶۴۱۵۹	۴۲/۸۸۶۳۷	۴۲/۸۸۶۳۷	۰/۹۹۷۳۳۵
...
۱۷	۱/۰۰۴۸۲۸	۷/۴۴۹۴۸	۵۴۲	۹۴/۸۳/(۵۱۴)	۰/۱۵۱۶۰۰	۴۲/۹۴۲۵۵	۰/۹۹۷۰۳۱

با توجه به نتایج فوق، نهان‌نگاری پیشنهادی در حالت مقدار مناسب α ، در مقابل حملات مقاوم است.

جدول (۶): نهان‌نگاری با در نظر گرفتن بیشینه بی‌نظمی بلوک‌ها

α	۱/۰۰۰۴۹۳	۱/۰۰۴۹۳	۱/۰۰۴۹۳	۱/۰۰۴۹۳	پوشش ظرفیت از پیام ۴۰۹۶ بیتی	آشکارسازی از پیام ۴۰۹۶ بیتی
BER (H= ۰/۰۷۶۴)	۰/۱۴۳۵	۰/۱۳۵۹	۰/۱۴۰۶	۰/۱۴۹۴	۹۵/۹۹٪	۹۵/۹۹٪
BER (H= ۰/۰۷۶۴۲)	۰/۱۵۱۸	۰/۱۳۸۱	۰/۱۴۵۲	۰/۱۳۸۹	۹۹/۸۵٪	۹۹/۸۵٪
BER (H= ۳/۸۲۰۹)	۰/۲۳۵۷	۰/۲۲۴۵	۰/۲۲۹۴	۰/۲۳۸۴	۷۲/۶۳٪	۷۲/۳۸٪

افزایش ظرفیت به کمک فریم‌های ویدیوی خام: در این مقاله از ویدیو Snowdays.avi تعداد ۴۶ فریم برای درج ۲۳۲۰۴ بیت گرفته شده و بعد از درج اطلاعات به‌روش شکل (۵-الف) در تمام فریم‌ها، مجدداً فیلم با نام myFile.avi بازسازی شده‌است. با توجه به انتخاب $K_1 = ۰/۰۱$ ، $K_3 = ۰/۰۳$ در ضریب کیفیت تمامی بلوک‌ها (Q_j) و انتخاب بردار وزن $(\omega_{f_D}(\alpha), \omega_{f_E}(\alpha)) = (۰/۶۵, ۰/۴۵)$ مقدار مناسب α برای همه فریم‌ها محاسبه شده است. طبق جدول (۷) بیش‌ترین ظرفیت در فریم دارای آنتروپی نسبتاً پایین (۷/۴۵۶۷۲) به‌دست آمده‌است (شکل ۸).



شکل (۸): نهان‌نگاری در فریم‌های ویدیو Snowdays.avi

۴-۵. مصالحه بین سه ویژگی شفافیت، مقاومت و ظرفیت

مصالحه بین سه ویژگی شفافیت، مقاومت و ظرفیت موضوعی است که در طراحی روش پیشنهادی در نظر گرفته شده است. مصالحه‌ای میان قابلیت شناسایی و میزان داده‌ای که در یک تصویر نهان‌نگاری می‌شود، وجود دارد. اگر میزان اطلاعات زیادی

نهان نگاری صورت گرفت و مقادیر AUC، برای هر حالت نهان کاو WAM و FARID نیز محاسبه شد. هر چه مقدار AUC مربوط به یک طبقه بند بزرگ تر باشد کارایی نهایی طبقه بند مطلوب تر ارزیابی می شود. در واقع هر چه AUC به عدد یک نزدیک تر باشد، کارایی قوی تر نهان کاو را نشان می دهد و هر چه به ۰/۵ نزدیک تر باشد، کارایی ضعیف تر نهان کاو را نشان می دهد مطابق جدول (۹)، روش پیشنهادی نسبت به JSteg رفتار مقاوم تری در برابر نهان کاوهای WAM و FARID داشت.

جدول (۹): بررسی روش پیشنهادی و JSteg در مقابل نهان کاوها

	AUC _{WAM}	AUC _{FARRID}
روش پیشنهادی	۰/۶۲۵	۰/۵۹۷
JSteg	۰/۸۵۵	۰/۸۲۳

۵. نتیجه گیری

نهان نگاری مبتنی بر آشکارسازی مناسب، با مصالحه سه مؤلفه شفافیت، مقاومت و ظرفیت ارتباط مستقیم دارد. با مقایسه تجربی نهان نگاری در ضرایب فرکانس پایین و فرکانس میانی تبدیل موجک، می توان مشاهده کرد که برای حفظ شفافیت، در بخش فرستنده، از درج اطلاعات به شیوه طیف گسترده در ضرایب فرکانس میانی موجک استفاده شده است. اما این موضوع باعث کاهش مقاومت می شود که در این مقاله نشان داده شده است. با به دست آوردن پارامتر ضریب قدرت مناسب درج اطلاعات (α)، مقاومت کاهش نمی یابد و در واقع برای بهبود مقاومت، در بخش گیرنده، ارائه راه کاری برای کاهش خطای آشکارسازی داده نهان در الگوریتم ML مطرح شده است. برای حفظ ظرفیت نهان نگاری، راه کار دو مرحله ای ارائه شد که به ترتیب برای محاسبه ظرفیت مناسب به کمک پوشانه های با آنتروپی پایین و برای پوشش درج کل داده های محرمانه به علت نداشتن یک بانک مناسب با مولفه های تاثیر گذار هم چون کنتراست، انرژی و غیره، است. با این وجود پیشنهاد نویسندگان مقاله استفاده از فریم های ویدیویی خام است.

برای تحقیقات آینده روش های دیگر به جز تبدیل موجک را می توان مورد بررسی قرار داد. تبدیل موجک با وجود داشتن مزایای فراوان، نقاط ضعف هایی دارد که محققان را بر این می دارد که روش های جدیدی را پایه گذاری نمایند. این تبدیل دارای دو مشکل اصلی است. مشکل اول، حساس بودن نسبت به تغییرات؛ یعنی هر گاه در ضرایب تبدیل موجک تغییری صورت گیرد، باعث تغییرات زیادی در سیگنال ورودی می شود. این اشکال به خاطر انجام عمل نمونه برداری کاهشی می باشد. مشکل دوم، جهت های

۱۸	۱/۰۰۴۷۵۳	۷/۴۵۶۷۲	Max=۵۵۸	۹۳/۹/(۵۳۴)	۰/۱۶۰۹۳۱	۴۲/۱۸۶۹۹	۰/۹۹۶۷۷۹
۱۹	۱/۰۰۴۹۲۱	۷/۴۶۵۱۴۵	۵۵۳	۹۵/۱۲/(۵۲۶)	۰/۱۴۸۸۲۴	۴۲/۱۷۹۴۱۷	۰/۹۹۷۰۹۶
...
۲۴	۱/۰۰۴۷۳۸	Min=۷/۳۷۴۷۶۴	۴۹۵	۹۳/۳۳/(۴۶۴)	۰/۱۶۲۶۱۶	Max=۴۵/۱۲۵۸	Max=۰/۹۹۸۰۳
...
۴۶	۱/۰۰۴۹۲۵	۷/۴۸۸۶۵۸	۵۱۳	Max=۹۶/۱/(۴۹۳)	Min=۰/۱۳۸۹۸۶	۴۱/۸۰۶۰۶	۰/۹۹۷۰۴۳

الگوریتم پیشنهادی را طبق مقاله [۳۸]، با پوشانه های تصاویر انتخابی آزمایش کردیم، به طوری که تصویر پوشانه از سطح امنیت خوبی برخوردار بود، میانگین نتایج آزمون بر روی ۱۰۰ تصویر به صورت جدول (۸) حاصل شد که نتیجه تمام پارمترها در حالت پیشینه بود.

جدول (۸): میانگین نتایج تست بر روی ۱۰۰ تصویر

α Optimum	Entropy of Steg.	Bits of Message	Percent of Detected (Bits)	BER	PSNR	SSIM
۱/۰۰۴۷۳۷	۷/۶۵۲۱۵۷	۵۵۷	۹۶/(۴۹۳)	۰/۱۶۵۱۰۷	۴۵/۳۷۶۴	۰/۹۹۹۰۱

۴-۶. بررسی در برابر نهان کاو WAM و FARID

درج در فریم های ویدیوی خام در برابر نهان کاو WAM و FARID مورد آزمایش قرار گرفت. در ابتدا از حدود ۲۴۰۰ تا ۶۰۰۰ فریم (حدود چهار دقیقه ویدیو) آماده کرده و بر روی ۱۲۰۰ تا ۳۰۰۰ فریم با نرخ ۲۵٪ درج به روش پیشنهادی انجام شده است. ۱۵۰۰ فریم برای آموزش و نصف دیگر برای تست استفاده شد؛ به کمک طبقه بندی FLD مقادیر AUC، برای هر حالت نهان کاو WAM و FARID محاسبه شد. سپس در مرحله دیگر، در فریم ها به شیوه JSteg (دلیل مقایسه با این روش، شباهت های ساختاری و پرکاربرد بودن JSteg با این روش پیشنهادی بوده است) درج

- Grid," International Conference on Information Science and Control Engineering, 1313-1316. 2016.
- [8] P. Arora¹, and M. Chandana, "Efficient Watermarking Algorithm for Digital Images," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 8, August 2015.
- [9] J. Wang, G. Liu, Y. Dai, and J. Sun, "Locally optimum detection for Barni multiplicative watermarking in DWT domain," Signal Processing, Vol. 88, pp. 117-130. 2008.
- [10] J. A. Bagaskara, T. W. Purboyo, and R. A. Nugrahaeni, "Analysis of JPEG Image Steganography Using SPread Spectrum Method," International Journal of Applied Engineering Research, ISSN 0973-4562, Vol. 12, pp. 13944-13950. Number 23. 2017.
- [11] B. Padmasri, and M. Amuthasurabi, "Spread Spectrum Image Steganography with advanced Encryption Key Implementation," IJARCSSE, Vol. 3, Issue 3, March 2013.
- [12] I. Cox, J. Kilian, and T. Leighton, "Secure Spread Spectrum watermarking for multimedia," IEEE Trans. Image process, Vol. 6, no. 12, pp. 1673-1687, Dec 1997.
- [13] I. J. Cox, M. L. Miller, and A. L. Mckellips, "Watermarking as communications with side information," Proceeding of the IEEE, Vol. 87, pp. 1127-1141, 1999.
- [14] V. Solachidis, and I. Pitas, "Optimal detector for multiplicative watermarks embedded in the DFT domain of non-white signals," EURASIP Journal on Applied Signal Processing, Vol. 16, pp. 522-532, 2004.
- [15] M. N. Do, and M. Vetterli, "The Contourlet transform: An efficient directional multiresolution image representation," IEEE Trans. Image Process, Vol. 14, no. 12, pp. 2091-2106, 2005.
- [16] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "A new decoder for the optimum recovery of nonadditive watermarks," IEEE Trans. Image Process, Vol. 10, no. 5, pp. 755-766, 2001.
- [17] S. Liu H. Yao, and W. Gao, "Steganalysis of data hiding techniques in wavelet domain," in Proc. of Int. Conf. on Information Technology: Coding and Computing, ITCC, pp. 751-754, 2004.
- [18] P. C. Su, and C. C. J. Kuo, "Steganography in JPEG 2000 compressed images," IEEE Trans. Consum. Electron, pp. 824-832, 2003.
- [19] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm," Hong Kong, IMECS 2011.
- [20] S. D. Seyyedi, V. Sadau, and N. Ivanov, "A Secure Steganography Method Based on Integer Lifting Wavelet Transform," International Journal of Network Security, Vol. 18, no. 1, PP. 124-132, Jan 2016.

انتخابی محدود؛ تنها سه جهت افقی عمودی و اریب را می‌توان برای تبدیل موجک در نظر گرفت. همچنین در روش ضربی هرچه تبدیل مورد نظر سیگنال میزبان را به صورت تنک‌تری نمایش دهد، عملکرد روش در آن حوزه بهتر می‌گردد. لذا برای غلبه بر ضعف‌های تبدیل موجک، استفاده از تبدیل‌های چنددقتی جدانشدنی مانند کانتورلت و ریچلت گسسته سبب افزایش چشمگیر عملکرد روش‌های ضربی برای تصاویر می‌گردد. یا طبق مقاله [۳۹] استفاده از $DTCWT^2$ علاوه بر پوشش اشکالات DWT، سرعت درج را هم می‌توان بالا برد. که می‌توان در تحقیقات آینده در نظر گرفت. لازم به ذکر است که با توجه به تنک‌بودن ضرایب پوشانه تبدیل کانتورلت، ضرایب این تبدیل برای جایگذاری به روش ضربی بسیار مناسب است. همچنین چون موضوع فریم‌های ویدیو مطرح است، می‌توان مبحث ماتریس هم‌رخدادی سطح خاکستری هر فریم را براساس همبستگی و مقادیر پیکسل‌های فریم استخراج کرد تا براساس آن‌ها برای الگوریتم آشکارسازی مناسب تصمیم‌گیری دقیق‌تری صورت گیرد.

۶. مراجع

- [1] R. Cogranne, and F. Retraint, "Application of hypothesis testing theory for optimal detection of LSB matching data hiding," Signal Processing, Vol. 93, Issue 7, pp. 1724-1737, 2013.
- [2] S. Bajracharya, and R. Koju, "An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Images International," Journal Engineering and Manufacturing, Vol. 1, pp. 49-59, 2017.
- [3] G. Bhatnagar, B. Raman, and Q. M. J. Wu, "Robust watermarking using fractional wavelet packet transform," Iet Image Processing, Vol. 4, pp. 386-397, 2012.
- [4] S. Ramakrishnan, T. Gopalakrishnan, and K. Balasamy, "A wavelet based hybrid SVD algorithm for digital image watermarking," Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.3, September 2011.
- [5] R. Dejeay, and S. Rajesh, "An improved wavelet domain digital watermarking for image protection. International," Journal of Wavelets Multiresolution & Information Processing, Vol. 08(01), pp. 19-31. 2010.
- [6] K. C. Liu, "Wavelet-based watermarking for color images through visual masking. AEU," International Journal of Electronics and Communications, Vol. 64(2), pp. 112-124. 2010.
- [7] Q. Chen, and M. Xiong, "Dual Watermarking Based on Wavelet Transform for Data Protection in Smart

1 Lack of directional selectivity

2- Dual-Tree Complex Wavelet Transform

- [30] P. Moulin, and M. K. Mihcak, "A framework for evaluating the data hiding capacity of image sources," *IEEE Trans. Image Processing*, Vol. 11, pp. 1029-1042, 2002.
- [31] A. D. Ker, "A capacity result for batch steganography," *Signal Processing Letters*, Vol. 14, no. 8, pp. 525-528, 2007.
- [32] R. Esfahani, Z. Norozi, and G. Jandaghi, "Cover Selection for More Secure Steganography," *International Journal of Security and Its Applications (IJSIA)*, Vol. 12, no. 1, pp. 21-36, 2018.
- [33] A. D. Ker, "Perturbation Hiding and the Batch Steganography Problem," *Proc. of 10th Information Hiding Workshop*, 2008.
- [34] A. D. Ker, "Batch steganography and pooled steganalysis," *Proc. of 8th Information Hiding Workshop*, pp. 265-281, 2006.
- [35] A. D. Ker, T. Penvy, J. Kodovsky, and J. Fridrich, "The Square Root Law of Steganographic Capacity," *Proc. of 10th ACM Workshop on Multimedia and security*, 2008.
- [36] N. Kingsbury, "Complex Wavelets for Shift Invariant Analysis and Filtering of Signals," *Applied and Computational Harmonic Analysis*, Vol. 10, issue. 3, pp. 234-253, 2001.
- [37] A. Sarkar, K. Solanki and B. S. Manjunath, "Further study on YASS: Steganography based on Randomized Embedding to Resist Blind Steganalysis," *Proc. of SPIE - Security, Steganography, and Watermarking of Multimedia Contents*, 2008.
- [38] R. Esfahani, M. A. Akhaee, and Z. Norozi, "A Fast Video Watermarking Algorithm Using Dual Tree Complex Wavelet Transform," *Springer, Multimedia Tools and Application (DOI: 10.1007/s11042-0-18-6892-6)*, Vol. 77, P. 1-17, 2018.
- [21] P. Meerwald, "Digital image watermarking in the wavelet transform domain", Master's Thesis, Salzburg University, Salzburg, Austria, January 2001.
- [22] D. L. Donoho, and I. M. Johnstone, "Ideal adaptation via wavelet shrinkage," *Biometrika*, Vol. 81, pp. 425-455, 1994.
- [23] A. Fabien, and P. Petitcolas, "Watermarking schemes evaluation," *IEEE Signal Processing*, Vol. 17, no. 5, pp. 58-64, September 2000.
- [24] M. A. Akhaee, S. M. E. Saheaeian, and F. Marvasti, "Contourlet Based Image Watermarking Using Optimum Detector in a Noisy Environment," *IEEE Trans. on Image Processing*, Vol. 8, no 6, Apr. 2010.
- [25] M. A. Akhaee, S. M. E. Saheaeian, F. Marvasti, and B. Sankur, "Robust Scaling-Based Image Multiplicative Watermarking Technique Using Maximum Likelihood Decoder With Optimum Strength Factor," *IEEE Trans. on Multimedia*, Vol 11, no 5, pp. 822-833, Aug. 2009.
- [26] F. Gembicki, and Y. Haimes, "Approach to performance and sensitivity multiobjective optimization: The goal attainment method," *IEEE Transactions on Automatic Control*, Vol. 20, Issue: 6, pp.769-771, Dec 1975.
- [27] J. Fridrich, T. Pevny, and J. Kodovsky, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities," *Proc. of MM&Sec'07, ACM*, 2007.
- [28] R. Chandramouli, and N. D. Memon, "Steganography Capacity: A Steganalysis Perspective," *Proc. SPIE Security and Watermarking of Multimedia Contents*, pp. 173-177, 2003.
- [29] C. Cachin, "An information theoretic model for steganography," *2nd Int. Workshop on Information Hiding*, pp. 306-318, 1998.

Steganography on Raw Video Based on Proper Detection and Compromise between the Parameters of Transparency, Resistance and Capacity

R. Esfahani, Z. Norouzi*, M. A. Akhaei

*Imam Hossein Comprehensive University

(Received: 10/06/2018, Accepted: 05/03/2019)

ABSTRACT

One of the major weaknesses of steganography algorithms in detection, is the lack of proper estimation of the data on the recipient side. The appropriate detection in the steganography algorithm is directly related to the tradeoff between the three parameters of transparency, resistance and capacity. The proposed algorithm uses a proper tradeoff between these three parameters. Due to this issue, in this article the inclusion of information in the intermediate frequency coefficients of the wavelet by the Spread Spectrum method has been used in order to maintain transparency. The reduction of resistance is prevented by obtaining the appropriate amplification coefficient parameter for embedding of information. Proper measurement of is also assessed by the error bit rate. Setting the proper capacity in a cover and the full coverage of secret data embedding are the two suggested steps related to the capacity parameter. In the first step, the proper capacity means the proper tradeoff between the capacity parameter and the transparency parameter, i.e. the steganography has the proper values of the SSIM and PSNR parameters. The use of low entropy covers leads to low capacity but also high resistance. In this case, the error bit rate is also reduced, which means getting close to the appropriate value of and the appropriate resistance. In the second step, the use of video frames of Windows Media Video is proposed for full coverage of secret data embedding. Since there may be a massive amount of secret data and a single cover may not be sufficient, a cover bank is required. As creating an image bank with close statistical properties may be difficult and time consuming, the video frames of Windows Media Video have been used.

Keywords: Spread Spectrum, Proper Detection, Intermediate Frequency Coefficients of the Wavelet, amplification coefficient , Error Bit Rate

* Corresponding Author Email: znorouzi@ihu.ac.ir