نشریه علمی «پدافند الکترونیکی و سایبری»

سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۶۵-۵۱

نهان‌نگاری ویدیوی خام مبتنی‌بر آشکارسازی مناسب با مصالحه بین پارامترهای شفافیت، مقاومت و ظرفیت

رضا اصفهانی[۱]، زین‌العابدین نوروزی*[۲]، محمدعلی اخایی[۳]

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

(دریافت: ۹۷/۹/۱۴، پذیرش: ۹۸/۳/۲۸)

چکیده

یکی از ضعف‌های عمده الگوریتم‌های نهان‌نگاری، عدم تخمین مناسب در سمت گیرنده از داده‌ها در آشکارسازی می‌باشد. آشکارسازی مناسب در الگوریتم نهان‌نگاری، 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 به‌شیوه طیف‌گسترده در ضرایب فرکانس میانی موجک استفاده شده است. با به‌دست‌آوردن پارامتر ضریب قدرت مناسب درج اطلاعات (α)، از کاهش مقاومت جلوگیری‌شده است. سنجش مناسب‌بودن 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 به‌معنی مصالحه مناسب پارامتر ظرفیت با پارامتر شفافیت است، یعنی نهان‌نگاری 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 بیت‌خطا کاهش یافته و این به‌معنی نزدیک‌شدن به‌مقدار مناسب α و به‌عبارتی 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 به‌هم، 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

نهان‌نگاری در فریم ویدیو یکی از راه‌حل‌های موثر برای مقابله با بسیاری از مسائل هم‌چون مخفی‌کردن اطلاعات بدون ایجاد حساسیت است، به‌طوری‌که 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 نهان‌نگاری‌شده 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 نهان‌نگاری معتبر، ایجاد ظرفیت مناسب جهت درج اطلاعات محرمانه، نامحسوس بودن نهان‌نگاره، مقاومت آن در مقابل حمله‌های مختلف و حفظ شفافیت[۲] می‌باشد. ایده اصلی در این مقاله استفاده از نهان‌نگاری به‌روش طیف‌گسترده ضربی در ضرایب فرکانس میانی تبدیل موجک است. در دو مقاله [۳-۲] نهان‌نگاری در حوزه DWT است و پارامتر مقاومت بیشتر مورد نظر است. در مقاله [۴] مبتنی‌بر DWT و تجزیه مقدار منفرد[۳] نهان‌نگاری صورت گرفته‌است. مقاله [۵] یک نوع بهبودیافته از حوزه DWT را معرفی کرده‌است. 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 به‌نسبت خوبی را فراهم نموده‌اند.

نهان‌نگاری در ضرایب فرکانس میانی تبدیل موجک سبب شفافیت روش خواهد شد، ولی به‌دلیل 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 هم‌چون LSB

*نویسنده پاسخگو: znrozi@ihu.ac.ir

1- Robustness
2- Transparency
3- Singular Value Decomposition (SVD)

بهره برد، بلکه استفاده از طیف‌گسترده مناسب‌تر است. در مقاله [۸] بر موضوع طیف‌گسترده پرداخته ولی در این تحقیق، نشان‌گذاری مورد بحث قرار گرفته‌است. در مرجع [۹] یک آشکارساز محلی به‌روش ضربی به‌کمک 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 به‌میزان روشنایی پنجره‌ها (اندازه ماتریس‌ها) برای هر تصویر متمرکز شده‌است.

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 به‌روش طیف‌گسترده تصاویر[1] (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 مشخص‌شده 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 به‌صورت ریاضی تحلیل کرد. اگرچه نسخه‌های متفاوتی برای درج در نهان‌نگاری روش طیف‌گسترده ارائه‌شده 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 [۱۵-۱۴]. 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 به‌دست آوردن روابط احتمال خطا و ظرفیت به‌سادگی روش جمعی نیست و دیگر نمی‌توان از روابط تئوری اطلاعات و مخابرات بهره برد و نیاز به طراحی آشکارسازی مناسب دارد. در روش ضربی هرچه تبدیل مورد نظر سیگنال پوشانه را به‌صورت تنک‌تر[2] 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[3] استفاده شده‌است. 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 به‌وجود می‌آید. تبدیل موجک توصیف چند رزولوشنی[4] سیگنال است و کدگشایی[5] به‌صورت 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 به‌منظور پردازش زیرباندها، به‌صورت مستقل است.
۳. تبدیل موجک دارای ساختار شناخته شده‌ای به‌نام 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 به‌چشم می‌خورند.

به‌طور 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 بینائی انسان قابل درک نیست، اما در برابر حملات آسیب‌پذیر است. نهان‌سازی در زیرباندهای HL و LH مصالحه‌ای بین کیفیت و آسیب‌پذیری است. روش‌های جایگذاری در دامنه موجک به اندازه روش‌های حوزه DCT مورد بررسی و تحلیل قرار نگرفته‌اند.

در این مقاله از شباهت بیشینه (ML[6]) برای آشکارسازی مناسب بهره‌برداری شده است. تخمین شباهت بیشینه (MLE[7]) روشی برای محاسبه و تخمین پارامترهای یک مدل آماری است،

1- Spread Spectrum Image Steganography (SSIS)

2- Sparse
3- Haar
4- Approximation Subband
5- Decode
6- Maximum Likelihood
7- Maximum Likelihood Estimation

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 $x_1, x_2, ..., x_n$ وجود داشته باشد که مستقل از هم و دارای توزیع احتمال نامشخص f_0 باشند. f_0 به‌طور محتمل متعلق به یک خانواده مشخص از توزیع‌های نرمال مانند $\{f(0|\theta), \theta \in \Theta\}$ می‌باشد که مدل پارامتری نامیده می‌شود، بنابراین، $f(0|\theta) = f0$ می‌باشد و $\Theta =$ $\{\theta_0, \theta_1, ..., \theta_q\}$ 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:

$$f(x_1, x_2, ..., x_n | \theta) = f(x_1|\theta).f(x_2|\theta) \ ... \ f(x_n|\theta) \qquad (۱)$$

در نگاه دیگر، می‌توان گفت مشاهدات $x_1, x_2, ..., x_n$ 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.

$$L(\theta | x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n | \theta) = \prod_{i=1}^{n} f(x_i|\theta) \qquad (۲)$$

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

$$\ln L(\theta | x_1, x_2, ..., x_n) = \prod_{i=1}^{n} \ln f(x_i|\theta) \ , \ \hat{\ell} = \frac{1}{n} \ln L \qquad (۳)$$

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 شده‌ی $x_1, x_2, ..., x_n$ 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، اکسترمم بنا شده بر تابع هدف زیر است.

$$\hat{\ell}(\theta|x) = \frac{1}{n} \prod_{i=1}^{n} \ln f(x_i|\theta) \qquad (۴)$$

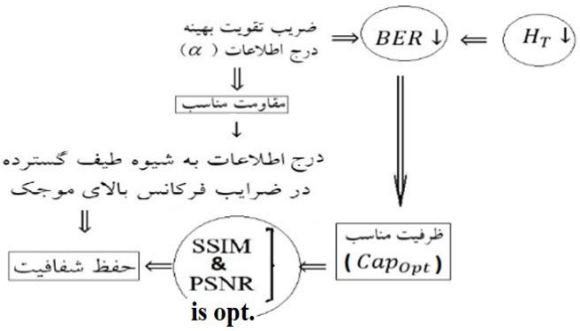
و مشابه نمونه‌ای آن شباهت لگاریتمی میانگین عبارت $\ell(\theta) = E\left[\ln f(x_i|\theta)\right]$ می‌باشد. در سیستم‌های دیجیتال اثر نویز و سایر عوامل مزاحم، سبب به‌اشتباه انداختن گیرنده در تشخیص بیت می‌شوند و به‌طور کلی میزان سلامت سامانه مخابراتی را می‌توان در انتقال با کم‌ترین اشتباه در مقصد سنجید، به‌همین منظور تعداد نسبی بیت های استخراج شده اشتباه، تعیین کننده نرخ خطای بیت (BER [1]) است. در این مقاله از BER برای ارزیابی آشکارسازی بهره گرفته 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 [۱۸-۱۷]. راه‌کاری که در این مقاله پیشنهاد می‌شود، استفاده از ضرایب فرکانس میانی تبدیل گسسته موجک برای ایجاد شفافیت مناسب استفاده شده است. روش تبدیل موجک یکی از روش‌های حوزه تبدیل است که در مقالات از آن استفاده می‌شود. در مقاله [۱۹] یک روش نهان‌نگاری بر مبنای تبدیل موجک است، که براساس الگوریتم ژنتیک در حوزه تبدیل موجک کار شده‌است و ظرفیت بالا در آن مورد نظر است. نهان‌نگاری بر اساس تبدیل موجک 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 شده‌است، 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 میانی کیفیت را کاهش نمی‌دهد ولی از مقاومت خوبی برخوردار نیست. به‌همین علت در این مقاله درج نهان‌نگاری در زیرباندهایی با فرکانس میانی پیشنهاد می‌شود. در روش پیشنهادی برای ارتقاء شفافیت نهان‌نگاری از ضرایب فرکانس میانی مبتنی بر طیف‌گسترده ضربی استفاده شده است که توان نهان‌نگاره متناسب با توان

1- Bit Error Rate

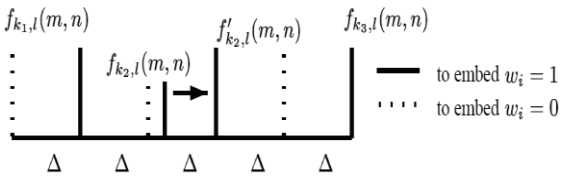
سیگنال تغییر خواهد کرد که این موضوع باعث کاهش مقاومت می‌شود. برای بهبود عملکرد مقاومت، در بسیاری از پژوهش‌ها از الگوریتم ML برای آشکارسازی داده استفاده شده است. راه‌کار اصلی پیشنهادی در این روش، نوآوری در ارائه الگوریتم آشکارسازی است که بتواند با کاهش خطای آشکارسازی نهان‌نگاره، مقاومت روش را افزایش دهد. 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 ویدیو 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 به‌علت خواصی 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 عموما 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 (مناطقی از تصویر که تغییرات سطح خاکستری زیاد است) برای مخفی‌کردن اطلاعات نهان استفاده می‌کند، الگوریتمی است که از زیرباندهای با فرکانس میانی برای 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[1] (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.

$$P(y_1, y_2, ..., y_N \mid 1) \underset{0}{\overset{1}{\gtrless}} P(y_1, y_2, ..., y_N \mid 0) \qquad (۵)$$

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

$$\begin{aligned} &y_{1|1} = \alpha.w_1 + n_1 \rightarrow y_{1|1} \sim N(\alpha\mu, \sigma^2_{y|1}) \\ &y_{1|0} = \alpha^{-1}.w_1 + n_1 \rightarrow y_{1|0} \sim N(\alpha^{-1}\mu, \sigma^2_{y|0}) \\ &\sigma^2_{y|1} = \alpha^2\sigma^2 + \sigma^2_n \\ &\sigma^2_{y|0} = \alpha^{-2}\sigma^2 + \sigma^2_n \end{aligned} \qquad (۶)$$

1- Reconstruction Point

واریانس نویز σ_n^2 به‌شکل زیر تخمین‌زده می‌شود و اگر انحراف معیار نویز در سیگنال تصویر σ^2 باشد، این مقدار به‌کمک ضرایب جزیی تبدیل موجک (HH_1) به‌وسیله تخمین‌گر مقاوم میانه طبق مرجع [۲۲] قابل تخمین‌زدن است:

$$\sigma_{approx} = \frac{Median(|Y_i|)}{0.6745};\ Y_i \in subband\ HH_1 \qquad (۷)$$

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

که در آن، L تقریب باند گسسته ضربه پاسخ است. با توجه به این‌که ضرایب تبدیل موجک در هر مرحله تجزیه، زیرنمونه می‌شوند، این ضرایب در مدل iid[1] در نظر گرفته شده‌اند. در نتیجه توزیع این ضرایب در یک بلوک مشخص با N ضریب $(y_1, y_2, ..., y_N)$ بعد از درج بیت یک و بیت صفر طبق رابطه(۸) می‌باشد:

$$P(y_1, y_2, ..., y_n \mid 1) = \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|1}^2}} e^{\beta_1}$$
$$P(y_1, y_2, ..., y_n \mid 0) = \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|0}^2}} e^{\beta_0} \qquad (۸)$$

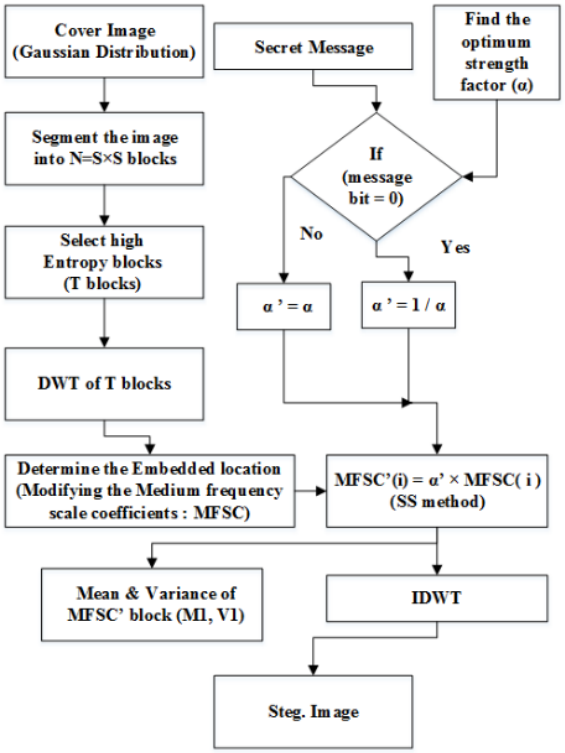
که در آن، $\beta_1 = \frac{(y_i - \alpha\mu)^2}{2\sigma^2_{y|1}}$ و $\beta_0 = \frac{(y_i - \alpha\mu)^2}{2\sigma^2_{y|0}}$ می‌باشند.با توجه به رابطه (۳)، آشکارساز مناسب با شیوه ML به شکل رابطه زیر تخمین زده می‌شود:

- اگر $\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|1}^2}} e^{\beta_1} > \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|0}^2}} e^{\beta_0}$ آنگاه عدد یک جایگذاری می‌شود.
- اگر $\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|1}^2}} e^{\beta_1} < \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_{y|0}^2}} e^{\beta_0}$ آنگاه عدد صفر جایگذاری می‌شود.

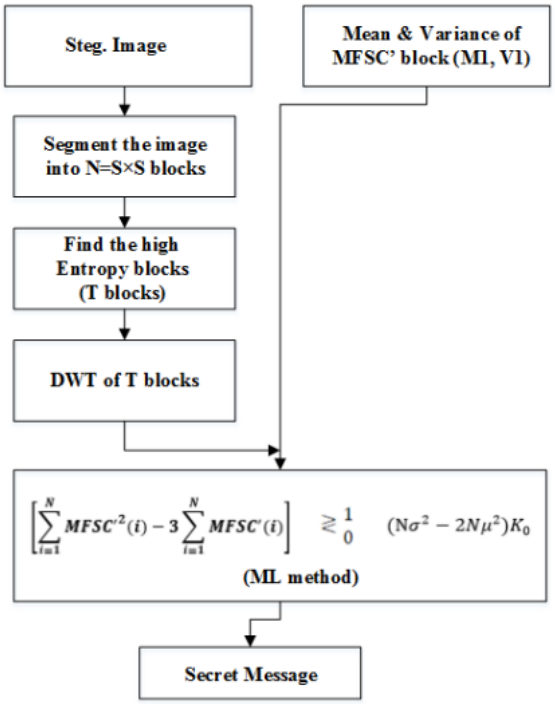
بعد از لگاریتم‌گیری طرفین، ساده‌سازی رابطه و فرض $\alpha = 1$ می‌توان بیان کرد که آشکارسازی مناسب در محیط‌های بـا نویز کم و $\alpha = 1$ طبق رابطه زیر محاسبه خواهد شد:

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

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): نهان‌نگاری در تصویر به شیوه موجک دوبعدی با سه سطح و فیلتر موجک هار

1- Identically Independently Distributed

۳-۲. افزایش مقاومت با مناسب‌سازی ضریب قدرت α

یکی از ویژگی‌های مهم الگوریتم‌های نهان‌نگاری مقاومت آن‌ها در برابر حملات می‌باشد، و در طراحی و بررسی کارآیی آن‌ها باید این ویژگی را مد نظر داشت. عمومی‌ترین حملات نهان‌نگاری، حملات مکانی هستند که از آن جمله می‌توان به چرخش، برش[1] و جابجایی اشاره کرد. برخی از حملات به‌صورت غیرعمدی پس از منتشر شدن تصویر رخ می‌دهند که فشرده‌سازی از این نوع است. اما گروهی دیگر مانند حملات حذفی به‌صورت عمدی صورت می‌گیرند. تمام روش‌های تست مقاومت استیرمارک[2] ارائه شده توسط پتیت‌کولاس[3] و همکارانش در[۲۳] جهت مقایسه و برآورد الگوریتم‌های نهان‌نگاری به‌کار می‌رود. حملات در این محک شامل حملات هندسی (اعوجاج‌های هندسی، مقیاس‌دهی، برش و غیره)، اعمال نویز و سایر عملیات پردازش سیگنال مانند فشرده‌سازی، اعمال فیلتر میانگین و یا اعمال فیلتر میانه است. که در این مقاله جهت ارزیابی مقاومت از آن استفاده شده است.

با مناسب‌سازی ضریب قدرت α و در واقع کاهش احتمال خطای آشکارسازی، مقاومت الگوریتم بهتر خواهد شد. در روش پیشنهادی، دو شیوه بازخوردی و محاسباتی برای یافتن α مناسب مطرح شده است. در روش محاسباتی، در ابتدا احتمال خطای آشکارسازی سیستم (با وجود نویز سفید گوسی) را با توجه به مقاله [۲۴، ۲۵] طبق رابطه (۹) می‌توان به‌دست آورد.

$$p_e = \frac{1}{2}p_{e|1} + \frac{1}{2}p_{e|0} = \frac{1}{2}\left[\frac{1}{\sqrt{2\pi N\sigma_{y|1}^2}}\cdot\frac{a_1}{a_2}\int_0^{\infty} Y\left(\frac{N}{2},\frac{x}{2}\right)e^{-\delta_1}dx\right] + \frac{1}{2}\left[\frac{1}{\sqrt{2\pi N\sigma_{y|0}^2}}\cdot\frac{b_1}{b_2}\int_0^{\infty} Y\left(\frac{N}{2},\frac{x}{2}\right)e^{-\delta_2}dx\right] \quad (۹)$$

که در آن، $\delta_1 = \frac{(\frac{T'-a_1x}{a_2}\mathrm{N}\alpha\mu)^2}{2N\sigma_{y|1}^2}$ و $\delta_2 = \frac{(\frac{T'-b_1x}{b_2}\mathrm{N}\alpha^{-1}\mu)^2}{2N\sigma_{y|0}^2}$ می‌باشند.

حال برای هر بلوک رابطه ضریب کیفیت (۱۰) را داریم [۲۴، ۲۵]:

$$Q_j = \frac{(\mu_C\mu_S + (\mathrm{K_1 l})^2)}{((\mu_C^2)+(\mu_S^2)+(\mathrm{K_1 l})^2)} \times \frac{((2(\frac{1}{N-1})\sum_{i=1}^{N}(HFCS(i)-\mu_C)(\mathrm{HFSC'(i)}-\mu_S))+(\mathrm{K_2 l})^2)}{((\sigma_C^2)+(\sigma_S^2)+(\mathrm{K_2 l})^2)} \quad (۱۰)$$

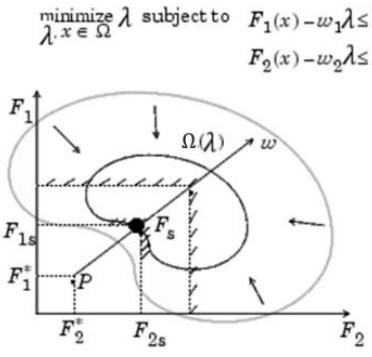
که در آن، l بازه دینامیکی تغییرات نمونه‌های تصویر است (۲۵۵ برای ۸ بیت) و $K_1, K_2 << l$ (در اینجا $K_1 = 0.01$ و $K_2 = 0.03$). از ضریب کیفیت تمامی بلوک‌ها، میانگین حسابی می‌گیریم تا اندیس کیفیت نهایی حاصل شود. اما چون قضاوت بصری عموماً بر روی بدترین بلوک‌ها صورت می‌پذیرد، از میانگین هندسی استفاده کرده‌ایم.

با تعریف اندیس اندازه‌گیری کیفیت، دو تابع هدف (۱۱) مورد نظر است. تابع $f_D(\alpha)$ که بیان‌گر نقش α در مسیر اعوجاج بوده و تابع یکنوا و صعودی از α است و تابع α که بیان‌گر مقاومت الگوریتم بوده و تابع اکیداً نزولی است.

$$f_D(\alpha) = 1 - Q(\alpha) \ , \ f_E(\alpha) = p_e \quad (۱۱)$$

ایده ما در اینجا پیدا کردن α مناسب برای کمینه‌کردن هر دو تابع هدف است. چون ماهیت دو تابع باهم تفاوت دارد، نمی‌توان به‌صورت وزن‌دار جمع کرد. لذا از روش مطرح شده جمبیکی[4] [۲۶] استفاده می‌کنیم. در این روش برای متناسب‌سازی مقدار m تابعی که بین آن‌ها مصالحه وجود دارد، یک‌سری اهداف طراحی $F^* = [\mathrm{F_1^*}, \mathrm{F_2^*}, \cdots, \mathrm{F_m^*}]$ به‌همراه مجموعه توابع هدف $F = [\mathrm{F_1}, \mathrm{F_2}, \cdots, \mathrm{F_m}]$ در نظر گرفته می‌شود که با اتخاذ وزن دلخواه $\omega = [\omega_1, \omega_2, \cdots, \omega_m]$، با کمینه‌سازی رابطه (۱۲)، آنگاه ناحیه مناسب $\boldsymbol{\lambda}$ حاصل می‌شود. در شکل (۴) چگونگی این فرآیند برای دو تابع هدف آمده است.

$$\underset{\lambda, x\in\Omega}{\text{minimize}}\ \lambda \quad \text{subject to} \quad \mathrm{F_i}(x) - \omega_i\lambda \le \mathrm{F_i^*} \ , \ i = 1,2,\ldots,m \quad (۱۲)$$



شکل (۴): یافتن مقدار مناسب λ به روش جمبیکی

که در آن، Ω ناحیه حصول در فضا و پارامترهای x و λ متغیر کمکی بدون علامت هستند. بردار وزن ω کمک به برقراری مصالحه مناسب بین اهداف را بر عهده دارد. یعنی اگر بتوان یک هدف را با مقادیر بیشتر تحمل کرد، وزن کمتری به آن تخصیص داده می‌شود و بالعکس. $\Omega(\lambda)$ یک ناحیه قابل دسترس در فضای

1 Clipping
2 Stirmark
3 Petitcolas
4 Gembicki

توابع هدف است. کم‌ترین مقدار λ در F_S رخ می‌دهد، جایی که بـــــردار $F^* + \omega\lambda$ مرز پایینی اهداف را قطع می‌کند. مقدار مناسب α که معادل λ است، کمی بزرگ‌تر از 1 است. به‌عنوان مثال در نمودار مربوط به جدول (۳) نحوه به‌دست 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 به‌دست آوردیم تا در برابر حملاتی مانند مقیاس، بُرش، فیلتر میانه، فیلتر گوسی و چرخش مقاومت داشته باشد. به‌عنوان 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. به‌عبارت دیگر ظرفیت نهان‌نگاری، ظرفیت قابل جایگذاری برای حداکثر میزان داده‌ای[1] 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. به‌علت فقدان مدل‌های آماری دقیق برای تصاویر طبیعی، روش‌های نهان‌نگاری از دید مدل تئوری ضرایبDCT مورد بررسی قرار نگرفته‌اند [۲۷]. محققان معتقدند که برای به‌دست آوردن جواب قابل‌قبول، 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] به‌جای بررسی مدل تئوری، به آخرین روش‌های نهان‌کاوی توجه شده است. یک مدل مناسب برای تصاویر، فرمتJPEG 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[2] از امنیت نهان‌نگاری، بررسی می‌کند. ویژگی‌های تصویر پوشانه، pdf[3] تصاویر پوشانه را مدل می‌کند. امنیت سیستم نهان‌نگاری می‌تواند با فاصله KL[4] میان توزیع آماری تصاویر بدون پیام P_C و تصاویر حاوی پیام P_Sدر فضای ویژگی ارزیابی شود. فاصله KL در رابطه (۱۳) آمده است. طبق تعریف بهبودیافته کشین، الگوی جایگذاری امن است اگـــــر آنتروپی نسبی میان P_C و P_S برابر با ε-امنیت[5] باشد یعنی $H(P_C \mid P_S) = \varepsilon_{Secure}$. با توجه به [۳۲] اگر نهان‌نگاری امن کامل باشد، پارامترهای SSIM و PSNR دارای مقادیر مناسب و خوبی هستند که به‌معنی 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.

$$H(P_c|P_s) = \sum_{I\in Cover} P_c(I) log \frac{P_c(I)}{P_s(I)} \quad \therefore \{H(P_c|P_s) \to 0\} \Rightarrow \{Cap_{Opt}\ (Capacity \to Optimum)\} \qquad (۱۳)$$

هدف تحقیق [۲۰] تعیین ظرفیت نهان‌نگاری در تصاویر JPEG (بیش‌ترین میزان داده‌ای که به‌صورت غیرقابل تشخیص می‌تواند در یک تصویر JPEG جایگذاری شود) با در نظر گرفتن روش‌های نهان‌نگاری است. به‌علاوه با آزمایش الگوریتم‌های نهان‌نگاری منتخب، تاثیر المان‌ها و اصول طراحی بررسی می‌شود. به‌عنوان 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 موجک به‌صورت 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.

$$H_T \downarrow \Rightarrow \{BER \downarrow \ \& \ D \uparrow\} \quad \therefore \quad Cap_{Opt} \geq D \qquad (۱۴)$$

که $\mathbf{H_T}$ سطح آستانه بیشینه بی‌نظمی و D میزان آشکارسازی است. به‌طور کلی بیش‌ترین میزان آنتروپی برای یک متغیر

1- Payload
2- Cachin
3- probability density function
4- Kullback-beibler
5- ε Secure
6- Quality Factor

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.

$$P_f = 1 - (1 - BER)^F \quad \text{احتمال نادرستی بیت‌ها} \qquad (۱۵)$$

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

$$P_f = (1 - BER)^F \quad \text{احتمال درستی بیت‌ها} \qquad (۱۶)$$

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

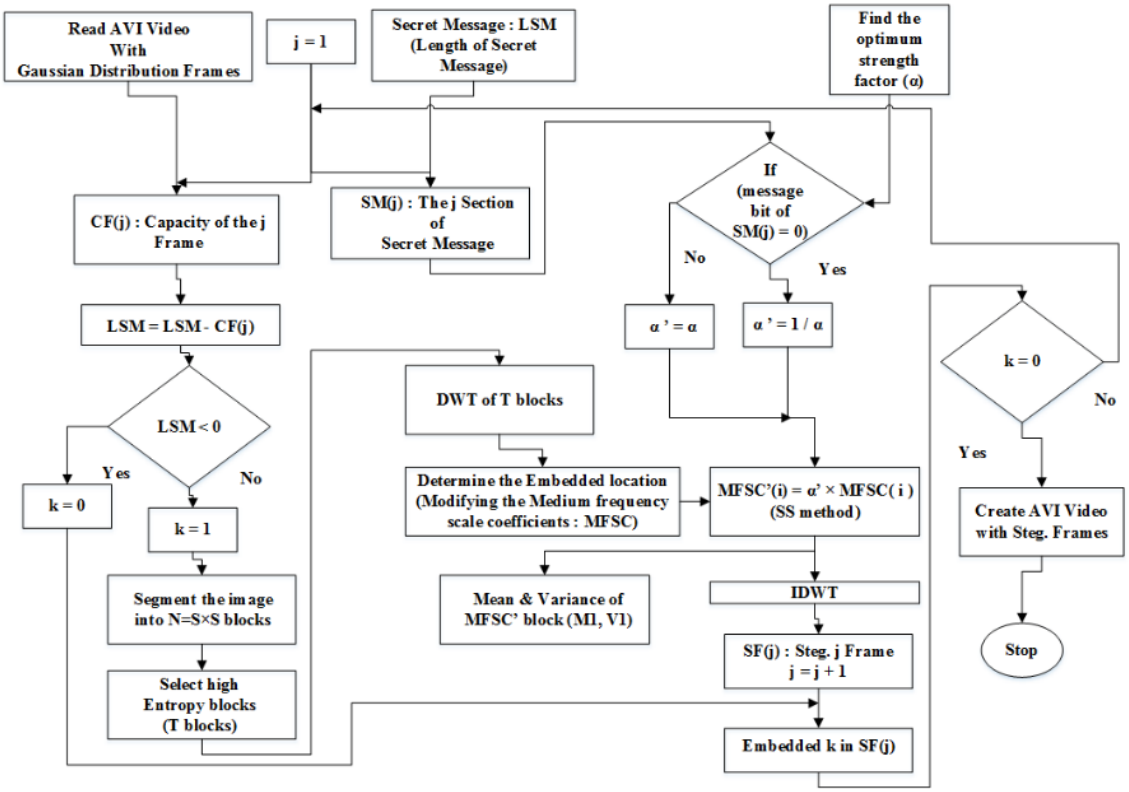
$$\begin{aligned} H_T &= -\sum_{i=1}^{n} P_t(x_i) log_2 P_t(x_i) \\ &= -\sum_{i=1}^{n} \left(1 - BER_{x_i}\right)^{F_{x_i}} log_2 \left(1 - BER_{x_i}\right)^{F_{x_i}} \\ &\therefore H_T \downarrow \implies BER \downarrow \end{aligned} \qquad (۱۷)$$

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

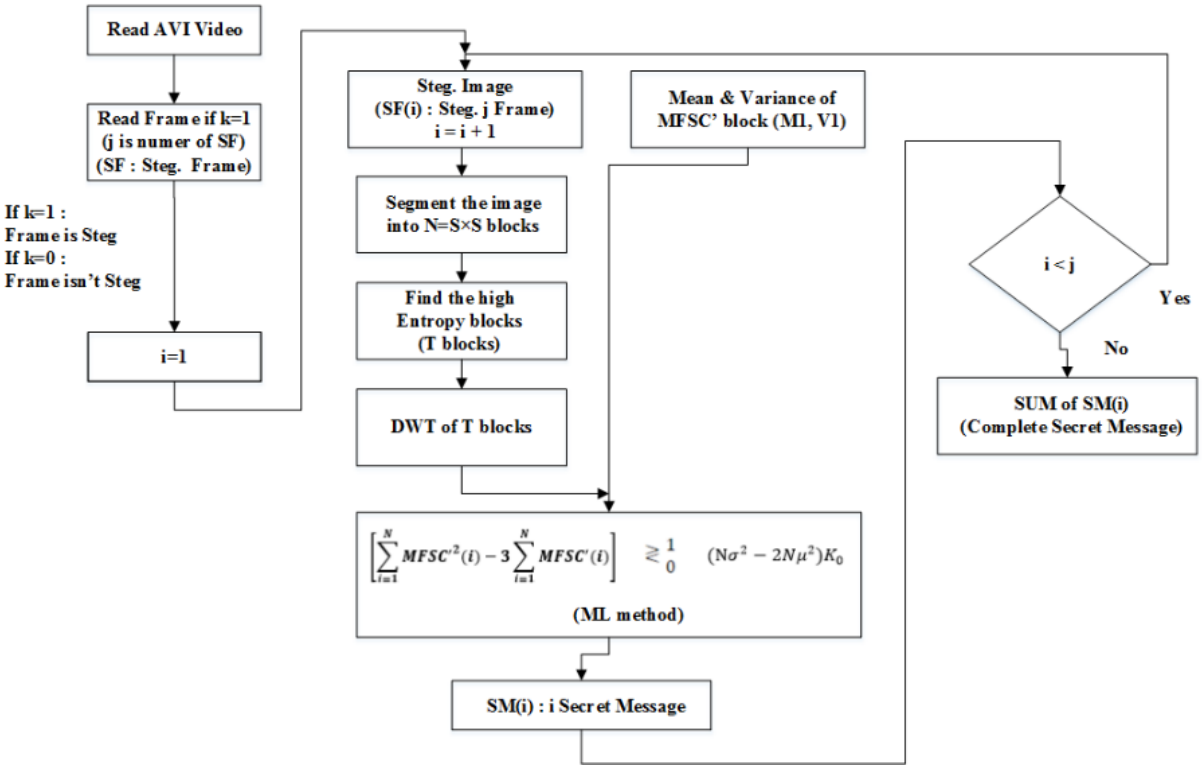
- فریم‌های ویدیوی خام: ممکن است اندازه ظرفیت مناسب، کوچک‌تر از کل داده محرمانه برای درج باشد، آن‌گاه می‌توان نهان‌نگاری دسته‌ای را مطرح کرد. نهان‌نگاری دسته‌ای مساله پنهان‌کردن و نهان‌کاوی را به چندین شیء پوشانه تعمیم می‌دهد [۳۱]. کِر[1] در [۳۱] ظرفیت نهان‌نگاری دسته‌ای را تعریف می‌کند و به‌صورت تئوری 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[2] 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 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[3]» 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 مخفی‌کردن 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 نهان‌کاوی دسته‌ای[4] 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 تصویرحاوی پیام و چند تصویر بدون پیام است. در [۳۵] نشان داده‌شده 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[5] عرضه‌شده در نوامبر ۱۹۹۲ توسط مایکروسافت، به‌دلیل 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 j 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 به‌معنی ادامه داشتن است و *k=0* یعنی آخرین تصویر درج است.

1- Ker
2- Fridrich
3- Static batch steganography
4- Pooled steganalysis approach
5- Audio Video Interleave



الف) ساختار جاسازی داده



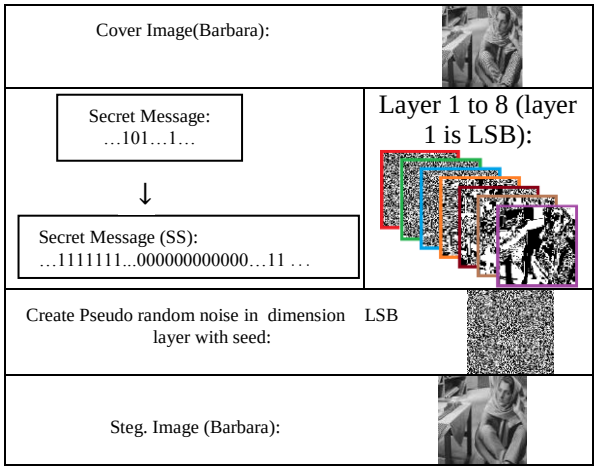
ب) ساختار استخراج داده

شکل (۵): نهان‌نگاری در فریم‌های ویدیوی خام

۴. نتایج تجربی

۴-۱. مقایسه روش ضربی و جمعی

در شکل (۶) مثال درج به‌شکلی ساده در حالت طیف‌گسترده آورده شده‌است. درج به‌روش‌های جمعی و ضربی صورت گرفته است.



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

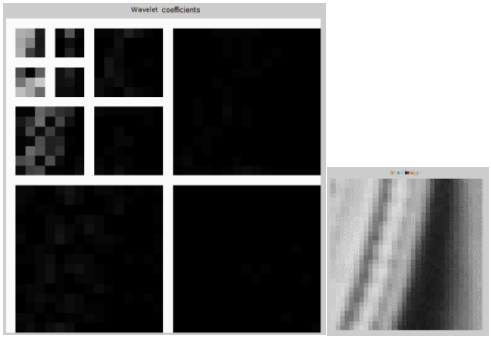
همان‌طور که در جدول (۱) بخش نتایج تجربی قابل مشاهده است، روش ضربی در مقایسه با روش جمعی در حوزه مکان دارای درصد آشکارسازی کم‌تری است زیرا متناسب‌سازی پارامتر، به‌دست آوردن روابط احتمال خطا و ظرفیت به‌سادگی روش جمعی نیست. در روش ضربی هرچه تبدیل مورد نظر سیگنال میزبان به‌صورت تنک‌تر نمایش داده شود، عملکرد روش در آن حوزه بهتر می‌گردد. لذا استفاده از تبدیل‌های چنددقتی جدانشدنی مانند کانتورلت و ریجلت گسسته سبب افزایش چشم‌گیر عملکرد روش‌های ضربی برای تصاویر می‌گردد [۳۶، ۲۴].

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

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

۴-۲. نتایج شفافیت

به‌عنوان 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 به‌کمک موجک دوبعدی با سه سطح و فیلتر موجک هار و به‌شیوه طیف‌گسترده عمل نهان‌نگاری اطلاعات (شامل یک بردار ۲۰۰ بیتی) در ضرایب فرکانس میانی موجک بلوک‌های ۳۲×۳۲ از تصویر صورت می‌گیرد. شکل (۷- الف) اولین بلوک ۳۲×۳۲ از تصویر است و شکل (۷- ب) ضرایب تبدیل موجک اولین بلوک ۳۲×۳۲ از تصویر را نمایش می‌دهد.



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

ج) تصویر بالا: اصلی؛ تصویر پائین: نهان‌نگاری‌شده

شکل (۷): نهان‌نگاری در تصویر Barbara به شیوه‌ی 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[1]) را نشان می‌دهد.

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

[1] Low Frequency Scale Coefficients

۴-۳. نتایج مقاومت

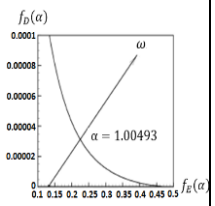
مطابق با جدول (۳) با انتخاب بردار وزن

$$(\omega_{f_D(\alpha)}, \omega_{f_E(\alpha)}) = [۰/۶۵, ۰/۴۵]$$

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

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

$f_E(\alpha)$	$f_D(\alpha)$	α
۰/۴۱۵	۰/۰۰۰۰۰۰۲۵	۱/۰۰۳
۰/۳۴۵	۰/۰۰۰۰۰۰۷۷	۰/۰۰۳۵
۰/۲۸۲	۰/۰۰۰۰۰۱۵	۰۱/۰۰۴
۰/۲۴	۰/۰۰۰۰۰۲۶	۱/۰۰۴۵
۰/۲۳	۰/۰۰۰۰۰۲۵	/۰۰۴۹۳ ۱
۰/۲	۰/۰۰۰۰۰۴۱	۱/۰۰۵
۰/۱۷۵	۰/۰۰۰۰۰۵۸	۱/۰۰۵۵
۰/۱۵	۰/۰۰۰۰۰۷۹	۱/۰۰۶
۰/۱۳۵	۰/۰۰۰۰۱۰۵	۱/۰۰۶۵



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 ۱/۰۰۴۹۳) 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 ۳۲×۳۲ باربارا با آنتروپی کل تصویر ۷/۶۴۱۸ آورده شده‌است. درج در تمام بلوک‌های ۳۲×۳۲، بدون در نظر گرفتن بیشینه بی‌نظمی بلوک‌ها می‌باشد. طول پیام ۴۰۹۶ بیت است و درج در ضرایب فرکانس میانی موجک انجام شده‌است.

حال اگر در جدول قبل، در بلوک‌های دارای بیشینه بی‌نظمی، درج صورت گیرد، مقدار α کم‌تر شده و به‌عبارتی بهتر می‌شود. به‌عنوان مثال در حالت ۱/۰۰۴۹۳ = α مقدار BER برابر با ۰/۱۳۵۹ خواهد بود و درحالت ۱/۴۹۳ = α مقدار BER برابر با ۰/۱۴۹۴ خواهد بود. نتایج تست تخمین اطلاعات به‌شیوه ML در آشکارسازی مناسب با روش ضربی نیمه‌کور نهان‌نگاری در تصویر ۳۲×۳۲ باربارا با آنتروپی‌های مختلف در جدول (۶) آمده است.

جدول (۵): نتایج نهان‌نگاری بدون در نظرگرفتن بیشینه بی‌نظمی بلوک‌ها

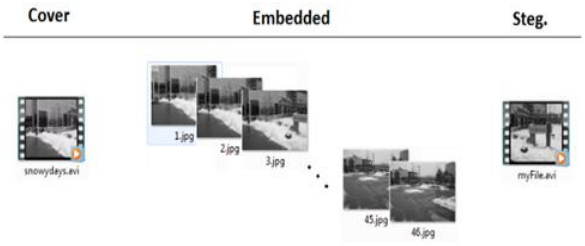
حمله مقیاس	
ضریب مقیاس	BER
۰/۹	۰/۱۲۰۱
۱/۱	۰/۱۷۶
۱/۴	۰/۱۹۳
۱/۷	۰/۲۲۳
۲	۰/۲۸۹
حمله بُرش	
بُریدن	BER
۵٪	۰/۱۷۸
۱۰٪	۰/۲۰۱
۱۵٪	۰/۲۴۱
حمله فیلتر میانه	
فیلتر میانه	BER
۳×۳	۰/۱۸۵
۵×۵	۰/۲۷۴
حمله فیلتر گوسی	
فیلتر میانه	BER
۳×۳	۰/۱۸۹
۵×۵	۰/۲۷۸
۷×۷	۰/۲۸۹
حمله چرخش	
زاویه چرخش (درجه)	BER
۵	۰/۲۱۲
۲	۰/۲۱۱
۱	۰/۱۹۲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

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	۱/۰۴۹۳	۱/۴۹۳	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= ۰/۷۶۴۲)	۰/۱۵۱۸	۰/۱۳۸۱	۰/۱۴۵۲	۰/۱۳۸۹	۹۹/۸۵٪	۹۹/۸۵٪
BER (H= ۳/۸۲۰۹)	۰/۲۳۵۷	۰/۲۳۴۵	۰/۲۲۹۴	۰/۲۳۸۴	۷۲/۶۳٪	۷۲/۳۸٪

افزایش ظرفیت به کمک فریم‌های ویدیی 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 فریمِ دارای آنتروپی نسبتاً پایین (۷/۴۵۶۷۲)، به‌دست آمده‌است (شکل ۸).



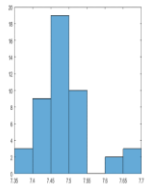
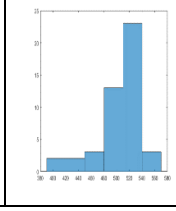
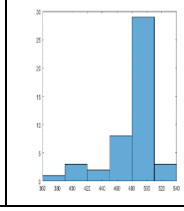
شکل (۸): نهان‌نگاری در فریم‌های ویدیو Snowdays.avi

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 نهان نگاری می‌شود، وجود دارد. اگر میزان اطلاعات زیادی در یک تصویر جایگذاری شود آنگاه قابلیت شناسایی افزایش می‌یابد[۳۷]. همان‌طور که در جدول (۷) نشان داده‌شده با در نظرگرفتن سطح آستانه آنتروپی ۷/۵ موارد ذیل به‌دست آمده است:

- مناسب‌ترین *ظرفیت* (در حالت بیش‌ترین مقدار SSIM و PSNR به‌عبارتی *شفافیت* فریم) در فریم دارای پایین‌ترین آنتروپی (۷/۳۷۴۷۶۴) به‌دست آمده‌است.
- کم‌ترین BER (با درنظرگرفتن 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 برروی فریم‌های ویدیوی خام

Entropy of cover	No. of message embedded bits	No. of message detected bits
		

Frame No.	$\alpha_{Optimum}$	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)	۰/۱۵۸۳۹۴	۴۲/۶۶۹۴	۰/۹۹۷۳۵۳
۳	۱/۰۰۴۷۴۹	۷/۶۵۶۲۵۴	۴۱۷	۹۳/۷۶٪(۳۹۱)	۰/۱۶۲۳۵۰	43.5623 ۴۳/۵۶۲۳	۰/۹۹۷۷۵۵
۴	۱/۰۰۴۷۴۱	۷/۶۴۲۱۵۶	۴۵۲	Min= ۹۳/۵۸٪(۴۳۶)	Max= ۰/۱۶۴۱۵۹	۴۲/۸۸۶۳۷	۰/۹۹۷۳۳۵
...	...	...	...	...	...	...	...
۱۷	۱/۰۰۴۸۲۸	۷/۴۴۹۴۸	۵۴۲	۹۴/۸۳٪(۵۱۴)	۰/۱۵۱۶۰۰	۴۲/۹۴۲۵۵	۰/۹۹۷۰۳۱

۱۸	۱/۰۰۴۷۵۳	۷/۴۵۶۷۲	Max=۵۵۸	۹۳/۹٪(۵۲۴)	۰/۱۶۰۹۳۱	۴۲/۱۸۶۹۹	۰/۹۹۶۷۷۹
۱۹	۱/۰۰۴۹۳۱	۷/۴۶۵۱۴۵	۵۵۳	۹۵/۱۲٪(۵۲۶)	۰/۱۴۸۸۲۴	۴۲/۷۹۴۱۷	۰/۹۹۷۰۹۶
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
۳۴	۱/۰۰۴۷۳۸	Min= ۷/۳۷۴۷۶۴	۴۹۵	۹۳/۷۳٪(۴۶۴)	۰/۱۶۲۶۲۶	Max= ۴۵/۱۳۵۸	Max= ۰/۹۹۸۰۳
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
۴۶	۱/۰۰۴۹۳۵	۷/۴۸۸۶۵۸	۵۱۳	Max= ۹۶/۱٪(۴۹۳)	Min= ۰/۱۳۸۹۸۶	۴۱/۸۰۶۰۶	۰/۹۹۷۰۴۳

الگوریتم پیشنهادی را طبق مقاله [۳۸] ، با پوشانه‌های تصاویر انتخابی آزمایش کردیم، به‌طوری که تصویر پوشانه از سطح امنیت خوبی برخوردار بود، میانگین نتایج آزمون برروی ۱۰۰ تصویر به‌صورت جدول(۸) حاصل شد که نتیجه تمام پارمترها در حالت بیشینه بود.

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

$\alpha_{Optimum}$	Entropy of Steg.	Bits of Message	Percent of Detected (Bits)	BER	PSNR	SSIM
۱/۰۰۴۷۳۷	۷/۶۵۲۱۵۷	۵۵۷	۹۶٪(۴۹۲)	۰/۱۶۵۱۰۷	۴۵/۲۷۶۴	۰/۹۹۹۰۱

۴-۶. بررسی در برابر نهان‌کاو WAM و FARID

درج در فریم‌های ویدیوی خام در برابر نهان‌کاو WAM و FARID مورد آزمایش قرار گرفت. در ابتدا از حدود ۲۴۰۰ تا ۶۰۰۰ فریم (حدود چهار دقیقه ویدیو) آماده کرده و بر روی۱۲۰۰ تا ۳۰۰۰ فریم با نرخ ۲۵٪ درج به‌روش پیشنهادی انجام شده است. ۱۵۰۰ فریم برای آموزش و نصف دیگر برای تست استفاده شد؛ به کمک طبقه‌بندی FLD مقادیر AUC، برای هر حالت نهان‌کاو WAM و FARID محاسبه شد. سپس در مرحله دیگر، در فریم‌ها به‌شیوه JSteg، (دلیل مقایسه با این روش، شباهت‌های ساختاری و پرکاربرد بودن JSteg با این روش پیشنهادی بوده است) درج نهان‌نگاری صورت گرفت و مقادیر AUC، برای هر حالت نهان‌کاو WAM و FARID نیز محاسبه شد. هر چه مقدار AUC مربوط به یک طبقه‌بند بزرگ‌تر باشد کارآیی نهایی طبقه‌بند مطلوب‌تر ارزیابی می‌شود. در واقع هرچه AUC به‌عدد یک نزدیک‌تر باشد، کارآیی قویِ‌ترِ نهان‌کاو را نشان می‌دهد و هرچه به ۰/۵ نزدیک‌تر باشد، کارآیی ضعیف‌ترِ نهان‌کاو را نشان می‌دهد مطابق جدول (۹)، روش پیشنهادی نسبت به JSteg رفتار مقاوم‌تری در برابر نهان‌کاوهای WAM و FARID داشت.

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

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

۵. نتیجه‌گیری

نهان‌نگاری مبتنی بر آشکارسازی مناسب، با مصالحه سه مؤلفه شفافیت، مقاومت و ظرفیت ارتباط مستقیم دارد. با مقایسه تجربی نهان‌نگاری در ضرایب فرکانس پایین و فرکانس میانی تبدیل موجک، می‌توان مشاهده کرد که برای حفظ شفافیت، در بخش فرستنده، از درج اطلاعات به‌شیوه طیف‌گسترده در ضرایب فرکانس میانی موجک استفاده شده است. اما این موضوع باعث کاهش مقاومت می‌شود که در این مقاله نشان داده شده است. با به‌دست‌آوردن پارامتر ضریب قدرت مناسب درج اطلاعات (α)، مقاومت کاهش نمی‌یابد و در واقع برای بهبود مقاومت، در بخش گیرنده، ارائه راه‌کاری برای کاهش خطای آشکارسازی داده نهان در الگوریتم ML مطرح شده است. برای حفظ ظرفیت نهان‌نگاری، راه‌کار دو مرحله‌ای ارائه شد که به‌ترتیب برای محاسبه ظرفیت مناسب به کمک پوشانه‌های با آنتروپی پایین و برای پوشش درج کل داده‌های محرمانه به‌علت نداشتن یک بانک مناسب با مولفه‌های تاثیرگذار هم‌چون کنتراست، انرژی و غیره، است. با این وجود پیشنهاد نویسندگان مقاله استفاده از فریم‌های ویدیویی خام است.

برای تحقیقات آینده روش‌های دیگر به جز تبدیل موجک را می‌توان مورد بررسی قرار داد. تبدیل موجک با وجود داشتن مزایای فراوان، نقاط ضعف‌هایی دارد که محققان را بر این می‌دارد که روش‌های جدیدی را پایه‌گذاری نمایند. این تبدیل دارای دو مشکل اصلی است. مشکل اول، حساس بودن نسبت به تغییرات؛ یعنی هرگاه در ضرایب تبدیل موجک تغییری صورت گیرد، باعث تغییرات زیادی در سیگنال ورودی می‌شود. این اشکال به خاطر

انجام عمل نمونه‌برداری کاهشی می‌باشد. مشکل دوم، جهت‌های انتخابی محدود[1]؛ 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 به‌صورت 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 ریجلت 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. Dejey, 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 Communica-tions, Vol. 64(2), pp. 112-124. 2010.

[7] Q. Chen, and M. Xiong, "Dual Watermarking Based on Wavelet Trans-form for Data Protection in Smart 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," Proceding 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.

1 Lack of directional selectivity

2- Dual-Tree Complex Wavelet Transform

[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.

[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.

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

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

R. Esfahani, Z. Norozi*, 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: znrozi@ihu.ac.ir