# ارائه یک روش پنهان‌شکنی از تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک

حیدر باجلان [۱]، محمد پویان[۲]، سید وهاب شجاع الدینی[۳]

[۱] دانشگاه آزاد اسلامی واحد قزوین، دانشکده مهندسی برق، پزشکی و مکاترونیک، h.bajalan@qiau.ac.ir

[۲] دانشگاه شاهد، دانشکده مهندسی، pooyan@shahed.ac.ir

[۳] سازمان پژوهش های علمی و صنعتی ایران، پژوهشکده برق و فناوری اطلاعات، shojadini@irost.ir

**چکیده.**

در این مقاله، یک روش پنهان‌شکنی برای تصاویر پنهان‌نگاری شده در حوزه موجک ارائه شده است. در این روش، ویژگی‌های استخراج شده شامل گشتاورهای تابع مشخصه حاصل از هیستوگرام مرتبه دوم بدست آمده از تصویر می‌باشد. بردار ویژگی بدست آمده دارای ۲۴ بعد می‌باشد که شامل چهار مجموعه شش تایی از گشتاورهای تابع مشخصه دو بعدی است. هر مجموعه شش تایی گشتاورها از یک ماتریس هیستوگرام مرتبه دوم با یک جدایی خاص بدست می‌آید. بردار ویژگی بدست آمده برای دسته بندی به ماشین بردار پشتیبان داده می‌شود تا در مورد پوشانه یا گنجانه بودن تصویر تصمیم گیری کند. روش پیشنهادی برای پنهان‌شکنی از دو روش پنهان‌نگاری در حوزه موجک جدید بکار گرفته شد. نتایج آزمایش‌ها نشان می دهد که روش‌های پیشنهادی، نتایج آشکارسازی روش‌های پنهان‌شکنی موجود، که بر روی تصاویر پنهان‌نگاری شده در حوزه موجک آزمایش شده‌اند را بهبود می‌دهد.

**واژه‌های کلیدی**

پنهان‌شکنی، پنهان‌نگاری، تبدیل موجک، گشتاورهای تابع مشخصه.

## ۱- مقدمه

در پنهان‌نگاری دیجیتال، محیط دیجیتالی برای رمزگذاری و پنهان‌کردن دنباله‌ای از بیت‌های پیام، به گونه‌ای اصلاح می‌شود که ارتباط مخفی مورد شک قرار نگیرد. در پنهان‌شکنی دیجیتال، سعی می‌شود این نوع ارتباط پوشیده تشخیص داده شود[۱]. پنهان‌شکنی دو نوع است: پنهان‌شکنی فعال و پنهان‌شکنی غیر فعال. پنهان‌شکنی غیر فعال اقدام به تشخیص وجود یا عدم وجود پیام مخفی در تصویر می‌کند. اما پنهان‌شکنی فعال علاوه بر تشخیص وجود پیام به تخمین طول پیام، بیت‌های پیام، کلید رمز و ... می‌پردازد. پنهان‌شکنی فعال در مقایسه با پنهان‌شکنی غیر فعال بسیار مشکل‌تر است. تکنیک‌های پنهان‌شکنی اخیر بر روی حضور یا عدم حضور پیام مخفی تمرکز می‌کنند[۲].

از یک دیدگاه الگوریتم‌های پنهان‌نگاری به دو گروه تقسیم می‌شوند. دسته ای از آنها روش‌های حوزه مکان نام دارند که به طور مستقیم به سیگنال اعمال می‌شوند. دسته ای دیگر روش‌های حوزه تبدیل نام دارند که بر روی تبدیل یافته سیگنال اعمال می‌شوند. سه حوزه عمده تبدیل، تبدیل فوریه گسسته (DFT)، تبدیل کسینوسی گسسته (DCT) و تبدیل موجک گسسته (DWT) می‌باشند[۳] . برای هر یک از الگوریتم‌های حوزه‌های تبدیل، روش‌های پنهان‌شکنی خاصی ارائه شده است. در این تحقیق یک روش پنهان‌شکنی غیر فعال که برای تصاویر پنهان‌نگاری شده در حوزه موجک بکار می رود، ارائه گردیده است.

فرید، یک روش پنهان‌شکنی ارائه کرد که در آن بوسیله فیلترهای آیینه‌ای متعامد (QMF) تصویر را در حوزه موجک تجزیه نمود. وی در روش خود آماره‌های مرتبه بالاتر شامل میانگین، واریانس، خمیدگی و درجه اوج نمودار آماری را از تابع چگالی احتمال مربوط به هر زیرباند تبدیل موجک تصویر استخراج کرد. وی همچنین آماره های مشابهی را از دامنه ضرایب پیش بینی شده هر زیرباند که بوسیله یک پیش بینی کننده خطی بهینه پیشگویی شده‌اند، استخراج نمود. ویژگی‌های بدست آمده برای دسته بندی به یک طبقه بندی کننده خطی فیشر (FLD) داده شدند[۴]. لیو و فرید، روش فرید را با ماشین بردار پشتیبان (SVM) به عنوان دسته-بندی کننده بکار بردند. این روش به روش پنهان‌شکنی بر مبنای موجک (WBS) معروف است[۵].

شی، روش پنهان‌شکنی را ارائه کرد که در آن ویژگی‌های مورد استفاده شامل گشتاورهای آماری توابع مشخصه تصویر اصلی، تصویر خطای پیشگویی شده و زیرباندهای تبدیل موجک آنها می‌باشد. دسته بندی کننده مورد استفاده وی، شبکه عصبی مصنوعی است[۶].

در الگوریتم پنهان‌شکنی فراگیر ارائه شده توسط چن، ابتدا از مقادیر قدرمطلق ضرایب تبدیل کسینوسی گسسته بلوکی آرایه دو بعدی JPEG تصویر ورودی، بوسیله موجک هار تبدیل موجک سه سطحی گرفته می‌شود. سپس برای هر زیرباند بدست آمده از آرایه دو بعدی JPEG ، سه هیستوگرام مرتبه دوم افقی، عمودی و قطری تولید می‌شود. سپس برای هر هیستوگرام مرتبه دوم، گشتاورهای تابع مشخصه دو بعدی محاسبه می شوند[۷]. ونگ و همکاران نشان دادند که تغییرات در گشتاورهای آماری تابع مشخصه در اثر جاسازی پیام، نسبت به تغییرات گشتاورهای تابع چگالی احتمال بیشتر مشهود است[۸].

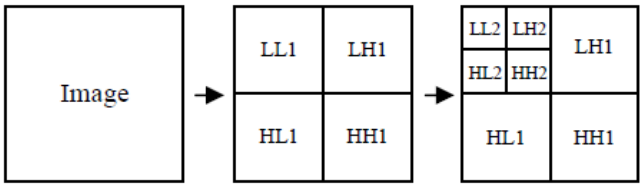
با توجه به اینکه روش‌های پنهان‌شکنی موجود اعمال شده بر روی تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک، نرخ آشکارسازی بالایی را بدست نیاورده‌اند، در این مقاله سعی شده است روشی غیر فعال برای پنهان‌شکنی از تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک با نرخ آشکارسازی بهتر ارائه شود. در روش ارائه شده چهار هیستوگرام مرتبه دوم افقی، عمودی، قطری و قطری آینه‌ای از تصویر تولید می‌شود. بعد از بکاربردن DFT دو بعدی بر روی هر هیستوگرام مرتبه دوم و بدست آوردن تابع مشخصه دو بعدی، دو نوع گشتاور تابع مشخصه حاشیه‌ای برای سه مرتبه اول (مراتب اول، دوم و سوم) در دو جهت فرکانسی محاسبه می‌شوند. بردار ویژگی بدست آمده به SVM داده می‌شود تا در مورد پوشانه یا گنجانه بودن تصاویر تصمیم گیری کند. روش پیشنهادی برای پنهان‌شکنی از دو روش پنهان‌نگاری در حوزه موجک جدید بکار گرفته شد. نتایج آزمایش‌ها نشان می دهد که روش پیشنهادی، نتایج آشکارسازی روش‌های پنهان‌شکنی موجود، که بر روی تصاویر پنهان‌نگاری شده در حوزه موجک آزمایش شده‌اند را بهبود می‌دهد.

در ادامه این مقاله، در بخش دوم چهار چوب نظری مورد استفاده در الگوریتم پیشنهادی پنهان‌شکنی شامل هیستوگرام مرتبه دوم، گشتاورهای تابع مشخصه و ماشین بردار پشتیبان معرفی می‌شوند. در بخش سوم به معرفی روش پیشنهادی پنهان‌شکنی برای پنهان‌شکنی از تصاویر پنهان نگاری شده در حوزه موجک پرداخته می‌شود. در بخش چهارم پایگاه داده مورد استفاده و آزمایش‌های انجام شده به همراه نتایج آنها آورده شده است. بخش پنجم هم به خلاصه و نتیجه گیری و ارائه پیشنهاداتی برای کارهای آینده اختصاص دارد.

## ۲- چهارچوب نظری

### ۲-۱- تبدیل موجک

تبدیل موجک یک روش متداول برای کاربردهای پردازش تصویر است. با بکار بردن تبدیل موجک بر روی یک تصویر با ابعاد $N \times N$، می توان آن را به چهار زیر بخش (زیر باند) تقریب (LL)، جزئیات افقی (LH)، جزئیات عمودی (HL) و جزئیات قطری (HH) با ابعاد $\left\{\frac{N}{2} \times \frac{N}{2}\right\}$ تجزیه کرد[۹]. با به کار بردن دوباره تبدیل موجک بر روی زیرباند تقریب LL1 ، چهار زیر باند تجزیه شده در سطح دوم تجزیه موجک حاصل می‌شود. شکل (۱) نحوه اعمال تبدیل موجک با دو سطح تجزیه را بر روی یک تصویر نشان می‌دهد.




**شکل ۱: تبدیل موجک دو بعدی یک تصویر در دو سطح تجزیه[۱۰]**

### ۲-۲- هیستوگرام مرتبه دوم

هیستوگرام مرتبه دوم یا ماتریس رخداد توام، معیاری از رخداد پیوستگی جفت هایی از پیکسل‌ها است که بوسیله فاصله و جهت مشخص شده از هم جدا شده‌اند. فاصله را با $\rho$ و زاویه نسبت به محور افقی را با $\theta$ نشان می‌دهیم. رابطه هیستوگرام مرتبه دوم به صورت زیر تعریف می‌شود:

$$h_d(j_1, j_2; \rho, \theta) = \frac{N(j_1, j_2; \rho, \theta)}{N_T(\rho, \theta)} \qquad (۱)$$

که $N(j_1, j_2; \rho, \theta)$ تعداد جفت پیکسل ها می‌باشد به گونه‌ای که $j_1$ مقدار پیکسل اول و $j_2$ مقدار پیکسل دوم است. $N_T(\rho, \theta)$ هم تعداد کل جفت پیکسل‌هایی از تصویر با جدایی $(\rho, \theta)$ است. هیستوگرام مرتبه دوم متناظر با یک آرایه دو بعدی، اغلب ماتریس وابستگی یا ماتریس رخداد توأم نامیده می شود[۱۱].

### ۲-۳- گشتاورهای تابع مشخصه

می دانیم اساساً هیستوگرام تصویر، تابع جرم احتمال تصویر (PMF) است. از ضرب هر مؤلفه PMF در یک ضربه واحد شیفت یافته مربوطه، تابع چگالی احتمال (PDF) حاصل می‌شود. در مفهوم تبدیل فوریه گسسته بدیهی است که ضربه های واحد می‌توانند نادیده گرفته شوند. بنابر این PDF می تواند به عنوان نسخه نرمالیزه شده یک هیستوگرام در نظر گرفته شود. طبق [۱۲]، یک تفسیر از تابع مشخصه (CF) این است که CF تبدیل فوریه PDF است.

گشتاورهای تابع مشخصه یک هیستوگرام یک بعدی به صورت زیر تعریف می‌شوند:

$$M_n = \frac{\sum_{j=1}^{\frac{N}{2}} f_j^n |H(f_j)|}{\sum_{j=1}^{\frac{N}{2}} |H(f_j)|} \qquad (۲)$$

که $H(f_j)$ مؤلفه CF در فرکانس $f_j$ ، $N$ تعداد نهایی نقاط در محور افقی هیستوگرام است. توجه کنید که $H(f_0)$ مؤلفه فرکانس صفر از CF، بخاطر اینکه فقط مجموع تمامی مؤلفه های هیستوگرام گسسته را معرفی می‌کند، عمداً از محاسبه گشتاورها خارج شده است. این مقدار برای یک تصویر، تعداد نهایی پیکسلها است که در طی فرایند مخفی‌سازی داده، تغییری نمی‌کند. حذف $H(f_0)$ در رابطه (۲) می‌تواند حساسیت گشتاورها را نسبت به مخفی سازی داده را افزایش دهد که این مطلب در [۱۳] نشان داده شده است.

به ازای $(n = 1)$، گشتاور مرتبه اول حاصل می‌شود که مرکز جرم تابع مشخصه هیستوگرام است. به ازای $(n = 2,3)$ هم گشتاورهای مراتب دوم و سوم بدست می‌آیند و...

گشتاورهای تابع مشخصه یک هیستوگرام مرتبه دوم به صورت زیر تعریف می‌شوند:

$$M_{u,n}=\frac{\sum_{j=1}^{\frac{N}{2}}\sum_{i=1}^{\frac{N}{2}}u_i^n|H(u_i,v_j)|}{\sum_{j=1}^{\frac{N}{2}}\sum_{i=1}^{\frac{N}{2}}|H(u_i,v_j)|} \qquad (۳)$$

$$M_{v,n}=\frac{\sum_{i=1}^{\frac{N}{2}}\sum_{j=1}^{\frac{N}{2}}v_j^n|H(u_i,v_j)|}{\sum_{i=1}^{\frac{N}{2}}\sum_{j=1}^{\frac{N}{2}}|H(u_i,v_j)|} \qquad (۴)$$

که $H(u_i,v_j)$ مؤلفه تابع مشخصه دو بعدی در فرکانس $(u_i,v_j)$ مربوط به DFT است و $N$ تعداد نهایی مقادیر سطوح خاکستری تصویر است. همانطور که از روابط (۳) و (۴) ملاحظه می‌شود دو مجموعه گشتاور حاشیه‌ای مربوط به جهت های فرکانسی $u$ و $v$ می توان بدست آورد. باز هم به ازای $(n = 1,2,3)$ گشتاورهای مراتب اول و دوم و سوم بدست می‌آیند و... [۱۴].

## ۲-۴- ماشین بردار پشتیبان

ماشین بردار پشتیبان (SVM) یک تکنیک شناخته شده است که به طور گسترده برای طبقه بندی و مسائل رگرسیون مورد استفاده قرار می‌گیرد[۱۵]. برای اهداف طبقه بندی، SVM به عنوان یک تکنیک یادگیری بانظارت کار می‌کند که سعی می کند یک ابرصفحه با جدایی حاشیه‌ای حداکثری از دو کلاس را ایجاد کند (همچنین یک مسأله با بیش از دو کلاس می تواند به یک مسأله با دو کلاس کاهش داده شود[۱۶]). این ابرصفحه به عنوان نتیجه‌ای از مسأله بهینه‌سازی زیر بدست می‌آید:

$$\begin{cases} Minimize \quad Z(\omega,\xi)=\frac{1}{2}\|\omega\|^2+\frac{C}{m}\sum_{i=1}^{m}\xi_i \\ Subject\ to\ y_i(\langle\emptyset(x_i),\omega\rangle+b)\geq 1-\xi_i \quad (i=1\dots m) \\ \xi_i\geq 0 \qquad (i=1\dots m) \end{cases} \qquad (۵)$$

که m تعداد الگوهای آموزش، $\langle . \rangle$ ضرب نقطه ای، $\emptyset$ یک تابع انتقال ضمنی، $y_i$ یک برچسب کلاسی$(1^{+}_{-})$، $x_i$ یک نقطه داده، $\xi$ کران بالای خطا و C مقدار جریمه است[۱۷].

SVM برای اینکه بتواند مساله ابعاد خیلی بالا را با استفاده از این روش‌ها حل کند، از قضیه دوگانی لاگرانژ برای تبدیلِ مساله مینیمم‌سازی مورد نظر به فرم دوگانی آن، که در آن به جای تابع پیچیده $\emptyset$ که ما را به فضایی با ابعاد بالا می‌برد تابعِ ساده‌تری به نامِ تابع هسته (کرنل) که در آن ضرب برداری تابع $\emptyset$ ظاهر می‌شود، استفاده می‌کند. از توابع هسته مختلفی از جمله هسته‌های نمایی، چندجمله‌ای و سیگمایی و ... می‌توان استفاده نمود. هسته با انتقال $\emptyset(x_i)$ ، با تساوی $k(x_i,x_j)=\emptyset(x_i)\ .\ \emptyset(x_j)$ در ارتباط است. یکی از هسته های متداول تابع پایه ای شعاعی(گوسین) (RBF) است که رابطه آن به صورت زیر هستند:

$$k(x_i,x_j)=\ e^{-\gamma\|x_i-x_j\|^2} \quad ,for\ \gamma>0 \qquad (۶)$$

که گاهی اوقات بوسیله $\gamma=\frac{1}{2\sigma^2}$ پارامتری می‌شود.

معمولاً یک روش اعتبار سنجی (CV) برای انتخاب بهینه پارامتر کرنل SVM بکار می‌رود و با توجه به اینکه روش‌های اعتبار سنجی هم لزوماً بهترین پارامتر را در اختیار ما قرار نمی‌دهند، همیشه احتمال اینکه بهترین پارامتر را نیابیم وجود دارد[۱۸].

یک روش اعتبارسنجی برای انتخاب پارامتر بهینه کرنل SVM در ادامه شرح داده می‌شود[۱۸]:

۱- لیستی از پارامترها را انتخاب می‌کنیم. برای هر پارامتر انتخاب شده، پنج مورد آزمایش اعتبار سنجی بر روی مجموعه آموزشی انجام می‌دهیم.

۲- پارامتری که منجر به کمترین نرخ خطای اعتبار سنجی می‌شود را انتخاب می‌کنیم.

۳- بهترین پارامتر را برای ایجاد یک مدل به عنوان پیش‌بینی‌کننده، بکار می‌بریم.

## ۳- روش پیشنهادی پنهان‌شکنی

در این بخش الگوریتمی برای پنهان‌شکنی تصاویر پنهان‌نگاری شده در حوزه موجک پیشنهاد می‌شود. در این الگوریتم ابتدا یک پیش‌پردازش بر روی تصاویر مورد آزمایش انجام می‌شود که طی آن تصاویر ورودی به تصاویر سطح خاکستری با ابعاد ۵۱۲×۵۱۲ پیکسل تبدیل می‌شوند. چهار هیستوگرام مرتبه دوم با چهار جدایی ذکر شده در معادله (۷) تولید می‌شود:

$$(\rho,\theta)=\left\{(1,0),\left(1,-\frac{\pi}{2}\right),\left(1,-\frac{\pi}{4}\right),\left(1,+\frac{\pi}{4}\right)\right\} \qquad (۷)$$

که به ترتیب هیستوگرام مرتبه دوم افقی، هیستوگرام مرتبه دوم عمودی و هیستوگرام مرتبه دوم قطری و هیستوگرام مرتبه دوم قطری آینه‌ای نامیده می‌شوند. این جدایی‌ها در شکل (۲) به ترتیب با زوج‌های $(x, a), (x, b), (x, c), (x, d)$ مشخص می‌شود.

| | |
|---|---|
| e | d |
| x | b |
| a | c |

**شکل ۲: همسایگان پیکسل x در جهت های افقی(b)، عمودی (a)، قطری(c) و قطری آینه ای(d)**

در روش پیشنهادی، بعد از بکاربردن DFT دو بعدی بر روی تمامی هیستوگرام‌های مرتبه دوم و بدست آوردن تابع مشخصه دو بعدی آنها، سه مرتبه اول (مراتب اول، دوم و سوم) از دو نوع گشتاور حاشیه‌ای تابع مشخصه در دو جهت فرکانسی از هر هیستوگرام مرتبه دوم استخراج می‌شود که به عنوان ویژگی برای دسته بندی استفاده می‌شوند. رابطه محاسبه تبدیل فوریه دو بعدی به شکل زیر است:

$$H(u,v) = \sum_{x=0}^{N_1-1}\sum_{y=0}^{N_2-1} h(x,y)\, e^{-j2\pi xu/N_1 - j2\pi yv/N_2} \quad (۸)$$

که $h(x,y)$ مقدارهیستوگرام مرتبه دوم، $N_1, N_2$ ابعاد ماتریس هیستوگرام مرتبه دوم و $H(u,v)$ مقدار DFT دوبعدی می‌باشد.

با توجه به اینکه چهار هیستوگرام مرتبه دوم بر روی تصویر محاسبه می‌شوند و از هر کدام از آنها شش گشتاور حاشیه ای تابع مشخصه محاسبه می‌شوند، بردار ویژگی بدست آمده دارای ۲۴ بعد است. بردار ویژگی بدست آمده به ماشین بردار پشتیبان داده می‌شود تا در مورد پوشانه یا گنجانه بودن تصاویر تصمیم‌گیری کند. کرنل مورد استفاده در SVM ، کرنل RBF می‌باشد.

روش اعتبارسنجی که برای انتخاب بهینه پارامتر σ از کرنل تابع پایه ای شعاعی در نظر گرفته شد، در ادامه شرح داده می‌شود:

۱-با توجه به اینکه پارامتر σ باید عدد صحیح مثبتی باشد، اعداد یک تا ۱۰۰ را به عنوان لیست پارامترها انتخاب می‌کنیم. دلیل این انتخاب آن است که با آزمایش‌های فراوان به این نتیجه رسیدیم که مقدار σ بهینه، تقریباً در همه موارد از ۱۰۰ کمتر است و چون می‌خواهیم الگوریتم بهترین عملکرد را در انتخاب پارامتر کرنل داشته باشد و خطای مرحله پیش‌بینی را به حداقل برسانیم، روش اعتبارسنجی را به ازای تمامی ۱۰۰ پارامتر انتخاب شده انجام می‌دهیم تا پارامتر بهینه بدست آید.

۲-مجموعه تصاویر در نظر گرفته شده برای آموزش را به دو قسمت $X_{train}$ و $X_{valid}$ تقسیم می کنیم. تعداد $\frac{3}{5}$ از تصاویر که نیمی از آنها پنهان‌نگاری شده اند ونیمی دیگر پاک هستند را به عنوان $X_{train}$ برای آموزش در نظر می‌گیریم. تعداد $\frac{2}{5}$ دیگر از تصاویر را که نیمی از آنها پنهان‌نگاری شده اند و نیمی دیگر پاک هستند را به عنوان تصاویر معتبر $X_{valid}$ جهت اعتبارسنجی در نظر می‌گیریم.

۳- تصاویر معتبر $X_{valid}$ را توسط SVM ، برای هر پارامتر σ انتخاب شده آزمایش می‌کنیم.

۴- پارامتری که منجر به بیشترین نرخ پیش بینی درست می‌شود را می‌یابیم.

۵-بهترین پارامتر را برای ایجاد یک مدل به عنوان پیش بینی کننده در کرنل RBF و برای مرحله آزمایش بکار می‌بریم.

## ۴- نتایج آزمایشات

### ۴-۱-انتخاب پایگاه داده

محیط پیاده‌سازی برای آزمایش‌های عملی، برنامه مطلب نسخه (R2011b) 7.13.0.564 می باشد. آزمایشات بر روی ۱۳۰۰ تصویر از پایگاه داده تصاویر رنگی غیر فشرده (UCID) انجام گرفت. از آنجا که تصاویر این پایگاه رنگی بوده، همه آنها به تصاویر سطح خاکستری تغییر داده شدند. ۶۵۰ عدد از تصاویر، یک بار توسط روش پنهان‌نگاری در حوزه موجک خسروی[۱۹] و بار دیگر توسط روش پنهان‌نگاری در حوزه موجک معتمدی[۱۰]، پنهان‌نگاری می شوند. ۶۵۰ تصویر باقیمانده به عنوان تصاویر پنهان‌نگاری نشده (پوشانه) در نظر گرفته می‌شوند. در هر دو روش پنهان‌نگاری، تصویر Jet-F16 که در شکل (۳) نشان داده شده است، به عنوان پیام مخفی در نظر گرفته می‌شود.

**شکل ۳: تصویر Jet-F16 به عنوان پیام مخفی**

### ۴-۲- مقایسه نتایج پنهان‌شکنی روش پیشنهادی

در این قسمت، نتایج پنهان‌شکنی بدست آمده از روش پیشنهادی که بر روی روش‌های پنهان‌نگاری خسروی و معتمدی آزمایش شده‌اند، در جدول های (۱) و (۲) آورده شده است. همچنین نتایج روش پیشنهادی، با نتایج روش پنهان‌شکنی شی که بر روی روش پنهان‌نگاری خسروی آزمایش شده است[۱۹] و همچنین با نتایج روش پنهان‌شکنی فرید که بر

**جدول ۱: مقایسه نتایج پنهان شکنی روش پیشنهادی با روش پنهان شکنی شی و روش پنهان شکنی فرید، که بر روی روش پنهان نگاری خسروی با نرخ درج متفاوت پیکسلی پیام مخفی آزمایش شده اند.**

| secret image size | | 256*256 | 128*128 | 64*64 |
|---|---|---|---|---|
| Proposed Method | Detection Rate (%) | 85 | 73.67 | 67.65 |
| | Parameter $\sigma$ | 2 | 2 | 1 |
| | Feature Number | 24 | 24 | 24 |
| Shi Method | Detection Rate (%) [19] | 83.13 | 67.11 | 60.67 |
| | Feature Number | 78 | 78 | 78 |
| Farid Method | Detection Rate (%) [19] | 79.1 | 58.05 | 54.47 |
| | Feature Number | 24 | 24 | 24 |

**جدول ۲: مقایسه نتایج پنهان شکنی روش پیشنهادی با روش پنهان شکنی فرید، که بر روی روش پنهان نگاری معتمدی با نرخ های درج متفاوت α آزمایش شده است.**

| Alpha_ parameter | | 3 | 2 | 1 | 0.61 |
|---|---|---|---|---|---|
| Proposed Method | Detection Rate (%) | 96.67 | 96.67 | 95.67 | 55 |
| | Parameter $\sigma$ | 1 | 1 | 1 | 87 |
| | Feature Number | 24 | 24 | 24 | 24 |
| Farid Method | Detection Rate (%) [10] | %51 for $\alpha$ =1.2 | | | |
| | Feature Number | 24 | | | |

روی هر دو روش پنهان‌نگاری خسروی و معتمدی آزمایش شده است[۱۹ و۱۰]، مورد مقایسه قرار گرفته است.

در جدول های (۱) و (۲) پارامتر $\sigma$ مربوط به کرنل RBF از SVM که نرخ آشکارسازی بالاتری بدست می دهد، آورده شده است. با بررسی نتایج این جدول ها مشخص می شود که نتایج تحقیقات ما منجر به معرفی روشی شده است که نسبت به روشهای پنهان‌شکنی موجود فرید و شی، در پنهان‌شکنی از روشهای پنهان‌نگاری حوزه موجک خسروی و معتمدی بهتر عمل کرده است.

## ۵- نتیجه گیری و پیشنهادات

### ۵-۱- خلاصه و نتیجه‌گیری

با توجه به اینکه روش های پنهان‌شکنی موجود اعمال شده بر روی تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک، نرخ آشکارسازی بالایی را بدست نیاورده‌اند، در این مقاله سعی شد تا روشی غیر فعال، برای پنهان شکنی از تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک با نرخ آشکارسازی بهتر ارائه شود. در این الگوریتم ابتدا یک پیش پردازش بر روی تصاویر مورد آزمایش انجام می‌شود که طی آن تصاویر ورودی به تصاویر سطح خاکستری با ابعاد ۵۱۲×۵۱۲ پیکسل تبدیل می‌شوند. سپس چهار هیستوگرام مرتبه دوم افقی، عمودی، قطری و قطری آینه ای از تصویر تولید می‌شود. بعد از بکاربردن DFT دو بعدی بر روی هر هیستوگرام مرتبه دوم و بدست آوردن تابع مشخصه دو بعدی، دو نوع گشتاور تابع مشخصه حاشیه ای برای سه مرتبه اول (مراتب اول، دوم و سوم) در دو جهت فرکانسی محاسبه می‌شوند. بردار ویژگی بدست آمده دارای ۲۴ بعد است که به ماشین بردار پشتیبان داده می‌شود تا در مورد پوشانه یا گنجانه بودن تصاویر تصمیم گیری کند. کرنل مورد استفاده در SVM ، کرنل RBF می‌باشد. روش پیشنهادی برای پنهان‌شکنی از دو روش پنهان‌نگاری

در حوزه موجک جدید بکار گرفته شد. آزمایشات بر روی ۱۳۰۰ تصویر از مجموعه تصاویر رنگی فشرده نشده ($UCID$) انجام گرفته است. بخشی از تصاویر توسط دو روش پنهان‌نگاری در حوزه موجک خسروی و معتمدی، پنهان‌نگاری شدند. نتایج آزمایش‌ها نشان می دهد که روش پیشنهادی نسبت به روشهای پنهان‌شکنی بر مبنای موجک موجود فرید و شی، در پنهان‌شکنی از روشهای پنهان‌نگاری حوزه موجک خسروی و معتمدی بهتر عمل کرده است و نرخ آشکارسازی را افزایش داده است. با توجه به نتایج بدست آمده می توان نتیجه گرفت که روش پیشنهادی می تواند گزینه مناسبی برای پنهان‌شکنی از روش های پنهان‌نگاری شده در حوزه موجک باشد.

## ۵-۲- پیشنهادات کارهای آینده

جهت اعتبار سنجی نتایج بدست آمده از روش پنهان‌شکنی پیشنهاد شده، اعمال این روش پنهان‌شکنی بر روی تعداد بیشتری از الگوریتم‌های پنهان-نگاری در حوزه موجک، پیشنهاد می‌شود. همچنین می‌توان روش پیشنهادی را بر روی روش‌های پنهان‌نگاری که در سایر حوزه ها انجام شده‌اند آزمایش کرد تا توانایی پنهان‌شکنی عام آن مشخص شود.

## مراجع


[1] R. Din and A. Samsudin, "Digital Steganalysis: Computational. Intelligence Approach," International Journal of Computers, vol. 3,. Issue 1, pp. 161-170, 2009.

[2] L.Wenzhe, X. Bo, Z. Zhe, R. Wenxia, "Active Steganalysis with Only One Stego Image", Sixth International Conference on Fuzzy Systems and Knowledge Discovery, Volume:5, pp: 345 - 348, 2009.

[3] S. Bhattacharyya, I. Banerjee, G. Sanyal, " A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science,Vol.2 , Issue 4, pp.1-16, 2011.

[4] H. farid, "Detecting hidden messages using higher-order statistical models", In: Proceedins of IEEE International Conference on Image processing, New York, USA, Volume .2, pp .905- 908 , 2002 .

[5] S. Lyu, H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines", in Proc.5th Int. Workshop on Info. Hiding, 2002.

[6] Y.Q. Shi, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network", in IEEE Multimedia and Expo (ICME), pp. 269–272, 2005.

[7] C. Chen, Y. Q. Shi, W. Chen, G. Xuan, "Statistical Moments Based Universal Steganalysis using JPEG 2-D Array and 2-D Characteristic Function", IEEE International Conference on Image Processing, pp. 105-108. 2006.

[8] Y. Wang and P. Moulin, "Optimized feature extraction for learning-based image steganalysis ", IEEE Transation Inf Forensic Secur, volume. 2, Issue . 1, pp . 31-45, March . 2007.

[9] S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation", IEEE Pattern Anal. and Machine Intell., vol. 11, no. 7, pp. 674–693, 1989.

[10] H. Motamedi, A. Jafari, "A New Image Steganography Based on Denoising Methods in Wavelet Domain", 9th International Conference on Information Security and Cryptology (ISC), pp. 18-25 ,2012 .

[11] W. K. Pratt, Digital Image Processing, 3rd Edition, John Wiley & Sons, Inc., 2001.

[12] A. Leon-Garcia, Probability and Random Processes for Electrical Engineering, 2nd Edition, Reading, MA: Addison-Wesley Publishing Company, 1994.

[13] Y.Q. Shi, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network", IEEE International Conference on Multimedia and Expo (ICME), pp. 269–272, 2005.

[14] C. Chen, Y. Q. Shi, W. Chen, G. Xuan, "Statistical Moments Based Universal Steganalysis using JPEG 2-D Array and 2-D Characteristic Function", IEEE International Conference on Image Processing, pp. 105-108, 2006.

[15] V. Vapnik, The Nature of Statistical Learning Theory. Information Science and Statistics: Springer, 1999.

[16] C.-W. Hsu and C.-J. Lin, "A comparison of methods for multi-class support vector machines", IEEE Transactions on Neural Networks, vol. 13, no. 2, pp. 415–425, 2002.

[17] J. Reyes-Lopez, S. Campos, H. Allende, R. Salas, "Zernike's Feature Descriptors for Iris Recognition with SVM", 30th International Conference of the Chilean Computer Science Society (SCCC), pp: 283 – 288, 2011.

[18] Y. W. Chen, C. J. Lin, "Combining SVMs with various feature selection strategies", in the book "Feature extraction, foundations and applications", springer, 2006.

[19] M. J. Khosravi, S. Ghandali, " A Secure Joint Wavelet Based Steganography and Secret Sharing Method", 7th International Conference on Information Assurance and Security (IAS), pp. 222-227, 2011.