آشکارسازی کور حضور اطلاعات محرمانه پنهان در تصاویر JPEG

زهرا برکیان[۱]

مرتضی خادمی[۲]، کیان کیقباد[۳]

چکیده

هدف از این مقاله، ارائه آشکارساز کوری برای تشخیص تصاویر JPEG حاوی پیام محرمانه (تصویر آلوده) از تصاویر بدون پیام محرمانه (تصویر پاک) است. این آشکارساز با استفاده از دسته بندی کننده رگرسیون خطی و با بکارگیری ویژگی هایی که بر پایه خواص SVD از تصاویر آلوده و پاک استخراج شده اند قادر است با دقت و سرعت مناسبی حضور اطلاعات در تصویر JPEG را تشخیص دهد. نحوه عملکرد آشکارساز پیشنهادی برای شکستن الگوریتم های استگانوگرافی Outguess، F5، PQ و MBS در مقایسه با روش های موجود آشکارسازی مورد بررسی قرار گرفته است.

کلید واژه

تجزیه مقدار واحد (SVD)- آشکارسازی کور- استگانوگرافی- JPEG

---

۱. کارشناس ارشد مخابرات، دانشگاه فردوسی مشهد

۲. دانشیار دانشکده برق، دانشگاه فردوسی مشهد khademi@um.ac.ir

۳. دکتری دانشگاه آزاد اسلامی، واحد بناب

تاریخ دریافت: ۱۰ دی ۱۳۹۰ تاریخ پذیرش: ۳ اسفند ۱۳۹۰

مقدمه

استگانوگرافی ، علم مخابرات نامرئی است. هدف اصلی این علم، برقراری ارتباط امن به صورت کاملاً غیر آشکار می باشد. در واقع یک سیستم استگانوگرافی باید به گونه ای پیام محرمانه را در یک حامل رسانه ای (صوت، تصویر، ویدیو و ...) پنهان کند که هیچ تغییر محسوسی در رسانه ایجاد نشده و شنود کننده غیرمجاز کانال (حمله کننده) نتواند به وجود اطلاعات سری پی ببرد. با این حال، تشخیص وجود پیام محرمانه در حامل با استفاده از الگوریتم های آشکارسازی امکان پذیر است. لازم به ذکر است اگر الگوریتمی بتواند با نرخ موفقیتی بیش از حدس تصادفی فقط حضور پیام را مشخص نماید سیستم استگانوگرافی شکسته شده است.

الگوریتم های آشکارسازی پیام به دو دسته تقسیم می شوند:

- آشکارسازی ویژه : این روش برای آشکارسازی یک الگوریتم استگانوگرافی خاص طراحی می شود لذا از دقت آشکارسازی مناسبی برخوردار است.
- آشکارسازی کور (عمومی) : این روش مستقل از الگوریتم استگانوگرافی است. اگرچه این روش ممکن است از دقت پایین تری نسبت به حالت قبل برخوردار باشد ولی نتایج قابل قبولی در برابر الگوریتم های جدید استگانوگرافی ارائه می دهد.

در این مقاله یک روش آشکارسازی کور جدید برای شکستن الگوریتم های استگانوگرافی با حامل JPEG ارائه می شود. اخیراً فرمت JPEG به عنوان حامل رسانه ای در الگوریتم های استگانوگرافی، مورد توجه بسیاری از محققان قرار گرفته است زیرا:

۱- JPEG یک فرمت عمومی بوده و به طور گسترده مورد استفاده قرار می گیرد بطوری که اگر از فرمت JPEG برای پنهان سازی اطلاعات استفاده شود، ظن کمتری به تصویر خواهد بود.

۲- تشخیص اینکه وجود خرابی در ضرایب DCT کوانتیزه شده، ناشی از کوانتیزاسیون با کیفیت پایین است یا پنهان سازی اطلاعات، مشکل است.

۳- تصاویر JPEG ظرفیت استگانوگرافی (ماکزیمم طول پیام محرمانه) خوبی را ارائه می دهند.

الگوریتم های استگانوگرافی JPEG را می توان در دو دسته "تبدیل" و "بر پایه مدل" تقسیم بندی نمود. الگوریتم های دسته اول از بیت های اضافی در حوزه تبدیل در فرایند پنهان سازی استفاده می کنند. از جمله این الگوریتم ها می توان، F۵، Outguess و PQ را نام برد. الگوریتم های دسته دوم، قبل و یا بعد از فرایند پنهان سازی، خواص آماری تصویر را مدل نموده و به دنبال حفظ این مدل هستند. الگوریتم های MB۱ و MB۲ در این دسته قرار می گیرند.

الگوریتم F۵، بیت های پیام را در ضرایب DCT که به صورت تصادفی انتخاب شده اند، پنهان نموده و با استفاده از ماتریس پنهان سازی تعداد تغییرات ایجاد شده توسط پیام را به حداقل می رساند. الگوریتم استگانوگرافی Outguess شامل دو مرحله است: در مرحله اول بیت های پیام در طول یک گام تصادفی در LSB ضرایب DCT پنهان شده (ضرایب با مقادیر صفر و یک در فرایند پنهان سازی حضور ندارند)، و سپس در مرحله دوم ضرایب باقی مانده از مرحله اول به منظور حفظ هیستگرام تصویر اصلی تغییر داده می شوند [۷]. در الگوریتم پنهان سازی PQ، بر روی تصویر حامل یک نوع عملیات کاهش اطلاعات

مانند کوانتیزاسیون اعمال می گردد. بعد از عملیات کوانتیزاسیون، ضرایب کوانتیزه شده به وسیله یک کلید تصادفی بر هم ریخته می شوند و به همین دلیل به این الگوریتم، "کوانتیزاسیون آشفته" می گویند. یک الگوریتم استگانوگرافی در صورتی امن خواهد بود که تصاویر حاوی پیام محرمانه هیچ رفتار غیرطبیعی و قابل آشکاری ناشی از پنهان سازی پیام، از خود نشان ندهند. به عبارتی دیگر تصاویر آلوده باید خواص آماری مشابه با تصاویر پاک داشته باشند. با پیشرفت اینترنت و مخابرات، ضرورت وجود روش هایی که بتواند تصاویر آلوده را از تصاویر پاک متمایز کند بیشتر احساس می شود.

برای طراحی یک روش آشکارسازی کور با دو مشکل مواجه هستیم. اولین مشکل یافتن و محاسبه ویژگی هایی است که قادرند تغییرات ایجاد شده در خصوصیات آماری تصویر پاک را در طی فرایند پنهان سازی مشخص کنند. دومین مشکل به دست آوردن الگوریتم دسته بندی کننده قدرتمندی است که بتواند تفاوت های به دست آمده از این ویژگی ها را برجسته نموده و دقت دسته بندی بالایی داشته باشد. از آنجایی که الگوریتم های استگانوگرافی JPEG ضرایبDCT را به صورت تصادفی تغییر می دهند وابستگی خطی در سطرها و ستون های تصویر پاک کاهش می یابد. کاهش وابستگی های خطی در سطرها و ستون ها، بوسیله چک کردن مقادیر واحد (SVD) قابل آشکارسازی است. لذا در روش پیشنهادی ویژگی ها با استفاده از SVD استخراج گردیده و سپس از دسته بندی کننده رگرسیون خطی به منظور افزایش سرعت و کاهش پیچیدگی الگوریتم آشکارسازی، استفاده شده است.

روش آشکارسازی پیشنهادی با پنج روش مطرح کنونی (Xuan et al.، WAM، WBS، BSM، FBS و Gul et al.) در زمینه آشکارسازی کور تصاویر JPEG مقایسه شده است. در روش BSM ویژگی ها از طریق بیان تصویر در حوزه مکانی به دست می آید. از آنجائیکه همبستگی میان بیت های مجاور بعد از پنهان سازی پیام، کاهش می یابد می توان با بررسی نمودار بیت هشتم و هفتم چندین ویژگی را استخراج نمود. در WBS از فیلترهای آینه ای درجه دوم (QMF) برای تجزیه تصویر در حوزه ویولت استفاده شده و سپس خواص آماری مرتبه بالاتر از قبیل میانگین، واریانس، کج شدگی و کشیدگی برای هر زیرگروه به عنوان ویژگی محاسبه می گردد. الگوریتم های FBS و Xuan et al. از توابع آماری مرتبه بالاتر و ماتریس هم رخداد تصویر برای تولید ویژگی استفاده می کنند. ویژگی ها در روش WAM، از خواص آماری باقیمانده نویز استخراج می شوند. در روش Gul et al.، از ویژگی های استخراج شده توسط خواص SVD و دسته بندی کننده Wiener filtering استفاده شده است.

در ادامه، در بخش ۲ الگوریتم تولید ویژگی و در بخش سه چگونگی انتخاب مؤثرترین ویژگی ها از میان ویژگی های استخراج شده با استفاده از آزمون فرضیه ANOVA بیان گردیده است. در بخش چهار دسته بندی کننده پیشنهادی مورد بررسی قرار گرفته و در بخش پایانی نتایج آشکارساز ارائه شده است.

الگوریتم تولید ویژگی

از آنجائیکه در طی فرایند پنهان‌سازی الگوریتم های استگانوگرافی JPEG، ضرایب DCT تغییر یافته در طی یک جایگشت، برهم ریخته می شوند، خواص آماری تصویر در مکان های متفاوتی

تغییر می کند ولی در تمام تصویر این تغییرات همدیگر را متعادل می سازند. برهم ریختن ضرایب DCT، امکان تشخیص مکان پیام پنهان شده در تصویر را کاهش می دهد. بر خلاف خواص آماری، حفظ وابستگی خطی در طول پنهان سازی امکان پذیر نیست زیرا هر تغییر کوچکی در یک سطر، وابستگی خطی را نیز تغییر می دهد. از آنجائیکه الگوریتم های استگانوگرافی JPEG ضرایبDCT را به صورت تصادفی تغییر می دهند وابستگی خطی در سطرها و ستون های تصویر کاهش می یابد. کاهش وابستگی های خطی در سطرها و ستون ها، بوسیله چک کردن مقادیر واحد (SVD) قابل آشکارسازی است.

SVD یک ابزار قدرتمند در جبر خطی است. این ابزار یک ماتریس $A \in R^{m\times n}$ را به ضرب دو ماتریس اورتونرمال $U \in R^{m\times n}$ و $V \in R^{n\times n}$ و ماتریس قطری $S \in R^{m\times n}$ تبدیل می کند (معادله ۱). عناصر قطری ماتریس S غیر منفی هستند و به صورت کاهشی مرتب شده اند ($\delta_1 \geq \delta_2 \geq \ldots \geq \delta_{\min(m,n)}$ که در آن m و n ابعادA می باشند). بردار مقدار واحد S_V، اعضای قطری ماتریس S است.

$$A = USV^T \tag{۱}$$

$$S_v = Diag(S) \tag{۲}$$

بر طبق قضیه مرجع [۸] برای ماتریس A، اگر i، تعداد سطرهای وابسته خطی و j، تعداد ستون های وابسته خطی و k، تعداد صفرهای بردار مقدار واحد باشد، داریم:

$$k = \begin{cases} i-1 & i > j \\ j-1 & i < j \end{cases} \tag{۳}$$

با توجه به آنچه گفته شد ویژگی ها زیر بر پایه SVD تعریف می گردند:

• ویژگی های نوع اول: این ویژگی ها میانگین تعداد صفرها در اندیس iام بردارهای Sv در بلوک هایی با اندازه W×W می باشند. R تعداد اعداد صحیح بلوک های W×W با ۵۰ درصد همپوشانی در تصویر M×N است. ویژگی های نوع یک به صورت زیر تعریف می شود:

$$f_W^{(1)} = \frac{1}{R}\sum_R \delta(S_v(i)), \quad W = 3,\ldots,20 \quad i = 1,\ldots,W \quad \delta(k) = \begin{cases} 1 & k = 0 \\ 0 & k \neq 0 \end{cases} \tag{۴}$$

• ویژگی های نوع دوم: این ویژگی ها میانگین مقادیر واحد در اندیس iام بردار Sv در بلوک های W×W می باشند.

$$f_W^{(2)}(i) = \frac{1}{R}\sum_R S_v(i) \quad W = 3,\ldots,20 \quad i = 1,\ldots,W \tag{۵}$$

• ویژگی های نوع سوم: واریانس ویژگی های نوع یک بر اساس i یا W. اگر i ثابت فرض شود واریانس ویژگی های نوع یک بر رویW و اگرW ثابت فرض شود واریانس بر روی i گرفته می شود. بنابراین

ویژگی های نوع ۳ دارای دو زیرمجموعه است.

• ویژگی های نوع چهارم: نحوه تعریف این ویژگی ها شبیه به نوع ۳ است فقط با این تفاوت که واریانس بر روی مجموعه ویژگی نوع ۲ است.

• ویژگی های نوع پنجم: این ویژگی ها همانند نوع سه هستند با این تفاوت که به جای شمارش تعداد مقادیر واحد صفر، تعداد مقادیر واحدی که بازه ای مانند $[10^{-16},10^{-8}]$ قرار می گیرند شمرده شده و سپس واریانس بر اساس i یا w گرفته می شود.

با توجه به این پنج نوع ویژگی جمعاً ۸۳۴ ویژگی تولید می شود.

در مرحله دوم آشکارسازی، باید مؤثرترین ویژگی ها، یعنی آن دسته از ویژگی هایی که در تصاویر پاک و آلوده با یکدیگر بیشترین تفاوت را دارند، انتخاب گردند. در روش آشکارسازی پیشنهادی از تست ANOVA برای انتخاب ویژگی های مؤثر استفاده شده که در ادامه مورد بررسی قرار می گیرد.

الگوریتم تولید ویژگی

برای تحلیل آماری ویژگی های پیشنهاد شده از تکنیک ANOVA استفاده می شود. ANOVA یک تکنیک آزمایش فرضیه آماری است که مشخص می کند آیا گروه های داده از نظر آماری با هم متفاوت هستند یا نه؟ در این روش آشکارسازی، ازANOVA یک طرفه برای آزمایش ویژگی های پیشنهاد شده استفاده گردیده است.

خروجی تابع ANOVA یک طرفه، مقدار p است. این مقدار بیانگر احتمال یافتن مشابهت میان میانگین گروه های داده است. لذا هر اندازه مقدار p کوچکتر باشد گروه های موجود در تست ANOVA با یکدیگر تفاوت بیشتری دارند. در عمل $p<0.05$ مطلوب می باشد.

برای چهار الگوریتم استگانوگرافیJPEG، دو گروه داده شامل بردارهای ویژگی (۸۳۴ ویژگی) که از روی ۵۰۰ تصویر پاک و آلوده (با نرخ های پنهان سازی متفاوت) محاسبه شده اند تشکیل شده و آزمایش ANOVA بر روی آن اعمال گردیده است. نتایج این آزمایش برای الگوریتم های استگانوگرافی JPEG به شرح زیر است:

• PQ: از میان ۸۳۴ ویژگی، ۱۰۵ ویژگی دارای مقدار p کمتر از ۰.۰۱ هستند. کمترین مقدار p برابر است با: p= ۸.۸۴۵۱e-۰۰۶

• F5: از میان ۸۳۴ ویژگی، ۷۴ ویژگی دارای مقدار p کمتر از ۰.۰۱ هستند. کمترین مقدار p برابر است با: p= ۱.۶۴۱۲e-۰۰۸

• Outguess: از میان ۸۳۴ ویژگی، ۸۰ ویژگی دارای مقدار p کمتر از ۰.۰۲ هستند. کمترین مقدار p برابر است با: p= ۰.۰۰۲۷

• MBS: از میان ۸۳۴ ویژگی، تنها ۳۰ ویژگی دارای مقدار p کمتر از ۰.۳ هستند. کمترین مقدار p برابر است با: p= ۰.۰۰۳۳

با توجه مقادیر p انتظار می رود ویژگی های SVD، ویژگی مناسبی برای شکستن الگوریتم استگانوگرافی MBS نباشند. در جدول ۱ نتایج آزمایش ANOVA (کوچکترین مقادیر p) برای

آشکارساز پیشنهادی بیان گردیده است. این آزمایش بر روی ۲۰۰۰ تصویر آلوده و پاک انجام شده است. تصاویر تشکیل دهنده مجموعه آموزشی که در اندازه های متنوع و با ۳۰۰ نوع دوربین مختلف گرفته شده اند از اینترنت دانلود گردیده اند.

اطلاعات محرمانه در تصاویر آلوده با استفاده از الگوریتم های استگانوگرافیJPEG و با نرخ های متفاوت، پنهان سازی شده است. الگوریتم های Outguess ، F۵ و MBS از اینترنت دانلود و الگوریتم PQ شبیه سازی شده است. در این آزمایش ازمیان ۸۳۴ ویژگی، ۱۵۴ ویژگی دارای مقدار p کمتر از ۰.۰۱ هستند.

حال باید از میان ویژگی های، مؤثرترین آنها به منظور عملکرد بهتر روش آشکارسازی، انتخاب شوند. الگوریتم انتخاب ویژگی به صورت زیر است:

- انتخاب ویژگی هایی که مقدار p آنها حداقل در دو الگوریتم استگانوگرافی مورد تأیید است.
- انتخاب ویژگی هایی که مقدار p آنها در الگوریتم های استگانوگرافی PQ، Outguess و F۵ کمتر از ۰.۰۰۱ است.
- انتخاب ویژگی هایی که مقدار p آنها در الگوریتم استگانوگرافی MBS کمتر از ۰.۰۵ است.

با استفاده از این الگوریتم انتخاب ویژگی، ۱۶۵ ویژگی انتخاب می شود.

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
p	۳,۵۸۶ ۱۱۰۱۰×	۳,۷۲۸ ۱۱۰۱۰×	۴,۵۱۵ ۱۱۰۱۰×	۴,۶۶۰ ۱۱۰۱۰×	۴,۸۹۹ ۱۱۰۱۰×	۵,۰۵۴ ۱۱۰۱۰×	۵,۰۵۶ ۱۱۰۱۰×	۵,۸۳۵ ۱۱۰۱۰×	۶,۳۴۰ ۱۱۰۱۰×	۶,۶۳۶ ۱۱۰۱۰×

جدول ۱. نتایج آزمایش ANOVA (کوچکترین مقادیر p)

دسته‌بندی کننده

با داشتن بردارهای ویژگی بر پایه SVD از هر تصویر آلوده و پاک، می توان یک دسته بندی کننده رگرسیون خطی طراحی نمود. بردارهای ویژگی اگر متعلق به تصاویر پاک باشند به مقدار -۱ و اگر متعلق به تصاویر آلوده باشند به مقدار ۱ برگشت داده می شوند. هر سطح تصمیم به عنوان یک ترکیب خطی از ویژگی‌ها در نظر گرفته می شود.

$$g_i \in \beta_1 f_{1i} + \beta_2 f_{2i} + \ldots + \beta_q f_{qi} \qquad (۶)$$

در معادله ۶، f بردار ویژگی محاسبه شده از تصویر iام و ضرایب رگرسیون می باشد.

ضرایب رگرسیون در مرحله آموزش تخمین زده می شود. برای یک تصویر، ابتدا بردار ویژگی f ساخته می شود، سپس مقدار g با استفاده از معادله ۷ محاسبه می گردد.

$$g = \beta_1 f_1 + \beta_2 f_2 + \ldots + \beta_q f_q \qquad (۷)$$

اگر مقدار محاسبه شده g بیشتر از صفر باشد تصویر آلوده است و در غیر اینصورت، تصویر پاک است.

در این پروژه برای بالا بردن دقت دسته بندی کننده از پنج دسته بندی کننده رگرسیون خطی به طور همزمان استفاده شده است که عبارتند از:

۱. دسته بندی کننده رگرسیون خطی طراحی شده بر اساس ۱۶۵ ویژگی کلی استخراج شده با

استفاده از مجموعه آموزشی شامل تصاویر پاک و آلوده به تمام الگوریتم های استگانوگرافی JPEG
۲. دسته بندی کننده رگرسیون خطی طراحی شده بر اساس ۱۰۵ ویژگی استخراج شده با استفاده از مجموعه آموزشی شامل تصاویر پاک و آلوده به الگوریتم استگانوگرافی PQ
۳. دسته بندی کننده رگرسیون خطی طراحی شده بر اساس ۷۴ ویژگی استخراج شده با استفاده از مجموعه آموزشی شامل تصاویر پاک و آلوده به الگوریتم استگانوگرافی F۵
۴. دسته بندی کننده رگرسیون خطی طراحی شده بر اساس ۸۰ ویژگی استخراج شده با استفاده از مجموعه آموزشی شامل تصاویر پاک و آلوده به الگوریتم استگانوگرافی Outguess
۵. دسته بندی کننده رگرسیون خطی طراحی شده بر اساس ۳۰ ویژگی استخراج شده با استفاده از مجموعه آموزشی شامل تصاویر پاک و آلوده به الگوریتم استگانوگرافی MBS

برای تشخیص پاک یا آلوده بودن تصویر، ابتدا پارامتر g۱ (معادله ۷) با استفاده از دسته بندی کننده اول محاسبه می گردد، با توجه به مقدار g۱ یکی از سه حالت زیر رخ می دهد:

۱. اگر g۱ بزرگتر مساوی ۰.۱ باشد، تصویر آلوده است.
۲. اگر g۱ کوچکتر مساوی ۰.۱- باشد، تصویر پاک است.
۳. اگر g۱ در بازه (۰.۱ ,۰.۱-) قرار دارد در این صورت با استفاده از دسته بندی کننده های دوم تا چهارم مقادیر g۴ ،g۳ ،g۲ و g۵ محاسبه می گردد. حال اگر حداقل دو تا از مقادیر g۱ تا g۵ و یا مجموع g۱ تا g۵ مثبت باشد تصویر آلوده و در غیر این صورت پاک تشخیص داده می شود.

نتایج آشکارسازی

در این بخش، نتایج روش آشکارسازی کور پیشنهادی ارائه شده و با روش های موجود آشکارسازی کور مقایسه می گردد. روش آشکارسازی کور پیشنهادی از دو جهت مورد بررسی قرار گرفته است: اول از جهت دقت آشکارسازی و دوم سرعت آشکارسازی که در ادامه بیان می گردد.

دقت آشکارسازی

معیار اندازه گیری دقت آشکارسازی AUR است. در این معیار سطح زیر منحنی ROC محاسبه می گردد. منحنی ROC، نمودار مثبت درست (احتمال اینکه جواب دسته بندی کننده مثبت باشد به شرط اینکه تصویر آلوده باشد) بر حسب مثبت اشتباه (احتمال اینکه جواب دسته بندی کننده مثبت باشد به شرط اینکه تصویر پاک باشد.) می باشد.

بدترین عملکرد یک دسته بندی کننده هنگامی اتفاق می افتد که منحنی ROC آن یک خط با زاویه ۴۵ درجه باشد. بدین معنی که دسته بندی کننده یک تصویر آلوده را با احتمال مساوی، آلوده یا پاک تشخیص می دهد. بنابراین می توان سطح زیر منحنی ROC را به عنوان دقت دسته بندی کننده بیان نمود.

در جداول ۲ تا ۵ مقادیر AUR آشکارساز پیشنهادی با سایر آشکارسازهای کور موجود، برای شکستن چهار الگوریتم معروف استگانوگرافی JPEG مقایسه شده است.

Embedding rate / Steganalysis method	0.4	0.2	0.1	0.05
FBS	NA	90.91	78.77	65.10
WBS	NA	57.77	53.27	50.76
BSM	NA	55.82	53.98	51.61
WAM	72.36	66.34	59.16	54.52
Xuan et al	64.77	61.97	57.01	54.03
Gul et al	67.60	64.16	59.31	55.66
Proposed	87.72	86.24	85.86	83.60

جدول ۲. مقادیر AUR آشکارساز پیشنهادی و آشکارسازهای موجود به ازای الگوریتم استگانوگرافی Outguess

Embedding rate / Steganalysis method	0.4	0.2	0.1	0.05
FBS	89.93	76.39	62.74	55.20
WBS	59.94	53.44	50.58	49.87
BSM	52.55	51.25	50.23	49.94
WAM	70.74	63.21	55.51	52.56
Xuan et al	54.95	53.21	50.84	50.67
Gul et al	66.37	58.87	53.25	51.54
Proposed	87.52	84.45	82.99	82.13

جدول ۳. مقادیر AUR آشکارساز پیشنهادی و آشکارسازهای موجود به ازای الگوریتم استگانوگرافی F۵

Embedding rate / Steganalysis method	0.4	0.2	0.1	0.05
FBS	56.95	52.64	50.87	50.27
WBS	55.54	52.82	51.90	50.79
BSM	55.34	53.33	52.16	51.23
WAM	62	NA	NA	NA
Xuan et al	71	NA	NA	NA
Gul et al	68	NA	NA	NA
Proposed	74.68	67.94	62.32	56.8

جدول ۴. مقادیر AUR آشکارساز پیشنهادی و آشکارسازهای موجود به ازای الگوریتم استگانوگرافی PQ

Embedding rate / Steganalysis method	0.4	0.2	0.1	0.05
FBS	79.01	64.65	57.06	53.35
WBS	56.79	53.41	50.85	50.14
BSM	53.62	51.53	50.85	50.11
WAM	85.91	81.24	70.55	59.81
Xuan et al	58.19	55.51	52.97	51.44
Gul et al	69.20	63.67	58.14	54.15
Proposed	53.31	53.2	52.8	52.4

جدول ۵. مقادیر AUR آشکارساز پیشنهادی و آشکارسازهای موجود به ازای الگوریتم استگانوگرافی MBS

بحث

همانطور که انتظار داشتیم دقت آشکارسازی با استفاده از دسته بندی کننده پیشنهادی نسبت به حالتی که از یک دسته بندی کننده رگرسیون خطی استفاده می شود بهبود یافته است. زیرا بیشترین خطا در دسته بندی کننده رگرسیون خطی در مقادیر g نزدیک به صفر رخ می دهد. بنابراین از آنجائیکه در دسته بندی کننده پیشنهادی بر روی این مقادیر چهار دسته بندی کننده دیگر نیز اعمال شده است، دقت دسته بندی کننده و در نتیجه آشکارساز پیشنهادی افزایش یافته است.

دقت آشکارسازی الگوریتم Outguess به ازای ظرفیت های استگانوگرافی متفاوت تقریباً یکسان است زیرا همانطور که در مقدمه اشاره شد در این الگوریتم ابتدا بیت های پیام در LSB ضرایب DCT پنهان شده و سپس به منظور حفظ هیستگرام اصلی تصویر، بقیه ضرایب تغییر داده می شوند. بنابراین عملاً در این الگوریتم بدون توجه به اندازه پیام تمام ضرایب DCT تغییر خواهند نمود. از این رو وابستگی خطی پیکسل ها در حوزه مکان به ازای نرخ های مختلف طول پیام محرمانه، تقریباً مشابه است.

همانطور که از تست ANOVA نیز انتظار داشتیم این الگوریتم نمی تواند به خوبی MBS را آشکار نماید زیرا این الگوریتم استگانوگرافی، یک الگوریتم بر پایه مدل است و از ضرایب DCT برای پنهان سازی استفاده نمی کند. آنچه که باعث تغییر وابستگی خطی سطرها و ستون-های تصویر در حوزه مکان می شود تغییر ضرایب DCT در حوزه تبدیل است.

در جدیدترین الگوریتم استگانوگرافی JPEG که در سال ۲۰۰۷ ارائه شده است (YASS) ابتدا پیام محرمانه در حوزه مکان پنهان شده سپس تصویر به JPEG تبدیل می شود. همانطور که در بالا نیز اشاره شد به طور کلی آشکارساز پیشنهادی هنگامی موفق است که اطلاعات محرمانه در ضرایب DCT پنهان شده و سپس تصویر در حوزه مکان مورد بررسی قرار گیرد و این دقیقاً عکس فرایندی است که در YASS اتفاق می افتد.

سرعت آشکارسازی

مدت زمان لازم برای تعیین پاک یا آلوده بودن تصویر ۱۰۰kb با استفاده از روش آشکارسازی پیشنهادی با سیستم کامپیوتری با خصوصیات ذیل حداکثر برابر ۱۰ دقیقه است.

- CPU: Dual Core Intel Pentium D ۹۴۵, ۳۴۱۶ MHz
- Motherboard: Gigabyte GA-۸I۹۴۵G
- RAM: ۱G
- OS Name: Microsoft Windows XP Professional SP۲

این زمان برای الگوریتم های BSM، FBS و WBS با سیستمی با مشخصات زیر به ترتیب برابر با ۱ ساعت، ۳ ساعت و ۱۲ ساعت می باشد [۲۳].

- CPU: Xeon Pentium ۴, ۲۸۰۰ MHz
- OS Name: Linux

تمام برنامه های آشکارساز پیشنهادی با زبان برنامه نویسی MATLAB پیاده سازی شده است. بدیهی است که اگر این برنامه ها با زبان C نوشته شوند سرعت بسیار بهبود خواهد یافت.

مراجع

[1] M. Kharrazi, H.T. Sencar, N. Memon, "Image Steganography:Concepts and Practice", Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, Singapore, Republic of Singapore, 2004.

[2] J.J. Eggers, R. Bäuml, B. Girod, "A Communications Approach to Image Steganography", Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, Vol. 4675, San Jose, California, 2002.

[3] J. Fridrich, M. Goljan, R. Du, "Steganalysis Based on JPEG Compatibility", Proc. SPIE Multimedia Systems and Applications IV, Vol. 4518, Denver, Colorado, pp. 2752001 ,280-.

[4] B. Li et al., "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, pp. 142173-, April 2011

[5] R. Bohme, A. Westfeld, "Breaking Cauchy model-based JPEG steganography with first order statistics", ESORICS 2004, LNCS 3193, pp. 1252004 ,140-.

[6] A. Westfeld, "High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm)", In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol. 2137, Springer-Verlag, Berlin Heidelberg New York, 2001.

[7] J. Fridrich, M. Goljan, D. Hogea, "Attacking the OutGuess", In: Proc. ACM: Special Session on Multimedia Security and Watermarking, Juan-les-

Pins, France, 2002.
[8] G. Gül, A.E. Dirik, I. Avcibas, "Steganalytic Features for JPEG Compression-Based Perturbed Quantization", IEEE SIGNAL PROCESSING LETTERS, Vol. 14, No. 3, March 2007.
[9] J. Fridrich, M. Goljan, D. Soukal, "Perturbed quantization steganography with wet paper codes" In: Proc. ACM Multimedia Security Workshop, pp. 415-, Magdeburg, Germany, September 202004 ,21-.
[10] I. Avcibas, N. Memon, B. sankur, "Image steganalysis with binary similarity measures", IEEE International Conference on Image Processing, Rochester, New York, September 2002.
[11] S. Lyu, H. Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", 5th International Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002.
[12] S. Lyu and H. Farid, "Steganalysis using color wavelet statistics and one-class support vector machines", SPIE Symposium on Electronic Imaging, San Jose, CA, , 2004.
[13] J. Fridrich, T. Pevny, "Towards multi–class blind steganalyzer for JPEG images", In: M. Barni, I. Cox, T. Kalker, H.J. Kim, (Eds): Proc. 4th Int. Workshop on Digital Watermarking, Sienna, Italy, pp. 3953-, September 2005.
[14] G. Xuan et al., "Steganalysis using high-dimensional features derived from co-occurrence matrix and class-wise non-principal components analysis (CNPCA)," in Int.Workshop on Digital Watermarking, Korea, Nov. 8–10, 2006
[15] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 607 201–1, 2006.
[16] G. Gul, F. Kurugollu, "SVD-Based Universal Spatial Domain Image Steganalysis", IEEE Transactions On Information Forensics and Security, Vol. 5, No. 2, June 2010
[17] G. Gul and F. Kurugollu, "A novel universal steganalyser design:Logsv," in IEEE Int. Conf. Image Processing (ICIP 2009), Cairo,Egypt, 2009.
[18] I. Avcibas, N. Memon, and B. Sankur, Steganalysis using image quality metrics, IEEE Trans. Image Processing, vol. 12, no. 2, pp. 2212003 ,229-.

[19] www.dpreveiw.com
[20] Software [Online] Available: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html.
[21] Software [Online] Available: http://www.outguess.org/.
[22] Software [Online] Available: http://www.philsallee.com/mbsteg/index.html
[23] M. Kharrazi, T.H. Sencar, N. Memon, "Benchmarking steganographic and steganalysis techniques", EI SPIE San Jose, CA, January 162005 ,20-.
[24] A. Slaby, "ROC Analysis with Matlab", Proceedings of the ITI 2007 29th Int. Conf. on Information Technology Interfaces, Cavtat, Croatia, June 25,28-2007
[25] K. Solanki, A. Sarkar, and B. S. Manjunath, "YASS: Yet another steganographic scheme that resists blind steganalysis," in 9th Int. Workshop on Information Hiding, Saint Malo, France, Jun. 2007.