Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 9, Number 4, Winter 2021, pp. 70-82
Received: 12/10/2019, Revised: 05/25/2020, Accepted: 11/24/2020

Secure Image Steganography with High Visual Image Quality Based on LSBM and Genetic Algorithm

Vajiheh Sabeti[1*], Sepideh Faiazi[2]
1*- Department of Engineering and Technology, Alzahra University, Tehran, Iran.
2- Department of Engineering and Technology, Alzahra University, Tehran, Iran.
[1*]v.sabeti@alzahra.ac.ir and [2] s.fayazi@student.alzahra.ac.ir

Corresponding author address: Vajiheh Sabeti, Faculty of Engineering and Technology, Alzahra University, Tehran, Iran, Post Code: 1993893973.

Abstract- The LSB matching method or LSBM is one of the simplest methods of steganography that has been proposed relatively successful attacks for its discovery. Visual image quality (imperceptibility) and lack of discovery by steganalysis attacks are two important criteria for any method of steganography. The main purpose of this paper is to provide a LSBM-based approach that is superior to LSBM in these two criteria. In the proposed method, the cover image is blocked and selected the best embedding sequence for each block using the genetic algorithm and the Linear Congruential Generator (LCG). The best sequence contains pixels whose LSB correspond most to data bits. The second step is to use the LSBM in the pixels of this embedding sequence. If the secret bit does not match the pixel's LSB, the pixel value should be incremented or decremented randomly by one unit. To make these random selections, a genetic algorithm has been used, so that the block has the least change in histogram compared to the original block. Comparing the parameter of visual image quality and the accuracy of the attacks in discovering this method, indicates the proper improvement of these criteria compared to the LSBM method.

Keywords- Steganography, Steganalysis, LSBM, Genetic algorithm, Linear Congruential Generator (LCG).

مجله علمی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۹، شماره ۴، زمستان ۱۳۹۹، صفحه ۷۰-۸۲
دریافت: ۱۳۹۸/۰۹/۱۹، بازنگری: ۱۳۹۹/۰۳/۰۵، پذیرش: ۱۳۹۹/۰۹/۰۴

یک روش پنهان‌نگاری تصویر ایمن با کیفیت بینایی تصویر بالا بر مبنای LSBM و الگوریتم ژنتیک

وجیهه ثابتی*[۱]، سیده سپیده فیاضی ۲
*۱- دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران
۲- دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران
[1*]v.sabeti@alzahra.ac.ir, [2] s.fayazi@student.alzahra.ac.ir

* نشانی نویسنده مسئول: وجیهه ثابتی، تهران، خیابان ده ونک، دانشگاه الزهرا، دانشکده فنی و مهندسی، کد پستی: ۱۹۹۳۸۹۳۹۷۳

چکیده- روش تطابق بیت کم ارزش (LSBM)، یکی از روش‌های ساده پنهان‌نگاری است که حملات نسبتاً موفقی برای کشف آن ارائه شده است. کیفیت بینایی تصویر (مشاهده ناپذیری) و عدم کشف توسط حملات پنهان‌شکنی، دو معیار مهم برای هر روش پنهان‌نگاری است. هدف اصلی در این مقاله ارائه روشی بر مبنای LSBM است که نسبت به آن، در این دو معیار برتری داشته باشد. در روش پیشنهادی تصویر پوشش بلوک‌بندی شده و برای هر بلوک با استفاده از الگوریتم ژنتیک و تابع تولید اعداد شبه تصادفی (LCG)، بهترین دنباله جاسازی انتخاب می‌شود. بهترین دنباله شامل پیکسل‌هایی است که بیت کم ارزش آنها با بیت‌های داده بیشترین مطابقت را داشته باشد. در مرحله دوم، با استفاده از LSBM در پیکسل‌های این دنباله جاسازی انجام می‌شود. پیکسل‌هایی که بیت کم ارزش آن‌ها با بیت داده موردنظر مطابقت ندارند، باید یک واحد افزایش یا کاهش یابند. برای انجام این انتخاب، از الگوریتم ژنتیک استفاده شده است، به نحوی که بلوک حاصل کمترین تغییر هیستوگرام را نسبت به بلوک اولیه داشته باشد. مقایسه معیارهای کیفیت تصویر و دقت حملات در کشف این روش، نشان دهنده بهبود مناسب این معیارها در مقایسه با روش LSBM است.

واژه‌های کلیدی: پنهان‌نگاری، پنهان‌شکنی، LSBM، الگوریتم ژنتیک، تابع LCG.

۱- مقدمه

با گسترش فناوری‌های ارتباطات دیجیتال و رشد سریع پهنای باند شبکه، اینترنت تبدیل به یک کانال رایج برای انتقال بسیاری از اسناد مانند، صوت، تصویر، ویدیو و متن دیجیتالی شده است. تا به حال روش‌های متعددی در زمینه سیستم‌های امنیتی و به منظور دست‌یابی به انتقال ایمن داده‌ها، ارائه شده است که این روش‌ها در دو دسته تحت عنوان رمزنگاری اطلاعات و پنهان‌سازی اطلاعات تقسیم‌بندی می‌شوند [۱ و ۲].

در رمزنگاری اطلاعات، پیام محرمانه به یک پیام ناخوانا تبدیل می‌شود. با این وجود، آشکار بودن وجود یک ارتباط رمز شده و محرمانه بین طرفین ارتباط، امری قابل توجه است. بنابراین در برخی موارد نیاز به یک ارتباط نامرئی، که توجه کسی را به خود جلب نکند، احساس می‌شود. در واقع این موضوع دلیلی بر نیاز به وجود مکانیسم پنهان‌سازی اطلاعات می‌باشد. پنهان‌سازی اطلاعات از دو شاخه‌ی پنهان‌نگاری[۱] و ته‌نقش‌نگاری[۲] تشکیل یافته است. هر دو روش پنهان‌نگاری و ته‌نقش‌نگاری برای پنهان‌سازی اطلاعات محرمانه مورد استفاده قرار می‌گیرند و ارتباط نزدیکی با هم دارند. با این وجود دارای اهداف متفاوتی می‌باشند. مهم‌ترین هدف پنهان‌نگاری، پنهان‌سازی وجود ارتباط محرمانه و محافظت از داده محرمانه می‌باشد. در مقابل، هدف از ته‌نقش‌نگاری حفظ یکپارچگی داده‌ی محرمانه بدون پنهان کردن وجود داده محرمانه می‌باشد. هدف اصلی ته‌نقش‌نگاری حفظ مالکیت معنوی محتوا می‌باشد

[۳].

با توجه به محبوبیت استفاده از تصاویر در ارتباطات، پنهان‌نگاری در تصاویر، یکی از حوزه‌های فعال در این زمینه می‌باشد. در پنهان‌نگاری فرستنده در یک ارتباط سرّی با استفاده از پنهان‌نگاری، فرآیند جاسازی داده در تصویر پوشش[۳] را انجام می‌دهد و تصویر پنهان‌نگاری‌شده[۴] را تولید و ارسال می‌کند. در مقابل گیرنده، فرآیند استخراج داده را از تصویر پنهان‌نگاری شده انجام می‌دهد [۴]. اگر C، C′، K و M به ترتیب نشان دهنده تصویر پوشش، تصویر پنهان‌نگاری‌شده، کلید (اختیاری) و داده موردنظر برای ارسال باشد، فرآیند جاسازی (E_m) و فرآیند استخراج (E_x) مطابق فرمول‌های ۱ و ۲ قابل نمایش هستند [۵].

$$E_m: C \oplus K \oplus M \rightarrow C' \quad (۱)$$

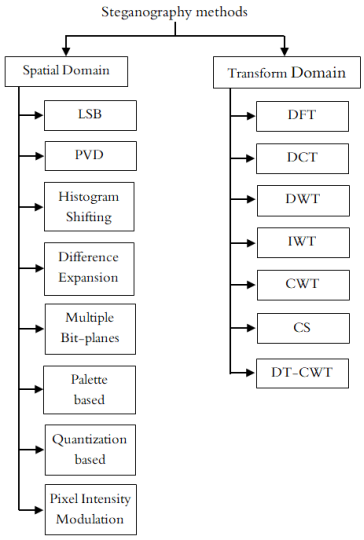
$$E_x(E_m(c.k.m)) \approx m \quad \forall c \in C.k \in K.m \in M \quad (۲)$$

یک روش پنهان‌نگاری خوب سه الزام اصلی دارد که عبارتند از: شفافیت ادراکی، ظرفیت حمل و امنیت. شفافیت ادراکی یعنی رسانه پنهان‌نگاری‌شده و رسانه پوشش نباید از نظر ادراکی تفاوتی محسوسی داشته باشند. معمولا از معیار PSNR برای سنجش شفافیت ادراکی استفاده می‌شود. ظرفیت حمل هر روش نشان دهنده حداکثر تعداد بیت‌هایی است که می‌تواند در رسانه پوشش مخفی کند. مفهوم امنیت، عدم توانایی حملات پنهان‌شکنی موجود در کشف تصاویر پنهان‌نگاری‌شده حاصل از این روش پنهان‌نگاری است [۲]. افزایش ظرفیت حمل، معمولا باعث کاهش دو معیار دیگر می‌شود. طراح روش برای پیشگیری از این اتفاق و ایجاد یک مصالحه میان این معیارها، باید از ایده‌های مختلف استفاده کند.

روش‌های پنهان‌نگاری مختلفی تا به حال ارائه شده است. اگرچه در ظاهر هر کدام از آنها الگوریتم‌های خاص متفاوتی برای جاسازی داده استفاده کرده‌اند، اما بررسی روش‌های پنهان‌نگاری مختلف نشان می‌دهد که برای هر الگوریتم‌های پنهان‌نگاری می‌توان چند پارامتر مهم تعریف کرد. این پارامترها عبارتند از: حوزه جاسازی، بستر جاسازی و روش جاسازی.

دو حوزه متداول برای جاسازی داده در تصاویر وجود دارد: حوزه مکان[۵] و حوزه تبدیل[۶]. معمولاً روش‌های پنهان‌نگاری، داده موردنظر را در یکی از این دو حوزه جاسازی می‌کنند. الگوریتم‌های پنهان‌نگاری در حوزه مکان، پیام را به طور مستقیم در شدت نور پیکسل‌های تصویر جاسازی می‌کنند، اما در الگوریتم‌های حوزه تبدیل، تصاویر ابتدا به حوزه تبدیل موردنظر (مثلاً DCT[۷]، DWT[۸] و...) منتقل می‌شوند و سپس پیام در ضرایب تبدیل جاسازی می‌شوند. یکی از دسته بندی‌های اخیر برای روش‌های پنهان‌نگاری براساس حوزه جاسازی، در شکل ۱ نمایش داده شده است [۳].

پارامتر دوم مشخص می‌کند که الگوریتم پنهان‌نگاری در حوزه موردنظر خود، از چه بستری برای جاسازی داده استفاده می‌کند. برای مثال در حوزه مکان، جاسازی ممکن است مستقیماً در مقدار یک پیکسل انجام شود و یا اینکه یک رابطه میان چند پیکسل تعریف شود و داده موردنظر در مقدار این رابطه جاسازی شود. مقدار تفاوت دو پیکسل همسایه، رایج‌ترین رابطه‌ای است که برای جاسازی داده در روش‌های PVD[۹] و روش‌های برمبنای آن [۶-۸] به عنوان بستر جاسازی استفاده شده است. علاوه بر مقدار تفاوت، روابط دیگری نیز تا به حال در الگوریتم‌های مختلف استفاده شده است. در [۹]، از مجموع دو پیکسل و در [۱۰-۱۲]، از مقدار تفاوت یک پیکسل با متوسط پیکسل‌های همسایه به عنوان بستر جاسازی استفاده شده است.



شکل ۱: دسته بندی روش‌های پنهان‌نگاری براساس حوزه جاسازی [۳]

در هر الگوریتم پنهان‌نگاری، پس از تعیین حوزه و بستر جاسازی باید روش جاسازی داده انتخاب شود. در این گام بستر انتخاب شده، به منظور جاسازی طوری تغییر می‌کند که بعداً و توسط الگوریتم استخراج، بتوان داده جاسازی شده را از آن استخراج نمود. می‌توان روش جاسازی را به سه دسته اصلی شامل جایگزینی بیت‌های کم‌ارزش، تطابق با بیت‌های کم‌ارزش و جاسازی مبتنی بر تابع استخراج تقسیم نمود [۱۳].

در روش اول که LSBF[۱۰] نامیده می‌شود، بیت کم ارزش نمونه‌های بستر با بیت‌های پیام جاگذاری می‌شوند. اما در روش دوم، در صورت تطابق بیت داده با بیت کم ارزش نمونه‌های بستر، تغییری در آن‌ها ایجاد نمی‌شود. در صورت عدم تطابق، نمونه‌های بستر به

صورتی تغییر داده می‌شوند که بیت کم ارزش آن‌ها با بیت‌های پیام تطابق یابند. این کار به روش‌های مختلفی انجام می‌شود. در ساده‌ترین روش به صورت تصادفی نمونه‌های بستر افزایش یا کاهش می‌یابند. از این روش به عنوان LSBM[11] یا جاسازی ± 1 [۱۰] یاد می‌شود. اما روش‌هایی پیشنهاد شده است که این انتخاب را به صورت تصادفی انجام نمی‌دهند، بلکه این انتخاب را به صورت هدفدار و برای رسیدن به یک هدف خاص انجام می‌دهند. بعضی از این اهداف عبارتند از: کمینه کردن تغییرات مقداری پیکسل‌ها (روش OPAP LSB [۱۴])، کمینه کردن تغییرات هیستوگرام (روش A-LSBM [۱۵])، کمینه کردن نویز اضافه شده به تصویر (روش CAS-D و CAS-NE [۱۶]).

روش LSBF به دلیل تشکیل زوج مقادیر در هیستوگرام تصویر پنهان‌نگاری‌شده به راحتی و با حملات مختلف قابل کشف است، اما LSBM این نقطه ضعف را ندارد. اما با پیشرفت علم پنهان‌شکنی حملات نسبتاً موفقی برای کشف LSBM نیز پیشنهاد شده است که به صورت خلاصه ایده تعدادی از آنها در جدول ۱ ارائه شده است. تمام این روش‌ها کارایی یکسانی ندارند و در اکثر موارد کارایی آن‌ها بستگی به نوع تصویر پوشش مورد استفاده دارد [۲۵]. ضعف روش LSBM این است که هیستوگرام تصویر و همبستگی بین پیکسل‌های مجاور را تغییر می‌دهد و این موضوع به روش‌های پنهان‌شکنی برای حمله به این روش، کمک می‌کند [۲۶]. با توجه به امنیت بیشتر روش LSBM نسبت به LSBF، ارائه روش‌های جدید برمبنای LSBM، منطقی‌تر است.

جدول ۱: خلاصه تعدادی از حملات ارائه شده برای LSBM

حمله	خلاصه ایده
[۱۷]	براساس ادعای افزایش تعداد رنگ‌های همسایه در تصاویر پنهان‌نگاری‌شده رنگی
[۱۸]	مدلسازی روش‌های پنهان‌نگاری به عنوان عامل اضافه کردن نویز
[۱۹]	مدلسازی روش LSBM در تصاویر سطح خاکستری و مفهوم مرکز ثقل هیستوگرام
[۲۰]	مدلسازی روش LSBM در تصاویر رنگی و مفهوم مرکز ثقل هیستوگرام
[۲۱]	براساس تأثیر LSBM بر روی کمینه‌ها و بیشینه‌های محلی هیستوگرام
[۲۲]	استخراج ۱۰ پارامتر از هیستوگرام تصویر و هیستوگرام همسایگی دو بعدی
[۲۳]	کشف LSBM در تصاویر غیرفشرده براساس ویژگی‌های مکانی
[۲۴]	حمله عام براساس یک بردار ویژگی شامل ۲۷ خصیصه

هدف روش پیشنهادی در این مقاله، پیشنهاد روشی جدید برای بهبود کیفیت تصویر پنهان‌نگاری شده و امنیت روش LSBM است. برای رسیدن به این هدف در روش پیشنهادی در دو مرحله‌ی انتخاب پیکسل‌ها برای جاسازی و تعیین مقدار پیکسل‌ها بعد از جاسازی داده از الگوریتم ژنتیک استفاده شده است. در مرحله اول با کمک الگوریتم ژنتیک، دنباله‌ای از پیکسل‌ها برای جاسازی انتخاب می‌شوند که بیت کم‌ارزش آن‌ها بیشترین تطابق را با بیت‌های داده موردنظر دارند. بدین ترتیب کمترین پیکسل‌ها نیاز به تغییر دارند و درنتیجه کیفیت تصویر پنهان‌نگاری‌شده افزایش می‌یابد. در مرحله دوم برای جاسازی داده از LSBM استفاده شده است و برای تصمیم‌گیری در مورد افزایش یا کاهش مقدار پیکسل‌هایی که نیاز به تغییر دارند از الگوریتم ژنتیک استفاده شده است. هدف اصلی در این مرحله انتخاب به نحوی است که تغییرات هیستوگرام تصویر پنهان‌نگاری شده‌ی نهایی نسبت به تصویر پوشش حداقل باشد. می‌توان امیدوار بود با کم کردن تغییرات هیستوگرام، احتمال موفقیت حملات آماری کمتر شود و روش پیشنهادی امنیت بیشتری نسبت به LSBM در برابر حملات داشته باشد.

در ادامه، در بخش دوم به مروری بر تعدادی از روش‌های پنهان‌نگاری که از الگوریتم‌های بهینه‌سازی استفاده کرده‌اند، پرداخته می‌شود. سپس در بخش سوم، الگوریتم پیشنهادی به‌صورت مفصل شرح داده شده است. در بخش چهارم، نتایج آزمون و مقایسه روش‌های پیشنهادی ارائه شده است و در انتها نتیجه‌گیری بیان می‌شود.

۲- مروری بر کارهای گذشته

با توجه به سه هدف افزایش ظرفیت جاسازی، افزایش کیفیت تصویر پنهان‌نگاری‌شده و افزایش امنیت در طراحی روش‌های پنهان‌نگاری، بعضی از روش‌ها انتخاب‌های خود را به‌عنوان یک مسئله جستجو در فضای بزرگی از راه‌حل‌ها برای برآورده کردن یک یا چند تا این اهداف مدل‌سازی کرده و برای حل آن از روش‌های بهینه‌سازی استفاده می‌کنند. استفاده از الگوریتم‌های بهینه‌سازی در روش‌های پنهان‌نگاری معمولاً پیش از مرحله جاسازی، در حین جاسازی و یا پس از جاسازی انجام می‌شود. در دسته پیش از مرحله جاسازی، معمولاً از الگوریتم بهینه‌سازی برای پیدا کردن بهترین مکان برای انجام جاسازی یا تغییر بیت‌های پیام استفاده می‌شود. در دسته دوم، الگوریتم بهینه‌سازی برای تعیین چگونگی ذخیره‌سازی داده و تعیین مقدار پیکسل پنهان‌نگاری‌شده استفاده می‌شود و در دسته سوم، الگوریتم بهینه‌سازی ضمن حفظ

داده جاسازی شده به کاهش تغییرات حاصل از جاسازی کمک می‌کند. در ادامه تعدادی از این روش‌ها به‌صورت مختصر معرفی می‌شوند.

یک روش پنهان‌نگاری توسط Tseng و همکارانش [۲۷] بر اساس OPAP و الگوریتم ژنتیک ارائه شده که با استفاده از تغییر ترتیب داده محرمانه سعی کرده است که شباهت تصویر پوشش و تصویر پنهان‌نگاری‌شده را افزایش دهد. خدایی و همکاران [۲۸] نیز در کنار LSBF، از الگوریتم ژنتیک برای تنظیم پارامترهای تابع هدف به‌منظور به دست آوردن بهترین شرایط در توزیع پیکسل‌ها استفاده کرده‌اند و توانسته‌اند کیفیت بصری تصویر پنهان‌نگاری‌شده را بهبود بخشند.

روش ارائه شده در [۲۹] از ترکیب پنهان‌نگاری و الگوریتم ژنتیک برای کاهش تغییرات پس از جاسازی استفاده می‌کند. به این صورت که ابتدا اطلاعات محرمانه در ۴ بیت کم ارزش پیکسل‌های تصویر جاسازی می‌شود. بعد از جاسازی کامل پیام، تصویر حاصل به بلوک‌های ۸×۸ تقسیم شده و بر روی هر بلوک الگوریتم ژنتیک اعمال می‌شود. تاثیر الگوریتم ژنتیک بر ۴ بیت با ارزش در هر پیکسل است تا با عدم از دست رفتن اطلاعات محرمانه جاسازی شده، کمترین تخریب در تصویر حاصل، ایجاد شود. نتایج بدست آمده نشان می‌دهد این روش توانسته PSNR[12] بهتری نسبت به روش‌های مقایسه شده داشته باشد.

در [۳۰] یک روش پنهان‌نگاری بر پایه الگوریتم مورچگان ارائه شده است. در روش ارائه شده از الگوریتم مورچگان برای تشخیص لبه استفاده می‌شود و سپس با استفاده از روش LSBF اطلاعات محرمانه در نواحی پیچیده (لبه) جاسازی می‌شوند. تشخیص نواحی پیچیده با استفاده از ماتریس فرمون انجام می‌شود که هر عنصر از این ماتریس متناظر با یک پیکسل از تصویر است. ماتریس فرمون با توجه به حرکت مورچه‌ها، که این حرکت با استفاده از تفاوت‌های محلی بین پیکسل‌ها و با توجه به شدت نور پیکسل‌های تصویر تعیین می‌شود، توسعه می‌یابد. برای مخفی کردن اطلاعات محرمانه، LSB پیکسل‌های منطقه پیچیده با بیت پیام جایگزین می‌شوند. یکی از امکانات روش ارائه شده تغییر ظرفیت جاسازی با توجه به پارامترهای انتخابی است.

Shah و همکاران در [۳۱]، یک روش پنهان‌نگاری با استفاده از الگوریتم ژنتیک ارائه داده‌اند. در این روش از ژنتیک برای پنهان‌سازی ماتریس ضرایب و نه پیام محرمانه، استفاده می‌شود. این روش به‌جای استفاده از روش LSB معمولی برای جایگذاری در تصویر از روش نگاشت داده استفاده می‌کند. بدین‌صورت که باید دو بیت از پیام در دو بیت از پیکسل تصویر پوشش ذخیره شود، اما بیت‌ها به‌جای قرارگیری در LSB های پیکسل در بهترین دو بیت از آن قرار می‌گیرند. نتایج حاصله در مقایسه با جایگذاری LSB معمولی که ۲ بیت را در تصویر جایگذاری می‌کند، نشان می‌دهد که این روش PSNR بهتری دارد و نسبت به حملات آنالیز هیستوگرام مقاوم‌تر است.

در [۳۲] روشی بر پایه ترکیب پنهان‌نگاری در حوزه مکان و الگوریتم ژنتیک ارائه شده است. از الگوریتم ژنتیک به منظور پیدا کردن بهترین مکان جاسازی استفاده شده است. هر کروموزوم در الگوریتم ژنتیک از ۵ ژن و در مجموع از ۱۹ بیت تشکیل شده، که هر ژن با توجه به مقداری که به آن تعلق می‌گیرد، تغییراتی در تصویر پوشش و یا پیام محرمانه ایجاد می‌کند. در این روش از روش LSBF برای پنهان‌نگاری استفاده شده است. مقایسه روش ارائه شده نسبت به روش پایه و سایر روش‌هایی که برای پنهان‌نگاری از الگوریتم ژنتیک بهره برده‌اند نشان از برتری این روش از لحاظ PSNR و ظرفیت جاسازی دارد.

Shah و همکاران [۳۳]، یک روش پنهان‌نگاری تصویر در حوزه‌ی دامنه مکانی، مبتنی بر الگوریتم ژنتیک، با ظرفیت جاسازی بالا و کیفیت بصری مناسب پیشنهاد داده‌اند. در این روش دو بیت از داده‌ی محرمانه در هر پیکسل از تصویر پوشش جاسازی می‌شود. جاسازی داده در تصویر پوشش به‌صورت ترتیبی انجام نمی‌گیرد. برای تولید مسیر شبه تصادفی، تابع LCG[13] مورد استفاده قرار گرفته شده است. از الگوریتم ژنتیک برای اصلاح پارامترهای LCG استفاده می‌شود. داده‌های محرمانه قبل از جاسازی در تصویر پوشش با استفاده از جهت و قطبیت اصلاح می‌شوند و سرانجام بعد از جاسازی کل پیام در تصویر، OPAP برای بهبود هر چه بیشتر کیفیت تصویر پنهان‌نگاری‌شده اعمال می‌شود.

ثابتی و همکاران در [۳۴] روش‌هایی پیشنهاد کرده‌اند که ایده اصلی آن‌ها ترکیب روش LSBM و الگوریتم ژنتیک است و تمام آن‌ها یک چهارچوب یکسان دارند. اولین روش پیشنهادی GLSBM نامیده شده است. روش GLSBM، همان روش LSBM است با این تفاوت که برای تصمیم‌گیری در مورد افزایش یا کاهش مقدار پیکسل‌هایی که LSB آن‌ها با بیت پیام مطابقت ندارد، از الگوریتم ژنتیک استفاده می‌شود. هدف الگوریتم ژنتیک در این روش تولید تصویر پنهان‌نگاری‌شده‌ای است که هیستوگرام آن با هیستوگرام تصویر پوشش کمترین تفاوت را داشته باشد. برای بهبود این روش، ایده‌ی تکرار اجرای الگوریتم GLSBM با کلیدهای متفاوت و یافتن بهترین کلید پیشنهاد شده است. با تغییر کلید، ترتیب انتخاب پیکسل‌ها برای جاسازی تغییر می‌کند.

روش نهایی، روش MKGM (روش GLSBM چندکلیدی مبتنی بر بلوک‌بندی) است که مهم‌ترین تفاوت آن با روش قبلی بلوک‌بندی تصویر پوشش و اجرای روش قبلی روی هر بلوک تصویر پوشش و تولید بلوک‌های متناظر در تصویر پنهان‌نگاری‌شده به‌صورت مجزا در هر اجرا است. نتایج آزمون نشان‌دهنده احتمال کشف کمتر روش نهایی نسبت به روش‌های قبلی و روش LSBM اصلی است، اما از لحاظ معیار PSNR تقریباً مشابه یکدیگر هستند و بهبود چشمگیری اتفاق نیفتاده است.

جدول ۲: مقایسه روش های موجود

مرجع	نام روش	روش جاسازی	الگوریتم بهینه سازی	نقطه قوت	نقطه ضعف
[۲۹]	GA2017	4 LSBF	ژنتیک	افزایش ظرفیت	عدم توجه به امنیت
[۳۰]	ACO2018	LSBF	کلونی مورچگان	جاسازی در لبه	کاهش ظرفیت
[۳۱]	LCG	جایگزینی ۲ بیت	ژنتیک	• بهبود نسبی کیفیت تصویر • بررسی حملات آنالیز هیستوگرام	کاهش ظرفیت
[۳۲]	GA2019	LSBF	ژنتیک	افزایش ظرفیت	عدم توجه به امنیت
[۳۳]	LCG_GA	2 LSBF	ژنتیک	افزایش ظرفیت	عدم توجه به امنیت
[۳۴]	GLSBM	LSBM	ژنتیک	افزایش امنیت	عدم توجه کیفیت تصویر
[۳۴]	MKGM	LSBM	ژنتیک	افزایش امنیت	عدم موفقیت در بهبود چشمگیر کیفیت تصویر

در جدول ۲، خلاصه‌ی تعدادی از مقالاتی لیست شده‌اند که سعی کرده‌اند با استفاده از الگوریتم‌های بهینه‌سازی عملکرد روش‌های مبتنی بر جاسازی در بیت‌های کم ارزش را بهبود دهند. با توجه به تناقض موجود میان ظرفیت و امنیت یک روش پنهان‌نگاری، معمولا روش‌هایی که با هدف افزایش ظرفیت جاسازی ارائه شده‌اند، مانند [۲۹]، [۳۲] و [۳۳]، در بهبود چشمگیر کیفیت تصویر نهایی موفق نبودند و به معیار امنیت نیز توجهی نکرده‌اند. از طرف دیگر روش‌هایی مانند [۳۰] و [۳۱] با کاهش ظرفیت جاسازی (کمتر از یک بیت در هر پیکسل)، توانسته‌اند در هدف افزایش کیفیت تصویر نهایی تاحدی موفق باشند. ولی یک نکته مشترک تمام ۵ روش ابتدایی استفاده از روش LSBF برای جاسازی است. با توجه به توضیح ارائه شده در بخش قبل، استفاده از LSBM برای جاسازی می‌تواند امنیت بیشتری را بدنبال داشته باشد. روش‌های ارائه شده در [۳۴] این برتری را نسبت به روش‌های قبلی دارد، اما این روش‌ها فقط در بهبود امنیت موفق بوده‌اند و روش MKGM هم با وجود درنظر گرفتن ایده چند کلیدی نتوانسته بهبود چشمگیری در کیفیت تصویر پنهان‌نگاری‌شده ایجاد کند. بنابراین ارائه یک روش پنهان‌نگاری مبتنی بر LSBM که با ظرفیت جاسازی مناسب، بتواند کیفیت و امنیت بهتری فراهم کند، می‌تواند هدف مناسبی برای طرح یک روش پنهان‌نگاری جدید باشد.

براساس اطلاعات بدست آمده از مقالات مختلف، الگوریتم ژنتیک رایج‌ترین الگوریتم بهینه‌سازی در میان الگوریتم‌های پنهان‌نگاری است و بر همین اساس در الگوریتم پیشنهادی در این مقاله نیز از این الگوریتم استفاده شده است. اما برخلاف اکثر روش‌های موجود که از PSNR به عنوان تابع برازندگی و LSBF به عنوان روش پایه برای جاسازی داده استفاده کرده‌اند، در روش پیشنهادی در این مقاله از دو تابع برازندگی متفاوت و LSBM به عنوان روش پایه استفاده شده است.

۳- روش پیشنهادی

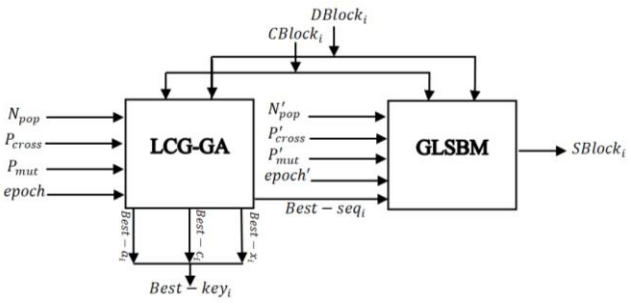
همان‌گونه که در بخش قبل اشاره شد، روش MKGM [۳۴] در افزایش امنیت روش LSBM موفق بوده است. ولی کیفیت تصویر پنهان‌نگاری شده در این دو روش تقریبا مشابه یکدیگر است. در این بخش روشی پیشنهاد می‌شود که سعی می‌کند علاوه بر حفظ امنیت روش MKGM، کیفیت تصویر پنهان‌نگاری‌شده‌ی بهتری نسبت به آن داشته باشد. در این صورت روش پیشنهادی نسبت به LSBM، کیفیت و امنیت بهتری خواهد داشت.

نمودار بلوکی روش پیشنهادی در شکل ۲ نشان داده شده است. طبق شکل ۲، الگوریتم روش پیشنهادی شامل دو مرحله اصلی است که این مراحل برای هر بلوک تصویر پوشش تکرار می‌شود و در خروجی یک بلوک تصویر پنهان‌نگاری‌شده تولید می‌شود. این مراحل عبارتند از:

۱. استفاده از ترکیب الگوریتم ژنتیک و LCG برای یافتن بهترین دنباله پیکسل‌ها برای جاسازی (LCG-GA)

۲. استفاده از ترکیب الگوریتم ژنتیک و LSBM برای یافتن بهترین مقدار پیکسل‌ها بعد از جاسازی (GLSBM)

علاوه بر بلوک تصویر پوشش و بلوک داده محرمانه، پارامترهای الگوریتم ژنتیک به عنوان ورودی در هر مرحله لازم است. خروجی مرحله اول، مجموعه کلیدها برای تولید بهترین ترتیب جاسازی و خروجی مرحله دوم، بلوک تصویر پنهان‌نگاری‌شده است. شبه کد این روش در شکل ۳ نمایش داده شده است. جدول ۳، شامل تمام اصطلاحات و پارامترهایی است که در ادامه برای بیان جزئی‌تر مراحل الگوریتم پیشنهادی از آن استفاده می‌شود.



شکل ۲: نمودار بلوکی روش پیشنهادی

ورودی: تصویر پوشش، داده محرمانه، اندازه بلوک

خروجی: تصویر پنهان‌نگاری شده، مجموعه بهترین کلیدها

۱. تصویر پوشش را با توجه به اندازه بلوک، بلوک‌بندی کنید.

۲. داده محرمانه را با توجه به تعداد بیت قابل جاسازی در هر بلاک، تقسیم‌بندی کنید.

۳. برای هر بلوک از تصویر پوشش مراحل زیر را تکرار کنید:

۳-۱. برای جاسازی بلوک داده محرمانه در بلوک تصویر پوشش، با استفاده از الگوریتم LCG-GA، بهترین دنباله پیکسل‌ها را انتخاب کنید.

۳-۲. براساس بهترین دنباله جاسازی حاصل از مرحله قبل و با استفاده از الگوریتم GLSBM، عملیات جاسازی بلوک داده در بلوک تصویر پوشش را انجام دهید.

شکل ۳: شبه کد روش پیشنهادی

جدول ۳: اختصارات استفاده شده در شرح الگوریتم

علامت اختصاری	تعریف پارامتر
$Cover$	تصویر پوشش
$Stego$	تصویر پنهان‌نگاری شده
$Data$	داده محرمانه
$CBlock_i$	بلوک i ام تصویر پوشش
$DBlock_i$	بلوک i ام داده
$SBlock_i$	بلوک i ام تصویر پنهان‌نگاری شده
$DBlock - size$	اندازه بلوک داده
N_{pop}	تعداد جمعیت ژنتیک مرحله اول
$Block - size$	اندازه هر بلوک
P_{cross}	احتمال تقاطع مرحله اول
P_{mut}	احتمال جهش مرحله اول
$epoch$	تعداد تکرار مرحله اول
$Best - Seq_i$	بهترین دنباله خروجی بلوک i ام
$Best - a_i$	بهترین مقدار a برای بلوک i ام
$Best - c_i$	بهترین مقدار c برای بلوک i ام
$Best - x_i$	بهترین مقدار x_0 برای بلوک i ام
$Best - key_i$	مجموعه بهترین a، c و x_0 برای بلوک i ام
N'_{pop}	تعداد جمعیت ژنتیک مرحله دوم
P'_{cross}	احتمال تقاطع مرحله دوم
P'_{mut}	احتمال جهش مرحله دوم
$epoch'$	تعداد تکرار مرحله دوم

۳-۱- گام اول جاسازی: LCG-GA

اولین گام هر روش پنهان‌نگاری، انتخاب پیکسل مناسب برای جاسازی است. علاوه بر تعیین پیکسل‌های مناسب باید ترتیب جاسازی در آن‌ها نیز مشخص شود. برای جاسازی کامل (۱۰۰٪)، باید در تمام پیکسل‌ها جاسازی انجام شود، اما باز هم ترتیب جاسازی می‌تواند تغییر کند. برای جاسازی کمتر از ۱۰۰٪، بنا بر طول داده موردنظر، باید پیکسل‌های مناسب و ترتیب جاسازی در آن تعیین شود. اما در تمام روش‌های پنهان‌نگاری، باید این مراحل به نحوی انجام شود که گیرنده نیز بتواند دقیقاً همان پیکسل‌ها و ترتیب جاسازی استفاده شده توسط فرستنده را شناسایی کند تا بتواند داده را به صورت کامل استخراج کند. به همین دلیل یکی از روش‌ها استفاده از توابع تولید اعداد شبه تصادفی است.

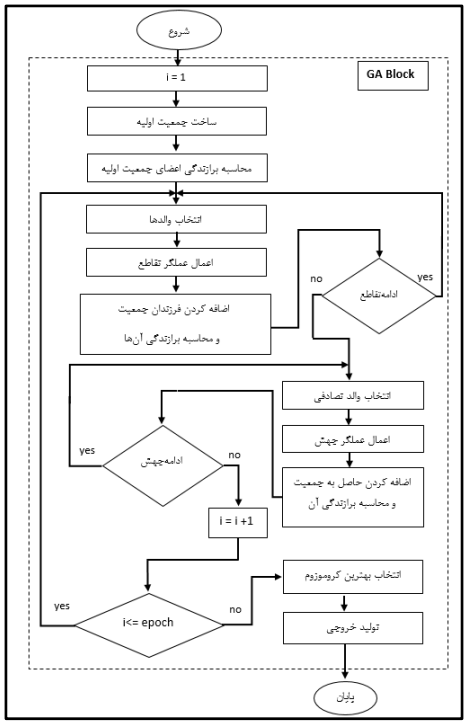
روش MKGM [۳۴]، برای این انتخاب از تابع ()rand، تابع تولید اعداد شبه تصادفی در Matlab، استفاده می‌کند، که نیاز به یک هسته ابتدایی دارد. اما در روش پیشنهادی برای انجام این کار از الگوریتم ژنتیک و LCG استفاده می‌شود. تابع LCG، یکی دیگر از توابع تولید اعداد شبه تصادفی است. این تابع برای تولید یک دنباله اعداد به مقدار هسته ابتدایی (x_0)، فاکتور افزایشی (a) و یک آفست (c) نیاز دارد و طبق رابطه بازگشتی ۳ تعریف می‌شود.

$$x_{n+1} = (a \times x_n + c) mod\ m \qquad (۳)$$

که در این فرمول x_n عدد n ام در دنباله خروجی، x_{n+1} عدد $n+1$ ام در این دنباله است. m محدوده‌ی اعدادی که تولید می‌شوند، را مشخص می‌کند.

با تغییر پارامترهایx_0، a و c دنباله اعداد خروجی LCG متفاوت است. به‌عبارت‌دیگر، پیکسل‌های انتخاب شده برای جاسازی در هر حالت متفاوت است. از طرف دیگر، در روش LSBM با توجه به مقدار پیکسل و مقدار بیت داده موردنظر، یکی از دو حالت عدم تغییر مقدار پیکسل یا تغییر یک واحدی پیکسل انجام می‌شود. بنابراین در هر دنباله از پیکسل‌های انتخابی، تعداد پیکسل‌هایی که باید تغییر کند متفاوت است. اگرچه با تغییر مقدارx_0، a و c دنباله‌های متفاوتی برای جاسازی تولید می‌شود، اما باید بتوان از میان دنباله‌های موجود، بهترین دنباله را برای جاسازی انتخاب کرد. یک دیدگاه برای انجام این انتخاب می‌تواند این‌گونه باشد که دنباله‌ای درنهایت برای جاسازی استفاده شود که کمترین تعداد پیکسل در آن نیاز به تغییر داشته باشد. با ایجاد کمترین تغییر در تصویر پوشش برای تولید تصویر پنهان‌نگاری‌شده، می‌توان امیدوار بود که تصویر پنهان‌نگاری‌شده کیفیت بهتری داشته باشد.

پیدا کردن بهترین مقدار برایx_0، a و c به نحوی که دنباله حاصل از آن شامل پیکسل‌هایی باشد که نیاز به کمترین تعداد تغییرات در آن وجود داشته باشد را می‌توان به‌صورت یک مسئله بهینه-سازی مدل کرد. برای حل این مسئله می‌توان از الگوریتم ژنتیک استفاده نمود. فلوچارت الگوریتم ژنتیک در شکل ۴ نمایش داده شده است. نحوه انجام این مراحل به مسئله‌ای بستگی دارد که قرار است توسط این الگوریتم پیاده‌سازی شود.



شکل ۴: فلوچارت اجرای الگوریتم ژنتیک

اولین گام تعریف ساختار یک کروموزوم به عنوان یک عضو از جمعیت و به عبارتی یک راه‌حل برای مسئله موردنظر است. در الگوریتم LCG-GA، ساختار کروموزوم j ام و تفسیر آن طبق فرمول ۴ و ۵ انجام می‌شود.

$$Chr_j = [g_1, g_2, \dots, g_{24}] \quad (۴)$$
$$g_k \in \{0,1\}, k \in [1,24], j \in [1, N_{pop}]$$

$$a_j = [g_1, \dots, g_8] \,.\, c_j = [g_9, \dots, g_{16}] \quad (۵)$$
$$x_{0_j} = [g_{17}, \dots, g_{24}]$$

بدین ترتیب هر کروموزوم شامل ۲۴ ژن است که این ژن‌ها مقدار صفر یا یک دارند. ۸ ژن ابتدایی بیانگر مقدار a و هشت ژن دوم بیانگر مقدار c و ۸ ژن سوم بیانگر مقدار x_0 است. با استفاده از این مقادیر می‌توان یک تابع LCG داشت که دنباله‌ی اعداد را تولید می‌کند. مطابق فرمول ۶ دنباله تولیدی کروموزوم j ام،Seq_j نامیده می‌شود.

$$Seq_j = LCG(a_j, c_j, x_{0_j}) \quad (۶)$$

گام دوم، تعیین تابع برازندگی یا تابع هدف مناسب است. از آن‌جا که هدف از انجام این مرحله، پیدا کردن دنباله جاسازی است که بیشترین تطابق بین پیکسل‌های دنباله و بیت متناظر پیام وجود داشته باشد، مقدار برازندگی تعریف شده برای هر کروموزوم عبارت است از تعداد پیکسل‌هایی از دنباله‌ی حاصل از اجرای تابع LCG متناظر کروموزوم موردنظر که بیت کم‌ارزش آن‌ها با داده‌ی مورد نظر برای جاسازی مطابقت ندارد. فرمول ۷ تابع برازندگی به‌کاربرده شده در روش پیشنهادی را بیان می‌کند. در شبه کد شکل ۵، نحوه‌ی محاسبه مقدار تابع هدف برای هر کروموزوم نمایش داده شده است.

$$Fitness(Chr_j) = Match - No(Chr_j, CBlock_i, DBlock_i) \quad (۷)$$

ورودی: بلوک تصویر پوشش، بلوک داده محرمانه، یک کروموزوم
خروجی: مقدار برازندگی

۱. مقدار اولیه برازندگی را صفر درنظر بگیرید.
۲. تابع LCG را با استفاده از عناصر کروموزوم موردنظر به عنوان پارامترهای تابع اجرا کنید و دنباله جاسازی را تولید کنید.
۳. به تعداد عناصر بلوک داده محرمانه این عملیات را تکرار کنید:
- اگر باقیمانده تقسیم پیکسل متناظر در دنباله برای جاسازی بیت داده موردنظر به ۲ با بیت داده موردنظر مساوی نیست، یک واحد مقدار برازندگی را افزایش دهید.

شکل ۵: شبه کد تابع Match-No در فرمول ۵

گام سوم الگوریتم ژنتیک، انجام عملیات تقاطع روی درصدی از جمعیت فعلی است. اگرP_{cross}، احتمال عملیات تقاطع و N_{pop}، تعداد اعضای جمعیت باشد، باید به تعداد $(P_{cross} \times N_{pop}) / 2$ بار عملیات تقاطع روی جمعیت انجام شود. در هر بار، دو کروموزوم والد که دارای کمترین مقدار تابع برازندگی در میان جمعیت فعلی هستند انتخاب شده و با استفاده از تقاطع تک نقطه‌ای دو کروموزوم جدید (فرزندان) ساخته می‌شوند. سپس در صورتی که دو فرزند تولید شده دارای برازندگی بهتری نسبت به دو کروموزوم با بیشترین مقدار تابع برازندگی در جمعیت باشند، به‌جای آن‌ها به جمعیت اضافه می‌شوند.

در گام بعد، باید روی درصدی از جمعیت عملیات جهش انجام شود کهP_{mut}، احتمال این عملیات را مشخص می‌کند. بنابراین تعداد عملیات جهش $P_{mut} \times N_{pop}$ بار است. برای اعمال عملگر جهش، ابتدا یک کروموزوم به‌صورت تصادفی از بین جمعیت انتخاب می‌شود و به‌صورت تصادفی مقدار یکی از ژن‌های آن معکوس می‌شود.

با انجام کامل مراحل تقاطع و جهش روی جمعیت فعلی، جمعیت جدید ساخته می‌شود. پارامتر *epoch*، تعداد تکرار الگوریتم را نشان می‌دهد. با پایان یافتن تکرارهای الگوریتم ژنتیک، الگوریتم LCG-GA برای یک بلوک کامل می‌شود. با پایان یافتن این مرحله، بهترین مسیر در بلوک موردنظر از تصویر پوشش به‌عنوان خروجی گام اول روش پیشنهادی آماده شده است ($Best - Seq_i$) و برای مرحله دوم الگوریتم ارسال می‌شود.

۳-۲- گام دوم جاسازی: GLSBM

در مرحله قبل، دنباله‌ای از پیکسل‌ها در تصویر پیدا شد که کم‌ارزش‌ترین بیت آن‌ها بیشترین تطابق را با دنباله داده موردنظر برای جاسازی دارد. در این مرحله، هدف جایگذاری پیام در دنباله به‌دست آمده از مرحله قبل، به‌گونه‌ای است که تصویر پنهان‌نگاری شده حاصل بیشترین امنیت را در برابر حملات موجود داشته باشد. معیار انتخاب در این گام، ایجاد کمترین تغییر در تصویر جهت جاسازی داده است. روش مبنا LSBM است و در این روش برای جاسازی در پیکسل، در صورت نیاز به تغییر، دو گزینه افزایش یا کاهش یک واحدی وجود دارد.

انتخاب هرکدام از این دو گزینه می‌تواند روی تصویر پنهان‌نگاری شده نهایی تأثیر بگذارد. در روش GLSBM، قرار است به کمک الگوریتم ژنتیک در مرحله جاسازی این انتخاب به‌گونه‌ای انجام شود که درنهایت به هدف موردنظر دست پیدا کنیم. برای توضیح این روش، باید مجدداً تمام مراحل الگوریتم ژنتیک، مطابق شکل ۳ و بنابر مسئله موردنظر، تعریف شوند. در روش GLSBM، هر کروموزوم طبق فرمول ۸ تعریف می‌شود:

$$Chr_j' = [g_1', g_2', \dots, g_L'\ ] \quad (۸)$$
$$g_k' = \{-1, 1\}, k \in [1, L], j \in [1, N_{pop}']$$

برای تولید یک کروموزوم ابتدایی، باید بیت کم‌ارزش پیکسل‌های دنباله $Best - Seq_i$ (خروجی مرحله اول) با بیت‌های داده به ترتیب مقایسه شوند. در صورت تطابق، مقداری در کروموزوم قرار نمی‌گیرد. به‌عبارت‌دیگر، در صورت عدم نیاز به تغییر مقدار پیکسل، نیازی به در نظر گرفتن ژنی در کروموزوم نیست. در صورت عدم تطابق به‌صورت تصادفی مقدار ۱+ یا ۱- در مقدار ژن مربوطه قرار می‌گیرد که بیانگر یکی از دو انتخاب افزایش یا کاهش تک واحدی مقدار پیکسل مربوطه است. بنابراین طول کروموزوم در روش GLSBM، به تعداد پیکسل‌هایی از دنباله $Best - Seq_i$ است که نیاز به تغییر دارد، بستگی دارد.

با مطالعه حملات خاص و مختلف ارائه شده برای کیفیت LSBM، این نکته قابل‌تأمل است که، همیشه یکی از موفق‌ترین ویژگی‌های استفاده شده برای شکست این روش، ویژگی‌های استخراج شده از هیستوگرام تصویر حاصل است. با کم کردن تغییرات هیستوگرام تصویر پنهان‌نگاری‌شده نسبت به تصویر پوشش، می‌توان احتمال موفقیت این حملات را کاهش داد. برای تعیین مقدار برازندگی هر کروموزوم در این مرحله، باید مقدار اختلاف هیستوگرام بلوک تصویر پوشش با بلوک هیستوگرام تصویر پنهان‌نگاری‌شده محاسبه شود. بنابراین ابتدا با استفاده از تابع تعریف شده در فرمول ۹، بلوک تصویر پنهان‌نگاری‌شده‌ی حاصل هر کروموزوم تولید می‌شود. شبه کد این تابع در شکل ۶ نمایش داده شده است.

$$SBlock_i = MakeStego(CBlock_i, Chr_j', DBlock_i, Best - Seq_i) \quad (۹)$$

ورودی: بلوک تصویر پوشش، بلوک داده محرمانه، یک کروموزوم، بهترین دنباله ترتیب جاسازی
خروجی: بلوک تصویر پنهان‌نگاری شده
۱. تمام پیکسل‌های بلوک تصویر پوشش را در بلوک تصویر پنهان‌نگاری‌شده کپی کنید.
۲. به تعداد عناصر بلوک داده محرمانه این عملیات را تکرار کنید:
- اگر باقیمانده تقسیم پیکسل متناظر در بهترین دنباله ترتیب جاسازی به ۲ با بیت داده موردنظر مساوی نیست، مقدار ژن متناظر در کروموزوم را به پیکسل موردنظر اضافه کنید.

شکل ۶: شبه کد تابع MakeStego در فرمول ۹

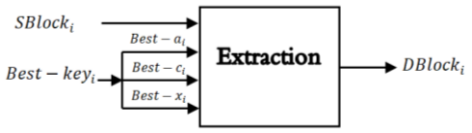
فرض کنید H_c، هیستوگرام بلوک تصویر پوشش و H_s، هیستوگرام بلوک تصویر پنهان‌نگاری‌شده‌ی حاصل از کروموزوم Chr_j' باشد. اگر h_i وh_i'، به ترتیب فراوانی سطح i در بلوک تصویر پوشش و تصویر پنهان‌نگاری‌شده باشد، مقدار برازندگی کروموزوم Chr_j' طبق فرمول ۱۰ محاسبه می‌شود.

$$Fitness(Chr_j') = Dif(H_c, H_s) = \sum_{i=0}^{255} |h_i - h_i'| \quad 0 \le i \le 255 \quad (۱۰)$$

نحوه انجام مراحل تقاطع و جهش در GLSBM، مشابه این مراحل در LCG-GA است. به همین دلیل برای کوتاه‌تر شدن بحث، از بیان مجدد آن‌ها خودداری می‌شود. در این الگوریتم، فرایند الگوریتم ژنتیک به‌اندازه پارامتر $epoch'$ تکرار می‌شود، تا الگوریتم GLSBM برای یک بلوک کامل شود. با پایان یافتن این مرحله، بلوک پنهان‌نگاری شده‌ی حاصل از بهترین کروموزوم در جمعیت نهایی به عنوان بلوک پنهان‌نگاری‌شده‌ی نهایی در تصویر پنهان‌نگاری‌شده قرار می‌گیرد.

۳-۳- الگوریتم استخراج

هر الگوریتم جاسازی، به یک الگوریتم استخراج نیاز دارد که گیرنده برای استخراج پیام این الگوریتم را اجرا می‌کند. نمودار بلوکی این الگوریتم در شکل ۷ نمایش داده شده است. عملیات استخراج روی هر بلوک تصویر پنهان‌نگاری‌شده تکرار می‌شود. گیرنده با استفاده از بلوک تصویر پنهان‌نگاری‌شده و اطلاع از کلیدهای استفاده شده در مرحله جاسازی، می‌تواند داده جاسازی شده را به صورت کامل استخراج کند. شبه کد الگوریتم استخراج در شکل ۸ نشان داده شده است. مراحل الگوریتم استخراج به صورت جزئی‌تر در ادامه شرح داده می شود.



شکل ۷: نمودار بلوکی الگوریتم استخراج

ورودی: تصویر پنهان‌نگاری شده، مجموعه بهترین کلیدها، اندازه بلوک
خروجی: داده محرمانه

۱. تصویر پنهان‌نگاری‌شده را با توجه به اندازه بلوک، بلوک‌بندی کنید.
۲. برای هر بلوک از تصویر پوشش مراحل زیر را تکرار کنید:
۲-۱. تابع LCG را با استفاده از کلیدهای جاسازی در این بلوک، اجرا کنید و بهترین دنباله جاسازی را تولید کنید.
۲-۲. به تعداد عناصر بلوک داده محرمانه این عملیات را تکرار کنید:
- باقیمانده تقسیم پیکسل متناظر در بهترین دنباله ترتیب جاسازی به ۲ را به عنوان بیت داده به دنباله داده محرمانه اضافه کنید.

شکل ۸: شبه کد الگوریتم استخراج

در هنگام استخراج، گیرنده باید مشابه فرستنده و با اطلاع از پارامتر Block-size، عملیات بلوک‌بندی کردن تصویر پنهان‌نگاری‌شده دریافتی را انجام دهد. سپس باید تلاش کند تا داده جاسازی شده در هر بلوک از تصویر پنهان‌نگاری‌شده را استخراج نماید. برای انجام این کار روی بلوک $SBlock_i$، لازم است گیرنده از $Best - Key_i$ که شامل بهترین مقادیر پارامترهای a، c و x_0 است، اطلاع داشته باشد. این مقادیر در واقع خروجی الگوریتم LCG-GA در اولین مرحله جاسازی است که فرستنده از آن برای شناسایی بهترین دنباله از پیکسل‌ها، استفاده کرد. گیرنده با استفاده از فرمول ۱۱، می‌تواند همان دنباله را مجدداً تولید کند.

$$Best - Seq_i \leftarrow LCG(best - a_i, best - c, best - x_i) \quad (۱۱)$$

پس گیرنده می‌تواند از کنار هم گذاشتن بیت‌های کم‌ارزش پیکسل‌های موجود در دنباله، داده جاسازی شده در این بلوک را شناسایی کند. فرمول ۱۲، نحوه انجام این کار را نشان می‌دهد.

$$mod(SBlock_i(Best - Seq_i), 2)DBlock_i(j) = \quad (۱۲)$$
$$\leq j \leq DBlock - size$$

۴- نتایج پیاده‌سازی

با هدف بهبود امنیت و کیفیت تصویر پنهان‌نگاری‌شده در LSBM، یک روش جدید پیشنهاد شد که در آن برای تصمیم‌گیری در دو مرحله انتخاب پیکسل‌ها برای جاسازی و نحوه تغییر مقدار پیکسل‌ها در اثر جاسازی از الگوریتم ژنتیک کمک گرفته شده است. این روش در Matlab 2016 پیاده‌سازی شد. با توجه به این‌که این روش بیشترین شباهت را به روش‌های موجود در [۳۴] دارد و این روش یکی از جدیدترین روش‌های چاپ شده در این حوزه است، برای مقایسه از این روش‌ها استفاده شده است. در جداول مقایسه‌ها روش GLSBM و MKGM که در بخش دوم معرفی شدند به همراه روش LSBM به عنوان روش پایه وجود دارند. در این جداول روش پیشنهادی، 2GA-LSBM نامیده شده است. به علاوه از روش‌های مبتنی بر LSBF مرور شده در جدول ۲ نیز استفاده شده است.

معیارهای موجود برای مقایسه روش‌های پنهان‌نگاری را می‌توان در سه دسته اصلی کیفیت تصویر پنهان‌نگاری شده، ظرفیت جاسازی و میزان مقاومت در برابر حملات تقسیم‌بندی کرد. از آن‌جا که ارائه کامل نتایج تمام آزمون‌های انجام شده امکان‌پذیر نیست، فقط نتایج مهم‌ترین آزمون‌ها در ادامه ارائه می‌شود. در این نتایج اندازه بلوک‌ها ۱۶×۱۶ و در الگوریتم‌های ژنتیک اجرا شده تعداد جمعیت برابر ۲۰، احتمال تقاطع برابر ۰/۷، احتمال جهش برابر ۰/۱ و تعداد تکرار برابر ۲۰ در نظر گرفته شده است.

۴-۱- کیفیت تصویر پنهان‌نگاری‌شده

همان‌طور که گفته شد یکی از اهداف روش ارائه شده بهبود کیفیت تصویر است، که یکی از معیارهای مهم در پنهان‌نگاری محسوب می‌شود. برای سنجش کیفیت تصویر از معیار PSNR استفاده شده است. در گام اول، روش پیشنهادی با روش‌های مبتنی بر LSBF موجود در جدول ۲ مقایسه شده است. برای این مقایسه از نتایج موجود در این مقالات برای درصد جاسازی ۰/۵ در تصاویر نمونه Lena، Baboon و Peppers استفاده شده است. جدول ۴، نتایج PSNR را برای این روش‌ها نشان می‌دهد. لازم به ذکر است که با توجه به این‌که در مقاله [۳۰] اعداد دقیق PSNR ذکر نشده است. نتایج جدول ۴ نشان می‌دهد که کیفیت تصویر پنهان‌نگاری‌شده در روش پیشنهادی نسبت به روش‌های مبتنی بر LSBF کاملا برتری دارد.

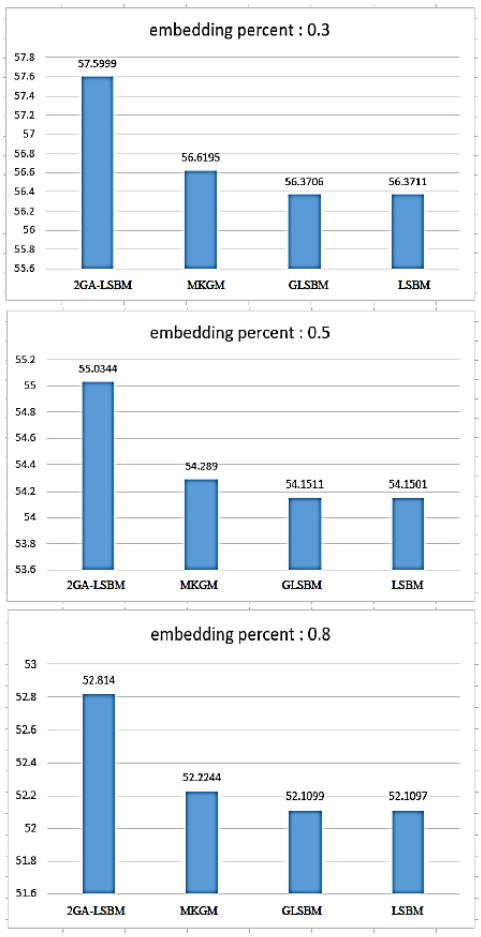
جدول ۴: معیار PSNR برای سه تصویر نمونه در روش‌های جاسازی مبتنی بر LSBF و روش پیشنهادی با درصد جاسازی ۰/۵

روش جاسازی	Lena	Baboon	Peppers
[۲۹] GA2017	۴۰/۸۷	۴۰/۰۱	۴۰/۳۸
[۳۰] ACO2018	< ۴۵	< ۴۵	< ۴۵
[۳۱] LCG	۵۱/۱۶	۵۱/۱۵	۵۱/۱۶
[۳۲] GA2019	۵۱/۳۶	۵۱/۳۵	۵۱/۳۶
[۳۳] LCG_GA	۴۶/۳۸	۴۶/۳۹	۴۶/۳۸
2GA-LSBM	۵۵/۰۳	۵۵/۰۴	۵۵/۰۱

در گام دوم، برای چند تصویر نمونه‌ی Lena، Baboon، Peppers و Boat مقدار این معیار برای درصدهای جاسازی ۰/۳، ۰/۵ و ۰/۸ در روش‌های مبتنی بر LSBM و روش پیشنهادی محاسبه شده‌اند. جدول ۵، نتایج PSNR را برای این روش‌ها نشان می‌دهد. نتایج این جدول نشان می‌دهد اگرچه نتایج این روش‌ها بیشتر به هم نزدیک هستند، اما باز هم برتری با روش پیشنهادی است. برای بررسی بیشتر میانگین PSNR برای ۲۵۰ تصویر از پایگاه داده NRCS در درصدهای جاسازی متفاوت برای روش پیشنهادی در مقایسه با روش MKGM و GLSBM محاسبه شده است که شکل ۹ این نتایج را نشان می‌دهد. این نمودار نیز برتری کیفیت تصویر پنهان‌نگاری‌شده‌ی حاصل از روش پیشنهادی را نسبت به روش‌های مبتنی بر LSBM نشان می‌دهد. از آن‌جا که در روش پیشنهادی ابتدا با استفاده از الگوریتم ژنتیک بهترین مسیر جاسازی از نظر تطابق بین پیکسل‌های تصویر و پیام محرمانه تعیین می‌گردد، کیفیت تصویر در روش پیشنهادی در درصدهای جاسازی مختلف همواره بهتر از روش‌های قبلی بوده و از این نظر برتری روش پیشنهادی کاملاً چشمگیر است و هدف افزایش کیفیت تصویر پنهان‌نگاری‌شده برآورده شده است.

جدول ۵: معیار PSNR برای چهار تصویر نمونه در روش‌های جاسازی مبتنی بر LSBM و روش پیشنهادی با سه درصد جاسازی مختلف

درصد جاسازی	روش جاسازی	Lena	Baboon	Boat	Peppers
۰/۳ bpp	[۱۰] LSBM	۵۶/۳۷	۵۶/۳۷	۵۶/۳۹	۵۶/۳۸
	[۳۴] GLSBM	۵۵/۶۸	۵۶/۴۱	۵۵/۳۵	۵۵/۶۵
	[۳۴] MKGM	۵۶/۵۷	۵۶/۶۸	۵۶/۵۳	۵۶/۶۱
	2GA-LSBM	۵۷/۶۰	۵۷/۵۸	۵۷/۶۱	۵۷/۶۰
۰/۵ bpp	[۱۰] LSBM	۵۴/۱۵	۵۴/۱۵	۵۴/۱۴	۵۴/۱۳
	[۳۴] GLSBM	۵۳/۶۴	۵۴/۱۶	۵۴/۱۳	۵۲/۱۱
	[۳۴] MKGM	۵۴/۳۲	۵۴/۴۱	۵۴/۲۶	۵۴/۳۴
	2GA-LSBM	۵۵/۰۳	۵۵/۰۴	۵۵/۰۳	۵۵/۰۱
۰/۸ bpp	[۱۰] LSBM	۵۲/۱۱	۵۲/۱۱	۵۲/۱۰	۵۲/۰۹
	[۳۴] GLSBM	۵۱/۶۱	۵۲/۱۳	۵۲/۱۲	۵۱/۴۵
	[۳۴] MKGM	۵۲/۱۰	۵۲/۱۲	۵۲/۱۶	۵۲/۱۲
	2GA-LSBM	۵۲/۸۰	۵۲/۸۱	۵۲/۸۱	۵۲/۸۲



شکل ۹: مقایسه PSNR برای درصدهای جاسازی مختلف

۴-۲- ظرفیت جاسازی

هر روش پنهان‌نگاری ظرفیت جاسازی مشخصی دارد. منظور از ظرفیت جاسازی، حداکثر تعداد بیتی است که می توان با استفاده از این روش در هر تصویر جاسازی کرد. معمولا در روش‌های حوزه مکان از واحد bpp (تعداد بیت در هر پیکسل) برای بیان مقدار جاسازی در یک تصویر استفاده می شود که حاصل تقسیم حداکثر تعداد بیت قابل جاسازی بر تعداد پیکسل‌های تصویر است. در جدول ۶، حداکثر ظرفیت جاسازی روش پیشنهادی و روش‌های قبلی آورده شده است.

جدول ۶: حداکثر ظرفیت جاسازی روش‌های قبلی و روش پیشنهادی

روش جاسازی	حداکثر ظرفیت جاسازی
[۲۹] GA2017	۴
[۳۰] ACO2018	< ۰/۵
[۳۱] LCG	۰/۵
[۳۲] GA2019	۴
[۳۳] LCG_GA	۲
[۳۴] GLSBM	۱
[۳۴] MKGM	۱
2GA-LSBM	۱

بعضی از روش ها مانند GA2017 [۲۹] و GA2019 [۳۲] ظرفیت بسیار زیاد و روش‌هایی مانند ACO2018 [۳۰] و LCG [۳۱] ظرفیت کمی دارند. اما روش‌های مبتنی بر LSBM از جمله روش پیشنهادی ظرفیت جاسازی حداکثر یک بیت در هر پیکسل را دارند.

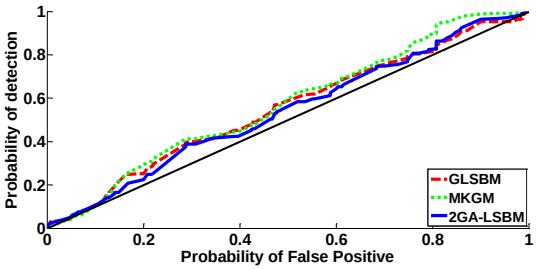
با توجه به وجود حملات عام موفق برای کشف روش‌های جاسازی، ظرفیت جاسازی بسیار بالا به تنهایی نمی‌تواند نقطه قوتی برای روش پنهان‌نگاری باشد. زیرا در صورت استفاده از این درصد جاسازی بالا، حتما حملات با دقت بالایی قادر به کشف آن روش خواهند بود. بنابراین اگر روشی بتواند داده کمی را به نحوی جاسازی کند که احتمال کشف آن پایین باشد، بسیار بهتر و کاربردی‌تر است نسبت به روشی که داده زیادی را با احتمال کشف بالا توسط حملات، در تصویر جاسازی کند. بنابراین فاکتور بسیار مهم‌تر امنیت روش پنهان‌نگاری است که در سطوح جاسازی یکسان سنجیده می‌شود.

۴-۳- امنیت در برابر حملات

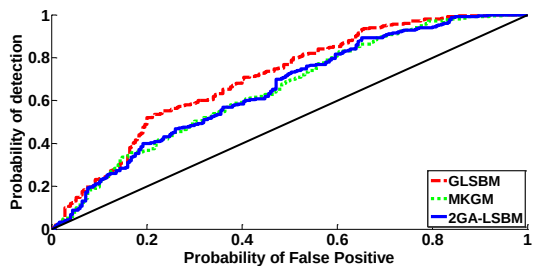
احتمال کشف کمتر توسط حملات، یک هدف مهم برای هر روش پنهان‌نگاری است. با توجه به امنیت پایین‌تر روش LSBF نسبت به LSBM و وجود حملات موفق زیاد برای کشف روش‌های مبتنی بر LSBF، برتری امنیت روش پیشنهادی نسبت به روش‌های مبتنی بر LSBF [۳۱-۲۹] کاملا قابل پیش‌بینی است. اما برای اطمینان بیشتر روش LCG [۳۱] به عنوان نماینده روش‌های مبتنی بر LSBF در سنجش میزان امنیت در نظر گرفته شده است. برای آزمایش این معیار از ۵۰۰ تصویر پایگاه داده NRCS استفاده شده است. حملات استفاده شده شامل ker1 [۱۹]، ker2 [۱۹]، CNGL [۲۲] و ALE [۲۳] می‌باشند که مخصوص روش جاسازی LSBM است. یکی از پارامترهای عددی نشان دهنده دقت هر حمله، مقدار AUC است، که این معیار عبارت است از مساحت میان نمودار ROC و قطر. این مساحت به‌گونه‌ای نرمالیزه می‌شود که مقدار آن برای یک روش کشف با موفقیت کامل، ۱ است. هر چه مقدار AUC به صفر نزدیک‌تر باشد، حمله موردنظر ناموفق‌تر و درنتیجه روش جاسازی امن‌تر است. جدول ۷، دقت کشف حملات مختلف (مقدار AUC) برای درصدهای جاسازی ۰/۳ و ۰/۵ را نشان می‌دهد. برای درک بهتر، نمودار ROC حاصل از دو حمله CNGL برای ظرفیت جاسازی ۰/۵ و ALE برای ظرفیت جاسازی ۰/۳ در شکل‌های ۱۰ و ۱۱ نشان داده شده است. هر چه نمودار ROC یک روش به قطر نزدیک‌تر باشد، نشان‌دهنده امنیت بالاتر آن روش یا به‌عبارت‌دیگر موفقیت کمتر حمله موردنظر در کشف روش است. بررسی نتایج جدول ۷ و نمودارهای شکل ۱۰ و ۱۱ نشان می‌دهد اگرچه GLSBM [۳۴] به‌تنهایی نتایجی مشابه و حتی در اندکی از موارد بدتر از LSBM دارد، اما روش MKGM [۳۴] و روش 2GA-LSBM امنیت بالاتری نسبت به روش LSBM دارند. به عبارت دیگر روش پیشنهادی در بهبود امنیت نسبت به روش LSBM موفق بوده است. بعلاوه بررسی نتایج روش LCG [۳۱] ادعای برتری کامل امنیت روش پیشنهادی نسبت به روش‌های مبتنی بر LSBF را تأیید می‌کند.

جدول ۷: دقت کشف روش‌های مختلف توسط چهار حمله

درصد جاسازی	نام روش	ker1	ker2	CNGL	ALE
۰/۳ bpp	[۱۰] LSBM	۰/۱۵۲۲	۰/۰۷۹۵	۰/۰۹۹۵	۰/۲۸۸۹
	[۳۱] LCG	۰/۸۹۸۶	۰/۶۸۸۱	۰/۰۸۹۹	۱
	[۳۴] GLSBM	۰/۱۵۹۰	۰/۰۶۲۲	۰/۱۲۹۵	۰/۲۸۴۰
	[۳۴] MKGM	۰/۰۸۶۷	۰/۰۵۷۹	۰/۰۸۹۰	۰/۲۷۲۴
	2GA-LSBM	۰/۰۸۵۶	۰/۰۵۶۶	۰/۰۸۴۲	۰/۲۷۱۹
۰/۵ bpp	[۱۰] LSBM	۰/۲۹۲۳	۰/۱۴۴۳	۰/۱۴۴۵	۰/۴۰۹۹
	[۳۱] LCG	۰/۹۴۴۳	۰/۸۲۲۸	۰/۲۳۵۰	۱
	[۳۴] GLSBM	۰/۲۸۳۴	۰/۱۳۴۹	۰/۱۰۹۶	۰/۴۰۳۸
	[۳۴] MKGM	۰/۱۵۸۷	۰/۰۷۴۸	۰/۱۲۵۲	۰/۳۰۵۵
	2GA-LSBM	۰/۲۰۷۶	۰/۱۱۹۹	۰/۰۹۸۰	۰/۳۰۹۷



شکل ۱۰: ROC حاصل از حمله CNGL در ۵۰٪ جاسازی



شکل ۱۱: ROCحاصل از حمله ALE در ۳۰٪ جاسازی

۴-۴- مدیریت کلید در روش پیشنهادی

تمام روش‌های پنهان‌نگاری و رمزنگاری در الگوریتم خود به کلیدهایی نیاز دارند که لازم است این کلیدها به نحوی به اطلاع گیرنده رسانده شود. باید این فرآیند به نحوی انجام شود که حداکثر امنیت (حداقل احتمال افشای کلیدها) وجود داشته باشد.

برای کلیدهای کوتاه، استفاده از یک کانال امن برای انجام این تبادل بهترین راه‌حل است. اما در بعضی از روش‌های پنهان‌نگاری با کلیدهای نسبتاً طولانی، از ایده تلفیق کلید و پیام اصلی استفاده می‌کنند و داده حاصل را در تصویر پوشش جاسازی می‌کنند. در این حالت برای استخراج بخش کلید به کلید کوتاهی نیاز است که این کلید از طریق کانال امن میان فرستنده و گیرنده تبادل می‌شود. سپس از کلید استخراج شده از تصویر، برای استخراج داده اصلی استفاده می‌شود.

طول کلید در روش پیشنهادی به طول بلوک‌ها بستگی دارد. برای هر بلوک، یک کلید ۲۴ بیتی محاسبه می‌شود و باید به اطلاع گیرنده رسانده شود. برای ارائه یک تحلیل عددی، یک تصویر ۵۱۲×۵۱۲ را در نظر بگیرید. اگر اندازه بلوک ۱۶×۱۶ در نظر گرفته شود، تصویر شامل ۱۰۲۴ بلوک است که با فرض جاسازی داده در تمام بلوک‌ها، طول کلید ۲۴۵۷۶ بیت است که نسبت به کل ظرفیت تصویر تقریباً ۰/۰۹۳ است. بدین ترتیب کمتر از ۱۰ درصد از ظرفیت تصویر را باید به جاسازی کلید اختصاص داد و می‌توان در مابقی تصویر، بیت‌های پیام محرمانه را جاسازی کرد. یک استراتژی برای جاسازی کلید می‌تواند به این ترتیب باشد: می‌توان بلوک‌های مشخصی از تصویر را برای جاسازی کلید استفاده کرد و جاسازی کلید در این بلوک‌ها را به روش GLSBM و با یک کلید کوتاه به عنوان هسته ابتدایی تابع rand انجام داد. با توجه به طول کلید، در ۹۴ بلوک از تصویر (شامل بلوک‌های اولین ردیف، آخرین ردیف و اولین ستون از تصویر) داده کلید ذخیره می‌شود و در بقیه بلوک‌ها داده اصلی به روش پیشنهادی جاسازی می‌شود.

اگر همین محاسبات را برای اندازه بلوک ۳۲×۳۲ تکرار کرد، تصویر شامل ۲۵۶ بلوک است که با فرض جاسازی داده در تمام بلوک‌ها، طول کلید ۶۱۴۴ بیت است که نسبت به کل ظرفیت تصویر تقریباً ۰/۰۲۳ است. بدین ترتیب کمتر از ۳ درصد از ظرفیت تصویر را باید به جاسازی کلید اختصاص داد و در مابقی تصویر، بیت‌های پیام محرمانه را جاسازی کرد. در این حالت ۶ بلوک از تصویر برای جاسازی کلید کافی است.

بنابراین محاسبات ارائه شده نشان می‌دهد حتی اگر کانال امنی برای تبادل کلید میان فرستنده و گیرنده وجود نداشته باشد، فرستنده می‌تواند بخشی از ظرفیت تصویر پوشش را برای جاسازی کلید اختصاص دهد و نگرانی در مورد غیرقابل استفاده عملی بودن روش پیشنهادی به دلیل نیاز به کلید را برطرف کند.

۵- نتیجه‌گیری

با کم کردن تغییرات تصویر پنهان‌نگاری‌شده نسبت به تصویر پوشش، می‌توان کیفیت تصویر پنهان‌نگاری‌شده را افزایش و احتمال موفقیت یک روش پنهان‌شکنی را کاهش داد. در روش پیشنهادی از الگوریتم ژنتیک برای رسیدن به این هدف استفاده شده است. در این روش تصویر پوشش بلوک‌بندی شده و الگوریتم جاسازی برای هر بلوک از تصویر شامل دو مرحله است. در مرحله اول که ترکیب الگوریتم ژنتیک و تابع LCG است، پیکسل‌هایی از بلوک برای جاسازی انتخاب می‌شوند که بیشترین مطابقت با دنباله پیام موردنظر را داشته باشند. در مرحله دوم برای جاسازی در این پیکسل‌ها از ترکیب الگوریتم ژنتیک و LSBM استفاده می‌شود تا ایجاد تغییرات در پیکسل‌ها برای جاسازی داده با هدف حداقل تغییر در هیستوگرام بلوک انجام شود. نتایج حاصل آمده از آزمون‌های مختلف نشان می‌دهد که روش پیشنهادی با حداکثر ظرفیت جاسازی یک بیت در هر پیکسل، دقت کشف پایین‌تری در مقابل حملات مختلف نسبت به LSBM دارد و بعلاوه کیفیت تصویر پنهان‌نگاری‌شده‌ی حاصل از آن نسبت به LSBM بهبود مناسبی داشته است. استفاده از بهینه‌سازی چندهدفه به جای استفاده از دو مرحله بهینه‌سازی تک‌هدفه به عنوان یک ایده برای کارهای آتی پیشنهاد می‌شود.

مراجع

[1] J. Kadhim, P. Premaratne, P.J. Vial and B. Halloran, "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and trends in Future Research," Neurocomputing, Vol. 335, pp. 299-326, 2019.

[2] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T. Ho and K.H. Jung, "Image Steganography in Spatial Domain: A Survey," Signal Processing: Image Communication, Vol. 65, pp.46-66, 2018.

[3] Y.J. Chanu, T. Tuithung and K.M. Singh, "A Short Survey on Image Steganography and Steganalysis Techniques". In 3rd National Conference on Emerging Trends and Applications in Computer Science, IEEE, pp. 52-55, 2012.

[4] V. Sabeti, S. Samavi, M. Mahdavi and S. Shirani, "Steganalysis and Payload Estimation of Embedding in Pixel Differences Using Neural Networks," Pattern Recognition, Vol. 43, No. 1, pp. 405-415, 2010.

[5] M.S. Subhedar and H.M. Vijay, "Current Status and Key Issues in Image Steganography: A Survey," Computer Science Review, Vol. 13, pp. 95-113, 2014.

[6] D.C. Wu and W.H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognition Letters, Vol. 24, No. 9-10, pp. 1613-1626, 2003.

[7] X. Zhang and S. Wang, "Vulnerability of Pixel-Value Differencing Steganography to Histogram analysis and Modification for Enhanced Security," Pattern Recognition Letters, Vol. 25, No. 3, pp. 331-339, 2004.

[8] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic Scheme Based on Pixel-Value Differencing and

LSB Replacement Methods," IEE Proceedings Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.

[9] C.M. Wang, N.I. Wu, C.S. Tsai and M.S. Hwang, "A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function," The Journal of Systems and Software, Vol. 81, No. 1, pp. 150-158, 2008.

[10] C.C. Chang and H.W. Tseng, "A Steganographic Method for Digital Images Using Side Match," Pattern Recognition Letter, Vol.25, No.12, pp. 1431-1437, 2004.

[11] P. Chen and W. Wu, "A Modified Side Match Scheme for Image Steganography," International Journal of Applied Science and Engineering, Vol. 7, No. 1, pp. 53-60, 2009.

[12] M. Hossain, S.A. Haque and F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information," The International Arab Journal of Information Technology, Vol. 7, No. 1, pp. 34-38, 2010.

[۱۳] م. مهدوی، "پنهان‌شکنی کمّی روش جایگزینی بیت کم‌ارزش مبتنی بر تحلیل هیستوگرام"، رساله دکترا، دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان ۱۳۹۰.

[14] C.K. Chan and L.M. Cheng, "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, Vol. 37, pp. 469–474, 2004.

[۱۵] م. مهدوی، ش. سماوی، م. اخوت و ص. اکرمی، "روش پنهان‌نگاری تطبیقی بر اساس اغتشاش جمع شونده،" پانزدهمین کنفرانس مهندسی برق ایران، اردیبهشت ۱۳۸۶.

[16] C. Liu, X. Li, X. Lu and B. Yang, "A Content-Adaptive Approach for Reducing Embedding Impact in Steganography," Proc. of the IEEE ICIP, pp. 1762-1765, 2009.

[17] A. Westfeld, "Detecting Low Embedding Rates". In Information Hiding, 5th International Workshop, LNCS, Vol. 2578, pp. 324-339, 2002.

[18] J.J. Harmsen and W.A. Pearlman, "Steganalysis of Additive Noise Modelable Information Hiding," Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, Vol. 5020, pp. 131-142, 2003.

[19] A. Ker, "Steganalysis of LSB Matching in Grayscale Images," IEEE Signal Processing Letters, Vol. 12, No. 6, pp. 441–444, 2005.

[20] A. Ker, "Resampling and the Detection of LSB Matching in Color Bitmaps," In Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE, Vol. 5681, pp. 1-15, 2005.

[21] J. Zhang, I.J. Cox and G. Doerr, "Steganalysis for LSB Matching in Images with High-Frequency Noise," Proceedings of the IEEE Workshop on Multimedia Signal Processing, pp. 385–388.

[22] G. Cancelli, I.J. Cox and G. Doerr, "Improved LSB Matching Steganalysis Based on the Amplitude of Local Extrema". in IEEE International Conference on Image Processing, 2008.

[23] F. Huang, B. Li and J. Huang, "Attack LSB Matching Steganography by Counting Alteration Rate of the Number of Neighbourhood Gray Levels." Proceedings of the IEEE ICIP, Vol. 1, pp. 401–404, 2007.

[24] M. Goljan, J. Fridrich and T. Holotyak, "New Blind Steganalysis and its Implications". in Security, Steganography, and Watermarking of Multimedia Contents VIII, Proceedings of SPIE, Vol. 6072, pp. 1-13, 2006.

[25] G. Cancelli, G. Doerr, I.J. Cox and M. Barni "A Comparative Study of +1 Steganalyzers". In IEEE Int. Workshop on Multimedia Signal Processing, IEEE Workshop on Multimedia Signal Processing (MMSP), 2008.

[26] Z. Xia, X. Wang, X. Sun, Q. Liu and N. Xiong, "Steganalysis of LSB Matching Using Differences Between Nonadjacent Pixels," Multimedia Tools and Applications, Vol. 75, No. 4, pp.1947-1962, 2016.

[27] L.Y. Tseng, Y.K. Chan, Y.A. Ho and Y.P. Chu, "Image Hiding with an Improved Genetic Algorithm and an Optimal Pixel Adjustment Process". In IEEE Eighth International Conference on Intelligent Systems Design and Applications, Vol. 3, pp. 320-325, 2008.

[28] M. Khodaei and K. Faez, "Image Hiding by Using Genetic Algorithm and LSB Substitution". In International Conference on Image and Signal Processing, pp. 404-411, 2010.

[29] A. Khamrui, D.D. Gupta, S. Ghosh and S. Nandy, "A Spatial Domain Image Authentication Technique Using Genetic Algorithm". In International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 577-584, Springer, 2017.

[30] S. Khan and B. Tiziano, "Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region," International Journal of Electrical and Computer Engineering (IJECE), Vol. 8, No. 1, pp. 379-389, 2018.

[31] P.D. Shah and R.S. Bichkar, "A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator". In International Conference on Intelligent Computing and Applications, Springer, Vol. 632, pp. 119-129, 2018.

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

[33] P.D. Shah and R.S. Bichkar, "Genetic Algorithm Based Imperceptible Spatial Domain Image Steganography Technique with High Payload Capacity," International Journal of Recent Technology and Engineering (IJRTE), Vol. 7, No. 5, 2019.

[34] و .ثابتی، س. س. فیاضی، ح. شیرین خواه، " بهبود امنیت روش پنهان‌نگاری LSBM با استفاده از الگوریتم ژنتیک، چند کلیدی و بلاک بندی"، نشریه مهندسی برق و مهندسی کامپیوتر ایران، سال ۱۸، شماره ۱، ص. ۴۹-۵۸، بهار ۹۹.

پاورقی‌ها:

[1] Steganography
[2] Watermarking
[3] Cover image
[4] Stego image
[5] Spatial domain
[6] Transform domain
[7] Discrete Cosine Transform (DCT)
[8] Discrete Wavelet Transform (DWT)
[9] Pixel Value Differncing (PVD)
[10] Least Significant Bit Flipping (LSBF)
[11] Least Significant Bit Flipping (LSBM)
[12] Peak Signal Noise to Ratio (PSNR)
[13] Linear Congruential Generator (LCG)