یک روش پنهان‌شکنی مبتنی بر الگوریتم F-Score + SVM برای تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک

حیدر باجلان[1]، محمد پویان[2]

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

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

چکیده

در این مقاله، یک روش پنهان‌شکنی برای تصاویر پنهان‌نگاری شده در حوزه موجک پیشنهاد می‌شود. در روش پیشنهاد شده، تصویر مورد آزمایش توسط تبدیل موجک گسسته هار سه سطحی به ۱۳ زیرباند تجزیه می‌شود (تصویر اصلی به عنوان زیرباند LL0 درنظر گرفته می شود). سپس هیستوگرام‌های مرتبه دوم افقی، عمودی، قطری و قطری آینه‌ای از هر زیرباند ساخته می‌شوند. سه مرتبه اول (مراتب اول، دوم و سوم) از دو نوع گشتاور تابع مشخصه حاشیه‌ای در دو جهت فرکانسی برای هر ماتریس هیستوگرام مرتبه دوم محاسبه می‌شوند. بردار ویژگی بدست آمده برای هر زیرباند دارای ۲۴ بعد می‌باشد. بردار ویژگی کل بدست آمده دارای ۳۱۲ بعد است. بدلیل زیاد بودن ابعاد بردار ویژگی، بوسیله الگوریتم انتخاب ویژگی F-Score + SVM تغییر یافته (که ترکیبی از تکنیک رتبه-بندی فیشر و ماشین بردار پشتیبان می‌باشد)، تعداد ویژگی ها کاهش می‌یابد و ویژگی‌های باقیمانده برای تشخیص تصاویر پنهان-نگاری شده از تصاویر پاک، به ماشین بردار پشتیبان داده می‌شوند. نتایج آزمایش‌ها نشان می دهد که الگوریتم پیشنهادی، نتایج آشکارسازی تکنیک‌های پنهان‌شکنی موجود، که بر روی تصاویر پنهان‌نگاری شده در حوزه موجک آزمایش شده‌اند را بهبود می‌دهد.

کلمات کلیدی

پنهان‌شکنی، پنهان‌نگاری، گشتاورهای تابع مشخصه، تبدیل موجک، الگوریتم F-Score + SVM.

۱- مقدمه

در پنهان‌نگاری[1] دیجیتال، محیط دیجیتالی برای رمزگذاری و پنهان کردن دنباله ای از بیت‌های پیام، به گونه ای اصلاح می‌شود که ارتباط مخفی مورد شک قرار نگیرد. در پنهان‌شکنی[2] دیجیتال، سعی می‌شود این نوع ارتباط پوشیده تشخیص داده شود [4]. روش‌های پنهان‌شکنی می‌توانند به روش-های فعال و روش‌های غیر فعال تقسیم شوند. پنهان شکنی غیر فعال به تشخیص وجود یا عدم وجود پیام مخفی در تصویر می‌پردازد. پنهان‌شکنی فعال اقدام به تخمین طول پیام، بیت‌های پیام، کلید رمز و ... می‌کند [12]. از دیدگاهی دیگر الگوریتم‌های پنهان‌نگاری به دو گروه تقسیم می‌شوند. دسته ای از آنها تکنیک‌های حوزه مکان نام دارند که به طور مستقیم به سیگنال اعمال می‌شوند. دسته ای دیگر تکنیک‌های حوزه تبدیل نام دارند که بر روی تبدیل یافته سیگنال اعمال می‌شوند. تکنیک‌های حوزه تبدیل مختلف، تبدیل فوریه گسسته(DFT)، تبدیل کسینوسی گسسته(DCT) و تبدیل موجک گسسته (DWT) می باشند [1].

در روش‌های پنهان‌نگاری در حوزه تبدیل موجک، پنهان سازی در ضرایب موجک تصویر انجام می شود. با ذخیره سازی اطلاعات در ضرایب موجک، تغییر در شدت روشنایی تصویر غیر قابل مشاهده خواهد بود. در روش پنهان نگاری ارائه شده توسط یانگ و دنگ ابتدا تبدیل آرنولد بر روی تصویر

رمز انجام می شود. سپس تبدیل موجک بر روی تصویر پوشانه و تصویر رمز تبدیل یافته اعمال می شود. ضرایب تبدیل موجک تصویر رمز کوانتیزه شده و داخل رشته های بیتی کد می شوند. سپس هر جزء از ضرایب تبدیل موجک (ضرایب تقریب، جزئیات افقی، جزئیات عمودی و جزئیات قطری) از تصویر رمز بوسیله الگوریتم بیت با کمترین ارزش، داخل ضرایب متناظر تبدیل موجک تصویر پوشانه اضافه می شوند[13].

خسروی و همکاران یک تکنیک پنهان نگاری جدید بر پایه ترکیب یک روش اشتراک رمز و تبدیل موجک را ارائه کردند. در این روش یک تصویر رمز به چند اشتراک (سهم) تقسیم می شود. سپس اشتراک ها وجمع کنترلی فلتچر-۱۶ از اشتراک ها با استفاده از یک تکنیک پنهان نگاری برمبنای موجک صحیح داخل تصاویر پوشانه مخفی می شوند. در بخش کدگشایی تصاویر پنهان نگاری شده، برای بازیابی سهم ها و در نتیجه بازیابی تصویر رمز بکار می روند. این روش پنهان نگاری در برابر حملات جدی نظیر RS و روش های پنهان شکنی آموزشی تحت نظارت، پایدار است.[7] .

یک روش پنهان نگاری بر مبنای موجک جدید، با استفاده از الگوریتم-های حذف نویز بوسیله آستانه گذاری ضرایب موجک توسط معتمدی و جعفری ارائه شد. در حقیقت داده رمز در اجزاء نویزی از محیط پوشانه مخفی می شود. این روش یک آستانه را بر اساس ضرایب موجک تصویر پوشانه، جهت تعیین اجزاء نویزی، محاسبه می کند. این روش ظرفیت داده پنهان شده را افزایش داده و کیفیت دیداری خوبی برای تصویر گنجانه دارد. در ضمن داده اضافه شده می تواند بدون مراجعه به تصویر اصلی از تصویر گنجانه، استخراج شود. این روش مقاومت بالایی در مقابل حملات پنهان شکنی دارد[9].

برای الگوریتم‌های پنهان‌نگاری در هر حوزه، تکنیک‌های پنهان‌شکنی خاصی ارائه شده است. فرید، یک روش پنهان‌شکنی پیشنهاد کرد که در آن تصویر را در حوزه موجک تجزیه نمود. وی در این روش آماره‌های مرتبه بالاتر (میانگین، واریانس، خمیدگی و درجه اوج نمودار آماری) از تابع چگالی احتمال هر زیر باند موجک را استخراج کرد. همچنین این ویژگی‌ها از زیرباندهای موجک تصویر خطای پیشگویی شده استخراج می شوند. سپس یک طبقه بندی کننده خطی فیشر برای تمایز بین تصاویر پنهان‌نگاری شده و تصاویر پاک استفاده شد [5]. لیو و فرید ماشین بردار پشتیبان (SVM) را به عنوان دسته‌بندی‌کننده در روش فرید به کار بردند [6]. شی، یک روش پنهان‌شکنی را ارائه کرد که در آن ویژگی‌های انتخاب شده شامل گشتاورهای آماری توابع مشخصه تصویر اصلی، تصویر خطای پیشگویی شده و زیرباندهای تبدیل موجک آنها می‌باشد. دسته بندی کننده انتخاب شده، شبکه عصبی مصنوعی است [11].

چن و همکاران با استفاده از هیستوگرام مراتب بالا، یک الگوریتم پنهان‌شکنی فراگیر ارائه کردند. در این الگوریتم بر روی مقادیر قدرمطلق ضرایب تبدیل کسینوسی گسسته بلوکی آرایه دو بعدی JPEG تصویر ورودی، تبدیل موجک هار سه سطحی اعمال می شود. سپس برای هر زیرباند، هیستوگرام‌های مرتبه دوم افقی، عمودی و قطری ساخته می‌شوند. سرانجام برای هر هیستوگرام مرتبه دوم، گشتاورهای تابع مشخصه دو بعدی محاسبه می‌شوند. سپس ماشین بردار پشتیبان با کرنل چند جمله ای درجه دوم به عنوان دسته‌بندی‌کننده استفاده می شود [2]. هان زنگ و همکاران، با استفاده از ماتریس هیستوگرام مرتبه دوم قطری آینه‌ای از هر زیر باند موجک تصویر، یک روش پنهان شکنی فراگیر را ارائه کردند. در این روش تبدیل لاپلاس بر روی ماتریس‌های هیستوگرام مرتبه دوم اعمال می‌شود. سپس واریانس‌های تبدیل‌های لاپلاس و گشتاورهای تابع مشخصه هیستوگرام‌های مرتبه دوم بعنوان ویژگی‌های آماری استخراج می‌شوند. سپس شبکه عصبی پس انتشار خطا برای دسته‌بندی و آشکارسازی انتخاب می‌شود [14]. این الگوریتم‌ها تعداد کمی از هیستوگرام‌های مرتبه دوم ضرایب زیرباندهای موجک مجاور را استفاده می‌کنند.

پنهان شکنی برمبنای گشتاورهای آماری توابع مشخصه موجک، توانایی تعمیم ضعیفی در برخی حوزه ها دارد. در روش پنهان‌شکنی کور ژانگ و ژنگ برای بهبود این ضعف، روش انتخاب ویژگی F-Score + SVM برای فیلتر کردن ویژگی های زائد و غیر ضروری محاسبه شده از گشتاورهای آماری توابع مشخصه موجک بکار گرفته شد. روش انتخاب ویژگی F-Score + SVM ترکیبی از تکنیک F-Score و ماشین بردار پشتیبان می‌باشد. تکنیک F-Score، یک تکنیک ساده اما مؤثر برای اندازه‌گیری جدایی دو مجموعه از اعداد است [15].

روش‌های پنهان‌شکنی موجود اعمال شده بر روی تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک، نرخ آشکارسازی بالایی را بدست نیاورده‌اند. یکی از دلایل این امر، آن است که اکثر روش‌های پنهان‌نگاری در حوزه موجک، پیام را در ضرایب زیرباندهای جزئیات تبدیل موجک مخفی می‌کنند که تغییر در ضرایب این زیر باندها تأثیر ناچیزی روی تصویر دارند.

در این مقاله یک روش پنهان‌شکنی غیر فعال برای تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک با نرخ آشکارسازی بالاتر پیشنهاد می‌شود. در روش پیشنهاد شده، تصویر مورد آزمایش توسط تبدیل موجک گسسته هار سه سطحی به ۱۳ زیرباند تجزیه می‌شود (تصویر اصلی به عنوان زیرباند LL0 درنظر گرفته می‌شود). سپس هیستوگرام‌های مرتبه دوم افقی، عمودی، قطری و قطری آینه‌ای از هر زیرباند ساخته می‌شوند. سه مرتبه اول (مراتب اول، دوم و سوم) از دو نوع گشتاور تابع مشخصه حاشیه‌ای در دو جهت فرکانسی برای هر ماتریس هیستوگرام مرتبه دوم محاسبه می‌شوند. در این روش، بدلیل زیاد بودن ابعاد بردار ویژگی، بوسیله الگوریتم انتخاب ویژگی F-Score + SVM تغییر یافته (که دارای روش اعتبارسنجی متفاوتی با الگوریتم F-Score + SVM بکار رفته در روش ژانگ و ژنگ است) تعداد ویژگی ها کاهش می‌یابد و ویژگی های باقیمانده برای تشخیص تصویر پنهان‌نگاری شده از تصویر پاک، به ماشین بردار پشتیبان داده می‌شوند.

این الگوریتم، نسبت به الگوریتم‌های پنهان‌شکنی موجود، تعداد هیستوگرام‌های مرتبه دوم بیشتری از ضرایب زیرباندهای موجک مجاور را استفاده می‌کند. از سویی دیگر، الگوریتم انتخاب ویژگی F-Score + SVM باعث می‌شود ویژگی‌های با تأثیر بیشتر انتخاب شوند. در نتیجه انتظار می‌رود نرخ آشکارسازی افزایش یابد. نتایج آزمایش‌ها نشان می‌دهد که الگوریتم پیشنهادی، نتایج آشکارسازی تکنیک‌های پنهان شکنی موجود اعمال شده بر روی تصاویر پنهان‌نگاری شده در حوزه موجک را بهبود می‌دهد.

ادامه این مقاله به صورت زیر سازماندهی می‌شود. در بخش دوم روش پیشنهادی معرفی می‌شود. این بخش شامل مفاهیم نظری مورد استفاده در الگوریتم پنهان‌شکنی پیشنهاد شده، طرح مسأله، الگوریتم پنهان‌شکنی پیشنهادی برای پنهان‌شکنی از تصاویر پنهان‌نگاری شده در حوزه موجک و نتایج آزمایش‌ها است. در بخش سوم هم نتیجه‌گیری ارائه می‌شود.

۲- روش پیشنهادی

۲-۱- مفاهیم نظری

در این بخش دوم مفاهیم نظری مورد استفاده در الگوریتم پنهان‌شکنی پیشنهاد شده معرفی می‌شوند.

۲-۱-۱- هیستوگرام مرتبه دوم

ماتریس هیستوگرام مرتبه دوم، معیاری از رخداد پیوستگی جفت‌هایی از پیکسل‌ها است که بوسیله فاصله و جهت مشخص شده از هم جدا شده‌اند. رابطه (۱) تعریف هیستوگرام مرتبه دوم را نشان می‌دهد.

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

که ρ و θ به ترتیب فاصله و زاویه نسبت به محور افقی هستند، عبارت صورت کسر یعنی $N(j_1, j_2; \rho, \theta)$ تعداد جفت پیکسل‌ها می‌باشد به گونه‌ای که j_1 مقدار پیکسل اول و j_2 مقدار پیکسل دوم است و $N_T(\rho, \theta)$ تعداد کل جفت پیکسل‌ها با جدایی (ρ, θ) است [10].

۲-۱-۲- گشتاورهای تابع مشخصه

اساساً هیستوگرام یک تصویر، تابع جرم احتمال تصویر است. از ضرب هر مؤلفه تابع جرم احتمال تصویر و یک ضربه واحد شیفت یافته مربوطه، تابع چگالی احتمال حاصل می‌شود. در مفهوم تبدیل فوریه گسسته بدیهی است که ضربه‌های واحد می‌توانند نادیده گرفته شوند. بنابراین تابع چگالی احتمال می‌تواند به عنوان نسخه نرمالیزه شده یک هیستوگرام در نظر گرفته شود. یک تفسیر از تابع مشخصه این است که تابع مشخصه تبدیل فوریه تابع چگالی احتمال است [8].

رابطه (۲) تعریف گشتاورهای تابع مشخصه یک هیستوگرام مرتبه اول را نشان می‌دهد:

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

که $H(f_j)$ مؤلفه تابع مشخصه در فرکانس f_j، N تعداد نهایی نقاط در محور افقی هیستوگرام است و n مرتبه گشتاور را نشان می دهد. روابط (۳) و (۴) گشتاورهای تابع مشخصه یک هیستوگرام مرتبه دوم را نشان می دهند.

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

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

که $H(u_i, v_j)$ مؤلفه تابع مشخصه دو بعدی در فرکانس (u_i, v_j) مربوط به تبدیل فوریه گسسته 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 جهت‌های فرکانسی u و v را می‌توان بدست آورد [2].

۲-۱-۳- الگوریتم انتخاب ویژگی F-Score + SVM

در الگوریتم F-Score + SVM، از تکنیک F-Score بعنوان یک فیلتر برای انتخاب ویژگی و از ماشین بردار پشتیبان به عنوان دسته بندی‌کننده استفاده شده است. [3].

F-Score ، یک تکنیک ساده است که جدایی (تفاوت) دو مجموعه از اعداد حقیقی را اندازه می‌گیرد. با توجه به بردار آموزشی u_k به ازای $k=1,\ldots,m$ ، اگر n_+ و n_- به ترتیب تعداد نمونه‌های مثبت و منفی باشند، مقدار F-Score مربوط به ویژگی شماره i ، طبق رابطه (۵) تعریف می‌شود.

$$F(i) \equiv \frac{(\bar{u}_i^{(+)} - \bar{u}_i)^2 + (\bar{u}_i^{(-)} - \bar{u}_i)^2}{\frac{1}{n_+ - 1}\sum_{k=1}^{n_+}(u_{k,i}^{(+)} - \bar{u}_i^{(+)})^2 + \frac{1}{n_- - 1}\sum_{k=1}^{n_-}(u_{k,i}^{(-)} - \bar{u}_i^{(-)})^2} \qquad (۵)$$

که میانگین ویژگی شماره i از تمام مجموعه داده، مجموعه داده مثبت و مجموعه داده منفی به ترتیب با $\bar{u}_i$ ، $\bar{u}_i^{(+)}$ و $\bar{u}_i^{(-)}$ نمایش داده شده است. همچنین $\bar{u}_{k,i}^{(+)}$، ویژگی شماره i از نمونه مثبت شماره k است و $\bar{u}_{k,i}^{(-)}$ ، ویژگی شماره i از نمونه منفی شماره k می‌باشد. صورت کسر، تمایز بین مجموعه‌های مثبت ومنفی را مشخص می‌کند و مخرج کسر، تمایز درونی هر مجموعه را معین می‌کند. هر ویژگی که مقدار F-Score بزرگتری داشته باشد توانایی تمایز بالاتری دارد. بنابراین، F-Score را به عنوان یک معیار انتخاب ویژگی بکار می‌بریم [3].

الگوریتم F-Score + SVM ، روشی ساده و کاملاً موثر برای انتخاب ویژگی است. ویژگی های با مقدار F-Score بالا انتخاب می‌شوند و سپس ماشین بردار پشتیبان برای آموزش و پیش بینی بکار می‌رود [3]. این فرایند در ادامه توضیح داده می‌شود.

۲-۲- طرح مسأله

روش‌های پنهان‌شکنی موجود اعمال شده بر روی تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک، نرخ آشکارسازی بالایی را بدست نیاورده‌اند. یکی از دلایل این امر، آن است که اکثر روش‌های پنهان‌نگاری در حوزه موجک، پیام را در ضرایب زیرباندهای جزئیات تبدیل موجک مخفی می‌کنند که تغییر در ضرایب این زیر باندها تأثیر ناچیزی روی تصویر دارند. برای تشخیص پنهان-نگاری در این ضرایب می‌توان با استفاده از ابزارهای موجود نظیر ماتریس هیستوگرام مرتبه دوم ضرایب زیرباندهای موجک مجاور و با در نظر گرفتن تعداد هیستوگرام‌های مرتبه دوم بیشتر، پیوستگی ضرایب مجاور را زیر نظر گرفت و به تشخیص تصاویر پنهان نگاری شده از تصاویر پاک پرداخت.

۲-۳- الگوریتم پنهان‌شکنی پیشنهادی

در این بخش یک الگوریتم پنهان‌شکنی برای 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.

۲-۳-۱- استخراج ویژگی

تبدیل موجک هار سه سطحی بر روی تصویر اعمال می‌شود. تصویر اصلی نیز به عنوان زیرباند LL0 در نظر گرفته می‌شود. از هر زیرباند، چهار هیستوگرام مرتبه دوم با چهار جدایی ذکر شده در معادله (۶) ساخته می‌شود.

$$(\rho,\theta)=\left\{(1,0),(1,-\frac{\pi}{2}),(1,-\frac{\pi}{4}),(1,+\frac{\pi}{4})\right\} \qquad (۶)$$

که به ترتیب هیستوگرام مرتبه دوم افقی، عمودی، قطری و قطری آینه‌ای نامیده می‌شوند. این جدایی‌ها در شکل (۱) به ترتیب با زوج های $(x,b),(x,a),(x,c),(x,d)$ مشخص می‌شوند.

در روش پیشنهادی، بعد از بکاربردن DFT دو بعدی بر روی تمامی هیستوگرام‌های مرتبه دوم هر زیرباند 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 می‌شوند. با توجه به اینکه چهار هیستوگرام مرتبه دوم برای هر زیرباند محاسبه می‌شوند و از هر هیستوگرام مرتبه دوم شش گشتاور حاشیه‌ای تابع مشخصه محاسبه می‌شوند، بردار ویژگی بدست آمده برای هر زیرباند دارای ۲۴ بعد است. در نتیجه یک بردار ویژگی ۳۱۲ بعدی حاصل می‌شود که می‌تواند برای دسته‌بندی به یک دسته‌بندی‌کننده داده شود.

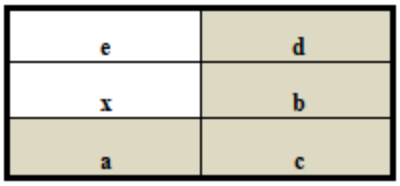
۲-۳-۲- انتخاب ویژگی

همانگونه که مشاهده می‌شود ابعاد ویژگی زیاد است و قطعاً تعداد زیادی از این ویژگی‌ها برای پنهان‌شکنی مطلوب نیستند. چنانچه همه ویژگی‌ها را به دسته‌بندی‌کننده ماشین بردار پشتیبان اعمال کنیم باعث کاهش عملکرد این دسته‌بندی‌کننده خواهد شد [15]. بنابر این برای اینکه تعداد ابعاد بردار ویژگی را کاهش دهیم از الگوریتم انتخاب ویژگی F-Score + SVM [3] تغییریافته، استفاده می‌کنیم. در نهایت ویژگی‌های انتخاب شده برای تشخیص تصاویر پنهان‌نگاری شده از تصاویر پاک، به یک دسته بندی کننده ماشین بردار پشتیبان داده می شوند. هنگام استفاده از ماشین بردار پشتیبان، کرنل تابع پایه شعاعی بکار رفته است. رابطه (۷)، تعریف کرنل تابع پایه‌ای شعاعی را نشان می‌دهد.

$$k(x_i,x_j)=e^{-\gamma\|x_i-x_j\|^2} \qquad (۷)$$

که $\gamma=1/2\sigma^2$ و σ پارامتر کرنل می‌باشد که عددی طبیعی و مثبت است.

فرآیند اجرای الگوریتم F-Score + SVM در روش پیشنهادی، به صورت زیر خلاصه می‌شود:



شکل (۱) : همسایگان پیکسل x در جهت‌های افقی(b)، عمودی (a)، قطری(c) و قطری آینه‌ای(d)

- محاسبه F-Score: F-Score هر ویژگی را طبق معادله (۵) محاسبه کنید.
- تعیین آستانه: به صورت زیر، تعدادی آستانه برای قطع‌کردن مقادیر F-Score بالا و پایین تعیین کنید:

الف- مرتب‌سازی: ابتدا مجموعه مقادیر F-Score را به صورت نزولی مرتب کنید.

ب- مقیاس‌بندی: مقادیر F-Score مرتب شده را با توجه به تعداد مجموعه F-Score ، مقیاس‌بندی کنید. شکل (۲)، نمودار نمونه مقادیر F-Score ویژگی‌های بدست آمده از روش پیشنهادی که به ترتیب نزولی مرتب و مقیاس‌بندی شده است را نشان می‌دهد.

ج- محاسبه گرادیان: گرادیان مقادیر F-Score مقیاس-بندی شده را نسبت به تعداد مجموعه F-Score مرتب شده محاسبه کنید. رابطه (۸) معادله گرادیان را نشان می‌دهد.

$$\nabla(F-Score)=\frac{\partial(F-Score)}{\partial(x)} \qquad (۸)$$

که $\nabla(F\text{-}Score)$ مقدار گرادیان عددی یک بعدی بردار مقادیر F-Score مقیاس بندی شده را در جهت محور x نشان می دهد. محور x ، تعداد مجموعه F-Score مرتب شده است.

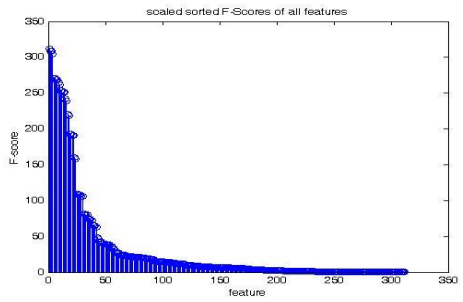
د- جداسازی: هر مقدار F-Score را که گرادیان آن بزرگتر از منفی یک است، به ترتیب جدا کنید.

ه- تعیین آستانه: به ازای تعداد مقادیر F-Score که گرادیان آنها بزرگتر از منفی یک است، آستانه تعیین کنید. به منظور اینکه تعداد آستانه‌ها خیلی زیاد نشود، کران بالایی برابر با یک ششم از تعداد مقادیر F-Score را برای تعداد آستانه‌ها انتخاب کنید.

- بکارگیری ماشین بردار پشتیبان برای هر آستانه: برای هر آستانه، مراحل زیر اجرا می‌شوند:

الف- تعدادی از ویژگی‌ها را دور بریزید: ویژگی‌های با مقدار F-Score زیر این آستانه را دور بریزید.

ب- داده‌های آموزشی را تقسیم کنید: داده‌های آموزشی را به U_{train} و U_{valid} با نسبت سه به دو تقسیم کنید.



شکل (۲): نمودار نمونه مقادیر F-Score ویژگی‌های بدست آمده از روش پیشنهادی که به ترتیب نزولی مرتب شده و مقیاس‌بندی شده است.

ج- بکارگیری ماشین بردار پشتیبان برای هر آستانه: U_{train} را به عنوان یک مجموعه آموزشی جدید در نظر بگیرید. با توجه به اینکه پارامترکرنل σ باید عدد صحیح مثبتی باشد، اعداد یک تا ۱۰۰ را به عنوان لیست پارامترها انتخاب کنید. به ازای هر پارامتر σ، ماشین بردار پشتیبان را برای بدست-آوردن یک پیش بینی کننده بکار ببرید؛ هر پیش بینی‌کننده را برای پیش بینی U_{valid} استفاده کنید. پارامتری که منجر به بالاترین نرخ پیش بینی درست می‌شود را یادداشت کنید.

- انتخاب آستانه: آستانه با کمترین خطای پیش بینی را انتخاب کنید.
- دسته بندی: ویژگی‌های با مقدار F-Score زیر آستانه انتخاب شده را دور بریزید. سپس پارامتر کرنل σ بدست آمده متناظر با آستانه با کمترین خطا را به عنوان پارامتر پیش‌بینی‌کننده SVM برای پیش‌بینی داده‌های آزمایش، بکار ببرید.

۲-٤- نتایج آزمایش‌ها

محیط آزمایش‌ها، مطلب نسخه 7.13.0.564 است. آزمایش‌ها بر روی ۱۳۰۰ تصویر از پایگاه داده تصاویر رنگی غیر فشرده (UCID) انجام می‌گیرد. تصویر Jet-F16 که در شکل (۳) نشان داده شده است، به عنوان پیام مخفی در نظر گرفته می‌شود. ۶۵۰ عدد از تصاویر، یک بار توسط روش پنهان‌نگاری خسروی [7] و بار دیگر توسط روش پنهان‌نگاری معتمدی [9]، مخفی می-شوند. هر دو روش پنهان‌نگاری در حوزه تبدیل موجک هستند. ۶۵۰ عدد تصویر باقیمانده به عنوان تصاویر پوشانه در نظر گرفته می‌شوند.

نتایج پنهان‌شکنی از دو روش های پنهان‌نگاری مورد آزمایش در جدول‌های (۱) و (۲) جدول‌بندی می‌شوند. در این جدول‌ها، نتایج روش پنهان‌شکنی پیشنهاد شده، با نتایج روش پنهان‌شکنی شی که بر روی روش پنهان‌نگاری خسروی آزمایش شده است [7] و همچنین با نتایج روش پنهان-شکنی فرید که بر روی هر دو روش پنهان‌نگاری آزمایش شده است [9,7]، مورد مقایسه قرار می‌گیرند. همچنین برای مشاهده لزوم کاهش ابعاد بردار ویژگی در الگوریتم پیشنهادی، نتایج روش پیشنهادی با نتایج حالت روش پیشنهادی بدون کاهش ابعاد بردار ویژگی مقایسه می شود. در جدول‌های (۱) و (۲) پارامترσ ، پارامتری از کرنل تابع پایه‌ای شعاعی از ماشین بردار پشتیبان است که نرخ آشکارسازی بالاتری بدست می‌آورد. در جدول (۲) پارامتر تنظیم کننده مقدار آستانه (α) طبق رابطه (۹) برای محاسبه مقدار آستانه ضرایب موجک (T) جهت تعیین اجزاء نویزی استفاده می شود که به طور مستقیم بر ظرفیت پنهان نگاری تأثیر می گذارد[9].

$$T = \min(\min(2(\frac{median(|c|)}{0.6745})^2 t(\alpha + \log(n_c / t)) - cumsum(|c_d(t)|^2), \max(|c_{fs}|)) \quad (۹)$$

که c ضرایب جزئی تبدیل موجک، n_c تعداد همه ضرایب موجک، c_{fs} مقدار همه ضرایب موجک، c_d مقدار ضرایب موجک صعودی، $t = 1 : \ldots : n_{cd}$ و n_{cd} تعداد ضرایب موجک در c_d می باشند. در رابطه (۹)، $cumsum$ مجموع تجمعی در امتداد ابعاد مختلف یک آرایه را محاسبه می کند[9].

با بررسی این جدول‌ها مشخص می‌شود که تحقیقات ما منجر به معرفی روشی شده است که در پنهان‌شکنی از روش پنهان‌نگاری حوزه موجک خسروی و روش پنهان‌نگاری حوزه موجک معتمدی نسبت به روش پنهان-شکنی فرید و روش پنهان‌شکنی شی بهتر عمل می‌کند. همچنین کاهش ابعاد بردار ویژگی در الگوریتم پیشنهادی منجر به نتایج بهتر می شود که دلیل آن این است که انتخاب ویژگی‌های با توانایی تمایز بیشتر، به عملکرد بهینه SVM کمک می کند.

۳- نتیجه

در این مقاله روشی غیر فعال، برای پنهان‌شکنی از تصاویر پنهان‌نگاری شده در حوزه تبدیل موجک با نرخ آشکارسازی بالاتر ارائه شد. در این الگوریتم ویژگی‌های استفاده شده شامل گشتاورهای تابع مشخصه هیستوگرام‌های مرتبه دوم افقی، عمودی، قطری و قطری آینه‌ای حاصل از تصویر و زیرباندهای تجزیه موجک سه سطحی تصویر است. در این روش بوسیله الگوریتم انتخاب ویژگی F-Score + SVM تغییر یافته، تعداد ویژگی‌ها کاهش یافته و ویژگی‌های باقیمانده برای دسته بندی به ماشین بردارپشتیبان داده شدند تا تصاویر گنجانه را از تصاویر پوشانه تشخیص دهد.

در الگوریتم F-Score + SVM تغییریافته، هنگام تقسیم داده‌های آموزشی، تعداد داده‌های U_{train} زیاد است و انتخاب تعداد داده های U_{train} و U_{valid}، به صورت تصادفی انجام نمی‌شود. در نتیجه ماشین بردار پشتیبان می‌تواند به درستی آموزش ببیند، لذا دقت عملیات بی‌جهت کاهش نمی‌یابد و این می‌تواند برتری روش F-Score + SVM تغییریافته نسبت به روش اصلی باشد.

روش پیشنهاد شده برای پنهان‌شکنی از دو روش پنهان‌نگاری در حوزه موجک جدید بکار گرفته شد. این الگوریتم، نسبت به الگوریتم‌های پنهان-شکنی موجود، تعداد هیستوگرام‌های مرتبه دوم بیشتری از ضرایب زیرباندهای موجک مجاور را استفاده می‌کند. همچنین الگوریتم انتخاب ویژگی F-Score + SVM باعث می‌شود ویژگی‌های با توانایی تمایز بیشتر انتخاب شوند. در نتیجه انتظار می‌رود نرخ آشکارسازی افزایش یابد. نتایج آزمایش‌ها نشان می-دهند که روش پیشنهادی نسبت به روش پنهان‌شکنی بر مبنای موجک فرید و روش پنهان‌شکنی بر مبنای موجک شی، در پنهان‌شکنی از روش پنهان-نگاری حوزه موجک خسروی و روش پنهان‌نگاری حوزه موجک معتمدی بهتر عمل می‌کند و نرخ آشکارسازی را افزایش می‌دهد. در نتیجه روش پیشنهادی می‌تواند گزینه مناسبی برای پنهان‌شکنی از تصاویر پنهان‌نگاری شده در حوزه موجک باشد.

شکل (۳) : تصویر Jet-F16 به عنوان پیام مخفی

جدول (۱) : نتایج پنهان‌شکنی روش‌های پیشنهاد شده، شی و فرید که بر روی روش پنهان‌نگاری خسروی آزمایش شده‌اند.

اندازه تصویر پیام		۲۵۶×۲۵۶	۱۲۸×۱۲۸	۶۴×۶۴
روش پیشنهادی	نرخ آشکارسازی (٪)	۹۲,۳۳	۷۸,۳۳	۷۷,۳۳
	σ - پارامتر کرنل SVM	۵	۳	۵
	تعداد ویژگی ها	۱۶۷	۴۰	۹۰
روش پیشنهادی بدون کاهش ابعاد ویژگی	نرخ آشکارسازی (٪)	۹۲	۷۵,۶۷	۷۰,۶۷
	σ - پارامتر کرنل SVM	۱۱	۲۳	۱۸
	تعداد ویژگی ها	۳۱۲	۳۱۲	۳۱۲
روش شی	نرخ آشکارسازی (٪) [7]	۸۳,۱۳	۶۷,۱۱	۶۰,۶۷
	تعداد ویژگی ها	۷۸	۷۸	۷۸
روش فرید	نرخ آشکارسازی (٪) [7]	۷۹,۱	۵۸,۰۵	۵۴,۴۷
	تعداد ویژگی ها	۲۴	۲۴	۲۴

جدول (۲) : نتایج پنهان‌شکنی روش پیشنهاد شده و روش فرید، که بر روی روش پنهان‌نگاری معتمدی آزمایش شده‌اند.

پارامتر تنظیم کننده مقدار آستانه(α)		۳	۲	۱	۰.۶۱
روش پیشنهادی	نرخ آشکارسازی (٪)	۹۸,۶۷	۹۷,۶۷	۹۶,۶۷	۷۷,۶۷
	σ - پارامتر کرنل SVM	۲	۹	۲	۴
	تعداد ویژگی ها	۹۰	۱۴۹	۷۸	۱۰۷
روش پیشنهادی بدون کاهش ابعاد ویژگی	نرخ آشکارسازی (٪)	۹۸,۶۷	۹۷	۹۶	۷۰,۳۳
	σ - پارامتر کرنل SVM	۳۲	۳۲	۲۶	۱۵
	تعداد ویژگی ها	۳۱۲	۳۱۲	۳۱۲	۳۱۲
روش فرید	نرخ آشکارسازی (٪) [9]	۵۱ برای α=۱,۲			
	تعداد ویژگی ها	۲۴			

مراجع

[1] Bhattacharyya, S., Banerjee, I., Sanyal, G., "*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, April 2011.

[2] Chen, C., Shi, Y. Q., Chen, W., Xuan, G., "*Statistical moments based universal steganalysis using JPEG 2-D array and 2-D characteristic function*", in Proc. of International Conference on Image Processing (ICIP), Atlanta, GA, USA, pp. 105-108, Oct. 2006.

[3] Chen, Y. W., Lin, C. J., "*Combining SVMs with various feature selection strategies*", Feature Extraction, Foundations and Applications, Studies in Fuzziness and Soft Computing, Springer-Verlag, vol. 207, pp 315-324, 2006.

[4] Din, R., Samsudin, A., "*Digital steganalysis: computational. intelligence approach,*" International Journal *of* Computers, vol. 3, Issue 1, pp. 161-170, 2009.

[5] Farid, H., "*Detecting hidden messages using higher-order statistical models*", in International Conference on Image Processing, Rochester, New York, USA, vol. 2, pp. 905-908, 2002 .

[6] Farid, H. and Lyu, S., "*Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines*", in: F.A.P. Petitcolas (ed.): Information Hiding. 5 th International Workshop. Lecture Notes in Computer Science, vol. 2578, Springer-Verlag New York, pp. 340–354, 2002.

[7] Khosravi, M. J., Ghandali, S., "*A secure joint wavelet based steganography and secret sharing method*", 7th International Conference on Information Assurance and Security (IAS), pp. 222-227, 2011.

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

[9] Motamedi, H., Jafari, A., "*A new image steganography based on denoising methods in wavelet domain*", 9th International Conference on Information Security and Cryptology (ISC), pp. 18-25 ,2012.

[10] Pratt, W. K., *Digital Image Processing*, 3rd ed. , John Wiley & Sons, New York, USA, 2001.

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

[12] Trivedi, S., Chandramouli, R., "*Active steganalysis of sequential steganography*," SPIE Conference, California, vol. 5020, pp. 123-130, 2003.

[13] Yang, B. and Deng, B., "*Steganography in gray images using wavelet*", in Proceedings of ISCCSP, 2006.

[14] Zong, H., Liu, F., Luo, X., "*A wavelet-based blind JPEG image steganalysis using co-occurrence matrix*", 11th International Conference on Advanced Communication Technology (ICACT), vol. 3, pp. 1933 – 1936, February 2009.

[15] Zhang, X., Zhong, S. P., "*Blind steganalysis method for BMP images based on statistical MWCF and F-score method*", International Conference on Wavelet Analysis and Pattern Recognition, pp. 442–447, Baoding, July 2009.

زیرنویس‌ها

[1] Steganography

[2] Steganalysis