

ارتباط احتمال کشف، ظرفیت و هزینه نهان نگاری با مدل سازی نهان کاو

ایمان غلام پور^{۱*}، روح الله امیری^۲

۱- استادیار، ۲- دانشجوی دکتری، دانشگاه صنعتی شریف

(دریافت: ۹۶/۰۵/۲۹، پذیرش: ۹۶/۰۷/۱۲)

چکیده

قابلیت کشف آماری یک نهان کاو بیان کننده توانایی آن در تشخیص تصاویر پاک از تصاویر درج شده است. نهان نگاری بهینه به گونه ای باید طراحی شود که نهان کاو نتواند تصاویر درج شده را تشخیص دهد. به همین دلیل، طراحی یک الگوریتم نهان نگاری بر مبنای کاهش قابلیت کشف آماری نهان کاو، هدفی مهم در نهان نگاری است. با این حال، ایجاد رابطه دقیق بین هزینه تغییر تصویر و قابلیت کشف آماری در حالت کلی مسئله ای حل نشده است. در این مقاله با مدل سازی نهان کاو توسط مدل های گرافیکی خاصی به نام مدل های موضوعی، به تخمین احتمال خطای نهان کاو به عنوان معیاری از قابلیت کشف آماری رسیده ایم. همچنین، بر اساس این معیار، تعریف جدیدی از ظرفیت نهان نگاری ارائه داده شده و رابطه آن را با هزینه تغییر تصویر بررسی گردیده است. همچنین، نشان داده شده است که روابط ریاضی حاصل بین پارامترهای نهان نگار و نهان کاو با ملاک های کلاسیک نظیر PSNR همخوانی دارد. سپس از رابطه هزینه تغییر تصویر و قابلیت کشف آماری به یک الگوریتم نهان نگاری مناسب رسیده ایم. با آزمون روی داده گان مناسب نشان داده شده است که الگوریتم حاصل در زمره بهترین الگوریتم های قابل تحلیل ریاضی است. لازم به ذکر است که تمرکز این مقاله روی حل یک مسئله تئوریک و بازتعریف مفاهیم نهان نگاری است به طوری که روش بهینه درج بر مبنای بهینه سازی فریب نهان کاو انجام گردد و نه به صورت کلاسیک بر مبنای کاهش فاصله تصویر پوشش و تصویر درج شده. با این حال عملاً به بهبود دقت اندکی در حدود ۰/۵٪ نیز حاصل شده است.

واژگان کلیدی: نهان نگاری، مدل نهان کاوی، ظرفیت نهان نگاری، هزینه تغییر پیکسل، قابلیت کشف آماری، مدل های موضوعی

۱- مقدمه

می برد؛ به گونه ای که ابتدا پیام را رمز کرده و سپس آن را درون یک پوشش دیجیتال پنهان می کنند. در این حالت، در صورتی که نهان کاو به وجود مرادده مخفی پی ببرد و حتی بتواند داده درون پوشش را استخراج کند، با یک متن رمز شده مواجه می شود و باز هم نمی تواند به محتوای پیام اصلی دست پیدا کند.

هدف نهان نگاری، ارسال اطلاعات به صورت مخفی در قالب پوشش های دیجیتال است و این هدف توسط روش های نهان کاوی که به دنبال کشف این ارتباط مخفی هستند، تهدید می شود [۴]- [۷]. قابلیت کشف آماری، یک ویژگی نهان کاو است که با معیارهای خاصی می توان آن را در سمت نهان نگار اندازه گیری کرد. از جمله برخی از این معیارها می توان به دیورژانس KL [۴] یا MMD^1 بین بردارهای ویژگی [۸] اشاره کرد. در [۹] و [۱۰] نشان داده شده است که ظرفیت نهان نگاری با ریشه دوم ابعاد تصویر رشد می کند. در نتیجه، در تصاویر با ابعاد بسیار بزرگ، نرخ درج اطلاعات به صورت امن به سمت صفر میل خواهد کرد.

ایده ارتباط پنهان بین افراد از دیرباز مورد توجه بوده است [۱]. در رمزنگاری با تبدیل پیام به شکل رمز شده، آن را برای افرادی که کلید رمزنگاری را در اختیار ندارند، غیرقابل فهم می سازد. با این حال، هر چند رمزنگاری مورد استفاده قدرتمند باشد، ارسال پیام رمز شده دشمن را بیش از حد معمول تحریک می کند. به همین دلیل، طرفین مرادده باید به صورتی با هم ارتباط برقرار کنند که دشمن متوجه انتقال اطلاعات بین آن ها نشود [۳-۲]. این نیاز موجب پیدایش زمینه ای به نام نهان نگاری شده است. نهان نگاری به صورت مخفی کردن پیام، درون پوشش های دیجیتال مانند تصویر انجام می گیرد و بدین طریق ارتباط بین طرفین مرادده مخفی نگاه داشته می شود. از جهت دیگر، علم نهان کاوی برای مقابله با نهان نگاری شکل گرفته است. استفاده توأم از رمزنگاری و نهان نگاری، سطح امنیت تبادل اطلاعات را بسیار بالا

موجب کمینه کردن قابلیت کشف آماری شوند. با این وجود، هنوز رابطه مشخصی بین هزینه تغییر پیکسل و قابلیت کشف آماری وجود ندارد؛ تنها می‌دانیم که هزینه تغییر پیکسل در نواحی هموار تصویر که به راحتی قابل مدل سازی هستند، باید بالاتر از نواحی نویزی و لبه‌ها باشد. در ساختار الگوریتم‌های جدید برای سادگی از اعوجاج جمع‌پذیر یا معادل جمع‌پذیر برای توابع اعوجاج غیر جمع‌پذیر استفاده می‌شود که در این صورت نیز قابل پیاده‌سازی با STC هستند [۲]. الگوریتم HUGO^۶ [۲۵]، اولین الگوریتمی است که به صورت عملی از کمینه کردن اعوجاج در ساختار خود بهره می‌برد. در این الگوریتم هزینه تغییر هر پیکسل به صورت مجموع وزن داری از اختلاف بین بردار ویژگی‌های تصویر پوشش و تصویر درج شده (در آن پیکسل) محاسبه می‌شود و در آن از بردار ویژگی‌های SPAM^۷ [۳۷] استفاده شده است. نحوه تخصیص هزینه، این الگوریتم حوزه مکان را تحت نمان کاوی با بردار ویژگی‌های SPAM غیر قابل کشف ساخته است. در الگوریتم WOW^۸ [۲۹] هزینه تغییر هر پیکسل از روی باقیمانده-های وزن دار فیلترهای موجک^۹ محاسبه می‌شود. این روش با این فرض ارائه شده است که مقدار باقیمانده فیلتر با قابلیت کشف آماری رابطه معکوس دارد. ایده این الگوریتم، در الگوریتم حوزه مکان S-UNIWARD^{۱۰} با تغییر کمی در تابع اعوجاج تکرار شده است [۳۰] هر دو روش ذکر شده، عملکردی به مراتب بهتر از الگوریتم HUGO تحت نمان کاوی با بردارهای ویژگی^{۱۱} SRM [۳۸] دارند. در ادامه به بررسی الگوریتم MG^{۱۲} [۳۱] می‌پردازیم که روند متفاوتی برای محاسبه هزینه تغییر پیکسل دارد. این الگوریتم با مدل سازی تصویر پوشش به صورت نرمال چندمتغیره، اطلاعات فیشر را به عنوان معیاری از کشف پذیری آماری محاسبه می‌کند. سپس این تابع را نسبت به احتمال تغییر هر پیکسل کمینه می‌کند. در مرحله بعد، هزینه تغییر هر پیکسل را از روی این احتمال‌ها محاسبه می‌کند. این الگوریتم در نرخ‌های درج پایین عملکردی مشابه HUGO دارد و با بالا رفتن میزان درج، همچنان خاصیت وفقی خود را حفظ می‌کند و عملکرد آن تحت نمان کاوی با بردارهای ویژگی SRM بهتر از HUGO خواهد بود. علاوه بر عملکرد مناسب این الگوریتم، اهمیت اصلی آن ایجاد ارتباط بین معیار نظری دیورژانس KL (به عنوان معیاری از قابلیت کشف آماری) و هزینه تغییر پیکسل است. با این وجود، همچنان ارتباط روشی بین هزینه تغییر پیکسل و قابلیت کشف آماری وجود ندارد [۳۹]-[۴۰]. پس از مقدمه، در بخش دوم

همچنین، اطلاعات فیشر^۱ به عنوان تقریبی از دیورژانس KL، ظرفیت سامانه‌های نمان نگاری را مشخص می‌کند [۱۱] که در [۱۲] یک تخمین زننده عملی برای آن ارائه شده است. در تمام این بررسی‌ها از دیورژانس KL به عنوان معیاری از قابلیت کشف آماری استفاده شده است که نمی‌تواند توصیف کننده کاملی از آن باشد. الگوریتم‌های نمان نگاری به سه دسته الگوریتم‌های مبتنی بر سنتز پوشش، انتخاب پوشش و تغییر پوشش تقسیم می‌شوند؛ که دو دسته اول صرفاً جنبه نظری دارند و الگوریتم‌های عملی نمان نگاری همگی بر پایه تغییر پوشش طراحی شده‌اند [۵]. الگوریتم‌های دسته سوم برای کاهش قابلیت کشف آماری از سه روش متفاوت استفاده می‌کنند. در روش اول تلاش می‌کنند که یک مدل مشخص از پوشش، در اثر درج ثابت بماند. گستره زیادی از الگوریتم‌های نمان نگاری بر این پایه استوارند؛ که از جمله آن‌ها می‌توان به روش‌های حفظ خواص آماری مرتبه اول [۱۳]-[۱۶]، روش‌های حفظ آمارگان مراتب بالاتر [۱۷] و یا روش‌های آماری تصحیح ویژگی [۱۸]-[۱۹] اشاره کرد. هرچند این الگوریتم‌ها بر اساس یک مدل خاص از پوشش کشف ناپذیرند، ولی در صورتی که نمان کاو از یک مدل دیگر برای توصیف پوشش استفاده کند، قابل کشف خواهند بود. در روش دوم که به الگوریتم‌های درج ماتریسی^۲ مشهور هستند، سعی می‌شود که تعداد تغییرات ناشی از درج کمینه شود [۲۰]-[۲۳]. در این روش‌ها، مکان تغییرات اهمیتی ندارد و از نظر آن‌ها هزینه تغییر پیکسل‌های مختلف یکسان هستند. در روش سوم که به DM^۳ مشهور است، نمان نگار با به کارگیری یک روش کدینگ، تابع اعوجاج مورد نظر خود را کمینه می‌کند. قوی‌ترین الگوریتم‌های نمان نگاری در سال‌های اخیر از این روش برای کاهش قابلیت کشف آماری استفاده می‌کنند [۲۴]-[۳۱]. در [۳۲] روش کدینگ کاغذ خیس^۴ ارائه شده است که در آن نیازی به اشتراک گذاشتن کانال نداریم. همچنین، تعدادی روش‌های کدینگ عملی طراحی شده‌اند که دارای عملکردی در نزدیکی باند نرخ-اعوجاج هستند [۳۳]-[۳۵]. از مهم‌ترین این روش‌ها می‌توان به STC^۵ اشاره کرد؛ این روش، تابع اعوجاج را به صورت جمع‌پذیر (نسبت به پیکسل‌های تصویر) در نظر می‌گیرد و با استفاده از کدینگ کاغذ خیس، در تصویر به گونه‌ای درج می‌کند که اعوجاج کل کمینه شود [۳۶]. به همین دلیل، طراحی یک الگوریتم نمان نگاری جدید، معادل طراحی یک تابع اعوجاج یا حتی تخصیص مناسب هزینه‌های تغییر پیکسل خواهد بود. در حالت ایده‌آل، هزینه تغییر هر پیکسل باید به گونه‌ای تعریف شود که

6- Highly Undetectable Stego

7- Subtractive Pixel Adjacency Matrix

8- Wavelet Obtained Weights

9- Wavelet

10- Spatial Universal Wavelet Relative Distortion

11- Spatial Rich Model

12- Multivariate Gaussian

1- Fisher Information

2- Matrix Embedding

3- Distortion Minimization

4- Wet Paper Coding

5- Syndrome Trellis Coding

است که آشکارسازی آن نسبت به روش‌های مبتنی بر جایگذاری LSB^۲ دشوارتر است. اگر احتمال ± 1 شدن برابر β_i باشد، توزیع پیکسل متناظر خروجی به صورت (۳) درمی‌آید.

$$q_j(\beta_i) = (1 - 2\beta_i)p_j + \beta_i(p_{j+1} + p_{j-1}) \quad (۳)$$

برای انتخاب نقاط مناسب برای تغییر و درج پیام بدون کدکردن محل درج از کدینگ کاغذ خیس استفاده می‌شود. ایده کدینگ کاغذ خیس برای اولین بار در [۳۲] مطرح شد. از این روش برای آشکارسازی اطلاعات درج‌شده بدون اطلاع از توزیع مکانی درج در پوشش استفاده می‌شود. فرض کنید تصویر پوشش مورد استفاده $\mathbf{X} = \{x_1, \dots, x_n\}$ دارای n پیکسل باشد و k عدد از آن‌ها قابل تغییر باشد. در نام‌گذاری کدهای کاغذ خیس این بخش معادل قسمت‌های خشک یک کاغذ ذهنی است که قابل نوشتن است. حال هدف این است که با تغییر مقادیر این پیکسل‌ها، پیام مورد نظر (m) در تصویر پوشش درج شود. اگر تصویر پس از درج را با \mathbf{Y} نشان دهیم و بردارهای به ترتیب بردارهای بیت‌های کم‌ارزش تصویر اولیه و ثانویه باشند، می‌خواهیم \mathbf{Y} را با تغییر روی \mathbf{X} به گونه‌ای بسازیم که رابطه (۴) برقرار باشد. در این رابطه، ماتریس \mathbf{D} یک ماتریس تصادفی از پیش به اشتراک گذاشته شده بین فرستنده و گیرنده است. از آن‌جایی که k پیکسل قابل تغییر داشتیم، بردار \underline{v} دارای k عنصر مجهول و $n-k$ عنصر صفر است. لذا می‌توان با حذف $n-k$ عنصر صفر از بردار \underline{v} و ستون‌های متناظر آن‌ها از ماتریس \mathbf{D} ، اندازه دستگاه معادلات فوق را کوچک کرد. لذا رابطه (۴) به رابطه (۵) خلاصه خواهد شد.

$$\mathbf{D}\underline{b}(y) = m \Rightarrow \quad (۴)$$

$$\mathbf{D}\underline{v} = m - \mathbf{D}\underline{b}(x); \quad \underline{v} = \underline{b}(y) - \underline{b}(x)$$

$$\mathbf{H}\underline{v} = \underline{s} \quad (۵)$$

که در آن، \mathbf{H} ماتریسی $m \times k$ و \underline{v} برداری با k عنصر است. در نتیجه، فرستنده باید این دستگاه معادلات با m معادله و k مجهول را حل کند. مشاهده می‌شود که این مسئله معادل کد برداری یک کد خطی $\mathcal{C}(k, k-m)$ با ماتریس توازن آزمایی^۳ \mathbf{H} است. یک روش عملی برای کمینه‌کردن اعوجاج جمع‌شونده در روش کدینگ کاغذ خیس استفاده از STC است [۳۶]. هدف این روش، یافتن بهترین نحوه درج برای کمینه‌کردن اعوجاج جمع‌شونده ناشی از درج است. در این روش، تصویر پوشش، هزینه تغییر هر پیکسل و پیام مورد نظر به عنوان ورودی دریافت می‌شود. با توجه به ساختار کدینگ کاغذ خیس، پیام‌ها در نقش

پیش‌نیازها و تعدادی از مرتبط‌ترین کارهای پیشین به همراه داگان آزمون و روش تحقیق گزارش شده در این مقاله شرح داده شده است. پس از معرفی مختصر مدل‌های گرافیکی موردنظر در بخش سوم، بخش چهارم به مدل‌سازی نهان‌کاو توسط مدل موضوعی LDA^۱ و ارائه معیاری از قابلیت کشف آماری براساس این مدل‌سازی اختصاص داده شده است که با توجه به این معیار، تعریفی از ظرفیت بیان شده است و رابطه آن با هزینه تغییر پیکسل بررسی شده است. همچنین، یک الگوریتم نهان‌نگاری مناسب براساس کمینه‌کردن قابلیت کشف آماری ارائه شده و عملکرد آن با الگوریتم‌های موجود مقایسه شده است. در بخش پنجم، از مجموعه ابزار تحلیلی به دست آمده در بخش چهارم، معیاری برای هزینه درج در تصویر ارائه و رابطه آن با نرخ درج و PSNR بررسی شده است. همچنین، رابطه ظرفیت نهان‌نگاری با ابعاد تصویر برای الگوریتم پیشنهادی بیان شده است. بخش ششم به نتیجه‌گیری و ارائه پیشنهادهایی برای ادامه کار اختصاص دارد.

۲- روش تحقیق

مبنای روش نهان‌نگاری در این مقاله، روش MG است که از اولین الگوریتم‌های نهان‌نگاری مبتنی بر محتوای سیگنال پوشش محسوب می‌شود. در این روش، از $D_{KL}(P \| Q)$ ، یعنی تابع دیورژانس بین توابع چگالی پیکسل‌ها در تصویر پوشش و تصویر نهان‌نگاری شده به عنوان معیاری از قابلیت کشف آماری یاد شده است و قصد دارد که درج بهینه و هزینه تغییر پیکسل متناظر با آن‌ها را به نحوی بیابد که این معیار کمینه شود [۳۱]. در نتیجه، تابع اعوجاج ناشی از درج با (۱) بیان می‌شود:

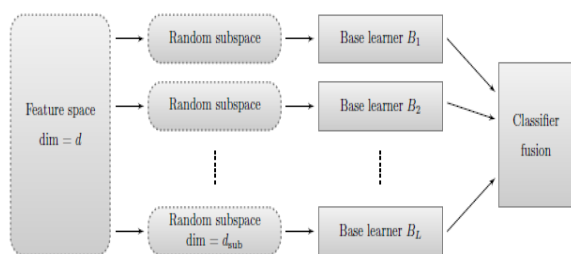
$$D = \sum_{i=1}^n D_{KL}(p^{(i)} \| q^{(i)}(\beta_i)) \quad (۱)$$

که در آن، $p^{(i)}$ و $q^{(i)}(\beta_i)$ به ترتیب نشان‌دهنده توزیع پیکسل i -ام تصویر پوشش و درج‌شده هستند و β_i نرخ درج در پیکسل i -ام است. با نوشتن بسط تیلور برای دیورژانس در (۱):

$$D = \sum_{i=1}^n \beta_i^2 I_i(0) / 2 \quad (۲)$$

که در آن، $I_i(0)$ نشان‌دهنده اطلاعات فیشر است. در [۴۱] نشان داده شده است که با مدل‌سازی پوشش می‌توان مقدار اطلاعات فیشر را محاسبه کرد. برای سادگی، توزیع پیکسل‌های پوشش را گوسی کوانتیزه شده و مستقل به صورت $Q_\Delta(N(0, v_i))$ در نظر گرفته می‌شود. در این‌جا فرض می‌شود از درج به صورت LSBM استفاده گردد که در [۴۲] نشان داده شده

داریم و ابعاد بردار ویژگی نیز بالا است، عملکردی مشابه SVM با پیچیدگی بسیار پایین‌تر از آن خواهد داشت. پیچیدگی بسیار پایین این روش، به نمان کاو این قابلیت را می‌دهد که در یک زمان متعارف از ویژگی‌های آماری با ابعاد بالا و مجموعه تصاویر آموزش زیادتری استفاده کند و در نتیجه بتواند سامانه‌های نمان‌نگاری مدرن را بهتر شناسایی کند. طبقه‌بند مرکب از چندین طبقه‌بند پایه برای آموزش تشکیل شده است. هر کدام از این طبقه‌بندها روی یک زیرفضای تصادفی از فضای ویژگی، آموزش می‌بینند. همان‌گونه که در شکل (۱) مشاهده می‌شود، تصمیم‌نهایی در مرحله آزمون براساس مجموع تصمیم‌های طبقه‌بندهای پایه اعلام می‌شود. در دو بخش بعد به مقدمه‌ای از مدل‌های موضوعی و روش به‌کاررفته پرداخته‌ایم.



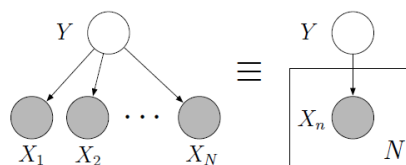
شکل (۱): ساختار طبقه‌بند مرکب

۳- مدل‌های گرافیکی

برای نمایش توزیع احتمال مدل‌های موضوعی، از ساختاری به نام مدل گرافیکی استفاده می‌شود. این مدل به‌صورت یک گراف جهت‌دار تعریف می‌شود که در آن گره‌ها متغیرهای تصادفی و یال‌ها وابستگی‌های احتمالی بین متغیرها را نشان می‌دهند. در این مدل، گره‌های خاکستری نشان‌دهنده متغیرهای مشاهده شده و مستطیل‌ها نشان‌دهنده یک ساختار تکرارشونده هستند. شکل (۲) ساختار یک مدل گرافیکی ساده را نشان می‌دهد که بیان‌گر مدل بی‌ز ساده‌انگارانه و تابع چگالی احتمال

$$p(y, x_1, \dots, x_N) = p(y) \prod_{i=1}^N p(x_i | y)$$

است.



شکل (۲): مدل گرافیکی بی‌ز ساده‌انگارانه (Naive Bayes)

در شکل (۳) مدل گرافیکی مربوط به مدل موضوعی LDA نشان داده شده است. این مدل به‌دلیل شباهتش به مسئله مورد نظر ما در این مقاله مبنای پژوهش قرار گرفته است [۴۵]. در این شکل z یک موضوع، w یک سند و w_i ها کلمات موجود در این

سندرم یک کد پیچشی^۱ ظاهر می‌شوند و درگیرنده، بدون به اشتراک‌گذاری کانال قابل استخراج هستند. در نتیجه، مسئله بهینه‌سازی در نظر گرفته‌شده در STC به‌صورت رابطه (۶) است.

$$\min_{\underline{y}} \sum_{i=1}^n \rho_i(x, y_i), \quad y_i \in \{0, 1\} \quad (6)$$

$$s.t. \quad \underline{H} \underline{y} = m$$

الگوریتم‌های Hugo [۳۵]، S-UNIWARD [۳۰] و چند الگوریتم دیگر نیز از طی این مسیر با ملاک‌های دیگری به‌جای دیورژانس به‌دست آمده‌اند. در [۴۶] ملاک بهینه‌سازی برای اولین بار از دید نمان کاو مطرح شده است. در این روش، ملاک بهینه تشخیص نمان‌نگاری به‌عنوان ملاک بهینه‌سازی نمان‌نگاری به‌کار رفته است. در این مقاله ما این مهم را با مدل‌سازی نمان کاو با مدل‌سازی رفتار آن به کمک مدل‌های گرافیکی انجام داده‌ایم. مزیت این روش آن است که از روی نتیجه اعمال یک نمان کاو روی یک مجموعه داده می‌توان مدلی از رفتار آن به‌دست آورد و با پیچیده‌کردن مدل گرافیکی جنبه‌های بیشتری از نمان کاو را مدل کرد و ملاک‌هایی برای ارزیابی نمان کاوی و نمان‌نگاری ایجاد نمود. لازم به ذکر است که گونه‌های دیگری از نمان‌نگاری تطبیقی با استفاده از گراف معرفی شده است (مثلاً در [۴۷]) که به موضوع مورد بحث ما ارتباط خاصی ندارد و بدون توجه به نمان کاو مورد استفاده قرار می‌گیرد.

پس از معرفی روش‌های نمان کاوی به‌صورت طبقه‌بندی نظارت‌شده، بردار ویژگی‌های مختلفی از روی ویژگی‌های آماری تصویر استخراج شدند. در این مقاله از بردار ویژگی‌های ۱۲۷۵۳ بعدی SRMQ1 استفاده شده است [۳۸]. این بردار ویژگی، وابستگی بین باقی‌مانده‌های نویزی که با استفاده از فیلترهای بالاگذر خطی و غیرخطی گوناگون ایجاد می‌شوند را استخراج می‌کند. در این مقاله از مجموعه تصاویر Corel استفاده شده است [۴۳]. این مجموعه تصاویر شامل ۸۱۸۵ تصویر فشرده‌نشده با ابعاد ۵۱۲×۵۱۲ است که دارای تصاویری از موضوعات مختلف مانند مناظر طبیعی، اشخاص، حیوانات، اشیاء، ساختمان‌ها، آثار هنری و غیره است.

این مجموعه تصاویر قبلاً در نمان‌نگاری مانند [۴۴] استفاده شده است. این تصاویر را به تصاویر خاکستری ۸-بیتی تبدیل نموده و با فرمت (tif) ذخیره کرده‌ایم. به‌دلیل پیچیدگی بالای SVM^۲ برای بردارهای ویژگی با ابعاد بالا، در این مقاله از طبقه‌بند مرکب استفاده می‌شود [۴۸]. این روش برای مسائلی که تعداد زیادی زوج تصویر پوشش و درج‌شده در مجموعه آموزش

نهان‌نگاری براساس فریب مدل نهان‌کاو و آزمون آن روی یک دادگان شناخته‌شده بررسی شده است.

در بین مدل‌های موضوعی موجود، LDA عملکرد بهتری در طبقه‌بندی داده‌ها دارد. همچنین، بسیاری از مدل‌های موضوعی جدیدتر بر پایه LDA طراحی شده‌اند. به‌علاوه، این ساختار برای ارتباط‌دادن هزینه تغییر پیکسل به ظرفیت نهان‌نگاری و قابلیت کشف آماری مناسب است. بر این اساس، فرض می‌شود که نهان‌کاو از این مدل برای نهان‌کاوی تصاویر استفاده می‌کند.

در این ساختار فرض می‌شود هر تصویر یک سند باشد که از تعدادی پیکسل به‌عنوان کلمات تشکیل شده است. همچنین دو موضوع وجود دارد که به ترتیب پاک (C) و درج‌شده (S) نام دارند. با توجه به مدل گرافیکی LDA، با دریافت یک تصویر، توزیع هر موضوع در این تصویر از رابطه (۸) به‌دست می‌آید. در عمل، پارامترهای مدل به‌گونه‌ای تعیین می‌شود که این مدل بتواند به‌خوبی مجموعه اسناد دریافتی را توصیف کند [۴۵].

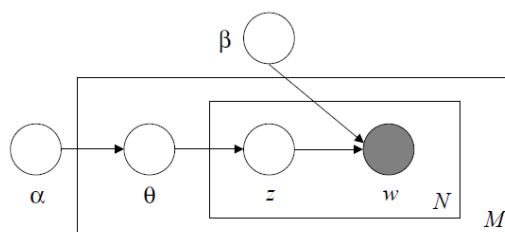
$$P(\theta_1, \theta_2 | \mathbf{X}, Model) = \frac{P(\theta_1, \theta_2, \mathbf{X} | Model)}{P(\mathbf{X} | Model)} = \frac{P(\theta | \alpha_{Model}) \prod_{i=1}^n \sum_{z_i \in Z} P(z_i | \theta) P(x_i | z_i, \beta_{Model})}{\int_{\theta} P(\theta | \alpha_{Model}) \prod_{i=1}^n \sum_{z_i \in Z} P(z_i | \theta) P(x_i | z_i, \beta_{Model}) d\theta} \quad (\lambda)$$

$$= \frac{\theta_1^{\alpha_1-1} \theta_2^{\alpha_2-1} \prod_{i=1}^n \{\theta_1 P(x_i | Clean) + \theta_2 P(x_i | Steg)\}}{\int_{\theta} \theta_1^{\alpha_1-1} \theta_2^{\alpha_2-1} \prod_{i=1}^n \{\theta_1 P(x_i | Clean) + \theta_2 P(x_i | Steg)\} d\theta}$$

در (۸) منظور از مدل، پارامترهایی هستند که طی فرآیند آموزش محاسبه می‌شوند. همچنین، \mathbf{X} در این نمایش، نشان‌دهنده یک سند با تعداد کلمات n است.

برای ایجاد ارتباط بین پارامترهای مدل و اثر نهان‌نگاری، تصویر $\mathbf{X} = (x_1, \dots, x_n)$ با توزیع هر یک از پیکسل‌ها به‌صورت $x_i \sim N(0, \sigma_i^2)$ و مستقل از هم مدل می‌شوند. همچنین، در نهان‌نگاری از درج به‌صورت LSBM استفاده می‌شود. در [۴۲] نشان داده شده است که تشخیص روش‌های نهان‌نگاری مبتنی بر LSBM نسبت به جایگذاری LSB دشوارتر است. به همین دلیل، در نهان‌نگاری، LSBM نسبت به جایگذاری LSB ترجیح داده شده است [۳۱]. اگر احتمال ± 1 شدن برابر $\beta/2$ باشد، تابع چگالی احتمال پیکسل‌های تصویر نهان‌نگاری شده به‌صورت (۹) بیان می‌شود.

سند هستند. مدل LDA توانسته است با تعریف وزن هر موضوع در سند به‌صورت یک متغیر تصادفی، این مشکلات را حل نماید. براساس این مدل، هر سند w بدین‌صورت تولید می‌شود که ابتدا سهم هر موضوع در سند از توزیع $\theta \sim Dir(\alpha)$ مشخص می‌شود. سپس به ازای هر کلمه w_n از این سند، یک موضوع z_n با توزیع $z_n \sim Multinomial(\theta)$ انتخاب شده و سپس کلمه w_n با توزیع $p(w_n | z_n, \beta)$ تولید می‌شود. توزیع احتمال مشترک بردارهای θ ، z و w در رابطه (۷) نشان داده شده است.



شکل (۳): مدل موضوعی LDA

$$p(\theta, \mathbf{z}, \mathbf{w} | \alpha, \beta) = p(\theta | \alpha) \prod_{n=1}^N p(z_n | \theta) p(w_n | z_n, \beta) \quad (7)$$

که در آن، θ مخلوطی از موضوعات است که سهم هر موضوع در سند را مشخص می‌کند، w برداری از N کلمه موجود در سند و z برداری از موضوعات متناظر با هر کلمه در سند است. مقادیر α, β پارامترهای مربوط به مدل هستند که در روند آموزش محاسبه می‌شوند. در صورتی که k موضوع داشته باشیم، توزیع $p(\theta | \alpha)$ به‌صورت دیریکله k -بعدی مطابق رابطه (۸) است.

$$p(\theta | \alpha) = \frac{\Gamma(\sum_{i=1}^k \alpha_i)}{\prod_{i=1}^k \Gamma(\alpha_i)} \theta_1^{\alpha_1-1} \dots \theta_k^{\alpha_k-1} \quad (\lambda)$$

توزیع احتمال حاشیه‌ای هر سند را می‌توان با جمع و انتگرال‌گیری روی θ و z به‌دست آورد. در نتیجه خواهیم داشت:

$$p(\mathbf{w} | \alpha, \beta) = \int p(\theta | \alpha) \left(\prod_{n=1}^N \sum_{z_n} p(z_n | \theta) p(w_n | z_n, \beta) \right) d\theta$$

۴- مدل‌سازی نهان‌کاو

در این بخش با مدل‌سازی گرافیکی نهان‌کاو، احتمال خطای نهان‌کاو به‌عنوان معیاری از قابلیت کشف آماری بیان و محاسبه می‌شود. براساس این معیار، تعریف جدیدی از ظرفیت ارائه و رابطه آن را با هزینه تغییر پیکسل بررسی کرده‌ایم. رابطه هزینه تغییر پیکسل و قابلیت کشف آماری، با ارائه یک الگوریتم

خطاهای P_{MD} و P_{FA} را از صفر تا یک جابه‌جا می‌کند. همچنین، در روند آموزش LDA، از توزیع دیریکله متقارن ($\alpha_1 = \dots = \alpha_k$) استفاده می‌شود. لذا بدون اعمال نظر خاص، ما نیز مقادیر α_1 و α_2 را برابر در نظر می‌گیریم.

در این قسمت قصد داریم با فرض استفاده از نهان‌کاو قسمت قبل، میزان درج بهینه در هر پیکسل تصویر را برای سطح درج α بیت بر پیکسل بیابیم. به عبارتی، باید از دید نهان‌نگار به گونه‌ای در تصویر درج شود که احتمال لورفتن تصویر درج‌شده کمینه شود. لذا با مسئله بهینه‌سازی (۱۳) روبرو هستیم.

$$\begin{cases} \max_{\beta} E_{\mathbf{X}|\text{Steg}}[P(\theta_1 > 0.5)] \\ \text{s.t. } \frac{1}{n} \sum_{i=1}^n h(\beta_i) = \alpha \end{cases} \quad (13)$$

که در آن، $P(\theta_1 > 0.5)$ عبارت است از:

$$P(\theta_1 > 0.5) = \int_{0.5}^1 f_{\theta_1} d\theta_1 = \frac{\int_{0.5}^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} \prod_{i=1}^n \{1 - \beta_i (1-\theta_1) (1 - e^{-\frac{1}{2\sigma_i^2} \cosh(\frac{x_i}{\sigma_i^2})})\} d\theta_1}{\int_0^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} \prod_{i=1}^n \{1 - \beta_i (1-\theta_1) (1 - e^{-\frac{1}{2\sigma_i^2} \cosh(\frac{x_i}{\sigma_i^2})})\} d\theta_1}$$

در این جا با استفاده از تقریب‌های ساده‌کننده، تخمینی از تابع هدف به دست آورده و با استفاده از آن به بررسی ظرفیت نهان‌نگاری و همچنین ارائه یک الگوریتم نهان‌نگاری می‌پردازیم.

در اولین تقریب، با توجه به کوچک بودن مقادیر β_i ها، از جملات حاصل ضرب آن‌ها در رابطه تابع هدف صرف نظر می‌شود. در نتیجه خواهیم داشت:

$$P(\theta_1 > 0.5) = (a - bY) / (a' - b'Y)$$

$$, Y = \sum_{i=1}^n \beta_i (1 - e^{-\frac{1}{2\sigma_i^2} \cosh(\frac{x_i}{\sigma_i^2})}) \quad \text{که در آن،}$$

$$, a' = \int_0^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} d\theta_1, \quad a = \int_{0.5}^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} d\theta_1$$

$$, b' = \int_0^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2} d\theta_1 \quad \text{و} \quad b = \int_{0.5}^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2} d\theta_1$$

با محاسبه این انتگرال‌ها، رابطه (۱۳) به صورت (۱۴) ساده می‌شود:

$$P(\theta_1 > 0.5) = (1 - \frac{b}{a} Y) / (2 - Y) \quad (14)$$

$$f_{\beta}(x_i, \sigma_i^2) = \frac{\beta}{2} f(x_i, -1, \sigma_i^2) \pm (9)$$

$$+ (1-\beta) f(x_i, 0, \sigma_i^2) + \frac{\beta}{2} f(x_i, 1, \sigma_i^2)$$

که در آن، $f(x_i, \mu_i, \sigma_i^2)$ تابع چگالی گوسی با میانگین μ_i و واریانس σ_i^2 است. با استفاده از فرضیات فوق، رابطه استنتاج (۸) به صورت (۱۰) درمی‌آید.

$$P(\theta_1, \theta_2 | \mathbf{X}, Model) = \frac{\theta_1^{\alpha_1-1} \theta_2^{\alpha_2-1} \prod_{i=1}^n \{\theta_1 f(x_i, 0, \sigma_i^2) + \theta_2 f_{\beta_i}(x_i, \sigma_i^2)\}}{\int_0^1 \theta_1^{\alpha_1-1} \theta_2^{\alpha_2-1} \prod_{i=1}^n \{\theta_1 f(x_i, 0, \sigma_i^2) + \theta_2 f_{\beta_i}(x_i, \sigma_i^2)\} d\theta} \quad (10)$$

از آن جایی که دو موضوع وجود دارد، θ_i ها ($i = 1, 2$) روی خط $\theta_1 + \theta_2 = 1$ در ناحیه اول مختصات قرار می‌گیرند. لذا با جایگذاری $\theta_2 = 1 - \theta_1$ در رابطه و اندکی ساده‌سازی به توزیعی بر حسب θ_1 می‌رسیم که آن را f_{θ_1} می‌نامیم.

$$f_{\theta_1} = P(\theta_1, \theta_2 | \mathbf{X}, Model) = \frac{\theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} \prod_{i=1}^n \{1 - \beta_i (1-\theta_1) (1 - e^{-\frac{1}{2\sigma_i^2} \cosh(\frac{x_i}{\sigma_i^2})})\}}{\int_0^1 \theta_1^{\alpha_1-1} (1-\theta_1)^{\alpha_2-1} \prod_{i=1}^n \{1 - \beta_i (1-\theta_1) (1 - e^{-\frac{1}{2\sigma_i^2} \cosh(\frac{x_i}{\sigma_i^2})})\} d\theta_1}$$

برای تصمیم‌گیری در مورد یک تصویر، آن تصویر را به موضوعی که بیشترین احتمال را دارد، نسبت می‌دهیم. لذا قاعده تصمیم‌گیری به صورت (۱۱) قابل بیان است.

$$D = \begin{cases} \theta_1 > 0.5 \Rightarrow \text{Clean} \\ \theta_1 < 0.5 \Rightarrow \text{Steg} \\ \theta_1 = 0.5 \Rightarrow \text{Clean or Steg} \end{cases} \quad (11)$$

بر این اساس، میانگین احتمال خطای نهان‌کاو به صورت (۱۲) محاسبه می‌شود.

$$P_E = \frac{1}{2} (P_{MD} + P_{FA}) \quad (12)$$

$$= \frac{1}{2} (E_{\mathbf{X}|\text{Steg}}[P(\theta_1 > 0.5)] + E_{\mathbf{X}|\text{Clean}}[P(\theta_1 < 0.5)])$$

که در آن، P_{MD} و P_{FA} به ترتیب احتمال عدم کشف تصویر درج‌شده و احتمال تشخیص تصویر پاک به عنوان تصویر درج‌شده هستند. همچنین، توزیع تصاویر پاک و درج‌شده برای میانگین‌گیری نیز مشابه قسمت قبل، به ترتیب توزیع گوسی و گوسی مخلوط^۱ برای هر پیکسل فرض شده است. عدم تقارن پارامترهای دیریکله α_1 و α_2 که طی روند آموزش محاسبه می‌شوند، احتمال

برای این منظور از روش بهینه‌سازی لاگرانژ^۳ استفاده می‌شود. با تشکیل لاگرانژین و مشتق‌گرفتن نسبت به β_i ها می‌توان نوشت:

$$L = \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right) - \frac{1}{\lambda} \left(\sum_{i=1}^n h_3(\beta_i) - n\alpha \right) \quad (۱۸)$$

$$\frac{\partial}{\partial \beta_i} \rightarrow \frac{2}{\beta_i} \ln\left(\frac{2}{\beta_i} - 2\right) = 4\lambda \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right), \quad i = 1, \dots, n$$

حل هریک از معادلات (۱۸)، معادل حل معادله $x \ln(x-2) = 4\lambda (\cosh(1/\sigma_i^2) - 1)$ است که در آن، برای حل سریع این معادله برای همه پیکسل‌ها، مقادیر تابع معکوس $y = x \ln(x-2)$ با محاسبه تابع در فواصل کوچک در یک جدول ذخیره می‌شود. برای داشتن نقطه کمینه باید مشتق دوم تابع هدف نسبت به β_i مثبت باشد؛ در نتیجه، باید $\lambda > 0$ باشد. مقدار λ نیز از شرط مسئله محاسبه می‌شود. از طرفی، بین احتمال تغییر پیکسل و هزینه تغییر پیکسل برای کمینه‌کردن اعوجاج جمع‌پذیر رابطه $\beta_i = 1 / (1 + \exp(k\rho_i))$ با استفاده از این رابطه، می‌توان هزینه تغییر پیکسل را برحسب β_i های محاسبه‌شده در قسمت قبل به‌دست آورد. در ادامه، ρ_i ها به بزرگ‌ترین مقدار آن‌ها نرمالیزه می‌شود:

$$\rho_i = \ln(1/\beta_i - 1) \quad (۱۹)$$

لازم به ذکر است که برای جلوگیری از جهش روشنایی پیکسل، هزینه افزودن +1 برای پیکسل‌های با روشنایی ۲۵۵ و افزودن -1 برای پیکسل‌های با روشنایی صفر برابر با بیشترین هزینه منظور می‌شود.

در نهایت، می‌توان با استفاده از نسخه سه-سطحی STC [۳۶]، با پروفایل هزینه تعریف‌شده در رابطه (۱۹) برای درج در تصاویر استفاده کرد. واریانس هر پیکسل به‌صورت واریانس نمونه‌ای در یک همسایگی کوچک (مثلاً یک بلوک 3×3) از آن پیکسل محاسبه می‌شود. همچنین، به‌دلیل پایداری عددی، بیشینه واریانس هر پیکسل و ۱ به‌عنوان واریانس آن پیکسل در نظر گرفته می‌شود.

۵- نتایج و بحث

این بخش به بررسی رفتار الگوریتم پیشنهادی از نظر درج در نواحی مختلف تصویر و ارتباط آن با توزیع روشنایی در تصویر اختصاص دارد. سپس، عملکرد الگوریتم با بهترین الگوریتم‌های موجود مقایسه می‌شود.

در تقریب دوم، از آنجایی که X_i ها مستقل هستند، با استفاده از قضیه حد مرکزی^۱ $E_{X|Steg} [P(\theta_1 > 0.5)]$ می‌توان نوشت:

$$E_{X|Steg} [P(\theta_1 > 0.5)] = E_{Y|Steg} [(1 - bY/a) / (2 - Y)]$$

که در آن، متغیر تصادفی Y دارای توزیع گوسی به‌صورت $Y \sim N(\mu_Y, \sigma_Y^2)$ است. با اندکی محاسبه، میانگین و واریانس Y قابل محاسبه است:

$$\mu_Y = \sum_{i=1}^n \mu_i(\beta_i) = - \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right) \quad (۱۵)$$

$$\sigma_Y^2 = \sum_{i=1}^n v_i^2(\beta_i) = - \sum_{i=1}^n \left\{ \beta_i^4 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right)^2 + \sum_{i=1}^n \left\{ \frac{1}{4} \beta_i^2 e^{-\frac{1}{\sigma_i^2}} \left(e^{\frac{1}{\sigma_i^2}} - 1 \right)^2 \left(2 + \beta_i \left(e^{\frac{1}{\sigma_i^2}} - 1 \right) \left(e^{\frac{1}{\sigma_i^2}} + 3 \right) \right) \right\} \right\}$$

طبق رابطه (۱۵)، $\sigma_Y^2 = O(\beta^2)$ است. لذا در حالتی که $\beta \rightarrow 0$ توزیع Y به سمت تابع ضربه^۲ میل می‌کند؛ یعنی $f_Y(y) = \delta(y - \mu_Y)$ است. با این فرض، رابطه تابع هدف به‌صورت رابطه (۱۶) ساده می‌شود.

$$E_{Y|Steg} \left[\frac{1 - \frac{b}{a} Y}{2 - Y} \right] = \frac{1 - \frac{b}{a} \mu_Y}{2 - \mu_Y}$$

$$= \frac{1 + \frac{b}{a} \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right)}{2 + \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right)} \quad (۱۶)$$

طبق رابطه (۱۶)، تابع هدف به‌ازای مقادیر مختلف پارامتر دیریکله، تابعی نزولی از $\sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right)$ است. در نتیجه، دو مسئله بهینه‌سازی P_1 و P_2 در رابطه (۱۷) با هم معادل هستند:

$$P_1 : \begin{cases} \max_{\beta} E_{X|Steg} [P(\theta_1 > 0.5)] \\ s.t. \quad \frac{1}{n} \sum_{i=1}^n h_3(\beta_i) = \alpha \end{cases} \quad (۱۷)$$

$$P_2 : \begin{cases} \min_{\beta} \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i^2}\right) - 1 \right) \\ s.t. \quad \frac{1}{n} \sum_{i=1}^n h_3(\beta_i) = \alpha \end{cases}$$

برای حل مسئله بهینه‌سازی دوم، رابطه (۱۷) مناسب‌تر است.

۱-۵- احتمال تغییر پیکسل

در الگوریتم پیشنهادی، هزینه تغییر پیکسل به ویژگی‌های تصویر وابسته است. تصویر ارائه شده در شکل (۴- الف) دارای تنوعی مناسب از نظر قسمت‌های نویزی و هموار است و در [۲۹] نیز به کار رفته است. در شکل (۴)، احتمال تغییر پیکسل برای الگوریتم‌های مختلف نشان داده شده است. همان‌گونه که مشاهده می‌شود، الگوریتم پیشنهادی ما نیز یک الگوریتم وفقی محتوامحور است. به عبارتی، احتمال تغییر پیکسل در قسمت‌های نویزی و لبه‌ها بیشتر از قسمت‌های هموار تصویر است. همچنین، با توجه به شباهت رفتار الگوریتم پیشنهادی به MG، انتظار می‌رود کارایی این دو الگوریتم نیز مشابه هم باشند.



الف) تصویر پوشش



ج) S-UNIWARD



ب) HUGO



د) الگوریتم این مقاله LDA-G

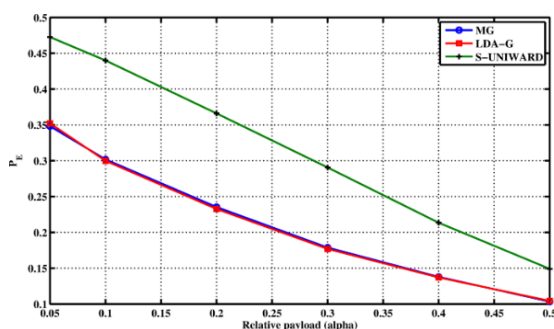


ج) MG

شکل (۴): مقایسه احتمال تغییر پیکسل برای الگوریتم‌های نهان‌نگاری مختلف. مقادیر احتمال درج در بازه $[0, 1/3]$ هستند و تیره‌ترین نقاط مشخص‌کننده احتمال درج $1/3$ هستند و روشن‌ترین نقاط احتمال درج صفر را نشان می‌دهند.

۲-۵- نهان‌کاوی

در این مقاله به منظور بررسی عملکرد الگوریتم پیشنهادی در نرخ‌های درج مختلف، از روش نهان‌کاوی ذکر شده در [۴۸] استفاده شده است. تصاویر پوشش استفاده شده از مجموعه تصاویر Corel انتخاب شده‌اند [۴۳]. این مجموعه تصاویر شامل ۸۱۸۵ تصویر فشرده نشده با ابعاد 512×512 است. تصاویر انتخاب شده توسط بردار ویژگی‌های 12753 بعدی SRM با $q=1$ توصیف می‌شوند [۳۸]. در نهایت، عملکرد نهان‌کاوی بر اساس میانگین احتمال خطای نهان‌کاوی به صورت $P_E = \min_{p_{FA}} (p_{MD} + p_{FA}) / 2$ سنجیده می‌شود. احتمال خطای ذکر شده در شکل (۵)، میانگین ۱۰ بار اجرای الگوریتم نهان‌کاوی [۴۸] با تنظیمات پیش فرض است. همان‌طور که در [۳۱] نشان داده شده است، MG عملکرد بهتری نسبت به HUGO دارد. در این بررسی، عملکرد الگوریتم پیشنهادی را نسبت به بهترین الگوریتم‌های موجود می‌سنجیم. همان‌گونه که انتظار می‌رفت، عملکرد الگوریتم پیشنهادی، مشابه MG است. مشاهده می‌شود که همچنان عملکرد الگوریتم S-UNIWARD بهتر از سایر الگوریتم‌ها است. البته باید توجه کرد که ساختار تابع اعوجاج استفاده شده در S-UNIWARD پیچیده‌تر است و رابطه بین پیکسل‌های مجاور را در نظر می‌گیرد؛ در حالی که در الگوریتم پیشنهادی، پیکسل‌های پوشش مستقل از هم فرض شده‌اند. در نتیجه، استفاده از مدل‌های پیچیده‌تری برای توصیف تصویر پوشش، مانند توزیع گوسی توأم^۱ یا استفاده از زنجیره مارکوف^۲ (که همبستگی بین پیکسل‌های مجاور را نیز در نظر می‌گیرند) می‌تواند به تولید الگوریتم‌های نهان‌نگاری بهتر بینجامد.



شکل (۵): میانگین احتمال خطای نهان‌کاوی P_E بر حسب نرخ درج α برای الگوریتم‌های مختلف. نمودارهای مربوط به MG و LDA-G تقریباً منطبق شده‌اند.

۳-۵- بررسی ویژگی‌های دیداری الگوریتم

پیشنهادی

در این قسمت، قصد داریم افت کیفیت تصویر و تغییرات آماری

1- Jointly Gaussian

2- Markov Chain

$$C(\varepsilon) = \{Sup(\alpha) : 1 - h(\overline{p_E}(\alpha)) \leq \varepsilon\} \quad (21)$$

که در آن، $h(x)$ نشان‌دهنده آنتروپی باینری است و به صورت $h(x) = -x \ln(x) - (1-x) \ln(1-x)$ تعریف می‌شود. احتمال خطای نهان‌کاو عددی در بازه $0 \leq \overline{P_E} \leq 0.5$ است. نهان‌کاو در صورت دریافت تصاویر با درج صفر، به صورتی کاملاً تصادفی تصمیم می‌گیرد و $\overline{P_E}$ در این حالت به مقدار بیشینه خود یعنی 0.5 می‌رسد. آنتروپی باینری در بازه $(0, 0.5)$ تابعی یک‌به‌یک از $\overline{P_E}$ است. در نتیجه، دو تعریف (۲۱) و (۲۲) از ظرفیت، معادل یکدیگرند. در رابطه (۲۲)، $\varepsilon_1 = 0.5 - h^{-1}(1 - \varepsilon)$ است.

$$C(\varepsilon_1) = \{Sup(\alpha) : 1/2 - \overline{p_E}(\alpha) \leq \varepsilon_1\} \quad (22)$$

رابطه ظرفیت نهان‌نگاری با ویژگی‌های تصویر پوشش و الگوریتم درج را می‌توان از این تعریف استخراج نمود. با توجه به رابطه (۲۲) و روش پیشنهادی این مقاله، ظرفیت نهان‌نگاری به صورت رابطه (۲۳) محاسبه می‌شود. این رابطه نشان می‌دهد که مقدار داده امن به پراکندگی تصویر پوشش، اندازه تصویر و الگوریتم درج وابسته است. همچنین، در دو حالت حدی $\beta \rightarrow 0$ و $\sigma^2 \rightarrow \infty$ ابهام نهان‌کاو بیشینه است و این به معنی امنیت کامل است. این دو حالت به ترتیب نشان‌دهنده تصویر بدون درج و تصویر بسیار نویزی هستند.

$$1/2 - \overline{p_E}(\alpha) \leq \varepsilon_1 \Rightarrow$$

$$1/2 - \left(\frac{1 - \frac{b}{a} \mu_Y}{2 - \mu_Y} + \frac{1}{2} \right) / 2 \leq \varepsilon_1 \quad (23)$$

$$\Rightarrow \sum_{i=1}^n \beta_i^2 \left(\cosh\left(\frac{1}{\sigma_i}\right) - 1 \right) \leq \varepsilon_2$$

که در آن، $\varepsilon_2 = 8\varepsilon_1 / (1 - 2b/a - 4\varepsilon_1)$ است. همچنین، از آن جایی که رابطه با فرض سه-سطحی بودن درج به دست آمده

$$\text{است، شرط } \sum_{i=1}^n h_3(\beta_i) = n\alpha \text{ نیز باید برقرار باشد. از این جا}$$

می‌توان قضیه ریشه دوم ظرفیت نهان‌نگاری را نتیجه گرفت که به آن اشاره نمی‌کنیم. این نتیجه مشابه نتیجه‌ای است که تحت عنوان قانون ریشه دوم برای ظرفیت نهان‌نگاری براساس تعریف کاپچین [۴] مطرح شده است [۱۰]. طبق این قضیه، میزان کل داده امن برابر $m(n) = n\alpha = O(\sqrt{n} \ln(n))$ است؛ بنابراین، با افزایش ابعاد تصویر، نمی‌توان با نرخ قبل در تصویر درج کرد.

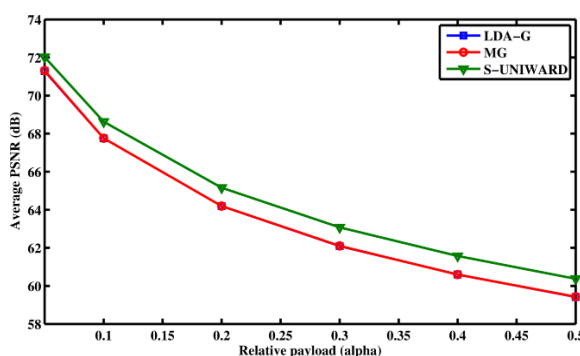
۵-۵- هزینه درج در تصویر

در بخش ۴ دیدیم که احتمال خطای نهان‌کاو، برحسب تابعی از واریانس و میزان درج در پیکسل‌های تصویر تغییر می‌کند. در رابطه (۲۴)، هزینه درج در تصویر به گونه‌ای تعریف شده است که هرچه مقدار این تابع کمتر باشد، ابهام نهان‌کاو افزایش می‌یابد.

آن را در اثر درج توسط الگوریتم پیشنهادی بررسی کنیم. نسبت مقدار بیشینه سیگنال به نویز، PSNR نامیده می‌شود که بیان‌کننده افت کیفیت ناشی از درج در تصویر است؛ این ملاک برای تصویر پوشش IC و تصویر درج‌شده IS بدین صورت تعریف می‌شود [۴۹].

$$PSNR(IS, IC) = 10 \{ \log_{10} [Max P^2] - \log_{10} \left[\frac{1}{n} \sum_{i=1}^n (IS(i) - IC(i))^2 \right] \} \quad (20)$$

که در آن، $Max P$ بیشینه روشنایی پیکسل‌ها است که برای تصاویر خاکستری ۸-بیتی برابر ۲۵۵ است. در شکل (۶)، رابطه میانگین PSNR و درج نسبی α برای الگوریتم‌های مختلف نشان داده شده است. این میانگین روی ۱۰۰ تصویر گرفته شده است.



شکل (۶): میانگین PSNR برحسب نرخ درج برای روش‌های مختلف. نمودارهای LDA-G و MG تقریباً منطبق شده‌اند.

همان‌گونه که مشاهده می‌شود، برای همه الگوریتم‌های بررسی‌شده، کیفیت تصاویر پس از درج به روش پیشنهادی افت زیادی نخواهد کرد. همچنین، عملکرد الگوریتم پیشنهادی از نظر PSNR، مشابه الگوریتم MG و اندکی ضعیف‌تر از الگوریتم S-UNIWARD است.

۵-۴- ظرفیت نهان‌نگاری

همان‌گونه که در شکل (۵) مشاهده می‌شود، احتمال خطای نهان‌کاو $\overline{P_E}$ تابعی نزولی از نرخ درج نسبی α است. در صورتی که سطح مشخصی از کشف‌پذیری قابل تحمل باشد تا جایی می‌توان در یک تصویر درج کرد که ابهام نهان‌کاو در مورد درج از این سطح قابل تحمل کمتر نشود؛ مقدار داده قابل درج در این سطح آستانه را ظرفیت نهان‌نگاری می‌نامیم. ظرفیت نهان‌نگاری را به‌طور دقیق‌تر به این صورت تعریف می‌کنیم:

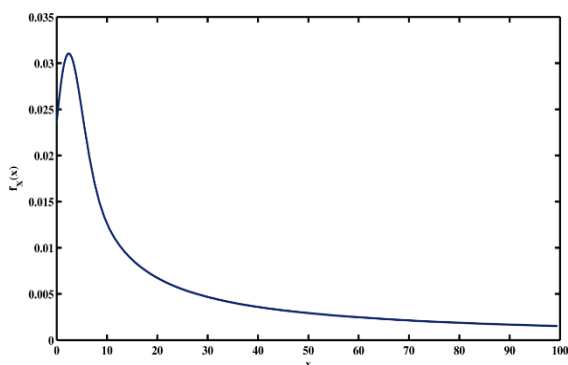
تعریف: یک سیستم نهان‌نگاری را ε -امن می‌نامیم هرگاه، فاصله ابهام نهان‌کاو از حالت بیشینه کمتر از ε باشد. بر این اساس، ظرفیت نهان‌نگاری برای هر الگوریتم درج به صورت (۲۱) تعریف می‌شود.

$$y = \frac{1}{2\lambda\beta} \ln\left(\frac{2}{\beta} - 2\right) = g(\beta) \quad (29)$$

از آن جایی که $g(x)$ تابعی اکیداً نزولی است، معادله $g(x) = cte$ تنها یک نقطه جواب دارد و می‌توان نوشت:

$$f_{\beta}(x) = |g'(x)| f_Y(g(x)) \quad ; 0 \leq x \leq 2/3 \quad (30)$$

توزیع واریانس پیکسل‌ها به صورت آماری محاسبه می‌شود. در شکل (۷)، تابع چگالی احتمال واریانس برای ۱۰۰ تصویر با ابعاد 512×512 ، به صورت تجربی رسم شده است.



شکل (۷): تابع چگالی احتمال تجربی واریانس پیکسل‌ها

حال با استفاده از توزیع تجربی واریانس و روابط فوق، رابطه هزینه درج در تصویر و نرخ درج را به دست می‌آوریم. همان‌گونه که در شکل (۸) مشاهده می‌شود، رابطه این دو متغیر به صورت تابعی دو ضابطه‌ای است. این رابطه با انطباق دو چندجمله‌ای بر شکل (۸) تخمین زده شده است.

$$IC_n(\alpha) = \begin{cases} 6.7 \times 10^{-1} \alpha^2 - 3 \times 10^{-2} \alpha + 6.1 \times 10^{-3} & ; \alpha < 0.45 \\ 8.6 \times 10^{-2} \alpha + 9 \times 10^{-2} & ; \alpha \geq 0.45 \end{cases}$$

به کمک این تقریب و تعریف ظرفیت در بخش قبل و تعریف ظرفیت در رابطه (۲۳)، می‌توان رابطه داده امن با ابعاد تصویر را به صورت به این صورت بررسی کرد:

$$IC(\alpha) \leq \varepsilon \Rightarrow \begin{cases} n(6.7 \times 10^{-1} \alpha^2 - 3 \times 10^{-2} \alpha + 6.1 \times 10^{-3}) \leq \varepsilon & ; \alpha < 0.45 \\ n(8.6 \times 10^{-2} \alpha + 9 \times 10^{-2}) \leq \varepsilon & ; \alpha \geq 0.45 \end{cases}$$

$$\Rightarrow \begin{cases} \alpha = O\left(\frac{1}{\sqrt{n}}\right) \rightarrow m(n) = O(\sqrt{n}) & ; \alpha < 0.45 \\ \alpha = O\left(\frac{1}{n}\right) \rightarrow m(n) = O(1) & ; \alpha \geq 0.45 \end{cases}$$

نتیجه این بررسی‌ها نشان می‌دهد که برای سطوح امنیت بالا (مربوط به نرخ‌های درج کمتر از 0.45 bpp)، میزان داده امن با ریشه دوم ابعاد تصویر رشد می‌کند. این ویژگی نتایج تحقیقات

$$IC = \sum_{i=1}^n \beta_i^2 (\cosh(1/\sigma_i^2) - 1) \quad (24)$$

برای مستقل شدن این تابع از الگوریتم درج، مقدار بهینه این تابع را برای الگوریتم پیشنهاد شده در بخش قبل، محاسبه می‌کنیم. بر این اساس، مقدار بهینه این تابع به ازای هر نرخ درج، تنها وابسته به واریانس پیکسل‌های تصویر است. با جایگذاری رابطه (۱۸) در رابطه (۲۴)، هزینه درج در تصویر به صورت رابطه (۲۵) محاسبه می‌شود.

$$IC = \frac{1}{2\lambda} \sum_{i=1}^n \beta_i \ln\left(\frac{2}{\beta_i} - 2\right) \quad (25)$$

با در نظر گرفتن یک توزیع آماری برای واریانس پیکسل‌ها، مقدار هزینه درج در تصویر و نرخ درج قابل محاسبه است. با حذف λ ، می‌توان رابطه این دو متغیر را با یکدیگر یافت. بدین منظور، هزینه درج در تصویر نرمالیزه شده و نرخ درج بر حسب توزیع β محاسبه شده است. در روابط (۲۶-۳۳) β_i ها نمونه‌های این متغیر تصادفی هستند؛ از آن جایی که تعداد پیکسل‌های تصویر به اندازه کافی زیاد است، میانگین نمونه‌ها تقریب مناسبی از میانگین آماری است.

$$IC_n = \frac{1}{n} IC = \frac{1}{2\lambda} \times \frac{1}{n} \sum_{i=1}^n \beta_i \ln\left(\frac{2}{\beta_i} - 2\right) \quad (26)$$

$$= \frac{1}{2\lambda} \int x \ln\left(\frac{2}{x} - 2\right) f_{\beta}(x) dx$$

$$\alpha = \frac{1}{n} \sum_{i=1}^n h_3(\beta_i) = \int h_3(x) f_{\beta}(x) dx \quad (27)$$

$$\beta, \frac{2}{\beta} \ln\left(\frac{2}{\beta} - 2\right) = 4\lambda (\cosh\left(\frac{1}{\sigma^2}\right) - 1)$$

تابعی از متغیر تصادفی σ^2 است. برای محاسبه IC_n و α ، تابع چگالی احتمال متغیر تصادفی β را در دو مرحله بر حسب تابع چگالی احتمال σ^2 قابل محاسبه است. در مرحله اول داریم:

$$y = \cosh\left(\frac{1}{\sigma^2}\right) - 1 \quad ; \sigma^2 \geq 0 \Rightarrow \quad (28)$$

$$f_Y(y) = \frac{f_{\sigma^2} \left(\frac{1}{\ln((y+1) + \sqrt{y^2 + 2y})} \right)}{\sqrt{y^2 + 2y} \left(\ln((y+1) + \sqrt{y^2 + 2y}) \right)^2} \quad ; y \geq 0$$

در مرحله دوم، از روی تابع چگالی احتمال متغیر تصادفی Y ، تابع چگالی احتمال β را می‌یابیم. رابطه بین این دو متغیر تصادفی به صورت رابطه (۲۹) است.

با فرض LSBM بودن مکانیسم درج، نرخ تغییرات به صورت رابطه (۳۳) تقریب زده می‌شود؛ در نتیجه، مشابه قسمت قبل با استفاده از توزیع β محاسبه می‌شود.

$$CR = \sum_{i=1}^n \beta_i / n = \int x f_{\beta}(x) dx \quad (33)$$

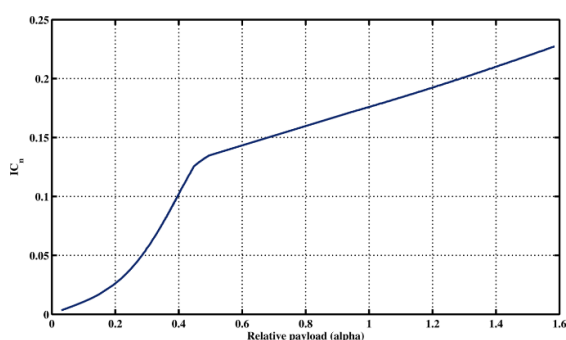
در نهایت با حذف λ ، رابطه PSNR و IC_n مطابق شکل (۹) به دست می‌آید. همان‌گونه که مشاهده می‌شود، تصاویر با هزینه درج بالاتر، دارای PSNR کمتری هستند و کیفیتشان در اثر درج بیشتر افت می‌کند. در نتیجه، تابع هزینه تعریف‌شده، حساسیت مناسبی نسبت به افت کیفیت ناشی از درج دارد.

۶- نتیجه‌گیری

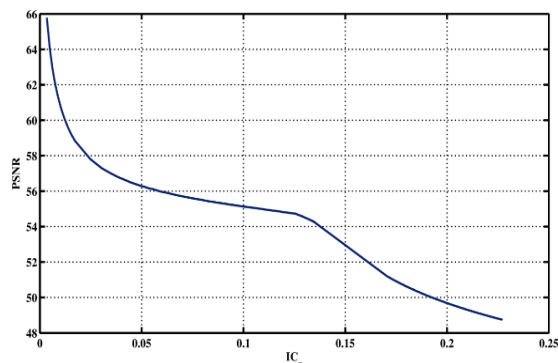
در این مقاله، به دنبال بررسی ارتباط هزینه تغییر پیکسل با ظرفیت نهان‌نگاری و قابلیت کشف آماری بودیم. یافتن این رابطه، مسئله مهم حل‌نشده‌ای در نهان‌نگاری است. با مدل‌سازی نهان‌کاو توسط مدل موضوعی LDA، معیاری از قابلیت کشف آماری ارائه کردیم. برای یافتن این معیار، تصویر پوشش را به صورت نرمال چندمتغیره مدل کردیم. همچنین، با استفاده از این معیار، تعریفی جدید از ظرفیت را بیان نموده و رابطه آن را با هزینه تغییر پیکسل بررسی کردیم. با این تعریف از ظرفیت، رابطه ظرفیت با ابعاد تصویر پوشش (که در نهان‌نگاری به قانون ریشه دوم، معروف است) تایید شد. همچنین، رابطه بین هزینه تغییر پیکسل با قابلیت کشف آماری را با ارائه الگوریتمی مناسب، به دست آوردیم. این الگوریتم براساس بیشینه‌کردن احتمال خطای نهان‌کاو، (به عنوان معیار قابلیت کشف آماری) هزینه تغییر پیکسل را محاسبه و در تصویر درج می‌کند. این الگوریتم، یک الگوریتم وقتی محتوا محور است و عملکردی مشابه الگوریتم MG دارد. با استفاده از توزیع لاپلاس برای پیکسل‌ها بهبودی در حدود ۵٪ نسبت به MG حاصل می‌شود. البته عملکرد آن از بهترین الگوریتم موجود، یعنی S-UNIWARD که فاقد زیرساخت تحلیلی مورد نظر مقاله است، ضعیف‌تر است. لازم به ذکر است که هدف این مقاله، ایجاد رابطه‌ای بین هزینه تغییر پیکسل و قابلیت کشف آماری بود. البته به نظر می‌رسد که دستیابی به الگوریتم‌های نهان‌نگاری قوی‌تر با استفاده از مدل‌های بهتر برای تصویر پوشش، قابل حصول است. با استفاده از مدل نهان‌کاو، معیاری برای هزینه درج در تصویر ارائه کرده و رابطه این معیار را با نرخ درج و PSNR بررسی کردیم. برای الگوریتم پیشنهادی، رابطه ظرفیت نهان‌نگاری را با ابعاد تصویر بررسی کرده و مشاهده شد که قانون ریشه دوم ظرفیت نهان‌نگاری برای نرخ‌های درج بالا، برقرار نیست. برای ادامه این مسیر با مدل‌های مناسب‌تر پوشش می‌توان به نتایج جدید و بهبودهایی رسید.

قبلی [۹]-[۱۱] را تایید می‌کند. در عین حال، برای سطوح امنیت پایین‌تر (مربوط به نرخ‌های درج بیشتر از 0.45 bpp) محدودیت بیشتری وجود دارد؛ تا جایی که با افزایش ابعاد تصویر نمی‌توان اطلاعات بیشتری در تصویر درج کرد.

از طرفی در [۱۰]، قانون ریشه دوم تنها با فرض β کوچک اثبات شده است؛ در حالی که در بررسی فعلی، برقراری این ویژگی تا نرخ درج 0.45 bpp نشان داده شده است. همچنین، ویژگی ذکر شده برای نرخ درج‌های بالا، ویژگی مهمی است که در تحقیقات قبلی به آن اشاره نشده است. این نکته می‌تواند برتری تحلیل ارائه شده در این مقاله را تایید کند.



شکل (۸): تغییرات هزینه درج در تصویر بر حسب نرخ درج



شکل (۹): تغییرات PSNR بر حسب هزینه درج در تصویر

هدف از تعریف هزینه درج در این بخش، بررسی حساسیت تابع هزینه تعریف شده به تغییرات کیفیت تصویر پس از درج است. از آنجایی که مکانیسم درج به صورت ± 1 فرض شده است، رابطه PSNR به صورت رابطه (۳۱) ساده می‌شود:

$$PSNR = 10 \times \log_{10}[Max P^2] - 10 \times \log_{10}[CR] \quad (31)$$

که در آن، CR بیان‌کننده نرخ تغییرات در تصویر است و به صورت رابطه (۳۲) تعریف می‌شود:

$$CR = 1 - \frac{1}{n} \sum_{i=1}^n \delta[IS(i) - IC(i)] \quad (32)$$

که در آن، $\delta[n]$ تابع ضربه است.

multimedia workshop on Multimedia and security, pp. 123–132, 2008.

۷- منابع

- [19] V. K. Chonev and A. D. Ker, "Feature restoration and distortion metrics," in Media Watermarking, Security, and Forensics XIII, Proc. SPIE, vol. 7880, pp. 0G01–0G14, 2011.
- [20] R. Crandall, "Some notes on steganography," Steganography Mailing List, 1998.
- [21] F. Galand, and G. Kabatiansky, "Information hiding by coverings," In Proceedings ITW2003, pp. 151-154, 2003.
- [22] M. van Dijk, and F. Willems, "Embedding information in grayscale images," In Proceedings of the 22nd Symposium on Information and Communication Theory, pp. 147–154, 2001.
- [23] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," IEEE Trans. Inf. Forensics Security, vol. 3, pp. 390-394, 2006.
- [24] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, Proc. SPIE, vol. 6505, pp. 0201–0215, 2007.
- [25] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in 12th International Workshop on Information Hiding, vol. LNCS 6387, pp. 161–177, 2010.
- [26] T. Filler and J. Fridrich, "Gibbs construction in steganography," IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 705–720, 2010.
- [27] F. Huang, J. Huang, and Y.-Q. Shi, "New channel selection rule for jpeg steganography," IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1181–1191, 2012.
- [28] L. Guo, J. Ni, and Y. Q. Shi, "An efficient jpeg steganographic scheme using uniform embedding," in IEEE International Workshop on Information Forensics and Security, pp. 169–174, 2012.
- [29] V. Holub, and J. Fridrich, "Designing steganographic distortion using directional filters," in IEEE Workshop on Information Forensic and Security, pp. 234–239, 2012.
- [30] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in Proceedings of the first ACM workshop on Information hiding and multimedia security, pp. 59–68, 2013.
- [31] J. Fridrich and J. Kodovský, "Multivariate gaussian model for designing additive distortion for steganography," in IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, Canada, pp. 2949–2953, 2013.
- [32] J. Fridrich, M. Goljan, D. Soukal, and P. Lisoněk, "Writing on wet paper," In IEEE Transactions on Signal Processing, Special Issue on Media Security, vol. 53, pp. 3923–3935, 2005.
- [33] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in 8th International Workshop on Information Hiding, vol. LNCS 4437, Springer Berlin Heidelberg, pp. 314–327, 2007.
- [34] R. Zhang, V. Sachnev, and H. Kim, "Fast bch syndrome coding for steganography," in 11th International Workshop on Information Hiding, vol. LNCS 5806, Springer Berlin Heidelberg, pp. 48–58, 2009.
- [35] W. Zhang, X. Zhang, and S. Wang, "Near-optimal codes for information embedding in gray-scale signals," IEEE Trans. Inf. Theory, vol. 56, no. 3, pp. 1262–1270, 2010.
- [36] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3-2, pp. 920–935, 2011.
- [1] Wikipedia Encyclopedia, "Steganography," [Online]. Available: <http://en.wikipedia.org/wiki/Steganography>.
- [2] G. J. Simmons, "The prisoner's problem and the subliminal channel," Advances in Cryptology, CRYPTO '83, pp. 51–67, 1983.
- [3] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevný, "Moving steganography and steganalysis from the laboratory into the real world," 1st ACM IH&MMSec. Workshop, Montpellier, France, 2013.
- [4] C. Cachin, "An information-theoretic model for steganography," Information and Computation, vol. 192, no. 1, pp. 41–56, 2004.
- [5] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.
- [6] R. Böhme, "Advanced Statistical Steganalysis," Springer Berlin Heidelberg, 2010.
- [7] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, April 2011.
- [8] T. Pevný and J. Fridrich, "Benchmarking for steganography," in 10th International Workshop on Information Hiding, vol. LNCS 5284, Springer Berlin Heidelberg, pp. 251–267, 2008.
- [9] A. D. Ker, T. Pevný, J. Kodovský, and J. Fridrich, "The Square Root Law of steganographic capacity," In Proceedings of the 10th ACM Multimedia & Security Workshop, pp. 107–116, Oxford, UK, 2008.
- [10] T. Filler, A. D. Ker, and J. Fridrich, "The Square Root Law of steganographic capacity for Markov covers," In Proceedings SPIE, Electronic Imaging, Security and Forensics of Multimedia XI, vol. 7254, pp. 1–11, San Jose, CA, 2009.
- [11] T. Filler and J. Fridrich, "Fisher information determines capacity of ϵ -secure steganography," In Information Hiding, 11th International Workshop, vol. 5806 LNCS, pp. 31–47, Darmstadt, Germany, 2009.
- [12] A. D. Ker, "Estimating steganographic fisher information in real images," in 11th International Workshop on Information Hiding, vol. LNCS 5806, Springer Berlin Heidelberg, pp. 73–88, 2009.
- [13] N. Provos, "Defending against statistical steganalysis," in 10th USENIX Security Symposium, pp. 323–335, 2001.
- [14] A. Westfeld, "F5—a steganographic algorithm," in 4th International Workshop on Information Hiding, vol. LNCS 2137, Springer Berlin Heidelberg, pp. 289–302, 2001.
- [15] X. Zhang, S. Wang, and K. Zhang, "Steganography with least histogram abnormality," in Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, vol. LNCS 2776, Springer Berlin Heidelberg, pp. 395–406, 2003.
- [16] P. Sallee, "Model-based steganography," in Second International Workshop on Digital Watermarking, vol. LNCS 2939, Springer Berlin Heidelberg, pp. 154–167, 2003.
- [17] A. Sarkar, K. Solanki, U. Madhow, S. Chandrasekaran, and B. Manjunath, "Secure steganography: Statistical restoration of the second order dependencies for improved security," in IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 2, pp. II–277–280, 2007.
- [18] J. Kodovsk and J. Fridrich, "On completeness of feature spaces in blind steganalysis," in Proceedings of the 10th ACM

- [44] J. Zhang, I. Cox, and G. Doerr, "Steganalysis for LSB matching in images with high frequency noise," IEEE 9th Workshop on Multimedia Signal Processing, pp. 385–388, 2007.
- [45] D. Blei, A. Ng, and M. Jordan, "Latent Dirichlet allocation," Journal of Machine Learning Research, vol. 3, pp. 993–1022, 2003.
- [46] V. Sedighi, R. Cogramne, and J. Fridrich, "Content-Adaptive Steganography by Minimizing Statistical Detectability," IEEE TIFS, vol. 11, no. 2, pp. 221–234, 2016.
- [47] M. Shamalizade, Z. Nowrouzi, M. Sabzinejad, and M. Karami, "Adaptive Image Steganography based on Graph Entropy with Improved Security Effectivity," Advanced Defence Sci. & Tech., Journal, 5 July 2017. (In Persian)
- [48] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 432–444, 2012.
- [49] X. Wang, C. Chang, C. Lin, and M. Chu Li, "A novel multi-group exploiting modification direction method based on switch map," Signal Process, vol. 92, pp. 1525–1535, 2012.
- [37] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 215–224, 2010.
- [38] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882, 2012.
- [39] P. Moulin and Y. Wang, "New results on steganographic capacity," In Proceedings of the Conference on Information Sciences and Systems, CISS, Princeton, NJ, 2004.
- [40] T. Filler, "Imperfect stegosystems-asymptotic laws and near-optimal practical constructions," Dissertation, Binghamton University State University of New York, 2011.
- [41] J. Fridrich, "Effect of cover quantization on steganographic fisher information," IEEE Transactions on Information Forensics and Security, 2013.
- [42] T. Pevný, J. Fridrich, and A. D. Ker, "From blind to quantitative steganalysis," IEEE Transactions on Information Forensics and Security, vol. 7, pp. 445–454, 2012.
- [43] C. Corporation, "Corel stock photo library 3, Ontario, Canada.

Relating the Detection Rate, Capacity and the Cost of Steganography by Steganographer Modeling

I. Gholampour*, R. Amiri

*University of Qom

(Received: 20/08/2017, Accepted: 04/10/2017)

ABSTRACT

Statistical detectability of a steganalyser declares its ability to distinguish between cover and stego images. Optimum steganographer must be designed to confuse the corresponding steganalysers in detecting stego images. Thus, designing a steganographic algorithm based on reducing statistical detectability is of great importance. Unfortunately establishing a perfect relation between pixel cost and statistical detectability is still an open problem. In this paper, we have modelled steganalyser by special graphical models, called topic models, to estimate the error rate of a steganalyser in terms of the steganographic pixel cost. Moreover, we have redefined the steganographic capacity and pixel cost based on such models. It is also shown that the new criteria are compatible with classical ones, like PSNR. Then, an algorithm is designed as per such criteria. It is shown empirically that the presented algorithm is comparable to the best analytically designed algorithms presented so far. It is worth mentioning that the paper is focused on establishing a mathematical basis for the relation between the steganalyzer error and pixel cost and not improving the current algorithms. Nonetheless, as compared to the rivals, a small improvement, about 0.5% in steganalysis error, has also been achieved.

Keywords: Steganography, Steganalysis Model, Capacity, Pixel Cost, Statistical Detectability, Topic Models

* Corresponding Author Email: imangh@sharif.ir