مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۱، بهار ۱۳۹۶، ص ۲۶-۱۹

روشی جدید برای نهان‌نگاری در تصاویر رنگی با استفاده از تبدیل ستون ترکیبی در تصویر HSV

محمدمهدی علیان‌نژادی[۱]، زهرا امیری[۲]، هدی مشایخی[۳*]

۱- دانشجوی دکتری، ۲-کارشناس ارشد، ۳- استادیار، دانشگاه صنعتی شاهرود

(دریافت: ۹۴/۱۱/۱۴، پذیرش: ۹۵/۰۸/۱۰)

چکیده

نهان‌نگاری به‌صورت گسترده در سامانه‌های امنیت اطلاعات مورد استفاده قرار می‌گیرد. در نهان‌نگاری، هدف پنهان کردن اطلاعات به‌گونه‌ای است که تنها شخص فرستنده و گیرنده از وجود ارتباط و اطلاعات مطلع باشند. نهان‌نگاری در رسانه‌های مختلفی مانند تصویر، صدا و متن صورت می‌گیرد. فرآیند پنهان‌سازی اطلاعات درون تصویر در دو حوزه مکان و تبدیل می‌تواند انجام گیرد. در روش‌های حوزه تبدیل، ابتدا تصویر اصلی توسط تبدیلی مانند تبدیل فرکانسی به فضای دیگری منتقل می‌گردد، سپس اطلاعات در ضرایب این تبدیل جاسازی می‌شوند. در این مقاله، یک روش مبتنی بر حوزه تبدیل برای پنهان کردن متن در تصویر رنگی مدل HSV ارائه شده است. بعد از تبدیل تصویر به مدل HSV، تصویر به قطعه‌هایی تقسیم شده و تبدیل ستون ترکیبی در هر قطعه اجرا می‌شود. سپس پیام مورد نظر در قطعات تبدیل‌یافته ذخیره می‌شود. نتایج ارزیابی‌ها و مقایسه‌های انجام‌شده، ظرفیت بالای ذخیره‌سازی روش پیشنهادی و افزایش امنیت در این روش را نشان می‌دهد.

واژه‌های کلیدی: نهان‌نگاری، تبدیل ستون ترکیبی، تصویر رنگی HSV

۱- مقدمه

نهان‌نگاری یک روش برای پنهان کردن پیام در رسانه است. نهان‌نگاری به مفهوم مخفی کردن اطلاعات در یک رسانه است درحالی‌که رمزنگاری به مفهوم غیرقابل فهم کردن یک پیام محرمانه است [۱]. نهان‌نگاری در رسانه‌های مختلفی مانند تصویر، صدا و متن صورت می‌گیرد. یک روش نهان‌نگاری خوب باید خصوصیات ظرفیت کافی و غیر محسوس بودن[۱] را داشته باشد [۳-۲]. از آنجایی که درک تصویری انسان از تغییرات در تصاویر محدود است بنابراین تصاویر نوعی رسانه پوششی مناسب در نهان‌نگاری محسوب می‌شوند. سه جنبه مهم در نهان‌نگاری ظرفیت، امنیت و استحکام است. از آنجایی که بهبود هم‌زمان این سه جنبه ممکن نیست، در منابع گذشته از این سه جنبه به عنوان مثلث نهان‌نگاری یاد شده است؛ به عبارت دیگر، با بهبود هر یک از این سه جنبه، یکی دیگر از جنبه‌ها و یا حتی هر دو جنبه دیگر تضعیف می‌شود [۱, ۴-۶].

در هر سامانه نهان‌نگاری باید الگوریتم‌های جاسازی و استخراج مشخص باشد. وظیفه الگوریتم جاسازی، قرار دادن پیام محرمانه در رسانه پوششی به‌صورت برگشت‌پذیر است. الگوریتم استخراج نیز پیام محرمانه را از درون رسانه حاوی پیام استخراج می‌کند. شکل (۱) بخش‌های مختلف یک سامانه نهان‌نگاری ساده پیشنهادی را نشان می‌دهد.

الگوریتم‌های نهان‌نگاری متعددی برای ساختارهای مختلف تصویر ارائه شده است [۷]. فرآیند نهان‌نگاری اطلاعات در تصویر به دو دسته روش‌های حوزه مکان و روش‌های حوزه تبدیل تقسیم می‌شوند [۹-۸]. روش‌های حوزه مکان، همان جاسازی اطلاعات در صفحات بیتی تصویر است [۱۰]. روش‌های تبدیل نیز ابتدا تصویر را با یک تبدیل (مثل تبدیل فوریه) به حوزه دیگری انتقال داده و سپس پیام را در آن جاسازی می‌کنند [۱۱]. در تحقیقات اخیر نهان‌نگاری، تأکید بر استفاده از حوزه تبدیل بوده است [۱۳-۱۲].

در این مقاله روشی برای نهان‌نگاری پیام در تصویر در حوزه تبدیل ارائه شده است. روش ارائه شده قابلیت درج پیام محرمانه در تصویر پوششی، و هم‌چنین بازیابی آن را دارد. در روش پیشنهادی ابتدا تصویر از مدل رنگ RGB به مدل رنگ HSV انتقال می‌یابد. سپس صفحه S تصویر طی تبدیل ستون ترکیبی[۲] به حوزه تبدیل برده می‌شود. پیام محرمانه در صفحه بیتی صفر صفحه S تبدیل یافته ذخیره می‌شود. نهایتاً تصویر با مدل رنگ

* رایانامه نویسنده مسئول: hmashayekhi@shahroodut.ac.ir

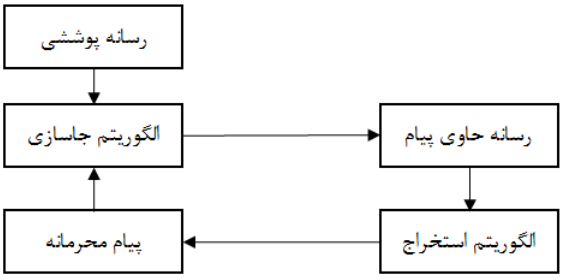
1- Imperceptibility

2- Mixed column transform

HSV با کمک تبدیل ستون ترکیبی معکوس و تبدیل مدل رنگ HSV به RGB، به مدل رنگ RGB تبدیل شده و حاوی پیام محرمانه است. در این مقاله، جاسازی پیام در مؤلفه غلظت تصویر انجام می‌شود که پس از برگرداندن تصویر از مدل HSV به مدل RGB، تأثیر کمتری بر روی کیفیت تصویر می‌گذارد. همچنین، استفاده از ضرایب تبدیلات فضای رنگ HSV باعث می شود که تشخیص پیام محرمانه سخت‌تر شود [۱۴]. استفاده از تبدیل ستون ترکیبی که بر مبنای محاسبات چند جمله‌ای کاهش‌ناپذیر است، نیازمندی‌های یک سامانه پنهان‌نگاری شامل ظرفیت بالا، پنهان‌سازی مناسب بصری و امنیت را ارائه می‌کند [۱۵]، اما استفاده از این روش در فضای رنگی HSV مورد بررسی قرار نگرفته است.

امنیت روش پیشنهادی با معیارهای کمی کیفیت تصویر و هم‌چنین یک ابزار نهان‌کاوی [۱۶] در بر گیرنده حملات آماری بررسی شده است. روش پیشنهادی در این مقاله با روش مرجع [۱۵] مقایسه شده است. در این مرجع روشی بر پایه تبدیل ستون ترکیبی و مدل رنگ RGB ارائه شده است. همچنین نتایج نهان‌کاوی روش پیشنهادی با استفاده از روش اخیراً پیشنهاد شده رده‌بندی جمعی[1] [۱۷] ارائه و مقایسه شده است. نتایج آزمایش‌ها نشان‌دهنده افزایش امنیت در روش پیشنهادی می‌باشد.

در ادامه، در بخش ۲ به معرفی روش‌های مورد استفاده در این تحقیق پرداخته شده است. روش پیشنهادی در بخش ۳ توصیف می‌شود. در بخش ۴ آزمایش‌ها و نتایج الگوریتم پیشنهادی مورد بررسی قرار می‌گیرد. نتیجه‌گیری پژوهش در بخش ۵ بیان خواهد شد.



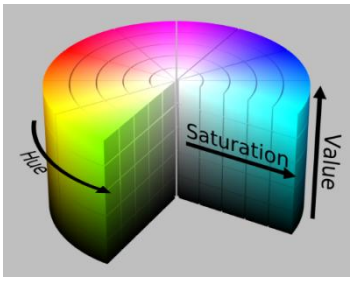
شکل (۱). یک سامانه نهان‌نگاری عمومی

۲- روش‌های پیش‌نیاز مورد استفاده

در این بخش به معرفی تبدیل ستون ترکیبی و مدل رنگی HSV و صفحات بیتی تصویر پرداخته شده است.

۲-۱- مدل رنگی HSV

مدل‌های رنگی متفاوتی به عنوان استاندارد معرفی شده‌اند. نمونه‌هایی از مدل‌های رنگی متداول عبارتند از: RGB، HSV، CMY(K)، YIQ، YCbCr و Lab. یکی از دلایل استفاده از مدل‌های رنگ متفاوت، میزان متفاوت اثرگذاری خرابی‌های مختلف بر روی هر یک از مدل‌های رنگ و مؤلفه‌های آن است. برای مثال تغییر روشنایی تصویر، هر سه مؤلفه مدل RGB را تحت تأثیر قرار می‌دهد، از این جهت برای بهسازی تصویر باید هر سه مؤلفه را به‌سازی نمود. در حالی‌که در مدل YIQ تغییر روشنایی تنها مؤلفه Y را تحت تأثیر قرار داده است. از این‌رو با به‌سازی تنها این مؤلفه، تصویر مطلوب به‌دست می‌آید. مدل رنگ HSV از سه مؤلفه طول موج رنگ[2] (H) ، غلظت[3] (S) و شدت روشنایی[4] (V) تشکیل شده است و به سامانه بینایی انسان بسیار شبیه است. هر طول موج، بیانگر یک رنگ خاص مانند قرمز، زرد و بنفش است. غلظت، درصد خلوص رنگ یا اشباع رنگ را نشان می‌دهد که مبین معیاری از درجه رقیق شدن رنگ خالص توسط نور سفید است. مؤلفه V نیز شدت روشنایی رنگ را نشان می‌دهد [۱۸]. در شکل (۲) این مدل رنگی مشاهده می‌شود. در این مقاله، جاسازی پیام در مؤلفه غلظت تصویر انجام می‌شود که پس از برگرداندن تصویر از مدل HSV به مدل RGB، تأثیر کمتری بر روی کیفیت تصویر می‌گذارد. همچنین، استفاده از ضرایب تبدیل‌های فضای رنگ HSV باعث می‌شود که تشخیص پیام محرمانه سخت‌تر شود [۱۴].



شکل (۲). مدل رنگی HSV متشکل از سه مؤلفه طول موج، غلظت و شدت روشنایی [۱۸]

۲-۲- ماتریس بیتی تصویر

تصویر یک آرایه دو بعدی از پیکسل‌هایی است که هر پیکسل یک مقدار هشت بیتی دارد. اگر همه بیت‌های اول از هشت بیت ذخیره شده برای پیکسل‌های تصویر حفظ شود و سایر بیت‌ها ارزشی معادل با صفر داشته باشند آنچه حاصل می‌شود صفحه بیتی صفر تصویر است و همین‌طور می‌توان برای بیت دوم تا هشتم این عمل را انجام داد و صفحات بیتی معادل را به‌دست آورد. آنچه اهمیت دارد دانستن این موضوع است که صفحه بیتی متعلق به بیت اول از سایر صفحات کم اهمیت‌تر است و در

1- Ensemble classification

2- Hue
3- Satuaration
4- Value

تصاویر نشان‌دهنده جزییاتی است که چشم انسان بـه سـختی آن را می‌تواند درک کند. از طرف دیگر، هرچه به صفحات بیتی بالاتر می‌رویم اهمیت آن بیشتر شده و جزییات بیشتری از تصویر را در بر دارد. از همین رو، می‌توان از این خصوصیت استفاده کـرد و در صفحات کم ارزش‌تر تصویر پیام را ذخیره نمود.

۲-۳- تبدیل ستون ترکیبی

تبدیل ستون ترکیبی یک عملیات درهم آمیختن است کـه در آن چهار بایت مربوط به هر سـتون مـاتریس ورودی بـا یکـدیگر بـر اساس یک تبدیل خطی معکوس‌پذیر ترکیب می‌شوند. به عبـارت دیگر، تبدیل ستون ترکیبی یک تابع تبدیل چهار بایتی است کـه چهار بایت را به عنوان ورودی گرفته و سـپس چهـار بایـت را بـه عنوان خروجی بر اساس ترکیب خطی ورودی‌ها محاسبه می‌کند. روش AES[1] بر مبنای تبدیل ستون ترکیبی طراحی شـده اسـت. تابع تبدیل ستون ترکیبی چهار بایت را به عنوان ورودی گرفته و چهار بایت را به عنوان خروجی تولید می‌کند که در آن هر بایـت ورودی بر روی هر یک از چهار بایت خروجی مؤثر است [۱۵]. در این روش هر ستون به عنوان یک چند جمله‌ای در حوزه گـالوانی [۱۹] در نظر گرفتـه مـی‌شـود. در بخـش ۱ و ۳ نحـوه محاسـبه تبدیل ستون ترکیبی و عکس آن توضیح داده شده است.

۳- روش پیشنهادی

روش‌های نهان‌نگاری عموماً از دو بخش قرار دادن پیام در رسـانه و استخراج پیام از رسانه تشکیل می‌شوند. در ادامه به معرفی این دو بخش پرداخته شده است. در این مقاله روشی برای نهان‌نگاری بـر مبنـای تبـدیل سـتون ترکیبـی پیشـنهاد شـده اسـت. روش پیشنهادی برای بهبود کیفیت بصری تصویر و همچنـین افـزایش امنیـت نهـان‌نگـاری از فضـای رنگـی HSV اسـتفاده مـی‌کنـد. معیارهای ارزیابی کیفیت تصویر و همچنـین ارزیـابی بـا حمـلات آماری نشان‌دهنده امنیت بالای روش پیشنهادی است.

۱-۳- مرحله قرار دادن پیام

در این قسمت پیام در تصویر نهان‌نگاری می‌شود. برای نهان‌نگاری از تبـدیل سـتون ترکیبـی اسـتفاده شـده اسـت و پیـام در کم‌ارزش‌ترین صفحه بیتی تصـویر تبـدیل یافتـه قـرار مـی‌گیـرد. الگوریتم قرار دادن پیام به صورت زیر است.

گام اول. تبدیل تصویر ورودی از مد رنگ RGB به مد رنگ HSV

در این گام، تصویر ورودی با مد رنگ RGB بـه تصـویری بـا مـد رنگ HSV تبدیل می‌شود. از آنجـایی کـه قـرار اسـت پیـامی در بیت‌های تصویر ذخیره شود، بنابراین نیاز بـه یـک تبـدیل نرمـال شده در بازه صفر تا ۲۵۵ با مقادیر صحیح وجود دارد. این تبـدیل با رابطه زیر انجام می‌شود.

$$H = \begin{cases} 0 & ,\Delta = 0 \\ round\left(255 * 60 * \left(\frac{G-B}{\Delta} mod\ 6\right)\right) & ,C_{max} = R \\ round\left(255 * 60 * \left(\frac{B-R}{\Delta} + 2\right)\right) & ,C_{max} = G \\ round\left(255 * 60 * \left(\frac{R-G}{\Delta} + 4\right)\right) & ,C_{max} = B \end{cases} \quad (۱)$$

$$S = \begin{cases} 0, \mathrm{C_{max}} = 0 \\ round\left(\frac{\Delta}{C_{max}} * 255\right) & ,C_{max} \neq 0 \end{cases} \quad (۲)$$

$$V = C_{max} \quad (۳)$$

$$C_{max} = \max(R, G, B) \quad (۴)$$

$$C_{min} = \min(R, G, B) \quad (۵)$$

$$\Delta = C_{max} - C_{min} \quad (۶)$$

اگرچه خطای کوانتیزه کردن مقادیر S و V باعث می‌شود که تبدیل پیشنهادی کامل نباشد، اما نتایج این مقاله نشان می‌دهـد که تبدیل پیشنهادی می‌تواند خطای نهان‌نگاری را کاهش دهد.

گام دوم. ساخت صفحه S تبدیل یافته

در این گام، صفحه S تصویر به بلاک‌های ۴*۴ تقسیم شـده و بـر روی هر بلاک تبدیل ستون ترکیبی انجام می‌شـود. سـپس بـا در کنار هم قرار دادن بلاک‌های تبـدیل یافتـه، صـفحه‌ای جدیـد بـا عنوان صفحه S تبدیل یافته ساخته می‌شود. انتخاب صفحه S بـر اساس آزمایش و تجربه انجام شده است. تبـدیل سـتون ترکیبـی یک ماتریس ۴*۴، به صورت زیر محاسبه می‌شود.

$$R = TA \quad (۷)$$

کـه در آن، R، T و A بـه ترتیـب مـاتریس نتیجـه تبـدیل، ماتریس تبدیل و ماتریس ورودی تبـدیل هسـتند. مقـدار عـددی ماتریس تبدیل و همچنـین مـاتریس بسـط یافتـه T و R در زیـر مشخص است.

$$\underbrace{\begin{bmatrix} r_{00} & r_{01} & r_{02} & r_{03} \\ r_{10} & r_{11} & r_{12} & r_{13} \\ r_{20} & r_{21} & r_{22} & r_{23} \\ r_{30} & r_{31} & r_{32} & r_{33} \end{bmatrix}}_{Result\ Matrix} = \quad (۷)$$

$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{Transform\ Matrix} \times \underbrace{\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}}_{Input\ Data}$$

1- Advanced Encryption Standard

فرض کنید قرار است نتیجه تبدیل برای ورودی زیر محاسبه شود.

$$\underbrace{\begin{bmatrix} 06 & A2 & B0 & 2F \\ A4 & 42 & C2 & F0 \\ 45 & 23 & D3 & B3 \\ 09 & 34 & DB & AB \end{bmatrix}}_{Input\ Data}$$

در اولین مرحله برای محاسبه مقادیر ماتریس نتیجه تبدیل، مقادیر ماتریس انتقال و ماتریس بلاک ورودی به صورت چند جمله‌ای نوشته می‌شوند.

$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{Transform\ Matrix} \times \underbrace{\begin{bmatrix} 06 & A2 & B0 & 2F \\ A4 & 42 & C2 & F0 \\ 45 & 23 & D3 & B3 \\ 09 & 34 & DB & AB \end{bmatrix}}_{Input\ Data}$$

$$\xrightarrow{convert\ to\ polynomial} \underbrace{\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix}}_{Transform\ Matrix} \times$$

$$\underbrace{\begin{bmatrix} x^2+x & x^7+x^5+x & x^7+x^5+x^4 & x^5+x^3+x^2+x+1 \\ x^7+x^5+x^2 & x^6+x & x^7+x^6+x & x^7+x^5+x^4 \\ x^6+x^2+1 & x^5+x+1 & x^7+x^6+x^4+x+1 & x^7+x^6+x^5+x^4+x+1 \\ x^3+1 & x^5+x^4+x^2 & x^7+x^6+x^4+x^3+x+1 & x^7+x^5+x^3+x+1 \end{bmatrix}}_{Block\ Data}$$

در مرحله دوم، حاصل‌ضرب عناصر به شکل ماتریسی با کمک جبر بول انجام می‌شود. به طور مثال برای محاسبه عنصر مقدار r_{00} مراحل زیر طی می‌شود.

$$r_{00} = x(x^2 + x) + (x + 1)(x^7 + x^5 + x^2)$$

$$+1(x^6 + x^2 + 1) + 1(x^3 + 1)$$

که پس از محاسبه رابطه بالا بر حسب جبر بول مقدار r_{00} برابر $x^8 + x^7 + x^5 + x^3 + x^2$ می‌شود. همان‌طور که در این مثال نیز پیش آمد، ممکن است نتیجه محاسبات چند جمله‌ای از درجه بیشتر از ۷ باشد که قابل تبدیل به یک عدد ۸ بیتی نیست؛ بنابراین در این مرحله درصورتی که مقدار نتیجه از درجه ۷ بیشتر بود، نتیجه با کمک چند جمله‌ای $x^8 + x^4 + x^3 + x + 1$ تقلیل می‌یابد.

گام سوم. جاسازی پیام محرمانه در صفحه S تبدیل یافته

در این گام، پیام محرمانه در صفحه بیتی صفر از صفحه S تبدیل یافته جاسازی می‌شود. در مرحله اول این گام، پیام محرمانه به صورت کد اسکی و سپس رشته‌ای از بیت‌های صفر و یک تبدیل می‌شود. در مرحله دوم، ۳۲ بیت حاوی طول رشته بیتی به ابتدای رشته بیتی افزوده می‌شود. این ۳۲ بیت برای تعیین طول پیام در فرایند استخراج مورد استفاده قرار می‌گیرد. در مرحله سوم، رشته بیتی به ترتیب از چپ به راست و از بالا به پایین در صفحه بیتی صفر صفحه S جاسازی می‌شود. به طور مثال فرض کنید قرار است رشته بیتی $\{a_0, a_1, a_2, a_3, \dots, a_{14}, a_{15}\}$ در صفحه بیتی با ابعاد ۵*۵ جاسازی شود. شکل (۳) این جاسازی را نشان می‌دهد. همان‌طور که مشاهده می‌شود بخشی از صفحه که پیام در آن ذخیره نشده است، بدون تغییر باقی می‌ماند.

b_{00}^0	b_{01}^0	b_{02}^0	b_{03}^0	b_{04}^0
b_{10}^0	b_{11}^0	b_{12}^0	b_{13}^0	b_{14}^0
b_{20}^0	b_{21}^0	b_{22}^0	b_{23}^0	b_{24}^0
b_{30}^0	b_{31}^0	b_{32}^0	b_{33}^0	b_{34}^0
b_{40}^0	b_{41}^0	b_{42}^0	b_{43}^0	b_{44}^0

a_0	a_1	a_2	a_3	a_4
a_5	a_6	a_7	a_8	a_9
a_{10}	a_{11}	a_{12}	a_{13}	a_{14}
a_{15}	b_{31}^0	b_{32}^0	b_{33}^0	b_{34}^0
b_{40}^0	b_{41}^0	b_{42}^0	b_{43}^0	b_{44}^0

شکل (۳). بالا: صفحه بیتی صفر پیش از جایگذاری؛ پایین: صفحه بیتی صفر پس از جایگذاری پیامی به طول ۱۶ بیت

گام چهارم. ساخت تصویر حاوی پیام محرمانه با مد رنگ HSV

در این گام، تصویر حاوی پیام محرمانه با مد رنگ HSV با عکس تبدیل ستون ترکیبی بر روی تصویر ساخته شده در مرحله سوم ساخته می‌شود. عکس تبدیل ستون ترکیبی به صورت زیر محاسبه می‌شود.

$$A = T'R \qquad (۸)$$

که در آن، T' معکوس ماتریس T خواهد بود.

گام پنجم. تبدیل تصویر حاوی پیام محرمانه از مد رنگ HSV به مد رنگ RGB

برای تبدیل تصویر با مد رنگ HSV نرمال شده بین صفر تا ۲۵۵ با مقادیر صحیح به مد رنگ RGB می‌توان از روابط زیر استفاده نمود.

$$H' = \frac{H}{255} * 360 \quad (۹)$$

$$S' = \frac{S}{255} \quad (۱۰)$$

$$V' = \frac{V}{255} \quad (۱۱)$$

که در آن، $0 \le S' \le 1$، $0 \le V' \le 1$ و $0 \le H' \le 360$ است. برای تبدیل تصویر HSV به تبدیل RGB می‌توان از روابط زیر استفاده نمود.

$$C = V' * S' \quad (۱۲)$$

$$X = C * \left(1 - \left|\frac{H}{60} \bmod 2 - 1\right|\right) \quad (۱۳)$$

$$M = V' - C \quad (۱۴)$$

$$(R', G', B') = \begin{cases} (C, X, 0) & 0 \le H' < 60 \\ (X, C, 0) & 60 \le H' < 120 \\ (0, C, X) & 120 \le H' < 180 \\ (0, X, C) & 180 \le H' < 240 \\ (X, 0, C) & 240 \le H' < 300 \\ (C, 0, X) & 300 \le H' \le 360 \end{cases} \quad (۱۵)$$

$$(R, G, B) = \big(round\big((R' + M) * 255\big), round\big((G' + M) * 255\big), round\big((B' + M) * 255\big)\big) \quad (۱۶)$$

که در آن، (R, G, B) صفحات رنگی تصویر حاوی پیام محرمانه است.

۳-۲- مرحله استخراج پیام

در این قسمت پیام نهان‌نگاری شده از تصویر استخراج می‌شود. مراحل انجام این کار به صورت زیر است.

گام اول. تبدیل تصویر ورودی از مد رنگ RGB به مد رنگ HSV

گام دوم. ساخت صفحه S تبدیل یافته

گام سوم. استخراج پیام محرمانه از صفحه S تبدیل یافته

گام اول و دوم استخراج پیام محرمانه دقیقاً مشابه گام اول و دوم مرحله جاسازی پیام محرمانه است. در گام سوم، پیام محرمانه از صفحه بیتی صفر صفحه S تبدیل یافته استخراج می‌شود. در این گام، ۳۲ بیت طول رشته و رشته بیتی، به ترتیب از چپ به راست و از بالا به پایین از صفحه بیتی صفر صفحه S استخراج می‌شود. سپس رشته بیتی به بخش‌های ۸ بیتی تقسیم شده و هر بخش به عنوان کد اسکی کاراکتری از پیام در نظر گرفته می‌شود.

۴- آزمایش‌ها و نتایج

در این بخش ابتدا معیارهای ارزیابی معرفی شده‌اند و پس از آن با انجام آزمایش‌های مختلف روش پیشنهادی مورد ارزیابی قرار گرفته است.

۴-۱- معیارهای ارزیابی

در این مقاله، کیفیت و امنیت تصاویر حاصل از نهان‌نگاری توسط معیارهای زیر مورد ارزیابی قرار می‌گیرد.

۴-۱-۱- نسبت سیگنال به نویز (PSNR)[1]

این معیار توان سیگنال به توان نویز را اندازه می‌گیرد. هر چه این مقدار بزرگ‌تر باشد (مخرج به سمت صفر میل کند)، تصویر مورد آزمایش به تصویر اصلی نزدیک‌تر بوده و کیفیت بهتری را ارائه می‌دهد. این معیار در بسیاری از تحقیقات پردازش تصویر مورد استفاده قرار می‌گیرد. این معیار بدون یکا و به صورت دسی‌بل تخمین‌زده شده و به صورت معادله ۱۷ تعریف می‌شود [۱۵ و۲۰].

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{MSE_{avg}}\right) \quad (۱۷)$$

$$MSE = \frac{1}{hw}\sum_{i=1}^{h}\sum_{j=1}^{w}\left(x_{ij} - y_{ij}\right)^2 \quad (۱۸)$$

در معادلات (۱۷) و (۱۸) w و h به ترتیب نمایانگر عرض و طول تصویر و همچنین x_{ij} و y_{ij} مقادیر پیکسل [i, j] در تصویر اصلی و تصویر مورد آزمایش است. مقدار MSE_{avg} به صورت زیر به‌دست می‌آید.

$$MSE_{avg} = \frac{MSE_R + MSE_G + MSE_B}{3} \quad (۱۹)$$

که در آن، MSE_R، MSE_G و MSE_B به ترتیب میانگین مربع‌های خطا در کانال‌های قرمز، سبز و آبی هستند.

۴-۱-۲- میانگین شباهت ساختاری (MSSIM)

این معیار در سال‌های اخیر بیشتر توجهات را به خود اختصاص داده است. معیار شباهت ساختاری ترکیبی از سه معیار نسبتاً مستقل از هم است که شامل مقایسه بین درخشندگی[2]، وضوح[3] و ساختار[4] هر دو تصویر تغییریافته (Y) و اصلی (X) است.

1- Peak Signal-to-Noise Ratio
2- Luminance
3- Contrast
4- Structural

این معیار به صورت زیر تعریف می‌شود.

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (۲۰)$$

که در آن، μ_x و μ_y مقادیر میانگین و $\sigma_x, \sigma_y, \sigma_{xy}$ مقادیر انحراف معیار تصویر اصلی و تصویر مورد آزمایش است. MSSIM میانگین SSIM صفحه‌های رنگی RGB است. هر چه مقدار MSSIM به یک نزدیک‌تر باشد تصویر دارای کیفیت بهتری است [۲۰].

۴-۲- نتایج آزمایش‌ها

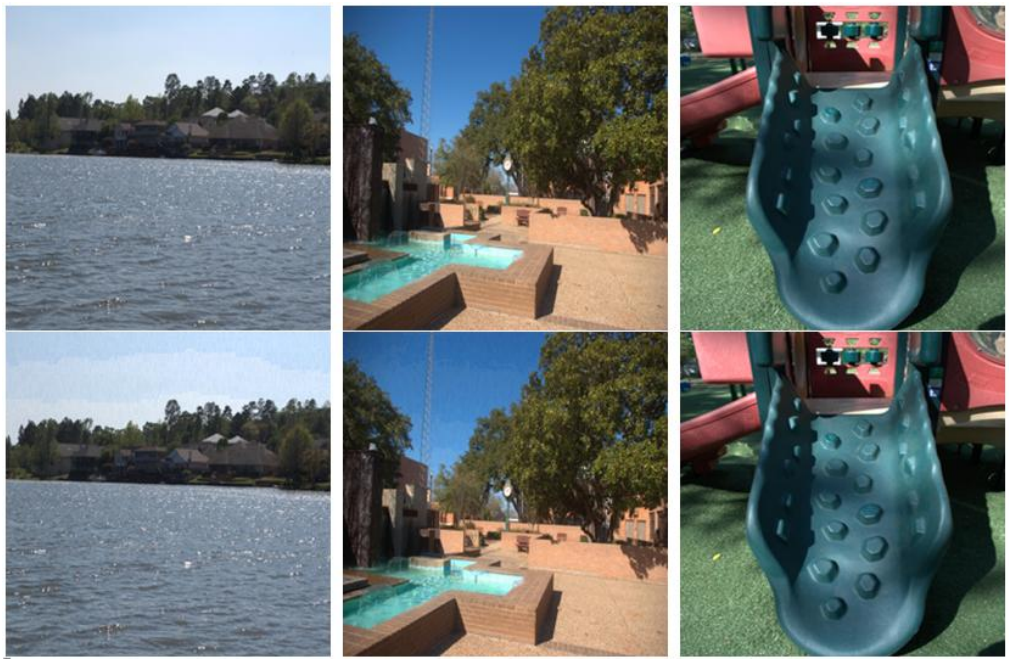
روش ارائه شده توسط ۵۰۰ تصویر در اندازه‌های ۲۵۶*۲۵۶، برگرفته از پایگاه داده مرجع [۲۱] مورد ارزیابی قرار گرفته است. سه تصویر رنگی از این پایگاه داده در شکل (۴) مشاهده می‌شود. با استفاده از روش پیشنهادی و روش ارائه شده در مقاله [۱۵] پیامی با ۵۰ و ۱۰۰ درصد ظرفیت نهان‌نگاری در تصاویر مجموعه آزمایش جاسازی شده است. روش ارائه شده در مقاله [۱۵] پیام‌ها را در مد تصویر RGB و در صفحات R، G و B قرار می‌دهد. نتایج موجود در جدول‌های (۲-۱) نشان می‌دهد که روش ارائه شده در این مقاله در هر دو ظرفیت، کارایی بالاتری دارد. از آنجایی که تأثیر انواع خرابی‌ها در مدهای مختلف تصویری متفاوت است، بنابراین انتخاب مد تصویر مناسب برای نهان‌نگاری دارای اهمیت زیادی است. همچنین شکل (۴) نتایج حاصل از نهان‌نگاری پیام با ۱۰۰ درصد ظرفیت روش در سه تصویر را نشان می‌دهد. نتایج حاکی از آن است که چشم انسان توانایی تشخیص وجود پیام محرمانه در تصویر را ندارد

جدول (۱). نتایج جاسازی پیام در مجموعه تصاویر آزمایشی با معیار MSSIM

نرخ جاسازی		MSSIM (روش پیشنهادی)	MSSIM (روش کانال B در مقاله [۱۵])	MSSIM (روش کانال G در مقاله [۱۵])	MSSIM (روش کانال R در مقاله [۱۵])
٪۵۰	**میانگین**	۰/۹۸۵۱	۰/۹۷۳۰	۰/۹۷۲۸	۰/۲۰۹۷
	انحراف معیار	۰/۰۱۱۱	۰/۰۰۹۳	۰/۰۰۹۳	۰/۰۰۹۴
٪۱۰۰	**میانگین**	۰/۹۷۴۳	۰/۹۴۵۴	۰/۹۴۵۳	۰/۹۴۵۲
	انحراف معیار	۰/۰۱۵۸	۰/۰۱۵۸	۰/۰۱۶۱	۰/۰۱۶۲

جدول (۲). نتایج جاسازی پیام در مجموعه تصاویر آزمایشی با معیار PSNR

نرخ جاسازی		PSNR (روش پیشنهادی)	PSNR (روش کانال B در مقاله [۱۵])	PSNR (روش کانال G در مقاله [۱۵])	PSNR (روش کانال R در مقاله [۱۵])
٪۵۰	میانگین	۴۳/۵۸۲	۳۹/۵۲۱	۳۹/۵۴۶	۳۹/۵۲۳
	انحراف معیار	۲/۱۲	۰/۱۳۶	۰/۱۰۹	۰/۱۱۷
٪۱۰۰	میانگین	۴۱/۰۰۹	۳۶/۶۰۷	۳۶/۶۱۷	۳۶/۶۰۵
	انحراف معیار	۱/۷۸۴	۰/۱۰۳	۰/۰۹۷	۰/۱۰۲



شکل (۴). بالا: تصاویر پوششی؛ پایین: تصاویر حامل پیام با نرخ ۱۰۰ درصد با روش پیشنهادی HSV؛ ارزیابی بصری وجود پیام را در تصویر نشان نمی‌دهد.

۴-۳- نهان‌کاوی با ابزار StegExpose

برای ارزیابی بیشتر امنیت روش پیشنهادی از ابزار StegExpose ارائه شده در مرجع [۱۶] استفاده شده است. این ابزار با روش های مختلفی مانند تحلیل RS [۲۲]، تحلیل جفت نمونه [۲۳]، حمله آماری chi-square [۲۴] و حمله آماری تفاوت هیستوگرام [۲۵]، امنیت روش را بررسی می کند. همان‌طور که مشاهده می‌شود ابزار فوق قادر به تشخیص تصاویر نهان‌نگاری شده در روش پیشنهادی نبوده در حالی که برخی تصاویر روش مرجع [۱۵] را کشف می‌نماید.

۴- ۴- نهان‌کاوی با رده‌بندی جمعی

یکی از روش‌های اخیر نهان‌کاوی که دقت مناسبی ارائه می‌دهد، رده‌بند جمعی است که در مرجع [۱۷] ارائه شده است. در این روش امنیت نهان‌نگاری به صورت تجربی توسط رده‌بندهای دودویی که بر روی تصویر پوششی و نسخه نهان‌نگاری شده آن آموزش می‌بینند، ارزیابی می‌شود. گرچه این روش ارزیابی، مصنوعی بوده و مطابق کاربردهای دنیای واقعی نیست، اما امکان ارزیابی امنیت روش نهان‌نگاری که هدف این بخش است را فراهم می‌کند [۲۶].

جدول (۳). نتایج نهان‌کاوی با ابزار StegExpose [۱۶] بر روی مجموعه تصاویر آزمایشی

نرخ جاسازی		تعداد موارد تشخیص داده شده توسط ابزار
٪۵۰	روش پیشنهادی	۰
	(روش کانال R در مقاله [۱۵])	۲۶
	(روش کانال G در مقاله [۱۵])	۱۰
	(روش کانال B در مقاله [۱۵])	۱۴
٪۱۰۰	روش پیشنهادی	۰
	(روش کانال R در مقاله [۱۵])	۵۰۰
	(روش کانال G در مقاله [۱۵])	۳۶۶
	(روش کانال B در مقاله [۱۵])	۳۷۱

برای اعمال روش رده‌بند جمعی، از رده‌بند پایه جداساز خطی فیشر[1] استفاده می‌شود. همچنین با استفاده از روش SPAM که در مرجع [۲۷] ارائه شده است از هر تصویر پوششی و هر تصویر پنهان‌سازی شده تعداد ۶۸۶ ویژگی استخراج می‌شود. امنیت روش توسط معیارهای TPR (نرخ مثبت واقعی) و FPR (نرخ مثبت کاذب) ارزیابی شده است. نتایج جدول (۴) نشان می‌دهد که رده‌بند جمعی توانایی دسته‌بندی تصاویر حاوی پیام و تصاویر پوششی را در روش پیشنهادی این مقاله و روش پیشنهادی مقاله [۱۵] ندارد. همچنین اعداد جدول (۴) نشان می‌دهد اگر چه معیار TPR برای روش پیشنهادی بدتر از معیار TPR برای روش مقاله [۱۵] است، ولی معیار FPR آن بهتر از مقاله [۱۵] است. بالا بودن همزمان معیارهای TPR و FPR نشانگر آن است که رده‌بند تمایل به پاسخ مثبت دارد نه پاسخ واقعی.

جدول (۴). نتایج نهان‌کاوی با رده‌بندی جمعی بر روی مجموعه تصاویر آزمایشی

نرخ جاسازی	روش‌ها	TPR	FPR
٪۵۰	روش پیشنهادی	۰/۷۷۰۰	۰/۵۹۵۰
	(روش کانال R در مقاله [۱۵])	۰/۵۵۵۰	۰/۴۲۰۰
	(روش کانال G در مقاله [۱۵])	۰/۶۱۰۰	۰/۴۸۵۰
	(روش کانال B در مقاله [۱۵])	۰/۵۷۰۰	۰/۴۳۰۰
٪۱۰۰	روش پیشنهادی	۰/۸۴۰۰	۰/۵۵۵۰
	(روش کانال R در مقاله [۱۵])	۰/۷۱۰۰	۰/۴۲۵۰
	(روش کانال G در مقاله [۱۵])	۰/۷۱۰۰	۰/۴۳۰۰
	(روش کانال B در مقاله [۱۵])	۰/۷۱۰۰	۰/۴۳۰۰

۵- نتیجه‌گیری

در این مقاله روشی برای نهان‌نگاری پیام محرمانه در تصویر رنگی ارائه شده است. روش ارائه شده با استفاده از تبدیل ستون ترکیبی پیام محرمانه را در صفحه بیتی صفر تصویر HSV ذخیره می‌کند. روش ارائه شده با بهره‌گیری از تأثیر متفاوت خرابی‌های تصویر به بهبود روش نهان‌نگاری پیام محرمانه با تبدیل ستون ترکیبی پرداخته است. نتایج آزمایش‌ها نشانگر کارایی روش ارائه شده از نظر میزان شباهت (جدول‌های (۲-۱)) تصویر بدون پیام و تصویر حاوی پیام و امنیت روش ارائه شده (جدول‌های (۴-۳)) است. از طرف دیگر ارزیابی‌های بصری نیز نشان می‌دهد که چشم انسان توانایی تشخیص وجود پیام را ندارد.

۶- مراجع

[1] M. M. AlyanNezhadi and Z. Amiri, "A Novel Method for image hiding text by changing the spaces in text," presented in the first International Conference on Electrical Engineering and Computer Science, Tehran, Iran, 1394(in Persian).

[2] A. Rana, N. Sharma, and A. Kaur, "Image steganography method based on kohonen neural network," International Journal of Engineering Research and Applications, Papers, vol. 2, pp. 2234-2236, 2012.

[3] A. Agarwal, "Security enhancement scheme for image steganography using S-DES technique," International journal of advanced research in computer science and software engineering, vol. 2, 2012.

[4] M. K. Ramaiya, N. Hemrajani, and A. K. Saxena, "Improvisation of Security Aspect in Steganography Applying DES," In 2013 International Conference on Communication Systems and Network Technologies (CSNT), pp. 431-436, 2013.

[5] A. Nag, S. Ghosh, S. Biswas, D. Sarkar, and P. P. Sarkar, "An image steganography technique using X-box mapping," In 2012 International Conference on Advances in Engineering, Science and Management (ICAESM), pp. 709-713, 2012.

1- Fisher Linear discriminant

[6] H. Ge, M. Huang, and Q. Wang, "Steganography and steganalysis based on digital image," In 2011 4th International Congress on Image and Signal Processing (CISP), pp. 252-255, 2011.
[7] D. H. Kekre, A. B. Patankar, and D. Koshti, "Performance comparison of simple orthogonal transforms and wavelet transforms for image steganography," International Journal of Computer Applications (0975–8887), vol. 44, 2012.
[8] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.
[9] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms," In Photonics West 2001-Electronic Imaging, pp. 505-516, 2001.
[10] H. Ahmadi and S. Vali, "A novel Steganography method based on differential pixel value," Presented in 7'th international conference on information technology and science, urmia, Iran, 1394(in Persian).
[11] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, pp. 727-752, 2010.
[12] M. Esmaili, "An improved steganography algorithm based on SVD to reduce the problem of false-positive detection," presented in first national conference on Metaheuristic algorithms and applications in science and engineering, Iran, 1393(in Persian).
[13] H. SaboohiAbyez and M. Hosseini, "A complete solution for high-capacity steganography in discrete wavelet domain," presented in first national conference on computer and electrical engineering in the north of Iran, Bandaranzali, Iran, 1393(in Persian).
[14] M. ZabihiNezhad, H. Naji, and M. Kamandar, "increasing the capacity of steganography in color images using the HSV color space," presented in first national conference on advances in computer and electrical engineering, Khayam, Iran, 1393(in Persian).
[15] W. M. Abduallah, A. M. S. Rahma, and A.-S. K. Pathan, "Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach," Computers & Electrical Engineering, vol. 40, pp. 1390-1404, 2014.
[16] B. Boehm, "StegExpose-A Tool for Detecting LSB Steganography," arXiv preprint arXiv:1410.6656, 2014.
[17] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble Classifiers for Steganalysis of Digital Media," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 432-444, 2012.
[18] A. Q. Khan, A. Akhtar, and M. Z. Ahmad, "Autonomous Farm Vehicles: Prototype of Power Reaper," arXiv preprint arXiv:1501.02379, 2015.
[19] W. Stallings, "Cryptography and Network Security," Principles and Practice, Pearson Education, 2002.
[20] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," In Pattern Recognition (ICPR), 2010 20th International Conference on, pp. 2366-2369, 2010.
[21] Q. Liu, [Online]. Available: http://www.shsu.edu/~qxl005/New/Downloads/#image_database, 1 april 2016.
[22] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," In Proceedings of the 2001 workshop on Multimedia and security: new challenges, pp. 27-30, 2001.
[23] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," Signal Processing, IEEE Transactions on, vol. 51, pp. 1995-2007, 2003.
[24] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," In Information Hiding, pp. 61-76, 1999.
[25] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference image histogram," In 2003 IEEE International Conference on Acoustics, Speech and Signal Processing, 2003. Proceedings. (ICASSP'03), vol. 3, pp. III-545-8, 2003.
[26] [26] H. Vojtěch and J. Fridrich, "Digital image steganography using universal distortion," Proceedings of the first ACM workshop on Information hiding and multimedia security. ACM, pp. 59-68, 2013.
[27] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," IEEE Trans. on Info. Forensics and Security, vol. 5, no. 2, pp. 215-224, 2010.

A New Steganography Method in Colored Images Using Mixed Column Transform in HSV Color Model

M. M. AlyanNezhadi, Z. Amiri, H. Mashayekhi*

*Shahrood University of technology

(Received: 03/02/2016 , Accepted: 31/10/2016)

ABSTRACT

Steganography is largely used in information security systems. In steganography, the goal is to hide the information such that only the sender and receiver are aware of the communication and information. Steganography is carried out on different media such as image, sound and text. It can be performed in both transform and spatial domains. In transform domain methods, first the cover image is transformed into a different domain using, for example, a frequency transform. Then, the secret message is embedded in the conversion coefficients. In this paper, a new steganography method based on the transform domain is proposed to conceal text in an HSV color image. After converting the image to HSV, it is divided into blocks and the mixed column transfer is applied on each block. The secret message is embedded in the transferred columns. Simulation results and comparisons show the high capacity and increased security of the proposed method.

Keywords: Steganography, Mixed Column Transform, Colored HSV Image

* Corresponding Author Email: hmashayekhi@shahroodut.ac.ir