

## ارائه الگوریتم جدید رمزنگاری تصویر دیجیتال با استفاده از الگوریتم‌های تبدیل آرنولد و تکامل تفاضلی

رسول جمالی اوئلیق\*<sup>۱</sup>، علی فرزانه<sup>۲</sup>

۱- دانشجوی کارشناسی ارشد نرم‌افزار، ۲- استادیار، گروه مهندسی کامپیوتر، واحد شبستر، دانشگاه آزاد اسلامی، شبستر، ایران  
(دریافت: ۹۵/۰۹/۰۸، پذیرش: ۹۶/۰۵/۱۸)

### چکیده

رمزنگاری تصاویر به‌عنوان یکی از روش‌های حفظ امنیت اطلاعات در ارسال و دریافت آن به شمار می‌رود. در این میان، روش‌های زیادی جهت رمزنگاری وجود دارد. واضح است که استفاده از ترکیبی از این الگوریتم‌ها می‌تواند باعث افزایش امنیت الگوریتم رمزنگاری گردد. در این مقاله سعی شده است که با ترکیب دادن الگوریتم تبدیل آرنولد با یکی از الگوریتم‌های تکاملی به نام الگوریتم تکامل تفاضلی، یک روش جدید جهت رمزنگاری تصاویر دیجیتال ارائه شود. الگوریتم تکامل تفاضلی پاسخ‌های بهینه را به‌روشنی منحصربه‌فرد خود تولید می‌کند که موجب می‌شود تا روش رمزنگاری تصویر متفاوت بوده و موجب افزایش امنیت و مقاومت الگوریتم رمزنگاری گردد. یک تصویر دیجیتال ابتدا با الگوریتم تبدیل آرنولد رمزنگاری می‌شود و سپس روی این تصویر، تکامل تفاضلی اعمال می‌گردد. بدین ترتیب، مقاومت تصویر رمزنگاری‌شده در مقابل انواع حملات افزایش می‌یابد.

**کلمات کلیدی:** تصویر دیجیتال، رمزنگاری تصویر دیجیتال، تبدیل آرنولد، تکامل تفاضلی

### ۱- مقدمه

این تصاویر یکی از روش‌های حفظ امنیت آن‌ها است. رمزنگاری به مفهوم، دانش تغییر دادن اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به طوری که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمزنگاری‌شده باشد و شخصی که از یکی یا هر دو آن‌ها اطلاع ندارد نتواند به اطلاعات دسترسی پیدا کند. رمزنگاری یک تصویر دیجیتال نیز به معنای ایجاد تغییر در آن با استفاده از یک الگوریتم رمزنگاری است، به طوری که دسترسی به اطلاعات آن ممکن نباشد [۱-۲]. برای رمزنگاری تصاویر دیجیتال الگوریتم‌های زیادی وجود دارند که از آن جمله می‌توان به تبدیل Fibonacci، تبدیل Biker، تبدیل Affine و ... اشاره کرد. تبدیل آرنولد یکی از روش‌های رمزنگاری تصاویر دیجیتال است که توسط یک ریاضیدان روسی به نام ولادیمیر آرنولد ارائه شده است. این الگوریتم یکی از معروف‌ترین و پرکاربردترین الگوریتم‌ها در زمینه رمزنگاری تصاویر است که اغلب برای تصاویر مربعی کاربرد دارد ولی در سال‌های اخیر با ایجاد تغییر در روش استفاده از آن،

گسترش روزافزون اینترنت در عصر کنونی، سبب تحول چشمگیری در عرصه ارتباطات دیجیتال شده است. اینترنت به‌عنوان محیطی برای به اشتراک گذاشتن و تبادل ساده و سریع انواع محصولات دیجیتال متنی، صوتی و تصویری، موجب رشد کمی و کیفی تولید این محصولات شده است. با افزایش تولید و همه‌گیر شدن استفاده از این محصولات، صاحبان این آثار به تدریج نگران حفاظت حقوق خود شدند. به این ترتیب، بحث حفاظت از اطلاعات دارای حق کپی، برای جلوگیری از پامال شدن حقوق این مولفان، ضروری به نظر می‌رسید.

تصاویر دیجیتال یکی از داده‌های مهم در ارسال اطلاعات هستند که کاربردهای زیادی مانند کاربردهای نظامی، تجاری، پزشکی و ... دارند. لذا حفظ امنیت و جلوگیری از دسترسی‌های غیرمجاز به آن‌ها یک امر مهم و ضروری است. رمزنگاری کردن

1 -Vladimir Arnold

\* رایانامه نویسنده مسئول: Ra2jamali@yahoo.com

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_{k-1} \\ y_{k-1} \end{bmatrix} \pmod N \quad (۴)$$

از رابطه (۴)، این نتیجه حاصل می شود که اگر مختصات  $(x, y)$  مانند چندین بار از نقطه‌ای به نقطه دیگر انتقال داده شوند، در نهایت، بعد از  $T$  بار تکرار این عمل، به مکان اولیه خود باز خواهند گشت. این  $T$  به نام دوره تناوب تبدیل گفته می شود که وابسته به اندازه تصویر بوده و با استفاده از آن تعیین می شود [۷، ۹-۱۰].

### ۲-۱- رمزنگاری با استفاده از تبدیل آرنولد

هر تصویر دیجیتال به صورت یک ماتریس مربعی دوبعدی نشان داده می شود. اگر اندازه تصویر  $N$  باشد، اندازه ماتریس آن  $N \times N$  است. اگر  $(x, y)$  مختصات مکان اولیه یک پیکسل مانند  $p$  باشد،  $(x, y) \in \{0, 1, 2, 3, \dots, N-1\}$  و این مختصات،  $k$  بار تغییر مکان داده شوند، پیکسل  $p$  از مکان اولیه خود به جای دیگری نقل مکان خواهد کرد. اگر این عمل بر روی تمامی پیکسل‌های تصویر انجام شود، مکان اولیه تمامی پیکسل‌ها تغییر یافته و تصویر به صورت رمزنگاری شده درمی آید [۷ و ۹].

### ۳- الگوریتم تکامل تفاضلی

امروزه اختراع روش‌های محاسباتی حل مسئله برای مقابله با روش‌های گوناگون بسیار مورد توجه محققین است. بسیاری از مسائل بهینه‌سازی در دنیای واقعی مهندسی به‌طور فزاینده‌ای در حال پیچیده شدن هستند. بنابراین، الگوریتم‌های بهینه‌سازی با عملکرد بالا مورد نیاز است [۳].

الگوریتم‌های تکاملی راه‌حل خوبی برای مسائل بهینه‌سازی هستند. این الگوریتم‌ها بر پایه اصول تکامل زیستی بنا نهاده شده‌اند. هر الگوریتم، تکاملی از دو مرحله مقداردهی اولیه و تکاملی تشکیل شده است. در مرحله مقداردهی اولیه، جمعیت اولیه بر اساس یک توزیع تصادفی یکنواخت به نحوی انتخاب می شود که تمام فضای مسئله را پوشش دهد. سپس در مرحله تکامل، شایستگی افراد درون جمعیت بر اساس یک تابع شایستگی از پیش تعیین شده مشخص می شود. در گام بعدی مرحله تکامل، فرزندان جدید با استفاده از دو عمل باز ترکیبی و جهش ایجاد می شوند. سپس با استفاده از روشی از پیش تعیین شده، افراد نسل بعدی از میان والدین و فرزندان انتخاب می شوند. این چرخه تا زمانی ادامه می یابد که شرط خاتمه الگوریتم برقرار باشد [۳].

تصاویر غیرمربعی را نیز می توان با این الگوریتم رمزنگاری نمود. این الگوریتم با جابه‌جا کردن پیکسل‌های یک تصویر رمزنگاری را انجام می دهد.

الگوریتم تکامل تفاضلی نیز جزو الگوریتم‌های تکاملی است. این الگوریتم‌ها اغلب برای مسائل بهینه‌سازی کاربرد دارند. لیکن به دلیل این که نحوه تولید یک مجموعه از پاسخ‌ها در این الگوریتم‌ها به یک روش خاصی انجام می شود لذا استفاده از این روش‌ها در رمزنگاری تصاویر نیز می تواند مفید واقع شود. روش تولید یک مجموعه از پاسخ‌ها در الگوریتم تکامل تفاضلی نسبت به دیگر الگوریتم‌های تکاملی به‌طور کاملاً خاص و منحصر به فردی انجام می شود که موجب سریع تر شدن و امنیت بیشتر این الگوریتم در مقایسه با سایر موارد گردیده است. در این مقاله سعی شده است تا با ترکیب الگوریتم‌های تبدیل آرنولد و تکامل تفاضلی روشی جدید جهت رمزنگاری تصاویر دیجیتال ارائه گردد. نتایج حاصل از آزمایشات نشان می دهند که روش پیشنهادی از قدرت رمزنگاری قوی تر و مقاومت بیشتر بر خوردار است.

### ۲- تبدیل آرنولد

این الگوریتم یک فرآیند تکراری جهت رمزنگاری تصاویر است که پیکسل‌ها را از مکانی به مکان دیگر انتقال می دهد. این تبدیل بر روی تصاویر مربعی اعمال می شود. بدین ترتیب که مختصات یک پیکسل را گرفته و بر اساس یک الگوریتمی، مختصات جدید جهت انتقال را به دست می آورد. ساده ترین نوع این الگوریتم، تبدیل دوبعدی آن می باشد که با استفاده از رابطه زیر حاصل می شود:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \quad (۱)$$

که در آن،  $(x, y)$  مکان اولیه یک پیکسل و  $(x', y')$  مکان جدید انتقال یافته همان پیکسل و  $N$  اندازه ماتریس تصویر مربعی است. با توجه به این رابطه، جهت انتقال هر پیکسل از نقطه‌ای به نقطه دیگر برای اولین بار:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \pmod N \quad (۲)$$

جهت انتقال برای دومین بار:

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \pmod N \quad (۳)$$

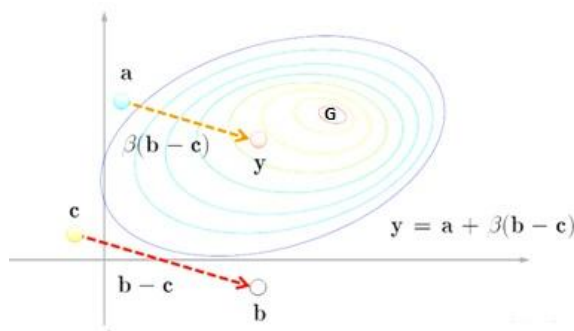
لذا برای انتقال  $K$  امین بار مختصات هر پیکسل:

a, b و c با استفاده از عملگر تقاطع با x ترکیب شده و جواب جدیدی به نام z حاصل می شود [۵ و ۱۲].

$$x = (x_1, x_2, x_3, \dots, x_n) \rightarrow z = (z_1, z_2, z_3, \dots, z_n) \quad (5)$$

$$y = (y_1, y_2, y_3, \dots, y_n)$$

$$y = a + \beta(b - c) \quad \text{به طوری که:}$$



شکل (۱): روش انجام جهش و ایجاد پاسخ موقت

برای تشکیل مجموعه J، از روش تقاطع دوجمله‌ای به صورت زیر استفاده می شود.

- ابتدا  $J_0$  به صورت تصادفی از میان اعداد صحیح ۱ تا n انتخاب می شود.
- عدد  $J_0$  به مجموعه J (که در ابتدا خالی است) افزوده می شود.
- به ازای تمام مقادیر J از ۱ تا n، عملیات زیر تکرار می شوند:
  - یک عدد تصادفی مانند  $r_j$  که دارای توزیع یکنواخت در بازه [۰, ۱] است تولید می شود.
  - اگر  $r_j$  کمتر یا مساوی  $P_{CR}$  (پارامتر احتمال تقاطع) باشد، عدد J به مجموعه J اضافه می شود [۱۲].

$$z_j = \begin{cases} y_j, & r_j \leq P_{CR} \text{ or } J = j_0 \\ x_j & \text{otherwise} \end{cases}$$

#### ۴- روش پیشنهادی

در این بخش روش جدیدی با استفاده از ترکیب الگوریتم‌های تبدیل آرنولدی و تکامل تفاضلی جهت رمزنگاری یک تصویر دیجیتال به شرح زیر ارائه داده می شود. این روش شامل دو مرحله، رمزنگاری و رمزگشایی است.

##### ۴-۱- مرحله اول: رمزنگاری

این مرحله شامل سه زیرمرحله به شرح ذیل است:

- ۱- ابتدا روی یک تصویر دیجیتال (I) تبدیل آرنولدی اعمال می شود تا تصویر، رمزنگاری گردد. بدین ترتیب، تصویر رمزنگاری شده اولیه حاصل می شود (SI).

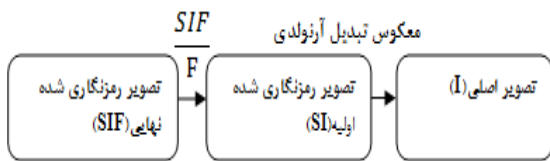
الگوریتم تکامل تفاضلی اولین بار در سال ۱۹۹۵ توسط استورن و پرایس معرفی شد. آن‌ها نشان دادند که این الگوریتم توانایی خوبی در بهینه‌سازی توابع غیرخطی مشتق‌ناپذیر دارد که به‌عنوان روشی قدرتمند و سریع برای مسائل بهینه‌سازی در فضاهای پیوسته معرفی شده است. این الگوریتم جهت غلبه بر عیب اصلی الگوریتم ژنتیک، یعنی فقدان جستجوی محلی در این الگوریتم ارائه شده است. تفاوت اصلی بین الگوریتم‌های ژنتیکی و الگوریتم تکامل تفاضلی در عملگر انتخاب است. در عملگر انتخاب الگوریتم ژنتیک، شانس انتخاب یک جواب به‌عنوان یکی از والدین وابسته به مقدار شایستگی آن می باشد، اما در الگوریتم تکامل تفاضلی، همه جواب‌ها دارای شانس مساوی جهت انتخاب شدن می باشند. یعنی شانس انتخاب شدن آن‌ها وابسته به مقدار شایستگی آن‌ها نمی باشد، پس از این که یک جواب جدید با استفاده از یک عملگر جهش خود-تنظیم و عملگر تقاطع تولید شد، جواب جدید با مقدار قبلی مقایسه شده و در صورت بهتر بودن، جایگزین می گردد [۳، ۵، ۱۱-۱۲].

همانند دیگر الگوریتم‌های بهینه‌سازی مبتنی بر جمعیت، DE نیز شامل دو مرحله مقداردهی اولیه و تکامل است. در مرحله اول، اگر هیچ اطلاعاتی در مورد مسئله وجود نداشته باشد، جمعیت به‌طور تصادفی تولید می شود. در مرحله تکامل، افراد جمعیت از طریق جهش، بازترکیبی و فرایند انتخاب، بارها و بارها بهبود می یابند تا زمانی که معیار انتخاب خاتمه الگوریتم ارضاء شود [۳].

الگوریتم تکامل تفاضلی از دو جهت ترتیب انجام تقاطع و جهش با سایر الگوریتم‌های تکاملی متفاوت است. بدین ترتیب که ابتدا با استفاده از عملگر جهش یک پاسخ موقت تولید می شود و سپس با استفاده از عملگر تقاطع، یک پاسخ جدید ایجاد می شود. گام و طول جهش نیز از فاصله و تفاضل میان پاسخ‌های موجود در جمعیت ایجاد می شوند [۱۲].

در شکل (۱)، برای رسیدن به نقطه هدف (G)، سه عضوی از جمعیت به‌طور تصادفی انتخاب می شوند ( $a \neq b \neq c$ ). تفاضل بین نقاط b و c، یعنی بردار b-c در یک ضریب مقیاس ( $\beta$ ) ضرب شده و به a افزوده می شود و بدین ترتیب، نقطه y به‌عنوان یک پاسخ موقت جدید حاصل می شود. در ادامه این پاسخ موقت با استفاده از عملگر تقاطع با اعضای جمعیت قبلی ترکیب می شود. در واقع، به ازای هر x از جمعیت قبلی، یکسری a, b و c در واقع، به ازای هر x از جمعیت قبلی، یکسری a, b و c ( $a \neq b \neq c \neq x$ ) انتخاب شده و پاسخ موقت (y) حاصل از

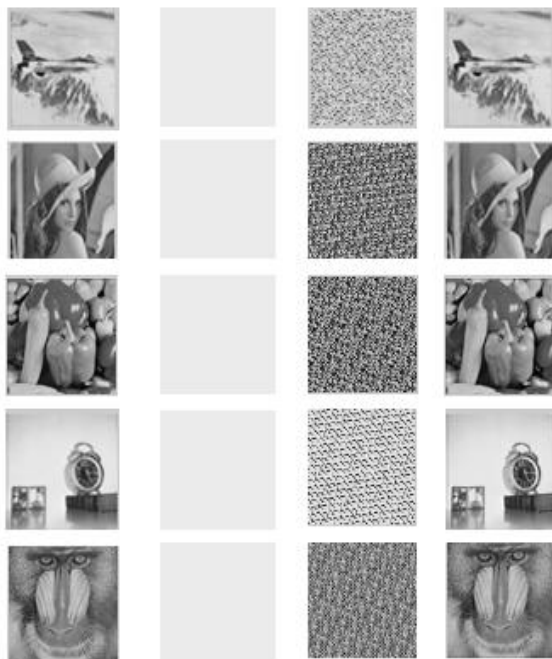
شکل (۳)، گام‌های این مرحله را نشان می‌دهد.



شکل (۳): مراحل رمزگشایی تصویر

### ۵- نتایج شبیه‌سازی

برای جلوگیری از انواع حملات مختلف، باید تضمین شود که تصویر اصلی و تصویر رمزنگاری شده هیچ‌گونه تشابه آماری نداشته باشند. تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از ترسیم تعداد مشاهدات هر میزان شدت روشنایی بیان می‌کند. توزیع به نسبت یکنواخت تصویر، نشان‌دهنده کیفیت خوب روش رمزنگاری است. در شکل‌های بعدی نتایج حاصل شده از اعمال روش پیشنهادی بر روی پنج تصویر مختلف (شکل (۴) و تحلیل هیستوگرام هر کدام از آنها (اشکال ۵-۹) آورده شده است.



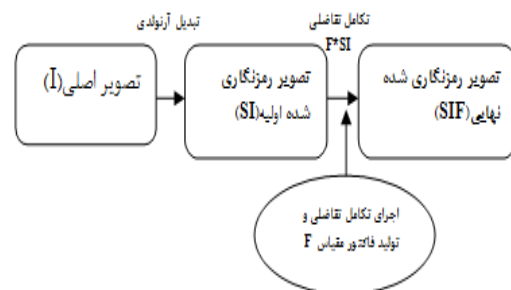
(الف) (ب) (ج) (د)

شکل (۴): (الف) تصویر اصلی، (ب) تصویر رمزنگاری شده با تبدیل آرنولدی، (ج) تصویر رمزنگاری شده نهایی با روش پیشنهادی، (د) تصویر رمزگشایی شده

۲- الگوریتم تکامل تفاضلی اجرا شده و یک فاکتور مقیاس (F) تولید می‌کند. این فاکتور مقیاس به صورت یک ماتریس هم‌مرتبه با ماتریس تصویر رمزنگاری شده است.

۳- جهت افزایش مقاومت و امنیت تصویر رمزنگاری شده، این تصویر (SI) در فاکتور مقیاس حاصل از اجرای الگوریتم تکامل تفاضلی (F) ضرب می‌شود که در نهایت، تصویر رمزنگاری شده نهایی حاصل از ترکیب دو الگوریتم تبدیل آرنولدی و تکامل تفاضلی حاصل می‌گردد (SIF).

در واقع، استفاده از فاکتور مقیاس تکامل تفاضلی جهت بالابردن مقاومت الگوریتم رمزنگاری است. بدین ترتیب، تصویر رمزنگاری شده در مقابل انواع حملات مختلف مقاومت بیشتری داشته و قابل رمزگشایی نخواهد بود، چون الگوریتم تکامل تفاضلی یک الگوریتم ساده، سریع و مقاوم در مقایسه با سایر انواع الگوریتم‌های تکاملی است و هدف از استفاده از این الگوریتم، رسیدن به بهترین بهره‌وری در مقاومت الگوریتم پیشنهادی در برابر انواع حمله‌ها روی تصویر رمزنگاری شده است، زیرا که الگوریتم DE، بهترین فاکتور مقیاس را که به صورت یک ماتریس است (نه یک عدد ثابت) تولید می‌کند [۵ و ۱۱]. شکل (۲) گام‌های این مرحله را نشان می‌دهد.



شکل (۲): مراحل رمزنگاری تصویر

### ۴-۲- مرحله دوم: رمزگشایی

این مرحله، معکوس مرحله اول است که شامل دو زیرمرحله به شرح زیر است:

۱- ابتدا تصویر رمزنگاری شده نهایی بر مقدار فاکتور مقیاس تکامل تفاضلی تقسیم می‌شود که نتیجه حاصل از این مرحله تصویر رمزنگاری شده اولیه (SI) یا همان تصویر رمزنگاری شده توسط تبدیل آرنولدی است.

۲- سپس روی این تصویر، معکوس تبدیل آرنولدی اعمال می‌شود تا تصویر رمزگشایی نهایی شود. در نهایت، تصویر اصلی اولیه حاصل می‌گردد.

روش پیشنهادی را بر روی تصاویرهای مختلف از نوع خاکستری در اندازه های ۶۴×۶۴ اعمال کرده و نتایج تحلیل هیستوگرام هرکدام از آنها و نیز تصاویر رمزنگاری شده نهایی با روش پیشنهادی را برای هر یک از آنها رسم کردیم. نتایج به دست آمده نشان می دهند که تصاویر رمزنگاری شده و تصویر اصلی نسبت به هم کاملاً متفاوتند و هیستوگرام تصاویر رمزنگاری شده دارای توزیع نسبتاً یکنواختی می باشند. علاوه بر این، پارامترهای "میانگین مجذور خطا" (MSE) و "بیشترین نسبت تفاوت" (PSNR) دو معیار سنجش کیفیت الگوریتم های رمزنگاری بین دو تصویر اصلی و رمز شده هستند که اولی میزان انباشتگی خطا بین دو تصویر اصلی و رمز شده را نشان می دهد و هرچقدر مقدار آن کمتر باشد، نشان دهنده کیفیت بالاتر آن است. دومی میزان بیشترین نسبت تفاوت بین دو تصویر اصلی و رمز شده را نشان می دهد که هرچقدر میزان آن بیشتر باشد، نشان دهنده کیفیت بالاتر است [۵ و ۲۴].

جدول های (۱-۵) زیر نتایج حاصل شده برای این دو پارامتر را جهت مقایسه کیفیت رمزنگاری چندین الگوریتم رمزنگاری با روش پیشنهادی نشان می دهند.

جدول (۱): مقادیر MSE و PSNR برای تصویر هواپیما

الگوریتم معیار	MSE	PSNR
تبدیل آرنولدی	۹۶۳۵۵۵	۹/۹۸۸۵
تبدیل آرنولدی با الگوریتم زنبورعسل	۱۳۲۲۹۰	۴۵/۶۹۰۷
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۳۹۰۷۲	۵۷/۸۰۵
روش پیشنهادی	۰/۱۳۷۹۶	۳۴/۰۳۳۵

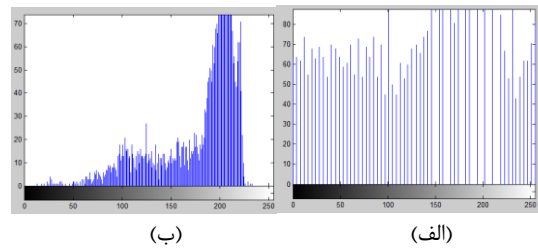
جدول (۲): مقادیر MSE و PSNR برای تصویر لنا

الگوریتم معیار	MSE	PSNR
تبدیل آرنولدی	۱۱۳/۰۶۲۰	۹/۳۳۲۶
تبدیل آرنولدی با الگوریتم زنبورعسل	۵۴/۵۴۸۶	۱۳/۴۵۹۴
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۳/۱۱۵۰	۵/۷۹۴۱
روش پیشنهادی	۰/۱۹۶۸	۳۶/۸۸۷۵

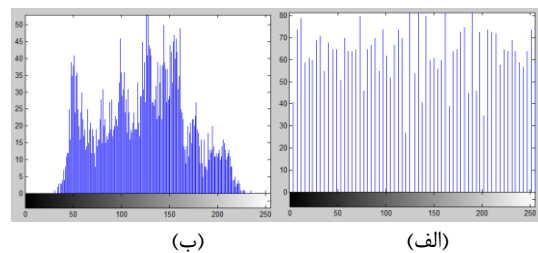
جدول (۳): مقادیر MSE و PSNR برای تصویر فلفل

الگوریتم معیار	MSE	PSNR
تبدیل آرنولدی	۱۱۳/۸۸۸۲	۹/۳۶۲۴
تبدیل آرنولدی با الگوریتم زنبورعسل	۵۸/۰۲۹۱	۱۲/۱۹۰۸
تبدیل آرنولدی با الگوریتم ژنتیک	۲۴۴/۱۴۹۲	۵/۹۵۰۷
روش پیشنهادی	۳/۱۷۹۷	۲۴/۸۰۳۴

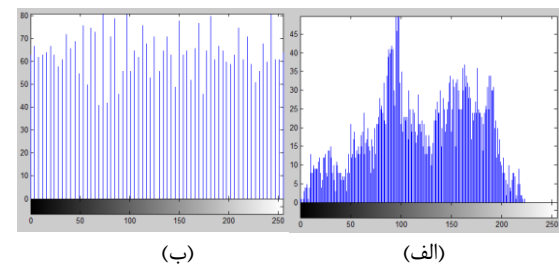
- 1- Mean Squared Error
- 2- Peak Signal to Noise Ratio



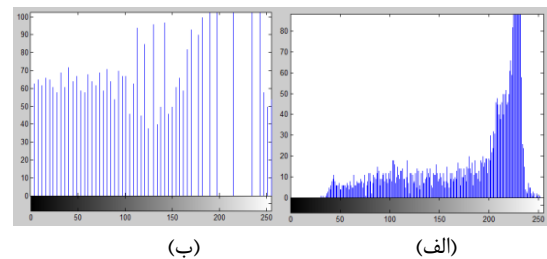
شکل (۵): الف) تحلیل هیستوگرام تصویر هواپیما، ب) تحلیل هیستوگرام تصویر رمزنگاری شده نهایی هواپیما



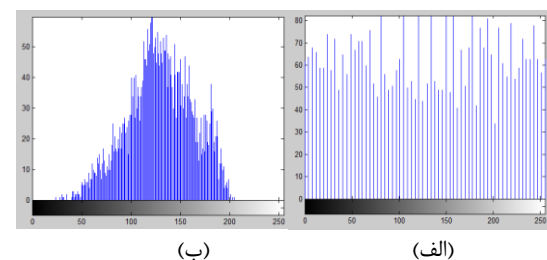
شکل (۶): الف) تحلیل هیستوگرام تصویر لنا، ب) تحلیل هیستوگرام تصویر رمزنگاری شده نهایی لنا



شکل (۷): الف) تحلیل هیستوگرام تصویر فلفل، ب) تحلیل هیستوگرام تصویر رمزنگاری شده نهایی فلفل



شکل (۸): الف) تحلیل هیستوگرام تصویر ساعت، ب) تحلیل هیستوگرام تصویر رمزنگاری شده نهایی ساعت



شکل (۹): الف) تحلیل هیستوگرام تصویر میمون، ب) تحلیل هیستوگرام تصویر رمزنگاری شده نهایی میمون

در مقایسه با سایر الگوریتم‌های تکاملی به دلیل استفاده از فاکتور مقیاس چندگانه که به صورت یک ماتریس است و نه یک عدد، موجب افزایش مقاومت روش رمزنگاری می‌گردد [۵]. علاوه بر این، به علت این که سایر الگوریتم‌های تکاملی عمل جهش را با استفاده از یک تابع توزیع احتمالی انجام می‌دهند ولی در این الگوریتم شیوه انجام جهش با استفاده از تفاضل بین اعضا انجام می‌پذیرد، لذا استفاده از این روش موجب بهبود فرآیند رمزنگاری می‌شود.

## ۷- مراجع

- [1] E. Hoseyni and SH. B. shokuhi, "Image scramble using chaotic function," 9th conference of Electronic Engineering of IRAN, Elm & Sanaat university. (In Persian).
- [2] S. A. Isfahani and D. Bakhshesh, "A hybrid method for scrambling image using Hyperchaotic function and Evolutionary operators," Eighth international conference of Security Community of iran, Mashhad university, 23 and 24th, 2012. (In Persian)
- [3] M. Abieshagh and M. Eftekhari, "ninth symposium on Advances in Science and Technology," Mashhad, 13 Azar of 2015. (In Persian)
- [4] C. Li and D. Lin, "Cryptanalysis of an Image Scrambling Encryption Algorithm," College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China, 2016.
- [5] A. Musarrat and C. Wook Ahn, "Millie Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain," Elsevier, 2014.
- [6] P. Premaratne and M. Premaratne, "Key-based sxrambling for secure image communicatin," in Emerging Intelligent Computing Technology and Applications, University of Wollongong, 2012.
- [7] L. Wu, J. Zhang, w. Deng, and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," IEEE, ICISE, 2009.
- [8] D. Vang, C.-C. Chang, Y. Liu, G. Song, and Y. Liu, "Digital Image Scrambling Algorithm Based on Chaotic Sequence Decomposition and Recombinatic of Pixel Values," International Journal of Network Security, 2015.
- [9] M. Li, T. Liang, and Y.-j. He, "Arnold Transform Based Image Scrambling Method," Atlantis Press, 2013.
- [10] X. Zhang, G. Zhu, W. Wang, M. Wang, and S. Ma, "Period Law of Discrete Two-dimensional Arnold Transformation," IEEE, 2010.
- [11] R. Stone and K. Price, "Differential Evolution, A Simple and Efficient Heuristic for Global Optimization over Continuous Spaces," Journal of Global Optimization, 1997.
- [12] K. Tomar, "A Review Paper of Different Techniques on Digital Image Watermarking Scheme for Robustness," IJARCSSE, vol. 5, Issue2, 2015.
- [13] A. Jadhav and M. kolhekar, "Digital Watermarking in Video for Copy Right Protection," IEEE, ICESC, 2014.
- [14] R. Bala, "A Brief Survey on Robust Video Watermarking Techniques, IJES, vol. 4, Issue2, 2015.

جدول (۴): مقادیر MSE و PSNR برای تصویر ساعت

الگوریتم	MSE	PSNR
معیار		
تبدیل آرنولدی	۹۷/۳۲۴۷	۹/۹۴۵۰
تبدیل آرنولدی با الگوریتم زنبور عسل	۴۸/۳۶۳۸	۱۲/۹۸۲۰
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۲/۳۹۷۷	۵۸/۰۶۴
روش پیشنهادی	۰/۱۹۵۶	۳۶/۹۱۴۵

جدول (۵): مقادیر MSE و PSNR برای تصویر میمون

الگوریتم	MSE	PSNR
معیار		
تبدیل آرنولدی	۱۰۵/۶۱۳۰	۹/۹۴۵۰
تبدیل آرنولدی با الگوریتم زنبور عسل	۵۱/۷۱۵۳	۱۲/۹۸۲۰
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۴/۸۲۲۵	۵۸/۰۶۴
روش پیشنهادی	۰/۰۶۲۳	۳۶/۹۱۴۵

با مقایسه MSE جدول‌های فوق، این نتیجه حاصل می‌شود که مقدار این پارامتر برای روش پیشنهادی کمتر از دیگر الگوریتم‌ها است و مقدار پارامتر PSNR روش پیشنهادی بیشتر از سایر الگوریتم‌ها است. بنابراین، این نتیجه حاصل می‌شود که کیفیت روش پیشنهادی، بالاتر از دیگر الگوریتم‌های مشابه در زمینه رمزنگاری تصویر است.

از نظر هزینه محاسباتی نیز روش پیشنهادی در مقایسه با سایر روش‌های مشابه رمزنگاری تصویر مانند استفاده از الگوریتم ژنتیک (GA)، الگوریتم ازدحام ذرات (PSO) و کلونی زنبور عسل (ABC)، به علت استفاده از الگوریتم تکامل تفاضلی، پیچیدگی زمانی کمتری دارد. چراکه الگوریتم تکامل تفاضلی یکی از انواع الگوریتم‌های بهینه‌سازی است که در مقایسه با سایر الگوریتم‌های بهینه‌سازی، پیچیدگی زمانی کمتری دارد [۲۱-۲۳].

## ۶- نتیجه‌گیری

در این مقاله یک روش جدید ساده و سریع رمزنگاری با استفاده از ترکیب دو الگوریتم تبدیل آرنولدی و تکامل تفاضلی ارائه شد. نتایج به دست آمده از بررسی‌ها نشان می‌دهند که استفاده از الگوریتم تکامل تفاضلی به همراه تبدیل آرنولدی، باعث افزایش امنیت و مقاومت الگوریتم رمزنگاری می‌شود زیرا که الگوریتم تکامل تفاضلی یکی از انواع الگوریتم‌های تکاملی است که

- 1- Genetic Algorithm
- 2- Particle Swarm Optimization
- 3- Artificial Bee Colony

- [20] N. Tiwari and Sharmila, "Digital Watermarking Applications, Parameter Measures and Techniques," International Journal of Computer Science and Network Security, IJCSNS, March 2017.
- [21] M. Iwan, R. Akmeliawati, T. Faisal, and H. Al-Assadi, "Performance Comparison of Differential Evolution and Particle Swarm Optimization In Constrained Optimization," Procedia Engineering, 2012.
- [22] P. Civicioglu and E. Bosdok, "A conceptual comparison of the Cuckoo-search," particle swarm optimization, differential evolution and artificial bee colony algorithms, Artificial Intelligence, April 2013.
- [23] B. Hegerty, C. Hung, and K. Kasprak, "A Comparative Study on Differential Evolution and Genetic Algorithms for Some Combinatorial Problems," IEEE, 2008.
- [24] J. Champan, "Matlab Programing for Engineers," Thomson Learning, 2007.
- [25] C. Moler, "A proprietary programming language," Mthworks.com. Available: <https://www.mathworks.com>
- [15] A. Phadikar, S. P. Maity, and B. Verma, "Region based QIM digital watermarking scheme for image database in DCT domain," Comput. Electr. Eng., vol. 37, 2011.
- [16] H. H. Tsai, Y. J. Jhuang, and Y. S. Lai, "An SVD based image watermarking in wavelet domain using SVR and PSO," Appl. Soft Comput., 2012.
- [17] S. Tyagi, H. V. Singh, R. Agarwal, and S. K. Gangwar, "International Cnference on Emergind Trends in Electrical Electronics & Sustainable Energy systems," IEEE, 2016.
- [18] S. Pathak, S. Tiwari, and S. Agarwal, "Digital Image Watermarking in Wavelet Domain using chaotic Sequence," International Conference on Futuristic Trends in Engineering, Science, Humanities, and Technology January, Gwalior, 2016.
- [19] Hemani and S. Singh, "A survey of Digital Watermarking Techniques and Performance Evaluation Metrics," International Journal of Engineering Trends and Technology, IJETT, April 2017.

---

## A Hybrid Scrambling Algorithm Using Arnold Transformation and Differential Evolution

R. Jamali Avilaq\*, A. Farzan

\*Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran

(Received: 28/11/2016, Accepted: 09/08/2017)

### ABSTRACT

*Scrambling in exchange of information is an important issue in safeguarding information security. There are many scrambling techniques and combining these algorithms increase the security of scrambling techniques. In this paper, we explain a new scrambling algorithm using combining Differential Evolution and Arnold transformation algorithms. Differential Evolution raises the security and robustness of algorithms because of its optimal responses. In our technique, a digital image is made by scrambling the Arnold transformation with the Differential Evolution algorithm for this scrambled image, so this increases the robustness of scrambling. Experimental results show that the proposed scheme can scramble an image with different other methods and the original image can be extractable from the scrambled image.*

**Keywords:** Digital Image, Scrambling, Arnold Transformation, Differential Evolution

---

\* Corresponding Author Email: Ra2jamali@yahoo.com