هشتمین کنفرانس بین المللی انجمن رمز ایران
دانشگاه فردوسی مشهد -۲۳ و ۲۴ شهریور ۱۳۹۰

یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی

سید عبدالحمید اصفهانی[۱]، داوود بخشش [۲]

[۱] دانشگاه آزاد اسلامی، واحد قاینات
hamidcom86@gmail.com

[۲] دانشگاه بجنورد ، دانشکده علوم پایه
dbakhshesh@gmail.com

چکیده

هر چند که توابع فوق آشوب[۱] به دلیل پیچیدگی و بزرگ بودن فضای کلید آنها نسبت به دیگر توابع آشوب ، مقاومت بیشتری در مقابل حملات هکرها دارند اما الگوریتم هایی که تنها از توابع فوق کیاس برای رمزنگاری تصویر استفاده می‌کنند از مقاومت کافی در برابر حملات برخوردار نیستند. در این مقاله یک روش جدید جهت رمز کردن تصاویر بر پایه توابع فوق آشوب و عملگر ترکیب ارائه شده است. در این روش ما از قابلیتهای توابع فوق آشوب که شامل حساسیت به مقادیر اولیه ، رفتار شبه تصادفی و غیر تناوبی بودن تابع می باشد ، بهره می گیریم. همچنین استفاده از عملگر ترکیب در ترکیب کردن مقدار پیکسل ها باعث افزایش قدرت الگوریتم در برابر حمله کننده‌ها[۲] می شود. روش ترکیبی در برابر بسیاری از الگوریتم‌های حمله کننده از قدرت و امنیت کافی برخوردار است. علاوه بر این به جهت افزایش امنیت، رمزگذاری تصویر به صورت برداری انجام می شود و ابعاد تصویر نیز به همراه مقادیر پیکسل‌ها رمزگذاری می‌شود. بیشترین نسبت تفاوت (PSNR) بین تصویر رمز شده و تصویر اولیه ۱۱ است این عدد نشان می‌دهد که تصویر رمز شده به اندازه کافی با تصویر اولیه متفاوت است.

کلمات کلیدی

رمزنگاری تصویر ، تابع فوق آشوب ، الگوریتم تکاملی ، عملگر ترکیب ، الگوریتم حمله

۱- مقدمه

در جهان دیجیتال امروزی امنیت تصاویر دیجیتال بیش از پیش اهمیت پیدا کرده است. در سالهای اخیر سرعت زیادی در رشد انتقال تصاویر دیجیتالی از طریق کامپیوتر بویژه اینترنت صورت گرفته است.در بیشتر حالات کانال‌های ارتباطی به اندازه کافی امن نبوده و توسط دزدان و هکرها مورد هجوم قرار می گیرند.بنابراین امنیت و پنهان سازی تصاویر یک امر مهم در فناوری اطلاعات می باشد. روشهای زیادی برای این کار پیشنهاد شده‌اند که روشهای مبتنی بر نظریه آشوب از ویژگی‌های منحصربفردی برخوردار هستند.در اصل سیستمهای آشوبناک [۳] دارای چندین ویژگی هستند که آنها را به عنوان بخش اساسی ساختاردهی سیستم های رمزگذاری تبدیل نموده است.اولین بار در سال ۱۹۸۹ از سیستم آشوب برای رمزنگاری استفاده شد[4] از آن به بعد تحقیقات زیادی جهت ارائه و آنالیز الگوریتم های رمزنگاری بر پایه آشوب ارائه گردیده است این تحقیقات بیشتر ویژگی هایی از آشوب مانند حساس و

وابسته بودن به مقادیر اولیه، شبه تصادفی بودن مقادیرآشوب و غیر تناوبی بودن تابع را مورد بحث قرار داده اند[1,2] در بعضی از الگوریتم های رمزنگاری از ترکیب تابع کیاس با الگوریتم های دیگر استفاده شده است مثلا تابع کیاس با شبکه های عصبی .[13]در سال های اخیر الگوریتم های دیگری که بر اساس توابع کیاس عمل میکنند، ارائه شدند از آن جمله می توان به الگوریتم رمزنگاری سریع[12]، الگوریتم رمزنگاری بلاکی[11] و... اشاره کرد. یک الگوریتم رمزنگاری خوب باید علاوه بر این مسائل، باید نسبت به کلیدهای اشتباه حساس باشد و فضای کلید آن به باید به اندازه کافی بزرگ باشد تا بتواند در مقابل حملات کورکورانه و شدید مقاومت کافی داشته باشد. توابع فوق آشوب [3,4] به دلیل پیچیدگی که در آنها وجود دارد و نیز بزرگ بودن فضای کلید آنها نسبت به توابع آشوب معمولی، مقاومت بیشتری در مقابل حملات هکرها دارند. هرچند که این الگوریتم ها در مقابل حملات کورکورانه مقامت خوبی دارند اما در مقابل دیگر الگوریتم های حمله امنیت کافی برخوردار نیستند روما و بلیت در تحقیق خود نشان دادند که الگوریتم هایی که بر اساس توابع فوق کیاس تصویر را رمز می کنند در مقابل حمله ها مقاوم نیستند.[7] کاربرد عمده الگوریتم های تکاملی در بهینه سازی مقادیر است اما از این الگوریتم در موارد دیگری همچون رمزنگاری استفاده شده است.[5,6] از آن جمله می توان الگوریتم های بهبود یافته پنهان سازی با ژنتیک[۴] را نام برد .این روش به وسیله سیستم (GIC) بهبود یافت. سپس الگوریتم رمزگذاری بر پایه عملگر ترکیب می باشد پیشنهاد شد[7-9] این الگوریتم قدرت توابع کیاس را در رمز کردن تصویر ندارند در الگوریتم های کیاس تصویر رمزشده در مقایسه با تصویر اولیه تفاوت بسیار زیادی دارد و به عبارتی مقدار بیشترین نسبت تفاوت بین تصویر اولیه و کد رمز شده زیاد است که در الگوریتم های تکاملی اینچنین نیست.

در این مقاله سعی شده است تا از ویژگی های هر دو روش یعنی قدرت رمزنگاری توابع فوق آشوب و امنیت الگورتیم ژنتیک استفاده شود.

در روش ارائه شده ابتدا از تصویر اولیه را به یک بردار نگاشت میدهیم سپس این بردار با استفاده از عملگر ترکیب و توابع آشوب رمزگذاری می شود.مقاله ارائه شده شامل بخش های زیر می باشد .در بخش ۲ انواع روش های حمله به یک تصویر رمز شده را شرح می دهیم و در بخش ۳ مراحل الگوریتم پیشنهادی را مرور می کنیمکه شامل تبدیل تصویر به بردار ، رمز گذاری بردار ودر نهایت رمزگشایی تصویر حاصل می باشد ، در بخش ۳ در مورد نتایج آزمایشگاهی الگوریتم پیشنهادی بحث می کنیم و در نهایت در بخش ۴ به بحث و نتیجه گیری مربوط می باشد.

۲- روش‌های حمله

یک الگوریتم حمله کننده سعی می کند تا بر اساس دانش و اطلاعاتی که بدست آورده است تصویر رمز شده را رمزگشایی کند. دانش الگوریتم می تواند مواردی همچون تصویر رمز شده ، دسترسی محدود به مکانیزم رمز نگاری و رمز گشایی باشد ولی این الگوریتم ها هیچ دسترسی به کلید رمز ندارند بدیهی است هرچه دانش و اطلاعات الگوریتم بیشتر باشد رمزگشایی تصویر آسانتر خواهد بود روش های حمله را بر اساس میزان دسترسی به اطلاعات می توان به چهار سطح تقسیم کرد :[7]

۱. الگوریتم هایی که تنها به کد رمز شده تصویر دسترسی دارند
۲. الگوریتم هایی که علاوه بر کد رمز شده تصویر ، به یک یا چند تصویر به همراه کد رمز مربوطه آنها دسترسی دارند
۳. الگوریتم هایی که دسترسی محدود به مکانیزم رمز نگاری تصویر دارند به طوری که می توانند چند تصویر دلخواه را رمز کرده و از کد رمز شده آن استفاده کنند
۴. الگوریتم هایی که دسترسی محدود به مکانیزم رمز گشایی تصویر دارند به طوری که می توانند چند کد رمزتصویر دلخواه را رمزگشایی کرده و تصویر اولیه را بدست آورند.

الگوریتم های دسته اول و دوم به دلیل قدرت کمی که در رمز گشایی دارند بیشتر برای حمله به کد رمزهایی استفاده می شوند که توسط مکانیزم های ساده رمزنگاری شده اند. برای حمله به الگوریتم های رمزنگاری پیچیده تر مانند رمزنگاری با توابع کیاس از الگوریتم‌های طبقه سوم و چهارم استفاده می شود

روما و بلیت در تحقیق خود نشان دادند که الگوریتم هایی که بر اساس توابع فوق کیاس مقدار تصادفی بدست می آورند و آنرا با مقدار پیکسل ها ترکیب می کنند در مقابل حمله ها مقاوم نیستند آنها در تحقیق خود با استفاده از توابع فوق کیاس (برای بدست آوردن مقادیر تصادفی) و عملگر یای انحصاری (جهت ترکیب آن با مقدار هر پیکسل) یک تصویر را رمز نگاری کردند و سپس بدون داشتن کلید تصویر را رمزگشایی کردند

برای این کار آنها ابتدا تصویری را با استفاده از توابع فوق کیاس و عملگر یای انحصاری رمز کردند بدین صورت که برای هر پیکسل مقدار خروجی تابع فوق کیاس را بر ۲۵۶ تقسیم کرده و مقدار باقیمانده آن با مقدار پیکسل مربوطه یای انحصاری می شود سپس با استفاده از دو روش مختلف تصویر اصلی را بدون دسترسی به کلید به دست آوردند.

روش اول با استفاده از دسترسی محدود به الگوریتم رمزنگاری در سه مرحله تصویر اصلی را بازیابی می کند

۱. تصویری هم اندازه تصویر اصلی ولی با مقادیر صفر توسط الگوریتم رمزنگاری ، رمز می شود و کد رمز حاصل(B) را با کد رمز تصویر اصلی(C) توسط یای انحصاری ترکیب می کنیم و حاصل را (P) می نامیم
۲. تصویری هم اندازه تصویر اصلی که مقدار هر پیکسل آن برابر شماره ستون است توسط الگوریتم رمزنگاری ، رمز می شود و کد رمز حاصل(J) را با تصویر(B) را توسط یای انحصاری ترکیب می کنیم و بر اساس ترتیب مقادیر هر سطر مقادیر سطرهای (P) جابجا می شود.
۳. تصویری هم اندازه تصویر اصلی که مقدار هر پیکسل آن برابر شماره سطرآن است توسط الگوریتم رمزنگاری ، رمز می شود و کد رمز حاصل(I) را با تصویر(B) توسط یای انحصاری ترکیب می کنیم و بر اساس ترتیب مقادیر بدست آمده سطرهای (P) جابجا می شود.

جدول شماره (۱) این روش را نشان می دهد. همانطور که در این جدول مشاهده می شود پس از جابجایی سطرها در تصویر P تصویر اصلی بدست می‌آید.

روش دوم برای حمله به تصویر رمز شده تقریبا شبیه به روش اول است با این تفاوت که در این روش الگوریتم حمله کننده دسترسی محدود به الگوریتم رمزگشایی دارد این الگوریتم در سه مرحله تصویر اصلی را بازیابی می شود

۱. تصویری هم اندازه تصویر اصلی ولی با مقادیر صفر توسط مکانیزم رمزگشایی ، رمزگشایی می شود و تصویر حاصل(B) را با کد رمز تصویر اصلی(C) توسط یای انحصاری ترکیب می کنیم و حاصل را (P) می نامیم

۲. تصویری هم اندازه تصویر اصلی که مقدار هر پیکسل آن برابر شماره ستون است توسط الگوریتم رمزنگاری ، رمز می شود و با استفاده از عملگر یای انحصاری کد رمز حاصل(J) را با تصویر(B) ترکیب می کنیم و بر اساس ترتیب مقادیر هر سطر مقادیر سطرهای (P) جابجا می شود.

۳. تصویری هم اندازه تصویر اصلی که مقدار هر پیکسل آن برابر شماره سطرآن است توسط الگوریتم رمزنگاری ، رمز می شود و کد رمز حاصل(I) را با تصویر(B) توسط عملگر یای انحصاری ترکیب می کنیم و بر اساس ترتیب مقادیر بدست آمده سطرهای (P) جابجا می شود.

جدول (۱) : مراحل الگوریتم حمله[7]

$\begin{pmatrix}114&192&86&156\\114&130&130&145\\102&99&76&211\\76&136&218&86\end{pmatrix}$	$\begin{pmatrix}165&226&86&156\\115&203&130&145\\154&56&76&211\\44&24&218&86\end{pmatrix}$	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}233&106&222&60\\21&24&187&255\\24&74&23&205\\176&216&95&182\end{pmatrix}$	$\begin{pmatrix}76&136&218&86\\102&211&76&99\\130&114&130&145\\156&192&86&114\end{pmatrix}$
تصویر اصلی	تصویر رمز شده	تصویر صفر هم اندازه تصویر اصلی(M)	تصویر B تصویر رمز شده M	تصویر P
$\begin{pmatrix}1&2&3&4\\1&2&3&4\\1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}232&104&221&56\\20&28&184&253\\26&75&20&201\\180&218&92&183\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&4&3&2\\2&1&3&4\\4&2&3&1\end{pmatrix}$	$s1=[1\ 2\ 3\ 4]$ $s2=[1\ 4\ 3\ 2]$ $s3=[2\ 1\ 3\ 4]$ $s4=[4\ 2\ 3\ 1]$	$\begin{pmatrix}76&136&218&86\\102&99&76&211\\114&130&130&145\\114&192&86&156\end{pmatrix}$
تصویر هم اندازه تصویر اصلی مقدار هر پیکسل شماره ستون	تصویر J	ترکیب یای انحصاری B و J	ترتیب جابجایی مقادیر هر سطر	تصویر P پس از جابجایی مقادیر هر سطر
$\begin{pmatrix}1&1&1&1\\2&2&2&2\\3&3&3&3\\4&4&4&4\end{pmatrix}$	$\begin{pmatrix}237&110&218&56\\22&27&184&252\\26&72&21&207\\177&217&94&183\end{pmatrix}$	$\begin{pmatrix}4&4&4&4\\3&3&3&3\\2&2&2&2\\1&1&1&1\end{pmatrix}$	$s1=[4\ 3\ 2\ 1]$	$\begin{pmatrix}114&192&86&156\\114&130&130&145\\102&99&76&211\\76&136&218&86\end{pmatrix}$
تصویر هم اندازه تصویر اصلی مقدار هر پیکسل شماره سطر	تصویر I	ترکیب یای انحصاری B و I	ترتیب جابجایی سطرها	تصویر P پس از جابجایی مقادیر هر سطر

۳- رمزنگاری ترکیبی

۳-۱- رمزنگاری

الگوریتم بکار رفته تصویر را در سه مرحله رمز می‌کند در قدم اول ماتریس تصویر به بردار تبدیل می‌شوند این مسئله باعث می‌شود تا اندازه تصویر همراه با مقادیر تصویر رمز شوند در مرحله دوم با استفاده از توابع فوق کیاس دو پیکسل از این بردار انتخاب می‌شود و در مرحله بعد مقادیر این دو پیکسل با استفاده از تابع ترکیب با همدیگر ترکیب می‌شوند. در این روش مقادیر پیکسل ها با همدیگر ترکیب می شوند وبه عبارت دیگر هر پیکسل با پیکسل دیگری در تصویر رمز می شود این مسئله باعث می‌شود تا امنیت الگوریتم در الگوریتم های حمله افزایش یابد.

۳-۱-۱- تبدیل ماتریس تصویر به بردار

یکی از مهمترین مسائلی که در این روش مد نظر قرار گرفته است رمز کردن اندازه تصویر می باشد. بر خلاف روش ها والگوریتم های پیشین که عمل رمزگذاری را تنها بر روی مقادیر پیکسل ها انجام می شد ، در این روش اندازه تصویر نیز به همراه مقادیر پیکسل های موجود درتصویر اولیه رمزگذاری می شود.بدین ترتیب که ما ابتدا ماتریس تصویر را به یک بردار (آرایه یک بعدی) تبدیل می کنیم ،این بردار یک بردار سطری بوده که از کنار هم گذاشتن سطرهای تصویر بدست می‌آید این کار موجب افزایش امنیت در رمزنگاری تصویر می شود.

۳-۱-۲- توابع فوق آشوب

توابع فوق آشوب قابلیتهای چون حساسیت به مقادیر اولیه ، رفتار شبه تصادفی و غیر تناوبی بودن تابع دارند این ویژگی ها باعث اهمیت این تابع در رمزنگاری شده است تابع فوق آشوب با توجه به بزرگ بودن فضای کلید آن نسبت به تابع آشوب معمولی امنیت بالاتری دارد این توابع در زیر آمده است.

$$x_1 = \pi * \sin(x_1 + x_2)$$
$$x_2 = \pi * \cos((x_1 + x_2) * x_3) \qquad (۱)$$
$$x_3 = \pi * \cos(x_2 * x_3)$$

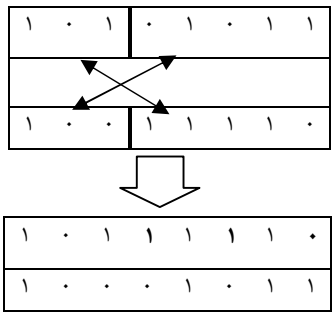
سه عدد x1 , x2 , x3 خروجی توابع فوق آشوب بالا پس از n بار تکرار است این اعداد، اعدادی حقیقی هستند.تابع mod(xi , m) این اعداد را به اعدادی صحیح در بازه [0 m] نگاشت می کنند اگر اندازه تصویر کلید I*J باشد با استفاده از خروجی تابع فوق آشوب و روابط زیر می توان دو پیکسل به آدرس های (p_1) و (p_2) در بردار مشخص کرد و مقدار (p_3) در عملگر ترکیب مورد استفاده قرار می گیرد.

$$p_1 = fix(\mathrm{mod}(abs(x_1 * 1000)), array\_size)$$
$$p_2 = fix(\mathrm{mod}(abs(x_2 * 1000)), array\_size) \quad (۲)$$
$$p_3 = fix(\mathrm{mod}(abs(x_3 * 1000)), 8)$$

بدین ترتیب ما با استفاده از توابع فوق آشوب دو پیکسل از بردار تصویر را جهت عمل رمزگذاری استخراج می کنیم .البته نکته قابل ذکر این است که پیکسل های انتخاب شده از بردار تصویر نباید تکراری باشد، که این هدف نیز با استفاده از توابع فوق آشوب و الگوریتم های خاص قابل دستیابی می باشد.. بعد از انتخاب مقادیر p_1,p_2,p_3 این مقادیر با توجه به کاربرد خاص به تابع ترکیب جهت انجام عمل رمزگذاری و تشکیل بردار رمزگذاری شده داده می شوند.

۳-۱-۳- استفاده از عملگر ترکیب جهت رمزگذاری

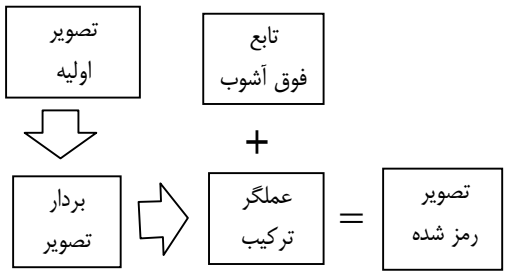
در این مقاله ما از این الگوریتم به شکل متفاوتی استفاده کرده ایم. از انجا که عملگر ترکیب نقش مهمی در بهینه سازی را در الگوریتم ژنتیک بر عهده دارد. اما در اینجا از این عملگر جهت بالا بردن امنیت الگوریتم در مقابل انواع حملات استفاده شده است.این عملگر به شکل های مختلفی از قبیل یک نقطه ای ، دو نقطه ای و... تعریف می شود.در این مقایه ما از روش یک نقطه ای که مورد نظر را با استفاده از توابع فوق آشوب تولید می کنیم ، که همان مقدار p3 تولید شده در مرحله قبل رابطه(۳) است، وعمل ترکیب را بر روی پیکسل های از بردار که توسط مقادیر p1,p2 (والد ها) مشخص شده اند ، انجام می دهیم. از انجایی که تصویر دارای 256 سطح خاکستری می باشد، بنابریان هر پیکسل را می توان توسط 8 بیت نمایش داد . مسئله ای که در اینجا به وجود می آید این است که مقادیر اندازه تصویر که می تواند از ۲۵۶ بزرگتر و فضایی بیش از 8 بیت داشته باشد. . برای حل این مشکل ما برای ذخیره سازی اندازه تصویر از 16 بیت استفاده می کنیم.



شکل (۱)- عمل ترکیب تک نقطه ای

۳-۲- رمزگشایی

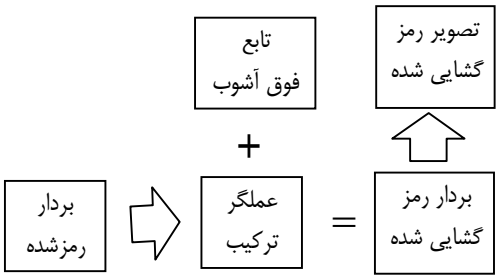
شکل (۲) مراحل رمز نگاری یک تصویر با استفاده از توابع فوق آشوب و تصویر کلید نشان می دهد



شکل (۲)- نمودار کلی مراحل رمزنگاری

الگوریتم رمزگشایی مشابه الگوریتم رمزنگاری است برای این کار ابتدا ابتدا خروجی تابع فوق آشوب رابطه (۱) را پس از n بار تکرار بدست می آوریم با توجه به این مقادیر و رابطه (۲) دو پیکسل از بردار کلید و نقطع تقاطع مشخص میشود حال دوباره عمل ترکیب را تکرار می کنیم تا داده ها تصویر مقادیر اولیه خود را بدست آورند. پس از رمز گشایی بردار با استفاده از دو درایه پایانی بردار که ابعاد تصویر را نشان می دهند تصویر رمزگشایی شده بدست می آید

شکل (۳) مراحل رمز گشایی یک تصویر با استفاده از توابع فوق آشوب و تصویر کلید نشان می دهد



شکل (۳)- نمودار کلی مراحل رمز گشایی

۴- پیاده سازی

جهت بررسی قدرت و استحکام الگوریتم هر تصویر رمزگذاری شده با تصویر رمزگشایی شده از نقطه نظر بیشترین نسبت تفاوت مقایسه گردید.رابطه بیشترین نسبت تفاوت[۵] بین دو تصویر به صورت زیر محاسبه می‌شود.

$$PSNR = 10 * \log\left(\frac{Max}{MSE}\right) \quad (۳)$$

در اینجا Max در واقع ماکزیمم مقدار ممکن پیکسل از هر سطح رنگ می باشد و میانگین مجذور خطا[۶] نیز به صوزت زیرمحاسبه می گردد.

$$MSE = \frac{1}{3mn}\sum_{RGB}\sum_{j=0}^{m-1}\sum_{k=0}^{n-1}\left(E(j,k) - D(j,k)\right)^2 \quad (۴)$$

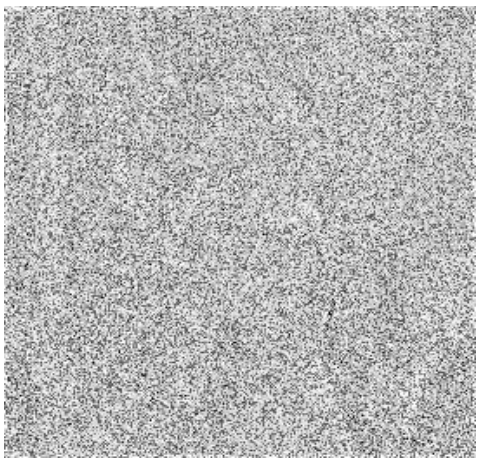
n,m ابعاد تصاویر می باشند.D,E بر لایه رنگی منفردی از تصویر رمزگذاری شده و رمزگشایی دلالت دارند. مقدار بیشترین نسبت تفاوت بین تصویر رمز شده و تصویر اولیه ۱۱ است این عدد نشان می دهد که تصویر رمز شده به اندازه کافی با تصویر اولیه متفاوت است علاوه بر این میانگین مجذور خطا بین تصویری که به درستی رمز شده با تصویر اولیه صفر است

شکل (۴) : تصویر لنا

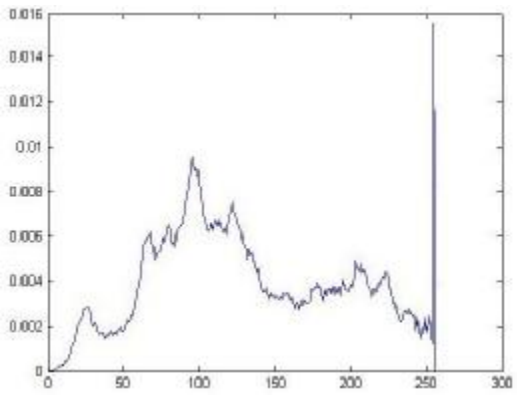
تصاویر رمزگذاری شده تصویر لنا است که در شکل (۴) نشان داده شده است .ابعاد آن ۵۱۲*۵۱۲ می باشد این تصویر توسط تابع فوق آشوب با پارامتر های جدول (۲) رمز شده است حاصل این رمز نگاری در شکل (۵) آمده است

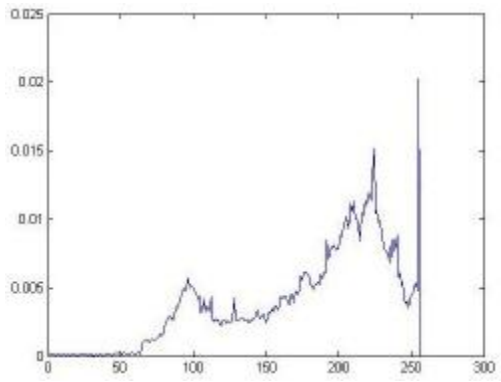
جدول (۲)- مقادیر تابع فوق آشوب

Iteration	x3	x2	x1
10	0.5	0.0004	0.001



شکل (۵) –تصویر رمز شده با الگوریتم پیشنهادی



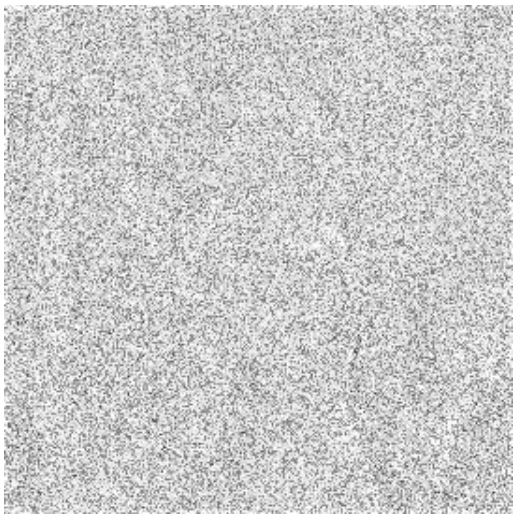


شکل (۶) – الف)هیستوگرام تصویر اصلی
ب) هیستوگرام تصویر رمز شده

در پایان زمانی که یک کلید اشتباه معرفی شد مقدار بیشترین نسبت تفاوت تصویر رمزگذاری شده و تصویر تخریب شده به میزان قابل توجهی تفاوت دارد. تفاوت بین تصویر اولیه و تصویر که به اشتباه رمزنگاری شده است بدین معناست که این الگوریتم به اندازه کافی قدرتمند بوده که بتواند مقابل جزئی ترین تغییرات در پارامترهای کلید مقاومت کند. در حالی که مقایسه بین یک تصویر رمزگذاری شده و تصویر اولیه مقدار میانگین مجذور خطا صفر است.

جدول(۳)- کلید نادرست تابع فوق آشوب مقدار x2 به اندازه ۰,۰۰۰۰۱

Iteration	x3	x2	x1
10	0.5	0.0004۱	0.001



شکل (۷) –رمزنگاری با پارامترهای جدول(۲)

۵- نتیجه گیری

در این مقاله یک روش جهت رمز کردن تصاویر با استفاده از توابع فوق آشوب و عملگر ترکیب مربوط به الگوریتم ژنتیک ارائه گردید. در این روش ما از قابلیتهای توابع فوق آشوب که شامل حساسیت به مقادیر اولیه ، رفتار شبه تصادفی ، بزرگ بودن فضای کلید و غیر تناوبی بودن تابع می باشد بهره گرفته ایم هرچند که این توابع در مقابل حملات کورکورانه مقامت خوبی دارند

اما در مقابل دیگر الگوریتم های حمله امنیت کافی برخوردار نیستند. استفاده از روش های ترکیبی دیگر می تواند امنیت روش را افزیش دهد.این توابع به همراه قابلیتهای بالای عملگرهای تکاملی که می توان از آن جمله به جستجوی عمومی برای بدست آوردن بهینه را نام برد ، بهره می گیریم. عملگر ترکیب در الگوریتم های تکاملی وابسته به مقادیر تصادفی بود ولی در روش پیشنهادی این وابستگی توسط به کارگیری توابع آشوب جهت تولید نقطه تقاطع در عملگر ترکیب از بین می رود. علاوه بر این روش ما برخلاف روش های پیشین دارای این نوآوری و مزیت است که رمزگذاری تصویر را به صورت برداری انجام داده و ابعاد تصویر نیز به همراه مقادیر پیکسل ها رمزگذاری می شود ودر نتیجه امنیت به طور قابل توجهی افزایش می یابد. مقدار بیشترین نسبت تفاوت بین تصویر رمز شده و تصویر اولیه ۱۱ است این عدد نشان می دهد که تصویر رمز شده به اندازه کافی با تصویر اولیه متفاوت است علاوه بر این میانگین مجذور خطا بین تصویری که به درستی رمز شده با تصویر اولیه صفر است و پس از رمز گشایی با کلیدهای صحیح تصویری کاملاً مساوی با تصویر اولیه حاصل می شود اگر هر گونه تغییری در کلید داشته باشیم تصویر را نمی توان به درستی رمز گشایی کرد این تغییر می تواند در کلید تابع آشوب رخ داده باشد.

مراجع

[1] Wang Yong-Ying, Wang Yu-Rong, Wang Yong, Li Hui-Juan, Sun Wen-Jia. Optical image encryption based on binary Fourier transform computer- generated hologram and pixel scrambling technology. Opt Lasers Eng 2007;45:761–5.

[2] Singh N, Sinha A. Optical image encryption using fractional Fourier transform and chaos. Opt Lasers Eng 2008;46(2):117–23.

[3] T.Gao , Z.ChenA “new image encryption algorithm based on hyper-chaos” Physics Letters A 372 (2008) 394–400

[4] R.Valerij. “Symmetry of the modified Mandelbrot set”. Pi in the Sky 2005(9):20–1.

[5] Menzes A. J., Paul, C., Van Dorschot, V.,Vanstone, S. A., “Handbook of AppliedCryptography”, CRS Press 5th Printing; 2001.

[6] National Bureau Standards, “Data Encryption Standard (DES),” FIPS Publication 46; 1977.

[7] Rhouma.R, Belghith.S "Cryptanalysis of a new image encryption algorithm based on hyper-chaos" Physics Letters ,pp. 5973–5978 ,2008

[8] Tragha A., Omary F., Mouloudi A.,”ICIGA:Improved Cryptography Inspired by Genetic Algorithms”, Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.

[9] Mohammed A.F. “Image Encryption Using Genetic Algorithm”. InformationTechnology Journal 5 (3): 516-519, (2006),ISSN 1812-5638.

[10] A Almarimi, A Kumar. “A new aproach for dataencryption using gentic algorithms”

[11] A.Jolfaei ,A.Mirghadri "Image Encryption Using Chaos and Block Cipher", Computer and Information Science, Vol. 4, pp. 172-179, ISSN1913-8989 ,2011.

[12] Liao, X, Chen, G, Wang, Y"A new chaos-based fast image encryption algorithm", Applied Soft Computing Journal, Vol. 1, pp. 514-520, ISSN 1568-4946,2009.

[13] Kadir, Abdurahman; Wang, "A chaotic image encryption algorithm based on perceptron model ", Nonlinear Dynamics, Vol. 62, pp. 615-623, 2011.

---

[1] hyper-chaos
[2] attacks
[3] Chaotic
[4] ICIGA
[5] Peak Signal to Noise Ratio
[6] Mean Square Error