نشریه علمی- ترویجی محاسبات نرم

شمارهٔ پنجم/ بهار و تابستان ۹۳/ صفحهٔ ۵۰-۶۱

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 مرحلهٔ اول، پیکسل‌های تصویر به‌ترتیب خوانده شده و هر پیکسل با قوانین اتوماتای سلولی ترکیبی جایگزین می‌شود. در مرحلهٔ بعد، پیکسل‌های رمزشده به عدد باینری تبدیل می‌شود. سپس، عمل جایگزینی هر بیت از پیکسل با استفاده از اتوماتای سلولی ترکیبی صورت می‌گیرد. شمارهٔ قانون استفاده‌شده برای هر پیکسل، توسط یک رابطه بازگشتی تعیین می‌شود. بدیهی است مراحل رمزگشایی تصویر با توجه به برگشت‌پذیری اتوماتای استفاده‌شده به‌صورت معکوس قابل اجراست. نتایج آزمایش‌ها نشان می‌دهد روش پیشنهادی از لحاظ معیارهای کمّی نتایج مطلوبی دارد.

واژه‌های کلیدی: رمزنگاری، اتوماتای سلولی برگشت‌پذیر، اتوماتای سلولی ترکیبی.

۱. مقدمه

پیشرفت سریع در علم ارتباطات و شبکه‌های کامپیوتری و توسعهٔ 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 کلمهٔ Cryptography است که برگرفته از لغات kryptos به مفهوم «محرمانه» و graphien به‌معنای «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 ریاضیِ 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؛ به‌طوری‌که 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، مسئلهٔ امنیت برای تصاویر دیجیتال مورد توجه فراوان قرار گرفته است. تصاویر دیجیتال می‌تواند دربرگیرندهٔ اطلاعات تجاری، نظامی، سیاسی یا پزشکی باشند؛ بنابراین، حفظ امنیت اطلاعات در ارسال تصاویر دیجیتال اهمیت زیادی دارد.

الگوریتم‌های رمزنگاری مختلفی برای متن مانند RSA[1]، DES[2] 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[3] و جایگزینی[4] پیکسل‌هاست. روش جابه‌جایی چیدمان پیکسل‌ها در تصویر را تغییر می‌دهد. در این روش، طبق یک رابطهٔ برگشت‌پذیر، موقعیت پیکسل‌ها تغییر می‌کند و تصویر رمز شده به‌دست می‌آید و در مقصد چیدمان اولیه پیکسل‌ها بازیابی 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 رابطهٔ ریاضی تغییر می‌کند و سپس، در مقصد معکوس عملیات رمزنگاری انجام می‌شود و مقادیر پیکسل‌ها بازیابی می‌شوند [٦ و ٧].

در رمزنگاری پیچیدگی عملیات و نحوهٔ 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 دههٔ ٤٠ میلادی توسط Von Newmann 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[5] ارائه می‌شود. ساختار تعریف‌شده شامل دو مرحلهٔ رمزنگاری شامل رمزنگاری پیکسل‌های تصویر و مرحلهٔ دیگر، رمزنگاری بیت‌های رمزشده حاصل از مرحلهٔ 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 به‌خوبی انجام دهد. گفتنی است ساختار پیشنهادی با توجه به برگشت‌پذیر بودن

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

3. Scrambling
4. Substitution
5. Hybrid Cellular Automata

قوانین استفاده‌شده در اتوماتای سلولی، برگشت‌پذیر است و با انجام هریک از مراحل به‌صورت معکوس، رمزگشایی تصویر انجام می‌شود.

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

۲.۱. مروری بر کارهای گذشته

تاکنون روش‌های رمزنگاری زیادی ارائه شده است. در این روش‌ها سعی شده است تا الگوریتم رمزنگاری تصاویر را به‌گونه‌ای رمز کند تا قابل مشاهده برای دیگران نباشند و به‌راحتی قابل رمزگشایی نباشند؛ برای مثال، یکی از روش‌های مورد استفاده روش مبتنی بر توابع آشوب است [۳، ٦ و ۷].

اتوماتای سلولی یکی دیگر از انواع سیستم‌های دینامیکی است که امروزه به‌طور گسترده و موفقیت‌آمیزی، در ارائهٔ روش‌های قدرتمند رمزنگاری استفاده می‌شود. اتوماتای سلولی به‌دلیل خاصیت تصادفی و رفتار پیچیده و غیرقابل پیش‌بینی 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، دنباله‌ای از اعداد تصادفی تولید کرد و سپس، درهم‌ریزی تصویر را با استفاده از این اعداد انجام داد [١٤].

در سال ۲۰۱۳ میلادی، FaselQadir و همکارانش روش قبل را با اندکی تغییر مورد استفاده قرار دادند [۱۵]. شایان ذکر است روش‌های درهم‌ریزی تصویر به‌دلیل عدم تغییر هیستوگرام، امنیت بالایی ندارند.

در سال ۲۰۱۲ میلادی، Jin روشی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی به روش جایگزینی پیکسل‌ها معرفی کرد [١٦]. این روش دارای خاصیت تناوبی بود. تناوبی بودن به این معنی که با استفاده از چندین قانون متوالی به‌صورت چرخشی می‌توان به تصویر اصلی دست یافت. در نتیجه، با اجرای یک تناوب کامل الگوریتم رمزگشایی انجام می‌شود.

در سال ۲۰۱۳ میلادی، Abdo و همکارانش روشی بر مبنای جایگزینی پیکسل‌ها ارائه کردند. در این روش، از اتوماتای سلولی با استفاده از خاصیت تناوبی استفاده شد [۱۷]. در این روش، حلقه‌هایی از قوانین برگشت‌پذیر تشکیل می‌شود و سپس با استفاده از عدد تصادفی حلقه‌ای از قوانین انتخاب می‌گردد و بر روی تصویر اعمال می‌شود تا تصویر رمزشده به‌دست آید. در هر دو روش مذکور [١٦ 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 می‌کند، امکان شناسایی این تعداد قوانین مشکل است؛ بنابراین، حمله و رمزگشایی آن سخت‌تر است.

۲. اتوماتای سلولی

اتوماتای سلولی یک مدل ریاضی برای سیستم‌های دینامیکی گسسته است که از تعدادی سلول تشکیل شده است. این سلول‌ها در کنار یکدیگر یک شبکه را تشکیل می‌دهند که این شبکه می‌تواند دارای ابعاد مختلفی باشد.

اتوماتای سلولی دارای ٤ مؤلفه به فرم $CA = \{C, S, V, F\}$ است. مؤلفه C نشان‌دهندهٔ سلول اتوماتا و S نشان‌دهندهٔ حالت سلول است. مؤلفهٔ V نشان‌دهندهٔ ابعاد اتوماتا و نوع همسایگی می‌باشد. مؤلفهٔ F قوانین انتقال اتوماتای سلولی است. در هر زمان، سلول وضعیت خود را براساس شمارهٔ قانون انتقال تغییر می‌دهد. قوانین انتقال چگونگی تغییر حالت سلول را مشخص می‌کنند. این تغییر بستگی به حالت فعلی سلول و حالت سلول‌های همسایگانش دارد [۸ و ۱۸].

نمونه‌ای از اتوماتای سلولی شامل همسایگی یک‌بعدی و حالت مرزی تناوبی با قانون انتقال ۳۰ 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 ۳۰ 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 شمارهٔ 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 [۰ ۱ ۱ ۰ ۱ ۱ ۰ ۱] در نظر گرفته شود، برای اجرای قانون شماره ۳۰ و همسایگی سه‌تایی برای تعیین حالت بعدی به شیوهٔ زیر عمل می‌شود.

با توجه به همسایگی سه‌تایی، سه پیکسل اول [۰ ۱ ۱] انتخاب می‌شود. با توجه به قانون (شکل ۱) حالت بعدی ۱ در نظر گرفته می‌شود. به همین ترتیب، برای سه پیکسل بعد [۱ ۱ ۰] 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 اولیهٔ 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].

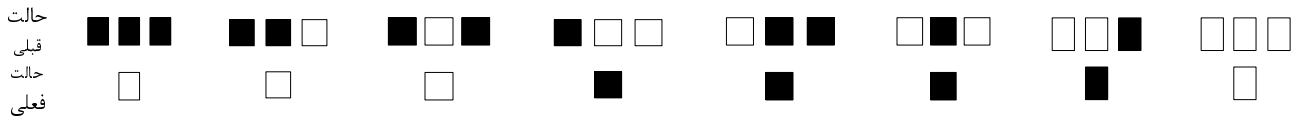
در اتوماتای سلولی برگشت‌پذیر برای تعیین حالت بعدی اتوماتا به وضعیت فعلی و یک لحظه قبل از آن، یعنی t و $t-1$ احتیاج می‌باشد. برای هر سلول اتوماتا در لحظهٔ $t-1$ دو حالت صفر و یک وجود دارد. همچنین، در لحظهٔ t برای همسایگی با شعاع یک، هشت حالت می‌توان تعریف کرد. این دو لحظه در شکل ۲ نشان داده شده است. سطر اول مربوط به وضعیت $t-1$ و سطر دوم مربوط به لحظه t است. حال با توجه به شمارهٔ قانون می‌توان حالت سلول را برای لحظهٔ 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 ۳۰ و ۲۲۵ در سطر سوم شکل ۲ نشان داده شده است.

نمونه‌ای از عملکرد اتوماتای سلولی برگشت‌پذیر با قانون ۳۰ 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

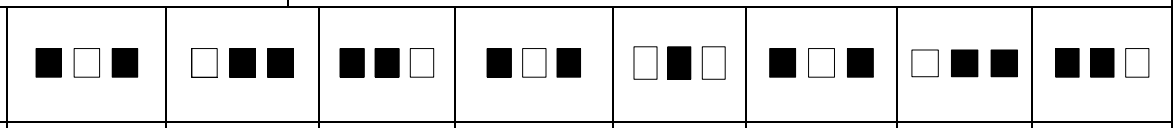
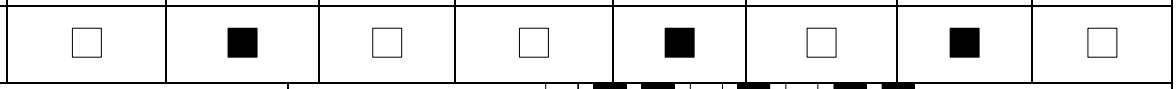
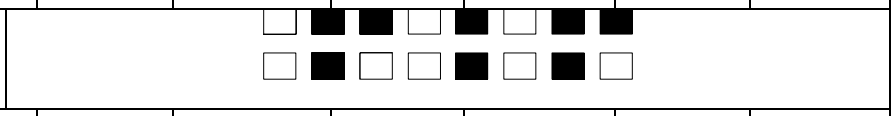
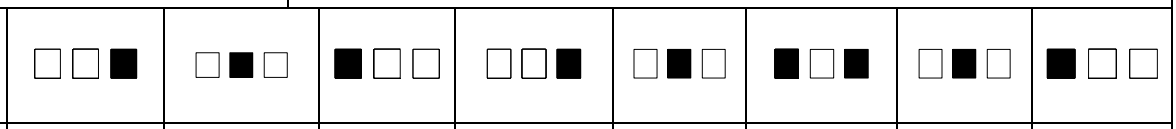
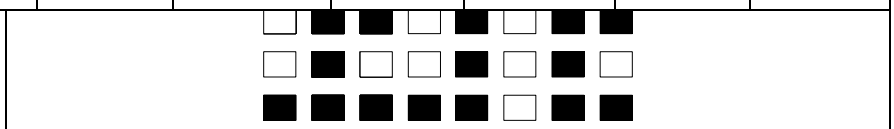
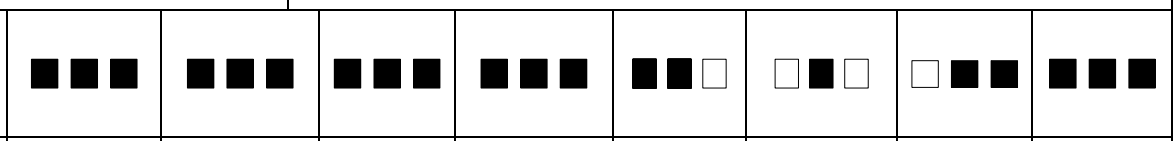
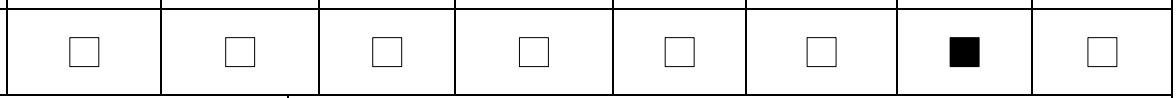
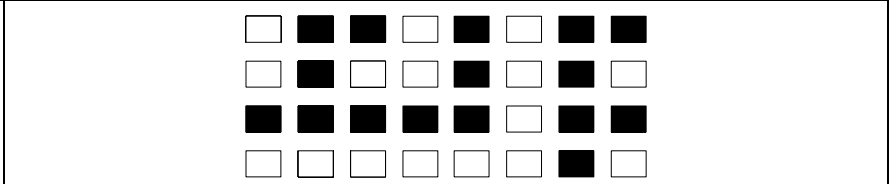
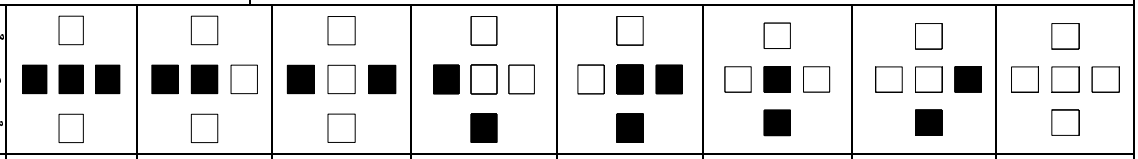
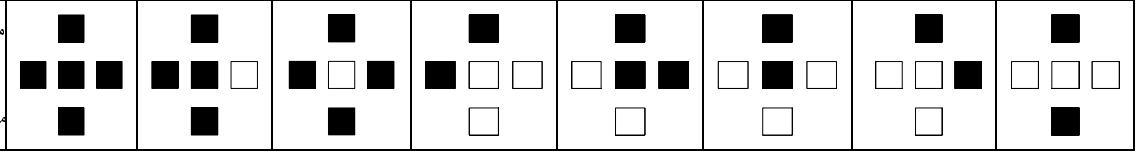
اتوماتای سلولی ترکیبی عملکردی مشابه اتوماتای سلولی یکنواخت و معمولی دارد. تنها تفاوت آن داشتن قوانین مختلف برای هر سلول است. در این نوع اتوماتا می‌توان قانون با شمارهٔ متفاوتی را برای هر سلول در نظر گرفت و با توجه به آن، حالت بعدی هر سلول را تعیین کرد؛ برای مثال، برای یک سلول قانون ۳۰ تعیین‌کنندهٔ حالت‌های بعدی و برای سلول دیگری قانون ۹۰ تعیین‌کنندهٔ حالت بعدی و برای سلول‌های دیگر نیز قوانین مشخصی در نظر گرفته می‌شود.

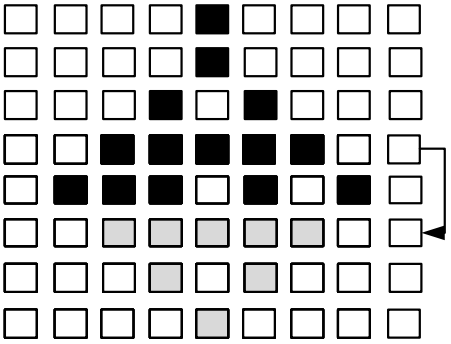
اگر قوانین برای تمام سلول‌های اتوماتا یکسان باشد، اتوماتا یکنواخت و در غیر این صورت غیریکنواخت نامیده می‌شود [۲۱]. اتوماتای سلولی ترکیبی را به نام اتوماتای سلولی غیریکنواخت نیز می‌شناسند. نتیجهٔ این کار به‌عنوان رفتار جدیدی از اتوماتای سلولی شناخته می‌شود.



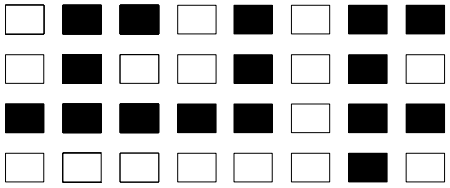
شکل (۱): اتوماتای سلولی با قانون ۳۰

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

سطر اول								
دسته‌بندی سه‌تایی پیکسل‌ها								
حالت بعدی								
خروجی مرحله اول								
دسته‌بندی سه‌تایی پیکسل‌ها								
حالت بعدی								
خروجی مرحله دوم								
دسته‌بندی سه‌تایی 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 برگشت‌پذیر با قانون ۳۰



شکل (۳): عملکرد اتوماتای سلولی برگشت‌پذیر

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 می‌شود.

$$f(x_{n+1}) = 1 - 2(x_n)^2 \qquad x_n \in [-1,+1] \qquad (۱)$$

با استفاده از این تابع و کلید اولیهٔ x_0 که در نظر گرفته می‌شود، به تعداد پیکسل‌های تصویر اصلی قانون اتوماتا تولید شده و برای هر پیکسل متناظر با قانون تولیدشده رمزنگاری صورت می‌گیرد؛ برای مثال، با کلید ۰/٦ ، ۵ خروجی به‌صورت [۰/٦ ۰/۲۸ ۰/۸٤۳۲ ۰/٤۲۲۰۰- ۰/٦٤۳۹] به‌دست می‌آید. برای تبدیل این ۵ خروجی به قوانین اتوماتا ابتدا این اعداد گرد شده و در ۱۰۰ ضرب می‌شوند. در نتیجه، خروجی به‌صورت [٦۰ ۲۸ ٤۲ ۸٤ ٦٤] می‌شود و از این قوانین برای رمزنگاری پیکسل‌ها نظیر به نظیر استفاده می‌شود.

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

۱. ابتدا با توجه به اندازهٔ تصویر، قوانین اتوماتای سلولی ترکیبی توسط فرمول (۱) تولید می‌شود. در این مرحله، x_0 به‌عنوان کلید اولیه رمزنگاری در نظر گرفته می‌شود.

۲. هر پیکسل از تصویر با یکی از قوانین تولید شده طبق عملکرد اتوماتای سلولی برگشت‌پذیر رمز می‌شود.

۳. در مرحلهٔ دوم پیکسل‌های رمزشده به باینری تبدیل می‌شوند. ۸ قانون جدید نیز با استفاده از رابطهٔ (۱) تولید می‌شود.

٤. هر کدام از بیت‌های این رشته باینری با یکی از قوانین تولید شده رمزنگاری می‌شوند. بیت‌ها در کنار یکدیگر قرار داده می‌شوند. شایان ذکر است این کار برای تمام پیکسل‌ها صورت می‌گیرد و تصویر رمزشده تولید می‌شود.

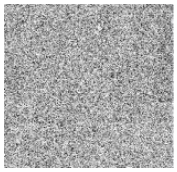
در مرحلهٔ رمزگشایی، مراحل فوق به‌صورت معکوس اعمال می‌شود. با استفاده از تصویر رمزشده، پیکسل‌های ماتریس رمز خوانده می‌شوند و با توجه به مقدار اولیه x_0 و تابع بازگشتی استفاده‌شده می‌توان قوانین را تولید کرد. سپس از قوانین تولیدشده به‌عنوان کلید اتوماتای سلولی برگشت‌پذیر استفاده شده و پیکسل‌های رمزشده طبق معکوس الگوریتم رمز، رمزگشایی می‌شوند. مراحل ۱ تا ٤ همراه با یک مثال در جدول ۲ نشان داده شده است.

جدول (۲): مثالی از عملکرد روش پیشنهادی

ورودی اولیه	10 20
کلید اولیه X_0=0.6	قوانین تولیدشده متناظر با هر پیکسل: 60 28
رمزنگاری پیکسل‌ها با قانون متناظرشان توسط اتوماتای سلولی برگشت‌پذیر (مرحله اول)	10 → Cellular automata R=60 → 228؛ 20 → Cellular automata R=28 → 195
رمزنگاری هر بیت با قانون متناظرش توسط اتوماتای سلولی برگشت‌پذیر (مرحله دوم)	228 → 1 1 1 0 0 1 0 0؛ R1=60 R2= 28 R3= 84 R4=42 R5=64 R6= 17 R7= 94 R8= 77؛ 0 1 0 0 0 1 0 0 → 68؛ 195 → 1 1 0 0 0 0 1 1؛ R1=60 R2= 28 R3= 84 R4=42 R5=64 R6=17 R7= 94 R8= 77؛ 1 0 0 0 0 1 1 0 → 134
خروجی نهایی	68 134

۴. نتایج رمزنگاری

نتایج حاصل از اجرای الگوریتم بر روی تصویر cameraman و boats با اندازهٔ ۲۵۶×۲۵۶ با کلیدهای متفاوت در ادامه نشان داده شده است. شکل‌های ۵ تا ۷ تصویر اصلی، تصویر رمزشده و تصویر رمزگشایی‌شده با کلیدهای ۰/۶، ۰/۷ و۰/۸ را به‌ترتیب نشان می‌دهد. برای نمونه، در شکل ۵ ابتدا کلید x_0 =۰/۶ در نظر گرفته شده است. سپس به اندازهٔ سایز تصویر cameraman، قانون اتوماتای سلولی تولید شده است. پیکسل‌های تصویر به‌ترتیب، با قانون متناظرشان رمز شدند. نحوهٔ 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 مرحلهٔ بعد، هر کدام از پیکسل‌ها به رشتهٔ باینری تبدیل شده و هر بیت با قانون متناظر رمز می‌شود. این مرحله نیز برای تمام پیکسل‌ها اجرا شده و در نهایت، تصویر رمزشده به‌دست می‌آید. برای نشان دادن حساسیت الگوریتم به کلید در شکل (۸) سعی شده است که تصویر رمزشده با کلید ۰/۶ را با کلید دیگری رمزگشایی کرد. همان‌گونه که مشاهده می‌شود رمزگشایی به‌صورت 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.

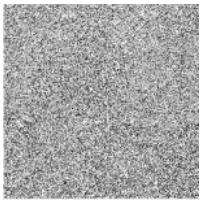

الف. تصویر اصلی ب. تصویر رمزشده ج. تصویر رمزگشایی‌شده

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



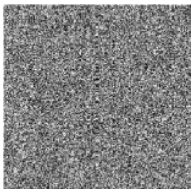
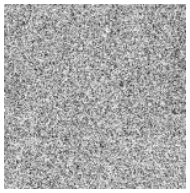
الف. تصویر اصلی ب. تصویر رمزشده ج. تصویر رمزگشایی‌شده

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

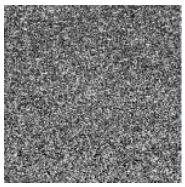

الف. تصویر اصلی ب. تصویر رمزشده ج. تصویر رمزگشایی شده

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

الف. تصویررمزشده با کلید ۰/۷ ب. تصویر رمزگشایی با کلید ۰/٤

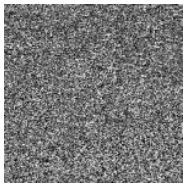
شکل ۸: نتایج خروجی الگوریتم در رمزگشایی با کلید نادرست


الف) تصویراصلی ب) تصویر رمزشده ج) تصویررمزگشایی‌شده

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

الف) تصویر اصلی

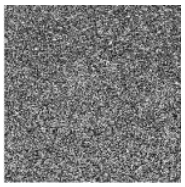


ب) تصویر رمزشده

ج) تصویر رمزگشایی‌شده

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

الف) تصویر اصلی



ب) تصویر رمزشده

ج) تصویر رمزگشایی‌شده

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

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 معرفی‌شده بر روی روش پیشنهادی به همراه دو روش Jin و Abdo بررسی شود.

۶. تحلیل آماری

یکی از معیارهای ارزیابی برای تحلیل آماری،[1] همبستگی است. هرچه همبستگی پیکسل‌های همسایه در تصویر رمزشده کمتر باشد، عملکرد الگوریتم مطلوب‌تر است [۱۹]. معیار همبستگی در رابطهٔ (۲) بیان شده است.

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۲)$$

$$D(x) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j^2) \qquad (۳)$$

$$D(y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j^2) \qquad (۴)$$

1. Statistical Analysis

$$Cov(x,y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j^2) \sum_{j=1}^{M \times N} (y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j^2) \qquad (۵)$$

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

۷. تمایز تصویر اصلی و رمزشده

یک خاصیت ایدئال برای تصویر رمز، حساس بودن نسبت به تغییرهای جزئی در تصویر اصلی است. در حمله‌های تفاضلی،[2] مهاجم تلاش می‌کنند با ایجاد یک تغییر کوچک در تصویر، تغییر حاصل در تصویر رمز را مشاهده کند و به این ترتیب، رابطهٔ بین تصویر اصلی و رمز آشکار شود. با این کار می‌توان کلید را شناسایی کرد. سه معیار ارزیابی دیگر UACI،[3] NPCR،[4] MAE[5] است. بدیهی است توابع ذکرشده، توابع استاندارد برای محاسبهٔ میزان تشابه دو تصویر هستند [۲۲ و

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

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

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i,j) - P(i,j)| \quad (٦)$$

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\ \% \quad (٧)$$

$$D(i,j) = \begin{cases} 0 & if \quad C_1(i,j) = C_2(i,j) \\ 1 & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \quad (٨)$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{|C(i,j) - \bar{C}(i,j)|}{255} \right] \times 100\% \quad (٩)$$

در جدول (۳)، نتایج روش پیشنهادی با دو روش معرفی‌شده در [۱٦ 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 رمزشده، 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 معرفی‌شده 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	۰/۰۰٦۵

در جدول (٤) مقادیر تابع ارزیابی برای الگوریتم معرفی‌شده در این مقاله نشان داده شده است. در جدول (۵)، مقادیر توابع ارزیابی برای الگوریتم‌های معرفی‌شده در [۱٦ 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 به‌ازای تغییر یک پیکسل در تصویر ورودی بیشترین میزان تغییر در خروجی ایجاد شده است.

جدول (۴): معیارهای ارزیابی برای تصویر cameraman

الگوریتم	UACI	NPCR	MAE
تصویر رمز مرجع[۱۶]	۱۵/۰۱۵۱	۴۹/۳۰۵۷	۳۹/۵۷۷۲
تصویر رمز مرجع[۱۷]	۱۳/۸۲۴۶	۴۹/۴۲۳۲	۳۸/۶۳۵۹
تصویر رمز روش پیشنهادی	۳۲/۳۹۵۴	۶۷/۸۶۵۰	۶۷/۳۰۳۵

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

۸. مقاومت در برابر حملات متن معلوم و متن انتخابی

در حملهٔ متن اصلی معلوم، متن رمز معلوم،[1] دشمن سعی دارد تا با داشتن جفت متن اصلی و رمزشده با کلیدهای یکسان، متن اصلی را کشف کند. در حملهٔ متن انتخابی،[2] دشمن این توانایی را دارد که متن انتخابی را رمز کند تا بتواند به تصاویر رمزشدهٔ دیگر این الگوریتم دست یابد. در روش پیشنهادی فضای کلید برابر با ٢٥٦^{m*n} است که در آن،

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

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 حملهٔ متن اصلی معلوم، متن رنز 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 به‌خوبی 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.

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 قابل‌اجراست. 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.

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. Wolframe, "*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.