

دریافت مقاله: ۹۳/۵/۲۱

پذیرش مقاله: ۹۳/۷/۱۶

ارائه روشی برای رمزنگاری تصاویر با استفاده از اتوماتای سلولی ترکیبی

زینب مهرنهاد^{۱*}، علی محمد لطیف^۲

^۱ دانشجوی کارشناسی ارشد، دانشکده برق و کامپیوتر، دانشگاه یزد، یزد، ایران

z-mehrnahad@stu.yazd.ac.ir

^۲ استادیار، دانشکده برق و کامپیوتر، دانشگاه یزد، یزد، ایران

alatif@yazd.ac.ir

چکیده: در این مقاله، یک ساختار جدید برای رمزنگاری تصویر با استفاده از اتوماتای سلولی ترکیبی ارائه می‌شود. رمزنگاری تصویر در روش پیشنهادی، در دو مرحله صورت می‌گیرد. در مرحله اول، پیکسل‌های تصویر به ترتیب خوانده شده و هر پیکسل با قوانین اتوماتای سلولی ترکیبی جایگزین می‌شود. در مرحله بعد، پیکسل‌های رمز شده به عدد باینری تبدیل می‌شود. سپس، عمل جایگزینی هر بیت از پیکسل با استفاده از اتوماتای سلولی ترکیبی صورت می‌گیرد. شماره قانون استفاده شده برای هر پیکسل، توسط یک رابطه بازگشتی تعیین می‌شود. بدیهی است مراحل رمزگشایی تصویر با توجه به برگشت پذیری اتوماتای استفاده شده به صورت معکوس قابل اجراء است. نتایج آزمایش‌ها نشان می‌دهد روش پیشنهادی از لحاظ معیارهای کمی نتایج مطلوبی دارد.

واژه‌های کلیدی: رمزنگاری، اتوماتای سلولی برگشت پذیر، اتوماتای سلولی ترکیبی.

۱. مقدمه

پیشرفت سریع در علم ارتباطات و شبکه‌های کامپیوتری و توسعه سیستم‌های رسانه‌های دیجیتال، باعث تحول عظیمی در زندگی بشر شده است. این تحول علاوه بر دارا بودن مزایای فراوان، معایبی نیز دارد. یکی از مشکل‌های موجود سوءاستفاده از رسانه‌های دیجیتال است. به همین دلیل، حفظ امنیت اطلاعات مورد توجه قرار گرفته است. یکی از روش‌های متداول در حفظ امنیت اطلاعات، رمزنگاری است. تاکنون روش‌های زیادی برای رمزنگاری این رسانه‌ها ارائه شده است [۱].

لغت رمزنگاری در زبان انگلیسی معادل کلمه Cryptography است که برگرفته از لغات kryptos به مفهوم «محرمانه» و graphien به معنای «نوشتن» است. علم رمزنگاری بر مبنای مفاهیم و مقدمات اولیه‌ای نظیر تئوری اعداد، اطلاعات و آمار تعریف شده است. در رمزنگاری، ابتدا رسانه با استفاده از عملیات ریاضی برگشت‌پذیر تغییر داده می‌شود و سپس ارسال می‌گردد. در مقصد برای رمزگشایی آن، عملیات معکوس صورت می‌گیرد. کلید رمزنگاری به‌عنوان عنصر اصلی در عملیات رمزنگاری محسوب می‌شود؛ به طوری که بدون داشتن کلید در مقصد، حتی با دانستن الگوریتم رمزنگاری، عملیات معکوس امکان‌پذیر نیست.

امروزه در بین رسانه‌های دیجیتال، تصاویر دیجیتال کاربرد و اهمیت زیادی پیدا کرده‌اند. به همین دلیل، مسئله امنیت برای تصاویر دیجیتال مورد توجه فراوان قرار گرفته است. تصاویر دیجیتال می‌تواند دربرگیرنده اطلاعات تجاری، نظامی، سیاسی یا پزشکی باشند؛ بنابراین، حفظ امنیت اطلاعات در ارسال تصاویر دیجیتال اهمیت زیادی دارد.

الگوریتم‌های رمزنگاری مختلفی برای متن مانند ^۱RSA، ^۲DES ارائه شده است. تفاوت تصاویر با متن، از جمله حجم زیاد داده‌های تصویری و وابسته بودن پیکسل‌ها در تصاویر، باعث می‌شود تا این الگوریتم‌ها برای تصاویر کارآمد

نباشند؛ بنابراین برای تصاویر، روش‌های رمزنگاری ویژه‌ای وجود دارد [۲].

از مهم‌ترین روش‌های رمزنگاری برای تصاویر جابه‌جایی^۳ و جایگزینی^۴ پیکسل‌هاست. روش جابه‌جایی چیدمان پیکسل‌ها در تصویر را تغییر می‌دهد. در این روش، طبق یک رابطه برگشت‌پذیر، موقعیت پیکسل‌ها تغییر می‌کند و تصویر رمز شده به دست می‌آید و در مقصد چیدمان اولیه پیکسل‌ها بازبازی می‌شود. الگوریتم‌هایی مثل تبدیل آرنولد، تبدیل منحنی هیلبرت، دنباله بی‌نظم از این قبیل هستند [۳-۵].

در روش جایگزینی، سطح روشنایی پیکسل‌ها توسط عملیات منطقی و محاسباتی با یک رابطه ریاضی تغییر می‌کند و سپس، در مقصد معکوس عملیات رمزنگاری انجام می‌شود و مقادیر پیکسل‌ها بازبازی می‌شوند [۶ و ۷].

در رمزنگاری پیچیدگی عملیات و نحوه پیاده‌سازی سخت‌افزاری و نرم‌افزاری اهمیت دارد. اتوماتای سلولی با ویژگی‌های ذاتی خود مانند امکان پردازش موازی، یک ریختی، غیرقابل پیش‌بینی بودن رفتار آن و پیاده‌سازی ساده گزینه مناسبی برای رمزنگاری تصویر است.

اتوماتای سلولی در دهه ۴۰ میلادی توسط Von Neumann ارائه شد [۸]. بعد از آن، تحقیق‌های گسترده‌ای روی اتوماتای سلولی صورت گرفت. در سال‌های اخیر، از اتوماتای سلولی در رمزنگاری [۹ و ۱۰]، پردازش تصویر [۱۱ و ۱۲] و امنیت اطلاعات [۱۳] استفاده شده است.

در این مقاله، رمزنگاری تصویر با استفاده از اتوماتای سلولی ترکیبی^۵ ارائه می‌شود. ساختار تعریف‌شده شامل دو مرحله رمزنگاری شامل رمزنگاری پیکسل‌های تصویر و مرحله دیگر، رمزنگاری بیت‌های رمز شده حاصل از مرحله اول توسط اتوماتای سلولی ترکیبی است. در واقع، ساختار ارائه‌شده با روش جایگزینی هم‌زمان در سطح بیتی و هم در سطح پیکسل‌ها می‌تواند رمزنگاری تصویر را به خوبی انجام دهد. گفتنی است ساختار پیشنهادی با توجه به برگشت‌پذیر بودن

3. Scrambling
4. Substitution
5. Hybrid Cellular Automata

1. Rivest-Shamir-Adleman (RSA)
2. Data Encryption Standard (DES)

قوانین استفاده شده در اتوماتای سلولی، برگشت پذیر است و با انجام هریک از مراحل به صورت معکوس، رمزگشایی تصویر انجام می شود.

ساختار مقاله به فرم زیر است. در بخش دوم، به معرفی اتوماتای سلولی ترکیبی پرداخته می شود. در بخش بعد، روش پیشنهادی توضیح داده می شود، سپس در بخش چهارم، نتایج حاصل از اجرای الگوریتم نشان داده می شود و در بخش پایانی، نتیجه گیری لازم ارائه می شود.

۲.۱. مروری بر کارهای گذشته

تاکنون روش های رمزنگاری زیادی ارائه شده است. در این روش ها سعی شده است تا الگوریتم رمزنگاری تصاویر را به گونه ای رمز کند تا قابل مشاهده برای دیگران نباشند و به راحتی قابل رمزگشایی نباشند؛ برای مثال، یکی از روش های مورد استفاده روش مبتنی بر توابع آشوب است [۳، ۶ و ۷].

اتوماتای سلولی یکی دیگر از انواع سیستم های دینامیکی است که امروزه به طور گسترده و موفقیت آمیزی، در ارائه روش های قدرتمند رمزنگاری استفاده می شود. اتوماتای سلولی به دلیل خاصیت تصادفی و رفتار پیچیده و غیر قابل پیش بینی که دارد، برای رمزنگاری کارآمد است.

در سال ۲۰۰۸ میلادی، Ruisong روشی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی معرفی کرد. او ابتدا با استفاده از اتوماتای سلولی، دنباله ای از اعداد تصادفی تولید کرد و سپس، درهم ریزی تصویر را با استفاده از این اعداد انجام داد [۱۴].

در سال ۲۰۱۳ میلادی، FaselQadir و همکارانش روش قبل را با اندکی تغییر مورد استفاده قرار دادند [۱۵]. شایان ذکر است روش های درهم ریزی تصویر به دلیل عدم تغییر هیستوگرام، امنیت بالایی ندارند.

در سال ۲۰۱۲ میلادی، Jin روشی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی به روش جایگزینی پیکسل ها معرفی کرد [۱۶]. این روش دارای خاصیت تناوبی بود. تناوبی بودن به این معنی که با استفاده از چندین قانون متوالی

به صورت چرخشی می توان به تصویر اصلی دست یافت. در نتیجه، با اجرای یک تناوب کامل الگوریتم رمزگشایی انجام می شود.

در سال ۲۰۱۳ میلادی، Abdo و همکارانش روشی بر مبنای جایگزینی پیکسل ها ارائه کردند. در این روش، از اتوماتای سلولی با استفاده از خاصیت تناوبی استفاده شد [۱۷]. در این روش، حلقه هایی از قوانین برگشت پذیر تشکیل می شود و سپس با استفاده از عدد تصادفی حلقه ای از قوانین انتخاب می گردد و بر روی تصویر اعمال می شود تا تصویر رمز شده به دست آید. در هر دو روش مذکور [۱۶ و ۱۷] با توجه به تناوبی بودن الگوریتم، احتمال حمله و رمزگشایی تصویر وجود دارد.

در روش پیشنهادی، از اتوماتای سلولی ترکیبی استفاده شده است. با توجه به اینکه اتوماتای سلولی ترکیبی از قوانین متعددی برای رمزنگاری استفاده می کند، امکان شناسایی این تعداد قوانین مشکل است؛ بنابراین، حمله و رمزگشایی آن سخت تر است.

۲. اتوماتای سلولی

اتوماتای سلولی یک مدل ریاضی برای سیستم های دینامیکی گسسته است که از تعدادی سلول تشکیل شده است. این سلول ها در کنار یکدیگر یک شبکه را تشکیل می دهند که این شبکه می تواند دارای ابعاد مختلفی باشد.

اتوماتای سلولی دارای ۴ مؤلفه به فرم $CA = \{C, S, V, F\}$ است. مؤلفه C نشان دهنده سلول اتوماتا و S نشان دهنده حالت سلول است. مؤلفه V نشان دهنده ابعاد اتوماتا و نوع همسایگی می باشد. مؤلفه F قوانین انتقال اتوماتای سلولی است. در هر زمان، سلول وضعیت خود را براساس شماره قانون انتقال تغییر می دهد. قوانین انتقال چگونگی تغییر حالت سلول را مشخص می کنند. این تغییر بستگی به حالت فعلی سلول و حالت سلول های همسایگانش دارد [۸ و ۱۸].

وضعیت $t-1$ و سطر دوم مربوط به لحظه t است. حال با توجه به شماره قانون می‌توان حالت سلول را برای لحظه بعد تعیین کرد. در این روش، دو قانون برای اتوماتا در نظر گرفته می‌شود. یکی از قوانین R_1 و دیگری $R_2 = 2^n - R_1 - 1$ است. این موضوع برای دو قانون 30 و 225 در سطر سوم شکل ۲ نشان داده شده است.

نمونه‌ای از عملکرد اتوماتای سلولی برگشت‌پذیر با قانون 30 در شکل ۳ نشان داده شده است. سطر اول بردار ورودی و سطر دوم تکرار بردار است. طبق شکل ۲، با داشتن بردار در دو زمان t و $t-1$ حالت بعدی سلول‌ها مشخص می‌شود. سطرهای بعدی را می‌توان به همین ترتیب تولید کرد. برای برگشت‌پذیری اتوماتا سطر چهارم (زمان $t-1$) را بعد از سطر پنجم (زمان t) قرار داده و قوانین اتوماتای برگشت‌پذیر طبق شکل ۲ اعمال می‌شود. به این ترتیب، برگشت‌پذیری صورت می‌گیرد و بردار اولیه حاصل می‌شود. در شکل ۳، مراحل برگشت‌پذیری با رنگ خاکستری نشان داده شده است.

۲.۲. اتوماتای سلولی ترکیبی

اتوماتای سلولی ترکیبی عملکردی مشابه اتوماتای سلولی یکنواخت و معمولی دارد. تنها تفاوت آن داشتن قوانین مختلف برای هر سلول است. در این نوع اتوماتا می‌توان قانون با شماره متفاوتی را برای هر سلول در نظر گرفت و با توجه به آن، حالت بعدی هر سلول را تعیین کرد؛ برای مثال، برای یک سلول قانون 30 تعیین‌کننده حالت‌های بعدی و برای سلول دیگری قانون 90 تعیین‌کننده حالت بعدی و برای سلول‌های دیگر نیز قوانین مشخصی در نظر گرفته می‌شود.

اگر قوانین برای تمام سلول‌های اتوماتا یکسان باشد، اتوماتا یکنواخت و در غیر این صورت غیریکنواخت نامیده می‌شود [۲۱]. اتوماتای سلولی ترکیبی را به نام اتوماتای سلولی غیریکنواخت نیز می‌شناسند. نتیجه این کار به‌عنوان رفتار جدیدی از اتوماتای سلولی شناخته می‌شود.

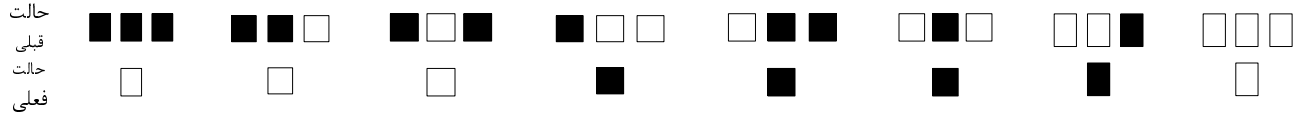
نمونه‌ای از اتوماتای سلولی شامل همسایگی یک‌بعدی و حالت مرزی تناوبی با قانون انتقال 30 در شکل ۱ نشان داده شده است. سطر اول هشت حالت ممکن برای سلول‌ها با همسایگی شعاع یک و سطر دوم حالت بعدی هر سلول را نشان می‌دهد. بدیهی است عدد 30 به‌صورت باینری در ردیف دوم قرار داده شده است. برای رمزنگاری با استفاده از اتوماتای سلولی ابتدا حالت سلول با همسایگی‌ها مشخص شده، سپس حالت بعد با توجه به شماره قانون مشخص می‌شود و جایگزین حالت قبلی سلول می‌شود؛ برای مثال، در جدول ۱ اگر پیکسل سیاه با ۱ و پیکسل سفید با ۰ نشان داده شود و بردار اولیه برای ورودی اتوماتا به‌صورت $[1\ 1\ 0\ 1\ 0\ 1\ 1\ 0]$ در نظر گرفته شود، برای اجرای قانون شماره 30 و همسایگی سه‌تایی برای تعیین حالت بعدی به شیوه زیر عمل می‌شود.

با توجه به همسایگی سه‌تایی، سه پیکسل اول $[1\ 1\ 0]$ انتخاب می‌شود. با توجه به قانون (شکل ۱) حالت بعدی ۱ در نظر گرفته می‌شود. به همین ترتیب، برای سه پیکسل بعد $[1\ 0\ 1]$ قانون اعمال شده و حالت بعدی سلول صفر می‌شود. این روند برای پیکسل‌های بعدی ادامه دارد. برای پیکسل اول و آخر نیز حالت مرزی تناوبی در نظر گرفته می‌شود. روند کلی تا ۳ مرحله در جدول ۱ نشان داده شده است.

۱.۲. اتوماتای سلولی برگشت‌پذیر

در اتوماتای سلولی برگشت‌پذیر، با داشتن هر حالت فعلی می‌توان به حالت اولیه آن دسترسی پیدا کرد. به این معنی که اتوماتای برگشت‌پذیر بر مبنای محاسبات دقیق می‌تواند عقب‌گرد کند؛ بنابراین، تمام مراحل قابل ردیابی و بازگشت‌پذیر است [۸، ۱۹ و ۲۰].

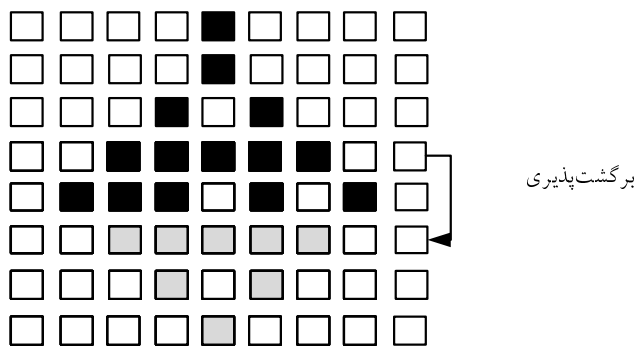
در اتوماتای سلولی برگشت‌پذیر برای تعیین حالت بعدی اتوماتا به وضعیت فعلی و یک لحظه قبل از آن، یعنی t و $t-1$ احتیاج می‌باشد. برای هر سلول اتوماتا در لحظه $t-1$ دو حالت صفر و یک وجود دارد. همچنین، در لحظه t برای همسایگی با شعاع یک، هشت حالت می‌توان تعریف کرد. این دو لحظه در شکل ۲ نشان داده شده است. سطر اول مربوط به



شکل (۱): اتوماتای سلولی با قانون ۳۰

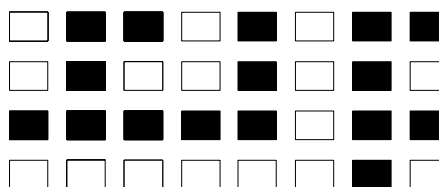
جدول (۱): روند عملکرد اتوماتای سلولی با قانون ۳۰

سطر اول								
دسته‌بندی سه تایی پیکسل‌ها	حالت بعدی							
خروجی مرحله اول								
دسته‌بندی سه تایی پیکسل‌ها	حالت بعدی							
خروجی مرحله دوم								
دسته‌بندی سه تایی پیکسل‌ها	حالت بعدی							
خروجی مرحله سوم								
مرحله قبل (t-1)	مرحله فعلی (t)	مرحله بعد (t+1)						
مرحله قبل (t-1)	مرحله فعلی (t)	مرحله بعد (t+1)						



شکل (۲): اتوماتای سلولی برگشت پذیر با قانون ۳۰

خروجی مرحله سوم



شکل (۳): عملکرد اتوماتای سلولی برگشت پذیر

ترکیبی توسط فرمول (۱) تولید می شود. در این مرحله، x_0 به عنوان کلید اولیه رمزنگاری در نظر گرفته می شود.

۲. هر پیکسل از تصویر با یکی از قوانین تولید شده طبق عملکرد اتوماتای سلولی برگشت پذیر رمز می شود.

۳. در مرحله دوم پیکسل های رمز شده به باینری تبدیل می شوند. ۸ قانون جدید نیز با استفاده از رابطه (۱) تولید می شود.

۴. هر کدام از بیت های این رشته باینری با یکی از قوانین تولید شده رمزنگاری می شوند. بیت ها در کنار یکدیگر قرار داده می شوند. شایان ذکر است این کار برای تمام پیکسل ها صورت می گیرد و تصویر رمز شده تولید می شود.

در مرحله رمزگشایی، مراحل فوق به صورت معکوس اعمال می شود. با استفاده از تصویر رمز شده، پیکسل های ماتریس رمز خوانده می شوند و با توجه به مقدار اولیه x_0 و تابع بازگشتی استفاده شده می توان قوانین را تولید کرد. سپس از قوانین تولید شده به عنوان کلید اتوماتای سلولی برگشت پذیر استفاده شده و پیکسل های رمز شده طبق معکوس الگوریتم رمز، رمزگشایی می شوند. مراحل ۱ تا ۴ همراه با یک مثال در جدول ۲ نشان داده شده است.

۳. روش پیشنهادی برای رمز تصویر

روش پیشنهادی برای رمز تصویر براساس عملکرد اتوماتای سلولی ترکیبی است. در ابتدا تابع زیر برای تعیین شماره قانون تعریف می شود.

$$f(x_{n+1}) = 1 - 2(x_n)^2 \quad x_n \in [-1, +1] \quad (1)$$

با استفاده از این تابع و کلید اولیه x_0 که در نظر گرفته می شود، به تعداد پیکسل های تصویر اصلی قانون اتوماتا تولید شده و برای هر پیکسل متناظر با قانون تولید شده رمزنگاری صورت می گیرد؛ برای مثال، با کلید $0/6$ ، 5 خروجی به صورت $[0/6 \ 28 \ 0/8 \ 32 \ 0/4 \ 22 \ 0/0 \ 6 \ 39]$ به دست می آید. برای تبدیل این 5 خروجی به قوانین اتوماتا ابتدا این اعداد گرد شده و در 100 ضرب می شوند. در نتیجه، خروجی به صورت $[64 \ 42 \ 84 \ 28 \ 60]$ می شود و از این قوانین برای رمزنگاری پیکسل ها نظیر به نظیر استفاده می شود.

در روش پیشنهادی، طی دو مرحله، رمزنگاری تصویر صورت می گیرد. مراحل رمزنگاری در زیر توضیح داده شده است.

۱. ابتدا با توجه به اندازه تصویر، قوانین اتوماتای سلولی

جدول (۲): مثالی از عملکرد روش پیشنهادی

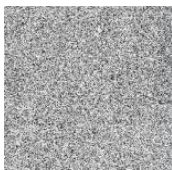
ورودی اولیه	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 5px;">10</td> <td style="padding: 5px;">20</td> </tr> </table>	10	20
10	20		
کلید اولیه $X_0=0.6$	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 5px;">60</td> <td style="padding: 5px;">28</td> </tr> </table>	60	28
60	28		
رمزنگاری اتوماتای سلولی برگشت‌پذیر (مرحله اول)			
رمزنگاری هر بیت با قانون متناظرش توسط اتوماتای سلولی برگشت‌پذیر (مرحله دوم)			
خروجی نهایی	<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 5px;">68</td> <td style="padding: 5px;">134</td> </tr> </table>	68	134
68	134		

۴. نتایج رمزنگاری

نتایج حاصل از اجرای الگوریتم بر روی تصویر cameraman و boats با اندازه 256×256 با کلیدهای متفاوت در ادامه نشان داده شده است. شکل‌های ۵ تا ۷ تصویر اصلی، تصویر رمز شده و تصویر رمزگشایی شده با کلیدهای $0/6$ ، $0/7$ و $0/8$ را به ترتیب نشان می‌دهد. برای نمونه، در شکل ۵ ابتدا کلید $x_0 = 0/6$ در نظر گرفته شده است. سپس به اندازه سایز تصویر cameraman، قانون اتوماتای سلولی تولید شده است. پیکسل‌های تصویر به ترتیب، با قانون متناظرشان رمز شدند. نحوه رمزنگاری مطابق عملکرد اتوماتای سلولی برگشت‌پذیر است. بعد از یک دوره رمز کردن تمام پیکسل‌های تصویر با همان کلید اولیه، ۸ قانون تولید می‌شود. در مرحله بعد، هر کدام از پیکسل‌ها به رشته باینری تبدیل شده و هر بیت با قانون متناظر رمز می‌شود. این مرحله نیز برای تمام پیکسل‌ها اجرا شده و در نهایت، تصویر رمز شده به دست می‌آید. برای نشان دادن حساسیت الگوریتم به کلید در شکل (۸) سعی شده است که تصویر رمز شده با کلید $0/6$ را با کلید دیگری رمزگشایی کرد. همان‌گونه که مشاهده می‌شود رمزگشایی به صورت صحیح انجام نشده و تصویر کاملاً نامفهوم است. در شکل‌های ۹ تا ۱۱ این الگوریتم بر روی تصویر boats اعمال شده و نتایج نشان داده شده است.



الف. تصویر اصلی



ب. تصویر رمز شده

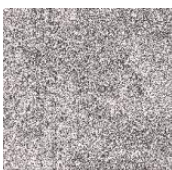


ج. تصویر رمزگشایی شده

شکل (۵): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۶



الف. تصویر اصلی



ب. تصویر رمز شده

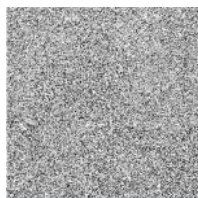


ج. تصویر رمزگشایی شده

شکل (۶): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۷



الف. تصویر اصلی

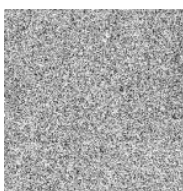


ب. تصویر رمز شده

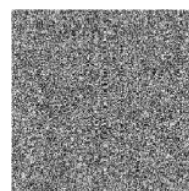


ج. تصویر رمزگشایی شده

شکل (۷): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۸



ب. تصویر رمزگشایی با کلید ۰/۴

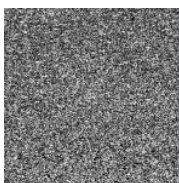


الف. تصویر رمز شده با کلید ۰/۷

شکل ۸: نتایج خروجی الگوریتم در رمزگشایی با کلید نادرست



ج (تصویر رمزگشایی شده)

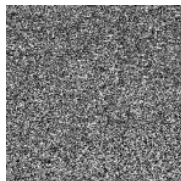


ب (تصویر رمز شده)



الف (تصویر اصلی)

شکل (۹): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۶

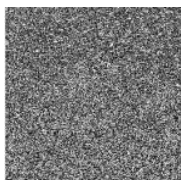


ج) تصویر رمزگشایی شده

ب) تصویر رمز شده

الف) تصویر اصلی

شکل (۱۰): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۷



ج) تصویر رمزگشایی شده

ب) تصویر رمز شده

الف) تصویر اصلی

شکل (۱۱): نتایج خروجی الگوریتم پیشنهادی با کلید ۰/۸

$$\text{Cov}(x,y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j^2) \quad (5)$$

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

در این روابط، X و Y روشنایی دو پیکسل همسایه در تصویر و M×N تعداد پیکسل‌های تصویر است.

۷. تمایز تصویر اصلی و رمز شده

یک خاصیت ایدئال برای تصویر رمز، حساس بودن نسبت به تغییرهای جزئی در تصویر اصلی است. در حمله‌های تفاضلی^۲، مهاجم تلاش می‌کند با ایجاد یک تغییر کوچک در تصویر، تغییر حاصل در تصویر رمز را مشاهده کند و به این ترتیب، رابطه بین تصویر اصلی و رمز آشکار شود. با این کار می‌توان کلید را شناسایی کرد. سه معیار ارزیابی دیگر UACI^۳، NPCR^۴، MAE^۵ است. بدیهی است توابع ذکر شده، توابع استاندارد برای محاسبه میزان تشابه دو تصویر هستند [۲۲] و

۵. تحلیل و ارزیابی روش پیشنهادی

در مراجع گذشته برای ارزیابی روش پیشنهادی چندین آزمون پیشنهاد شده است [۱۶ و ۱۷]. در این مقاله، سعی شده است تا آزمون‌های معرفی شده بر روی روش پیشنهادی به همراه دو روش Jin و Abdo بررسی شود.

۶. تحلیل آماری

یکی از معیارهای ارزیابی برای تحلیل آماری^۱، همبستگی است. هرچه همبستگی پیکسل‌های همسایه در تصویر رمز شده کمتر باشد، عملکرد الگوریتم مطلوب‌تر است [۱۹]. معیار همبستگی در رابطه (۲) بیان شده است.

$$r_{xy} = \frac{\text{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (2)$$

$$D(x) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j^2) \quad (3)$$

$$D(y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j^2) \quad (4)$$

2. Differential Attack
3. Unified Average Changing Intensity (UACI)
4. Mean Absolute Error (MAE)
5. Number of Pixel Change Rate (NPCR)

1. Statistical Analysis

در جدول (۴) مقادیر تابع ارزیابی برای الگوریتم معرفی شده در این مقاله نشان داده شده است. در جدول (۵)، مقادیر توابع ارزیابی برای الگوریتم‌های معرفی شده در [۱۶] و [۱۷] با الگوریتم پیشنهادی نشان داده شده است. همان‌طور که در جدول مشاهده می‌شود، این مقادیر برای روش پیشنهادی نسبت به دو روش دیگر بیشترین مقدار را دارد؛ یعنی به‌زای تغییر یک پیکسل در تصویر ورودی بیشترین میزان تغییر در خروجی ایجاد شده است.

جدول (۴): معیارهای ارزیابی برای تصویر cameraman			
MAE	NPCR	UACI	الگوریتم
۳۹/۵۷۷۲	۴۹/۳۰۵۷	۱۵/۰۱۵۱	تصویر رمز مرجع [۱۶]
۳۸/۶۳۵۹	۴۹/۴۲۳۲	۱۳/۸۲۴۶	تصویر رمز مرجع [۱۷]
۶۷/۳۰۳۵	۶۷/۸۶۵۰	۳۲/۳۹۵۴	تصویر رمز روش پیشنهادی

همان‌طور که در جدول مشاهده می‌شود، این مقادیر برای روش پیشنهادی زیاد است؛ یعنی به‌زای تغییر یک پیکسل در تصویر ورودی، تغییر زیادی در خروجی ایجاد می‌شود.

۸. مقاومت در برابر حملات متن معلوم و متن انتخابی

در حمله متن اصلی معلوم، متن رمز معلوم^۱ دشمن سعی دارد تا با داشتن جفت متن اصلی و رمز شده با کلیدهای یکسان، متن اصلی را کشف کند. در حمله متن انتخابی^۲، دشمن این توانایی را دارد که متن انتخابی را رمز کند تا بتواند به تصاویر رمز شده دیگر این الگوریتم دست یابد. در روش پیشنهادی فضای کلید برابر با $256^{m \times n}$ است که در آن،

[۲۳]. هر چه این سه مقدار بیشتر باشند، الگوریتم رمزنگاری عملکرد مطلوب‌تری دارد.

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i, j) - P(i, j)| \quad (6)$$

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i, j)}{M \times N} \times 100 \% \quad (7)$$

$$D(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j) \\ 1 & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases} \quad (8)$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{|C(i, j) - \bar{C}(i, j)|}{255} \right] \times 100 \% \quad (9)$$

در جدول (۳)، نتایج روش پیشنهادی با دو روش معرفی شده در [۱۶] و [۱۷] مقایسه شده است.

با توجه به اعداد جدول می‌توان مشاهده کرد همان‌طور که انتظار می‌رود همبستگی پیکسل‌های تصویر اصلی زیاد است. در تصاویر رمز شده، این میزان کمتر شده و پیکسل‌ها وابستگی کمتری نسبت به یکدیگر دارند. در روش پیشنهادی، این مقدار نسبت به دو روش دیگر کمتر بوده و این نشان می‌دهد که ساختار معرفی شده نسبت به دو روش مورد بررسی، عملکرد بهتری دارد.

جدول (۳): مقادیر میزان همبستگی در راستای افقی، عمودی و قطری برای تصویر cameraman

تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز مرجع [۱۶]	-۰/۰۳۶۹	-۰/۰۳۸۳	-۰/۰۱۱۴
تصویر رمز مرجع [۱۷]	۰/۰۱۲۲	۰/۰۱۴۹	-۰/۰۱۷۸
تصویر رمز روش پیشنهادی	۰/۰۱۷۷	۰/۰۰۲۲	۰/۰۰۶۵

1. Known Plain-Text Attack
2. Chosen Plain-Text Attack

در این مقاله، روش جدیدی برای رمزنگاری تصویر معرفی شد که در دو مرحله، به رمزنگاری تصویر می‌پردازد. بدیهی است با توجه به برگشت‌پذیری اتوماتای سلولی مراحل رمزگشایی قابل اجراست. نتایج اعمال این الگوریتم بر روی تصاویر cameraman و boats توسط توابع ارزیابی مانند $UACI$ ، MAE ، $NPCR$ مقایسه شده است. نتایج نشان می‌دهد که این روش توانایی مناسبی برای رمزنگاری اطلاعات دارد. همچنین با استفاده از اتوماتای سلولی برگشت‌پذیر و اتوماتای سلولی ترکیبی، از قوانین متعدد و مختلفی برای هر پیکسل استفاده شده است که این فضای کلید بزرگ عمل رمزگشایی و شناسایی کلید را مشکل‌تر می‌سازد.

$m*n$ سایز تصویر اصلی است؛ بنابراین، فضای کلید بسیار بزرگ است. همچنین در تابع استفاده‌شده برای تولید قوانین از تابعی استفاده شده که در هر تکرار، مقادیر مختلفی تولید می‌کند. بنابراین با توجه به فضای کلید و تصادفی بودن آن، امکان حمله ضعیف است و این روش در مقابل دو حمله متن اصلی معلوم، متن رنژ معلوم و متن انتخابی مقاوم است.

۹. نتیجه‌گیری

اتوماتای سلولی یک ابزار مفید برای رمزنگاری است. با توجه به خاصیت تصادفی بودن اتوماتای سلولی، می‌توان تصویر را به خوبی و با کیفیت بالا رمز کرد. اتوماتای سلولی برگشت‌پذیر نیز این قابلیت را دارد تا بتوان روش‌های رمزنگاری برگشت‌پذیر بر روی تصویر را معرفی کرد.

مراجع

- [1] D. Van De Ville, W. Philips, R. Van de Walle, and I. Lemahieu, "Image scrambling without bandwidth expansion," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 6, pp. 892-897, 2004.
- [2] G. Ye, X. Huang, and C. Zhu, "Image encryption algorithm of double scrambling based on ASCII code of matrix element," International Conference on Computational Intelligence and Security, pp. 843-847, 2007.
- [3] Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solitons & Fractals, Elsevier, Vol. 29, No. 2, pp. 393-399, 2006.
- [4] J. Lv, J. Lu, and S. Chen, "Chaotic time series analysis and its application," Publishing house of Wuhan university, Wuhan, pp. 57-66, 2002.
- [5] W. Ding, W. Q. Yan, and D. X. Qi, "Digital image scrambling technology based on Arnold transformation," Journal of Computer Aided Design & Computer Graphics, Chines Academy of Science, Vol. 4, No. 13, pp. 338-341, 2001.
- [6] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, Elsevier, Vol. 24, No. 9, pp. 926-934, 2006.
- [7] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," Physics Letters A, Elsevier, Vol. 346, No. 1-3, pp. 153-157, 2005.
- [8] J. Von Neumann, "Theory of self-reproducing automata," University of Illinois Press, 1966.
- [9] J. Jin and Z. h. Wu, "A secret image sharing based on neighborhood configurations of 2-D cellular automata," Optics & Laser Technology, Elsevier, Vol. 44, No. 3, pp. 538-548, 2012.
- [10] Z. Eslami, S. Razzaghi and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," Pattern Recognition, Elsevier, Vol. 43, No. 1, pp. 397-404, 2010.
- [11] P. L. Rosin, "Image processing using 3-state cellular automata," Computer Vision and Image Understanding, Elsevier, Vol. 114, No. 7, pp. 790-802, 2010.
- [12] C. Kauffmann and N. Piché, "Seeded ND medical image segmentation by cellular automaton on GPU," International Journal of Computer Assisted Radiology and Surgery, Springer, Vol. 5, No. 3, pp. 251-262, 2010.
- [13] Z. Eslami and J. Z. Zarepour Ahmadabadi, "A verifiable multi-secret sharing scheme based on

- cellular automata*," Information Sciences, Elsevier, Vol. 180, No. 15, pp. 2889-2894, 2010.
- [14] Y. Ruisong and L. Huiliang, "A novel image scrambling and watermarking scheme based on cellular automata," International Symposium on Electronic Commerce and Security, pp. 938-941, 2008.
- [15] F. Qadir, M. Peer, and K. Khan, "Digital image scrambling based on two dimensional cellular automata," International Journal of Computer Network & Information Security, MECS Publisher, Vol. 5, No. 2, pp. 36-41, 2013.
- [16] J. Jin, "An image encryption based on elementary cellular automata," Optics and Lasers in Engineering, Elsevier, Vol. 50, No. 12, pp. 1836-1843, 2012.
- [17] A. Abdo, S. Lian, I. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," Communications in Nonlinear Science and Numerical Simulation, Elsevier, Vol. 18, No. 1, pp. 136-147, 2013.
- [18] S. Wolfram, "Theory and Application of Cellular Automata." Singapore: World scientific Publishing, 1986.
- [19] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," Communications in Nonlinear Science and Numerical Simulation, Elsevier, Vol. 18, No. 11, pp. 3075-3085, 2013.
- [20] T. Toffoli and N. H. Margolus, "Invertible cellular automata: A review," Physica D: Nonlinear Phenomena, Elsevier, Vol. 45, pp. 229-253, 1990.
- [21] M. Esnaashari and M. Meybodi, "A novel clustering algorithm for wireless sensor networks using irregular cellular learning automata," in International Symposium on Telecommunications, pp. 330-336, 2008.
- [22] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," Communications in Nonlinear Science and Numerical Simulation, Elsevier, Vol. 17, No. 7, pp. 2943-2959, 2012.
- [23] A. Jolfaei, and A. Mirghadri, "Survey: image encryption using Salsa20," International Journal of Computer Science Issues, Vol. 7, No. 5, pp. 213-220, 2010.