نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۱، بهار ۱۴۰۰؛ ص ۸۴- ۷۳

علمی– پژوهشی

بهبود عملکرد روش نهان‌نگاری تطبیقی از طریق انتخاب هوشمندانه کلیدهای جاسازی با استفاده از الگوریتم‌های بهینه‌سازی

وجیهه ثابتی[1*]

۱- استادیار، دانشگاه الزهرا، تهران، ایران

(دریافت: ۱۳۹۹/۰۶/۰۵، پذیرش: ۱۳۹۹/۰۷/۲۲)

چکیده

در روش‌های نهان‌نگاری تطبیقی از ایده ظرفیت جاسازی متغیر در نواحی تصویر با توجه به یکنواخت یا لبه بودن آن‌ها، استفاده می‌شود. روش ALSBMR یک روش تطبیقی است که دو مرحله اصلی دارد: انتخاب پیکسل‌های مناسب برای جاسازی و جاسازی در آن‌ها با استفاده از روش LSBMR. در این روش، دو کلید توافقی میان فرستنده و گیرنده برای مشخص نمودن زاویه چرخش بلاک‌ها و انتخاب مسیر جاسازی استفاده می‌شود. در روش اصلی این کلیدها بدون هیچ ملاک و معیار مشخص و به‌صورت تصادفی توسط فرستنده انتخاب و به اطلاع گیرنده می‌رسد. در روش پیشنهادی، انتخاب کلید به‌عنوان یک مسئله بهینه‌سازی مدل شده است و از دو الگوریتم بهینه‌سازی ژنتیک (GA) و الگوریتم بهینه‌سازی آموزش-یادگیری (TLBO) برای یافتن کلیدهای بهینه استفاده‌شده است. برای بررسی بیشتر از دو تابع برازندگی اختلاف بین تصویر میزبان و نهان‌نگاری شده و همچنین اختلاف هیستوگرام تصویر میزبان و تصویر نهان‌نگاری شده استفاده شده است. نتایج نشان می‌دهد، کیفیت و امنیت تصویر نهان‌نگاری شده در روش پیشنهادی نسبت به روش پایه بهبود یافته است. با توجه به این‌که تمام روش‌های نهان‌نگاری نیاز به کلیدهای جاسازی دارند، هوشمند کردن فرآیند انتخاب این کلیدها می‌تواند به بهبود عملکرد روش‌های نهان‌نگاری موجود کمک کند.

کلید واژه‌ها: نهان‌نگاری، نهان‌کاوی، نهان‌نگاری تطبیقی، الگوریتم ژنتیک، الگوریتم بهینه‌سازی آموزش-یادگیری

Improving Adaptive Steganography Performance with Intelligent Embedding Key Selection Using Optimization Algorithms

V. Sabeti[1]*

*Assistant Professor, Alzahra University, Tehran, Iran

(Received: 00/00/2019; Accepted: 00/00/2020)

Abstract

Adaptive steganography methods use variable embedding capacity according to the uniformity or edges of image areas. ALSBMR is an adaptive method with two main stages: Selecting suitable pixels, and embedding them using the LSBMR method. This method utilizes two adaptive keys between the sender and the receiver to determine the block rotation angle and select the embedding path. In the original method, the keys are randomly selected by the sender with no specific criteria and then sent to the receiver. The proposed method models key selection as an optimization problem and uses Genetic Algorithm (GA) and Teaching-Learning-Based Optimization (TLBO) to find the optimal keys. Two fitness functions are used to further evaluate the difference as well as the histogram difference between the cover and stego images. The results show that the image embedded with the proposed method has improved quality and security compared to the base method. Since all steganography methods require embedding keys, intelligent key selection can improve the performance of existing steganography methods.

Keywords: Steganography, Steganalysis, Adaptive steganography, Genetic algorithm, TLBO algorithm

*Corresponding Author E-mail:v.sabeti@alzahra.ac.ir

۱- مقدمه

با پیشرفت در فناوری ارتباطات دیجیتال و رشد قدرت کامپیوتر در ذخیره‌سازی، اختلالات در تضمین حفظ حریم شخصی افراد به‌طور فزاینده‌ای به یک چالش تبدیل شده است. با ورود دوران دیجیتال و استفاده عمومی از اینترنت و ایمیل برای تبادل افکار، امنیت اطلاعات منتقل‌شده از یک کانال باز به یک مسئله اساسی تبدیل شده و بنابراین محرمانه بودن و یکپارچگی داده‌ها برای محافظت در برابر دسترسی و استفاده غیرمجاز، مورد نیاز است. این مسئله باعث رشد تحقیقات در زمینه پنهان‌سازی اطلاعات شده است. تاکنون روش‌های مختلفی برای حفاظت از حریم خصوصی مورد بررسی و توسعه قرار گرفته است. رمزنگاری و نهان‌نگاری دو روش محبوب در این زمینه هستند. رمزنگاری اغلب برای محافظت از محرمانه بودن اطلاعات از طریق ناخوانا کردن پیام‌ها استفاده می‌شود. بااین‌حال، پیام‌های غیرقابل تشخیص ممکن است سوءظن حریف را افزایش دهند و احتمالاً منجر به نابودی این روش ارتباطی شوند [۱].

در نهان‌نگاری آنچه که مهم است، پنهان نگاه داشتن وجود اطلاعات یا ارتباطات است. هرگاه دشمن از وجود اطلاعات یا ارتباطات مطلع شود، نهان‌نگاری شکست خورده است. به‌طورکلی نهان‌نگاری فرایند جاسازی پیام از پیش تعیین‌شده در یک رسانه میزبان به روشی است که کاهش کیفیت را به حداقل برساند. رسانه میزبان می‌تواند یک تصویر، صوت، ویدیو و یا متن باشد [۲].

روش‌های نهان‌نگاری در تصاویر بر اساس ذات فرآیند جاسازی به دو حوزه مکان و تبدیل تقسیم‌بندی می‌شوند. در حوزه مکان، داده محرمانه به‌صورت مستقیم در مقدار پیکسل‌ها جاسازی می‌شود که دو روش LSB و PVD از روش‌های پایه در این حوزه هستند [۹- ۳]. از طرف دیگر، در حوزه تبدیل یا فرکانس، ضرایب تبدیل بیت‌های پیام محرمانه را نگهداری می‌کنند. روش‌های نهان‌نگاری در ضرایب DCT [۱۰] و DWT [۱۱] در این دسته قرار می‌گیرند.

ملاک دیگر برای دسته‌بندی روش‌های نهان‌نگاری، نحوه تعیین ظرفیت جاسازی هر پیکسل است. هر الگوریتم نهان‌نگاری به دو روش می‌تواند ظرفیت جاسازی هر پیکسل از تصویر را مشخص کرده و داده موردنظر را در آن جاسازی کند. براین اساس، الگوریتم‌های نهان‌نگاری را می‌توان به دو دسته تقسیم کرد: روش‌های غیرتطبیقی، روش‌های تطبیقی.

در روش‌های غیرتطبیقی، ظرفیت جاسازی هر پیکسل ثابت است و به نواحی اطراف آن پیکسل توجهی نمی‌شود. در این روش‌ها بدون توجه به ویژگی‌های سیستم بینایی انسان، داده جاسازی شده در کل تصویر توزیع می‌شود و تفاوتی میان نواحی مختلف تصویر قائل نمی‌شوند. روش‌های این گروه با دو هدف مختلف، ظرفیت پیکسل‌ها را مشخص می‌کنند. هدف تعدادی از آن‌ها، ظرفیت جاسازی زیاد و کیفیت تصویر قابل قبول است. بیشترین ظرفیت جاسازی در روش‌های این گروه، ۳ بیت در هر پیکسل است، درحالی‌که کیفیت تصویر در حد قابل قبول (بالاتر از ۴۰db) بماند. هدف گروه دیگر، کارایی جاسازی بالا با تغییرات اندک در تصویر است. این روش‌ها بر روی حداقل کردن تغییرات تصویر در زمان جاسازی مقدار نسبتاً کمی از پیام تمرکز دارند (به‌طور نرمال دو بیت یا کمتر). کارایی جاسازی به‌عنوان نسبت بین تعداد بیت جاسازی‌شده به مقدار تغییرات ایجادشده تعریف می‌شود. روش LSBMR [۳] در این گروه قرار دارد.

دسته دوم، روش‌های تطبیقی است که ظرفیت هر پیکسل با توجه به پیکسل‌های همسایه مشخص می‌شود. با توجه به در نظر گرفتن ساختار محلی تصویر در تعیین ظرفیت هر پیکسل، ظرفیت جاسازی کلی تصویر با توجه به ویژگی‌های آن متفاوت است. این روش‌ها مطابق ویژگی سیستم بینایی انسان عمل می‌کنند. ایده اصلی این روش‌ها جاسازی بیشتر در نواحی لبه تصویر و جاسازی کمتر در نواحی یکنواخت تصویر است. این روش‌ها پس از شناسایی نواحی مناسب جاسازی و تعیین ظرفیت هر پیکسل، دنباله داده محرمانه را در حوزه، بستر و به روش موردنظر جاسازی می‌کنند. گیرنده باید بتواند نواحی که فرستنده در آن داده جاسازی کرده است را به‌درستی شناسایی کند تا داده جاسازی‌شده را به‌صورت کامل از آن استخراج کند. بسیاری از تحقیقات اخیر بر روی روش‌های تطبیقی انجام‌شده است. تلاش برای پیدا کردن نواحی مناسب برای جاسازی داده با هدف تولید تصویر نهان‌نگاری شده با کمترین انحراف [۱۲] وکنترل ظرفیت جاسازی براساس ویژگی‌های تصویر [۱۳] نمونه ای از این تحقیقات است. استفاده از فرآیند جاسازی مبتنی بر لبه [۱۶- ۱۴] نیز یکی از ایده های مهم در این حوزه است.

روش‌های یادگیری ماشین به‌صورت موفقیت‌آمیزی برای کاربردهای مختلف پردازش تصویر در گذشته استفاده شده است. با تنظیم روش‌های یادگیری ماشین و استفاده از خاصیت پیشگویی هوش مصنوعی، می‌توان کمک گرفت تا داده بیشتری با انحراف کمتر در تصویر میزبان جاسازی کرد [۱۷]. الگوریتم ژنتیک به‌عنوان ابزاری برای حل مسائل جستجو و بهینه‌سازی در طراحی یک مدل نهان‌نگاری تصویر استفاده شده است [۱۸]. شبکه‌های عصبی [۱۹] و الگوریتم PSO [۲۰] نیز از دیگر روش‌های یادگیری محبوب هستند که برای بهبود شفافیت و ظرفیت استفاده شده است [۱].

یکی از روش‌های تطبیقی که بهبود مؤثری نسبت به روش‌های ابتدایی مانند LSBM و LSBMR داشته است، روش ALSBMR است [۳]. این روش یکی از روش‌های تطبیقی است، که طبق مطالعات انجام‌شده، در پنهان کردن اطلاعات محرمانه موفق عمل کرده است. هدف اصلی در این مقاله، شناسایی نقطه ضعف این روش و بهبود آن با استفاده از الگوریتم‌های بهینه‌سازی است. در اجرای مراحل روش ALSBMR، دو کلید توافقی میان فرستنده و گیرنده برای مشخص نمودن زاویه چرخش بلاک‌ها و انتخاب مسیر جاسازی استفاده می‌شود که این کلیدها بدون هیچ ملاک و معیار مشخص و به‌صورت تصادفی توسط فرستنده انتخاب و به اطلاع گیرنده رسانده می‌شود. در روش پیشنهادی، انتخاب کلید به‌عنوان یک مسئله بهینه‌سازی مدل شده است و از دو الگوریتم بهینه‌سازی ژنتیک و الگوریتم بهینه‌سازی آموزش- یادگیری (TLBO) برای یافتن کلیدهای بهینه استفاده شده است. با توجه به اینکه تمام روش‌های نهان‌نگاری نیاز به کلیدهای جاسازی دارند، هوشمند کردن فرآیند انتخاب این کلیدها می‌تواند به بهبود عملکرد روش‌های نهان‌نگاری کمک کند.

در ادامه، در بخش دوم به‌طور مختصر روش‌های LSBMR و ALSBMR به‌عنوان روش‌های پایه بررسی می‌شوند و سپس الگوریتم روش پیشنهادی به‌صورت کامل معرفی می‌شود. در بخش سوم، نتایج ارزیابی روش پیشنهادی با دو الگوریتم بهینه‌سازی و دو تابع برازندگی مختلف و برای دو مجموعه تصویر آزمون بررسی می‌شود. در بخش چهارم نتیجه‌گیری نهایی ارائه می‌شود.

۲- روش تحقیق

روش‌های جاسازی در بیت کم‌ارزش از ساده‌ترین و رایج‌ترین روش‌های نهان‌نگاری هستند. روش LSBM یکی از این روش‌ها است. در این روش، در صورت تطابق بیت داده با بیت کم‌ارزش پیکسل، تغییری در پیکسل ایجاد نمی‌شود. در صورت عدم تطابق، مقدار پیکسل به‌صورت تصادفی کاهش یا افزایش می‌یابد. با توجه به وجود حملات موفق برای کشف این روش، بسیاری از محققان روش‌هایی برای بهبود امنیت این روش پیشنهاد کرده‌اند که در ادامه دو روش که مبنای روش پیشنهادی هستند، بررسی می‌شوند و سپس روش پیشنهادی معرفی می شود.

۲-۱- روش LSBMR

هدف این روش، تغییر روش LSBM به نحوی است که تغییرات کمتری در اثر جاسازی در تصویر میزبان ایجاد شود [۳]. این روش در ادامه LSBMR نام‌گذاری شده است. در این روش جاسازی در دو پیکسل به‌صورت هم‌زمان انجام می‌شود. فرض کنید x_i و x_{i+1} پیکسل‌های تصویر میزبان هستند که بناست دو بیت داده m_i و m_{i+1} در آن‌ها جاسازی شوند و دو پیکسل حاصل از این جاسازی در تصویر نهان‌نگاری شده با y_i و y_{i+1} نشان داده شود. جاسازی به نحوی انجام می‌شود که بیت m_i پیام برابر LSB پیکسل y_i در تصویر نهان‌نگاری شده باشد و بیت m_{i+1}، تابعی از دو پیکسل y_i و y_{i+1} باشد. تابع موردنیاز باید دو شرط زیر را داشته باشد ($\forall l,n \in z$):

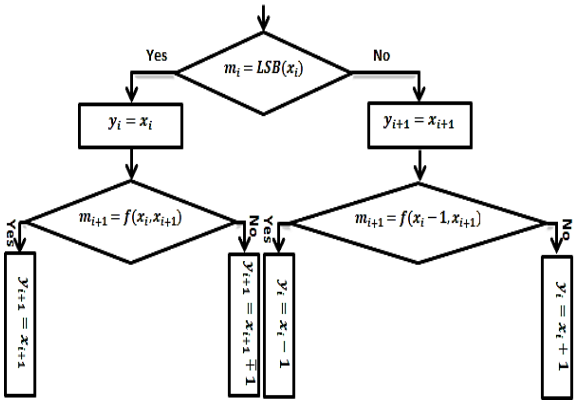
$$f(l-1,n) \neq f(l+1,n) \quad (۱)$$

$$f(l,n) \neq f(l,n+1)\,, f(l,n) \neq f(l,n-1) \quad (۲)$$

l و n دو عدد صحیح هستند که ورودی‌های تابع می‌باشند. برای استفاده از این تابع y_i و y_{i+1} جایگزین آن‌ها می‌شوند. دو شرط بالا به این دلیل الزامی است که ممکن است پیکسل اول نیاز به تغییر داشته یا نداشته باشد. در هر دو صورت باید بتوان انتخابی انجام داد که به روش موردنظر داده قابل‌استخراج باشد. تابع زیر این ویژگی را دارد:

$$f(y_i, y_{i+1}) = LSB(\lfloor {}^{y_i}/_{2} \rfloor + y_{i+1}) \quad (۳)$$

الگوریتم این روش در شکل (۱) نمایش داده شده است. در این روش تعداد تغییرات موردنیاز برای جاسازی یک بیت داده برابر ۰/۳۷۵ می‌شود، درحالی‌که این معیار در روش LSBM برابر ۰/۵ است.



شکل ۱. الگوریتم جاسازی دو بیت m_i و m_{i+1} در دو پیکسل x_i و x_{i+1} به روش LSBMR

۲-۲- روش ALSBMR

یکی از مقاوم‌ترین روش‌های تطبیقی، روش ALSBMR است. مزیت اصلی این روش، استفاده از روش LSBMR [۳] در مرحله جاسازی است که باعث افزایش مقاومت آن نسبت به روش‌های دیگر شده است. در این روش ابتدا تصویر میزبان به بلاک‌های با اندازه $B_z \times B_z$ تقسیم‌بندی می‌شود. مقدار B_z از ابتدا به‌صورت یک ثابت تعیین می‌شود. هر بلاک با یک درجه تصادفی

$\{۲۷۰،۱۸۰،۹۰،۰\}$ چرخانده می‌شود. این درجه در ابتدا توسط یک کلید مشخص می‌شود. سپس تصویر به‌دست‌آمده پیمایش می‌شود و بردار سطری v از روی آن ساخته می‌شود. این بردار به واحدهای جاسازی شامل دو پیکسل متوالی (x_i, x_{i+1}) تقسیم می‌شود.

حال باید یک حد آستانه مناسب برای مقدار تفاوت در بلاک دوتایی یافت به‌گونه‌ای که پیام M در بلاک‌های با مقدار تفاوت بزرگ‌تر از حد آستانه قابل جاسازی باشد. فرض کنید $EU(t)$ زوج پیکسل‌هایی است که قدر مطلق تفاوت آن‌ها بزرگ‌تر یا مساوی t باشد.

$$EU(t) = \{(x_i, x_{i+1}) || x_i - x_{i+1}| \geq t, \forall (x_i, x_{i+1}) \in v\} \quad (۴)$$

حد آستانه T بدین ترتیب محاسبه می‌شود:

$$T = arg\,\max_t \{2 * |EU(t)| \geq |M|\} \quad (۵)$$

اگر حد آستانه مساوی صفر شود، این روش مشابه روش LSBMR می‌شود. حال در مجموعه زیر به روش LSBMR جاسازی انجام می‌شود. ترتیب انتخاب واحدهای جاسازی به‌صورت تصادفی است. $B_z \times B_z$

$$EU(T) = \{(x_i, x_{i+1}) || x_i - x_{i+1}| \geq T, \forall (x_i, x_{i+1}) \in v\} \quad (۶)$$

با توجه به این‌که در قسمت قبلی روش LSBMR به‌تفصیل شرح داده‌شده است، از بیان مجدد آن در اینجا اجتناب می‌شود. ممکن است بعد از جاسازی مقادیر جدید خارج از بازه [۲۵۵ و ۰] شود یا مقدار تفاوت جدید کمتر از حد آستانه T باشد. در این صورت نیاز به مرحله اصلاح وجود دارد.

بعد از جاسازی داده، تصویر به‌دست‌آمده به بلاک‌های $B_z \times B_z$ تقسیم‌بندی شده و برخلاف درجه استفاده‌شده در ابتدا چرخانده می‌شود تا تصویر نهان‌نگاری شده نهایی تولید شود.

۲-۳- روش پیشنهادی

هدف اصلی در این مقاله بهبود روش ALSBMR به‌عنوان یک روش تطبیقی است. به همین دلیل الگوریتم روش ALSBMR به‌صورت دقیق‌تر بررسی می‌شود. برای درک بهتر، در شکل (۲)، الگوریتم این روش ترسیم‌شده است. بر اساس این شکل، روش ALSBMR شامل مراحل زیر است:

۱) بلاک بندی تصویر میزبان (پارامتر B_Z، اندازه بلاک، یک ثابت ورودی است)

۲) برای هر بلاک تصویر: تعیین درجه چرخش (با توجه به کلید توافقی key_1) و چرخش هر بلاک

۳) تعیین حد آستانه (با توجه به‌اندازه داده موردنظر)

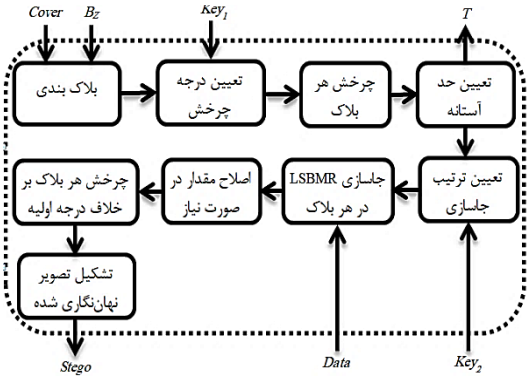
۴) تعیین ترتیب جاسازی در زوج پیکسل‌های مناسب (با توجه به کلید توافقی key_2)

۵) جاسازی به روش LSBMR در هر زوج پیکسل مناسب

۶) اصلاح مقدار زوج پیکسل‌ها (در صورت نیاز)

۷) برای هر بلاک تصویر: تعیین درجه چرخش اولیه (با توجه به کلید توافقی key_1) و چرخش بلاک با درجه مخالف اولیه.

۸) تشکیل تصویر نهان‌نگاری شده



شکل ۲. الگوریتم ALSBMR

تمام روش‌های نهان‌نگاری، در الگوریتم جاسازی خود به یک یا چند کلید نیاز دارند. این کلیدها اغلب اعدادی هستند که فرستنده و گیرنده بر روی آن‌ها توافق می‌کنند. شخص سوم (دشمن) با آگاهی از الگوریتم جاسازی و بدون اطلاع از کلید، قادر به استخراج پیام نیست. اما اگر کلیدی در الگوریتم جاسازی استفاده نشود، شخص سوم به‌راحتی می‌تواند داده را استخراج کند. یکی از کاربردهای کلیدها در الگوریتم جاسازی، تعیین نحوه توزیع پیام در تصویر است. به‌عبارت‌دیگر، با کلید می‌توان مکان جاسازی داده را مشخص کرد. برای مثال در الگوریتم ALSBMR، دو کلید key_1 و key_2، طبق توضیحات قبلی، برای تعیین درجه چرخش هر بلاک و تعیین ترتیب جاسازی در زوج پیکسل‌های منتخب استفاده می‌شود.

ایده روش پیشنهادی، انتخاب کلیدهای الگوریتم ALSBMR به نحوی است که بتوان نتایج بهتری کسب کرد. در این روش با تغییر این دو کلید، می‌توان مکان جاسازی داده را تغییر داد. مقادیر ممکن برای کلیدها، مقادیر بسیار زیادی است که پیدا کردن بهترین مقدار را می‌توان به شکل یک مسئله بهینه‌سازی مدل کرد. هدف نهایی یافتن مقادیری برای key_1 و key_2 است که به ازای آن‌ها کارایی الگوریتم جاسازی بهبود یابد. دو معیار رایج برای سنجش الگوریتم‌های جاسازی امنیت در برابر حملات (کشف ناپذیری) و کیفیت تصویر نهان‌نگاری شده (مشاهده ناپذیری) است که معیارهای مشخصی برای سنجش آن‌ها وجود دارد.

معیارهای کیفیت تصویر نهان‌نگاری شده مانند PSNR و MSE، نشان‌دهنده تغییرات تصویر نهان‌نگاری شده نسبت به تصویر میزبان است. هرچه این تغییرات کمتر باشد، مقدار این معیارها بهتر است و تصویر نهان‌نگاری شده کیفیت بهتری دارد.

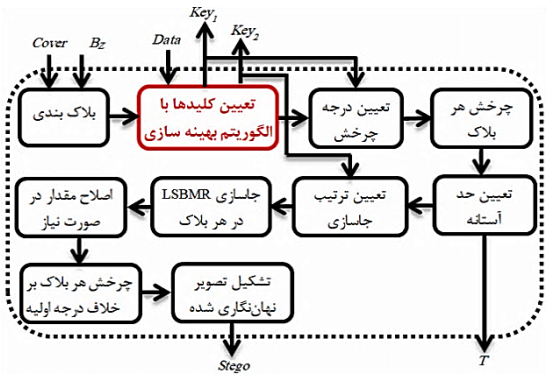
از طرف دیگر، حملات با استفاده از تغییرات ایجادشده در تصویر نهان‌نگاری شده قادر به کشف آن‌ها هستند. بنابراین، اگر روش جاسازی به نحوی باشد که برای جاسازی داده تغییرات کمتری در تصویر میزبان ایجاد کند، احتمال کشف آن روش کمتر است. بنابراین با کم کردن تغییرات تصویر نهان‌نگاری شده نسبت به تصویر میزبان، می‌توان به بهبود هر دو معیار موردنظر امیدوار بود. به‌عبارت‌دیگر، اگر بتوان کلیدهایی یافت که با استفاده از آن‌ها الگوریتم جاسازی با حداقل تغییرات در تصویر میزبان بتواند تصویر نهان‌نگاری شده را تولید کند، تصویر نهان‌نگاری شده تولیدشده بیشترین کیفیت و کمترین احتمال کشف در برابر حملات موجود را خواهد داشت.

الگوریتم کلی روش پیشنهادی در شکل (۳) نشان داده شده است. مقایسه شکل (۲) و (۳) نشان می‌دهد که تفاوت روش پیشنهادی نسبت به الگوریتم اصلی ALSBMR، اضافه شدن یک مرحله مجزا برای تعیین کلیدها است که خروجی این مرحله، key_1 و key_2، در مرحله بعدی الگوریتم استفاده می‌شود. بنابراین فرستنده باید بعد از تعیین شدن این کلیدها، آن‌ها را در اختیار گیرنده قرار دهد.

برای حل این مسئله بهینه‌سازی، می‌توان از الگوریتم‌های مختلفی استفاده کرد. در ادامه نحوه انجام این گام با استفاده از الگوریتم بهینه‌سازی ژنتیک (به‌عنوان یک روش بهینه‌سازی قدیمی موفق) و الگوریتم بهینه‌سازی TLBO (به‌عنوان یک روش بهینه‌سازی نسبتاً جدید و جذاب) شرح داده می‌شود.

۲-۳-۱- روش GA-ALSBMR

درصورتی‌که در روش پیشنهادی برای انتخاب کلیدها از الگوریتم ژنتیک استفاده شود، روش پیشنهادی GA-ALSBMR نامیده شده است.



شکل ۳. الگوریتم کلی روش پیشنهادی

اولین گام تعریف ساختار یک کروموزوم به‌عنوان یک عضو از جمعیت و به عبارتی یک راه‌حل برای مسئله موردنظر است. در روش GA-ALSBMR، هر کروموزوم شامل ۴۰ ژن است. مقدار هر ژن، صفر یا یک است. ۲۰ ژن ابتدایی، معادل باینری key_1 و ۲۰ ژن دوم، معادل باینری key_2 است. بدین ترتیب مقدار این کلیدها در بازه $[0, 2^{19}]$ می‌تواند باشد. لازم به ذکر است که تعداد ژن‌های هر کلید می‌تواند به انتخاب فرستنده تغییر کند.

گام دوم، تعیین تابع برازندگی یا تابع هدف مناسب است. دو هدف مختلف برای این مرحله در نظر گرفته شده است: کمترین تغییر در تصویر میزبان و کمترین تغییر در هیستوگرام تصویر میزبان. با توجه به این‌که از الگوریتم بهینه‌سازی تک هدفه استفاده می‌شود، یکی از این توابع می‌تواند به‌عنوان تابع هدف در نظر گرفته شود. بنابراین، بر اساس استفاده از هرکدام از توابع هدف، یک روش پیشنهادی متفاوت وجود دارد.

در صورت استفاده از تابع هدف اول، از آنجا که هدف از بهینه‌سازی کلیدها، یافتن مقادیری از کلید است که با استفاده از آن‌ها در مرحله جاسازی کمترین تغییر در تصویر میزبان ایجاد شود، بنابراین، باید تصویر نهان‌نگاری شده حاصل از کلیدهای هر کروموزوم را تولید کرده و با تصویر میزبان مقایسه کرد.

اگر chr_j، کروموزوم jام در جمعیت باشد و $Cover$ و $Stego$ نیز به ترتیب نشان‌دهنده تصویر میزبان و نهان‌نگاری شده با ابعاد $M\times N$ باشند، مقدار برازندگی هر کروموزوم طبق فرمول زیر محاسبه می‌شود.

$$Fit(chr_j) = \sum_{i=1}^{M}\sum_{j=1}^{N} |\, Cover(i,j) - Stego(i,j)|^2 \qquad (۷)$$

این معیار همان پارامتر MSE است که در محاسبه PSNR نیز کاربرد دارد. در صورت استفاده از تابع هدف دوم، از آنجا که هدف از بهینه‌سازی کلیدها، یافتن مقادیری از کلید است که با استفاده از آن‌ها در مرحله جاسازی کمترین تغییر در هیستوگرام تصویر میزبان ایجاد شود، بنابراین باید تصویر نهان‌نگاری شده حاصل از کلیدهای هر کروموزوم را تولید کرده و هیستوگرام آن را با هیستوگرام تصویر میزبان مقایسه کرد. اگر H_c و H_S نشان‌دهنده هیستوگرام تصویر میزبان و نهان‌نگاری شده باشند، مقدار برازندگی هر کروموزوم در حالت دوم، طبق فرمول زیر محاسبه می‌شود.

$$Fit(chr_j) = \sum_{i=0}^{255} |H_c(i) - H_s(i)| \qquad (۸)$$

اگر N_{pop}، نشان‌دهنده تعداد کروموزوم حاضر در جمعیت هر نسل باشد، باید در ابتدای الگوریتم به این تعداد، کروموزوم تصادفی تولید کرد. سپس مقدار تابع برازندگی موردنظر هر کروموزوم را محاسبه کرد. در هر تکرار الگوریتم ژنتیک، دو مرحله عملیات تقاطع و جهش انجام می‌شود. برای هرکدام از این اعمال یک احتمال رخداد تعیین می‌شود.

اگر P_{cross}، نشان‌دهنده احتمال عملیات تقاطع باشد، در هر تکرار الگوریتم ژنتیک به تعداد $(P_{cross} \times N_{pop})/2$ عملیات

تقاطع باید انجام شود. در هر عملیات تقاطع، دو عضو جمعیت فعلی به عنوان والد انتخاب می‌شوند و از ترکیب آن‌ها دو فرزند جدید ساخته می‌شود. سپس مقدار تابع برازندگی هر فرزند محاسبه می‌شود. درصورتی‌که هر فرزند از بدترین عضو جمعیت (کروموزوم با بیشترین مقدار تابع برازندگی) بهتر باشد، برای تولید جمعیت جدید فرزند جایگزین آن می‌شود. برای انجام عملیات تقاطع، از ترکیب دونقطه‌ای استفاده‌شده است.

بعد از کامل کردن عملیات تقاطع، عملیات جهش انجام می‌شود. اگر P_{mut}، نشان‌دهنده احتمال عملیات جهش باشد، در هر تکرار الگوریتم به تعداد $P_{cross} \times N_{pop}$ عملیات جهش انجام شود. در هر عملیات جهش، یک ژن تصادفی از کروموزوم معکوس می‌شود. اگر مقدار ژن انتخاب‌شده، صفر است تبدیل به یک می‌شود و بالعکس. سپس مقدار تابع برازندگی کروموزوم جدید محاسبه‌شده و درصورتی‌که از کروموزوم اصلی بهتر باشد، در جمعیت جایگزین آن می‌شود.

شرط پایان الگوریتم، تکرار آن به تعداد دفعات از پیش مشخص‌شده است. با پایان یافتن الگوریتم، بهترین کروموزوم (کروموزوم با کمترین مقدار تابع برازندگی) انتخاب‌شده و با کلیدهای حاصل از آن ادامه الگوریتم ALSBMR انجام می‌شود تا تصویر نهان‌نگاری شده موردنظر تولید شود.

۲-۳-۲- روش TLBO-ALSBMR

درصورتی‌که در روش پیشنهادی، برای انتخاب کلیدها از الگوریتم TLBO استفاده شود، روش پیشنهادی TLBO-ALSBMR نامیده شده است. الگوریتم TLBO یا الگوریتم بهینه‌سازی مبتنی بر آموزش-یادگیری، توسط رائو و همکارانش پیشنهاد شده است [۲۱]. ایده اصلی این روش، از یک فرآیند یادگیری از مدرسه کلاسیک شبیه‌سازی شده است. الگوریتم این روش در شکل (۴) نشان داده شده است. در این مقاله برای اولین بار از این روش در نهان‌نگاری استفاده شده است.

اولین گام در این الگوریتم، تعریف ساختار هر فرد حاضر در یک نسل است. اگر x_i، iامین نفر در جمعیت باشد، مقداردهی اولیه آن با فرمول زیر انجام می‌شود.

$$x_i = unifrand\ (varMin, varMax, varSize) \qquad (۹)$$

پارامترهای *varmin*، *varMax* و *varSize* به ترتیب نشان دهنده تعداد، حداقل و حداکثر مقدار متغیرها است. در روش پیشنهادی مقدار این پارامترها به ترتیب ۲، ۱ و ۱۰۰۰۰۰ انتخاب شده است. البته مقدار حداقل و حداکثر متغیرها قابل تغییر است. باید برای هر x_i، مقدار تابع برازندگی محاسبه شود. تابع برازندگی استفاده‌شده، مشابه توابع روش قبلی است.

در گام بعد، میانگین اعضای جمعیت، x_{mean}، محاسبه می‌شود و فردی که بهترین کیفیت (کمترین مقدار تابع برازندگی) دارد به‌عنوان معلم انتخاب می‌شود که با $x_{teacher}$ نشان داده می‌شود. بقیه افراد به‌عنوان دانش‌آموز شناخته می‌شوند.

در فاز آموزش، هر دانش‌آموز تحت تأثیر اختلاف بین دانش معلم و کیفیت میانگین کل دانش آموزان قرار می‌گیرد. نحوه انجام این آموزش، به‌صورت معادله زیر است:

$$x_{newi}=x_i + r \times (x_{teacher} - T_f \times x_{mean}) \qquad (۱۰)$$

T_f، عامل آموزش و در بازه [۲و۱] قرار دارد. r، یک عدد تصادفی یکنواخت و در بازه [۱و۰] است. اگر برازندگی x_{newi} بهتر از برازندگی x_i باشد، جایگزین x_i می شود.

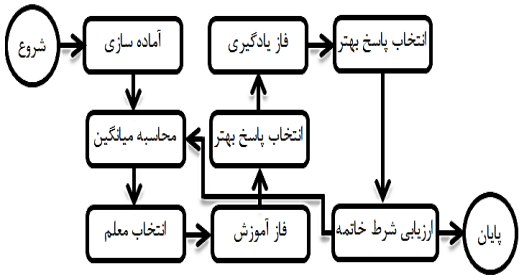
در مرحله بعد، فاز یادگیری هر دانش‌آموز با یک دانش‌آموز دیگر که به‌صورت تصادفی انتخاب شده است، انجام می‌شود و اگر راه‌حل تولیدشده جدید بهتر باشد، خود را به‌روزرسانی می‌کند. فرض کنید یک فرد تصادفی x_j برای تعامل و آموختن به فرد x_i انتخاب شود، در این حالت دو اتفاق امکان‌پذیر است:

اگر x_j بهتر از x_i باشد، اصلاح x_i با فرمول ۱۱ و در غیر این صورت با فرمول ۱۲ انجام می‌شود:

$$x_{newi}=x_i + r \times (x_j - x_i) \qquad (۱۱)$$

$$x_{newi}=x_i + r \times (x_i - x_j) \qquad (۱۲)$$

پس از محاسبه x_{newi}، مقدار تابع برازندگی برای این عضو جدید محاسبه می‌شود. اگر x_{newi} بهتر از x_i باشد، x_{newi} جایگزین x_i می‌شود.



شکل ۴. الگوریتم بهینه‌سازی TLBO

شرط خاتمه الگوریتم تعداد تکرار در نظر گرفته شده است. با پایان یافتن الگوریتم، بهترین عضو از میان جمعیت انتخاب می‌شود و با کلیدهای حاصل از آن ادامه الگوریتم ALSBMR انجام می‌شود تا تصویر نهان‌نگاری شده موردنظر تولید شود.

۳- نتایج و بحث

پس از پیشنهاد الگوریتم نهان‌نگاری جدید، باید این الگوریتم در محیطی نرم‌افزاری پیاده‌سازی شده و کارایی آن سنجیده شود. علاوه بر سنجش هر روش به‌تنهایی، باید کارایی این روش نسبت به دیگر روش‌های موجود نیز مقایسه شود. روش‌های پیشنهادی

در نرم‌افزار Matlab پیاده‌سازی شده است. برای مقایسه از روش ALSBMR استفاده شده است. مقایسه روش‌های پیشنهادی با این روش، میزان بهبود روش‌های پیشنهادی را بهتر نشان می‌دهند. برای سنجش کارایی الگوریتم نهان‌نگاری، معیارهای متفاوتی وجود دارد. اما این معیارها را در سه بخش می‌توان تقسیم‌بندی کرد: ظرفیت جاسازی، کیفیت تصویر نهان‌نگاری شده (مشاهده ناپذیری)، امنیت در برابر حملات (کشف ناپذیری). البته در هرکدام از بخش‌ها، معیارهای مختلفی برای اندازه‌گیری و سنجش وجود دارد. با توجه به اینکه روش پیشنهادی در این مقاله قابلیت جاسازی حداکثر یک بیت در هر پیکسل را دارد، بنابراین حداکثر ظرفیت جاسازی روش‌های GA_ALSBMR و TLBO_ALSBMR مشابه روش‌های LSBM و ALSBMR است. بنابراین از نظر ظرفیت جاسازی، تمام این روش‌ها یکسان هستند و هیچ‌کدام از روش‌ها، برتری بر دیگر روش‌ها ندارد. بنابراین ارزیابی و مقایسه روش‌ها بر اساس دو معیار کیفیت تصویر نهان‌نگاری شده و امنیت انجام می‌شود.

یکی از ویژگی‌های مهم روش‌های نهان‌نگاری، وابستگی عملکرد آن‌ها به مجموعه آزمون استفاده‌شده برای ارزیابی است. هر روش نهان‌نگاری ممکن است در بعضی از مجموعه تصاویر عملکرد متفاوتی نسبت به مجموعه تصاویر آزمون دیگر داشته باشد. در این بخش برای انجام ارزیابی جامعتر از دو مجموعه تصاویر آزمون استفاده شده است.

- پایگاه داده تصاویر NRCS: این پایگاه داده شامل تصاویر مرتبط با منابع طبیعی و محافظت از آن‌ها در آمریکا است.
- پایگاه داده تصاویر Camera: این پایگاه داده مجموعه‌ای از تصاویر گرفته‌شده با ۲۴ دوربین دیجیتال مختلف است. این تصاویر از مناظر طبیعی، ساختمان‌ها و ... گرفته شده است. تصاویر این پایگاه داده با فرمت خام ذخیره شده‌اند، یعنی تحت هیچ فشرده‌سازی با اتلافی قرار نگرفته‌اند.

از هرکدام از دو پایگاه داده آزمون NRCS و Camera، ۲۰۰ تصویر تصادفی انتخاب شده است که در ادامه از آن‌ها برای آزمون استفاده می‌شود. در ادامه برای اشاره به هرکدام از این دو مجموعه از همین اسامی NRCS و Camera استفاده می‌شود.

با توجه به اینکه روش ALSBMR یک روش تطبیقی است، بنابراین انتظار می‌رود بیشترین تغییرات در نواحی لبه تصویر رخ دهد. برای مشاهده این واقعیت، می‌توان تصویر تفاوت که نشان‌دهنده اختلاف تصویر میزبان و نهان‌نگاری شده است را بررسی کرد. در شکل (۵)، تصویر تفاوت حاصل از جاسازی ۰/۱ bpp، ۰/۲ bpp و ۰/۳ bpp برای تصویر Lena نشان داده شده است. نواحی سفید در این تصویر نشان‌دهنده پیکسل‌هایی است که در اثر جاسازی تغییریافته‌اند. این تصاویر به‌خوبی نشان می‌دهند که نواحی تغییریافته نواحی لبه تصویر هستند و با افزایش درصد جاسازی نواحی لبه بیشتری شناسایی‌شده و جاسازی در آن‌ها انجام می‌شود.

(الف) (ب) (ج)

شکل ۵. تصویر تفاوت الف) ۰/۱ bpp ب) ۰/۲ bpp ج) ۰/۳ bpp

۳-۱- بررسی کارایی روش TLBO-ALSBMR

در این قسمت کارایی روش پیشنهادی که ترکیب ALSBMR و TLBO است، مورد ارزیابی قرار می‌گیرد. در این روش برای تشخیص مقدار key_1 و key_2 از الگوریتم بهینه‌سازی TLBO استفاده می‌شود. در الگوریتم بهینه‌سازی، امکان استفاده از دو تابع برازندگی وجود دارد. در این قسمت کارایی هر دو تابع مقایسه می‌شود. در صورت استفاده از تابع MSE، از روش پیشنهادی با عنوان TLBO_ALSBMR1 و در صورت استفاده از تابع اختلاف هیستوگرام، از روش پیشنهادی با عنوان TLBO_ALSBMR2 یاد می‌شود.

در جدول (۱ و ۲)، میانگین PSNR برای دو سطح جاسازی ۰/۳ bpp و ۰/۵ bpp در دو مجموعه تصاویر NRCS و Camera برای روش ALSBMR اصلی و دو روش پیشنهادی مبتنی بر TLBO نمایش داده شده است. با توجه به این‌که روش

TLBO_ALSBMR1 به دنبال بهینه کردن مقدار MSE است، بنابراین انتظار می‌رود بهبود PSNR بیشتری نسبت به روش TLBO_ALSBMR2 داشته باشد. نتایج جدول (۱ و ۲) این ادعا را تأیید می‌کند.

معیار سنجش بعدی، مقدار کشف پذیری در برابر حملات است. حملات استفاده‌شده شامل Ker1 [۲۲]، Ker2 [۲۲]، CNGL [۲۳] و ALE [۲۴] می‌باشند. جدول (۳ و ۴)، دقت کشف حملات مختلف را برای دو سطح جاسازی ۰/۳ bpp و ۰/۵ bpp برای تصاویر مجموعه NRCS و Camera به تفکیک نشان می‌دهد. در شکل (۶)، یک نمونه از نمودارهای ROC حاصل از حمله Ker1 برای تصاویر NRCS در سطح جاسازی bpp ۰/۵ نشان داده شده است. نتایج جدول (۳ و ۴) نشان می‌دهد با توجه به این‌که روش TLBO_ALSBMR2 به دنبال کمتر کردن تغییرات هیستوگرام است، در اکثر موارد این روش احتمال کشف کمتری در برابر حملات دارد.

جدول ۱. میانگین PSNR برای مجموعه تصاویر NRCS در سطوح جاسازی مختلف برای روش‌های مبتنی بر TLBO

	۰/۳ bpp	۰/۵ bpp
ALSBMR	۵۶/۹۱	۵۴/۵۹
TLBO_ALSBMR1	۵۷/۴۷	۵۵/۱۸
TLBO_ALSBMR2	۵۷/۲۰	۵۴/۹۴

جدول ۲. میانگین PSNR برای مجموعه تصاویر Camera در سطوح جاسازی مختلف برای روش‌های مبتنی بر TLBO

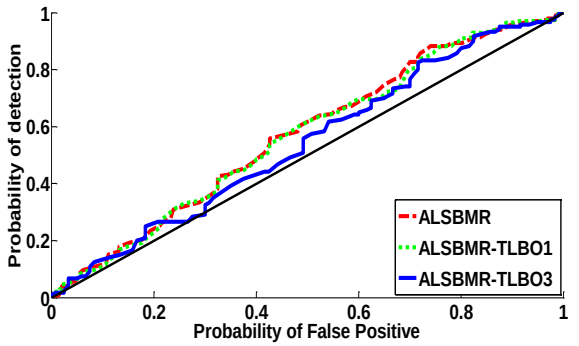
	۰/۳ bpp	۰/۵ bpp
ALSBMR	۵۶/۲۹	۵۳/۵۰
TLBO_ALSBMR1	۵۶/۸۶	۵۴/۰۶
TLBO_ALSBMR2	۵۶/۶۱	۵۳/۸۲

جدول ۳. دقت کشف روش‌های ALSBMR و دو روش پیشنهادی مبتنی بر TLBO توسط چهار حمله برای تصاویر NRCS

درصد جاسازی	نام روش	Ker1	Ker2	CNGL	ALE
۰/۳ bpp	ALSBMR	۰/۰۶۸۵	۰/۰۰۹۶	۰/۰۵۶۳	۰/۲۷۱۸
	TLBO_ALSBMR1	۰/۰۶۵۹	۰/۰۱۰۵	۰/۰۷۹۰	۰/۲۵۷۲
	TLBO_ALSBMR2	۰/۰۶۳۹	۰/۰۰۸۲	۰/۰۲۸۰	۰/۲۴۰۱
۰/۵ bpp	ALSBMR	۰/۱۴۱۵	۰/۰۰۲۴	۰/۰۱۷۳	۰/۴۶۶۸
	TLBO_ALSBMR1	۰/۱۳۳۱	۰/۰۱۲۴	۰/۰۲۵۰	۰/۵۰۲۲
	TLBO_ALSBMR2	۰/۰۸۳۱	۰/۰۰۲۰	۰/۰۱۶۲	۰/۴۵۱۸

جدول ۴. دقت کشف روش‌های ALSBMR و دو روش پیشنهادی مبتنی بر TLBO توسط چهار حمله برای تصاویرCamera

درصد جاسازی	نام روش	ker1	ker2	CNGL	ALE
۰/۳ bpp	ALSBMR	۰/۰۰۶۸	۰/۰۰۵۳	۰/۰۱۳۲	۰/۱۵۷۹
	TLBO_ALSBMR1	۰/۰۱۷۱	۰/۰۰۵۹	۰/۰۰۹۴	۰/۱۸۵۳
	TLBO_ALSBMR2	۰/۰۰۶۱	۰/۰۰۲۱	۰/۰۳۵۸	۰/۱۴۴۸
۰/۵ bpp	ALSBMR	۰/۰۲۹۸	۰/۱۷۱۹	۰/۰۳۸۸	۰/۵۷۳۹
	TLBO_ALSBMR1	۰/۰۴۹۸	۰/۱۶۴۲	۰/۰۰۷۰	۰/۵۸۰۸
	TLBO_ALSBMR2	۰/۰۲۵۳	۰/۱۶۱۶	۰/۰۴۷۴	۰/۵۶۰۸



شکل ۶. نمودار ROC حمله Ker1 برای مجموعه NRCS

۳-۲- بررسی کارایی روش GA-ALSBMR

در این قسمت کارایی روش پیشنهادی که ترکیب ALSBMR و الگوریتم ژنتیک است، مورد ارزیابی قرار می‌گیرد. در این روش برای تشخیص مقدار key_1 و key_2 از الگوریتم بهینه‌سازی ژنتیک استفاده شده است. در الگوریتم بهینه‌سازی، امکان استفاده از دو تابع برازندگی وجود دارد. در این قسمت کارایی هر دو تابع مقایسه می‌شود. در صورت استفاده از تابع MSE، از روش پیشنهادی با عنوان GA_ALSBMR1 و در صورت استفاده از تابع اختلاف هیستوگرام، از روش پیشنهادی با عنوان GA_ALSBMR2 یاد می‌شود.

در جدول (۵) و (۶)، میانگین PSNR برای دو سطح جاسازی bpp ۰/۳ و bpp ۰/۵ در دو مجموعه تصاویر NRCS و Camera برای روش ALSBMR اصلی و دو روش پیشنهادی مبتنی بر GA نمایش داده شده است. با توجه به اینکه روش GA_ALSBMR1 به دنبال بهینه کردن مقدار MSE است، بنابراین انتظار می‌رود بهبود PSNR بیشتری نسبت به روش GA_ALSBMR2 داشته باشد. نتایج جدول (۵) و (۶) این ادعا را تأیید می‌کند.معیار سنجش بعدی، مقدار کشف پذیری در برابر حملات است. حملات استفاده‌شده مانند قسمت قبل شامل Ker1 [۲۲]، Ker2 [۲۲]، CNGL [۲۳] و ALE [۲۴] می‌باشند. جدول (۷) و (۸)، دقت

کشف حملات مختلف را برای دو سطح جاسازی ۰/۳ bpp و ۰/۵ bpp برای تصاویر مجموعه NRCS و Camera را به تفکیک نشان می‌دهد. نتایج این جدول‌ها، نشان‌دهنده احتمال کشف کمتر روش GA_ALSBMR2 نسبت به روش GA_ALSBMR1 و ALSBMR در اکثر موارد است.

۳-۳- مقایسه روش‌های پیشنهادی

در دو قسمت قبل روش‌های پیشنهادی مبتنی بر TLBO و ژنتیک هرکدام به‌تنهایی نسبت به ALSBMR اصلی ارزیابی شدند. در اغلب موارد بهبود وجود داشت. اما اگر بخواهید از میان چهار روش پیشنهادی، بهترین را انتخاب کنید، باید یک‌بار دیگر آمار ارائه‌شده در قسمت قبل مرور شود.

در جدول (۹ و ۱۰) میانگین PSNR برای چهار روش پیشنهادی در دو سطح جاسازی و برای دو مجموعه تصویر NRCS و Camera را نشان می‌دهد. بررسی این نتایج نشان می‌دهد اگرچه نتایج بسیار نزدیک است، اما در حالتی که از الگوریتم بهینه‌سازی TLBO و تابع هدف MSE استفاده شده است، تصاویر نهان‌نگاری شدهی تولیدشده بیشترین کیفیت و به عبارتی بهترین PSNR را کسب کرده‌اند. بنابراین، الگوریتم TLBO در بهینه کردن تابع هدف موردنظر موفق‌تر بوده است.

در جدول (۱۱ و ۱۲) دقت کشف توسط چهار حمله موردنظر برای چهار روش پیشنهادی در دو سطح جاسازی و برای دو مجموعه تصویر NRCS و Camera نشان داده شده است. بررسی این نتایج نشان می‌دهد در اکثر موارد نتایج بسیار نزدیک است. اگرچه دو روش GA_ALSBMR2 و TLBO_ALSBMR2 نتایج بهتری نسبت به دو روش دیگر کسب کرده‌اند، ولی هیچ‌کدام از این دو برتری محسوسی نسبت به یکدیگر ندارند و تقریباً عملکرد یکسانی دارند.

جدول ۵. میانگین PSNR برای مجموعه تصاویر NRCS در سطوح جاسازی مختلف برای روش‌های مبتنی بر GA

	۰/۳ bpp	۰/۵ bpp
ALSBMR	۵۶/۹۱	۵۴/۵۹
GA_ALSBMR1	۵۷/۴۵	۵۵/۱۳
GA_ALSBMR2	۵۷/۱۸	۵۴/۸۹

جدول ۶. میانگین PSNR برای مجموعه تصاویر Camera در سطوح جاسازی مختلف برای روش‌های مبتنی بر GA

	۰/۳ bpp	۰/۵ bpp
ALSBMR	۵۶/۲۹	۵۳/۵۰
GA_ALSBMR1	۵۶/۸۵	۵۴/۰۴
GA_ALSBMR2	۵۶/۵۹	۵۳/۸۱

جدول ۷. دقت کشف روش‌های ALSBMR و دو روش پیشنهادی مبتنی بر GA توسط چهار حمله برای تصاویر NRCS

درصد جاسازی	نام روش	Ker1	Ker2	CNGL	ALE
۰/۳ bpp	ALSBMR	۰/۰۶۸۵	۰/۰۰۹۶	۰/۰۵۶۳	۰/۲۷۱۸
	GA_ALSBMR1	۰/۰۶۳۵	۰/۰۱۳۳	۰/۰۱۵۶	۰/۲۳۱۹
	GA_ALSBMR2	۰/۰۵۸۷	۰/۰۰۹۰	۰/۰۱۱۷	۰/۲۲۹۶
۰/۵ bpp	ALSBMR	۰/۱۴۱۵	۰/۰۰۲۴	۰/۰۱۷۳	۰/۴۵۱۸
	GA_ALSBMR1	۰/۱۳۱۲	۰/۰۰۲۰	۰/۰۲۳۳	۰/۴۰۱۹
	GA_ALSBMR2	۰/۱۲۲۰	۰/۰۰۱۷	۰/۰۳۰۳	۰/۳۹۸۶

جدول ۸. دقت کشف روش‌های ALSBMR و دو روش پیشنهادی مبتنی بر GA توسط چهار حمله برای تصاویرCamera

درصد جاسازی	نام روش	Ker1	Ker2	CNGL	ALE
۰/۳ bpp	ALSBMR	۰/۰۰۶۸	۰/۰۰۵۳	۰/۰۰۹۴	۰/۱۵۷۹
	GA_ALSBMR1	۰/۰۰۷۷	۰/۰۱۰۶	۰/۰۴۴۶	۰/۱۸۳۱
	GA_ALSBMR2	۰/۰۰۲۷	۰/۰۰۴۶	۰/۰۱۹۶	۰/۱۵۱۱
۰/۵ bpp	ALSBMR	۰/۰۲۹۸	۰/۱۷۱۹	۰/۰۳۸۸	۰/۵۷۳۹
	GA_ALSBMR1	۰/۰۲۲۳	۰/۱۷۱۳	۰/۰۴۹۲	۰/۵۸۹۱
	GA_ALSBMR2	۰/۰۲۰۸	۰/۱۶۵۸	۰/۰۰۵۷	۰/۵۶۳۹

جدول ۹. میانگین PSNR برای مجموعه تصاویر NRCS در سطوح جاسازی مختلف برای روش‌های پیشنهادی

	۰/۳ bpp	۰/۵ bpp
TLBO_ALSBMR1	۵۷/۴۷	۵۵/۱۸
TLBO_ALSBMR2	۵۷/۲۰	۵۴/۹۴
GA_ALSBMR1	۵۷/۴۵	۵۵/۱۳
GA_ALSBMR2	۵۷/۱۸	۵۴/۸۹

جدول ۱۰. میانگین PSNR برای مجموعه تصاویر Camera در سطوح جاسازی مختلف برای روش‌های پیشنهادی

	۰/۳ bpp	۰/۵ bpp
TLBO_ALSBMR1	۵۶/۸۶	۵۴/۰۶
TLBO_ALSBMR2	۵۶/۶۱	۵۳/۸۲
GA_ALSBMR1	۵۶/۸۵	۵۴/۰۴
GA_ALSBMR2	۵۶/۵۹	۵۳/۸۱

جدول ۱۱. دقت کشف روش‌های پیشنهادی توسط چهار حمله برای تصاویر NRCS

درصد جاسازی	نام روش	Ker1	Ker2	CNGL	ALE
۰/۳ bpp	TLBO_ALSBMR1	۰/۰۶۵۹	۰/۰۱۰۵	۰/۰۷۹۰	۰/۲۵۷۲
	TLBO_ALSBMR2	۰/۰۶۳۹	۰/۰۰۸۲	۰/۰۲۸۰	۰/۲۴۰۱
	GA_ALSBMR1	۰/۰۶۳۵	۰/۰۱۳۳	۰/۰۱۵۶	۰/۲۳۱۹
	GA_ALSBMR2	۰/۰۵۸۷	۰/۰۰۹۰	۰/۰۱۱۷	۰/۲۲۹۶
۰/۵ bpp	TLBO_ALSBMR1	۰/۱۳۳۱	۰/۰۱۲۴	۰/۰۲۵۰	۰/۵۰۲۲
	TLBO_ALSBMR2	۰/۰۸۳۱	۰/۰۰۲۰	۰/۰۱۶۲	۰/۴۵۱۸
	GA_ALSBMR1	۰/۱۳۱۲	۰/۰۰۲۰	۰/۰۲۳۳	۰/۴۰۱۹
	GA_ALSBMR2	۰/۱۲۲۰	۰/۰۰۱۷	۰/۰۳۰۳	۰/۳۹۸۶

جدول ۱۲. دقت کشف روش‌های پیشنهادی توسط چهار حمله برای تصاویر Camera

درصد جاسازی	نام روش	Ker1	Ker2	CNGL	ALE
۰/۳ bpp	TLBO_ALSBMR1	۰/۰۱۷۱	۰/۰۰۵۹	۰/۰۰۹۴	۰/۱۸۵۳
	TLBO_ALSBMR2	۰/۰۰۶۱	۰/۰۰۲۱	۰/۰۳۵۸	۰/۱۴۴۸
	GA_ALSBMR1	۰/۰۰۷۷	۰/۰۱۰۶	۰/۰۴۴۶	۰/۱۸۳۱
	GA_ALSBMR2	۰/۰۰۲۷	۰/۰۰۴۶	۰/۰۱۹۶	۰/۱۵۱۱
۰/۵ bpp	TLBO_ALSBMR1	۰/۰۴۹۸	۰/۱۶۴۲	۰/۰۰۷۰	۰/۵۸۰۸
	TLBO_ALSBMR2	۰/۰۲۵۳	۰/۱۶۱۶	۰/۰۴۷۴	۰/۵۶۰۸
	GA_ALSBMR1	۰/۰۲۲۳	۰/۱۷۱۳	۰/۰۴۹۲	۰/۵۸۹۱
	GA_ALSBMR2	۰/۰۲۰۸	۰/۱۶۵۸	۰/۰۰۵۷	۰/۵۶۳۹

۳-۴- بررسی کارایی روش پیشنهادی نسبت به روش‌های موجود

در گام آخر لازم است عملکرد روش‌های پیشنهادی نسبت به جدیدترین و موفق‌ترین روش‌های موجود سنجیده شود. برای انجام این آزمون، تعدادی از روش‌های موجود که راهبردهای مختلفی در انتخاب مکان‌های مناسب برای جاسازی دارند، انتخاب شده‌اند. اگرچه از ارائه روش CBL [۲۵] چندین سال می‌گذرد، اما به دلیل راهبرد خاصی که در این روش برای انتخاب مکان جاسازی وجود دارد، این روش یکی از روش‌های مبتنی بر LSBM است که در تولید تصویر نهان‌نگاری شده با کیفیت بالا بسیار موفق بوده است. روش‌های دیگر انتخاب شده [۲۶-۲۹]، روش‌های جدیدتری هستند که از روش‌های بهینه سازی در فرآیند انتخاب مکان های مناسب برای جاسازی استفاده کرده‌اند.

نتایج ارائه شده در جدول ۱۳، میانگین PSNR برای پنج روش پیشین و روش پیشنهادی در دو سطح جاسازی برای مجموعه تصویر NRCS را نشان می‌دهد. بررسی این نتایج نشان دهنده موفقیت روش پیشنهادی در تولید تصاویر نهان‌نگاری شده با بهترین کیفیت (بیشترین PSNR) است.

جدول ۱۳. میانگین PSNR برای مجموعه تصاویر NRCS در سطوح جاسازی مختلف برای روش‌های پیشین و روش پیشنهادی

	۰/۳ bpp	۰/۵ bpp
CBL [۲۵]	۵۶/۳۵	۵۴/۱۴
LCG [۲۶]	۵۳/۳۷	۵۱/۱۵
GA2019[۲۷]	۵۳/۶۰	۵۱/۳۵
LCG-GA[۲۸]	۴۸/۶۰	۴۶/۳۸
MKGM [۲۹]	۵۶/۳۸	۵۴/۳۴
TLBO_ALSBMR1	۵۷/۴۷	۵۵/۱۸

در انتها ذکر چند نکته الزامی است:

- معمولا در روش‌های نهان نگاری برای انتخاب تصادفی مکان‌های جاسازی از توابع تولید اعداد شبه‌تصادفی استفاده می‌کنند که تعداد زیادی از این توابع وجود دارد و توانایی آنها در تولید اعداد کاملا تصادفی نیز متفاوت است. همه این توابع به یک یا چند هسته ابتدایی نیاز دارند. روش پیشنهادی در این مقاله به صورت ترکیبی با هر کدام از توابع تولید اعداد شبه تصادفی قابل استفاده است. به عبارت دیگر، روش پیشنهادی می‌تواند عملکرد هر تابع تولید اعداد شبه تصادفی را بهبود دهد، زیرا مرحله انتخاب هسته ابتدایی با توجه به تصویر میزبان انجام می‌شود. بنابراین مزیت ایده پیشنهادی، بهبود میزان تصادفی بودن مکان های جاسازی نیست، بلکه انتخاب مکان‌های جاسازی با توجه به تصویر میزبان و بیت‌های داده پیام است که این خاصیت در صورت استفاده از یک تابع تولید اعداد شبه تصادفی به تنهایی وجود ندارد.
- اگرچه انتخاب کلیدها به‌صورت هوشمندانه در این مقاله برای روش ALSBMR بررسی شد، اما از این ایده می‌توان برای اغلب روش‌های نهان‌نگاری استفاده کرد.
- نتایج نشان می‌دهد عملکرد روش پیشنهادی بیشتر به تابع برازندگی انتخاب‌شده بستگی دارد و روش بهینه‌سازی نسبتاً تأثیر کمتری دارد. انتخاب تابع برازندگی باید به نحوی انجام شود که تغییرات حاصل از جاسازی کمتر شود تا حملات در کشف تصاویر نهان‌نگاری شده موفقیت کمتری داشته باشند.
- نتایج بررسی نشان می‌دهد الگوی پیشنهادی می‌تواند برای تصاویر آزمون مختلف مناسب باشد و نسبت به روش پایه بهبود عملکرد اتفاق می‌افتد.
- در ازای بهبود عملکرد، زمان لازم برای جاسازی داده افزایش می‌یابد که با توجه به غیر برخط بودن اجرای فرآیند نهان‌نگاری در اغلب کاربردها، معیار زمان اجرا از اهمیت کمتری

برخوردار است و به عنوان معیار مقایسه روش‌های نهان‌نگاری لحاظ نمی‌شود. از طرفی، با توجه به پیشرفت روش‌های نهان‌کاوی و موفقیت آنها در کشف داده پنهان شده، بنابراین، ایده‌هایی که می‌توانند به پنهان‌سازی مطمئن تر داده‌ها کمک کنند، احتمالا زمان بیشتری برای انجام این کار نیاز دارند که استفاده از الگوریتم‌های بهینه سازی در فرآیند جاسازی یکی از این ایده‌ها است.

- روش پیشنهادی یک روش نهان‌نگاری است، بنابراین، حتما گیرنده داده ارسال شده را به صورت کامل و بدون هیچ خطایی از تصویر دریافتی استخراج می‌کند. البته شرط دشمن غیرفعال، شرط الزامی در کانال ارسال است و تصویر نهان‌نگاری شده تحت حملاتی از قبیل برش، اضافه شدن نویز، تغییر اندازه، فشرده سازی و ... قرار نمی‌گیرد.

۴- نتیجه‌گیری

برخلاف روش‌های نهان نگاری با ظرفیت جاسازی ثابت در تمام پیکسل‌ها، در روش‌های نهان‌نگاری تطبیقی ظرفیت جاسازی در نواحی تصویر با توجه به یکنواخت یا لبه بودن آن‌ها، تعیین می‌شود. روش ALSBMR، یک روش تطبیقی است که اجرای آن به دو کلید نیاز دارد که مانند اغلب روش‌های دیگر این کلیدها به‌صورت تصادفی توسط فرستنده انتخاب و به اطلاع گیرنده می‌رسد. در این مقاله، برای بهبود عملکرد روش ALSBMR ایده انتخاب کلیدها به‌صورت هوشمندانه پیشنهاد شده است. در روش پیشنهادی، برای یافتن کلیدهای بهینه از دو الگوریتم بهینه‌سازی ژنتیک (GA) و الگوریتم بهینه‌سازی آموزش- یادگیری (TLBO) استفاده شده است. نتایج نشان می‌دهد، کیفیت و امنیت تصویر تولید شده در روش پیشنهادی نسبت به روش پایه بهبود یافته است. اگرچه انتخاب هوشمندانه کلید جاسازی در این مقاله برای روش ALSBMR پیاده‌سازی شده است، اما با توجه به این‌که اغلب روش‌های نهان‌نگاری نیاز به کلیدهای جاسازی دارند، هوشمند کردن فرآیند انتخاب این کلیدها از طریق الگوی پیشنهادی در این مقاله می‌تواند به بهبود عملکرد روش‌های موجود کمک کند. اما انتخاب تابع برازندگی مناسب به عنوان یک مسئله باز نیاز به تحقیقات بیشتر دارد.

۵- مرجع‌ها

[1] Kadhim, I. J.; Premaratne, P.; Vial, P. J.; "Improved Image Steganography Based on Super-Pixel and Coefficient-Plane-Selection"; Signal Process. 2020, 171, 107481.

[2] Kadhim, I. J.; Premaratne, P.; Vial P. J.; Halloran, B.; "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research"; Neurocomputing 2018, 335, 299-326.

[3] Luo, W.; Huang, F.; Huang, J.; "Edge Adaptive Image Steganography Based on LSB Matching Revisited"; IEEE Trans. Inf. Forensics Secur. 2010, 5, 201-214.

[4] Hong, W.; Chen, T. S.; "A Novel Data Embedding Method using Adaptive Pixel Pair Matching"; IEEE Trans. Inf. Forensics Secur. 2011, 7, 176-184.

[5] Hussain, M.; Abdul Wahab, A. W.; Ho, A. T. S.; Javed, N.; Jung, K. H.; "A Data Hiding Scheme Using Parity-Bit Pixel Value Differencing and Improved Rightmost Digit Replacement"; Signal Process. Image Commun. 2017, 50, 44-57.

[6] Liao, X.; Qin, Z.; Ding, L.; "Data Embedding in Digital Images Using Critical Functions"; Signal Process. Image Commun. 2017, 58, 146–156,

[7] Chen, J.; "A PVD-Based Data Hiding Method with Histogram Preserving Using Pixel Pair Matching"; Signal Process. Image Commun. 2014, 29, 375–384.

[8] Shen, S. Y.; Huang, L. H.; "A Data Hiding Scheme Using Pixel Value Differencing and Improving Exploiting Modification Directions"; Comput. Secur. 2015, 48, 131–141.

[9] Hong, W.; Chen, T. S.; Luo, C. W.; "Data Embedding Using Pixel Value Differencing and Diamond Encoding with Multiple-Base Notational System"; J. Syst. Soft. 2012, 85, 1166–1175.

[10] Rabie, T.; Kamel, I.; "High-Capacity Steganography: A Global-Adaptive-Region Discrete Cosine Transform Approach"; Multimed. Tools Appl. 2017, 76, 6473–6493.

[11] Rabie, T.; Baziyad, M.; Kamel, I.; "Enhanced High Capacity Image Steganography Using Discrete Wavelet Transform and the Laplacian Pyramid"; Multimed. Tools Appl. 2018, 77, 23673-23698.

[12] Di, F.; Zhang, M.; Liao, X.; Liu, J.; "High-Fidelity Reversible Data Hiding by Quadtree-Based Pixel Value Ordering"; Multimed. Tools Appl. 2018, 78, 7125-7141.

[13] Al-Qershi, O. M.; Khoo, B. E.; "Controlling Hiding Capacity Using Image Characteristics with a 2D-DE Data Hiding Scheme"; AEU-Int. J. Electron C. 2014, 68, 346–350.

[14] Ghosal, S. K.; Mandal, J. K.; Sarkar, R.; "High Payload Image Steganography Based on Laplacian of Gaussian (LoG) Edge Detector"; Multimed.Tools Appl. 2018, 77, 30403-30418.

[15] Atta, R.; Ghanbari, M.; "A High Payload Steganography Mechanism Based on Wavelet Packet Transformation and Neutrosophic Set"; J. Vis. Commun. Image R. 2018, 35, 42-54.

[16] Gaurav, K; Ghanekar, U.; "Image Steganography Based on Canny Edge Detection, Dilation Operator and Hybrid Coding"; J. Inf. Secur. Appl. 2018, 41, 41-51.

[17] Atee, H. A.; Ahmad, R.; Noor, N. M.; Rahma, A. M. S.; Aljeroudi, Y.; "Extreme Learning Machine Based Optimal Embedding Location Finder for Image Steganography"; PLoS ONE 2017, 12, 1-23.

[18] Roy, R.; Laha, S.; "Optimization of Stego Image Retaining Secret Information Using Genetic Algorithm with 8-Connected PSNR"; Proc. Comput. Sci. 2015, 60, 468–477.

[19] Ghaleb Al-Jbara, H. A.; Mat Kiah, L. B.; Jalab, H. A.; "Increased Capacity of Image Based Steganography Using Artificial Neural Network"; AIP Conf. Proc. 2012, 1482 , 20–25.

[20] Nipanikar, S. I.; Deepthi, V. H.; Kulkarni, N.; "A Sparse Representation Based Image Steganography Using Particle Swarm Optimization and Wavelet Transform"; Alex. Eng. J. 2017, 57, 2343-2356.

[21] Rao, R. V.; Savsani, V. J.; Vakharia, D. P.; "Teaching–Learning-Based Optimization: A Novel Method for Constrained Mechanical Design Optimization Problems"; Comput. Aided Des. 2011, 43, 303-315.

[22] Ker, A.; "Steganalysis of LSB Matching in Grayscale Images"; IEEE Signal Process. Lett. 2005, 12, 441–444.

[23] Huang, F.; Li, B.; Huang, J.; "Attack LSB Matching Steganography by Counting Alteration Rate of the Number of Neighbourhood Gray Levels"; Proc. IEEE ICIP 2007, 1, 401-404.

[24] Cancelli, G.; Doerr, G.; Cox, I. J.; Barni, M.; "Detection of ±1 LSB Steganography Based on the Amplitude of Histogram Local Extrema"; IEEE Int. Con. Image Process. 2008, 1288-1291.

[25] Sabeti, V.; Samavi, S; Shirani, S.; "An Adaptive LSB Matching Steganography Based on Octonary Complexity Measure"; Multimed. Tools Appl. 2013, 64, 777-793.

[26] Shah, P. D.; Bichkar, R. S; "A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator"; Int. Con. Intelli. Comput. Appl. 2018, 119-129.

[27] Wazirali, R.; Alasmary, W.; Mahmoud, M. M; Alhindi, A.; "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms"; IEEE Acc. 2019, 7, 133496-133508.

[28] Shah, P.D.; Bichkar, R.S.; "Genetic Algorithm Based Imperceptible Spatial Domain Image Steganography Technique with High Payload Capacity"; Int. J. Rec. Tech. Eng. (IJRTE), 2019, 224-229.

[29] Sabeti, V.; Faiazi, S.; Shirinkhah, H.; "Improving Security of LSBM Steganography by Using of Genetic Algorithm, Multi-Key and Blocking"; Iranian J. Elec. Comp. Eng., 2020, 78, 49-58. (In Persian)