ارائه روشی نوین برای تولید دنباله بازگشتی در رمزنگاری تصویر با استفاده از الگوریتم ژنتیک

زهره طالبی نوش‌آباد[۱] و علی‌محمد لطیف[۲]

۱- کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر- دانشگاه یزد- یزد- ایران

z.talebi@stu.yazd.ac.ir

۲-استادیار، دانشکده مهندسی برق و کامپیوتر- دانشگاه یزد- یزد- ایران

alatif@yazd.ac.ir

چکیده: تصویر دیجیتال به علت ماهیت خاص خود دارای الگوریتم‌های رمزنگاری ویژه است. در اکثر روش‌های رمزنگاری تصویر، از یک دنباله ریاضی برای درهم‌ریزی تصویر استفاده می‌شود. دنباله‌های ریاضی استفاده شده تاکنون، یک رابطه ریاضی بازگشتی است که دارای یک مجموعه ضرایب هستند. با تغییر ضرایب تولید دنباله ریاضی، دنباله‌های مختلفی را می‌توان تولید کرد. برای ارزیابی الگوریتم، پس از رمزنگاری تصویر میزان درهم‌ریزی تصویر با معیارهای استانداردی محاسبه می‌شود. به علت پیچیدگی سیستم رمزنگاری تصویر و عدم رابطه مشخص بین ضرایب دنباله و معیارهای ارزیابی، انتخاب ضرایب مناسب دنباله برای رمزنگاری تصویر به آسانی امکان‌پذیر نیست. در این مقاله ضرایب رابطه بازگشتی توسط الگوریتم ژنتیک با در نظر گرفتن یک فرم عمومی برای رابطه بازگشتی و تعریف تابع برازندگی مناسب محاسبه می‌شوند؛ به گونه‌ای که دنباله یافته شده کارایی مطلوبی برای رمزنگاری تصویر داشته باشد. آزمایش‌ها نشان می‌دهد دنباله به دست آمده از الگوریتم ژنتیک نسبت به ضرایب تعدادی از روش‌ها نتایج رضایت‌بخش‌تری از خود نشان می‌دهد.

واژه‌های کلیدی: الگوریتم ژنتیک، درهم‌ریزی تصویر، رمزنگاری تصویر

۱- مقدمه

در سال‌های اخیر با گسترش فراوان استفاده از پست الکترونیک، ویدئو کنفرانس و پیام‌های چندرسانه‌ای روزانه اطلاعات خصوصی و عمومی افراد از طریق اینترنت انتقال می‌یابد. همچنین، توسعه شبکه‌های کامپیوتری و سرویس‌های چندرسانه‌ای دیجیتال باعث انتقال فراگیر تصاویر، ویدئو و داده‌های چندرسانه‌ای شده است.

با توجه به گستردگی سیستم‌های کاوش بصری[۱] در نقاط مهم مثل فرودگاه‌ها، مراکز تجاری، بانک‌ها، مدارس و مکان‌های استراتژیک نظامی، ویدئوها و تصاویر با رعایت نکات امنیتی تولید و پس از انتقال در مقصد ذخیره می‌شوند. بنابراین، فراهم کردن امنیت برای داده‌های چندرسانه‌ای برای اشخاص، شرکت‌ها و دولت‌ها یک نیاز حساس و ضروری است [۱].

رمزنگاری روشی مؤثر برای حفاظت از داده‌های چندرسانه‌ای است که این عمل با انتقال داده‌های چندرسانه‌ای به صورت یک قالب غیر قابل تشخیص در بستر شبکه انجام می‌شود. بدیهی است رمزنگاری داده‌های چندرسانه‌ای به صورتی انجام می‌شود که کاربران غیرمجاز از محتوای اصلی داده رمزشده اطلاعاتی به دست نیاورند.

با توجه به حجم بالای داده تصویری و ویدئویی و هم چنین ویژگی‌های خاص تصویر، استفاده از الگوریتم‌های کلاسیک رمزنگاری، مانند RSA[۲] و DES[۳] در رمزنگاری

---

[۱] تاریخ ارسال مقاله : ۱۳۹۱/۱۲/۲۵

تاریخ پذیرش مقاله : ۱۳۹۲/۱۲/۱۲

نام نویسنده مسؤول : زهره طالبی نوش‌آباد

نشانی نویسنده مسؤول : ایران – یزد – دانشگاه یزد – دانشکده مهندسی برق و کامپیوتر

تصویر ناکارآمد است؛ زیرا این الگوریتم‌ها وقت‌گیر بوده و در سیستم‌های بلادرنگ قابل استفاده نیستند [۲, ۳]. بنابراین برای داده تصویری روش‌های رمزنگاری ویژه با عنوان رمزنگاری تصویر[۴] توسعه داده شده است.

رمزنگاری تصویر با دو تکنیک جایگزینی[۵] و درهم‌ریزی[۶] انجام می‌شود. در تکنیک جایگزینی پیکسل‌های تصویر توسط محاسبات ریاضی با مقادیر برگشت‌پذیر دیگری جایگزین می‌شوند؛ ولی در تکنیک درهم‌ریزی، مکان پیکسل‌های تصویر با استفاده از روابط ریاضی عوض می‌شود [۴].

باید دقت نمود در رمزنگاری تصویر جابه‌جایی پیکسل‌ها باید به گونه‌ای انجام شود که تصویر رمزشده به کاربر غیرمجاز هیچ‌گونه اطلاعاتی از تصویر اصلی ندهد. درهم‌ریزی تصویر یکی از روش‌های رایج و مناسب رمزنگاری برای انتقال ایمن تصویر است. همچنین درهم‌ریزی تصویر به عنوان یک پیش‌پردازش برای واترمارکینگ و پنهان کردن تصویر نیز استفاده می‌شود [۵].

درهم‌ریزی تصویر در دو حوزه مکان[۷] و فرکانس[۸] انجام می‌شود. درهم‌ریزی در حوزه مکان با جابه‌جایی مستقیم سطوح روشنایی پیکسل‌های تصویر اصلی انجام می‌شود. برای درهم‌ریزی تصویر در حوزه فرکانس، ابتدا تصویر با یک تبدیل مناسب به حوزه فرکانس انتقال داده می‌شود و سپس تابع رمز روی تبدیل تصویر اعمال می‌شود. در پایان با محاسبه معکوس تبدیل، تصویر به حوزه مکان انتقال داده می‌شود [۶].

در سال‌های اخیر روش‌های متعددی برای درهم‌ریزی تصویر ارائه شده است که در بین این الگوریتم‌ها، روش‌های مبتنی بر آشوب کارایی خوبی از خود نشان داده‌اند. سیستم‌های آشوبگون رفتار پویای غیرخطی دارند. این سیستم‌ها شبه‌تصادفی و غیرهمگرا هستند و نسبت به وضعیت اولیه حساسیت دارند. نتیجه طبیعی حساسیت نسبت به وضعیت اولیه، ویژگی پخش‌شدگی[۹] است که در رمزنگاری تصویر مناسب است [۶]. همچنین، به علت فضای مناسب کلید رمز، سیستم‌های آشوبگون در برابر حمله جست‌وجوی جامع مقاوم هستند [۲]. شایان ذکر است که از سیستم‌های آشوب علاوه بر رمزنگاری در ارتباطات،برای بهینه‌سازی، کنترل و پردازش تصویر نیز استفاده می‌شود [۷].

در سال ۱۹۸۹ میلادی، Matthews سیستم پویای گسسته آشوبگون را برای رمزنگاری تصویر ارائه کرد [۸]. او برای تولید یک دنباله اعداد شبه‌تصادفی از نگاشت یک‌بعدی آشوبگون استفاده کرد. در سال ۱۹۹۴ میلادی، Biance از سیستم آشوبگون لجستیک[۱۰] برای رمزنگاری تصویر استفاده کرد که به امنیت مناسبی دست یافت [۸].

در سال ۲۰۰۶ میلادی، Gu و همکارش از دنباله آشوبگون دوبعدی برای رمزنگاری تصویر استفاده کردند [۶]. در سال ۲۰۰۷ میلادی، Hong و همکارانش از دنباله آشوبگون Lu برای رمزنگاری تصویر بهره بردند [۹]. الگوریتم آنها دارای فضای کلید بزرگ و در برابر حمله‌های آماری و خرابی‌ها مقاوم بود.

در سال ۲۰۰۹ میلادی، Yanling از دنباله آشوبگون برای رمزنگاری تصویر استفاده کرد [۱۰]. الگوریتم رمزنگاری وی آسان بود و امنیت و درهم‌ریزی خوبی داشت. در سال ۲۰۱۰ میلادی، Wang و همکارانش از سیستم فوق‌آشوبی[۱۱] برای رمزنگاری تصویر استفاده کردند که الگوریتم کارایی و بازده امنیتی مناسبی داشت [۸].

در تمام مراجع مطرح شده برای رمزنگاری تصویر از دنباله‌های زمانی در ریاضیات استفاده و در پایان کارایی الگوریتم‌های ارائه شده توسط معیارهای استاندارد سنجش تشابه ارزیابی شده است.

در رمزنگاری تصویر به علت پیچیدگی موجود، انتخاب نوع دنباله و مقادیر اولیه برای داشتن معیارهای مناسب به صورت تحلیلی امکان‌پذیر نیست. در این مقاله، با استفاده از الگوریتم ژنتیک[۱۲] یک دنباله مناسب برای رمزنگاری تصویر ارائه می‌شود.

برای یافتن دنباله، ابتدا یک فرم کلی رابطه بازگشتی در

نظر گرفته می‌شود و با استفاده از الگوریتم ژنتیک ضرایب مناسبی برای این رابطه محاسبه می‌شود. توسط روش پیشنهادی با تعریف یک تابع برازندگی[۱۳] مناسب، معیارهای مهم رمزنگاری تصویر در حد مطلوب و به طور همزمان برآورده می‌شوند.

ساختار مقاله به فرم زیر است: در بخش دوم دنباله زمانی دوبعدی معرفی می‌گردد؛ در بخش سوم الگوریتم ژنتیک معرفی می‌شود و در قسمت چهارم روش پیشنهادی بیان می‌شود. نتایج آزمایش‌ها و نتیجه‌گیری‌های لازم نیز در بخش پایانی ارائه می‌شود.

۲- دنباله زمانی دوبعدی

فرم کلی یک دنباله زمانی دوبعدی به صورت رابطه‌های ۱ و ۲ تعریف می‌شود:

$$x_{n+1} = a_1 + a_2 x_n + a_3 {x_n}^2 + a_4 y_n + a_5 {y_n}^2 + a_6 x_n y_n \quad (۱)$$

$$y_{n+1} = a_7 + a_8 x_n + a_9 {x_n}^2 + a_{10} y_n + a_{11} {y_n}^2 + a_{12} x_n y_n \quad (۲)$$

در این روابط مقدار دنباله در هر لحظه وابسته به مقادیر لحظه قبل است و اثرهای درجه اول و دوم و عامل غیرخطی ضرب دو مؤلفه در نظر گرفته می‌شوند. در این دنباله با مشخص بودن ضرایب دنباله و مقادیر اولیه x_0 و y_0 می‌توان سایر مقادیر تصادفی را تولید کرد.

بدیهی است با انتخاب a_2 در بازه $[0,4]$ و $a_3 = -a_2$، این دنباله به دنباله لجستیک تبدیل می‌شود [۱۱] و با انتخاب $a_4 = 1.55$، $a_5 = -1.3$، $a_8 = -1.1$ و $a_{10} = 0.1$، این دنباله به دنباله فوق آشوبی دو بعدی تبدیل می‌شود [۶].

۳- الگوریتم ژنتیک

ایده اصلی الگوریتم ژنتیک از نظریه تکاملی داروین گرفته شده است. نظریه داروین به این شرح است که آن دسته از صفات طبیعی که با قوانین طبیعی سازگاری بیشتری دارند، شانس بقای بیشتری دارند. شایان ذکر است که نظریه تکاملی داروین هیچ اثبات تحلیلی و قطعی ندارد؛ اما از نظر تجربی و آماری تأیید شده است.

افراد جدید یک جامعه از طریق زاد و ولد تولید می‌شوند. شانس بقای یک فرد در نسل جدید به ترکیب خاص کروموزومی وابسته است. در مراحل زاد و ولد ممکن است جهش‌هایی در خصوصیات یک فرد نسل جدید رخ دهد که در نتیجه موجودی با خصوصیات عالی و سازگاری بالا تولید شود. در روند زاد و ولد به گونه‌های برتر در هر نسل اجازه تولید مثل داده می‌شود و گونه‌های نامطلوب به تدریج از بین خواهند رفت و افراد نسل‌های جدید با گذشت زمان تکامل می‌یابند.

الگوریتم ژنتیک در سال ۱۹۷۰ میلادی توسط جان هلند[۱۴] ارائه شد. این الگوریتم در گروه الگوریتم‌های بهینه‌سازی تصادفی قرار دارد و برای بهینه‌سازی مسائل پیچیده با فضای جست‌وجوی ناشناخته مناسب است [۱۲]. الگوریتم ژنتیک در زیر به صورت خلاصه بیان شده است.

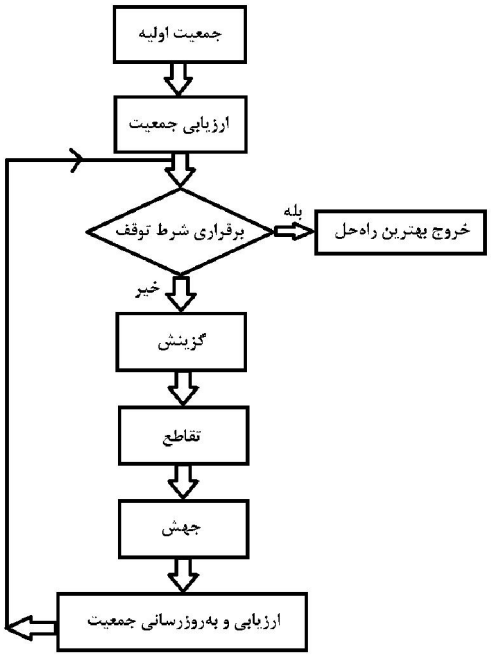
۱- در شروع الگوریتم مجموعه‌ای تصادفی از کاندیداهای جواب که جمعیت اولیه نامیده می‌شوند، تولید و در هر نسل با کاندیداهای جدیدی جایگزین می‌شوند.

۲- در هر تکرار الگوریتم جمعیت توسط تابع برازندگی ارزیابی می‌شود. سپس تعدادی از بهترین کاندیداها برای نسل بعد گزینش می‌شوند و جمعیت جدید را تشکیل می‌دهند.

۳- تعدادی از این جمعیت با استفاده از اپراتورهای ژنتیکی نظیر تقاطع[۱۵] و جهش[۱۶] برای تولید فرزندان جدید استفاده می‌شوند.

۴- مراحل فوق تا رسیدن به یک پاسخ مناسب ادامه می‌یابد.

مراحل مطرح شده برای اجرای الگوریتم ژنتیک در قالب یک روندنما در شکل ۱ مشاهده می‌شود.



شکل (۱): روندنمای الگوریتم ژنتیک

۴- روش پیشنهادی

روش پیشنهادی در این مقاله از دو بخش الگوریتم ژنتیک برای یافتن دنباله مناسب و الگوریتم درهم‌ریزی تصویر تشکیل شده است. ابتدا ضرایب دنباله زمانی دوبعدی محاسبه و سپس ضرایب به دست آمده برای درهم‌ریزی تصویر استفاده می‌شوند.

در این قسمت برخی از واژگان الگوریتم ژنتیک و تخصیص آنها به پارامترهای مسأله بیان می‌شود. به عناصر سازنده یک کروموزوم ژن گفته می‌شود که در این مسأله هر کدام از ضرایب دنباله زمانی دوبعدی یک ژن نامیده می‌شوند.

در الگوریتم ژنتیک به مجموعه‌ای از ژن‌ها کروموزوم گفته می‌شود که در روش پیشنهادی دوازده ضریب دنباله زمانی دو بعدی یک کروموزوم در نظر گرفته می‌شود. هر ژن کروموزوم در رابطه عمومی تولید دنباله زمانی دوبعدی جایگزین می‌شود و سپس دنباله دوبعدی تولید می‌شود. درهم‌ریزی تصویر با استفاده از این دنباله انجام و برازندگی با استفاده از رابطه ۳ محاسبه می‌شود.

$$Fitness\_Function = \alpha_1 UACI + \alpha_2 NPCR + \alpha_3 MAE + \alpha_4 r_{xy}(horizontal) + \alpha_5 r_{xy}(vertical) + \alpha_6 r_{xy}(diameter) \quad (۳)$$

در این رابطه برای اندازه‌گیری برازندگی از توابع همبستگی، UACI[۱۷]، NPCR[۱۸] و MAE[۱۹] استفاده شده است. بدیهی است توابع ذکر شده، توابع استاندارد برای محاسبه میزان تشابه دو تصویر هستند [۱۳]. هر چه مقدار *UACI*، *NPCR* و *MAE* بیشتر باشد، الگوریتم رمزنگاری عملکرد مطلوبتری دارد.

پیکسل‌های تصویر که در همسایگی هم قرار دارند، دارای همبستگی خاصی هستند. با اجرای درهم‌ریزی تصویر پیسکل‌هایی که در کنار هم قرار می‌گیرند، از قسمت‌های مختلف تصویر هستند و در این حالت میزان همبستگی پیکسل‌های همسایه به شدت کاهش می‌یابد. بنابراین، در رابطه برازندگی پیشنهادی عامل همبستگی هر چه کم‌تر باشد، عملکرد الگوریتم مطلوب‌تر است.

با توجه به این که چهار معیار در یک محدوده قرار ندارند، برای نگاشت معیارها در یک بازه از ضرایب استفاده شده است. این ضرایب می‌توانند با توجه به اهمیت هر معیار توسط کاربر افزایش یا کاهش یابند.

معیار همبستگی در رابطه چهار بیان شده است.شایان ذکر است در تابع برازندگی معیار همبستگی در سه راستای افقی، عمودی و قطری به صورت جداگانه استفاده می‌شود [۱۳].

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (۴)$$

$$Cov(x,y) = \frac{1}{M\times N} \times \sum_{j=1}^{M\times N}((x_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}x_j)(y_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}y_j)) \quad (۵)$$

$$D(x) = \frac{1}{M\times N}\sum_{j=1}^{M\times N}(x_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}x_j)^2 \quad (۶)$$

$$D(y) = \frac{1}{M\times N}\sum_{j=1}^{M\times N}(y_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}y_j)^2 \quad (۷)$$

در این روابط x و y روشنایی دو پیکسل همسایه در تصویر و $M \times N$ تعداد پیکسل‌های تصویر است.

رابطه ۸ مربوط به محاسبه MAE است که متوسط خطای مطلق است [۱۴].

$$MAE=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|C(i,j)-P(i,j)| \qquad (۸)$$

در این رابطه $C(i,j)$ و $P(i,j)$ به ترتیب مقادیر پیکسل‌های تصویر رمز و تصویر اصلی هستند.

رابطه ۹ مربوط به محاسبه $NPCR$ است که نرخ پیکسل‌های تغییریافته تصویر رمز به ازای یک بیت تغییر در تصویر اصلی است [۱۵].

$$NPCR=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}D(i,j)}{M\times N}\times 100\% \qquad (۹)$$

$$D(i,j)=\begin{cases}0 & if \quad C(i,j)=\overline{C}(i,j)\\ 1 & if \quad C(i,j)\neq\overline{C}(i,j)\end{cases} \qquad (۱۰)$$

در این رابطه, C $\overline{C}$ دو تصویر رمز هستند که تصاویر اصلی متناظرشان در یک پیکسل متفاوتند.

نحوه محاسبه $UACI$ در رابطه ۱۱ نشان داده شده است [۱۵].

$$UACI=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\frac{|C(i,j)-\overline{C}(i,j)|}{255}\right]\times 100\% \qquad (۱۱)$$

۴-۱- الگوریتم درهم‌ریزی تصویر

همان‌گونه که در قسمت قبل ذکر گردید، برای رمزنگاری تصویر با تکنیک درهم‌ریزی تصویر مکان پیکسل‌های تصویر تعویض می‌گردد.

در این مقاله درهم‌ریزی پیکسل‌های یک سطر (ستون) توسط سطر (ستون) دیگر تصویر انجام می‌شود [۶]. سطری (ستونی) که برای درهم‌ریزی به کار برده می‌شود با استفاده از دنباله زمانی دوبعدی انتخاب می‌شود.

الگوریتم درهم‌ریزی به صورت زیر است: فرض کنید A و B دو بردار باشند و قرار است بردار B توسط بردار A درهم ریخته شود. ابتدا بردار A به ترتیب صعودی مرتب می‌شود و بردار A' به دست می‌آید. سپس هر درایه بردار B به مکانی انتقال داده می‌شود که درایه بردار A' در آن مکان در بردار A قرار داشته است.

برای بیان واضح‌تر، درهم‌ریزی مورد نظر با استفاده از یک مثال توضیح داده می‌شود. در مثال زیر بردار B با شش عنصر توسط بردار A درهم ریخته می‌شود.

A = (0.53, 0.99, 0.03, 0.42, 0.12, 0.97)
A' = (0.03, 0.12, 0.42, 0.53, 0.97, 0.99)
P = (3 5 4 1 6 2)
B = (0.35, 0.91, 0.31, 0.85, 0.49, 0.99)
B' = (0.85, 0.99, 0.35, 0.31, 0.91, 0.49)

بردار P مکان اصلی درایه‌های بردار A' در بردار A است؛ و بردار B' درهم ریخته شده بردار B است.

۴-۲- الگوریتم تولید دنباله و درهم‌ریزی تصویر

در هر مرحله از اجرای الگوریتم ژنتیک با استفاده از ژن‌های کروموزوم‌ها یک دنباله زمانی دوبعدی تولید می‌شود و این دنباله برای درهم‌ریزی تصویر استفاده می‌شود. الگوریتم پیشنهادی به صورت مرحله به مرحله در قسمت زیر بیان شده است.

۱- یک سیستم آشوبگون دوبعدی و مقادیر اولیه (x_0, y_0) انتخاب می‌شوند که این مقادیر اولیه به عنوان کلید الگوریتم رمزنگاری استفاده می‌شوند.

۲- در این الگوریتم، ابتدا تصویر سطر به سطر و سپس ستون به ستون درهم ریخته می‌شود. پس از تولید زوج (x_1, y_1) مقدار x_1 به فاصله $0 \le x_1' < M$ و مقدار y_1 به فاصله $0 \le y_1' < N$ نگاشت می‌شود. شایان ذکر است اگر مقدار x_1' برابر با یک باشد (برابر با سطری که اکنون باید درهم ریخته شود)، یا y_1' برابر با یک باشد (برابر با ستونی که اکنون باید درهم ریخته شود)، زوج (x_1, y_1) حذف و محاسبه زوج بعدی دنباله تکرار می‌شود. سپس با استفاده از الگوریتم مطرح شده از x_1' امین سطر برای درهم‌ریزی اولین سطر و از y_1' امین ستون برای درهم‌ریزی اولین ستون استفاده می‌شود.

۳- زوج‌های بعدی دنباله مشابه مرحله قبل تولید و برای درهم‌ریزی سطر و ستون‌های بعدی استفاده می‌شوند.

شایان ذکر است می‌توان الگوریتم بیان شده را برای

درهم‌ریزی بیشتر تصویر تکرار کرد. برای انجام چنین عملی باید دنباله مورد نظر را به تعداد مورد نظر تولید کرد. الگوریتم هنگام رسیدن به سطر و ستون آخر تصویر مجددا از ابتدای تصویر تکرار می‌گردد.

پس از اجرای مراحل فوق تصویر رمز شده به دست می‌آید. تصویر رمز شده از فرستنده به گیرنده ارسال می‌شود. گیرنده تصویر رمز شده را دریافت می‌کند و برای استفاده از آن باید تصویر اصلی را بازیابی کند. بازیابی تصویر اصلی از تصویر رمز، معکوس فرایند درهم‌ریزی است؛ با این تفاوت که دنباله آشوبگون باید در جهت معکوس استفاده شود.

برای بازسازی تصویر اصلی از تصویر رمز، مراحل زیر انجام می‌شود:

۱- ابتدا دنباله آشوبگون به تعداد لازم تولید می‌شود؛ به گونه‌ای که شرایط دنباله را مانند مرحله رمزنگاری دارا باشد.

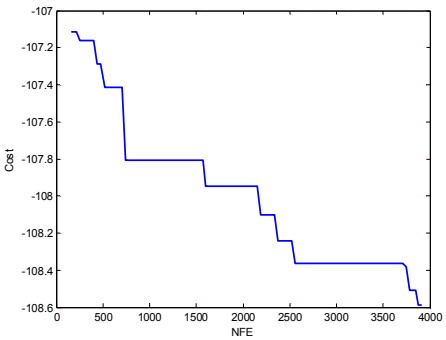
۲- دنباله از آخر به اول استفاده می‌شود؛ به عبارتی، زوج آخر برای درهم‌ریزی سطر و ستون آخر تصویر استفاده می‌شود؛ به طوری که ابتدا ستون آخر و سپس سطر آخر به حالت اول خود برمی‌گردند. این کار تا برگرداندن تمام پیکسل‌های تصویر به حالت اول خود ادامه می‌یابد.

۵- نتایج آزمایش‌ها

در این بخش از تصویر سطوح خاکستری «مرد عکاس»[۲۰] برای بررسی میزان تاثیرگذاری روش رمزنگاری پیشنهادی استفاده شده است.

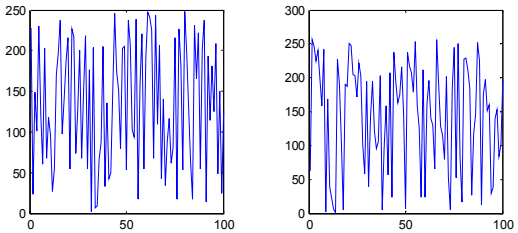
پارامترهای الگوریتم ژنتیک شامل تعداد جمعیت اولیه، احتمال تقاطع، احتمال جهش و تعداد تکرار الگوریتم (شرط توقف) به ترتیب برابر با ۵۰، ۰/۸، ۰/۰۲ و ۴۰۰۰ در نظر گرفته شده است. همچنین، در آزمایش‌ها ضرایب تابع برازندگی به ترتیب مقادیر ۸-، ۲-، ۳-، ۱۰۰+، ۱۰۰+ و ۱۰۰+ انتخاب شده است.

برای بررسی همگرایی الگوریتم ژنتیک از منحنی مقدار تابع برازندگی بر حسب تعداد تکرار استفاده شده است. در شکل (۲) تابع برازندگی بر حسب تعداد تکرار نشان داده شده است. محور عمودی بهترین هزینه در هر تکرار و محور افقی تعداد تکرار الگوریتم ژنتیک است. همان‌طور که ملاحظه می‌شود، با تکرار الگوریتم ژنتیک این مقدار کاهش می‌یابد. این کاهش نشان می‌دهد نحوه تغییر ضرایب رابطه بازگشتی به گونه‌ای است که در هر بار تکرار الگوریتم به جواب مناسب‌تری نزدیک می‌شود.



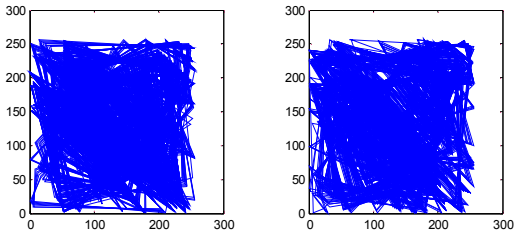
شکل (۲): نمودار بهترین هزینه بر حسب تعداد اجرای تابع برازندگی

برای مقایسه دنباله زمانی دوبعدی به دست آمده از الگوریتم ژنتیک، از سه دنباله دیگر استفاده شده است. این سه دنباله عبارتند از: دنباله فوق آشوبی [۶]، لجستیک [۱۱] و TD-ERCS [۱۶]. در این بخش نمودار دنباله بر حسب تعداد تکرار و نمودار میزان بی‌نظمی اعداد دنباله مشاهده می‌شود [۳, ۱۷]. این دو نمودار برای هر چهار دنباله در شکل‌های ۳ تا ۱۰ رسم شده است.



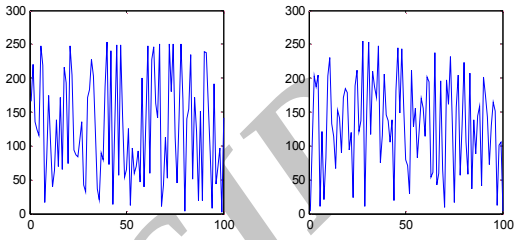
ب) مقادیر دنباله در راستای y الف) مقادیر دنباله در راستای x

شکل (۳): مقادیر دنباله الگوریتم ژنتیک بر حسب تعداد تکرار



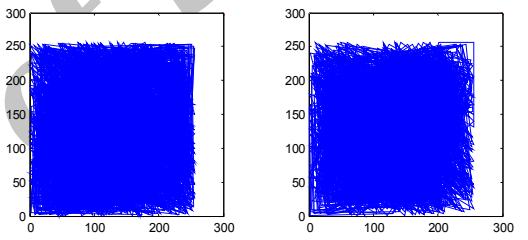
الف) الگوی رفتاری در راستای x ب) الگوی رفتاری در راستای y

شکل (۴): الگوی رفتاری دنباله الگوریتم ژنتیک



الف) مقادیر دنباله در راستای x ب) مقادیر دنباله در راستای y

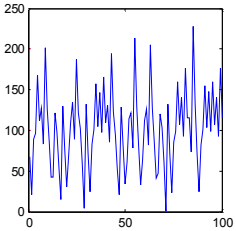
شکل (۵): مقادیر دنباله فوق‌آشوبی بر حسب تعداد تکرار



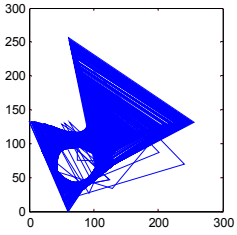
الف) الگوی رفتاری در راستای x ب) الگوی رفتاری در راستای y

شکل (۶): الگوی رفتاری دنباله فوق آشوبی

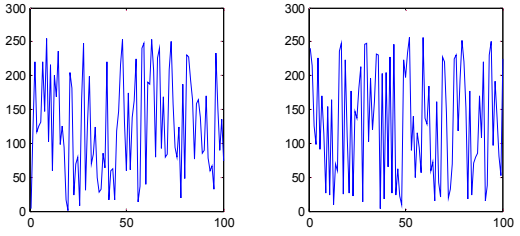
رفتار دنباله تولیدی توسط الگوریتم ژنتیک بر حسب زمان در شکل (۳) نشان داده شده است. مشاهده می‌شود که رفتار دنباله تولیدی تصادفی است و این دنباله هیچ نظم پریودیک ندارد. همچنین، برای نشان دادن غیرپریودیک بودن زوج‌های تولیدی و بی‌نظمی دنباله دوبعدی از شکل ۴ استفاده شده است. این رفتار در شکل‌های بعدی، برای سه دنباله دیگر نشان داده شده است.



شکل (۷): مقادیر دنباله یک‌بعدی لجستیک بر حسب تعداد تکرار

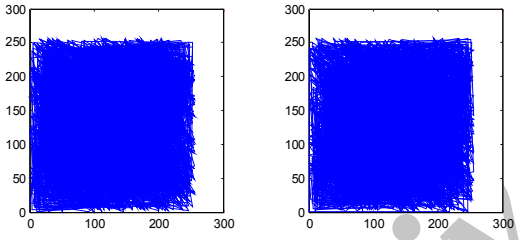


شکل (۸): الگوی رفتاری دنباله یک‌بعدی لجستیک



الف) مقادیر دنباله در راستای x ب) مقادیر دنباله در راستای y

شکل (۹): مقادیر دنباله TD-ERCS بر حسب تعداد تکرار



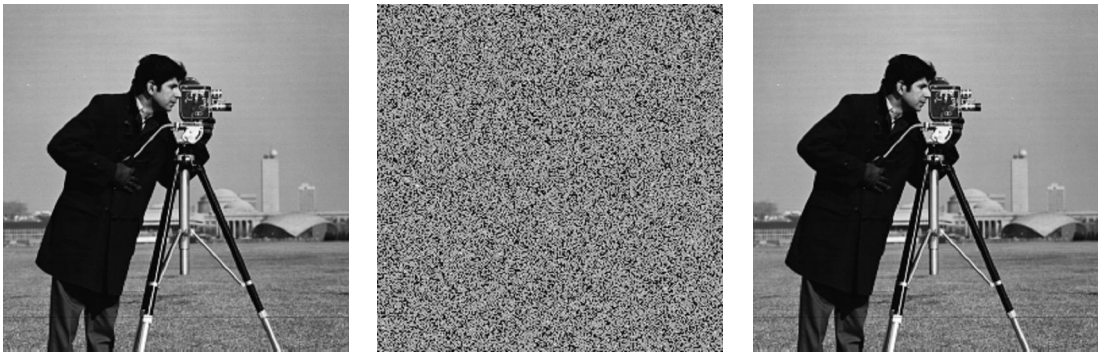
الف) الگوی رفتاری در راستای x ب) الگوی رفتاری در راستای y

شکل (۱۰): الگوی رفتاری دنباله TD-ERCS

در شکل‌های (۱۱) تا (۱۴) نتایج رمزنگاری تصویر با چهار دنباله الگوریتم ژنتیک، فوق آشوبی، لجستیک و TD-ERCS مشاهده می‌شود. همان طور که ملاحظه می‌شود، هر دنباله به خوبی توانسته است درهم‌ریزی تصویر را انجام دهد.

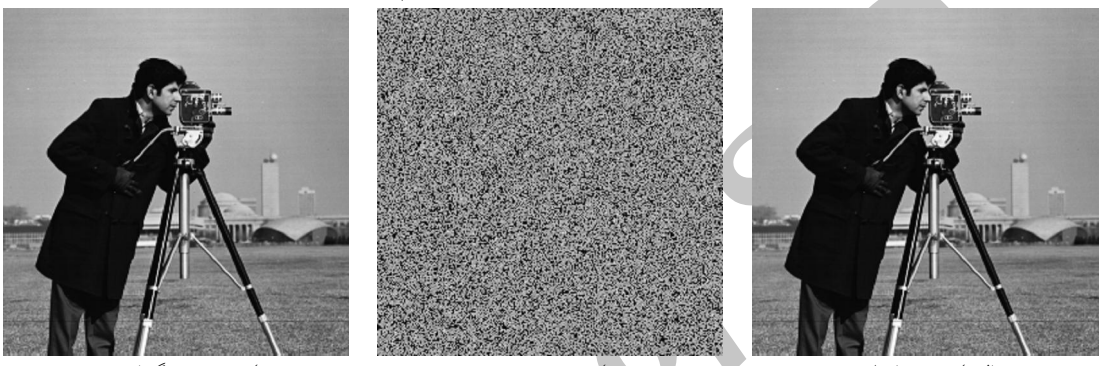
مقایسه تصویر رمز شده این چهار دنباله به روش بصری امکان‌پذیر نیست و به همین دلیل از معیارهای عددی برای مقایسه استفاده شده است. مقدار به دست آمده از توابع ارزیابی و هم چنین، مقدار تابع برازندگی برای چهار دنباله در جدول (۱) ارائه می‌شود. این معیارها شامل UACI، NPCR، MAE و میزان همبستگی در راستای افقی، عمودی و قطری است.

همان‌طور که از جدول مشاهده می‌شود، مقادیر معیارهای ارزیابی و تابع برازندگی برای دنباله حاصل از الگوریتم ژنتیک نسبت به بقیه دنباله‌ها بهتر است



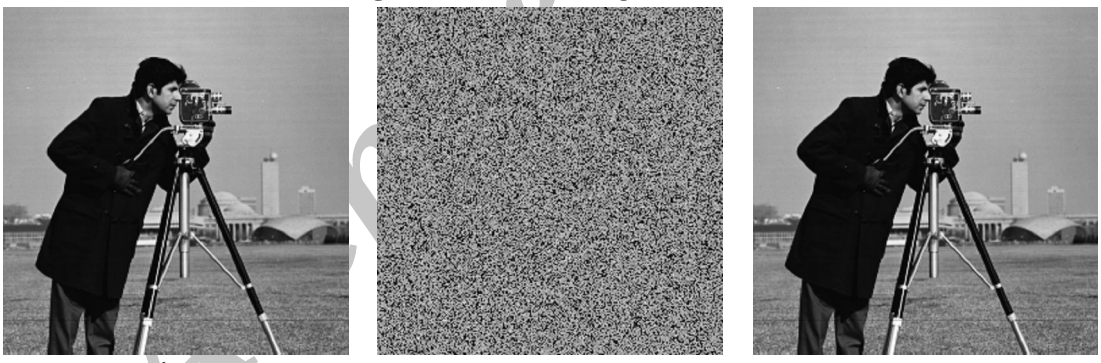
الف) تصویر اصلی ب) تصویر رمز شده ج) تصویر رمزگشایی شده

شکل ۱۱. نتایج رمزنگاری با دنباله الگوریتم ژنتیک



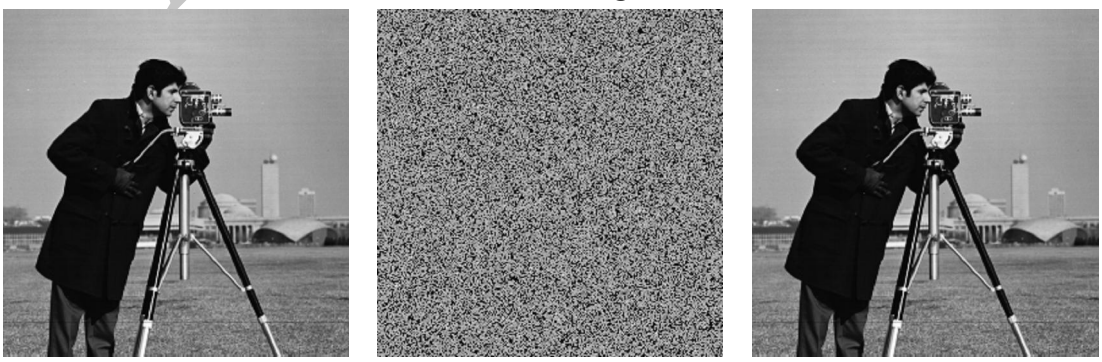
الف) تصویر اصلی ب) تصویر رمز شده ج) تصویر رمزگشایی شده

شکل ۱۲.نتایج رمزنگاری با دنباله فوق آشوبی



الف) تصویر اصلی ب) تصویر رمز شده ج) تصویر رمزگشایی شده

شکل ۱۳.نتایج رمزنگاری با دنباله لجستیک



الف) تصویر اصلی ب) تصویر رمز شده ج) تصویر رمزگشایی شده

شکل ۱۴. نتایج رمزنگاری با دنباله TD-ERCS

جدول (۱): مقادیر توابع ارزیابی و تابع برازندگی برای چهار دنباله مورد نظر

نام تابع ارزیابی	UACI	NPCR	MAE	مقدار تابع برازندگی
دنباله الگوریتم ژنتیک	۱۳/۲۶۷۳	۴۹/۶۴۹	۳۳/۹۱۲	-۱۰۷/۴۵۷۷
دنباله فوق آشوبی [۶]	۱۳/۲۴۴۱	۴۹/۲۴۱۶	۳۳/۶۸۵۵	-۱۰۴/۷۰۸۲
دنباله لجستیک [۱۱]	۱۳/۲۳۵۴	۴۹/۲۸۷۴	۳۳/۶۸۶۹	-۱۰۵/۶۵۱
دنباله TD-ERCS[۱۶]	۱۳/۲۴۲۴	۴۹/۵۹۲۶	۳۳/۷۰۵	-۱۰۶/۴۴۳۷

مقادیر تابع همبستگی در سه راستای افقی، عمودی و قطری برای تصویر اصلی و تصویر رمز شده با چهار دنباله متفاوت در جدول ۲ بیان شده است. این مقادیر نشان می‌دهند که الگوریتم ژنتیک نسبت به سایر دنباله‌ها عملکرد بهتری از خود نشان داده است.

جدول (۲): مقادیر میزان همبستگی در راستای افقی، عمودی و قطری

تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز ژنتیک	۰/۶۶۵۸	۰/۶۶۵۵	۰/۶۶۵۸
تصویر رمز فوق آشوبی	۰/۶۶۹۳	۰/۶۷۰۴	۰/۶۶۸۱
تصویر رمز لجستیک	۰/۶۶۵۷	۰/۶۶۷۱	۰/۶۶۶۲
تصویر رمز TD-ERCS	۰/۶۶۸۵	۰/۶۶۶۸	۰/۶۶۵۳

۶- نتیجه‌گیری

تصاویر دیجیتالی به علت وابستگی زیاد مقادیر پیکسل‌های همسایه و حجم بالای داده، دارای الگوریتم‌های رمزنگاری ویژه هستند.یکی از این الگوریتم‌ها، درهم‌ریزی پیکسل‌های تصویر است که در نتیجه محتویات تصویر برای کاربر غیرمجاز قابل فهم نیست.

در اکثر این روش‌ها درهم‌ریزی توسط یک دنباله زمانی انجام می‌شود. هر دنباله زمانی با یک رابطه بازگشتی و ضرایب از قبل تعیین شده تولید می‌شود و برای رمزنگاری همه تصاویر استفاده می‌شود. انتخاب ضرایب دنباله به طوری که دنباله برای رمزنگاری تصویر کارایی خوبی داشته باشد؛ به علت عدم رابطه مستقیم ضرایب دنباله با تصویر رمز شده امکان‌پذیر نیست.

در این مقاله با در نظر گرفتن یک دنباله عمومی بازگشتی، با استفاده از الگوریتم ژنتیک و تعریف یک تابع برازندگی مناسب، ضرایب دنباله به گونه‌ای محاسبه شدند که دنباله تولید شده معیارهای ارزیابی رمزنگاری تصویر را در حد مطلوب ارضا نماید. شایان ذکر است برای به دست آوردن ضرایب دنباله بازگشتی برای رمزنگاری هر تصویر، الگوریتم باید دوباره اجرا گردد که این موضوع و همچنین زمانبر بودن الگوریتم ژنتیک را می‌توان از محدودیت‌های روش پیشنهادی به حساب آورد. نتایج آزمایش‌ها نشان داد که عملکرد دنباله آشوبی به دست آمده از الگوریتم ژنتیک نسبت به تعدادی از دنباله‌های موجود کارایی مطلوبتری داشته است.

مراجع

[1] Corron, N. , Reed, B., Blakely, J., Myneni, K., Pethel, S., "Chaotic scrambling for wireless analog video", Communications in Nonlinear Science and Numerical Simulation, Vol. 15, No. 9, pp. 2504-2513, 2010.

[2] Pareek, N., Patidar, V., Sud, K., "Image encryption using chaotic logistic map", Image and Vision Computing, Vol. 24, No. 9 pp. 926-934, 2006.

[3] Kanso, A., Ghebleh, M. "A novel image encryption algorithm based on a 3D chaotic map" Communications in Nonlinear Science and Numerical Simulation, Vol. 17, No. 7, pp. 2943-2959, 2012.

[4] Xiangdong, L., Junxing, Z., Jinhai, Z., Xiqin, H., "Image scrambling algorithm based on chaos theory and sorting transformation", International Journal of Computer Science and Network Security, Vol.8, No.1, 64-68, 2008.

[5] Zhang, H., "A new image scrambling algorithm." IEEE International Conference on Machine Learning and Cybernetics, Vol. 2, pp. 1088-1092. 2008.

[6] Gu, G., Han, G., "The application of chaos and DWT in image scrambling", International Conference on Machine Learning and Cybernetics pp. 3729-3733, 2006.

[7] Alatas, B., "Chaotic bee colony algorithms for global numerical optimization", Expert Systems with Applications, Vol. 37, No. 8, pp. 5682-5687, 2010

[8] Wang, P., Gao, H., Cheng, M., Ma, X., "A new image encryption algorithm based on hyper chaotic mapping", IEEE International Conference on Computer Application and System Modeling,

Vol. 5, pp. V5-428. 2010.
[9] Hong-e, R., Jian, Z., Xing-jian, W., Zhen-wei, S., "Block sampling algorithm of image encryption based on chaotic scrambling", IEEE International Conference on Computational Intelligence and Security, pp. 773-776, 2007.
[9] Yanling, W., "Image scrambling method based on chaotic sequences and mapping", IEEE International Workshop Education Technology and Computer Science, Vol. 3, pp. 453-457.
[10] Ye, G., "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognition Letters, Vol. 31, No. 5, 347-354, 2010.
[11] Goldberg, D., Holland, J. "Genetic algorithms and machine learning", Machine learning, Vol. 3, No. 2, pp. 95-99, 1998.
[12] Rakesh, S., Kaller, A., Shadakshari, B., Annappa, B., "Image encryption using block based uniform scrambling and chaotic logistic mapping", International Journal on Cryptography and Information Security, Vol. 2, No. 1, pp. 49-57, 2012.
[13] Jolfaei, A., Mirghadri, A., "Survey: image encryption using Salsa20", International Journal of Computer Science Issues, Vol. 7, No. 5, pp. 213-220, 2010.
[14] Ye, R., Zhao, H., "An efficient chaos-based image encryption scheme using affine modular maps", International Journal of Computer Network and Information Security, Vol. 4, No. 7, pp. 41,2012.
[15] Feng-ying, H., Cong-xu, Z., "An novel chaotic image encryption algorithm based on tangent-delay ellipse reflecting cavity map ssystem", Procedia Engineering, Vol. 23, pp. 186-191, 2011.
[16] Wei, X., Guo, L., Zhang, Q., Zhang, J., Lian, S., "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", Journal of Systems and Software, Vol. 85, No. 2, pp.290-299, 2012.

[1]Visual Surveillance Systems
[2]Rivest-Shamir-Adleman (RSA)
[3]Data Encryption Standard (DES)
[4]Image Cryptography
[5]Substitution
[6]Scrambling
[7]Spatial Domain
[8]Frequency Domain
[9]Diffusion
[10]Logistic
[11]Hyper Chaotic
[12]Genetic Algorithm
[13]Fitness Function
[14]John Holland
[15]Crossover
[16]Mutation
[17] Unified Average Changing Intensity (UACI)
[18] Number of Pixel Change Rate (NPCR)
[19] Mean Absolute Error (MAE)
[20]Cameraman