استفاده از الگوریتم ژنتیک و تپه‌نوردی برای بهبود عملکرد پنهان‌نگاری اطلاعات در تصویر

وحیده رشیدزاده[۱]، ارشد، محمدعلی بالافر[۲]، استادیار، سید ناصر رضوی[۳]، استادیار

۱- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - v.rashidzade@gmail.com
۲- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - balafarila@tabrizu.ac.ir
۳- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران – n.razavi@tabrizu.ac.ir

چکیده: در این مقاله، روش جدیدی برای پنهان‌نگاری[۱] داده‌ها در تصویر مبتنی بر الگوریتم‌های ژنتیک[۲] و تپه‌نوردی[۳] ارائه شده است. روش پنهان‌سازی مورد استفاده در این مقاله، روش جاسازی LSB است. برای افزایش کیفیت تصویر پنهان‌نگاری‌شده و همچنین ظرفیت ذخیره‌سازی در روش ارائه شده از الگوریتم ژنتیک استفاده شده است که عمل پنهان‌سازی را به‌صورت یک عمل جستجو و بهینه‌سازی، مدل‌سازی کرده است. همچنین چون جستجو با الگوریتم ژنتیک عمل زمان‌گیری است، برای حل این مشکل از الگوریتم‌های جستجوی محلی[۴] و تپه‌نوردی بهره گرفته شده است. نتایج ارزیابی‌ها نشان می‌دهد که در روش ارائه شده کیفیت تصویر پنهان‌نگاری‌شده با افزایش ظرفیت پنهان‌سازی باز هم قابل قبول است. همچنین اعمال الگوریتم تپه‌نوردی باعث افزایش سرعت مخفی سازی می‌شود.

واژه‌های کلیدی: پنهان‌نگاری، روش پنهان‌نگاری LSB، الگوریتم ژنتیک، الگوریتم‌های جستجوی محلی، الگوریتم تپه‌نوردی.

Using Genetic and Hill Climbing Algorithms to Improve Performance of Image Steganography

Vahideh Rashidzadeh, MSc[1], Mohammad Ali Balafar, Assistant Professor[2], Seyed Naser Razavi, Assistant Professor[3]

1- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: v.rashidzade@gmail.com
2- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: balafarila@tabrizu.ac.ir
3- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: n.razavi@tabrizu.ac.ir

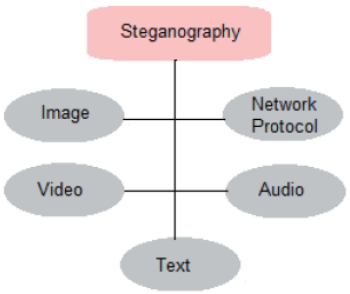
Abstract: In this paper, a new method based on genetic and hill Climbing algorithms for steganography in image is proposed. Data is embedded in LSB. In order to enhance image quality and storage capacity, genetic algorithm is utilized which model hiding as a search and optimization process. Also, to speed up the search function with genetic algorithm, local search and hill Climbing algorithms have been used. The findings show that the hiding image quality is acceptable while capacity is increased. Also, hill Climbing Algorithm speed up the hiding process.

Keywords: Steganography, LSB, genetic algorithm, local searching, hill climbing.

تاریخ ارسال مقاله: ۱۳۹۵/۰۳/۰۴
تاریخ اصلاح مقاله: ۱۳۹۵/۰۷/۰۷
تاریخ پذیرش مقاله: ۱۳۹۵/۰۸/۰۸
نام نویسنده مسئول: محمدعلی بالافر
نشانی نویسنده مسئول: ایران - تبریز - بلوار ۲۹ بهمن - دانشگاه تبریز - دانشکده مهندسی برق و کامپیوتر

۱- مقدمه

از زمانی که انسان‌ها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط مخفیانه یکی از خواسته‌های مهم افراد بوده است. گسترش روزافزون اینترنت و رشد سریع استفاده از آن، انسان‌ها را به‌سوی جهان دیجیتال و ارتباط از طریق داده‌های دیجیتالی سوق داده است. در این میان امنیت ارتباطات یک نیاز مهم است و هرروزه نیاز به آن بیشتر احساس می‌شود. در سالیان دراز مردم در جستجوی راه‌هایی برای ارتباطات امن بودند. یک راه ساده برای این مسئله استفاده از رمزنگاری[۵] است. در این روش اطلاعات به طریقی رمز می‌شود که برای شخص ثالث قابل فهم نیست. اما با آنکه رمزنگاری محتوای پیام را مخفی نگه می‌دارد، وجود ارتباط را مخفی نمی‌کند. پنهان‌نگاری شیوه دوم ارتباط محرمانه است. در پنهان‌نگاری علاوه بر مخفی ماندن اطلاعات، وجود ارتباط محرمانه باید مخفی بماند. پنهان‌نگاری به علم ارتباطات غیرقابل مشاهده اشاره می‌کند. برخلاف رمزنگاری که هدف امنیت اطلاعات است، پنهان‌نگاری به دنبال مخفی کردن خود پیام از دید دیگران است. پنهان‌نگاری عمل جاسازی اطلاعات و داده‌های سری در یک رسانه دیگر هست به‌گونه‌ای که ظاهر آن رسانه بیان‌کننده اطلاعات پنهان درون آن نباشد [۵-۱]. تقریباً همه فرمت‌های رقمی را می‌توان برای پنهان‌نگاری مورد استفاده قرار داد، اما فرمت‌هایی مناسب‌ترند که دارای درجه زیادی از افزونگی[۶] باشد. شکل ۱، انواع رسانه‌های مورد استفاده در پنهان‌نگاری را نشان می‌دهد [۶، ۷].



شکل ۱: رسانه‌های مورد استفاده در پنهان‌نگاری [۷]

روش‌های پنهان‌نگاری را می‌توان به دو گروه عمده تقسیم کرد: پنهان‌نگاری در دامنه مکانی[۷] و پنهان‌نگاری در دامنه تبدیلات[۸]. در روش پنهان‌سازی در حوزه مکان یا روش LSB که ساده‌ترین روش پنهان‌سازی پیام در تصویر است پیام در بیت‌های LSB هر پیکسل جاسازی می‌شود و به دو دسته LSB با طول ثابت و LSB با طول متغیر تقسیم می‌شود. در این روش چون دامنه تغییرات کم است برای همین برای چشم انسان قابل‌درک نیست، ولی مقاومت کمتری دارد. در روش پنهان‌نگاری در حوزه فرکانس تصویر ابتدا به حوزه فرکانس برده می‌شود و پنهان‌سازی در آنجا انجام می‌شود. از جمله روش‌های پنهان‌سازی در حوزه فرکانس روش تبدیل کسینوسی گسسته (DCT)، تبدیل فوریه گسسته (DFT) و تبدیل موجک گسسته (DWT) است [۳-۱ و ۸-۶]. برخی روش‌های پنهان‌نگاری برای بالا بردن معیارهای کارایی سیستم پنهان‌نگاری به‌وجود آمده‌اند. معیارهای مهم یک سیستم پنهان‌نگاری ظرفیت مخفی‌سازی[۹]، کیفیت[۱۰]، امنیت[۱۱] و مقاومت[۱۲] هستند. ازجمله این روش‌ها روش OPAP[۱۳] [۹]، است که در آن کیفیت بصری تصویر با پیچیدگی محاسباتی پایینی بالا می‌رود. روش‌های پنهان‌نگاری با الگوریتم ژنتیک برای دو منظور بالا بردن امنیت و شفافیت و بالا بردن ظرفیت پنهان‌سازی به‌کار گرفته می‌شوند [۱۰].

هدف این مقاله، ارائه روشی است که بتواند تصاویر امنیتی را طوری در تصویر پوشش پنهان‌سازی کرد که هم ظرفیت ذخیره‌سازی داده‌ها را بالا برد و هم به کیفیت بالایی برای پنهان‌نگاری تصاویر امنیتی دست یافت. برای رسیدن به این هدف از الگوریتم ژنتیک در این روش بهره گرفته شده است که مسئله پنهان‌نگاری را به‌صورت یک الگوریتم جستجو و بهینه‌سازی مدل‌سازی می‌کند و طبق کروموزوم[۱۴] موجود بهترین جا را در تصویر پوشش برای پنهان کردن تصویر امنیتی می‌یابد. همچنین برای بالا بردن سرعت روش ارائه شده، قبل از اجرای الگوریتم ژنتیک، از یک الگوریتم جستجوی محلی بهره گرفته شده است که در این روش الگوریتم جستجوی محلی استفاده‌شده، الگوریتم تپه‌نوردی است.

بخش‌های بعدی مقاله به‌صورت زیر سازمان‌دهی شده است: در بخش ۲، مروری بر کارهای پیشین خواهیم داشت. در بخش ۳، روش پیشنهادی و کارایی‌های آن بررسی می‌شود. در بخش ۴، نتایج حاصل از شبیه‌سازی این مقاله و در آخر در بخش ۵ نتیجه‌گیری بیان خواهد گردید.

۲- مروری بر کارهای پیشین

در یک مسئله پنهان‌نگاری معمولاً به دلایل زیر از الگوریتم ژنتیک استفاده می‌شود:

- برای بالا بردن امنیت تصویر پنهان‌نگاری‌شده[۱۵] در برابر حملات تحلیل پنهان‌نگاری[۱۶]
- برای بالا بردن ظرفیت ذخیره‌سازی با حفظ ویژگی کیفیت تصویر پنهان‌نگاری‌شده

با این‌که روش‌های پنهان‌نگاری امروزه کاربرد وسیعی پیدا کرده‌اند ولی این روش‌ها توسط الگوریتم‌های تحلیل پنهان‌نگاری به چالش کشیده می‌شوند [۱۱]. یکی از مهم‌ترین الگوریتم‌های تحلیل پنهان‌نگاری، الگوریتم RS[۱۷] است. که توسط Fridrich و همکاران [۱۳-۱۲]، ارائه شده است. که پیام مخفی‌شده را با تجزیه‌وتحلیل آماری مقادیر پیکسل‌ها تشخیص می‌دهد. برای اطمینان یافتن از امنیت داده‌های پنهان‌شده در مقابل حملات RS، shen wang و همکارانش [۱۴]، یک روش پنهان‌نگاری جدید مبتنی بر الگوریتم ژنتیک را ارائه داده است. در مقاله آن‌ها هیچ روش جدیدی برای پنهان‌سازی داده‌ها ارائه نشده است و روش پنهان‌نگاری که آن‌ها استفاده کرده‌اند روش LSB معمولی است. بعد از این‌که پیام مخفی در بیت‌های LSB تصویر

پوشش جاسازی شد، پیکسل‌های تصویر پنهان‌نگاری‌شده با استفاده از الگوریتم ژنتیک دست‌کاری می‌شوند تا مشخصات آماری تصویر حفظ شود. بنابراین وجود پیام مخفی در تصویر پنهان‌نگاری‌شده با تحلیل RS قابل تشخیص نیست. Vijay Kumar Sharma و همکاران [۱۵]، روشی را برای بالا بردن امنیت تصویر پنهان‌سازی شده در برابر حملات RS، با استفاده از الگوریتم ژنتیک ارائه داده‌اند که روش آن‌ها همانند روش shen wang است ولی روش ارائه شده دارای کیفیت بصری بهتری نسبت به روش shen wang است و در مقابله با حملات RS بهتر از آن عمل می‌کند و همچنین دارای پیچیدگی محاسباتی پایین‌تری نسبت به روش wang shen است. J.K.Mandal و همکارانش [۱۶]، روش پنهان‌نگاری مبتنی بر الگوریتم ژنتیک ارائه دادند و نام آن را DEGGA، نهادند. هدف اصلی روش آن‌ها پنهان‌سازی حجم زیادی از داده‌ها در تصویر پوشش است. در این روش حجم وسیعی از داده‌های تصویر سری در تصویر پوشش به‌صورت ماسک‌های ۳×۳ جاسازی می‌شوند. پنهان‌سازی در روش آن‌ها به روش LSB انجام می‌گیرد. بدین شکل که هر ۴ بیت از تصویر اصلی در ۴ بیت پایانی هر پیکسل از تصویر پوشش جاسازی می‌شود. بعد از آن عمل جهش[۱۸] روی تصویر جاسازی‌شده اعمال می‌شود. J.K.Mandal برای بالا بردن امنیت تصویر پنهان‌نگاری‌شده در روش خود از الگوریتم ژنتیک استفاده کرده است. G.Prema و همکارانش [۱۷]، روشی را برای پنهان‌سازی مبتنی بر LSB و همچنین الگوریتم ژنتیک و سهم‌بندی ارائه داده است. در روش ارائه شده توسط آن‌ها پیام اصلی در بیت‌های LSB، تصویر پوشش پنهان‌سازی می‌شود. سپس برای بالا بردن امنیت روش ارائه شده از الگوریتم ژنتیک و سهم‌بندی استفاده می‌شود. از الگوریتم ژنتیک برای دستکاری مکان پیکسل‌ها در تصویر پنهان‌نگاری‌شده استفاده می‌شود تا بدین ترتیب تشخیص پیام مخفی‌شده در آن را مشکل کند و در آخر با استفاده از سهم‌بندی تصاویر، تصویر پنهان‌نگاری‌شده را بین دو شریک بر اساس یک مقدار آستانه تقسیم می‌کند.

بین مقدار داده ذخیره‌شده و کیفیت تصویر پنهان‌نگاری‌شده نسبت عکس وجود دارد. یعنی هرچه مقدار داده‌ای که در میزبان ذخیره کنیم بیشتر باشد، کیفیت تصویر پنهان‌نگاری‌شده پایین‌تر می‌آید. روش‌های پنهان‌نگاری مبتنی بر الگوریتم ژنتیک می‌خواهند هم ظرفیت پنهان‌سازی را بالا ببرند هم کیفیت تصویر پنهان‌نگاری‌شده بالا بماند. Ran-Zan Wang و همکارانش [۱۸]، روش جدیدی برای پنهان‌سازی داده‌ها برای این منظور ارائه کرده‌اند که علاوه بر بالا بردن ظرفیت ذخیره‌سازی و کیفیت تصویر، امنیت تصویر پنهان‌نگاری‌شده را هم در مقابل دسترسی‌های غیرمجاز حفظ کنند. برای جلوگیری از دسترسی‌های غیر معتبر و افزایش عملکرد سیستم، روش تصادفی کردن عملیات LSB پیشنهاد شده است. یعنی k بیت برای جاسازی به‌صورت تصادفی جابجا می‌شوند. برای بالا بردن ظرفیت ذخیره‌سازی هم از الگوریتم ژنتیک در این روش بهره گرفته شده است. نتایج بررسی‌ها نشان می‌دهد که در این روش کیفیت تصویر پنهان‌نگاری مناسب است. همچنین ظرفیت ذخیره‌سازی این روش به‌اندازه ۱/۴ تا ۱/۲ تصویر میزبان است. Lifang Yu و همکارانش [۱۹]، روشی برای پنهان‌نگاری در تصاویر JPEG با عملکرد بالا ارائه نموده‌اند. روش ارائه‌شده توسط آن‌ها شامل دو بخش است. در ابتدا بهبودی برای پنهان‌نگاری LSB ارائه شده است که با حفظ مشخصات آماری مرتبه اول، به ظرفیت بالایی برای پنهان‌سازی دست یابد. بخش دوم به‌منظور به حداقل رساندن تخریب بصری تصویر پنهان‌نگاری‌شده، ترتیب بیت‌های پیام سری، به هم زده می‌شود، که پارامترهای این بی‌نظمی و به‌هم‌زدگی بر اساس الگوریتم ژنتیک به‌دست می‌آیند. نتایج بررسی‌ها نشان می‌دهد که روش ارائه‌شده دارای کیفیت بالای تصویر پنهان‌نگاری‌شده با حفظ ویژگی‌های هیستوگرام و ظرفیت بالا نسبت به روش‌های کلاسیک پنهان‌نگاری است. الهام قاسمی و همکاران [۱۰]، یک روش پنهان‌نگاری جدید مبتنی بر تبدیل موجک گسسته و الگوریتم ژنتیک ارائه کرده‌اند. در روش آن‌ها از الگوریتم ژنتیک برای ایجاد یک تابع نگاشت برای پنهان‌سازی داده‌ها در ضرایب تبدیل موجک تصویر پوشش، استفاده شده است. همچنین برای کاهش خطا بین تصویر پوشش و تصویر پنهان‌نگاری‌شده، عملیات اصلاح برای بهینه‌سازی پیکسل (OPAP) [۹]، روی تصویر پنهان‌نگاری‌شده انجام می‌شود. حمیدرضا رشیدی کنعان و همکاران [۲۰]، یک روش پنهان‌نگاری برای دست یافتن به کیفیت بالای تصاویر پنهان‌نگاری‌شده با الگوریتم ژنتیک ارائه داده‌اند. هدف اصلی آن‌ها در این مقاله، مدل‌سازی مسئله پنهان‌سازی به‌عنوان یک الگوریتم جستجو و بهینه‌سازی است. نتایج بررسی‌ها این روش نشان داده که روش آن‌ها نه‌تنها دارای کیفیت بالای تصاویر است بلکه دارای ظرفیت ذخیره‌سازی بالایی نیز است. عملیات پنهان‌نگاری در روش رشیدی کنعان در دو مرحله انجام می‌شود: اولین مرحله دستکاری داده‌های مخفی و مرحله بعدی جاسازی آن‌ها در تصویر پوشش است. در هر تصویر پوشش جاهای مختلفی برای پنهان‌نگاری بر اساس ترتیب بررسی پیکسل‌ها، نقاط شروع مختلف و ... وجود دارد. در این مقاله از الگوریتم ژنتیک که توسط گلدبرگ [۲۱]، در سال ۱۹۸۹ ارائه شده است، برای یافتن بهترین نقاط شروع، ترتیب بررسی پیکسل‌ها و یافتن بهترین PSNR تصویر پنهان‌نگاری‌شده استفاده می‌شود. بر اساس نظریه رشیدی کنعان، ترتیب بررسی پیکسل‌ها در یک تصویر می‌تواند مختلف باشد. ترتیب سطری از سطر اول تا آخر و از چپ به راست همان‌طور که در شکل ۲ نشان داده شده است، به‌عنوان Raster order شناخته می‌شود که معمولاً از این ترتیب برای بررسی پیکسل‌ها استفاده می‌شود.

ترتیب‌های بررسی مختلفی در یک تصویر وجود دارد، بنابراین اگر روشی باشد که همه ترتیب‌های ممکن را برای یافتن بهترین ترتیب برای جاسازی تصویر امنیتی در تصویر میزبان بررسی کند، نتیجه حاصل مطمئناً بهتر از روش LSB ساده خواهد بود. مسئله بعدی که

رشیدی کنعان به آن پرداخته است، نقطه شروع بررسی پیکسل‌ها است. به بیان دیگر در Raster order اگر برای جفت تصاویر اصلی و پوشش، نقطه شروع دیگری به‌جای پیکسل سطر اول ستون اول در نظر بگیریم، ممکن است به نتایج بهتری دست یابیم.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

شکل ۲: Raster order [۲۰]

10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	1	2	3	4
5	6	7	8	9

21	22	23	24	25
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

شکل ۳ : Raster order با نقاط شروع مختلف [۲۰]

برای جفت تصویر اصلی و میزبان، نقاط شروع مختلف و ترتیب‌های بررسی مختلف دارای PSNRهای مختلفی است و هیچ تضمینی وجود ندارد که نقطه شروع و ترتیب بررسی پیش‌فرض بهترین نتیجه را بدهد. در روش رشیدی کنعان، برای یافتن بهترین نقطه شروع و بهترین ترتیب بررسی از الگوریتم ژنتیک استفاده شده است تا یک تصویر پنهان‌نگاری‌شده با بالاترین PSNR را بیابد.

قبل از شروع توضیح الگوریتم پنهان‌نگاری به‌کار گرفته شده در روش رشیدی کنعان ، نمایش یک کروموزوم را در این روش بررسی می‌کنیم. کروموزوم به‌کار گرفته شده در این روش شامل ۷ ژن[۱۹] است که در جدول ۱ نشان داده شده است. ژن‌های X-offset و Y-offset ، نشان دهنده نقطه شروع بررسی و ژن Direction ترتیب بررسی پیکسل‌ها را نشان می‌دهد.

ژن Bit-Planes ، برای تعیین مکان LSB در هر پیکسل میزبان برای جاسازی بیت‌های تصویر سری است. توضیحات برای ژن‌های SB-Pole، SB-Dire و BP-Dire هم در جدول ۲ آمده است.

ژن‌های کروموزوم روش رشیدی کنعان به دو گروه تقسیم می‌شوند. گروه اول به ژن‌هایی اشاره دارد که مکان جاسازی بیت‌های تصویر امنیتی را در میزبان نشان می‌دهد.

گروه دوم ژن‌هایی هستند که روی بیت‌های تصویر امنیتی تغییراتی انجام می‌دهند تا با تصویر پوشش بیشتر منطبق شوند. روش پنهان‌سازی به‌کاررفته در این روش در فلوچارت شکل ۴، نشان داده شده است. در این فلوچارت نحوه ذخیره‌سازی داده در تصویر میزبان و ایجاد تصویر پنهان‌نگاری‌شده نشان داده شده است. Pratiksha Sethi و همکارانش [۲۲]، روشی برای پنهان‌نگاری داده‌ها ارائه داده‌اند که در آن ابتدا فایلی که قرار است پنهان‌سازی شود برای کوچک‌تر کردن اندازه‌اش ابتدا فشرده‌سازی می‌شود. سپس با استفاده از الگوریتم رمزنگاری AES، رمزنگاری می‌شود و در آخر داده رمزنگاری‌شده داخل یک تصویر پنهان‌سازی می‌شود. الگوریتم ژنتیک در این روش برای دسته‌بندی پیکسل‌های تصویر که داده در آن پنهان شده است به‌کار گرفته می‌شود تا نتوان داده پنهان‌نگاری‌شده در تصویر را شناسایی کرد. هدف اصلی روش ارائه توسط Pratiksha Sethi و همکارانش بالا بردن امنیت با به‌کارگیری روش رمزنگاری AES و به‌کارگیری الگوریتم ژنتیک برای پنهان‌سازی برای شناسایی داده پنهان شده در تصویر است.

جدول ۱: نمایش یک کروموزوم در روش رشیدی کنعان [۲۰]

نام ژن	محدوده مقدار	طول	توضیحات
Direction	۱۵-۰	۴ بیت	جهت بررسی پیکسل‌های تصویر میزبان
X-offset	۲۵۵-۰	۸بیت	آفست X نقطه شروع
Y-offset	۲۵۵-۰	۸بیت	آفست Y نقطه شروع
Bit-Planes	۱۵-۰	۴بیت	مکان LSB برای جاسازی داده سری
SB-Pole	۱-۰	۱بیت	قطب بیت‌های تصویر سری
SB-Dire	۱-۰	۱بیت	جهت بیت‌های تصویر سری
BP-Dire	۱-۰	۱بیت	جهت Bit-Plan

جدول ۲: همه مقادیر ممکن برای ژن‌های SB-Pole، SB-Dire و BP-Dire [۲۰]

نام ژن	مقدار	توضیحات
SB-Pole	۰	هیچ تغییری در بیت‌های تصویر اصلی ایجاد نمی‌شود
	۱	در این مورد، تمام بیت‌های تصویر اصلی معکوس می‌شوند
SB-Dire	۰	هیچ تغییری در بیت‌های تصویر اصلی ایجاد نمی‌شود
	۱	در این مورد، بیت‌های تصویر اصلی از ابتدا تا انتها معکوس می‌شوند
BP-Dire	۰	در این مورد، Bit-plane از جهت MSB به LSB استفاده می‌شود
	۱	در این مورد، Bit-plane از جهت LSB به MSB استفاده می‌شود

۳- روش پیشنهادی

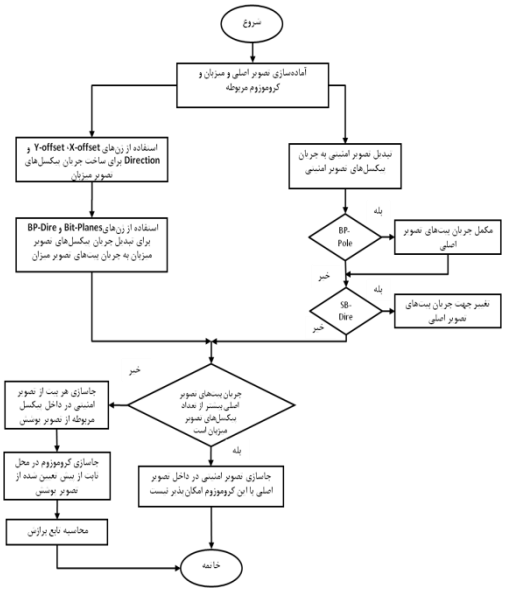
روش ارائه شده در این مقاله، یک روش پنهان‌سازی حوزه مکانی با استفاده از الگوریتم‌های ژنتیک و تپه‌نوردی است. در بخش‌های بعدی ابتدا هر یک از این مواد و روش‌ها را بررسی می‌کنیم و سپس به بررسی روش پیشنهادی می‌پردازیم.

۳-۱- بررسی مواد و روش‌ها

۳-۱-۱- پنهان‌سازی به روش LSB

پنهان‌نگاری در حوزه زمان یکی از ابتدایی‌ترین و ساده‌ترین روش‌های موجود است. در این روش اطلاعات امنیتی مستقیماً در بیت‌های

کم‌ارزش تصویر پوشش ذخیره می‌شوند به‌طوری‌که کیفیت تصویر پوشش و PSNR آن تنزل نکند. یکی از مهم‌ترین مزیت‌های پنهان‌نگاری به روش LSB این است که تغییرات با چشم انسان قابل درک نیستند.



شکل ۴: فلوچارت پنهان‌سازی روش پنهان‌نگاری رشیدی کنعان [۲۰]

۳-۱-۲- الگوریتم ژنتیک

الگوریتم ژنتیک، تکنیک جستجویی در علم رایانه برای یافتن راه‌حل تقریبی برای بهینه‌سازی و مسائل جستجو است. الگوریتم ژنتیک که به‌عنوان یکی از روش‌های تصادفی بهینه‌یابی شناخته‌شده، توسط جان‌هالند [۲۳]، ابداع شده است. درواقع الگوریتم‌های ژنتیک از اصول انتخاب طبیعی داروین برای یافتن فرمول بهینه جهت پیش‌بینی یا تطبیق الگو استفاده می‌کنند. در هوش مصنوعی الگوریتم ژنتیک، یک تکنیک برنامه‌نویسی است که از تکامل ژنتیکی به‌عنوان یک الگوی حل مسئله استفاده می‌کند. در الگوریتم‌های ژنتیک ابتدا به‌طور تصادفی، چندین جواب برای مسئله تولید می‌کنیم. این مجموعه جواب را جمعیت اولیه می‌نامیم. تکامل با جمعیت اولیه شروع می‌شود و در نسل‌های بعدی تکرار می‌شود. در هر نسل، مناسب‌ترین‌ها انتخاب می‌شوند. هر راه‌حل برای مسئله را یک کروموزوم می‌نامیم. هر کروموزوم حاوی تعدادی از ژن‌ها است. و یک تابع هدف به نام تابع برازش[۲۰] برای ارزیابی کیفیت هر کروموزوم استفاده می‌شود. گام بعدی ایجاد دومین نسل از جامعه است که بر پایه عملگرهای الگوریتم ژنتیک انجام می‌گیرد. عملیات الگوریتم ژنتیک تا زمانی تکرار می‌شود که یا به نتیجه مطلوب برسیم یا تعداد تکرارها به حداکثر برسد [۲۴، ۲۵].

۳-۱-۳- الگوریتم‌های جستجوی محلی

الگوریتم‌هایی مثل الگوریتم ژنتیک طوری طراحی شده‌اند که فضای جستجو را سیستماتیک بررسی کنند. برای این منظور یک یا چند مسیر در حافظه نگهداری می‌شود. وقتی هدف پیدا شد، مسیر رسیدن به آن هدف راه‌حل مسئله را تشکیل می‌دهد. ولی در بسیاری از مسائل مسیر رسیدن به هدف مهم نیست. بنابراین از نوع دیگری از الگوریتم‌ها، به نام الگوریتم‌های جستجوی محلی استفاده می‌شود. الگوریتم‌های جستجوی محلی، با استفاده از حالت فعلی عمل می‌کنند و فقط به همسایه‌های آن حالت منتقل می‌شوند. مسیرهایی که در جستجو ردیابی می‌شوند نگهداری نخواهند شد. به‌طور معمول، هر راه‌حل پیش رو، بیشتر از یک راه‌حل مجاور دارد. انتخاب هرکدام از راه‌حل‌ها برای حرکت، تنها با استفاده از اطلاعاتی است که درباره راه‌حل‌های مجاور راه‌حل فعلی در دست داریم و به همین جهت جستجوی محلی نامیده می‌شود. زمانی که راه‌حل مجاور به‌گونه‌ای انتخاب شود که به‌صورت محلی، معیار را به حداکثر برساند، این روش فرا ابتکاری[۲۱] را الگوریتم تپه‌نوردی می‌نامند [۲۶، ۲۷]. در علم کامپیوتر تپه‌نوردی، یک تکنیک بهینه‌سازی متعلق به خانواده جستجوی محلی است. این الگوریتم، حلقه‌ای است که در جهت افزایش مقدار حرکت می‌کند و فقط به همسایه‌های حالت فعلی نگاه می‌کند. وقتی به قله‌ای رسید که هیچ همسایه‌ای بلندتر از آن نیست، خاتمه می‌یابد. در حالت کلی بهینگی جوابی که این الگوریتم پیدا می‌کند محلی است و ممکن است در ماکزیمم محلی گیر کند. بنابراین با توجه به این مشکل، نقطه شروع در الگوریتم‌های جستجو محلی بسیار در ادامه اجرای الگوریتم تأثیرگذار خواهد بود. برای حل این مشکلات روش‌های مختلف تپه‌نوردی از قبیل تپه‌نوردی غیرقطعی[۲۲]، تپه‌نوردی اولین انتخاب[۲۳] و تپه‌نوردی شروع مجدد تصادفی[۲۴] به‌وجود آمدند.

۳-۱-۴- تپه‌نوردی اولین انتخاب

تپه‌نوردی اولین انتخاب ، تپه‌نوردی غیرقطعی را به این صورت پیاده‌سازی می‌کند که جانشین‌ها را به‌صورت تصادفی انتخاب می‌کند تا یکی از آن‌ها بهتر از حالت فعلی باشد. اگر مسئله دارای جانشین‌های زیادی باشد این روش مناسب است.

۳-۱-۵- تپه‌نوردی شروع مجدد تصادفی

تپه‌نوردی شروع مجدد تصادفی، دنباله‌ای از جستجوهای تپه‌نوردی است، که از حالت‌های اولیه تصادفی شروع می‌کنند و با رسیدن به هدف متوقف می‌شوند. در مسائل واقعی که تعداد مرکزیم محلی رشد نمایی دارد، پس از تعداد کمی شروع مجدد، ماکزیمم محلی خوبی پیدا می‌شود [۲۶، ۲۸ و ۲۹].

۳-۲- روش پیشنهادی

عملیات موجود در روش پیشنهادی در دو فاز پنهان‌سازی و جستجوی جمعیت‌های برگزیده انجام خواهد شد.

۳-۲-۱- فاز پنهان‌سازی

برای پنهان‌نگاری در روش ارائه‌شده، از روش پنهان‌نگاری براساس الگوریتم ژنتیک حمیدرضا رشیدی کنعان [۲۰]، استفاده شده است. روش پنهان‌سازی در روش ارائه‌شده همان‌طور در فلوچارت شکل ۴، آمده است به این شکل است که در ابتدا بر اساس کروموزوم موردنظر برای پنهان‌سازی جفت تصاویر اصلی و میزبان را آماده می‌کنیم. برای این کاربر اساس ژن‌های X-offset و Y-offset و همچنین ژن Direction ، تصویر پوشش جدید می‌سازیم. همچنین بر اساس ژن‌های SB-Pole و SB-Dire جریان بیت‌های تصویر اصلی را برای جاسازی آماده می‌کنیم. بعد از این‌که بررسی شد آیا تصویر میزبان گنجایش ذخیره‌سازی تصویر امنیتی را دارد یا خیر، جریان بیت‌های تصویر امنیتی بر اساس ژن‌های Bit-Planes و BP-Dire ، در پیکسل‌های تصویر میزبان جاسازی می‌شوند. همچنین خود کروموزوم هم در یک جای استاتیک و از قبل تعیین شده جاسازی می‌شود. بعد از این مراحل تصویر پنهان‌نگاری‌شده آماده است و تابع برازش که در اینجا PSNR است، برایش محاسبه می‌شود.

۳-۲-۲- عملیات جستجو و بهینه‌سازی

هدف از ارائه این مقاله، مدل‌سازی عمل پنهان‌نگاری به‌صورت عملیات جستجو و بهینه‌سازی است. یعنی برای یک جفت تصویر اصلی و میزبانی که در دست داریم، پیکسل‌های تصویر میزبان را بگردیم و بهترین مکان را برای پنهان کردن جریان بیت‌های تصویر اصلی بیابیم تا هم کیفیت تصویر پنهان‌نگاری‌شده را بالا ببریم، هم ظرفیت ذخیره‌سازی و هم به امنیت بالایی دست بیابیم. برای رسیدن به این هدف حمیدرضا رشیدی کنعان پنهان‌سازی با الگوریتم ژنتیک را پیشنهاد داده است. ولی ما در روش پیشنهادی برای رسیدن به سرعت بالایی برای عملیات جستجو روش بالا را با یک الگوریتم جستجوی محلی ترکیب کردیم. درواقع این روش یک روش جستجوی ژنتیکی محلی برای عملیات بهینه‌سازی است. روش جستجوی ژنتیکی محلی، در سال ۲۰۰۱ توسط Andrzej Jaszkiewicz مطرح شد [۳۰]. هدف از این روش، ارائه یک مجموعه از راه‌حل‌های تقریباً کارآمد در یک زمان کوتاه است که به کاربر اجازه انتخاب یک راه‌حل خوب از میان راه‌حل‌های ارائه شده را می‌دهد. در روش جستجوی ژنتیکی محلی، الگوریتم جستجوی محلی به هر نسل اعمال می‌شود و از میان هر نسل بهترین نتایج را برای تولید نسل بعدی انتخاب می‌کند.

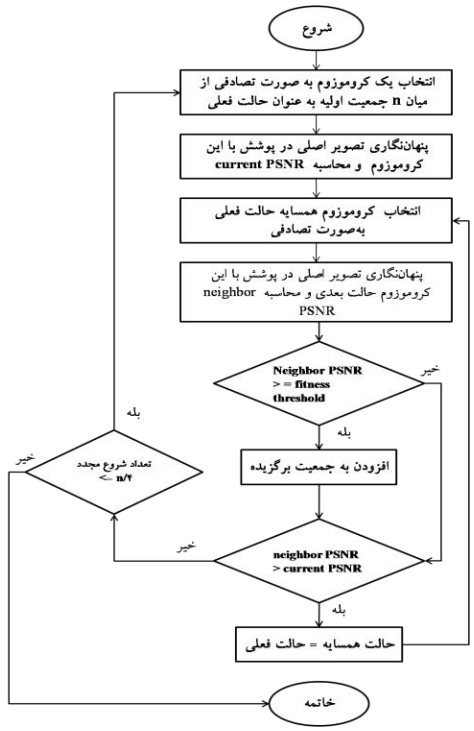
ما در این مقاله برای رسیدن به این اهداف از الگوریتم تپه‌نوردی استفاده کردیم. الگوریتم تپه‌نوردی برای یافتن یک بیشینه سراسری از میان جمعیت اولیه، از حالت فعلی شروع می‌کند و همسایه‌ها را یکی‌یکی بررسی می‌کند. اگر همسایه حالت فعلی بهتر از آن بود، به آن حالت منتقل می‌شود و حالت‌های قبلی را رها می‌کند. الگوریتم تپه‌نوردی کامل نیست چون همیشه در ماکزیمم محلی گیر می‌کند. همچنین ما دنبال یک ماکزیمم سراسری نیستیم بلکه دنبال مجموعه‌ای از جواب‌ها هستیم که بهتر از تابع برازش ما باشد. یکی از مدل‌های الگوریتم تپه‌نوردی، تپه‌نوردی شروع مجدد تصادفی است که این خواسته ما را برآورده می‌سازد. الگوریتم تپه‌نوردی با شروع مجدد تصادفی، مجموعه‌ای از الگوریتم‌های تپه‌نوردی است که از حالت تصادفی شروع می‌شوند و دنبال ماکزیمم سراسری هستند. ولی اینجا ما فقط دنبال ماکزیمم سراسری نیستیم بلکه هر جوابی که بهتر از تابع برازش باشد، آن را به‌عنوان جمعیت‌های برگزیده حفظ خواهیم کرد. الگوریتم تپه‌نوردی با شروع مجدد تصادفی، زمان اجرا را به‌طور چشمگیری کاهش داد. ولی PSNR آن نسبت به روش [۲۰]، کمتر شده است. دلیل آن هم این است که، در الگوریتم شروع مجدد تصادفی، اگر تعداد ماکزیمم‌های محلی زیاد باشد اکثر مواقع درست کار نمی‌کند. برای رسیدن به جواب بهینه ما روش شروع مجدد تصادفی را با الگوریتم تپه‌نوردی اولین انتخاب ترکیب کردیم. این روش هم مثل روش قبلی مجموعه‌ای از الگوریتم‌های تپه‌نوردی است با این تفاوت که در اینجا جانشین‌ها هم تصادفی انتخاب می‌شوند. این روش مجموعه جواب‌هایی که مدنظر ما هستند را می‌یابد. ولی زمان اجرایش کمی از روش قبلی بیشتر شده است. دلیل آن هم این است که چون این روش خیلی کم در ماکزیمم محلی گیر می‌کند، پس طول زمان جستجویش هم بیشتر است. ولی زمان جستجویش از روش [۲۰]، خیلی بهتر است. ولی در مقابل روش پیشنهاد شده مشکل روش قبلی که کم شدن میانگین PSNR بود را بهبود بخشیده است و همچنین PSNR این روش با روش [۲۰]، برابر است و در برخی جاها حتی بهتر از آن است. فلوچارت شکل ۵، عملیات گفته‌شده برای جستجو و یافتن جمعیت برگزیده در روش ارائه‌شده را نشان می‌دهد.

۳-۲-۳- مرحله تولید نسل جدید از میان جمعیت‌های برگزیده

برای تولید نسل جدید از میان جمعیت برگزیده مرحله قبل، ابتدا اندازه جمعیت برگزیده محاسبه می‌شود. اگر به‌اندازه‌ای بود که بتوان عمل Crossover را رویش انجام داد وارد این مرحله می‌شود.

عملگر Crossover با استفاده از دو رشته والد دو رشته فرزند به وجود می‌آورد. برای این کار قسمتی از بیت‌های والدین در بیت‌های فرزندان کپی می‌شود. انتخاب بیت‌هایی که باید از هر یک از والدین کپی شوند به روش‌های مختلف انجام می‌شود. که ما در روش ارائه شده از دو روش Crossover یک‌نقطه‌ای و دونقطه‌ای استفاده کرده‌ایم. بدین ترتیب نسل جدید از روی کروموزوم‌های برگزیده نسل قبلی تولید می‌شوند. بعد از تولید نسل جدید دوباره عملیات یافتن جمعیت برگزیده با الگوریتم تپه‌نوردی شروع می‌شود. این عملیات تا زمانی تکرار می‌شود که یا در نتایج نسل جدید نسبت به نسل قبلی بهبودی حاصل نشود یا تعداد تولیدات نسل جدید به حداکثر برسد.

بعد از این‌که عمل تولید نسل جدید پایان یافت الگوریتم پیشنهادی از میان جمعیت برگزیده، یک کروموزوم با بهترین دقت در PSNR را انتخاب می‌کند و آن را به‌عنوان جواب برمی‌گرداند.



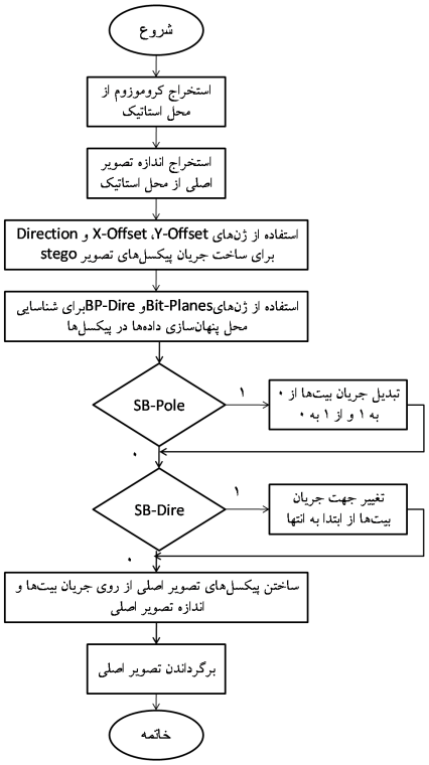
شکل ۵: عملیات جستجوی جمعیت برگزیده در روش ارائه شده

۳-۲-۴- بازیابی تصویر پنهان‌نگاری‌شده

همان‌طور که در فلوچارت شکل ۶، آمده است، برای بازیابی داده مخفی‌شده از تصویر پنهان‌نگاری‌شده، در قدم اول، باید کروموزومی که از آن برای پنهان‌نگاری استفاده کرده‌ایم را داشته باشیم. برای این کار کروموزوم را از محل استاتیک از قبل تعیین شده، استخراج می‌کنیم و ژن‌هایش را جدا می‌کنیم. براساس ژن‌های مربوط به تصویر میزبان یعنی X-Offset ، Y-Offset، Direction، Bit-Planes و BP-Dire محل جاسازی داده مخفی را می‌یابیم و داده مخفی را از آنجا استخراج می‌کنیم و بر اساس ژن‌های مربوط به جریان بیت‌های تصویر اصلی یعنی SB-Pole و SB-Dire، بررسی می‌کنیم که اگر تغییراتی در جریان بیت‌ها در مرحله پنهان‌سازی انجام شده باشد به حالت اولش برمی‌گردانیم و از روی جریان بیت‌هایی که در دست داریم جریان پیکسل‌ها و درنهایت تصویر امنیتی را درست می‌کنیم.

۴- نتایج ارزیابی‌ها

در این بخش کارایی روش پیشنهادی نسبت به روش [۲۰]، بررسی می‌شود. کارایی الگوریتم‌های پنهان‌سازی را از دیدگاه‌های مختلف از جمله کیفیت تصویر پنهان‌نگاری‌شده یا شفافیت، ظرفیت ذخیره‌سازی، زمان اجرا و امنیت می‌توان بررسی کرد که ما در ادامه این فصل روش پیشنهادی را بر اساس این معیارها بررسی خواهیم کرد. همچنین قابل ذکر است که در تمام ارزیابی‌های این مقاله، آزمایش‌ها را برای هر حالت ۲۰ بار اجرا شده است و در آخر میانگین نتایج ارزیابی‌شده را در جداول ثبت گردیده است. همچنین اندازه جمعیت اولیه در روش ارائه‌شده، ۲۰۰ کروموزوم در نظر گرفته شده است.



شکل ۶: فلوچارت بازیابی تصویر مخفی‌شده از تصویر پنهان‌نگاری‌شده

۴-۱- کیفیت و ظرفیت پنهان‌نگاری

کیفیت تصویر پنهان‌نگاری‌شده را از دو دیدگاه می‌توان بررسی کرد. قابلیت شناسایی توسط انسان به سیستم بینایی انسان مرتبط است. منظور از غیرقابل‌شناسایی بودن توسط انسان این است که یک فرد عادی با نگاه کردن به تصویر اولیه و تصویر حاوی پیغام نتواند بین دو تصویر تفاوتی قائل شود. از آنجا که این معیار دقیق نیست، باید معیاری تعریف کنیم تا توسط آن بتوانیم کارایی الگوریتم‌ها را در زمینه حفظ کیفیت تصویر بسنجیم. این مقیاس نسبت بیشینه سیگنال به نویز یا همان PSNR است. این مقیاس نشان دهنده میزان نویز اضافه‌شده به تصویر در اثر پنهان کردن اطلاعات در آن می‌باشد. رابطه (۱) میزان نسبت بیشینه سیگنال به نویز را در واحد دسی‌بل ارائه می‌دهد. همچنین از این نسبت به‌عنوان تابع برازش در این الگوریتم استفاده شده است.

$$PSNR = 10 \times \log_{10} \frac{(255)^2}{MSE} \qquad (۱)$$

در رابطه (۱) مقدار MSE، میانگین مجموع مربعات تصویر پوشش قبل و بعد از ذخیره‌سازی بیت‌های تصویر اصلی است. مقدار MSE با استفاده از رابطه (۲) محاسبه می‌شود.

$$MSE = \frac{1}{W \times H} \sum_{i-1}^{w} \sum_{j-1}^{H} \left(X_{i,j} - Y_{i,j} \right)^2 \quad (۲)$$

در رابطه (۲)، W*H اندازه طول و عرض تصویر است و $X_{i,j}$، مقدار پیکسل مربوطه قبل از ذخیره‌سازی و $Y_{i,j}$ نیز مقدار این پیکسل را بعد از ذخیره‌سازی نشان می‌دهد.

ظرفیت پنهان‌نگاری میزان اطلاعاتی است که می‌توان از طریق الگوریتم پنهان‌نگاری در تصاویر موردنظر ذخیره کرد، طوری که این جاگذاری از طریق روش‌های نهان‌کاوی قابل شناسایی نباشد. به‌عبارت دیگر ظرفیت پنهان‌نگاری حداکثر میزان داده‌ای است که می‌تواند بدون این‌که قابل شناسایی باشد جاگذاری شود. فاکتورهای کیفیت و ظرفیت پنهان‌سازی با یکدیگر نسبت عکس دارند. اگر برای کاربر کیفیت تصویر پنهان‌نگاری‌شده مهم باشد، پس باید داده کمتری در تصویر پوشش مخفی کند تا کیفیت آن تنزل نکند. ولی اگر برای کاربر ظرفیت پنهان‌نگاری در اولویت باشد، و کیفیت زیاد مسئله مهمی نباشد، می‌تواند داده بیشتری را در تصویر پوشش جاسازی کند.

برای ارزیابی کیفیت روش ارائه شده با ظرفیت‌های مختلف از دو تصویر «woman_darkhair» و «Baboon» با اندازه‌های ۱۲۸×۱۲۸ (شکل ۷)، به‌عنوان تصویر پوشش و از تصویر «Cameraman»، به‌عنوان تصویر امنیتی استفاده کرده‌ایم.

ابعاد تصویر امنیتی همان‌طور که در شکل ۸ نشان داده شده است، برای اندازه‌گیری ظرفیت‌های مختلف پنهان‌نگاری متفاوت است.

ظرفیت تصویر پوشش برای پنهان‌سازی را می‌توان به دو صورت بیت به ازای هر پیکسل یا به‌اصطلاح bpp و یا به‌صورت درصدی بیان کرد. جدول ۳، نتیجه اجرای روش ارائه‌شده برای دو تصویر پوشش شکل ۷ و همچنین تصاویر امنیتی شکل ۸ را نشان می‌دهد.

شکل ۷: تصاویر پوشش با اندازه‌های ۱۲۸×۱۲۸.الف) woman dark hair ب) Baboon

شکل ۸: تصویر امنیتی Cameraman در اندازه‌های مختلف

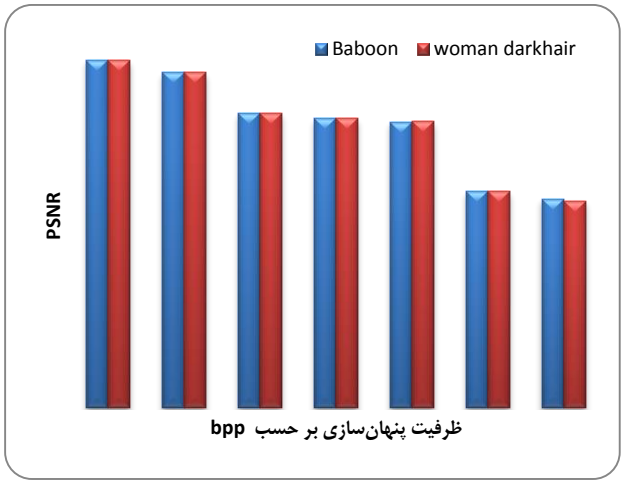
جدول ۳: نتایج ارزیابی روش ارائه شده برای تصاویر پوشش مختلف برحسب ظرفیت‌های مختلف پنهان‌سازی

ظرفیت		PSNR	
bpp	٪	woman darkhair	Baboon
۰/۵	٪ ۲۵/۶	۲۵/۵۴	۵۴/۲۶
۰/۸	٪ ۱۰	۵۲/۳	۵۲/۲۹
۱/۶۱	٪ ۲۰	۴۶/۰۱	۴۶/۰۲
۱/۹۶	٪ ۲۴/۶	۴۵/۱۹	۴۵/۲۰
۲	٪ ۲۵	۴۴/۶۵	۴۴/۶۳
۳	٪ ۳۷/۵	۳۳/۸۰	۳۳/۸۱
۴	٪ ۵۰	۳۲/۲۸	۳۲/۶۰

شکل ۹، نمودار جدول ۳ را نشان می‌دهد. با توجه به این نمودار و همچنین مقادیر جدول ۳ مشاهده می‌شود که نتایج روش ارائه شده از نظر PSNR و ظرفیت پنهان‌سازی رضایت‌بخش است. این نمودار نشان می‌دهد حتی زمانی که ظرفیت ذخیره‌سازی بالا می‌رود در آن صورت PSNR تصویر پنهان‌نگاری‌شده باز هم قابل قبول است.

۴-۲- زمان اجرا

الگوریتم‌های ژنتیک از لحاظ محاسباتی پرهزینه هستند. چون برای رسیدن به جواب بهینه باید فضای حالت بزرگی را به‌صورت سیستماتیک بررسی کنند. برای همین برای کاهش زمان اجرا، که هدف اصلی این مقاله است، ما سراغ روش‌های جستجوی محلی و تپه‌نوردی رفتیم. نتایج آزمایش‌هایی که در زیر آمده نشان از کاهش زمان اجرا در روش پیشنهادی می‌دهند. برای اجرای این ارزیابی هم از تصویر امنیتی «Cameraman»، با ابعاد مختلف همانند شکل ۸ و از تصویر پوشش «woman_darkhair»، با ابعاد ۱۲۸×۱۲۸، استفاده شده است.



شکل ۹: نمودار ارزیابی PSNR روش ارائه شده برای تصاویر پوشش مختلف برحسب ظرفیت‌های مختلف پنهان‌سازی

جدول ۴: ارزیابی زمان اجرای سه روش بیان‌شده برای تصویر پوشش woman darkhair با اندازه ۱۲۸× ۱۲۸ و تصویر امنیتی Cameraman با اندازه‌های مختلف

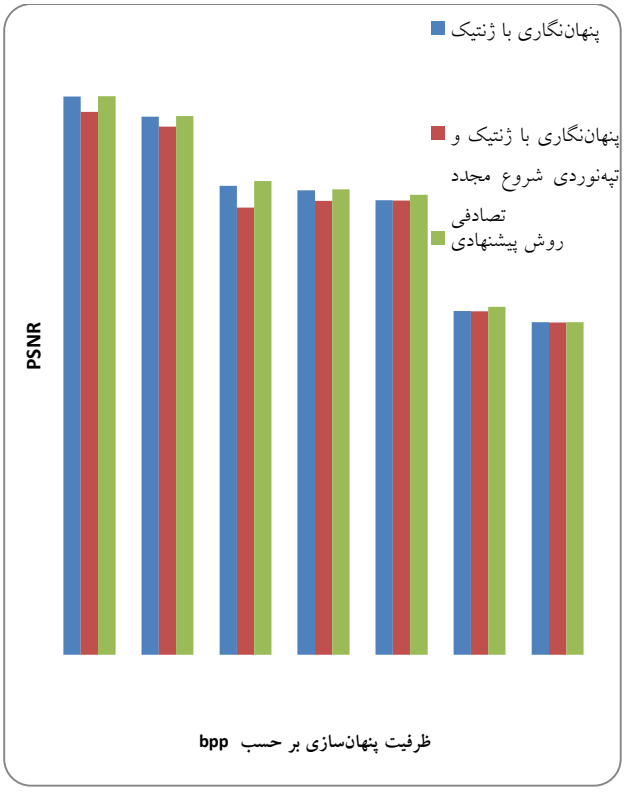
روش پیشنهادی	پنهان‌نگاری با ژنتیک و تپه‌نوردی شروع مجدد تصادفی	پنهان‌نگاری با ژنتیک [۲۰]	ظرفیت ذخیره‌سازی ٪	ظرفیت ذخیره‌سازی bpp
۲۱۷/۷۴	۱۵۵/۴	۲۳۰/۹۲	٪۶/۲۵	۰/۵
۱۵۹/۴۳	۱۳۲/۵۱	۲۲۵/۷۷	٪۱۰	۰/۸
۱۸۴/۷۷	۲۰۸/۷۷	۲۷۹/۶۶	٪۲۰	۱/۶۱
۲۵۲/۰۳	۱۸۷/۵۹	۲۹۱/۹۲	٪۶/۲۴	۱/۹۶
۲۸۶/۶۸	۲۳۹/۸۶	۳۷۱/۰۴	٪۲۵	۲
۵۵/۷۳	۲۹/۷۵	۷۳/۴۵	٪۳۷,۵	۳
۵۵/۲۶	۶۳/۳۵	۱۴۰۳/۰۸	٪۵۰	۴

با توجه به نتایج به‌دست‌آمده از این آزمایش و داده‌های جدول ۴، مشاهده می‌شود که روشی که در آن از الگوریتم ژنتیک با تپه‌نوردی شروع مجدد تصادفی استفاده شده است، در اکثر موارد زمان اجرای بهتری نسبت به دو روش دیگر دارد. ولی با دقت روی مقادیر جدول ۵، که نتایج PSNR را در همین آزمایش نشان می‌دهد، مشاهده می‌شود که این روش نسبت به دو روش دیگر مقادیر کمتری برای PSNR تصویر پنهان‌نگاری‌شده ارائه می‌دهد و چون هدف یک الگوریتم پنهان‌نگاری به حداکثر رساندن تمامی فاکتورهای بهینه‌سازی است، بنابراین روشی را انتخاب کردیم که هر دو فاکتور را بهبود دهد. روش پیشنهادی هم نسبت به دو روش دیگر PSNR بالایی دارد و هم زمان اجرایش بهتر است.

جدول ۵: ارزیابی PSNR سه روش بیان‌شده برای تصویر پوشش woman darkhair با اندازه ۱۲۸× ۱۲۸ و تصویر امنیتی Cameraman با اندازه‌های مختلف

روش پیشنهادی	PSNR			ظرفیت ذخیره‌سازی	
	پنهان‌نگاری با ژنتیک و تپه‌نوردی شروع مجدد تصادفی	پنهان‌نگاری با ژنتیک [۲۰]	٪	bpp
۵۴/۲۵	۵۲/۷۱	۵۴/۲۰	٪۶/۲۵	۰/۵
۵۲/۳۰	۵۱/۲۷	۵۲/۲۵	٪۱۰	۰/۸
۴۶/۰۱	۴۳/۴۳	۴۵/۵۳	٪۲۰	۱/۶۱
۴۵/۱۹	۴۴/۰۶	۴۵/۰۹	٪۲۴/۶	۱/۹۶
۴۴/۶۵	۴۴/۱۲	۴۴/۱۳	٪۲۵	۲
۳۰/۸۰	۳۳/۳۵	۳۳/۳۹	٪۳۷/۵	۳
۳۲/۲۸	۳۲/۲۶	۳۲/۳۱	٪۵۰	۴

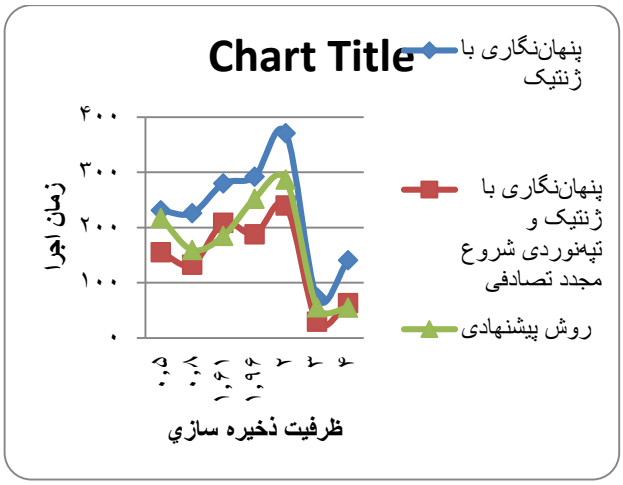
شکل ۱۰ و شکل ۱۱ هم نتایج این ارزیابی را به شکل نمودار نشان می‌دهند. نمودار شکل ۱۰ نشان می‌دهد که روش ارائه شده دارای PSNR بهتری نسبت به روش پنهان‌نگاری با الگوریتم ژنتیک [۲۰] و پنهان‌نگاری با الگوریتم ژنتیک تپه‌نوردی شروع مجدد تصادفی است. همچنین با توجه به نمودار شکل ۱۱، می‌توان مشاهده کرد که روش پیشنهادی دارای زمان اجرای بهتری نسبت به روش پنهان‌نگاری با الگوریتم ژنتیک است.



شکل ۱۰: نمودار ارزیابیPSNR روش‌های بیان‌شده برحسب ظرفیت‌های مختلف پنهان‌سازی

۵- نتیجه‌گیری

در این مقاله یک روش پنهان‌نگاری جدید با کیفیت بالا در حوزه مکان مبتنی بر الگوریتم‌های ژنتیک و تپه‌نوردی ارائه شده است. در روش ارائه‌شده، الگوریتم پنهان‌سازی به‌عنوان یک مسئله جستجو و بهینه‌سازی مدل‌سازی‌شده است. دلیل استفاده از الگوریتم ژنتیک یافتن بهترین مکان برای پنهان کردن تصویر امنیتی در تصویر پوشش است. دلیل استفاده از الگوریتم‌های جستجوی محلی در روش ارائه شده، صرفه‌جویی در زمان جستجو است. روش ارائه شده دارای ظرفیت بالای پنهان‌سازی، کیفیت بالای تصاویر پنهان‌نگاری‌شده و زمان اجرای پایین است. عملیات جاسازی در روش ارائه شده در دو فاز دستکاری و آماده‌سازی تصویر پوشش برای جاسازی و دستکاری بیت‌های تصویر امنیتی برای پنهان‌سازی انجام می‌شود. در روش ارائه‌شده چون تصویر امنیتی به جریانی از بیت‌ها تبدیل می‌شود، بنابراین می‌توان از هر فایل دیجیتالی دیگر اعم از صدا، فیلم و یا متن که بتواند به جریانی از بیت‌ها تبدیل شود را در تصویر میزبان ذخیره کرد. بنابراین یکی دیگر از مزیت‌های این روش این است داده امنیتی محدود به تصویر نیست.



شکل ۱۱: نمودار ارزیابی زمان اجرای روش‌های بیان‌شده برحسب ظرفیت‌های مختلف

مراجع

[1] Rana, M. S., Sangwan, B. S., & Jangir, J. S. (2012). Art of Hiding: An Introduction to Steganography. *International Journal of Engineering and Computer Science*, 1(1), 11-23.

[2] Shukla, A. K., Kumar, R., Bajpai, R. P., & Bharadwaj, L. M. (2004). Data Hiding in Digital Images: A Review. In *Procedings of the Pacific Rim Workshop on Digital Steganography, 2004* (pp. 186-190). ACROS Fukuoka, Fukuoka, Japan.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, no. 3, pp. 727–752, Mar. 2010.

[4] K. Bailey and K. Curran, "An evaluation of image based steganography methods," Multimed. Tools Appl., vol. 30, no. 1, pp. 55–88, Jun. 2006.

[5] S. Katzenbeisser and F. A. Petitcolas, Eds., Information Hiding Techniques for Steganography and Digital Watermarking, 1st ed. Norwood, MA, USA: Artech House, Inc., 2000.

[6] Singh, K. U. (2014). A Survey on Image Steganography Techniques. *International Journal of Computer Applications*, *97*(18).

[7] Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques.

[8] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26-34.

[9] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, Mar. 2004.

[10] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform," in Intelligent Control and Innovative Computing, S. I. Ao, O. Castillo, and X. Huang, Eds. Springer US, 2012, pp. 395–404.

[11] A. Nissar and A. H. Mir, "Classification of Steganalysis Techniques: A Study," Digit Signal Process, vol. 20, no. 6, pp. 1758–1770, Dec. 2010.

[12] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE Multimed., vol. 8, no. 4, pp. 22–28, Oct. 2001.

[13] J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images - State of the Art," in In Proceedings of SPIE, 2002, pp. 1–13.

[14] Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, *1*(1), 28-35.

[15] Sharma, V. K., & Shrivastava, V. (2011). Improving the performance of least significant bit substitution steganography against rs steganalysis by minimizing detection probability. *International Journal of Information and Communication Technology Research*, *1*(4).

[16] Mandal, J. K., & Khamrui, A. (2011). A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (DEGGA). *International Confrence on Electronic Systems (ICES-2011)*.

[17] G. Prema and S. Natarajan, "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application," in 2013 International Conference on Information Communication and Embedded Systems (ICICES), 2013, pp. 727–730.

[18] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognit., vol. 34, no. 3, pp. 671–683, Mar. 2001.

[19] L. Yu, Y. Zhao, R. Ni, and T. Li, "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm," EURASIP J. Adv. Signal Process., vol. 2010, no. 1, p. 876946, Jun. 2010.

[20] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," Expert Syst. Appl., vol. 41, no. 14, pp. 6123–6130, Oct. 2014.

[21] D. E. Goldberg, Genetic Algorithms in Search, Optimization and Machine Learning, 1st ed. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1989.

[22] P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," Procedia Comput. Sci., vol. 87, pp. 61–66, 2016.

[23] J. H. Holland, Adaptation in Natural and Artificial Systems. Cambridge, MA, USA: MIT Press, 1992.

[24] Nosrati, M., & Karimi, R. (2011). A Survey on Usage of Genetic Algorithms in Recent Steganography Researches. *World Applied Programming*, 206-210.

[25] D. A. Coley, An Introduction to Genetic Algorithms for Scientists and Engineers. River Edge, NJ, USA: World Scientific Publishing Co., Inc., 1998.

[26] S. J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 2nd ed. Pearson Education, 2003.

[27] V. Arya, N. Garg, R. Khandekar, A. Meyerson, K. Munagala, and V. Pandit, "Local Search Heuristic for K-median and Facility Location Problems," in Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing, New York, NY, USA, 2001, pp. 21–29.

[28] Anuradha Kasande and A.A. Agarkar, "An Enhancement in Quality of image & Anti- Steganalysis by Using Optimizing Image Steganography",

[29] IJEAT , 3(3) Feb. 2014.

[30] Skiena, S. S. (1998). The algorithm design manual: Text (Vol. 1). Springer Science & Business Media.

[31] A. Jaszkiewicz, "Genetic local search for multi-objective combinatorial optimization," Eur. J. Oper. Res., vol. 137, no. 1, pp. 50–71, Feb. 2002.

زیرنویس‌ها

[1] Steganography
[2] Genetic Algorithm
[3] Hill Climbing Algorithm
[4] Local Search Algorithms
[5] Cryptography
[6] Redundancy
[7] Spatial Domain
[8] Frequency Domain
[9] Hiding Capacity
[10] Perceptual Transparency
[11] Security
[12] Robustness
[13] Optimal Pixel Adjustment Process

[14] Chromosome
[15] Stego Image
[16] Steganalysis
[17] Regular Singular
[18] Mutation
[19] Gene
[20] Fitness Function
[21] Metaheuristic
[22] Stochastic hill climbing
[23] First choice hill climbing
[24] Random restart hill climbing algorithm