مجله علمی-پژوهشی
رایانش نرم و فناوری اطلاعات
جلد ۴، شماره ۳، سال ۱۳۹۴

تأثیر فضاهای رنگ در مخفی‌سازی اطلاعات در تصاویر رنگی

سید محمد علی جوادی[۱]، مریم حسن زاده [۲]
[۱]دانشگاه شاهد، تهران، Javadi_sma_ms@yahoo.com
[۲]دانشگاه شاهد، تهران، hasanzadeh@shahed.ac.ir

چکیده – پنهان نگاری شاخه ای از علم ارتباطات پوشیده است که هدف آن، پنهان کردن وجود اطلاعات است. در مقابل، علم نهان‌کاوی تشخیص و/یا تخمین اطلاعات مخفی شده با داشتن دانشی اندک (یا بدون هیچ دانشی) درباره الگوریتم پنهان نگاری است. با وجود آنکه تصاویر رنگی، ظرفیت پنهان نگاری بالایی دارند و استفاده از آن‌ها متداول است اما تحقیقات کمتری در حوزه‌ی مخفی سازی اطلاعات در آنها نسبت به تصاویر خاکستری صورت گرفته است، در این مقاله، پنهان نگاری و نهان‌کاوی تصاویر رنگی در فضاهای رنگ مختلف (از جمله *RGB*، *YUV*، *YIQ*، *YCbCr*، *HSV*)، به طور جامعی مورد بررسی قرار گرفته و روش‌های جدیدی نیز در این دو حوزه ارائه شده است. در حوزه پنهان‌نگاری، روش ساده و مقاومی برای پنهان سازی اطلاعات در تصاویر رنگی با استفاده از فضاهای رنگ *YUV* و *YCbCr* پیشنهاد شده است که تشخیص وجود پیام به دلیل استفاده از ضرایب تبدیلات دشوارتر شده است. مقاومت روش پیشنهادی با چند نهان کاو معروف ارزیابی شده است و نتایج نشان می دهد که در این روش مقاومت در برابر حملات نهان کاوی، نسبت به روش مبتنی بر استفاده از فضای *RGB*، افزایش یافته است. در حوزه نهان کاوی نیز، با بررسی فضاهای رنگ مختلف، روش نهان کاوی عام و جدیدی پیشنهاد شده است که مبتنی بر همبستگیِ مکانیِ پیکسل‌های مجاور در مؤلفه های فضاهای رنگ مختلف است. این روش مستقل از نوع روش پنهان‌نگاری طراحی شده، دارای قدرت تشخیص مناسبی است. در مجموع نتایج حاصل از این دو روش نقش استفاده مناسب و مؤثر از فضای رنگ را در مخفی سازی اطلاعات در تصاویر رنگی برجسته می سازد.

کلید واژه‌ها - پنهان نگاری، نهان‌کاوی، فضای رنگ، تصاویر رنگی.

۱ مقدمه

به دلیل رشد اینترنت یکی از مهمترین فاکتورهای فناوری اطلاعات و ارتباطات، امنیت است. رمزنگاری (Cryptography) به عنوان روشی برای امن کردن تبادل اطلاعات محرمانه است و تا کنون روش های مختلفی برای رمزنگاری و رمزگشایی به منظور حفاظت از پیام مخفی ارائه شده است. با این وجود، گاهی اوقات تنها حفاظت از محتوای پیام مخفی کافی نیست و باید از وجود پیام مخفی نیز محافظت شود. برای این منظور از پنهان-نگاری (Steganography) استفاده می‌شود. اشکال عمده رمزنگاری این است که اگر شخص ثالثی در هنگام ارسال اطلاعات از وجود اطلاعات محرمانه مطلع شود، حتی اگر به دلیل رمزنگاری قوی نتواند به این اطلاعات مخفی دست یابد، می‌تواند از رسیدن پیام به مقصد جلوگیری کند. اگر بتوان اطلاعات را به گونه‌ای فرستاد که وجود پیام نیز پنهان باقی بماند، امنیت افزایش یافته و پیام محرمانه خواهد ماند. در واقع، پنهان‌نگاری به دنبال تحقق چنین امری است. در مقابل روش‌های پنهان‌نگاری، روش‌های نهان‌کاوی (Steganalysis) قرار دارند که سعی دارند تصویر پوشش (cover image) را از تصویر گنجانه (stego image) تشخیص دهند [۱-۳].

با وجود استفاده گسترده از تصاویر دیجیتال در اینترنت و به دلیل افزونگی بالای موجود در این نوع فایل‌ها، تصاویر یکی از بهترین اشیاء پوشش برای پنهان‌نگاری هستند. تاکنون تحقیقات زیادی در حوزه پنهان‌نگاری در تصاویر خاکستری انجام شده است و در مقایسه با آن تحقیقات در حوزه تصاویر رنگی بسیار کم‌تر بوده است. در میان تحقیقات مذکور نیز اغلب از فضای رنگ متداول RGB استفاده شده است هدف اصلی در این مقاله بررسی تأثیر استفاده از اطلاعات فضاهای رنگ مختلف در پنهان-نگاری و نهان‌کاوی تصاویر رنگی است.

در این مقاله یک روش پنهان‌نگاری ساده و مقاوم با استفاده از فضای رنگ YUV و YCbCr ارائه شده است و میزان مقاومت آن در حملات نهان‌کاوی نشان داده شده است. در حوزه نهان-کاوی نیز روش جدیدی پیشنهاد شده است که در آن ویژگی‌ها از فضاهای رنگ (مانند فضاهای رنگ YUV، YIQ، YCbCr و HSV) به‌جای فضای رنگ RGB استخراج می شود. پایه روش پیشنهادی، مبتنی بر همبستگی مکانی پیکسل‌های مجاور در مؤلفه‌های رنگی مختلف است. این روش مستقل از نوع روش پنهان‌نگاری طراحی شده است. فضاهای رنگ اغلب از تجزیه مؤلفه‌های رنگ و روشنایی استفاده می‌کنند که در نتیجه همبستگی بین کانال‌های R، G و B از فضای رنگ RGB حذف

www.SID.ir
Archive of SID

می‌شود. همچنین این فضاهای رنگ، اثرات یک روش پنهان-نگاری را در کل بردار رنگ پیکسل یکپارچه می‌کنند، لذا اطلاعات مفیدتری برای نهان‌کاوی در مقایسه با استخراج ویژگی از فضای رنگ RGB فراهم می‌آورند.

ادامه این مقاله در چند بخش سازماندهی شده است. روش های مختلف پنهان‌نگاری و نهان‌کاوی تصاویر رنگی در فضاهای رنگ مختلف در بخش ۲، به طور جامع مورد بررسی قرار گرفته است. در بخش ۳ روش پنهان‌نگاری و نهان‌کاوی پیشنهادی به تفکیک ارائه شده است. نتایج حاصل از پیاده‌سازی روش‌های پیشنهادی در مقایسه با برخی روش‌های متداول، در بخش ۴ مورد بررسی قرار گرفته است. در بخش ۵ نیز نتیجه‌گیری کلی و پیشنهادهایی برای ادامه کار ارائه شده است.

۲ بررسی روش‌های پنهان‌نگاری و نهان‌کاوی تصاویر رنگی با استفاده از فضاهای رنگ مختلف

در این بخش روش‌های پنهان‌نگاری و نهان‌کاوی مختلف با استفاده از اطلاعات فضاهای رنگ مختلف مورد مطالعه قرار گرفته است.

۲-۱ پنهان نگاری با استفاده از فضاهای رنگ

روش LSB (Least Significant Bit) یکی از مهم‌ترین و متداول‌ترین روش‌های پنهان‌نگاری در دامنه مکانی تصاویر است. روش LSB به دو دسته کلی جایگزینی LSB (LSB replacement) و تطبیق LSB (LSB matching) تقسیم می-شود. این روش ترکیبی از مزایای ظرفیت بالا، نامحسوس بودن از نظر دیداری، و سهولت پیاده‌سازی را داراست. در این روش برای انتخاب پیکسل‌ها می‌توان از روش‌های مختلف استفاده کرد؛ اگر پیکسل‌ها به ترتیب برای تعبیه انتخاب شوند، به این روش جایگزینی ترتیبی LSB گفته می‌شود. در صورتی که پیکسل‌ها به صورت شبه تصادفی (به کمک یک کلید رمز مشترک بین ارسال‌کننده و دریافت‌کننده) به منظور تعبیه در نظر گرفته شوند، به این روش، جایگزینی تصادفی LSB گفته می‌شود. تصادفی بودن ترتیب تعبیه باعث می‌شود که خواندن مستقیم داده مخفی توسط نهان‌کاو مقدور نباشد و همچنین داده مخفی روی کل تصویر پوشش، پخش شود (هنگامی که داده مخفی کمتر از حداکثر ظرفیت تعبیه است) و روش در برابر حملات نهان‌کاوی مقاوم‌تر شود[۴].

به عنوان مثال در [۵-۷] روش‌هایی مبتنی برLSB ترتیبی ارائه شده است که در آنها شنودکننده‌ها می‌توانند به راحتی با یک اسکن ترتیبی پیام مخفی را به دست آورند. در مقابل، انتخاب تصادفی پیکسل‌ها نیاز به یک کلید پنهان‌نگاری برای فازهای تعبیه و استخراج اطلاعات دارد. لذا هماهنگی بین فرستنده و گیرنده و سربار مدیریت کلید را داراست[۸].

آقای حسین در سال ۲۰۱۰روش SCC [۸] را توسعه‌ای بر روش LSB ارائه کرده است. در این روش کانال رنگی که باید یک بیت در آن تعبیه شود، براساس الگویی خاص و به صورت تکراری انتخاب می شود. اگرچه امنیت آن از LSB ساده بیشتراست اما اگر از طریق اسکن ترتیبی، الگوی به کار رفته برای تعبیه اطلاعات کشف شود، کل داده مخفی استخراج خواهد شد. در مقابل ظرفیت این روش کمتر از روش LSB است، چرا که فقط در یک کانال رنگ از هر پیکسل تعبیه انجام می‌شود.

به منظور افزایش کیفیت تصویر گنجانه، در سال ۲۰۰۶ در [۹] روشی پیشنهاد شده است که داده‌ها در لبه‌های تصویر پوشش تعبیه می‌شوند. اگرچه مزیت این روش کیفیت بالای تصویر گنجانه است، اما ظرفیت این روش کم است.

آقای اوجا و همکارانش در سال ۲۰۰۹ در [۱۰] از چهار بیت کم ارزش در هر کانال رنگ RGB برای تعبیه داده استفاده کرده اند. در روش آنها از فیلتر میانه (Median filter) برای افزایش کیفیت تصویر گنجانه استفاده شده است و تفاضل تصویر پوشش و تصویر گنجانه نیز به عنوان کلید داده کدگذاری شده است. اگرچه این روش، ظرفیت پنهان‌نگاری زیادی دارد، اما فیلتر کردن، پیچیدگی محاسباتی را افزایش داده است و سربار مدیریت کلید نیز وجود دارد.

در روش تطبیق LSB، هر بیت داده مخفی با کم ارزش‌ترین بیت از بایت پیکسل مورد نظر در تصویر پوشش مقایسه می‌شود، اگر با هم یکسان باشند هیچ تغییری انجام نمی‌شود؛ در غیر این صورت آن بایت به صورت تصادفی یک واحد افزایش یا کاهش می‌یابد. با وجود این‌که شباهت زیادی بین روش‌های جایگزینی LSB و تطبیق LSB وجود دارد، اما مقاومتشان در برابر نهان کاوی یکسان نیست. شاید وجود تقارن ذاتی در جایگزینی LSB (پیکسل پوشش با مقدار زوج ممکن است بدون تغییر بماند یا ممکن است یک واحد به آن اضافه شود، اما هرگز کاهش نمی-یابد، برعکس این روند برای پیکسل‌های با مقدار فرد برقرار است) باعث شده است که این روش به آسانی تشخیص داده شود. این

Archive of SID

www.SID.ir

تقارن ذاتی در روش تطبیق LSB وجود ندارد لذا این روش در برابر حملات نهان‌کاوی مقاوم‌تر است[۴].

ایده روش پنهان‌نگاری مبتنی بر پیکسل نماینده در [۱۱] که آقای گوتب و همکاران در ۲۰۰۸ ارائه داده اند این است که از دو بیت کم ارزش یکی از کانال‌های R، G یا B به عنوان نماینده برای تعبیه داده در دو کانال دیگر استفاده می‌شود. عیب این روش این است که ظرفیت آن کم و وابسته به بیت‌های نماینده و تصویر پوشش است. همچنین این روش از تعداد بیت ثابتی (در هر کانال ۲ بیت) برای تعبیه داده استفاده می‌کند. الگوریتم دیگری برای توسعه این روش ارائه شده است، که روش بیت‌های متغیر مبتنی بر شدت روشنایی [۱۲] نام دارد. این الگوریتم حداقل ظرفیت برای هر تصویر پوشش را تضمین می‌کند و تعداد بیت‌های تعبیه شده در هر کانال متفاوت و وابسته به شدت روشنایی است. در مقابل از آنجایی که یکی از کانال‌های R، G یا B به‌عنوان کانال نماینده مورد استفاده قرار می‌گیرد، عملاً ظرفیت تعبیه در یکی از کانال ها از دست می رود.

در روش پنهان‌نگاری مبتنی بر تقسیم‌بندی تصویر و رمزنگاری RSA [۱۳] در ۲۰۱۲، تصویر و پیام به بلاک‌های هشت تایی تقسیم می‌شوند و هر بلاک پیام در یک بلاک تصویر با یک کلید تعریف شده توسط کاربر تعبیه می‌شود. در هر بلاک تصویر، یک کانال به عنوان کانال نماینده در نظر گرفته می‌شود و از دو کانال دیگر به منظور تعبیه چهار بیت استفاده می‌شود. البته در صورتی چهار بیت تعبیه می‌شود که تغییر مقدار در کانالی که تعبیه در آن انجام شده است، کمتر یا مساوی ۷ باشد. در این روش همچنین از الگوریتم رمزنگاری و رمزگشایی RSA در سمت فرستنده و گیرنده به منظور بالا بردن امنیت، استفاده شده است.

روش پنهان‌نگاری با افزایش کیفیت تصویر گنجانه [۱۴] که در سال ۲۰۱۲ ارائه شده است، پیام را مبتنی بر جستجویی درباره‌ی مقادیر یکسان بین بیت‌های پیام مخفی و پیکسل‌های تصویر، تعبیه می‌کند. مزیت عمده این روش، کیفیت مناسب و امنیت است. از معایب اصلی این روش، چگونگی ذخیره پیکسل-هایی است که در آن‌ها اطلاعات تعبیه شده است و نیز ارسال آن‌ها برای گیرنده است. لذا این مشکل شبیه مشکل سربار مدیریت کلید است که در بعضی از روش‌هایی که پنهان‌نگاری را مبتنی بر کلید انجام می‌دهند، وجود دارد.

روش MKA که در سال ۲۰۱۰ ارائه شد، روشی مبتنی بر LSB است که در آن می‌توان تا ۵ بیت کم ارزش از پیکسل‌ها را برای تعبیه استفاده کرد که البته وابسته به مقدار شدت روشنایی پیکسل و مقدار بیت جاری برای تعبیه است. مزیت این روش امنیت بالای آن به دلیل استفاده از یک کلید رمز هشت بیتی است [۸]. عیب اصلی این روش نیز همانند روش قبل ذخیره مکان پیکسل‌هایی است که در آن‌ها اطلاعات تعبیه شده و نیز نیاز به ارسال آن‌ها برای گیرنده است. همچنین ظرفیت این روش به نوع بیت داده و شدت روشنایی پیکسل‌های تصویر بستگی دارد. در روش توسعه‌یافته MKA، پیکسل‌های با شدت روشنایی کم نیز برای پنهان‌سازی اطلاعات استفاده می‌شوند. اگر از همه بایت‌های تصویر پوشش برای تعبیه استفاده شود، این الگوریتم ظرفیت پنهان‌سازی بالایی در مقایسه با MKA خواهد داشت و همچنین استفاده از کلید رمز هشت بیتی باعث افزایش امنیت روش می‌شود[۸]. اما در این روش نیز همانند روش MKA مشکل ذخیره پیکسل‌هایی که در آن‌ها اطلاعات تعبیه شده است و نیز ارسال آن‌ها برای گیرنده، وجود دارد.

چن هسینگ یانگ و همکارانش در سال ۲۰۱۰ روشی مبتنی بر مکان پنهان‌سازی اطلاعات و مقدار اطلاعات پنهان شده بر اساس مقادیر مختلف شدت روشنایی مؤلفه‌های رنگ R، G و B در هر پیکسل ارائه نموده‌اند. از جمله مزایای این روش این است که ظرفیت اطلاعات پنهان شده توسط این روش تقریبا ۲۴٪ تصویر پوشش است. از طرف دیگر از آنجایی که این روش همانند LSB در هر صفحه بیتی به صورت ثابت اطلاعات را تعبیه نمی-کند، می‌تواند از نشت اطلاعات به‌وسیله فیلترکردن صفحه بیتی جلوگیری کند. بنابراین این الگوریتم از لحاظ امنیتی نسبت به LSB امنیت بیشتری دارد و همچنین دارای قابلیت ضد نویز و ضد برش بودن است [۱۵].

روش Triple-A نیز روشی مبتنی بر LSB است. در این روش تعداد بیت‌ها و کانال‌های رنگ به صورت تصادفی انتخاب می-شوند. تصادفی انتخاب کردن تعداد بیت‌ها و کانال رنگ و نیز استفاده از الگوریتم AES باعث افزایش امنیت این روش می-شود[۱۶]. از معایب اصلی این روش، مدیریت سربار کلید است.

در روشی که آقای نیکوکار در سال ۲۰۱۰ پیشنهاد داده است، داده‌ها در یک سوم از حجم تصویر پوشش پنهان می‌شوند؛ در نتیجه این روش دارای ظرفیت پنهان‌نگاری بالایی است. علاوه بر این در این روش، از یک کلید مناسب برای رمز کردن داده‌ها استفاده می‌شود که باعث افزایش امنیت می‌شود[۱۷].

با توجه به مطالعاتی که در حوزه پنهان‌نگاری در تصاویر رنگی انجام شده است، اکثر روش‌های پنهان‌نگاری اطلاعات، پیام را به

Archive of SID

www.SID.ir

صورت مستقیم در فضای رنگ RGB تعبیه می‌کنند که در این زمینه مقالات زیادی با ظرفیت و مقاومت مختلف ارائه شده است. در مقابل، در سایر فضاهای رنگ (از جمله YUV، YIQ، YCbCr و HSV)، پنهان‌نگاری به ندرت انجام شده است. در سال ۲۰۰۷ روشی برای پنهان‌نگاری در فضای رنگ YUV ارائه شده است که به علت استفاده از تبدیلات فضای رنگ RGB به فضای رنگ YUV و برعکس، در هنگام استخراج اطلاعات، پیام تعبیه شده به صورت کامل قابل استخراج نیست و به عبارتی BER(bit error rate) وجود دارد [۱۸]. با وجود مزایایی که استفاده از فضاهای رنگ مختلف می تواند داشته باشد، این نکته (BER) می تواند یکی از دلایل استفاده نادر از سایر فضاهای رنگ در پنهان‌نگاری باشد.

هدف اصلی این مقاله، استفاده از اطلاعات فضاهای رنگ مختلف به منظور پنهان‌نگاری و نهان‌کاوی و ارزیابی آن‌ها در مقایسه با فضای رنگ RGB است. در حوزه پنهان نگاری، ایده اصلی این مقاله این است که از تبدیلات فضای رنگ برای تعبیه اطلاعات استفاده شود. هدف این است که این تبدیلات باعث مقاومت بیشتر روش پنهان نگاری در مقابل روش‌های نهان‌کاوی گردد. علاوه بر این ضرایب ماتریس تبدیل می تواند به عنوان کلید رمز استفاده می‌شود. چالش اصلی این ایده ظهور BER است که نویسندگان در [۱۹] نیز به آن اشاره کرده اند. در روش پیشنهادی این مقاله مشکل مذکور مرتفع گردیده است که شرح آن در بخش ۱.۳ آورده شده است.

در این مقاله، تأثیر استفاده از اطلاعات فضاهای رنگ در حوزه نهان‌کاوی نیز با ارائه یک روش نهان کاوی جدید مورد بررسی قرار گرفته است که در بخش های آتی به آن پرداخته خواهد شد.

۲-۲ نهان‌کاوی با استفاده از اطلاعات فضای رنگ

روش‌های مطرح در حوزه نهان‌کاوی تصاویر رنگی اغلب مبتنی بر پردازش‌های مستقل در هر یک از کانال‌های رنگ در فضای رنگ RGB می‌باشند. در ادامه برخی از این روش‌ها مورد بررسی قرار گرفته است.

خانم فردریچ و همکارانش، روشی ارائه نمودند که در آن پیکسل‌هایی که از نظر شدت روشنایی به هم نزدیک هستند و تفاوت آن‌ها در هر سه کانال رنگ بیش‌تر از یک نیست تعیین می‌شوند. سپس نشان داده اند که نسبت رنگ‌های نزدیک به کل تعداد رنگ‌های موجود در هنگامی که یک پیام جدید با طول انتخابی در تصویر پوشش بدون پیام تعبیه می‌شود، در مقایسه با هنگامی که در تصویر پوشش دو بار تعبیه صورت می گیرد، تفاوت قابل ملاحظه‌ای دارد. در این روش پردازش‌ها به صورت همزمان در سه کانال R، G و B انجام می‌شود [۲۰]. روش پیچیده‌تری نیز که دقت قابل توجهی در تشخیص تعبیه LSB حتی برای پیام‌های کوتاه فراهم می کند، توسط نویسنده مذکور ارائه شده است که به روش RS [۲۱] مشهور است. در این روش پردازش‌ها به صورت مستقل در سه کانال رنگ R، G و B انجام می‌شود.

آقای ابوالقاسمی و همکارانش روش نهان‌کاوی برای تصاویر خاکستری پیشنهاد کردند که در آن ترکیبی چندتایی از عناصر قطری ماتریس GLCM در فضای مکانی به عنوان ویژگی‌های نهان‌کاوی در نظر گرفته شده است. این ماتریس به فرآیند تعبیه اطلاعات حساس است [۲۲]. این روش را ککر و همکارانش برای تصاویر رنگی توسعه داده اند[۲۳]. در این توسعه در هر کانال رنگ از فضای رنگ RGB، GLCM به طور جداگانه محاسبه شده و حداکثر مقادیر سه کانال به عنوان نتیجه در نظر گرفته می‌شود.

آقای میترا و همکارانش روش نهان‌کاوی زوج رنگ همسایه را ارائه نمودند که به روش CCP مشهور است [۲۴]. ایده اصلی این روش مبتنی بر نسبت تعداد رنگ‌های واحد به تعداد کل پیکسل-ها در تصویر است که این نسبت معمولاً در تصاویر پاک یک به شش است. این نسبت در تصویر قبل از پنهان‌نگاری و بعد از پنهان‌نگاری محاسبه می‌شود، سپس تفاضل این دو مقدار تقسیم بر مقدار قبل از پنهان نگاری می‌شود و به عنوان ویژگی برای تفکیک بین تصویر گنجانه و تصویر پاک استفاده می‌شود. توسعه ای بر این روش نیز وجود دارد که از حد آستانه متغیر به منظور تمایز بین تصویر پاک و تصویر گنجانه استفاده می‌کند و آن را تحلیل زوج رنگ با حد آستانه متغیر (CPAVT) نامیده‌اند [۲۵]. روش مذکور از چگالی رنگ به عنوان حد آستانه متغیر استفاده می‌کند. این روش برای بعضی از گروه‌های تصاویر که به تعبیه LSB خیلی حساس نبودند، نتایج مطلوبی نداشته است. ایراد مذکور، در روش نهان‌کاوی CCPASST [۲۶] با تغییر روش تعیین حد آستانه رفع شده است. در این روش از شاخص SSIM به منظور تعیین حد آستانه استفاده می‌شود و نسبت به روش‌های CCP و CPAVT دارای نرخ تشخیص بهتری است. ککر و همکارانش روش CCPASST را توسعه دادند و از حد آستانه‌های متغیر مختلف به منطور نهان‌کاوی استفاده کردند [۲۷].

Archive of SID

www.SID.ir

S. Dumitrescu و همکارانش روش تحلیل زوج نمونه را ارائه دادند [۲۸]. مبنای این روش، یک ماشین وضعیت متناهی است که وضعیت‌های موجود در آن، مجموعه‌های انتخابی از زوج‌های نمونه هستند. روش تحلیل زوج نمونه توسط Peizhong و همکارانش توسعه داده شده است [۲۹] که آن‌ها معیارهای موجود در روش تحلیل زوج نمونه با تخمین حداقل مربعات را ترکیب کردند. این روش در مقایسه با روش تحلیل زوج نمونه دارای قدرت تشخیص بهتری است.

نویسندگان مقاله در [۳۰] روش نهان‌کاوی مبتنی بر همبستگی کانال‌های رنگ در نواحی همگن تصاویر رنگی را، بر پایه ترکیبی از همبستگی کانال‌های رنگ و همبستگی پیکسل‌های مجاور ارائه نموده‌اند که مستقل از نوع روش پنهان-نگاری طراحی شده است. این روش پتانسیل بالایی در نهان‌کاوی تصاویر حاصل از روش جایگزینی LSB و روش تطبیق LSB داشته است.

تمام روش‌های نهان‌کاوی بررسی شده در فوق، در حوزه فضای رنگ RGB ارائه شدند. روش‌های نهان‌کاوی معدودی نیز وجود دارند که از سایر فضاهای رنگ به منظور استخراج ویژگی برای نهان‌کاوی استفاده می‌کنند که در ذیل بدان اشاره می شود.

Xiang-Wei Kong و همکارانش روشی را مبتنی بر همبستگی محلی Hue در فضای رنگ HSI برای تصاویر رنگی پیشنهاد کرده‌اند. ایده اصلی این روش این است که تصویر را به بلاک‌هایی تقسیم می‌کنند و همبستگی Hue را برای هر یک از بلاک‌ها به طور مستقل چک می‌کنند. اگر نسبت پیکسل‌هایی که Hue متفاوتی با آن محیط دارند به کل پیکسل‌های بلاک بزرگ-تر از یک حد آستانه باشد، آن بلوک به عنوان ناحیه گنجانه در نظر گرفته می‌شود، در غیر این صورت جزء نواحی بدون تعبیه است [۳۱].

Yuan-lu Tu و Sheng-rong Gong، یک الگوریتم نهان‌کاوی سراسری با استفاده از تبدیل فضای رنگ YUV و ترکیب ویژگی-های DCT و DWT پیشنهاد کردند. در این روش۴۰ ویژگی از مؤلفه روشنایی و یک ویژگی از مؤلفه رنگ استخراج می شود[۳۲].

به طور کلی در حوزه نهان‌کاوی تصاویر رنگی، اکثر روش‌ها ویژگی‌هایشان را از فضای رنگ RGB استخراج می‌کنند و پردازش‌های مستقلی به منظور استخراج ویژگی در کانال‌های R، G و B انجام می دهند. به عبارت دیگر از همبستگی خاصی که بین کانال‌های رنگ در فضای RGB وجود دارد استفاده نمی کنند. این درحالی است که از آن سو اغلب الگوریتم‌های پنهان-نگاری از همبستگی میان کانال‌های R، G و B برای کاهش تغییرات مقدار رنگ در تصاویر بهره برده اند و معمولاً پیام را به طور مستقل در سه کانال تعبیه نمی‌کنند. از طرف دیگر همانطور که در این بخش مقاله نیز مشاهده شد روش‌های نهان کاوی اغلب از اطلاعاتی که سایر فضا های رنگ می‌تواند در اختیار قرار دهد بهره نبرده اند.

۳ روش‌های پیشنهادی به منظور پنهان‌نگاری و نهان کاوی

در این بخش روش پنهان‌نگاری و روش نهان‌کاوی پیشنهادی در زیربخش‌های جداگانه ارائه شده است.

۲-۳ ۳-۱ روش پنهان نگاری پیشنهادی

در بخش قبل ذکر شد که اکثر روش‌های پنهان‌نگاری در تصاویر رنگی، پیام را به طور مستقیم در فضای رنگ RGB تعبیه می‌کنند و در سایر فضاهای رنگ، پنهان‌نگاری به ندرت انجام شده است. در این بخش، پنهان‌نگاری در فضاهای رنگ مختلف را مورد بررسی قرار داده‌ایم. هدف از این بررسی افزایش مقاومت روش پنهان‌نگاری در برابر نهان کاوی و افزایش امنیت و دشوار شدن فرآیند تشخیص اطلاعات تعبیه شده است.

به عبارت دیگر مزیت مورد انتظار از پنهان‌نگاری با استفاده از تبدیلات فضاهای رنگ این است که استفاده از ضرایب این تبدیلات باعث دشوارتر شدن تشخیص وجود و استخراج پیام تعبیه شده شود. علاوه بر این ضرایب تبدیلات می‌تواند بخشی از کلید رمز تعبیه داده‌ها باشد و با تغییر در ضرایب، نرخ تشخیص اطلاعات کاهش داده شود.

بدنه‌ی اصلی روش پیشنهادی بدین صورت است که تصویر پوشش از فضای رنگ RGB به فضای رنگ دیگری (یکی از فضاهای رنگ YUV، YCbCr، YIQ و HSV) تبدیل می شود و در یک کانال از آن فضای رنگ تعبیه انجام شود و پس از تعبیه، تصویر مجدد به فضای رنگ RGB تبدیل شود.

Start

"Embedding phase":

Set S = YUV (or YCbCr).

Set M = The message for embedding.

Set Ch = Selected Channel for embedding.

Set I' = Converted image I from RGB To S.

Archive of SID

www.SID.ir

Embed *M* in *Ch channel of I'*.
Set *O* =Converted image (*I'*) from *S* To RGB.

//"Inner Decoder phase":
Set *E* =1
While *E* = 1 Do
Set *O'*= Converted image *O* from RGB to *S*
Set *M'*=Extraced Message from *Ch* of *O'*
If *M*=*M'* then
Set *E*=0.
Else
Find the Pixels where error occurs in.
Decrease the corresponding Y channel value of them by one.
Set *O* = Converted image O' from *S* to RGB.
End

Send RGB stego image (*O*) to Reciver
End

الگوریتم۱: شبه کد تعبیه به روش پیشنهادی در دو فضای رنگ YUV و YCbCr

در فرآیند تعبیه اطلاعات، از روش جایگزینی LSB که متداول‌ترین روش پنهان‌نگاری اطلاعات در تصاویر است، استفاده شده است و طی آن در هر پیکسل فقط یک بیت و آن یک بیت فقط در یکی از کانال‌ها (کانالی که به منظور تعبیه انتخاب شده است) تعبیه می‌شود. در فرآیند استخراج اطلاعات ابتدا تصویر رنگی به فضای رنگ مورد نظر تبدیل می‌شود و اطلاعات منطبق با روش تعبیه اطلاعات، استخراج می‌شود.

مشکل اصلی پنهان‌نگاری در فضاهای رنگی که از تبدیلات استفاده می‌کنند این است که (به دلیل خطای گردکردن در هنگام تبدیلات)، در هنگام استخراج اطلاعات، کمی BER حاصل می‌شود. به این مشکل در مراجع [۱۸و۱۹] نیز اشاره شده است. در این مقاله برای به صفر رساندن BER در دو فضای رنگ YUV و YCbCr روشی پیشنهاد شده است که در ذیل شرح داده شده است.

ایده روش پیشنهادی برای صفر کردن BER مبتنی بر این است که یک عمل تصحیح خطا در سمت فرستنده اعمال شود. در الگوریتم ۱ شبه کد الگوریتم تعبیه به همراه مرحله تصحیح خطا آورده شده است.

همان‌طور که در الگوریتم ۱ نشان داده شده است، روش پنهان‌نگاری پیشنهادی در هنگام تعبیه اطلاعات، دارای دو فاز است: فاز تعبیه و فاز دیکدر داخلی که در ادامه مراحل این الگوریتم شرح داده می شود.

در فاز تعبیه ابتدا تصویر پوشش از فضای رنگ RGB به فضای رنگ مورد نظر (فضای رنگ YUV یا YCbCr) تبدیل می‌شود.

یکی از کانال‌های تصویر، به منظور تعبیه اطلاعات انتخاب می‌شود و با استفاده از الگوریتم جایگزینی LSB، درکانال انتخاب شده تعبیه انجام می‌شود. پس از تعبیه، تصویر مجددا به فضای رنگ RGB تبدیل می‌شود.

به منظور تصحیح خطا، فاز دیکدر داخلی در هنگام تعبیه اطلاعات، در نظر گرفته شده است. این فاز مشخص می‌کند که چه بیت‌هایی از پیام تعبیه شده در سمت گیرنده، با خطا استخراج می‌شوند. به عبارتی دیگر، مکان این بیت‌ها (یعنی پیکسلی که بیت تعبیه شده در آن با خطا استخراج شده است) را تعیین می‌کند. فاز دیکدر داخلی تا هنگامی که BER صفر شود اجرا می‌شود و شامل مراحل زیر است.

الف) ابتدا تصویر گنجانه اولیه به فضای رنگ مورد نظر تبدیل می‌شود.

ب) پیام مخفی (*M'*) از کانالی که در فاز تعبیه به منظور تعبیه پیام انتخاب شده است، استخراج می‌شود و با پیامی که در فاز تعبیه پنهان شده است (*M*)، مقایسه می‌شود

پ) پس از مقایسه *M* با *M'* دو حالت ممکن است اتفاق بیفتد؛ حالت اول این است که پیام تعبیه شده M در فاز تعبیه با پیام استخراج شده *M'* در فاز دیکدر داخلی، یکسان باشد که این نشان‌دهنده این است که اطلاعات بدون خطا استخراج شده‌اند. به عبارتی در این حالت پنهان‌نگاری نیاز به تصحیح خطا ندارد و الگوریتم به پایان می‌رسد. حالت دوم هنگامی است که *M* با *M'* برابر نباشد، که این نشان‌دهنده این است که بعضی از بیت‌ها با خطا استخراج شده‌اند و تصحیح خطا ضروری است. برای این منظور، پیکسل یا پیکسل‌هایی که در آن‌ها خطا رخ داده است انتخاب می‌شوند؛ سپس به منظور تصحیح خطا، مقدار کانال Y پیکسل یا پیکسل‌های مذکور، یک واحد کاهش داده

Archive of SID

www.SID.ir

می‌شود.

ت) تصویر مجدد به فضای رنگ RGB تبدیل می‌شود و مراحل فاز دیکدر داخلی تا هنگامی که BER صفر شود ادامه می‌یابد.

پس از اتمام فاز دیکدر داخلی، تصویر به فضای رنگ RGB تبدیل می‌شود و برای گیرنده ارسال می‌شود.

نتایج حاصل از اعمال الگوریتم پیشنهادی در کانال‌های مختلف فضاهای رنگ مختلف در مقایسه با تعبیه اطلاعات در فضای رنگ RGB در بخش چهارم ارائه شده است و در مورد تأثیر روش پیشنهادی در افزایش مقاومت روش پنهان‌نگاری نیز بحث شده است.

۲-۴ ۳-۲ روش نهان‌کاوی پیشنهادی

اغلب الگوریتم‌های پنهان‌نگاری که در بخش ۲ مورد مطالعه و بررسی قرار گرفتند، از همبستگی میان کانال‌های R، G و B برای کاهش تغییرات مقدار رنگ در تصاویر استفاده می‌کنند. معمولاً آن‌ها پیام را به طور مستقل در سه کانال تعبیه نمی‌کنند، بلکه به صورت همزمان پیام را در همه کانال‌ها تعبیه می‌کنند. در مقابل، اکثر روش‌های نهان‌کاوی که مورد بررسی قرار گرفتند، ویژگی‌هایشان را از فضای رنگ RGB استخراج می‌کنند و پردازش‌های مستقلی به منظور استخراج ویژگی در کانال‌های R، G و B انجام می‌دهند. این روش‌ها از همبستگی که بین کانال-های رنگ در فضای RGB وجود دارد استفاده نکرده‌اند و همچنین به ندرت از اطلاعات سایر فضاهای رنگ استفاده شده است.

در روش پیشنهادی این مقاله، ویژگی‌ها از فضاهای رنگ YUV، YIQ، YCbCr وHSV به جای فضای رنگ RGB در تصاویر استخراج می‌شوند، به این دلیل‌که این فضاهای رنگ، تغییر مقدار سه کانال R، G و B را یکپارچه می‌کنند و دارای اطلاعات بیشتری برای تصمیم گیری در مورد وجود یا عدم وجود پیام در تصویر هستند.

ایده اصلی روش پیشنهادی مبتنی بر این است که در تصاویر رنگی طبیعی همبستگی مکانی وجود دارد و هنگامی که از تبدیلات فضای رنگ استفاده می‌شود این همبستگی مکانی واضح تر می‌شود. در شکل ۱ این همبستگی مکانی در کانال I از فضای رنگ YIQ برای بخش انتخاب شده از تصویر لنا، نشان داده شده است. اگر کوچک‌ترین تغییری حتی در یکی از کانال‌های R، G یا B انجام شود باعث خواهد شد که این همبستگی مکانی از بین برود. ما از این ایده استفاده کرده‌ایم و روشی مبتنی بر همبستگی مکانی پیکسل‌های مجاور در مؤلفه‌های فضاهای رنگ مختلف پیشنهاد نمودیم که مستقل از نوع روش پنهان‌نگاری طراحی شده است.

35	0.2392	0.2407	0.2375	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2362	0.2432	0.2432
74	0.2380	0.2407	0.2362	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2409	0.2445
35	0.2380	0.2394	0.2375	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2375	0.2421	0.2432
35	0.2392	0.2394	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2432	0.2432
35	0.2369	0.2407	0.2362	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2432	0.2432
35	0.2369	0.2418	0.2362	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2351	0.2432	0.2432
22	0.2392	0.2418	0.2385	0.2362	0.2351	0.2362	0.2351	0.2375	0.2362	0.2351	0.2432	0.2432
37	0.2394	0.2445	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2445
37	0.2383	0.2445	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2445
37	0.2394	0.2445	0.2445	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2445
37	0.2394	0.2445	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432
10	0.2394	0.2457	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432
10	0.2383	0.2445	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432	0.2432

شکل ۱: همبستگی مکانی پیکسل‌های مجاور از بخش انتخاب شده از تصویر لنا در کانال I از فضای رنگ YIQ

شکل ۲: فلوچارت روش نهان‌کاوی پیشنهادی

روش نهان‌کاوی پیشنهادی، مبتنی بر یادگیری نظارتی است که دارای دو فاز یادگیری و آزمایش است. فلوچارت کلی روش نهان‌کاوی پیشنهادی مطابق شکل ۲ است. بر اساس شکل ۲ در

www.SID.ir

فاز یادگیری، پایگاه داده‌ای از تصاویر به ماشین یادگیری داده می‌شود. ماشین یادگیری بهترین قوانین را با استفاده از این تصاویر یاد می‌گیرد که خروجی آن یک طبقه‌بندی‌کننده آموزش داده شده است. این طبقه‌بندی‌کننده آموزش داده شده در فاز آزمایش به منظور تمایز بین تصاویر پوشش و گنجانه استفاده می‌شود.

استخراج ویژگی یکی از مهم‌ترین مراحل در نهان‌کاوی است و شیوه‌ی استخراج ویژگی در روش پیشنهادی در ادامه تشریح شده است.

در مرحله اول تصویر ورودی به فضای رنگ مورد نظر تبدیل می‌شود (مثلاً یکی از فضاهای رنگ YUV، YIQ، YCbCr یا HSV). سپس برای تمام پیکسل‌های تصویر در فضای تبدیل شده، تفاضل شدت روشنایی (بردار شدت روشنایی در کانال دلخواه از فضای رنگ مورد نظر) بین پیکسل‌های مجاور محاسبه می‌شود. برای این منظور همان‌طور که در شکل ۳ نشان داده شده است، پیکسل مجاور پیکسل p در چهار جهت همسایگی با زاویه‌های صفر، ۴۵، ۹۰ و ۱۳۵ درجه (پیکسل q) در نظر گرفته می‌شود.

در مرحله دوم، مقادیر تفاضلی (برای کانالی که در مرحله قبل انتخاب شده است) محاسبه می‌شود. این مقدار را برای پیکسل مفروض P، و با در نظر گرفتن زاویه θ، $sign_\theta(p)$ می‌نامیم.

q_{135}	q_{90}	q_{45}
	P	q_0

شکل ۳: چهار همسایه پیکسل p در زاویه‌های صفر، ۴۵، ۹۰ و ۱۳۵ درجه

از آنجا که تصاویر طبیعی دارای همبستگی مکانی در پیکسل‌های مجاور می‌باشند، انتظار می‌رود که $sign_\theta$ مقدار صفر را با احتمال بیشتری نسبت به مقادیر دیگر کسب کند. ولی پس از تعبیه پیام، این همبستگی از بین می‌رود و ما انتظار وجود مقادیر مختلف برای $sign_\theta$ در تصاویر گنجانه را داریم. در واقع، علت این است که اغلب هنگام پنهان‌نگاری، پیام، بدون توجه به همبستگی کانال‌های رنگ، تعبیه می‌شود. به عبارت دیگر، تغییرات ایجاد شده در کانال‌های رنگ، مستقل از هم خواهند بود و کوچکترین تغییر در هریک از کانال‌ها باعث خواهد شد که این همبستگی مکانی از بین برود. ما از این حقیقت بهره جسته و از آن به عنوان مشخصه‌ای برای کشف وجود پیام پنهان استفاده کرده‌ایم. بدین ترتیب سه ویژگی پایه‌ای مبتنی بر همبستگی مذکور، به شرح زیر از تصویر استخراج می‌کنیم.

در مرحله‌ی اول، S_0، S_{45}، S_{90} و S_{135} طبق فرمول (۱) برای تصویری دلخواه با ابعاد $M\times N$ محاسبه می‌شود که عبارت است از نسبت تعداد پیکسل‌هایی که مقدار $sign$ محاسبه شده برای آن‌ها در زاویه مورد نظر صفر است به تعداد کل پیکسل‌های تصویر مورد نظر.

$$S_\theta = \frac{\#\left\{P \middle| sign_\theta(p)=0\right\}}{M\times N} \qquad (۱)$$

رابطه (۱)، مبنای محاسبه ویژگی‌های اصلی پیشنهادی برای نهان‌کاوی است. میانگین و واریانس چهار مقداری که بر اساس رابطه (۱) محاسبه شده اند، ویژگی اول (f_1) و دوم (f_2) را بر اساس رابطه (۲) تشکیل می‌دهند.

$$\begin{aligned}\mathbf{D} &= \left[S_0, S_{45}, S_{90}, S_{135}\right]\\ f_1 &= mean(\mathbf{D})\\ f_2 &= variance(\mathbf{D})\end{aligned} \qquad (۲)$$

به علت وجود همبستگی مکانی در تصاویر انتظار می رود در روابط فوق، f_1 در تصاویر پاک، بیش‌تر از تصاویر گنجانه و f_2 در تصاویر پاک کمتر از تصاویرگنجانه باشد.

پس از استخراج دو ویژگی مذکور در رابطه‌ی (۲)، در مرحله دوم پیامی به روش جایگزینی LSB در تصویر تعبیه می‌شود و عملیات قبل تکرار می‌شود؛ با این تفاوت که تصویر ورودی در این حالت، تصویری حاوی پیام است. تفاضل دو واریانس به دست آمده (قبل و بعد از پنهان‌نگاری)، ویژگی سوم را تشکیل می‌دهد.

$$\begin{aligned}\mathbf{D}' &= \left[S_0, S_{45}, S_{90}, S_{135}\right]\\ f_3 &= \left| Variance(\mathbf{D}) - Variance(\mathbf{D}') \right|\end{aligned} \qquad (۳)$$

در صورتی که تصویر ورودی اولیه حاوی اطلاعات مخفی باشد، انتظار می‌رود پنهان‌نگاری مجدد، تأثیر چندانی بر ویژگی‌های محاسبه شده نداشته باشد و مقدار ویژگی سوم نزدیک به صفر باشد.

پس از استخراج بردار ویژگی‌ها، انتخاب طبقه‌بندی‌کننده یکی دیگر از عناصر کلیدی در نهان‌کاوی است. در این مقاله از ماشین بردار پشتیبان (SVM) برای طبقه‌بندی داده‌ها استفاده شده است.

Archive of SID

www.SID.ir

۴ نتایج روش‌های پیشنهادی

در این بخش نتایج حاصل از روش‌های پیشنهادی برای پنهان‌نگاری و نهان‌کاوی آورده شده است. آزمایشات انجام شده در این بخش برای روش‌های پیشنهادی و سایر روش‌هایی که به منظور مقایسه با این روش‌ها آورده شده است، در شرایط کاملاً یکسانی انجام شده است و کلیه روش‌ها با استفاده از نرم افزار Matlab پیاده‌سازی شده‌اند.

۴-۵-۲-۱ نتایج پنهان‌نگاری در فضاهای رنگ مختلف

در این بخش نتایج حاصل از پیاده‌سازی پنهان‌نگاری در کانال‌های مختلف فضاهای رنگ RGB، YUV، YCbCr، YIQ و HSV مورد بررسی قرار داده شده است. معیارهای مقایسه در این بخش MSE، PSNR و BER می‌باشند که محاسبه آن‌ها برای تصویر I با ابعاد $M\times N$ طبق روابط زیر صورت می گیرد.

$$MSE = \frac{\sum_{k\in\{R,G,B\}}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_k(i,j)-I'_k(i,j)\right)^2}{3\times M\times N} \qquad (۴)$$

در فرمول (۴)، I تصویر اصلی و I' تصویر پس از پنهان‌نگاری است.

PSNR نیز بر اساس رابطه (۵) به دست می‌آید.

$$PSNR = 10\ \log\frac{\left(2^n-1\right)^2}{MSE} \qquad (۵)$$

معیار BER به منظور محاسبه‌ی خطای حاصل از تعبیه و بازیابی اطلاعات از تصویر استفاده می‌شود و به صورت درصد بیت‌های اشتباه استخراج شده از تصویر، نسبت به کل بیت‌های تعبیه شده در تصویر پوشش بیان می‌شود که رابطه آن در (۶) آمده است.

$$BER = \left(\left(\sum_{i=1}^{l}\left(M(i)-M'(i)\right)^2\right)\Big/_{L}\right)\times 100 \qquad (۶)$$

در فرمول (۶)، $M(i)$، i اُمین بیت پیام تعبیه شده در تصویر و $M'(i)$، i اُمین بیت پیام استخراج شده است. همچنین L طول پیام (تعداد کل بیت‌های تعبیه شده در تصویر) است.

از معیارهای MSE و PSNR برای تعیین کیفیت تصاویر پنهان‌نگاری شده و از معیار BER برای اندازه گیری خطا در هنگام استخراج اطلاعات استفاده می‌شود. بدیهی است هرچه مقدار BER کمتر و PSNR بیشتر باشد، روش بهتر و مطلوب‌تر است.

پنهان‌نگاری در فضاهای رنگ مختلف با استفاده از نرم‌افزار Matlab پیاده‌سازی شده است و برای انجام آزمایشات پیامی با ۳۳۳۷۹۲ بیت در ۹۵۰ تصویر رنگی ۲۴ بیتی با اندازه‌ی ۶۸۴×۴۸۸ و برعکس، تعبیه شده است (یعنی در یک کانال به طور کامل تعبیه انجام می‌شود) که نتایج آن در جدول ۱ آورده شده است.

مقادیری که در جدول ۱ موجود است، میانگین مقادیر حاصل از اعمال الگوریتم بر ۹۵۰ تصویر مختلف در کانال‌های مختلف فضاهای رنگ با تعبیه یک بیت در هر پیکسل است. همچنین مقدار BER به درصد بیان شده است. به عنوان مثال اگر BER در کانال Y از فضای رنگ YUV برابر ۰.۱۶ درصد است بدین معنی است که در هنگام استخراج اطلاعات از کانال، اطلاعات به طور میانگین در ۹۵۰ تصویر با ۰.۱۶ درصد خطا استخراج شده است. همچنین مقدار PSNR بیان‌کننده مقدار PSNR در کل تصویر است. به عنوان مثال اگر مقدار PSNRY در فضای رنگ YUV برابر ۴۷.۷۵ است یعنی مقدار PSNR به طور میانگین در کل ۹۵۰ تصویر اعمال شده است (یعنی در هر سه کانال فضای رنگ YUV و نه فقط در کانال Y).

همان‌طور که در جدول ۱ نشان داده شده است و با توجه به مقادیر PSNR و BER هر کانال می‌توان نتیجه گرفت که فضای رنگ RGB مناسب‌ترین فضای رنگ از نظر ظرفیت پنهان‌نگاری است؛ زیرا در این فضای رنگ BER در هر سه کانال برابر صفر است و مقدار PSNR آن‌ها نیز بالا است.

پس از فضای رنگ RGB، فضای رنگ HSV مناسب است؛ به این دلیل که BER در کانال V از این فضای رنگ برابر صفر است. علت این نتیجه این است که این کانال در هنگامی که تبدیلات فضای رنگ RGB به HSV و برعکس انجام می‌شود وابسته به دو کانال دیگر یعنی H و S نیست. اما باید به این نکته توجه داشت که در فضای رنگ HSV دو کانال S و H با توجه به BER بالایی که دارند به هیچ عنوان قابل استفاده نیستند. علت خطای موجود در این دو کانال به خاطر خطای گرد کردن در هنگام تبدیلات فضاهای رنگ است.

Archive of SID

www.SID.ir

بر اساس نتایج جدول ۱، مقادیر PSNR و BER در فضاهای رنگ YUV و YCbCr خیلی نزدیک به هم هستند. علت این امر، شباهت این دو فضای رنگ از نظر تبدیلات است. این دو فضای رنگ بعد از فضای رنگ HSV مناسب‌تر هستند؛ زیرا مقدار BER در این دو فضای رنگ بسیار پایین است. در این دو فضای رنگ، به ترتیب کانال Y (در فضای رنگ YUV و YCbCr) و سپس کانال‌های V و Cr و سرانجام کانال‌های U و Cb برای پنهان‌نگاری مناسب هستند. در فضای رنگ YIQ، کانال Y تا حدی برای پنهان‌نگاری مناسب است، در حالی‌که دو کانال I و Q برای پنهان‌نگاری مناسب نیستند. علت آن وجود BER زیاد در این دو کانال است. علت وجود BER در فضاهای رنگ YUV، YCbCr، YIQ و HSV به خاطر تبدیلات و خطای گرد کردن در هنگام تبدیلات است.

جدول ۱: مقایسه پنهان‌نگاری در فضاهای رنگ مختلف

فضای رنگ			
RGB	PSNR R	PSNR G	PSNR B
	۷۹.۵۵	۷۹.۵۵	۷۹.۵۵
	BER R	BER G	BER B
	صفر	صفر	صفر
YUV	PSNR Y	PSNR U	PSNR V
	۷۵.۴۷	۷۵.۴۷	۴۱.۴۸
	BER Y	BER U	BER V
	۱۶.۰	۳۹.۰	۴۰.۰
YcbCr	PSNR Y	PSNR Cb	PSNR Cr
	۵۶.۴۷	۷۵.۴۷	۴۱.۴۸
	BER Y	BER Cb	BER Cr
	۱۶.۰	۳۹.۰	۴۰.۰
YIQ	PSNR Y	PSNR I	PSNR Q
	۳۵.۴۹	۷۵.۴۷	۴۱.۴۸
	BER Y	BER I	BER Q
	۴۸.۰	۳۹۴.۰	۸۹.۳
HSV	PSNR H	PSNR S	PSNR V
	۸۴۵۰.۵۴	۴۲۶۶.۵۷	۲۹۰۶.۵۱
	BER H	BER S	BER V
	۹۳.۲۴	۴۶.۳۷	صفر
YUV modified	PSNR Y	PSNR U	PSNR V
	۹۰.۴۷	۸۹.۴۷	۵۷.۴۸
	BER Y	BER U	BER V
	صفر	صفر	صفر
YCbCr modified	PSNR Y	PSNR Cb	PSNR Cr
	۸۲.۴۷	۸۱.۴۷	۴۷.۴۸
	BER Y	BER Cb	BER Cr
	صفر	صفر	صفر

Archive of SID

www.SID.ir

در جدول ۱ نتایج روش پیشنهادی با YUV و YCbCr با دیکدر داخلی، YUV modified و YCbCr modified برای تصحیح خطا نیز نشان داده شده است. این دو روش فاز دیکدر داخلی را بر خلاف روش هایی که نتایج آن در سطرهای قبل نشان داده شده بود، به کار برده اند. علاوه بر اینکه خطای این دو روش صفر شده است، مقدار PSNR آنها نیز از روشی که به طور مستقیم پنهان‌نگاری را انجام می‌دهد، بیشتر است. در نتیجه این روش برای پنهان‌نگاری مناسب‌تر است.

یکی از نیازهای اصلی سیستم پنهان‌نگاری، مقاومت در برابر حملات نهان کاوی است. در این مقاله برای سنجش مقاومت پنهان‌نگاری در کانال‌های مختلف فضاهای رنگ مختلف، از روش‌های نهان‌کاوی WS [۳۵] و Sample Pair [۲۸] که دو روش نهان‌کاوی متداول و موفقند و همچنین روش نهان‌کاوی پیشنهادی این مقاله بر اساس استخراج ویژگی از کانال I از فضای YIQ، که در بخش ۲.۳ برای نهان‌کاوی ارائه شد، استفاده شده است (علت انتخاب کانال I از فضای رنگ YIQ این است که این کانال، بهترین نرخ تشخیص را دارد).

برای این منظور، همان ۹۵۰ تصویری که در مرحله قبل در کانال‌های مختلف در فضاهای رنگ مختلف پنهان‌نگاری شده‌اند مورد آزمایش قرار داده شده‌اند که نتایج آن در جدول ۲ آورده شده است. مقادیری که در جدول ۲ موجود است، میانگین مقادیر حاصل از اعمال الگوریتم بر ۹۵۰ تصویر مختلف در کانال-های مختلف فضاهای رنگ مختلف است.

همان‌طور که در جدول ۲ نشان داده شده است، اگر پنهان-نگاری به طور مستقیم در فضای رنگ RGB انجام شود به راحتی توسط نهان‌کاوها قابل تشخیص خواهد بود؛ اما در فضاهای رنگی که از ضرایب تبدیلات استفاده شده است، تشخیص پیام تعبیه شده سخت‌تر می‌شود. در نتیجه پنهان‌نگاری در فضاهای رنگ YUV، YCbCr، YIQ و HSV نسبت به RGB دارای مقاومت بیشتری در مقابل نهان‌کاوها است. همچنین نتایج حاصل از روش پنهان‌نگاری پیشنهادی با YUV Modified و YCbCr Modified نشان داده شده است.

در مجموع با توجه به مطالعات و پیاده‌سازی‌هایی که در حوزه پنهان‌نگاری درتصاویر رنگی در فضاهای رنگ مختلف انجام شده است نتایج زیر به دست آمده اند.

جدول ۲: نتایج نهان‌کاوی بر روی روش پنهان‌نگاری در فضاهای رنگ مختلف (درصد تشخیص)

فضای رنگ	درصدِ تشخیص مبتنی بر نهان کاوی Sample pair بر اساس کانال پنهان نگاری شده			درصدِ تشخیص مبتنی بر نهان کاوی WS بر اساس کانال پنهان نگاری شده			درصدِ تشخیص مبتنی بر روش نهان کاوی پیشنهادی بر اساس کانال پنهان نگاری شده		
RGB	کانال R	کانال G	کانال B	کانال R	کانال G	کانال B	کانال R	کانال G	کانال B
	71.37	78.10	93.93	41.58	99.15	12.63	80.94	81.15	80.94
YUV	کانال Y	کانال U	کانال V	کانال Y	کانال U	کانال V	کانال Y	کانال U	کانال V
	56.42	27.05	66.42	35.89	39.47	39.15	26.74	78.84	79.36
YCbCr	کانال Y	کانال Cb	کانال Cr	کانال Y	کانال Cb	کانال Cr	کانال Y	کانال Cb	کانال Cr
	56.31	27.05	68.63	36.00	39.58	38.95	26.95	78.84	79.24
YIQ	کانال Y	کانال I	کانال Q	کانال Y	کانال I	کانال Q	کانال Y	کانال I	کانال Q
	66.00	27.26	28.63	48.94	6.90	10.34	13.24	78.73	66.10
HSV	کانال H	کانال S	کانال V	کانال H	کانال S	کانال V	کانال H	کانال S	کانال V
	34.10	42.84	85.16	32.42	34.10	70.52	22.84	21.37	25.27
YUV Modified	کانال Y	کانال U	کانال V	کانال Y	کانال U	کانال V	کانال Y	کانال U	کانال V
	56.42	27.05	67.89	36	39.57	39.05	26.84	78.84	79.36
YCbCr Modified	کانال Y	کانال Cb	کانال Cr	کانال Y	کانال Cb	کانال Cr	کانال Y	کانال Cb	کانال Cr
	56.31	27.05	68.63	36.00	39.47	38.94	26.94	78.74	79.26

www.SID.ir

پنهان‌نگاری در فضای رنگ RGB به دلایل زیر نسبت به سایر فضاهای رنگ برتری دارد.

الف) BER در این فضای رنگ برابر صفر است.

ب) ظرفیت پنهان‌نگاری بالایی نسبت به سایر فضاهای رنگ دارد.

پ) مقدار PSNR بالایی دارد (کیفیت تصویر بالا است).

ت) پیچیدگی محاسباتی در این فضای رنگ پایین است (به دلیل این که نیاز به تبدیل فضا ندارد).

از طرف دیگر، فضاهای رنگ غیر از RGB مقاومت خوبی در برابر روش‌های نهان‌کاوی متداول دارند. از طرق دیگر به دلیل تبدیلاتی که از فضای رنگ RGB به فضای رنگ دیگر انجام می‌شود، خود این تبدیلات می‌تواند به عنوان کلید رمز باشد و سربار مدیریت کلید نداشته باشیم.

کانال V در فضای رنگ HSV برای پنهان‌نگاری مناسب است، زیرا BER در این کانال برابر صفر است و مقاومت آن نسبت به کانال‌های فضای رنگ RGB بیشتر است.

همچنین با توجه به روش پنهان‌نگاری پیشنهادی، پنهان‌نگاری در کانال‌های مختلف فضاهای رنگ YUV و YCbCr مناسب است، زیرا BER به صفر رسانده شده است و مقاومت آن‌ها نسبت به کانال‌های فضای رنگ RGB بیشتر است.

به طور کلی اشکال پنهان‌نگاری در فضاهای رنگی که از ضرایب تبدیلات استفاده می‌کنند، وجود BER در هنگام استخراج اطلاعات است و علت آن وجود خطای گرد کردن به هنگام تبدیلات RGB به فضای رنگ مورد نظر و برعکس است. البته در روش پیشنهادی این مقاله، BER در دو فضای رنگ YUV و YCbCr به صفر رسیده است؛ ولی در فضای رنگ YIQ و کانال‌های H و S فضای رنگ HSV همچنان BER وجود دارد.

با توجه به جمع‌بندی فوق، به منظور استفاده از یک روش مقاوم پنهان‌نگاری تصاویر رنگی، استفاده از کانال V فضای رنگ HSV و کانال‌های Y ، Cb و Cr از فضاهای رنگ YCbCr و کانال‌های Y ، U و V از فضای رنگYUV مناسب می‌باشد.

۲-۶-۴-۲ نتایج حاصل از روش نهان‌کاوی پیشنهادی

در این بخش نتایج حاصل از روش نهان‌کاوی پیشنهادی در کانال‌های مختلف فضاهای رنگ مختلف برای تشخیص جایگزینی LSB تصادفی و تطبیق LSB تصادفی آورده شده است. به دلیل این‌که نهان‌کاوی به منظور طبقه‌بندی تصاویر در دو دسته تصاویر پاک و تصاویر پنهان‌نگاری شده استفاده می‌شود، باید همانند سایر طبقه‌بندی‌کننده‌ها شامل دو مرحله‌ی یادگیری و آزمایش باشد. در این مقاله برای مرحله یادگیری طبقه‌بندی کننده، ۱۰۰ تصویر رنگی [۳۳] با اندازه ۶۸۴×۴۸۸ و برعکس استفاده شده است که ۵۰٪ از این تصاویر به صورت تصادفی انتخاب شده و پنهان‌نگاری در آن‌ها به روش جایگزینی LSB به صورت تصادفی انجام می‌شود. آموزش SVM برای نرخ‌های تعبیه ۱۰٪، ۲۰٪، ۳۰٪، ... و۱۰۰٪ به طور مستقل انجام می‌شود. منظور از نرخ پنهان‌نگاری، نسبت طول بردار پیام مخفی به طول بردار حاصل از کم ارزش‌ترین بیت در پیکسل‌های تصویر پوشش است. علاوه بر آموزش جایگزینی LSB، آموزش روش تطبیق LSB نیز به همین صورت انجام گرفته است.

برای تعیین دقت روش‌های نهان‌کاوی مختلف، در مرحله آزمایش،۹۵۰ تصویر مختلف [۳۳] دیگر انتخاب شده است که هر کدام در دو حالت پاک و گنجانه به طبقه‌بندی کننده ارائه می‌شوند. ارزیابی نهان‌کاوی براساس ماتریس اغتشاش (Confusion Matrix) در جدول ۳ و با استفاده از معیار میزان درستی (accuracy rate) (رابطه ۷) و همچنین منحنی ROC انجام می‌پذیرد.

جدول ۳ : ماتریس اغتشاش

True Type			
Detected		Stego	Cover
	Stego	TP	FP
	Cover	FN	TN

$$AccuracyRate = \frac{TP + TN}{TP + FN + TN + FP} \qquad (۷)$$

در فرمول (۷)، TP (True Positive) به این معنا است که تصویر گنجانه به صورت درست به عنوان تصویر گنجانه طبقه‌بندی شده است؛ FN (False Negative) به این معناست که تصویر گنجانه به صورت اشتباه به عنوان تصویر پوشش طبقه‌بندی شده است؛ TN (True Negative) نشان‌دهنده آن است که تصویر پوشش به صورت درست به عنوان تصویر پوشش طبقه‌بندی شده است و FP (False Positive) به این معناست که تصویر پوشش به صورت اشتباه به عنوان تصویر گنجانه طبقه‌بندی شده است.

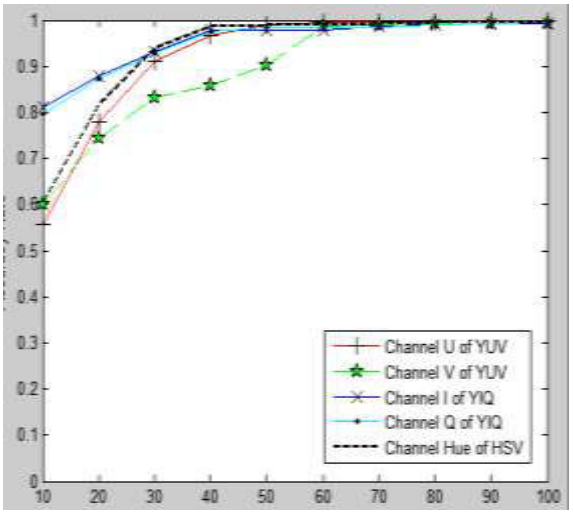
Archive of SID

www.SID.ir

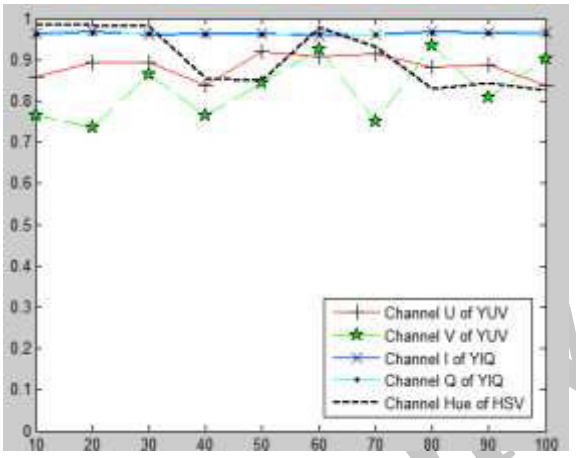
در شکل‌های ۴ و ۵، نمودار میزان درستی برای تشخیص جایگزینی LSB تصادفی و تشخیص تطبیق LSB تصادفی آورده شده است.

همان‌طور که در شکل‌های ۴ و ۵ نشان داده شده است، ویژگی‌هایی که از کانال I از فضای رنگ YIQ استخراج شده است، بیشترین نرخ تشخیص کلی در تشخیص جایگزینی LSB تصادفی و تشخیص تطبیق LSB را دارد. سپس به ترتیب کانال Q از فضای رنگ YIQ، کانال H از فضای رنگ HSV و کانال‌های U و V از فضای رنگ YUV قرار دارند.

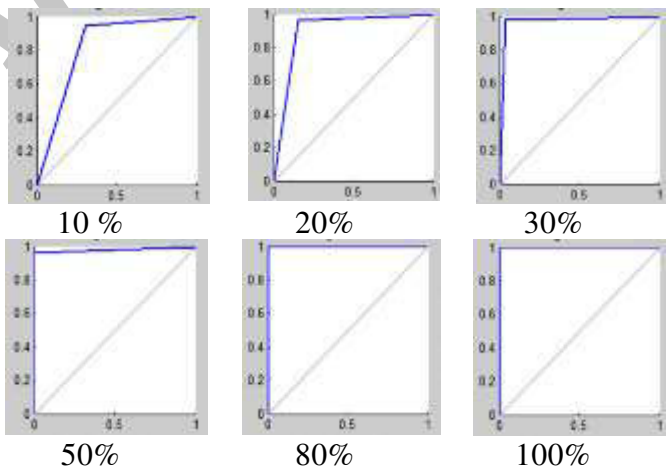
در شکل‌های ۶ و ۷، نمودار ROC نرخ‌های تعبیه ۱۰٪، ۲۰٪، ۳۰٪ ۵۰٪، ۸۰٪ و ۱۰۰٪ براساس استخراج ویژگی از کانال I از فضای رنگ YIQ آورده شده است (بدین علت که کانال I از فضای رنگ YIQ، بیشترین کارایی را در تشخیص جایگزینی LSBتصادفی و تطبیق LSB تصادفی دارد، انتخاب شده است). شکل‌های ۶ و ۷، بیان‌گر این موضوع هستند که روش نهان‌کاوی پیشنهادی، با تعداد ویژگی بسیار کم توانسته است روش‌های جایگزینی LSB و تطبیق LSB را بسیار خوب تشخیص دهد. این درحالی است که روش‌های نهان‌کاوی تطبیق LSB با تعداد ویژگی‌های زیاد، نرخ تشخیص خوبی ندارند.به طور کلی با توجه به آزمایشات انجام شده با استفاده از اطلاعات فضاهای رنگ مختلف در حوزه نهان‌کاوی تصاویر رنگی، نتایج زیر به دست آمده است.



شکل۴: نمودار میزان درستی بر اساس نرخ تعبیه برای تشخیص جایگزینی LSB تصادفی



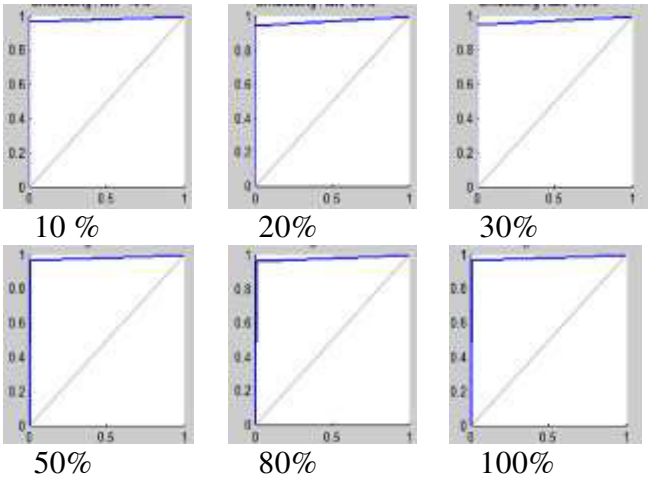
شکل ۵: نمودار میزان درستی بر اساس نرخ تعبیه برای تشخیص تطبیق LSB تصادفی



شکل ۶: ROC روش پیشنهادی با تعبیه به روش جایگزینی LSB تصادفی با نرخ‌های تعبیه مختلف (محور افقی میزان FP و محور عمودی میزان TP)

Archive of SID

www.SID.ir



شکل ۷: ROC روش پیشنهادی با تعبیه به روش تطبیق LSB تصادفی با نرخ‌های تعبیه مختلف (محور افقی میزان FP و محور عمودی میزان TP)

کانال I از فضای رنگ YIQ بهترین نرخ تشخیص را در هر دو روش جایگزینیLSB تصادفی و تطبیق LSB تصادفی دارد. سپس کانال Q از فضای رنگ YIQ بهترین نرخ تشخیص را در هر دو روش جایگزینیLSB تصادفی و تطبیق LSB تصادفی دارد. در واقع عملکرد مؤلفه رنگ اصلی به منظور نهان‌کاوی بهتر از مؤلفه روشنایی می‌باشد و در بین مؤلفه‌های رنگ، مؤلفه I که رنگ اصلی است و اطلاعات بیشتری نسبت به Q دارد، دارای نرخ تشخیص بالاتری است.

از جمله مزایای استخراج ویژگی از کانال I از فضای YIQ پایداری تشخیص است، یعنی در نرخ‌های تعبیه مختلف دارای نرخ تشخیص تقریباً یکسانی است. این در حالی است که در اکثر روش‌های نهان‌کاوی این مورد نقض می‌شود.

پس از کانال I و Q از فضای رنگ YIQ، به ترتیب کانال H از فضای رنگ HSV و کانال‌های U و V از فضای رنگ YUV دارای نرخ تشخیص خوبی در تشخیص روش جایگزینی LSB تصادفی و تشخیص تطبیق LSB تصادفی هستند.

کانال H در فضای رنگ HSV در نرخ‌های تعبیه ۱۰٪ و ۲۰٪ درصد دارای نرخ تشخیص خیلی بالا برای جایگزینی LSB تصادفی نیست؛ اما در نرخ‌های ۳۰٪ تا ۱۰۰٪ درصد دارای نرخ تشخیص بسیار بالاست.

کانال Y در فضاهای رنگ YIQ، YUV و YCbCr و کانال S و V از فضای رنگ HSV نتایج مطلوبی نداشته و به همین دلیل نتایج آن‌ها ترسیم نشده است. در واقع بر اساس ویژگی‌هایی که ما در مؤلفه‌های رنگ و روشنایی استخراج کردیم، مؤلفه‌های رنگ به منظور نهان‌کاوی مؤثرتر از مؤلفه روشنایی عمل می‌کنند.

روش پیشنهادی علاوه بر تشخیص جایگزینی LSB تصادفی، در تشخیص تطبیق LSB تصادفی نیز دارای نتایج خوبی است. این در حالی است که روش‌های تشخیص تطبیق LSB، با تعداد زیادی ویژگی پیچیده به سختی این نوع پنهان-نگاری را تشخیص می‌دهند.

به منظور دستیابی به نرخ بالای تشخیص بیشتر، سناریوهای ترکیبی (از جمله I+Q، I+U، I+V، I+S و U+V و ...) از کانال‌های رنگ مورد آزمایش قرار گرفتند که در سناریوهایی که I وجود داشت نرخ تشخیص نهان‌کاوی افزایش می‌یافت اما از نتایج مؤلفه I به تنهایی بهتر نبودند و به همین دلیل از ذکر نتایج آن صرف نظر شده است.

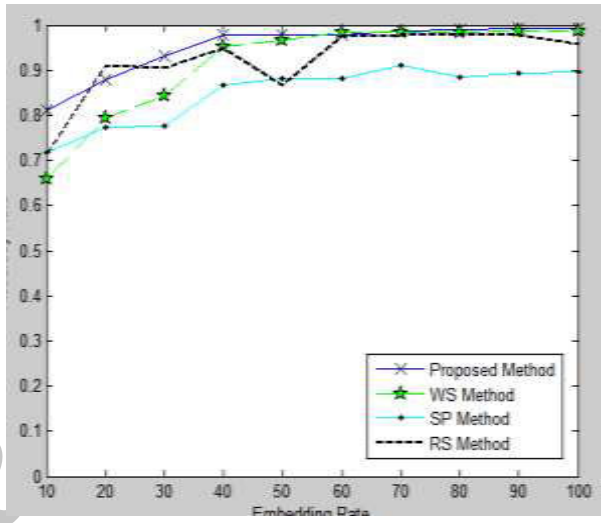
۲-۷ ۴-۳ نتایج حاصل از مقایسه روش نهان‌کاوی پیشنهادی با چند روش دیگر

در این بخش نتایج حاصل از مقایسه روش‌های نهان‌کاوی پیشنهادی با روش‌های نهان‌کاوی WS [۳۵] ، SP [۲۸] و RS [۲۱] آورده شده است. همچنین در روش‌های نهان‌کاوی RS، SP و WS، استخراج ویژگی از هر یک از کانال‌های تصویر رنگی (کانال R، G وB) به طور مستقل انجام می‌شود و بردار ویژگی را تشکیل می‌دهند. برای تعیین دقت روش‌های نهان‌کاوی مختلف، در این بخش نیز از معیار میزان درستی استفاده کرده‌ایم، که این معیار نشان‌دهنده‌ی تشخیص کلی روش‌ها در تشخیص جایگزینی LSB است (شکل ۸).

Archive of SID

www.SID.ir

همانطور که در شکل ۸ نشان داده شده است، روش نهان-کاوی پیشنهادی مبتنی بر استخراج ویژگی از فضای رنگ دارای بیشترین دقت است. از آن جایی که روش‌های WS، SP و RS به منظور تشخیص جایگزینی LSB به کار رفته‌اند بنابراین از مقایسه روش نهان‌کاوی پیشنهادی به منظور تشخیص تطبیق LSB صرف نظر شده است و این در حالی است که روش‌های نهان‌کاوی پیشنهادی دارای قدرت تشخیص بالایی در تشخیص تطبیق LSB هستند (در شکل ۵ نمودار تشخیص تطبیق LSB توسط روش پیشنهادی نشان داده شده است).



شکل ۸: نمودار میزان درستی برای تشخیص جایگزینی LSB تصادفی

۵ نتیجه گیری

در این مقاله، از اطلاعات فضاهای رنگ مختلف به منظور پنهان‌نگاری و نهان‌کاوی استفاده شده است. در زمینه پنهان-نگاری یک روش مقاوم پنهان‌نگاری در فضاهای رنگ مختلف پیشنهاد شده است که ایده اصلی به منظور پنهان‌نگاری این است که تصویر پوشش از فضای رنگ RGB به فضای رنگ دیگری تبدیل شود و در یک کانال از آن فضای رنگ با استفاده از الگوریتم LSB تعبیه انجام شود و پس از تعبیه، تصویر مجدداً به فضای رنگ RGB تبدیل شود. استفاده از تبدیلات فضای رنگ باعث امنیت بیشتر روش پنهان‌نگاری در مقابل روش‌های نهان-کاوی می شود. همچنین می توان از ضرایب تبدیلات به عنوان کلید رمز استفاده کرد. مشکلی که در استفاده از فضاهای رنگ غیر از RGB، وجود دارد وجود خطای BER است که در این مقاله با انجام اصلاحاتی در روال تعبیه پیام، BER در دو فضای رنگ YUV و YCbCr به صفر رسیده است.

در زمینه نهان‌کاوی نیز، روش نهان‌کاوی پیشنهاد شده است که ویژگی‌ها را از سایر فضاهای رنگ (از جمله فضاهای رنگ YUV، YIQ، YCbCr و HSV) به جای فضای رنگ RGB استخراج می‌کند. پایه روش پیشنهادی، مبتنی بر همبستگی مکانی پیکسل‌های مجاور در مؤلفه‌های فضاهای رنگ مختلف است و مستقل از نوع روش پنهان‌نگاری طراحی شده است. این فضاهای رنگ از تجزیه مؤلفه‌های رنگ و روشنایی بهره برده که در نتیجه باعث حذف همبستگی بین کانال‌های R، G و B از فضای رنگ RGB می‌شود. همچنین این فضاهای رنگ، اثرات یک روش پنهان‌نگاری را یکپارچه می‌کنند، بنابراین اطلاعات مفیدتری برای نهان‌کاوی در مقایسه با استخراج ویژگی از فضای رنگ RGB فراهم می‌کنند. نتایج حاصل از روش پیشنهادی نشان داد که این روش دارای قدرت تشخیص خوبی به منظور نهان‌کاوی تصاویر رنگی است. روش نهان‌کاوی پیشنهادی، حتی در نرخ‌های تعبیه پایین نیز از دقت قابل توجهی برخوردار است.

به منظور پیشنهادات ادامه کار در زمینه پنهان‌نگاری، می‌توان از یک کانال به عنوان کانال تنظیم‌کننده، استفاده کرد و در دو کانال دیگر تعبیه انجام شود. به منظور افزایش مقاومت نیز می-توان از روش‌های دیگر (غیر از LSB) استفاده کرد؛ به عنوان مثال می‌توان از فضای فرکانس به منظور تعبیه استفاده کرد.

مراجع

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography", Proc. Int. Conf. on Fifth Annual Information Security South Africa Conference(ISSA2005), Sandton, South Africa, 2005.

[2] Duncan Sellars, "An Introduction to Steganography", 2001, [Online]. Availible: http://www.zoklet.net/ totse/ en/ privacy/encryption/163947.html [Accessed: April 2011].

[3] J. D. Boissonnat and C. Delage, Essentials Of Image Steganalysis Measures, Journal of Theoretical and Applied Information Technology, 2010.

[4] Andrew D. Ker, "Resampling and the Detection of LSB Matching in Colour Bitmaps", Proceedings on Security, Steganography, and Watermarking of Multimedia Contents VII, pp.1-15, 21 March 2005.

[5] G.C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner", Forensic Science Communications, Vol. 6, No. 3,July 2004.

[6] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing: Spotlight, pp. 75-80, May-June 2001.

[7] K. Bailey, K. Curran, "An Evaluation of Image Based Steganography Methods", Multimedia Tools

Archive

www.SID.ir

[8] Mehdi Hussain, Mureed Hussain," Pixel Intensity Based High Capacity Data Embedding Method", Proc. Int. Conf. on Information and Emerging Technologies(ICIET), Karachi, pp. 1-5, 2010.

[9] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, Hamilton, New Zealand, pp.11- 19, 2006.

[10] Babita Ahuja, Manpreet Kaur, Manav Rachna "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[11] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, "Pixel indicator high capacity technique for RGB image based Steganography", 5 th IEEE International Workshop on Signal Processing and its Applications(WoSPA),University of Sharjah, Sharjah, U.A.E. 2008.

[12] Mohammad Tanvir Parvez , Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, 2008

[13] Gandharba Swain and Saroj Kumar Lenka, "A Novel Approach to RGB Channel Based Image Steganography Technique", International Arab of e-Technology,Vol 2,N0.4,pp.181-186, 2012.

[14] Atallah M. Al-Shatnawi , "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, pp.3907 – 3915, 2012.

[15] XIE Qing , XIE Jianquan, XIAO Yunhua, "A High Capacity Information Hiding Algorithm InColor Image", Proc. Int. Conf. on eBusiness and Information System Security (EBISS), pp. 1-4 , 2010.

[16] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, "Triple - A: Secure RGB Image Steganography Based on Randomization", IEEE/ACM international conference on computer systems and applications, pp. 400 - 403, 2009.

[17] Ali Akbar Nikoukar, "An Image Steganography Method with High Hiding Capacity Based on RGB Image", International Journal of Signal and Image Processing , pp. 238-241, 2010.

[18] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu, Daniel Borca, "Steganography in YUV color space" ,IEEE International Workshop on Robotic and Sensors Environments, Ottawa,CA, pp. 1-4, 2007.

[۱۹] سید محمد علی جوادی، مریم حسن زاده، "پنهان نگاری مقاوم اطلاعات در تصاویر رنگی با استفاده از فضاهای رنگ مختلف"، چهارمین کنفرانس فناوری اطلاعات و دانش، دانشگاه صنعتی نوشیروانی بابل، بابل، ایران، خرداد ۱۳۹۱.

[20] J. Fridrich, R. Du and M. Long, "Steganalysis of LSB Encoding in Color Images", Proceedings of ICME , New York, USA, 2000

[21] J. Fridrich, M. Goljan and R.Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images", Proc.of the ACM Workshop on Multimedia and Security, Ottawa,CA, pp. 27–30, 2001

[22] M.Abolghasemi, H.aghainia, K.Faez, M.A.Mehrabi, "LSB Data Hiding Detection Based On Gray Level Co-Occurrence Matrix", International Symposium On Telecommunications,2008, pp. 656- 659, 2008

[23] H.B.Kekre, A.A.Athawale and S.A.Patki," Steganalysis of LSB Embedded Images Using Gray Level Co-Occurrence Matrix", International Journal of Image Processing (IJIP), vol 5, pp.36-45, 2011

[24] Mitra S., Roy T. K., Mazumdar D. and Saha A. B. "Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis", IITKHACK04, pp. 23 – 24, 2004.

[25] KB Raja, Shankara N, Venugopal KR and L MPatnaik,"Steganalysis of LSB Embedded Images Using Variable Threshold Color Pair Analysis", Fourth International Conference on Intelligent Sensing and Information Processing(ICISIP), pp 11-16,2006.

[26] Geetha, S, Sivatha Sindhu, S.S.; Renganathan, R.; Janaki Raman, P.; Kamraj, N.," StegoHunter: Steganalysis of LSB Embedded Images Based on Stego-Sensitive Threshold Close Color Pair Signature ", Sixth Indian Conference on Computer Vision, Graphics & Image Processing ICVGIP, pp 281 - 288,2008

[27] H.B.Kekre, A.A.Athawale and S.A.Patki, "Improved Steganalysis Of Lsb Embedded Color Images Based On Stego-Sensitive Threshold Close Color Pair Signature", International Journal of Engineering Science and Technology (IJEST), vol. 3 ,No. 2 , pp. 836-842, 2011

[28] Sorina Dumitrescu, Xiaolin Wu and Zhe Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE Transactions on Signal Processing, Vol. 51,No. 7, pp. 1995 – 2007, July 2003.

[29] Peizhong Lu, Xiangyang Luo, Qingyang Tang and Li Shen," An Improved Sample Pairs Method for Detection of LSB Embedding ",6th International Workshop on Information Hiding,Toronro, Canada,Lecture Notes in Computer Science 3200 springer, 2005.

[30] Javadi. S.M.A, hassanzadeh . M, "Image Steganalysis Based On Color Channels Correlation In Homogeneous Areas In Color images", Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS 2012), Zanjan, Iran,2012.

[31] Xiang-Wei Kong, Wen-Feng Liu, and Xin-Gang You," Secret Message Location steganalysis Based on Local Coherences of Hue", PCM'05 Proceedings of the 6th Pacific-Rim conference on Advances in & Applications, Vol. 30, No. 1, pp. 55-88, July 2006

Archive of SID

www.SID.ir

Multimedia Information Processing , Vol 2, pp.301-311,2005

[32] Yuan-lu Tu , Sheng-rong Gong ," Universal Steganalysis Using Color Correlation andFeature Fusion", ISISE '08 Proceedings of the 2008 International Symposium on Information Science and Engieering, IEEE Computer Society Washington,DC, USA, Vol 01,pp.107-111, 2008.

[33] http://photogallery.nrcs.usda.gov.

[34] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Volume 2, April 2011.

[35] J. Fridrich and M. Goljan, "On Estimation Of Secret Message Length In LSB Steganography In Spatial Domain" in Security, Steganography, and Watermarking of Multimedia Contents VI, E. J. Delp III and P. W. Wong, eds., Proc. SPIE 5306, pp. 23-34, 2004.

Archive of SID

www.SID.ir