مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال ششم، شماره ۱، بهار ۱۳۹۷، ص ۹۳-۸۷

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

رسول جمالی اویلق*[۱]، علی فرزان[۲]

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 ترکیب‌دادن الگوریتم تبدیل آرنولدی 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 به‌روش 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 آرنولدی 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 آرنولدی، تکامل تفاضلی

۱- مقدمه

گسترش روزافزون اینترنت در عصر کنونی، سبب تحول چشمگیری در عرصه ارتباطات دیجیتال شده است. اینترنت به‌عنوان محیطی برای به اشتراک‌گذاشتن 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 همه‌گیرشدن 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 پایمال‌شدن حقوق این مولفان، ضروری به‌نظر 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. رمزنگاری‌کردن این تصاویر یکی از روش‌های حفظ امنیت آن‌ها است. رمزنگاری به مفهوم، دانش تغییردادن اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به‌طوری‌که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمزنگاری‌شده باشد و شخصی که از یکی یا هردوی 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، به‌طوری‌که دسترسی به اطلاعات آن ممکن نباشد [۲-۱]. برای رمزنگاری تصاویر دیجیتال الگوریتم‌های زیادی وجود دارند که از آن جمله می‌توان به تبدیل Fibonacci، تبدیل Biker، تبدیل Affine و ... اشاره کرد. تبدیل آرنولدی یکی از روش‌های رمزنگاری تصاویر دیجیتال است که توسط یک ریاضیدان روسی به نام ولادمیر 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،

* رایانامه نویسنده مسئول: Ra2jamali@yahoo.com

1 -Vladimir Arnold

تصاویر غیرمربعی را نیز می‌توان با این الگوریتم رمزنگاری نمود. این الگوریتم با جابه‌جاکردن پیکسل‌های یک تصویر رمزنگاری را انجام می‌دهد.

الگوریتم تکامل تفاضلی نیز جزو الگوریتم‌های تکاملی است. این الگوریتم‌ها اغلب برای مسائل بهینه‌سازی کاربرد دارند. لیکن به‌دلیل این‌که نحوه تولید یک مجموعه از پاسخ‌ها در این الگوریتم‌ها به یک روش خاصی انجام می‌شود لذا استفاده از این روش‌ها در رمزنگاری تصاویر نیز می‌تواند مفید واقع شود. روش تولید یک مجموعه از پاسخ‌ها در الگوریتم تکامل تفاضلی نسبت به دیگر الگوریتم‌های تکاملی به‌طور کاملاً خاص و منحصربه‌فردی انجام می‌شود که موجب سریع‌ترشدن و امنیت بیشتر این الگوریتم در مقایسه با سایر موارد گردیده است. در این مقاله سعی شده است تا با ترکیب الگوریتم‌های تبدیل آرنولدی و تکامل تفاضلی روشی جدید جهت رمزنگاری تصاویر دیجیتال ارائه گردد. نتایج حاصل از آزمایشات نشان می‌دهند که روش پیشنهادی از قدرت رمزنگاری قوی‌تر و مقاومت بیش‌تری برخوردار است.

۲- تبدیل آرنولدی

این الگوریتم یک فرآیند تکراری جهت رمزنگاری تصاویر است که پیکسل‌ها را از مکانی به مکان دیگر انتقال می‌دهد. این تبدیل بر روی تصاویر مربعی اعمال می‌شود. بدین ترتیب که مختصات یک پیکسل را گرفته و براساس یک الگوریتمی، مختصات جدید جهت انتقال را به‌دست می‌آورد. ساده‌ترین نوع این الگوریتم، تبدیل دوبعدی آن می‌باشد که با استفاده از رابطه زیر حاصل می‌شود:

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

که در آن، (x , y) مکان اولیه یک پیکسل و (x' , y') مکان جدید انتقال‌یافته 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:

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

جهت انتقال برای دومین بار:

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

لذا برای انتقال Kامین بار مختصات هر پیکسل:

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

از رابطه (۴)، این نتیجه حاصل می شود که اگر مختصاتی مانند (x , y) چندین بار از نقطه‌ای به نقطه دیگر انتقال داده شوند، درنهایت، بعد از T بار تکرار این عمل، به مکان اولیه خود باز خواهند گشت. این T به نام دوره تناوب تبدیل گفته می‌شود که وابسته به اندازه تصویر بوده و با استفاده از آن تعیین می شود [۵، ۷ و ۱۰-۹].

۲-۱- رمزنگاری با استفاده از تبدیل آرنولدی

هر تصویر دیجیتال به‌صورت یک ماتریس مربعی دوبعدی نشان داده می‌شود. اگر اندازه تصویر N باشد، اندازه ماتریس آن N×N است. اگر (x , y) مختصات مکان اولیه یک پیکسل مانند p باشد، $((x , y) \in \{۰,۱,۲,۳,...,N-۱\})$ 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 به‌صورت رمزنگاری‌شده درمی‌آید [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 درحال پیچیده‌شدن هستند. بنابراین، الگوریتم‌های بهینه‌سازی با عملکرد بالا مورد نیاز است [۳].

الگوریتم‌های تکاملی راه‌حل خوبی برای مسائل بهینه‌سازی هستند. این الگوریتم‌ها برپایه 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 براساس یک توزیع تصادفی یکنواخت به نحوی انتخاب می‌شود که تمام فضای مسئله را پوشش دهد. سپس در مرحله تکامل، شایستگی افراد درون جمعیت براساس یک تابع شایستگی از پیش تعیین‌شده مشخص می‌شود. در گام بعدی مرحله تکامل، فرزندان جدید با استفاده از دو عمل بازترکیبی و جهش ایجاد می‌شوند. سپس با استفاده از روشی از پیش تعیین‌شده، افراد نسل بعدی از میان والدین و فرزندان انتخاب می‌شوند. این چرخه تا زمانی ادامه می‌یابد که شرط خاتمه الگوریتم برقرار باشد [۳].

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 می‌باشد، اما در الگوریتم تکامل تفاضلی، همه جواب‌ها دارای شانس مساوی جهت انتخاب‌شدن می‌باشند. یعنی شانس انتخاب‌شدن آن‌ها وابسته به مقدار شایستگی آن‌ها نمی‌باشد، پس از این‌که 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 بهتربودن، جایگزین می‌گردد [۳، ۵ و ۱۲-۱۱].

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 می‌شود. در مرحله تکامل، افراد جمعیت از طریق جهش، بازترکیبی و فرایند انتخاب، بارها و بارها بهبود می‌یابند تا زمانی‌که معیار انتخاب خاتمه الگوریتم ارضاء شود [۳].

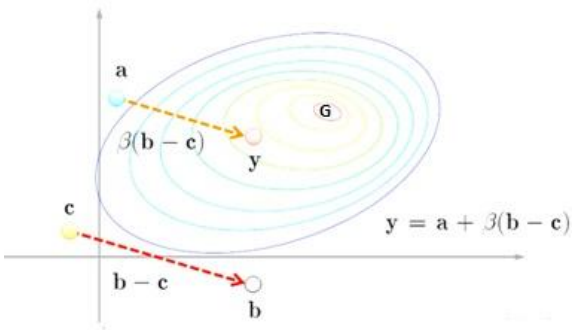
الگوریتم تکامل تفاضلی از دو جهت ترتیب انجام تقاطع و جهش با سایر الگوریتم‌های تکاملی متفاوت است. بدین ترتیب که ابتدا با استفاده از عملگر جهش یک پاسخ موقت تولید می‌شود و سپس با استفاده از عملگر تقاطع، یک پاسخ جدید ایجاد می‌شود. گام و طول جهش نیز از فاصله و تفاضل میان پاسخ‌های موجود در جمعیت ایجاد می‌شوند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

در شکل (۱)، برای رسیدن به نقطه هدف (G)، سه عضوی از جمعیت به‌طور تصادفی انتخاب می‌شوند ($a \neq b \neq c$). تفاضل بین نقاط b و c، یعنی بردار b-c در یک ضریب مقیاس (β) ضرب شده و به a افزوده می‌شود و بدین ترتیب، نقطه y به‌عنوان یک پاسخ موقت جدید حاصل می‌شود. در ادامه این پاسخ موقت با استفاده از عملگر تقاطع با اعضای جمعیت قبلی ترکیب می‌شود. 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 a، b و c با استفاده از عملگر تقاطع با x ترکیب شده و جواب جدیدی به‌نام z حاصل می‌شود [۵ و ۱۲].

$$\left.\begin{matrix} x = (x_1, x_2, x_3, \dots, x_n) \\ y = (y_1, y_2, y_3, \dots, y_n) \end{matrix}\right\} \rightarrow \boldsymbol{z = (z_1, z_2, z_3, \dots, z_n)} \qquad (۵)$$

به‌طوری‌که:

$$y = a + \beta(b - c)$$



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

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

- ابتدا j_0 به‌صورت تصادفی از میان اعداد صحیح ۱ تا n انتخاب می‌شود.
- عدد j_0 به مجموعه J (که در ابتدا خالی است) افزوده می‌شود.
- به ازای تمام مقادیر j از ۱ تا n، عملیات زیر تکرار می‌شوند:
  - یک عدد تصادفی مانند r_j که دارای توزیع یکنواخت در بازه [۰,۱] است تولید می‌شود.
  - اگر r_j کمتر یا مساوی P_{CR} (پارامتر احتمال تقاطع) باشد، عدد j به مجموعه J اضافه می‌شود [۱۲].

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

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 می‌شود. این روش شامل دو مرحله، رمزنگاری و رمزگشایی است.

۴-۱- مرحله اول: رمزنگاری

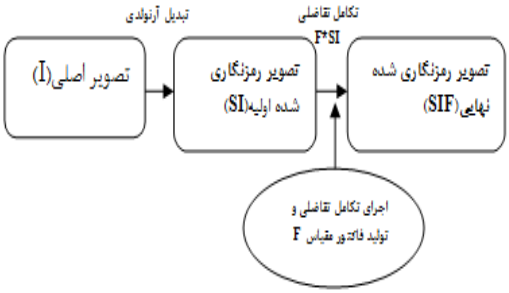
این مرحله شامل سه زیرمرحله به شرح ذیل است:

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

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

۳- جهت افزایش مقاومت و امنیت تصویر رمزنگاری‌شده، این تصویر (SI) در فاکتور مقیاس حاصل از اجرای الگوریتم تکامل تفاضلی (F) ضرب می‌شود که در نهایت، تصویر رمزنگاری‌شده 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 رمزنگاری‌شده درمقابل 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 رمزنگاری‌شده است، زیرا که الگوریتم DE، بهترین فاکتور مقیاس را که به‌صورت 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

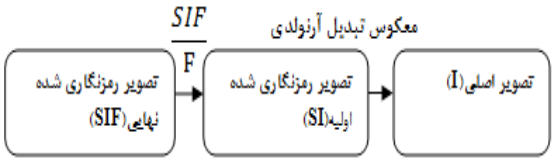
۴-۲- مرحله دوم: رمزگشایی

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

۱- ابتدا تصویر رمزنگاری‌شده نهایی بر مقدار فاکتور مقیاس تکامل تفاضلی تقسیم می‌شود که نتیجه حاصل از این مرحله تصویر رمزنگاری‌شده اولیه (SI) یا همان تصویر رمزنگاری‌شده 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.

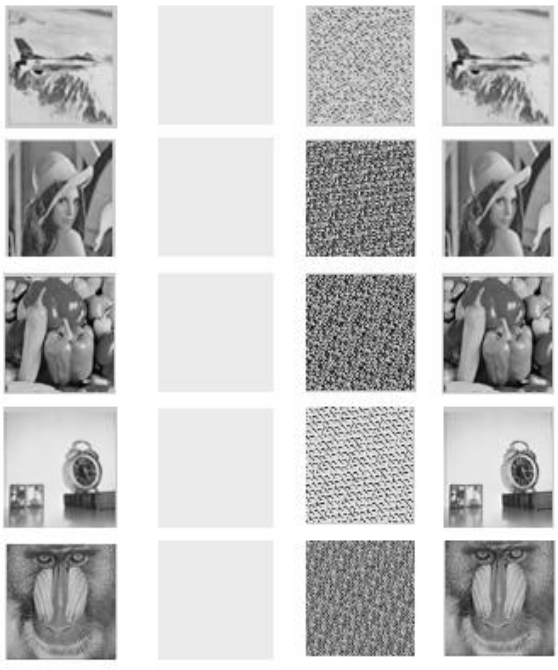
شکل (۳)، گام‌های این مرحله را نشان می‌دهد.



شکل (۳): مراحل رمزگشایی تصویر

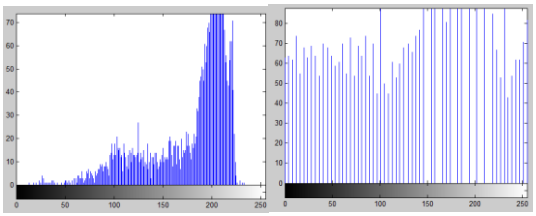
۵- نتایج شبیه‌سازی

برای جلوگیری از انواع حملات مختلف، باید تضمین شود که تصویر اصلی و تصویر رمزنگاری‌شده 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 حاصل‌شده از اعمال روش پیشنهادی بر روی پنج تصویر مختلف (شکل (۴) و تحلیل هیستوگرام هرکدام از آن‌ها (اشکال ۹-۵) آورده شده است.



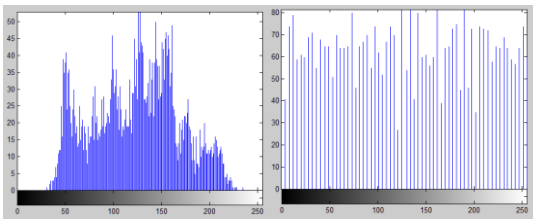
(الف) (ب) (ج) (د)

شکل (۴): الف) تصویر اصلی، ب) تصویر رمزنگاری‌شده با تبدیل آرنولدی، ج) تصویر رمزنگاری‌شده نهایی با روش پیشنهادی، د) تصویر رمزگشایی‌شده



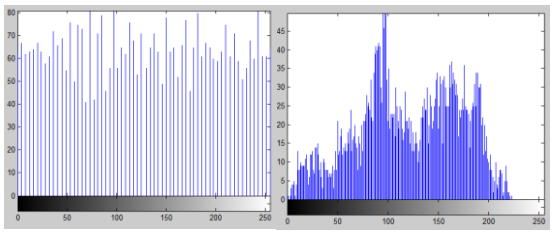
(ب) (الف)

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



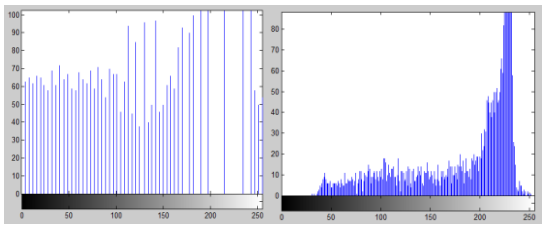
(ب) (الف)

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



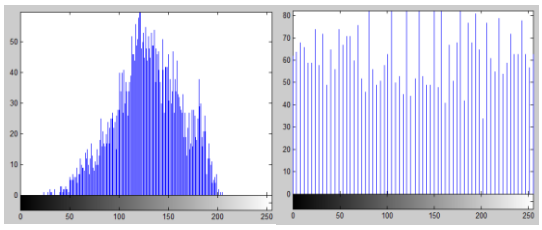
(ب) (الف)

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



(ب) (الف)

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



(ب) (الف)

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

روش پیشنهادی را بر روی تصویرهای مختلف از نوع خاکستری در اندازه های ۶۴×۶۴ اعمال کرده و نتایج تحلیل هیستوگرام هرکدام از آن‌ها و نیز تصاویر رمزنگاری‌شده نهایی با روش پیشنهادی را برای هریک از آن‌ها رسم کردیم. نتایج به‌دست‌آمده نشان می‌دهند که تصاویر رمزنگاری‌شده و تصویر اصلی نسبت به‌هم کاملاً متفاوتند و هیستوگرام تصاویر رمزنگاری‌شده دارای توزیع نسبتاً یکنواختی می‌باشند. علاوه‌بر این، پارامترهای "میانگین مجذور خطا" (MSE[1]) و "بیشترین نسبت تفاوت" (PSNR[2]) دو معیار سنجش کیفیت الگوریتم‌های رمزنگاری بین دو تصویر اصلی و رمزشده هستند که اولی میزان انباشتگی خطا بین دو تصویر اصلی و رمزشده را نشان می‌دهد و هرچقدر مقدار آن کمتر باشد، نشان‌دهنده کیفیت بالاتر آن است. دومی میزان بیشترین نسبت تفاوت بین دو تصویر اصلی و رمزشده را نشان می‌دهد که هرچقدر میزان آن بیشتر باشد، نشان‌دهنده کیفیت بالاتر است [۵ و ۲۴].

جدول‌های (۵-۱) زیر نتایج حاصل‌شده برای این دو پارامتر را جهت مقایسه کیفیت رمزنگاری چندین الگوریتم رمزنگاری با روش پیشنهادی نشان می‌دهند.

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

الگوریتم / معیار	MSE	PSNR
تبدیل آرنولدی	۹۶/۳۵۵۵	۹/۹۸۸۵
تبدیل آرنولدی با الگوریتم زنبورعسل	۱۳/۲۲۹۰	۴۵/۶۹۰۷
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۳/۹۰۷۲	۵/۷۸۰۵
روش پیشنهادی	۰/۳۷۹۶	۳۴/۰۳۳۵

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

الگوریتم / معیار	MSE	PSNR
تبدیل آرنولدی	۱۱۲/۰۶۲۰	۹/۳۳۲۶
تبدیل آرنولدی با الگوریتم زنبورعسل	۵۴/۵۴۸۶	۱۲/۴۵۹۴
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	۹/۲۶۲۴
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

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

الگوریتم / معیار	MSE	PSNR
تبدیل آرنولدی	۹۷/۳۲۴۷	۹/۹۴۵۰
تبدیل آرنولدی با الگوریتم زنبورعسل	۴۸/۳۶۳۸	۱۲/۹۸۲۰
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۲/۳۹۷۷	۵/۸۰۶۴
روش پیشنهادی	۰/۱۹۵۶	۳۶/۹۱۴۵

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

الگوریتم / معیار	MSE	PSNR
تبدیل آرنولدی	۱۰۵/۶۱۳۰	۹/۹۴۵۰
تبدیل آرنولدی با الگوریتم زنبورعسل	۵۱/۷۱۵۳	۱۲/۹۸۲۰
تبدیل آرنولدی با الگوریتم ژنتیک	۲۵۴/۸۲۲۵	۵/۸۰۶۴
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[1])، الگوریتم ازدحام ذرات (PSO[2]) و کلونی زنبور عسل (ABC[3])، به‌علت 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 [۲۳-۲۱].

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 به‌دست‌آمده 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 درمقایسه با سایر الگوریتم‌های تکاملی به‌دلیل استفاده از فاکتور مقیاس چندگانه که به‌صورت یک ماتریس است و نه یک عدد، موجب افزایش مقاومت روش رمزنگاری می‌گردد [۵]. علاوه‌بر این، به‌علت این‌که 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.

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

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.

[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.

[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

Journal of Electronical & Cyber Defence
Vol. 6, No. 1, 2017, Serial No. 21

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