یک روش ترکیبی برای بهبود پنهان‌نگاری در تصاویر با استفاده از روش‌های فرا ابتکاری

لادن ریاضی[1]، علیرضا پورابراهیمی[2*]، محمود البرزی[3] و رضا رادفر[4]

[1و3و4] دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

[2] دانشکده مدیریت، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران

چکیده

در این مقاله روشی برای بهبود عملیات پنهان‌نگاری و بالابردن امنیت، با استفاده از ترکیب الگوریتم‌های فراابتکاری ارائه شده است. هدف، دست‌یابی به مقدار بهبودیافته PSNR است؛ به‌گونه‌ای که کیفیت تصویر در فرایند پنهان‌نگاری حفظ شود. در این روش ابتدا هفت الگوریتم فراابتکاری متداول در این حوزه، از جمله بهینه‌سازی کلونی مورچه، زنبور عسل، جستجوی فاخته، ژنتیک، حرکت ذرات، تبرید شبیه‌سازی‌شده، کرم شب‌تاب انتخاب و کارایی الگوریتم‌های یادشده پس از اعمال به‌صورت انفرادی بر روی داده‌های موجود مورد ارزیابی قرار می‌گیرد. از میان الگوریتم‌های اعمال‌شده، سه الگوریتم جستجوی فاخته، کرم شب‌تاب، زنبور عسل که دارای بهترین مقدار تابع برازش و درنتیجه بالاترین کیفیت هستند، انتخاب شدند. تمامی شش حالت مختلف از ترکیب این سه الگوریتم به‌طور مجزا بررسی شد. بهترین ترکیب به‌کاررفته به‌ترتیب، الگوریتم های کرم شب‌تاب، زنبور عسل و جستجوی فاخته است که این ترکیب، میانگین نسبت سیگنال به نوفه برابر ۵۴/۸۹ را فراهم کرده است. ترکیب یادشده در مقایسه با الگوریتم‌های انفرادی بررسی‌شده بهینه‌سازی کلونی مورچه، زنبور عسل، جستجوی فاخته، ژنتیک، حرکت ذرات، تبرید شبیه‌سازی‌شده، کرم شب‌تاب، به‌ترتیب به میزان ۵۹/۲۹، ۲۹/۶۱، ۳۷/۴۳ ، ۵۲/۵۶، ۵۴/۸۴، ۵۷/۸۲ و ۳/۸۲ درصد بهبود در مقدار PSNR را ارائه می‌کند.

واژگان کلیدی: پنهان‌نگاری، الگوریتم‌های فرا ابتکاری، الگوریتم کرم شب‌تاب، الگوریتم زنبور عسل، الگوریتم جستجوی فاخته.

A hybrid method to improve Steganography in JPEG images using metaheuristic algorithms

Ladan Riazi[1], Alireza Pourebrahimi[2]*, Mahmood Alborzi[3] & Reza Radfar[4]

[1,3,4] faculty of economics and management, science and Research Branch, Islamic Azad University, Tehran, Iran

[2] faculty of management, Karaj Branch, Islamic Azad University, Karaj, Iran

Abstract

This paper presents a method for improving steganography and enhancing the security using combinatorial Meta-heuristic algorithms. The goal is to achieve an improved PSNR value in order to preserve the image quality in the steganography process.

Steganography algorithms, in order to insert message signal information inside the host data, create small changes based on the message signal in the host data, so that they are not visible to the human eye. Each cryptographic algorithm has two steps: insert a stego signal and extract it. You can use the area of the spatial or transformation area to insert the stego signal. Extraction can be done using the correlation with the original watermark or independently of it. Clearly, the choice of insertion method and how to extract are interdependent. In spatial techniques, information is stored directly in pixel color intensity but in the transform domain, the image is initially converted to another domain (such as frequency), and then the

* Corresponding author

*نویسندهٔ عهده‌دار مکاتبات

• تاریخ ارسال مقاله: ۱۳۹۷/۰۹/۱۵ • تاریخ پذیرش: ۱۳۹۸/۰۳/۲۹ • تاریخ انتشار: ۱۳۹۹/۱۲/۰۴ • نوع مطالعه: پژوهشی

[DOI: 10.29252/jsdp.17.4.15]

information is embedded in the conversion coefficients. Using optimization algorithms based on Metahuristic algorithms in this field is widely used and many researchers have been encouraged to use it. Using a suitable fitness function, these methods are useful in the design of steganography algorithms.

In this research, seven commonly used Metahuristic algorithms, including ant colony, bee, cuckoo search, genetics, Particle Swarm Optimization, Simulated Annealing and firefly were selected and the performance of these algorithms is evaluated individually on existing data after being applied individually.

Among the applied algorithms, cuckoo search, firefly and bee algorithms that have the best fitness function and therefore the highest quality were selected. All 6 different modes of combining these 3 algorithms were separately examined. The best combination is the firefly, bee and cuckoo search algorithms, which provides a mean signal-to-noise ratio of 54.89.

The proposed combination compared to the individual algorithms of optimization of ant colony, bee, cuckoo search, genetics, Particle Swarm Optimization, Simulated Annealing and firefly, provides 59.29, 29.61, 37.43, 52.56, 54.84, 57.82, and 3.82% improvement in the PSNR value.

Keywords: steganography, Metahuristic algorithms, firefly algorithm, bee algorithm, cuckoo search algorithms.

۱- مقدمه

یکی از موضوعات مهم در مبادله پیام‌های محرمانه اینترنتی مسأله امنیت تبادل اطلاعات است. پنهان‌نگاری (استگانوگرافی[1]) یکی از شاخه‌های علم مخفی‌سازی اطلاعات است که به‌دنبال رسیدن به یک سطح امنیتی مطلوب در تبادل اطلاعات محرمانه تجاری و نظامی است؛ به‌نحوی که تبادل فایل‌هایی حامل اطلاعات محرمانه، برای دیگران محسوس و مشخص نباشد. این روش‌ها می‌تواند به‌عنوان مکمل روش‌های رمزنگاری در مبادله اطلاعات محرمانه استفاده شود [2]. استگانوگرافی از لغت یونانی استگانوس (پوشاندن) و گرافتوس (نوشتن) گرفته شده و درواقع استگانوگرافی دانشی است برای پنهان‌کردن داده یا فایلی در فایل دیگر، به‌طوری که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند. زمانی که پیغامی به‌وسیله پنهان‌نگاری در یک فایل میزبان پنهان می‌شود، درصورتی که شخصی بداند نحوه ذخیره‌سازی اطلاعات در این فایل چگونه بوده و نوع الگوریتم مورد استفاده جهت پنهان‌نگاری را نیز بداند، آنگاه او قادر خواهد بود اطلاعات را بخواند. مخفی‌کردن یک اطلاعات می‌تواند در لابه‌لای قالب‌های مختلفی از اطلاعات مانند متن، صوت، تصویر و شبکه باشد [3].

هر الگوریتم پنهان‌نگاری دو مرحله دارد: درج سیگنال نهان‌نگاره[2] در تصویر و استخراج آن. برای درج سیگنال نهان‌نگاره می‌توان از حوزه مکان یا حوزه تبدیل استفاده کرد. استخراج آن می‌تواند با استفاده از همبستگی با نهان‌نگاره اصلی و یا مستقل از آن صورت گیرد. واضح است، انتخاب روش درج و نحوه استخراج نهان‌نگاره به هم وابسته‌اند [4]. در روش‌های حوزه مکان اطلاعات به‌طورمستقیم در شدت رنگ پیکسل‌ها دخیره می‌شوند؛ ولی در حوزهٔ تبدیل ابتدا تصویر به حوزه دیگری (مانند فرکانس) منتقل شده و سپس اطلاعات در ضرایب تبدیل جاسازی می‌شود.

الگوریتم‌های پنهان‌نگاری، به‌منظور درج اطلاعات سیگنال پیام در داخل داده میزبان، تغییرات کوچکی را بر اساس سیگنال پیام در داده میزبان، ایجاد می‌کنند؛ به‌نحوی که با چشم انسان قابل مشاهده نباشد. واضح است که با افزایش داده‌های جاسازی‌شده در یک تصویر، احتمال مشکوک‌شدن تحلیل‌گر به وجود پیام پنهان در تصویر مورد نظر بیشتر می‌شود و لذا، امنیت پیام پنهان‌شده مورد نظر، به خطر می‌افتد، لذا در این مقاله، روشی ارائه شده که با حفظ کیفیت تصویر پنهان‌نگاری‌شده، امنیت ارتقا یابد [1].

۲- مروری بر پژوهش‌های مرتبط

تا کنون پژوهش‌های زیادی در زمینه پنهان‌نگاری تصویر انجام شده است. در مرحله درج، داده‌های پنهان‌نگاری درون تصویر میزبان قرار داده می‌شوند. برای این کار داده‌ها می‌توانند در حوزه مکان یا در حوزه تبدیل در تصویر قرار داده شوند. قراردادن داده در حوزه مکان یک روش ساده با هزینه محاسباتی بسیار کم ولی دارای مقاومت ناچیزی در برابر فشرده‌سازی تصویر است. در زمان استفاده از حوزه تبدیل، ابتدا برروی تصویر میزبان یک تبدیل مانند تبدیل موجک[3]، کسینوس یا فوریه[4] اعمال می‌شود، سپس زیرمجموعه‌ای از ضرایب تبدیل انتخاب و بر اساس داده‌های پیام، ضرایب طوری تغییر داده می‌شوند که در برگیرنده پنهان‌نگاری شوند [5]. در پژوهش‌های اخیر پنهان‌نگاری، تأکید بر استفاده از تبدیل موجک است؛ بعد از این مرحله،

[1] Steganography
[2] Watermark
[3] Wavelet
[4] Fourier transform

[DOI: 10.29252/jsdp.17.4.15]

تصویر پنهان‌نگاری‌شده آماده انتشار خواهد بود. مراحل بعدی فرایند پنهان‌نگاری در سمت گیرنده انجام می‌گیرد. در گیرنده، از تصویر پنهان‌نگاری‌شده که تحت تأثیر حملات و تغییرات عمدی و غیرعمدی در زمان انتشار قرار گرفته است، داده‌های پنهان‌نگاری‌شده استخراج می‌شوند.

در [3] آلگوریتمی برای درج سیگنال نهان‌نگاره در یک تصویرخاکستری، به روش طیف گسترده در حوزه تبدیل گسسته کسینوسی ارائه شده و تصویر پنهان‌نگاری‌شده در برابر حملات عمدی و غیر عمدی، به‌ویژه در برابر فشرده‌سازی JPEG مقاوم شده است. در پژوهشی دیگر [6] تبدیل گسسته کسینوسی بر روی بلوک‌های ۸×۸ تصویر انجام می‌شود. در هر بلوک، مهم‌ترین ضریب AC در جدول برای درج هر ضریبی از سیگنال طیف گسترده نهان‌نگاره، انتخاب شده است.

کارهایی نیز با استفاده از تبدیل موجک انجام شده است که در این روش‌ها ابتدا تبدیل موجک تصویر به‌دست می‌آید و پس از به‌دست‌آوردن ضرایب موجک، اطلاعات موردنظر در آن جاسازی شده است. به‌عنوان مثال در یکی از کارهای صورت‌گرفته، پنهان‌نگاری براساس چندی‌سازی[1] ضرایب فرکانس پایین تبدیل موجک بنا شده و از الگوهای تکرارشونده موجود در نماد پنهان‌شده در استخراج آن بهره می‌برد [7]. در پژوهشی دیگری در این زمینه، پنهان‌نگاری با استفاده از تبدیل موجک افزونه انجام می‌شود. در این روش سیگنال نهان‌نگاره در بخش فرکانس پایین تصویر میزبان پنهان می‌شود. این روش دارای مقاومت بالایی است و نهان‌نگاره را می‌توان با خطای کمی از تصویر استخراج کرد. در ابتدا از ضرایب تبدیل موجک مختلط تصویر برای محاسبه یک ماسک دیداری استفاده شده و سپس با استفاده از این ماسک نهان‌نگاره‌ای که به خصوصیات تصویر وابسته باشد، تولید می‌شود. برای پنهان‌سازی نهان‌نگاره نیز از ضرایب تبدیل موجک مختلط سطح سوم استفاده شده است [5].

روش سنتی تشخیص کور تصویر JPEG پنهان‌نگاری‌شده از یک ویژگی یا درنهایت تلفیق دو ویژگی استفاده می‌کند. مطالعه [8] به چگونگی انتخاب یک ترکیبی از ویژگی‌های برتر برای دست‌یابی به تشخیص بهتر پرداخته است. این مطالعه با بهره‌گیری از ایدهٔ درختان هافمن و محاسبه ضریب همبستگی به انتخاب ویژگی‌ها پرداخته است. به‌طوری‌که در هر بار به ترکیب دو ویژگی که کمترین ضریب همبستگی را دارند، می‌پردازد.

[1] quantization

در پژوهش [9] روش LSB[2] به‌عنوان روش پایه در نظر گرفته شده و جهت بهبود کیفیت و امنیت تصویر، تصویر پوششی به n بلاک ۸*۸ پیکسلی تقسیم و پیام محرمانه نیز به n بخش تقسیم، سپس از الگوریتم PSO[3] جهت یافتن ماتریس جایگزینی بهینه برای جایگزینی پیام محرمانه در هر بلاک به جای کل تصویر استفاده می‌شود.

در مطالعه [10] ترکیب دو الگوریتم فراابتکاری PSO و SA مطالعه شده است. روش انجام کار بدین صورت است که در ابتدا الگوریتم PSO به داده‌ها اعمال شده و بهترین نتیجهٔ به‌دست‌آمده از این الگوریتم به‌عنوان پاسخ اولیه در SA مورد استفاده قرار گرفته است؛ بنابراین پاسخ همسایه تولیدشده در SA بر مبنای پاسخ به‌دست‌آمده در الگوریتم PSO است. نویسنده مقاله ادعا می‌کند که این روش نه تنها موجب بهبود کیفیت تصاویر می‌شود، بلکه امنیت اطلاعات کدشده را نیز به‌خوبی تضمین می‌کند.

در مطالعه [11] از الگوریتم ACO جهت پنهان‌کردن داده‌ها در پیکسل‌های لبه‌ای تصویر استفاده شده است. در پژوهشی دیگر [12] ابتدا تصاویر به بلوک‌هایی تقسیم، سپس الگوریتم ACO به‌صورت جداگانه بر روی هر بلوک از تصویر اعمال می‌شود. در مطالعه [13] روشی جهت پنهان‌کردن داده‌ها در حوزه فرکانس با استفاده از الگوریتم ژنتیک (GA) ارائه‌شده و پژوهش‌گر توانسته با روش پیشنهادی موجب بهبود میزان PSNR در تصاویر پنهان‌نگاری و در نتیجه بهبود کیفیت تصاویر شود.

(جدول-۱): فهرست الگوریتم‌های فراابتکاری به‌کاررفته در پنهان‌نگاری تصاویر

(Table-1): The list of algorithms used in the image steganography

نام الگوریتم	مخفف	مرجع
بهینه‌سازی کلونی مورچه	ACO[4]	[14]
الگوریتم زنبور عسل	BA[5]	[15] و [16]
الگوریتم جستجوی فاخته	CS[6]	[17]
الگوریتم ژنتیک	GA[7]	[18] و[19] و [20]
الگوریتم بهینه‌سازی حرکت ذرات	PSO[8]	[21] و [22] و [30]
تبرید شبیه‌سازی شده	SA[9]	[23]
الگوریتم بهینه‌سازی کرم شب‌تاب	FA[10]	[24]

[2] least significant bit
[3] Particle swarm optimization
[4] Ant Colony Optimization
[5] Bee Algorithm
[6] Cuckoo Search Algorithm
[7] Genetic Algorithm
[8] Particle Swarm Optimization
[9] Simulated Annealing
[10] Firefly Algorithm

[DOI: 10.29252/jsdp.17.4.15]

استفاده از الگوریتم‌های بهینه‌سازی مبتنی بر الگوریتم‌های فرا ابتکاری و الگوریتم‌های مبتنی بر محاسبات زیستی در این حوزه متداول بوده و پژوهش‌گران زیادی را به استفاده از آن ترغیب کرده است. با استفاده از یک تابع برازش[1] مناسب، این روش‌ها در طراحی الگوریتم‌های پنهان‌نگاری مفید هستند. جدول (۱) فهرست الگوریتم‌هایی است که در این حوزه به‌کار رفته‌اند.

۳- روش استفاده‌شده در این پژوهش

مراحل انجام روش به‌کاررفته در این پژوهش، به این قرار است که چندین الگوریتم فرابتکاری متداول در پنهان‌نگاری تصاویر بر اساس مراجع یادشده در بخش قبل، مورد استفاده قرار می‌گیرند. ابتدا این الگوریتم‌های معرفی‌شده به‌تنهایی بر روی داده‌های موجود اعمال و پس از آن الگوریتم‌ها با توجه به بهترین PSNR به‌دست‌آمده مرتب می‌شوند. از میان الگوریتم‌های اعمال‌شده، سه الگوریتمی که نتیجه بهتری را داشته باشند، برای استفاده در مرحله بعد انتخاب می‌شوند. شش حالت مختلف از ترکیب این سه الگوریتم به‌طور مجزا بررسی و نتیجه نهایی ثبت می‌شود و ترکیبی که بهترین نتیجه را حاصل کند، انتخاب می‌شود. در ادامه جزییات مربوط به ترکیب الگوریتم‌ها را شرح خواهیم داد.

۳-۱- تابع برازش به‌کار رفته

از آنجایی که در مسایل مربوط به پردازش تصویر پارامترهای PSNR[2] و MSE[3] برای ارزیابی کیفیت تصویر به‌کار می‌روند، در این پژوهش مقدار PSNR به‌عنوان تابع برازش مورد استفاده قرار می‌گیرد. درواقع هر چه میزان PSNR بیشتر باشد، نشان‌دهندهٔ این است که بازسازی تصویر بهتر صورت گرفته و کیفیت تصویر بالاتر است و در نتیجه امنیت پنهان‌نگاری بهتر حفظ خواهد شد.

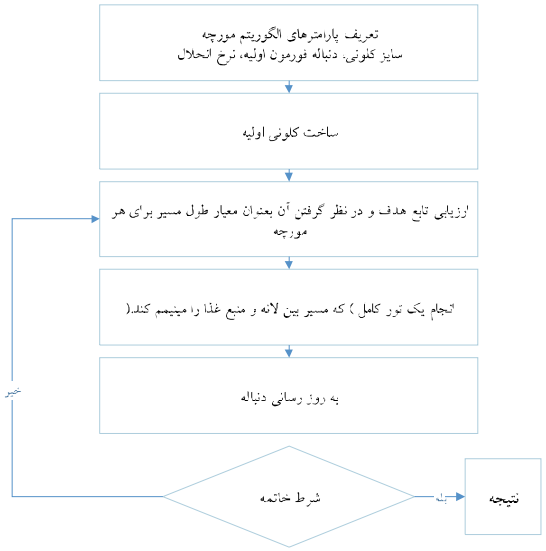
$$PSNR = 10 * \log_{10}(255^2/_{MSE}) \qquad (۱)$$

$$MSE = \frac{1}{W*H}\sum_{i=1}^{W}\sum_{j=1}^{H}(s_{ij} - c_{ij})^2 \qquad (۲)$$

c_{ij} و s_{ij} شدت پیکسل ij در تصویر پوششی[4] و تصویر به‌دست آمده[5] است. W و H تعداد پیکسل‌های موجود در طول و عرض تصویر اولیه است.

۳-۲- الگوریتم بهینه‌سازی کلونی مورچه (ACO) در پنهان‌نگاری تصاویر

طرح کلی از الگوریتم ACO عمومی در شکل (۱) ارائه شده است. مراحل زیر نحوه اجرای این الگوریتم فراابتکاری را در طرح پنهان‌نگاری تصاویر نشان می‌دهد [29].



(شکل-۱): شمای الگوریتم کلونی مورچه
(Figure-1): An Ant Colony Algorithm Schema

مرحله ۱: تعیین اندازه کلونی، دنباله فرمون اولیه، نرخ انحلال (σ)، تابع هدف، و تعداد نسل‌ها به‌عنوان معیار توقف الگوریتم.

مرحله ۲: تولید تصادفی یک جمعیت اولیه از مورچه‌ها، که مجموعه‌ای از راه‌حل‌های بالقوه را تشکیل می‌دهند. هر مورچه به‌صورت $X = \{x_1. x_2. \ldots . x_n\}$ نشان داده می‌شود. فرمول زیر نحوه تولید جمعیت اولیه را نشان می‌دهد.

$$f_{pheromone}(x_i) = e^{\frac{(x_i - x_i^*)^2}{2\sigma_i^2}} \qquad (۳)$$

که در آن است که x_i^* برابر با i‌ام امین مختصات بهترین نقطه پیداشده در بهینه‌سازی در فضای طراحی تکرار فعلی است. پارامتر σ_i شاخص تجمع مورچه‌ها برای مختصات i‌ام از فضای طراحی است. در تکرار نخست، x_i^* بر اساس یک توزیع یک‌نواخت در نظر گرفته می‌شود. همچنین σ_i دست‌کم سه برابر بزرگ‌تر از طول فاصله جستجو انتخاب می‌شود.

مرحله ۳: برای هر مورچه Xاز جمعیت:

تولید تصویر پنهان‌نگاری‌شده IW با استفاده از فرایند تعبیه‌سازی انجام شود.

[1] Fitness function
[2] peak signal to noise rate
[3] mean square error
[4] Cover Image
[5] stego-image

[DOI: 10.29252/jsdp.17.4.15]

• محاسبه همبستگی نرمال بین تصویر اصلی و تصویر پنهان‌نگاری شده: NC(I,IW)

اعمال یک حمله شناسایی اطلاعات پنهان‌نگاری‌شده از مجموع T حمله انتخاب‌شده به تصویر IW. این امر منجر به T تصاویر پنهان‌نگاری حمله شده متفاوت برای هر تصویر پنهان‌نگاری‌شده اصلی IW است. این تصاویر حمله‌شده را با $\{I'_W\}$ می‌شناسیم.

استخراج داده‌های پنهان‌نگاری‌شده از تصاویر مورد حمله واقع‌شده I'_W با استفاده از فرایند استخراج.

• محاسبه ضریب همبستگی نرمال بین اطلاعات پنهان‌شدهٔ اصلی W و مجموعه‌ای از اطلاعات استخراج‌شده.

• ساخت بردار ارزش‌های هدف، F (X) که به‌صورت زیر تعریف می‌شود:

$$F(X) = \left(\frac{1}{NC(I.I_W)}.\frac{1}{NC(W.W')}.\frac{1}{NC(I.W'_1)}.\dots.\frac{1}{NC(I.W'_T)}\right) \quad (۴)$$

• ارزیابی بردار ارزش‌های هدف و شناسایی بهترین مسیر

مرحله ۴: انتخاب بهترین مورچه به‌عنوان مورچه‌ای که کمترین مقدار را در تابع F (X) دارد.

مرحله ۵: به‌روزرسانی دنباله فرومون. این مرحله شاخص تجمع برای σi بعد iام برابر است با:

$$\sigma_i = \sqrt{\frac{1}{m}\sum_{i=1}^{m} y_i - y'} \quad (۵)$$

که در آن y برابر با iامین ستون از ماتریس کلونی C است. y' مقدار میانگین بردار y و m برابر با اندازهٔ کلونی است.

مرحله ۶: ذخیره مقدار Xbest در این نسل و نسل قبلی.

مرحله ۷: اگر شرط خاتمه (تعداد جمعیت) ارضا شده باشد، الگوریتم خاتمه می‌یابد؛ در غیر این صورت یک نسل جدید ایجاد شده و به مرحله ۳ باز می‌گردد.

۳-۳- الگوریتم بهینه‌سازی زنبور عسل (ABC[1]) در پنهان‌نگاری تصاویر

در الگوریتم بهینه‌سازی زنبور، درحالی‌که زنبورهای ناظر و کارگر به انجام فرایند بهره‌برداری در فضای جستجو مشغول هستند، پیشاهنگان کنترل فرایند اکتشاف را در دست دارند. در مرحله نخست، مجموعه‌ای از منابع غذایی به‌طور تصادفی بین $X_{min} = (x_{min.1}.\dots.x_{min.D})$ و $X_{max} = (x_{max.1}.\dots.x_{max.D})$ به‌صورت معادله زیر حساب می‌شود؛

[1] Artificial bee colony

که در آن $rand(0.1)$ یک عدد تصادفی با توزیع نرمال بین صفر و یک است.

$$X_{ij} = x_{min.j} + rand(0.1) * (x_{max.j} - x_{min.1}) \quad (۶)$$

در الگوریتم ABC، هر چرخه از جستجو از منابع غذایی جدید شامل سه مرحله است که در اینجا یک‌به‌یک مورد بحث قرار می‌دهیم:

زنبور عسل شاغل: زنبور به کار تولید یک راه حل جدید بسته به اطلاعات محلی پرداخته و مقایسه تناسب راه حل جدید را با راه حل قبلی آن انجام می‌دهد. اگر مقدار تناسب راه حل جدید بالاتر از راه حل فعلی آن باشد، راه حل جدید جایگزین راه حل قبلی می‌شود. در غیر این صورت با راه حل فعلی به کار خود به‌منظور تولید یک راه حل جدید ادامه خواهد داد. اگر راه حل جدید را با $y_i = (y_{i.1}.\dots.y_{i.D})$ نشان داده و راه حل قبلی را با $x_i = (x_{i.1}.\dots.x_{i.D})$ نشان دهیم، الگوریتم بهینه‌سازی مورچه بدین صورت عمل می‌کند:

$$y_{i.j} = x_{i.j} + \varphi_{i.j} * (x_{i.j} - x_{k.j}) \quad (۷)$$

که در آن $k \in \{1.2 \dots . SN\}. j \in \{1.2 \dots . D\}$ بوده و به‌صورت تصادفی انتخاب می‌شود؛ به‌طوری که شاخص K از i متفاوت باشد. j یک پارامتر تصادفی بین ۱- و ۱ است که تولید راه‌حل‌های جدید در همسایگی $x_{i.j}$ را انجام داده و نشان‌دهنده مقایسه بین دو موقعیت غذا مشاهده‌شده توسط یک زنبور عسل را نشان می‌دهند.

زنبور عسل ناظر: زنبورهای شاغل به اشتراک‌گذاری مقدار تابع برازش از منابع غذایی و اطلاعات موقعیت خود با زنبور عسل ناظر می‌پردازند. زنبور ناظر اطلاعات شهد گرفته‌شده را از تمام زنبورهای کارگر ارزیابی کرده و یک منبع غذایی را با درنظرگرفتن احتمال مربوط به مقدار تابع برازش آن انتخاب می‌کند.

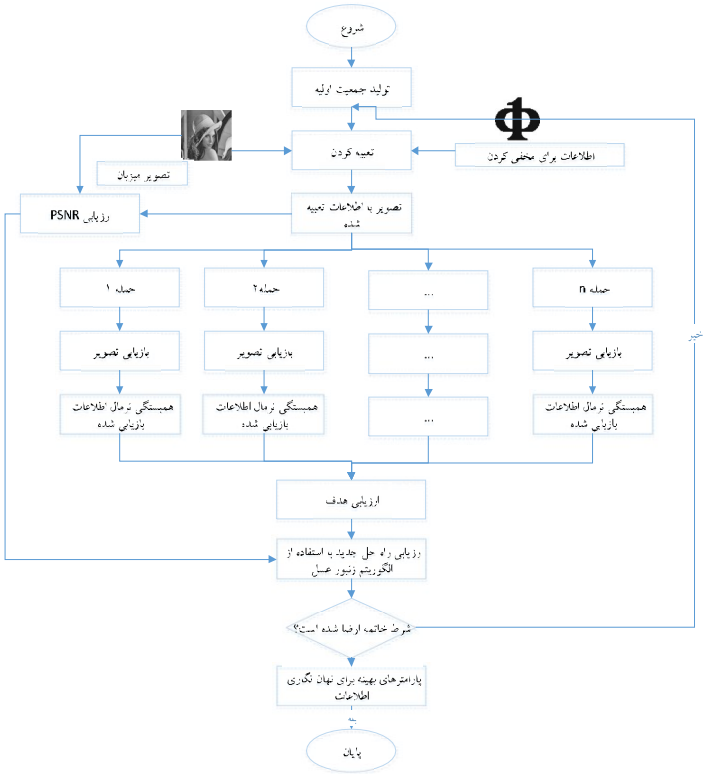
بدین ترتیب مقدار شهد از ماده غذایی افزایش می‌یابد و احتمال انتخاب آن منبع غذایی توسط سایر زنبورها نیز افزایش می‌یابد. پس از رسیدن به منطقه انتخاب شده، زنبور ناظر به انتخاب یکی دیگر از منابع غذایی در نزدیکی اطلاعات دریافتی ذخیره‌شده پرداخته و در صورت بهتربودن تابع برازش مقدار آن را جایگزین مقدار قبلی می‌کند. انتخاب یک منبع غذایی بر اساس احتمال P_i و به‌صورت زیر محاسبه می‌شود:

$$P_i = \frac{fit_i}{\sum_{i=1}^{SN} fit_i} \quad (۸)$$

[DOI: 10.29252/jsdp.17.4.15]

که در آن fit_i تابع برازش i امین راه حل در فضای مسأله است. SN برابر با تعداد راه‌حل‌ها یا برابر با تعداد زنبورهای کارگر است. fit_i به‌صورت زیر محاسبه می‌شود که در آن $f(X_i)$ تابع هدف اندازه‌گیری شده در i امین موقعیت غذایی است.

$$fit_i = \begin{cases} \frac{1}{f(X_i)} & if\ f(X_i) \geq 0 \\ 1 + abs(f(X_i)) & elsewhere \end{cases} \quad (۹)$$



(شکل-۲): پنهان‌نگاری تصویر با استفاده از الگوریتم جستجوی فاخته

(Figure-2): Image steganography using the Cuckoo search algorithm

۳-۴- الگوریتم جستجوی فاخته (CSA[1]) در پنهان‌نگاری تصاویر

مقداردهی جمعیت اولیه توسط مولد عدد تصادفی بین یک و پنجاه انجام می‌شود. اطلاعات موجود برای تعبیه‌سازی در فاکتور مقیاس‌پذیری ضرب و در بلوک مربوطه از تصویر میزبان تعبیه می‌شود. نحوه اجرای جستجوی فاخته در پنهان‌نگاری با کمک روندنمای شکل (۲) نمایش داده شده است. در مرحله بعد تصویر پنهان‌نگاری شده با چندین حمله روبه‌رو شده و اطلاعات مخفی‌شده از این تصاویر بازیابی می‌شود. تابع هدف برای هر تصویر محاسبه و سپس تصویری با بهترین تابع تناسب برای نسل بعدی انتخاب می‌شود. این روند تا ارضای معیار خاتمه الگوریتم ادامه می‌یابد.

۳-۵- الگوریتم ژنتیک (GA[2]) در پنهان‌نگاری تصاویر

برای استفاده از الگوریتم ژنتیک لازم است تا ابتدا ماتریس جایگزینی[3] به فرمت قابل فهم برای الگوریتم تبدیل شود. این فرمت یک بردار G از ژن‌هاست. هر درایه این آرایه با سطر مشابه در ماتریس جایگزینی متناظر است. برای مثال درایه شماره صفر با سطر شماره صفر متناظر است. مقادیر داخل خانه‌های آرایه حاوی اندیس ستون‌های استفاده‌شده در ماتریس است. به این صورت که عدد یک تنها در یکی از خانه‌های هر سطر وجود دارد [27] و [31].

گام‌های مورد استفاده در الگوریتم ژنتیک به شرح زیر است:

۱. ساخت جمعیت اولیه که با روش‌های مختلفی همچون الگوریتم اکتشافی و غیره ایجاد می‌شود.

[1] Cuckoo search Algorithm

[2] Genetic Algorithm

[3] Replacement

[DOI: 10.29252/jsdp.17.4.15]

۲. انتخاب و ترکیب نمونه‌های (آرایه) اولیه برای تولید نمونه جدید[1]. در مرحله تولید نمونه جدید از ترکیب تصادفی دو پدر برای تولید فرزند جدید استفاده می‌شود. درصورتی‌که فرزندهای تولیدشده حاوی ژن‌های تکرار شده باشند، این ژن‌ها با مقادیر ژن‌هایی که مورد استفاده قرار نگرفته‌اند، جایگزین می‌شوند. کل مرحله تولید نمونه جدید در یک تکرار ده تایی با ترکیب ده زوج تصادفی انتخاب شده انجام می‌شود.

۳. تغییر نمونه‌های فعلی و ساخت نمونه جدید که هدف اصلی آن جلوگیری از بهینه محلی است. چون در مرحله تولید نمونه جدید ممکن است از نمونه‌های مشابه برای ترکیب استفاده شده باشد.

۴. انتخاب نمونه با بهترین مقدار تناسب[2] در بین نمونه‌های تولیدشده در این نسل برای تولید نسل بعدی نمونه‌ها تا زمانی که شرط خاتمه ارضا شود. مقدار تناسب با اندازه‌گیری معیارهایی از قبیل PSNR انجام می‌شود.

برای بهبود کیفیت تصویر تولیدشده از روش بهبود پیونددهی مجدد مسیر[3] استفاده شده است. روش کار با انتخاب دو راه‌حل از بین فهرست راه‌کارهای موجود انتخاب شده است. در مخفی‌سازی تصاویر از این روش می‌توان بدین صورت استفاده کرد که پس از هر اجرای الگوریتم ژنتیک که تعداد ده تا از بهترین آرایه‌ها انتخاب می‌شوند و به‌طور تصادفی در گروه‌های دوتایی تقسیم می‌شوند، در هر گروه یکی از نمونه‌ها نقطه شروع و دیگری راهنما باشد. این روش پس از هر اجرای الگوریتم ژنتیک تعداد ده تا از بهترین آرایه‌ها را انتخاب کرده و به‌طور تصادفی در گروه‌های دوتایی تقسیم می‌شوند، در هر گروه یکی از نمونه‌ها نقطه شروع و دیگری راهنما باشد.

۳-۶- الگوریتم تبرید شبیه‌سازی‌شده (SA[4]) در پنهان‌نگاری تصاویر

در حل مسأله رمزنگاری تصاویر می‌توان بدین صورت عمل کرد که n جمعیت مطلوب نهایی را در این الگوریتم به‌عنوان پاسخ اولیه S برای الگوریتم SA در نظر گرفت. همچنین یک مقدار اولیه برای دما در نظر گرفته خواهد شد. در مرحله بعد با استفاده از الگوریتم SA یک جواب همسایه $\acute{S}$ برای مسأله تولید می‌شود. مقدار دلتا و PSNR برای این جواب محاسبه می‌شود. درصورتی‌که دلتا بزرگ‌تر از صفر باشد، $\acute{S}$ به‌عنوان جواب اویله در نظر گرفته می‌شود؛ در غیر این صورت $\acute{S}$ با احتمال $e^{-\Delta/T}$ به‌عنوان پاسخ فعلی انتخاب می‌شود. دمای جدید تنظیم می‌شود و درصورتی‌که مقدار T صفر نباشد یا تعداد تکرارها از بیشینه تکرارها بیشتر نباشد، دوباره یک جواب همسایه برای این مسأله در نظر گرفته می‌شود.

مراحل اعمال الگوریتم SA بر روی مسأله پنهان‌نگاری تصاویر به‌صورت زیر خواهد بود:

مرحله نخست: مقداردهی اولیه برای پاسخ ابتدایی S و همچنین بهترین راه حل یافت (bestsol) برای SA الگوریتم انجام و همچنین یک مقدار اولیه برای دمای T در نظر گرفته شود.

مرحله دوم: یک جواب همسایه 'S تولید و ارزش Δ و PSNR آن محاسبه خواهد شد. اگر $\Delta > 0$ باشد، آنگاه 'S به‌عنوان پاسخ فعلی انتخاب شده و اگر PSNR آن از bestsol بزرگتر باشد، bestsol الگوریتم با مقدار جدید به‌روزرسانی خواهد شد. در غیر این صورت الگوریتم به مرحله بعدی حرکت می‌کند.

مرحله سوم: یک عدد تصادفی با توزیع یکنواخت بین [۰، ۱] تولید می‌شود و در پارامتر r قرار می‌گیرد. اگر $r < e^{-\Delta/T}$ باشد، 'S به‌عنوان پاسخ فعلی معرفی خواهد شد.

مرحله چهارم: درجه حرارت جدید محاسبه شده و در پارامتر T مقداردهی می‌شود.

مرحله پنجم: اگر $T \neq 0$ و یا تکرار تعداد تکرار کمتر از بیشینه تکرارها باشد، به مرحله دوم رفته و در غیر این صورت الگوریتم متوقف و bestsol به‌دست‌آمده به‌عنوان جواب معرفی خواهد شد.

۳-۷- الگوریتم بهینه‌سازی حرکت ذرات (PSO[5]) در پنهان‌نگاری تصاویر

در الگوریتم حرکت ذرات، هر ذره p با 2k بعد به‌صورت $\boldsymbol{p} = \boldsymbol{p_0 p_1 \dots p_{2k-1}}$ نمایش داده می‌شود. که در آن $\boldsymbol{p_0}$ مکان عدد یک در سطر صفرم ماتریس جایگزینی، $\boldsymbol{p_1}$ مکان عدد یک در سطر نخست ماتریس جایگزینی و ... است. [28] یک ماتریس جایگزینی متناسب با ذره p در شکل (۳) به‌صورت نمونه مشاهده می‌شود. هر ذره با یک ماتریس جانشینی

[1] Crossover
[2] fitness
[3] PATH RELINKING REFINEMENT
[4] Simulated Annealing
[5] Particle swarm optimization

[DOI: 10.29252/jsdp.17.4.15]

همسان است؛ بنابراین، هر ذره با بهترین مقدار تابع تناسب به ماتریس جانشینی که می‌تواند تصویر پنهان‌نگاری‌شده را تولید کند، برابر است. هر ذره p باید یک بردار از اعداد صحیح در محدوده صفر تا 2K-1 باشد.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

{0 1 3 2}

(شکل-۳) : نگاشت ذره p باید یک بردار از اعداد صحیح در محدوده ۰ تا 2K-1 باشد

(Figure-3): The particle mapping p must be a vector of integers in the range 0 to 2K-1

شرح نحوه جستجو یک ماتریس جایگزینی از طریق الگوریتم PSO به‌صورت زیر خواهد بود:

مرحله ۱: مقدار دهی اولیه. به‌طور تصادفی K ذره اولیه تولید می‌شود. به هر ذره سرعت تصادفی Vi منتسب می‌شود. محاسبه PSNR برای هر ذره انجام شده وgbest را با مکان بهترین ذره که حاوی بالاترین مقدار PSNR است، مقداردهی می‌کنیم. در ادامه الگوریتم برای هر ذره داریم:

مرحله ۲: به‌روزرسانی سرعت و موقعیت هر یک از ذرات با استفاده از معادلات معرفی‌شده در فصل دوم.

مرحله ۳: محاسبه نتیجه نگاشت ذره i ام و سپس استنتاج PSNR مربوطه و بررسی اینکه این PSNR از مقدار مربوط به gbest بیشتر است یا خیر. در صورت بزرگ‌تربودن، مقدار gbest با مکان ذره iام به‌روزرسانی می‌شود.

مرحله ۴: اگر تعداد تکرارها از بیشینه تعداد تکرارها کوچک‌تر است، به مرحله دوم رفته و در غیر این‌صورت الگوریتم خاتمه یافته و بهترین خروجی را به‌عنوان نتیجه نهایی معرفی می‌کند.

۸-۳- الگوریتم کرم شب‌تاب (Firefly) در پنهان‌نگاری تصاویر

مراحل اعمال الگوریتم کرم شب‌تاب در مسأله پنهان‌نگاری تصاویر به قرار زیر است:

مرحله نخست: مقداردهی اولیه nکرم شب‌تاب به‌صورت تصادفی که در آن هر کرم شب‌تاب یک ردیف از ماتریس به‌اندازه m*m است. اندازه این ماتریس به اندازه محتوای مد نظر برای پنهان‌نگاری است.

مرحله دوم: برای هر کرم شب‌تاب i از جمعیت کرم‌های شب‌تاب داریم:

- تعبیه‌سازی متن در تصویر انجام شود.
- اعمال حمله شناسایی اطلاعات پنهان‌نگاری‌شده از مجموع T حمله انتخاب‌شده به تصویر پنهان‌نگاری‌شده. این امر منجر به T تصاویر پنهان‌نگاری حمله‌شده متفاوت برای هر تصویر پنهان‌نگاری‌شده اصلی می‌شود.
- استخراج داده‌های پنهان‌نگاری شده از تصاویر مورد حمله واقع‌شده با استفاده از فرایند استخراج.
- محاسبه تابع برازش PSNR برای هر تصویر و مقداردهی به تابع برازش مربوط به هر کرم شب‌تاب

مرحله سوم: به‌روزرسانی مکان هر کرم شب‌تاب با استفاده از تابع برازش به‌دست‌آمده.

مرحله چهارم: تکرار مرحله‌های دوم و سوم تا دست‌یابی به بیشینه تعداد حلقه‌ها.

۴- پیاده‌سازی روش پیشنهادی

در این پژوهش از تصاویر رنگی JPEG استاندارد در حوزه پردازش تصویر که دارای طیف رنگی غنی (هر سه پایه RGB) هستند، استفاده شده است. از میان تصاویر استاندارد به‌کار رفته در مقاله‌های پنهان‌نگاری از جمله منابع [25] و [26] تصاویر شکل (۴) جهت اعمال الگوریتم‌ها و ارزیابی انتخاب شده‌اند.

شبیه‌سازی‌ها در محیطی با پردازنده Intel® Core™ i7 CPU @2.3 GHz و با حافظه RAM ۶ گیگابایت اجرا شده و سیستم عامل مورد استفاده Windows 7 Ultimate 64Bit است.

الف) بابون ب) لنا ج) فلفل

(شکل-۴): تصاویر استفاده شده در این پژوهش

(Figure-4): Images used in this research

۱-۴- اعمال الگوریتم‌های فراابتکاری به‌صورت جداگانه

در این بخش پارامترها و نتایج اعمال الگوریتم‌های فراابتکاری به‌صورت جداگانه شرح داده شده است.

[DOI: 10.29252/jsdp.17.4.15]

۴-۱-۱- اعمال الگوریتم بهینه‌سازی کلونی مورچه

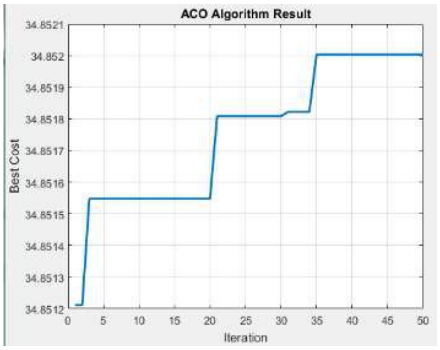
جدول (۲) نشان‌دهنده نحوه تنظیم پارامترها در الگوریتم بهینه‌سازی کلونی مورچه است که مورد استفاده قرار گرفته است.

(جدول-۲): پارامترهای مورد استفاده در الگوریتم بهینه‌سازی کلونی مورچه

(Table-2): Parameters used in ant colony optimization algorithm

پارامتر	توصیف	مقدار
m	تعداد کل مورچه‌ها	6
τ0	مقدار اولیه فرومون	0.5
τ	غلظت فرومون	2
α	وزن غلظت فرومون	1
β	ارزش تجربه	1
η	ارزش تجربه	0.7
T	تعداد سفرهای بازگشت	21
ρ	پارامتر از تبخیر فرومون	0.7
Q0	پارامتر عدد تصادفی	0.2
loop	تعداد تکرار	50

در شکل (۵) نتایج حاصل از اعمال روش ACO بر روی تصویر لنا قابل مشاهده است. همچنین طبق نتایج به‌دست‌آمده در جدول (۹)، در مقایسه روش ACO و LSB، کیفیت تصویر تا حد زیادی توسط روش پیشنهادی بهبود یافته است؛ بنابراین، می‌توان نتیجه گرفت که الگوریتم ACO قادر به پیداکردن یک ماتریس جانشینی خوب مؤثر است.

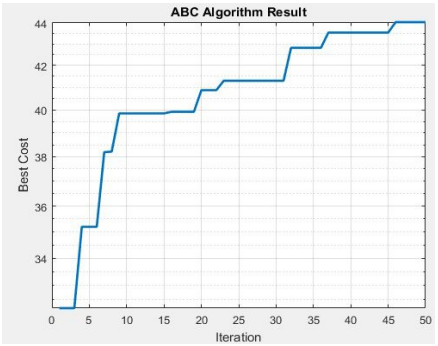


(شکل-۵): نمودار افزایش PSNR در تکرارهای مختلف اجرای الگوریتم ACO در تصویر لنا

(Figure-5): Diagram of PSNR increment in different repetitions of the ACO algorithm in the Lena image

۴-۱-۲- اعمال الگوریتم فراابتکاری زنبور عسل

شکل (۶) نحوه تغییر مقدار PSNR را در اعمال الگوریتم بهینه‌سازی زنبور بر روی تصویر لنا نشان می‌دهد. نتایج تکمیلی در جدول (۹) آمده است. پارامترهای این الگوریتم طبق جدول (۳) تنظیم شده‌اند.



(شکل-۶): نمودار افزایش مقدار PSNR در تکرارهای مختلف اجرای الگوریتم بهینه‌سازی زنبور عسل در تصویر لنا

(Figure-6): Diagram of PSNR increment in different repetitions of the Bee algorithm in the Lena image

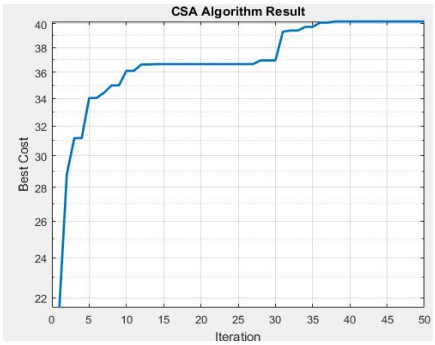
(جدول-۳): پارامترهای مورد استفاده در الگوریتم بهینه‌سازی زنبور عسل

(Table-3): Parameters used in the bee optimization algorithm

پارامتر	توصیف	مقدار
n	تعداد زنبورهای ناظر	20
m	تعداد مکان‌های انتخاب شده از مکان های بازدید شده	10
e	تعداد بهترین مکان‌ها از مکان های انتخاب‌شده	5
nep	تعداد زنبورهای تازه نفس برای بهترین مکان‌ها	6
t	تعداد زنبورهای استخدام شده برای سایر نقاط	4
loop	تعداد تکرار	50

۴-۱-۳- اعمال الگوریتم فرا ابتکاری جستجوی فاخته

شکل (۷) نحوه تغییر مقدار PSNR در اعمال الگوریتم فراابتکاری جستجوی فاخته را بر روی تصویر لنا نشان می‌دهد.



(شکل-۷): نمودار افزایش PSNR در تکرارهای مختلف اجرای الگوریتم بهینه‌سازی جستجوی فاخته در تصویر لنا

(Figure-7): Diagram of PSNR increment in different repetitions of the Cuckoo search optimization algorithm in the Lena image

از آنجا که مسألهٔ مورد بررسی، مسألهٔ پیچیده‌ای است و به‌احتمال نقاط بهینهٔ محلی و عموم متعددی داشته باشد و

[DOI: 10.29252/jsdp.17.4.15]

با توجه به مطالبی که بیان شد، تعداد لانه‌های الگوریتم‌های پیاده‌سازی ۷۵ لانه در نظر گرفته شده است. مقدار پارامتر β که برای محاسبهٔ اندازهٔ گام‌های تصادفی لِوی برابر ۱/۵ فرض شده است. بیشینه تعداد تکرارها به پنجاه تکرار است. پارامترهای این الگوریتم طبق جدول (۴) تنظیم شده‌اند.

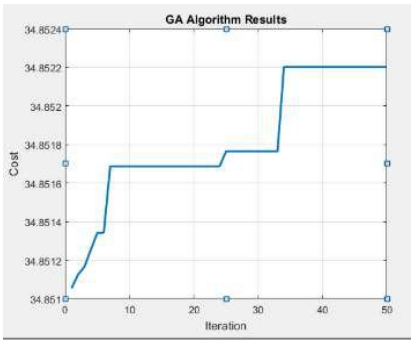
(جدول-۴): پارامترهای مورد استفاده در الگوریتم بهینه‌سازی جستجوی فاخته

(Table-4): Parameters used in Cuckoo Search Optimization Algorithm

پارامتر	توصیف	مقدار
Pa	احتمال شناسایی تخم‌های فاخته	1
a	انتقال لانه به مکان جدید	0.25
n	تعداد لانه ها	75
β	اندازهٔ گام‌های تصادفی	1.5
loop	تعداد تکرار	50

۴-۱-۴- اعمال الگوریتم فراابتکاری ژنتیک

شکل (۸) نحوه تغییر مقدار PSNR را در اعمال الگوریتم فراابتکاری ژنتیک را بر روی تصویر لنا نشان می‌دهد.



(شکل-۸) : نمودار افزایش PSNR در تکرارهای مختلف اجرای الگوریتم بهینه‌سازی ژنتیک در تصویر لنا

(Figure-8): Diagram of PSNR increment in different repetitions of the Genetic algorithm in the Lena image

پارامترهای تنظیم شده در اجرای الگوریتم مذکور، در جدول (۵) درج گردیده است.

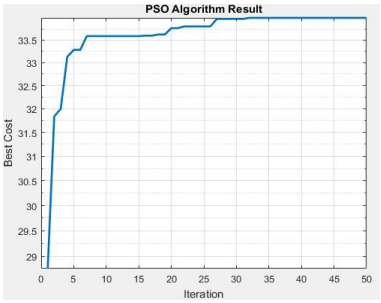
(جدول-۵): پارامترهای مورد استفاده در الگوریتم ژنتیک

(Table-5): Parameters Used in the Genetic Algorithm

پارامتر	توصیف	مقدار
nPop	اندازه جمعیت	100
n_gen	تعداد نسل‌ها	1000
λ	بردار وزن	10(مقدار اولیه)
rp	درصد تقاطع یا CrossOver	0.8
mu	درصد جهش یا Mutation	0.5

۴-۱-۵- اعمال الگوریتم فراابتکاری حرکت ذرات

شکل (۹) نحوه تغییر مقدار PSNR در اعمال الگوریتم فراابتکاری حرکت ذرات را بر روی تصویر لنا نشان می‌دهد. پارامترهای مورد استفاده در الگوریتم بهینه‌سازی حرکت ذرات در جدول (۶) نمایش داده شده است.



(شکل-۹): نمودار افزایش مقدار PSNR در تکرارهای مختلف اجرای الگوریتم بهینه‌سازی حرکت ذرات در تصویر لنا

(Figure-9): Diagram of PSNR increment in different repetitions of the Particle Swarm optimization algorithm in the Lena image

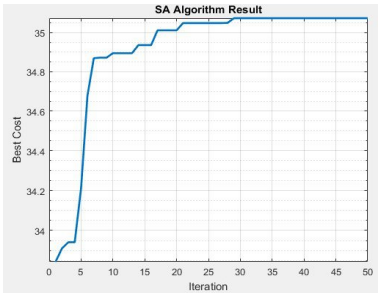
(جدول-۶): پارامترهای مورد استفاده در الگوریتم بهینه‌سازی حرکت ذرات

(Table-6): Parameters used in the Particle Swarm Optimization algorithm

پارامتر	توصیف	مقدار
nVar	تعداد پارامترهای تصمیم‌گیری	1
MaxIt	ماکزیمم تعداد حلقه‌ها	1000
w	وزن اولیه	1
wdamp	ضریب تغییر وزن	0.99
c1	نرخ یادگیری شخصی	1.5
c2	نرخ یادگیری عمومی	2
[Vmin, Vmax]	سرعت کمینه و بیشینه	[-4, 4]

۴-۱-۶- اعمال الگوریتم فراابتکاری تبرید شبیه‌سازی‌شده

شکل (۱۰) نحوه تغییر مقدار PSNR در اعمال الگوریتم فراابتکاری تبرید شبیه‌سازی‌شده را بر روی تصویر لنا نشان می‌دهد.



(شکل-۱۰): نمودار افزایش PSNR در تکرارهای مختلف اجرای الگوریتم تبرید شبیه‌سازی‌شده در تصویر لنا

(Figure-10): Diagram of PSNR increment in different repetitions of the Simulated Annealing algorithm in the Lena image

[DOI: 10.29252/jsdp.17.4.15]

جدول (۷) پارامترهای به‌کاررفته در الگوریتم تبرید شبیه‌سازی‌شده را نشان می‌دهد. نتایج نشان می‌دهد که روش پیشنهادی می‌تواند در بهبود کیفیت تصویر مؤثر باشد.

(جدول-۷): پارامترهای مورد استفاده در الگوریتم تبرید شبیه‌سازی‌شده

(Table-7): Parameters used in Simulated Annealing algorithm

پارامتر	توصیف	مقدار
nPop	اندازه جمعیت	100
nVar	تعداد پارامترهای تصمیم‌گیری	4
MaxIt	ماکزیمم تعداد حلقه‌ها	50
MIPTemp	ماکزیمم تعداد حلقه‌ها به ازای هر دما	2
nMove	تعداد همسایه‌های تولید شده در هر تکرار	2
T0	دمای اولیه	0
RRT	ضریب تغییر دما	0.9
loop	تعداد تکرار	100

۷-۱-۴- اعمال الگوریتم فراابتکاری کرم شب تاب

در این مرحله به اجرای الگوریتم کرم شب‌تاب در مسأله پنهان‌نگاری تصاویر می‌پردازیم. نحوه کار بدین صورت است که پس از تولید جمعیت اولیه، پارامترهای اولیه α و β را که در جدول (۸) به تفسیر آمده است، مقداردهی می‌کنیم.

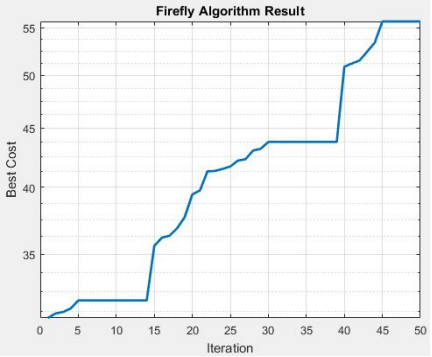
(جدول-۸): پارامترهای مورد استفاده در الگوریتم کرم شب تاب

(Table -8): Parameters used in the firefly algorithm

پارامتر	توصیف	مقدار
n	اندازه جمعیت(تعداد پارامترهای درخواست)	100
MaxIt	بیشینه تعداد حلقه‌ها	50
α	پارامتر تصادفی سازی	0.5
β	میزان جذابیت	0.2
rij	فاصله بین دو کرم i و j	طبق فرمول
I	تغییرات شدت نور	طبق فرمول
λ	ضریب جذب نور	1

هدف ما در این الگوریتم بهینه‌کردن مقدار PSNR در پنهان‌نگاری تصاویر است. شکل (۱۱) نحوه تغییر مقدار PSNR در اعمال الگوریتم فراابتکاری کرم شب‌تاب را بر روی تصویر لنا نشان می‌دهد.

تا زمانی که تعداد تکرارها از حد آستانه کمتر است، برای تمامی جمعیت کرم شب تاب، جمعیت به سمت کرم شب‌تاب با مقدار PSNR بهتر حرکت خواهد کرد. جذابیت هر کرم شب‌تاب به‌صورت معکوس با افزایش میزان فاصله کاهش خواهد یافت؛ بنابراین بر اساس مقادیر جدید برای مکان قرارگیری کرم‌ها، توابع هدف برای جمعیت موجود به‌روزرسانی می‌شود. در انتهای هر حلقه، تمامی کرم‌های شب‌تاب بر اساس تابع هدف PSNR مرتب شده و پاسخ بهینه به‌دست می‌آید. پارامترهای این الگوریتم طبق جدول (۸) تنظیم شده‌اند.



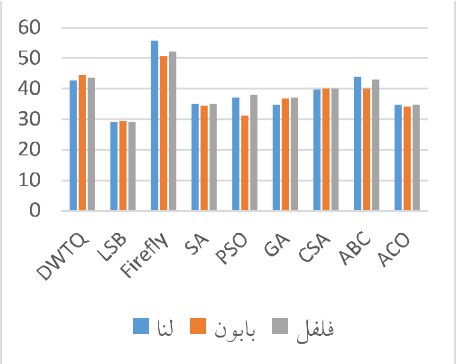
(شکل-۱۱): نمودار افزایش PSNR در تکرارهای مختلف اجرای الگوریتم کرم شب‌تاب در تصویر لنا

(Figure-11): Diagram of PSNR increment in different repetitions of the Firefly algorithm in the Lena image

۲-۴- شناسایی الگوریتم‌های برتر

در این مرحله پس از پیاده‌سازی تمامی روش‌های ابتکاری به‌کاررفته در حوزه پنهان‌نگاری تصاویر، لازم است تا از میان هفت الگوریتم پیاده‌سازی‌شده، سه الگوریتمی را که نتایج بهتری را بر روی داده‌ها نشان داده‌اند، برای مرحله بعدی شبیه‌سازی‌ها شناسایی کنیم. نتایج به‌دست‌آمده از مقایسه PSNR بر روی تصاویر مختلف در الگوریتم‌های مورد بررسی در این مقاله در جدول (۹) نمایش داده شده است.

نمودار شکل (۱۲) به مقایسه PSNR به‌دست‌آمده از اجرای این الگوریتم‌ها می‌پردازد.



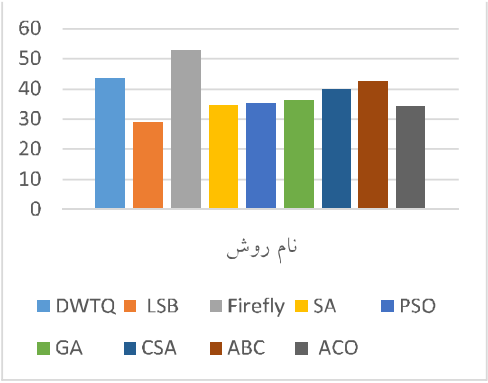
(شکل-۱۲): مقایسه PSNR به‌دست‌آمده از اعمال الگوریتم‌های ابتکاری

(Figure 12): Compar the PSNR obtained by applying the heuristic algorithms

همان‌طورکه در این تصویر نشان داده شده است، الگوریتم کرم شب‌تاب بهترین نتیجه را در میان تمامی الگوریتم‌ها داشته است. به‌منظور شناسایی بهتر الگوریتم‌های

[DOI: 10.29252/jsdp.17.4.15]

تأثیرگذار، میانگین PSNR به‌دست‌آمده بر روی همه تصاویر فلفل، بابون و لنا در شکل (۱۳) آمده است.



(شکل-۱۳): مقایسه میانگین مقدار PSNR بر روی هر سه تصویر مورد بررسی

(Figure-13): Comparison of the mean value of the PSNR on all three images

طبق نتایج به‌دست‌آمده، سه الگوریتم برتر عبارت‌اند از الگوریتم کرم شب‌تاب، الگوریتم فراابتکاری زنبور عسل و الگوریتم فرا ابتکاری جستجوی فاخته.

۳-۴- ترکیب نتایج الگوریتم‌های بهینه

تا اینجا به انتخاب سه الگوریتمی پرداخته شد که دارای بالاترین مقدار PSNR و تابع هدف تعریف‌شده هستند. این سه الگوریتم عبارتند از الگوریتم کرم شب‌تاب، الگوریتم فراابتکاری زنبور عسل و الگوریتم فرا ابتکاری جستجوی فاخته. از آنجایی که از میان روش‌های اعمال‌شده، الگوریتم کرم شب‌تاب بهترین نتیجه را داشته است، زین پس برای مقایسه نتایج به‌دست‌آمده از نتایج الگوریتم کرم شب‌تاب استفاده می‌کنیم.

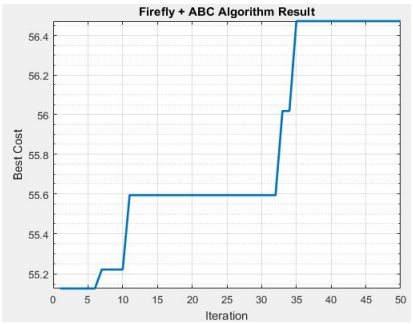
(جدول-۹): نتایج به‌دست‌آمده از مقایسه PSNR بر روی تصاویر مختلف در الگوریتم‌های مورد بررسی در این مقاله

(Table -9): Results obtained from comparison of PSNR on different images in the algorithms studied in this paper.

نام تصویر	ACO	ABC	CSA	GA		PSO	Firefly	SA
لنا	34.58	44.020	39.68	λ=10	34.851	37.06	55.72	35.13
				λ=30	34.19			
بابون	34.25	40.0256	40.15	λ=10	36.92	31.28	50.76	34.35
				λ=30	36.01			
فلفل	34.55	43.022	40.01	λ=10	37.21	38.02	52.159	34.86
				λ=30	36.74			
میانگین	34.46	42.35	39.94	-	35.98	35.45	52.87	34.78

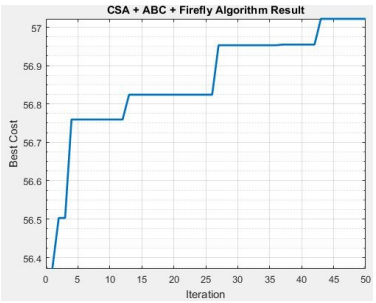
ترکیب شماره ۱: کرم شب‌تاب، زنبور عسل، جستجوی فاخته

طبق ترتیب گفته‌شده، در ابتدا الگوریتم کرم شب‌تاب اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های زنبور عسل و جستجوی فاخته اعمال می‌شوند. در شکل‌های (۱۴ و ۱۵) تأثیرگذاری دو الگوریتم ابتکاری دیگر بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.



(شکل-۱۴): اعمال الگوریتم زنبور عسل بر روی نتایج به‌دست‌آمده الگوریتم کرم شب‌تاب

(Figure-14): Applying the Bee Algorithm on the Results of the Firefly Algorithm



(شکل-۱۵): اعمال الگوریتم جستجوی فاخته بر روی نتایج به‌دست‌آمده الگوریتم زنبور عسل

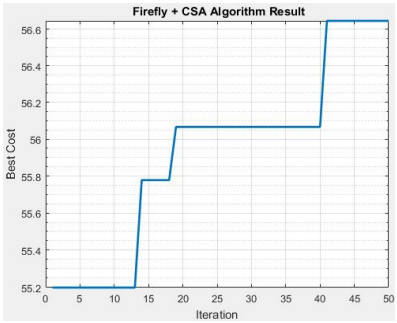
(Figure-15): Applying the Cuckoo Search Algorithm to the Results of the Bee Algorithm

- **ترکیب شماره ۲: کرم شب‌تاب، جستجوی فاخته، زنبور عسل**

طبق ترتیب گفته‌شده، که در ابتدا الگوریتم کرم شب‌تاب اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های جستجوی فاخته و زنبور عسل اعمال می‌شوند.

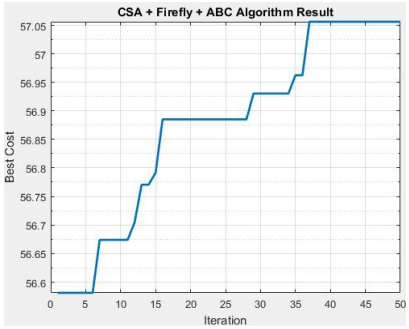
در شکل‌های (۱۶) و (۱۷) نحوه تأثیرگذاری دو الگوریتم ابتکاری دیگر بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.

[DOI: 10.29252/jsdp.17.4.15]



(شکل-۱۶): اعمال الگوریتم جستجوی فاخته بر روی نتایج به‌دست‌آمده الگوریتم کرم شب‌تاب

(Figure-16): Applying the Cuckoo Search Algorithm to the Results of the Firefly Algorithm

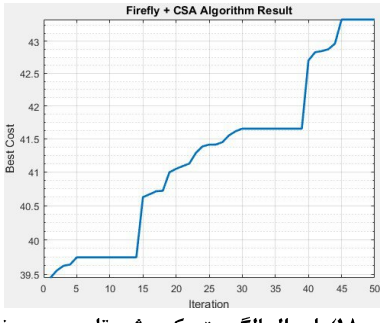


(شکل-۱۷): اعمال الگوریتم زنبور عسل بر روی نتایج به‌دست‌آمده الگوریتم جستجوی فاخته

(Figure-17): Applying the Bee Algorithm on the Results of the Cuckoo Search Algorithm

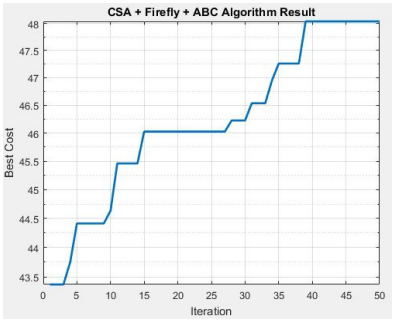
- **ترکیب شماره ۳: جستجوی فاخته، کرم شب‌تاب، زنبور عسل**

طبق ترتیب گفته‌شده، در ابتدا الگوریتم جستجوی فاخته اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های کرم شب‌تاب و زنبور عسل اعمال می‌شوند. در شکل‌های (۱۸) و (۱۹) نحوه تأثیرگذاری دو الگوریتم ابتکاری دیگر بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.



(شکل-۱۸): اعمال الگوریتم کرم شب‌تاب بر روی نتایج به‌دست‌آمده الگوریتم جستجوی فاخته

(Figure-18): Applying the firefly algorithm on the results obtained from the Cuckoo search algorithm

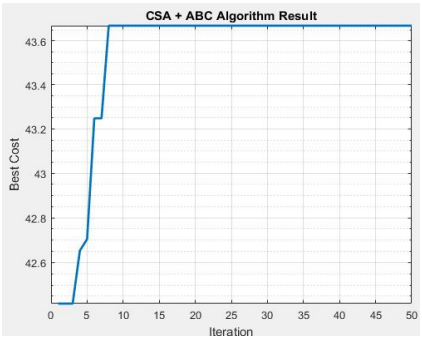


(شکل-۱۹): اعمال الگوریتم زنبور عسل بر روی نتایج به‌دست‌آمده الگوریتم کرم شب‌تاب و جستجوی فاخته در تصویر لنا

(Figure-19): Applying the Bee Algorithm on the Results of the Firefly Algorithm and Cuckoo Search in the Lena Image

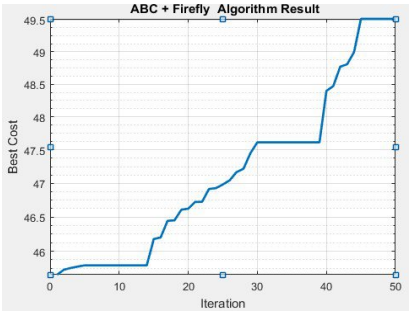
- **ترکیب شماره ۴: جستجوی فاخته، زنبور عسل، کرم شب‌تاب**

طبق ترتیب گفته‌شده، که در ابتدا الگوریتم جستجوی فاخته اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های زنبور عسل و کرم شب‌تاب اعمال می‌شوند. در شکل‌های (۲۰) و (۲۱) نحوه تأثیرگذاری دو الگوریتم ابتکاری دیگر بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.



(شکل-۲۰): اعمال الگوریتم زنبور عسل بر روی نتایج به‌دست‌آمده الگوریتم جستجوی فاخته در تصویر لنا

(Figure-20): Applying the Bee Algorithm on the Results of the Cuckoo Search Algorithm in the Lena Image



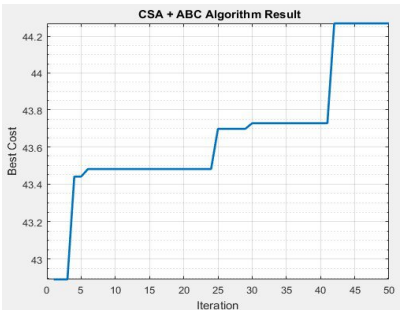
(شکل-۲۱): اعمال الگوریتم کرم شب‌تاب بر روی نتایج به‌دست‌آمده الگوریتم زنبور عسل در تصویر لنا

(Figure-21): Applying the firefly algorithm on the results obtained from the bee algorithm in the Lena image

[DOI: 10.29252/jsdp.17.4.15]

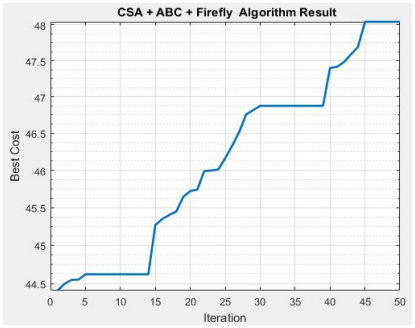
ترکیب شماره ۵: زنبور عسل، جستجوی فاخته، کرم شب‌تاب

طبق ترتیب گفته‌شده، که در ابتدا الگوریتم زنبور عسل اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های جستجوی فاخته و کرم شب‌تاب اعمال می‌شوند. در شکل‌های (۲۲) و (۲۳) نحوه تأثیرگذاری دو الگوریتم ابتکاری دیگر بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.



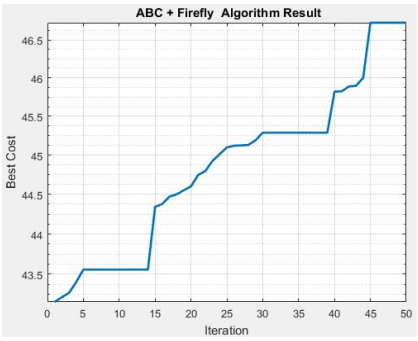
(شکل-۲۲): اعمال الگوریتم فاخته بر روی نتایج به‌دست‌آمده الگوریتم زنبور عسل در تصویر لنا

(Figure-22): Applying the Cuckoo Algorithm to the Results of the Bee Algorithm in the Lena Image



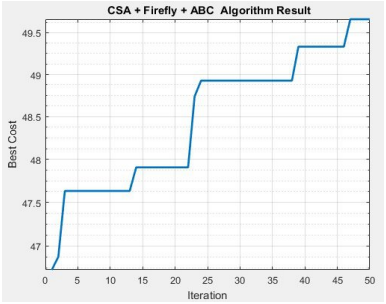
(شکل-۲۳): اعمال الگوریتم کرم شب‌تاب بر روی نتایج به‌دست‌آمده الگوریتم فاخته در تصویر لنا

(Figure-23): Applying the firefly algorithm on the results obtained from the Cuckoo algorithm in the Lena image



(شکل-۲۴): اعمال الگوریتم کرم شب‌تاب بر روی نتایج به‌دست‌آمده الگوریتم زنبور عسل در تصویر لنا

(Figure-24): Applying the firefly algorithm on the results obtained from the Bee algorithm Lena image



(شکل-۲۵): اعمال الگوریتم فاخته بر روی نتایج به‌دست‌آمده الگوریتم کرم شب‌تاب در تصویر لنا

(Figure-25): Applying the Cuckoo Algorithm to the Results of the Firefly Algorithm in the Lena Image

- **ترکیب شماره ۶: زنبور عسل، کرم شب‌تاب، جستجوی فاخته**

طبق ترتیب گفته‌شده، که در ابتدا الگوریتم زنبور عسل اعمال و در مرحله بعدی به‌ترتیب الگوریتم‌های جستجوی فاخته و کرم شب‌تاب اعمال می‌شوند. در شکل‌های (۲۴) و (۲۵) نحوه تأثیرگذاری دو الگوریتم ابتکاری دیگر را بر روی مسأله پنهان‌نگاری تصویر نشان داده شده است.

۵- نتایج و ارزیابی

شکل (۲۶) به مقایسه PSNR به‌دست‌آمده از شش مرحله قبل بر روی تصاویر مختلف می‌پردازد.

(شکل-۲۶): مقایسه مقدار PSNR در شش مرحله تعریف شده

(Figure-26): Compare the PSNR value in the six defined steps

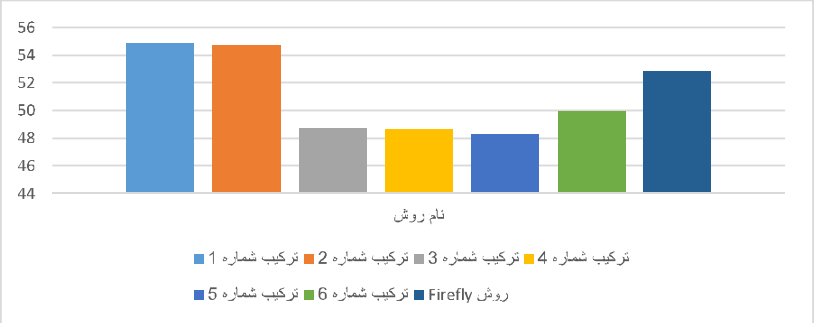
شکل (۲۷) به مقایسه میانگین PSNR به‌دست‌آمده در ترکیب‌های مورد بررسی می‌پردازد. نتایج درج‌شده در جدول (۱۰)، نشان می‌دهد که ترکیب شماره یک که حاصل از ترکیب به‌ترتیب الگوریتم‌های کرم شب‌تاب، زنبور عسل و جستجوی فاخته است، بهترین نتایج را در رسیدن به هدف برنامه ایجاد می‌کنند که این ترکیب، میانگین نسبت سیگنال به نوفه برابر ۵۴/۸۹ را فراهم کرده است.

ترکیب یادشده در مقایسه با الگوریتم‌های انفرادی بررسی‌شدهٔ بهینه‌سازی کلونی مورچه، زنبور عسل، جستجوی فاخته، ژنتیک، حرکت ذرات، تبرید شبیه‌سازی

[DOI: 10.29252/jsdp.17.4.15]

شده، کرم شب‌تاب، به‌ترتیب به میزان ۵۹/۲۹، ۲۹/۶۱، ۳۷/۴۳، ۵۲/۵۶، ۵۴/۸۴، ۵۷/۸۲ و ۳/۸۲ درصد بهبود در مقدار PSNR را ارائه می‌کند.

در جدول (۱۱)، مقدار PSNR پس از اعمال روش پیشنهادی و سایر روش‌های اعمال‌شده بر روی تصویر لنا در پژوهش‌های دیگر مقایسه شده است [32]، [33]، [34]، [35]، [36]. همان‌طور که مشاهده می‌شود، روش پیشنهادی در مقایسه با روش‌های یادشده، بیشترین میزان PSNR را حاصل کرده است.



(شکل-۲۷): مقایسه میانگین PSNR در روش‌های مورد بررسی

(Figure-27): Comparison of the mean PSNR in the investigated methods

(جدول-۱۰): مقدار PSNR پس از اعمال ترکیب‌های مختلف بر روی تصاویر

(Table-10): The amount of PSNR after applying different combinations on the images

نام تصویر	ترکیب شماره ۱	ترکیب شماره ۲	ترکیب شماره ۳	ترکیب شماره ۴	ترکیب شماره ۵	ترکیب شماره ۶	Firefly
لنا	57.12	57.02	48.03	49.5	48.01	49.6	55.72
بابون	53.04	53.1	49.3	49.18	48.1	50.18	50.76
فلفل	54.52	54.23	49.068	49.16	48.9	50.09	52.159
میانگین	54.89	54.78	48.80	49.28	48.34	49.96	52.88

(جدول-۱۱): مقایسه مقدار PSNR پس از اعمال روش‌های مختلف بر روی تصویر لنا در پژوهش‌های مختلف

(Table-11): Compare the amount of PSNR after applying different methods to the Lena image in different research

الگوریتم‌های مختلف	روش پیشنهادی	Wang	Yang	Liao	Mehdi	Zhaotong
میزان PSNR پس از اعمال الگوریتم روی تصویر لنا	57.12	44.1	38.24	41.48	39.09	42.74

۶- نتیجه‌گیری

در این مقاله یک روش مقاوم با درجه امنیتی بالا برای پنهان‌نگاری تصاویر ارائه شد. روش پیشنهادی در رمزنگاری تصاویر به‌منظور بهبود مقدار PSNR و دست‌یابی به ماتریس جایگزینی بهینه از الگوریتم‌های فرا ابتکاری استفاده می‌کند. ابتدا الگوریتم‌های معروف فراابتکاری در رمزنگاری تصاویر مورد استفاده قرار گرفته‌اند و به‌تنهایی بر روی داده‌های موجود اعمال شدند؛ پس از آن الگوریتم‌ها با توجه به بهترین PSNR به‌دست‌آمده مرتب شدند. سه الگوریتمی که بهترین مقدار PSNR را دارند، برای مرحله بعد انتخاب و ترکیب‌های مختلف آن‌ها مورد بررسی قرار گرفت. سه الگوریتم انتخاب‌شده عبارت‌اند از الگوریتم کرم شب‌تاب، الگوریتم جستجوی فاخته و الگوریتم بهینه‌سازی زنبور عسل با میانگین PSNR به‌ترتیب ۵۲/۸۷، ۴۲/۳۵ و ۳۹/۹۴. نتایج نشان می‌دهد که ترکیب شماره یک که حاصل از ترکیب به‌ترتیب الگوریتم‌های کرم شب‌تاب، زنبور عسل و جستجوی فاخته است با مقدار PSNR برابر با ۵۴/۸۹ بهترین نتایج را در رسیدن به پاسخ بهینه در مقایسه با ترکیب‌های شماره ۲، ۳، ۴، ۵، ۶ با میانگین PSNR به‌ترتیب ۵۴/۷۸، ۴۹/۸۰، ۴۹/۲۸، ۴۸/۳۴ و ۴۹/۹۶ فراهم می کند.

[DOI: 10.29252/jsdp.17.4.15]

ترکیب گفته‌شده در مقایسه با الگوریتم‌های انفرادی بررسی‌شده بهینه‌سازی کلونی مورچه، زنبور عسل، جستجوی فاخته، ژنتیک، حرکت ذرات، تبرید شبیه‌سازی‌شده، کرم شب‌تاب ، به‌ترتیب به میزان ۵۹/۲۹، ۲۹/۶۱، ۳۷/۴۳، ۵۲/۵۶، ۵۴/۸۴، ۵۷/۸۲ و ۳/۸۲ درصد بهبود در مقدار PSNR را ارائه می‌کند.

7- References ۷- مراجع

[۱] شمع علیزاده بایی محمدعلی، "بررسی الگوریتم‌های مخفی‌سازی پیام در نهان‌نگاری تصویر و طراحی الگوریتمی کارآمد"، مهندسی شناورهای تندرو، شماره ۵۲، صفحات ۴۲-۳۰، ۱۳۹۷.

[1] M. SH. Alizadeh, "Evaluation of message hiding algorithms in image steganography and efficient algorithm design", *High Speed Craft*, Vol. 52, pp. 42-30, 2018.

[2] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer", *Signal Process. Image Commun.*, vol. 29, no. 8, pp. 902–913, 2014.

[3] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," vol. 54, pp. 113–124, 2013.

[4] A.Benoraira, K. Benmahammed, and N. Boucenna, "Blind image watermarking technique based on differential embedding in DWT and DCT domains," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, pp. 1–11, 2015.

[5] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, 2014.

[6] N. A. Abbas, "Image watermark detection techniques using quadtrees," *Appl. Compute Informatics*, vol. 11, no. 2, pp. 102–115, 2015.

[7] M. Keyvanpour and F. M. Bayat, "Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the {DWT} domain," *Math. Compute. Model*, vol. 58, no. 1–2, pp. 56–67, 2013.

[8] Z. Xie and X. Wang, "A Heuristic Feature Combination Selection Method in Fusion Detection of JPEG Stegoimages," *in 2012 Fourth International Conference on Multimedia Information Networking and Security*, 2012, pp. 220–224.

[9] M. Kiamini, S. Fazli , " A High Performance Steganographic Method using JPEG and PSO Algorithm," IEEE, 2008.

[10] F. Sadeghi, M. K. Rafsanjani, and F. Z. Kermani, "Hiding Information in Image by Compound Meta-Heuristic Algorithm PSO-SA," *Int. J. Compute Sci. Artif. Intell*, vol. 3, no. 4, p. 125, 2013.

[11] K. Akshyata and I. Jain, "Data Hiding and Security using Steganography", *International Journal of Engineering and Management Research*, 2017.

[12] E. T. Zghaer and S. H. Hashem, "Ant Colony Optimization To Enhance Image Steganography", *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, 2017.

[13] A. Miri, K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm", *Optik*, vol. 145, pp.158-168.

[14] K. Loukhaoukha, J.-Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *J. Inf. Hiding Multimed. Signal Process.*, vol. 2, no. 4, pp. 303–319, 2011.

[15] J. S. Lee, J.-W. Wang, and K.-Y. Giang, "A new image watermarking scheme using multi-objective bees algorithm," *Appl. Math. Inf. Sci.*, vol. 8, no. 6, p. 2945, 2014.

[16] F. G. Mohammadi and M. S. Abadeh, "Image steganalysis using a bee colony based feature selection algorithm," Eng. Appl. Artif. Intell., vol. 31, pp. 35–43, 2014.

[17] M. Ali and C. W. Ahn, "An optimal image watermarking approach through cuckoo search algorithm in wavelet domain," Int. J. Syst. Assur. Eng. Manag., pp. 1–10, 2014.

[18] Y. H. Chen and H. C. Huang, "Reversible Image Watermarking Based on Genetic Algorithm," *in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, 2014, pp. 21–24.

[19] a L. Brazil, a Sanchez, a Conci, and N. Behlilovic, "Hybridizing genetic algorithms and path relinking for steganography," ELMAR 2011 Proc., no. September, pp. 285–288, 2011.

[20] M. Nosrati, A. Hanani, and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm," *in 2015 Fifth International Conference on Advanced Computing Communication Technologies*, 2015, pp. 102–107.

[21] B. Lei, F. Zhou, E.-L. Tan, D. Ni, H. Lei, S. Chen, and T. Wang, "Optimal and secure audio watermarking scheme based on self-adaptive particle swarm optimization and quaternion wavelet transform," *Signal Processing*, vol. 113, pp. 80–94, 2015.

[DOI: 10.29252/jsdp.17.4.15]

[22] X. Li and J. Wang, "A steganographic method based upon {JPEG} and particle swarm optimization algorithm," Inf. Sci. (Ny)., vol. 177, no. 15, pp. 3099–3109, 2007.

[23] G. S. Lin, Y. T. Chang, and W. N. Lie, "A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm," *IEEE Trans. Multimed.*, vol. 12, no. 5, pp. 345–357, Aug. 2010.

[24] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT--SVD and Firefly Algorithm," Expert Syst. Appl., vol. 41, no. 17, pp. 7858–7867, 2014.

[25] A. Miri, K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm", Optik, vol. 145, pp.158-168.

[26] S. Hemalatha, U. D. Acharya, and A. Renuka, "Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image," *Procedia Comput. Sci.*, vol. 47, pp. 272–281, 2015.

[27] M. Nosrati, A. Hanani, and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm," *in 2015 Fifth International Conference on Advanced Computing Communication Technologies*, 2015, pp. 102–107.

[28] Z. Li, Y. Hi, "Steganography with pixel-value differencing and modulus function based on PSO," *Information Security and Applications*, vol.43, pp. 47-52, 2018.

[29] F. G. Mohammadi , H. sajedi, "Region based Image Steganalysis using Artificial Bee Colony," *Visual Communication and Image Representation*, vol 14, pp. 214-226, 2017.

[30] S.I. Nipanikar, V. H. Deepthi, N. Kulkarni, "A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform," *Alexandria Engineering*, vol. 57, pp. 2343-2356, 2018.

[31] A. Miri, k. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," Optik, vol. 145, pp. 158-168, 2017.

[32] CM.Wang, NI. Wu, CS. Tsai, "A high quality steganographic method with pixel-value differencing and modulus function", J Syst Softw, Vol. 81, pp.150-158, 2008.

[33] CH. Yang, SJ. Wang, C. Weng, "Capacity-raising steganography using multi- -pixel differencing and pixel-value shifting operations", *Fundam Informaticae*, Vol. 98, pp.321-336, 2010.

[34] X. Liao, QY. Wen, ZL. Zhao, "A novel steganographic method with four-pixel differencing and modulus function", *Fundam Informaticae*, Vol. 118, pp. 281-289, 2012.

[35] M. Hussain, AWA. Wahab, ATS. Ho, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement", *Signal Pro- cess Image Commun*, Vol. 50, pp.44-57, 2017.

[36] Li. Zhaotong, He.Ying, "Steganography with pixel-value differencing and modulus function based on PSO", *Journal of Information Security and Applications*, vol. 43, pp. 47-52, 2018.

لادن ریاضی عضو هیأت علمی و استادیار دانشگاه آزاد اسلامی، مدرک کارشناسی خود را در رشته مهندسی رایانه گرایش نرم‌افزار در سال ۱۳۷۹ و مدرک کارشناسی ارشد خود را در رشته مهندسی رایانه گرایش هوش مصنوعی و رباتیک در سال ۱۳۸۲ و مدرک دکترای خود را در رشته مدیریت فناوری اطلاعات گرایش کسب و کار هوشمند در سال ۱۳۹۸ از دانشگاه آزاد اسلامی دریافت کرده‌اند. زمینه‌های پژوهشی مورد علاقه ایشان پردازش تصویر، هوش تجاری، سامانه‌های اطلاعات مدیریتی و آموزش الکترونیکی است.

نشانی رایانامه ایشان عبارت است از:

l_riazi@iauec.ac.ir

علیرضا پورابراهیمی عضو هیأت علمی و استادیار دانشگاه آزاد اسلامی، در سال ۱۳۸۶ مدرک دکترای خود را در رشته مدیریت صنعتی از دانشگاه آزاد اسلامی دریافت کرده است. وی از سال ۱۳۷۴ تا کنون به امر تدریس در دانشگاه‌های کشور اشتغال داشته‌اند و دارای تألیفات و پژوهش‌های متعدد علمی بوده‌اند. زمینه‌های پژوهشی مورد علاقه ایشان امنیت، الگوریتم‌های فراابتکاری و داده‌کاوی است.

نشانی رایانامه ایشان عبارت است از:

poorebrahimi@gmail.com

محمود البرزی عضو هیأت علمی و دانشیار دانشگاه آزاد اسلامی، در سال ۱۳۷۵ مدرک دکترای خود را در رشته مهندسی رایانه از دانشگاه برونل انگلستان دریافت کرده است. موضوعات پژوهشی

[DOI: 10.29252/jsdp.17.4.15]

مورد علاقه ایشان، هوش مصنوعی – شبکه‌های عصبی، شبیه‌سازی، روش‌های کمی و سامانه‌های اطلاعات مدیریت پیشرفته است.

نشانی رایانامه ایشان عبارت است از:
mahmood_alborzi@yahoo.com

رضا رادفر عضو هیأت علمی و استاد دانشگاه آزاد اسلامی، مدرک کارشناسی خود را در سال ۱۳۷۵ در رشته مدیریت صنعتی و کارشناسی ارشد خود را در سال ۱۳۷۸ در رشته مدیریت صنعتی گرایش تولید و عملیات و دکترای خود را در سال ۱۳۸۳ در رشته مدیریت صنعتی گرایش سامانه‌ها از دانشگاه آزاد اسلامی دریافت کرده‌اند. موضوعات پژوهشی مورد علاقه ایشان الگوریتم‌های ژنتیک، مدیریت فناوری و نوآوری، شبکه‌های عصبی است.

نشانی رایانامه ایشان عبارت است از:
r.radfar@srbiau.ac.ir

[DOI: 10.29252/jsdp.17.4.15]