رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر

زینب مهرنهاد و علی‌محمد لطیف

دانشکدهٔ برق و مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

چکیده

در این مقاله یک ساختار جدید برای رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر ارائه شده است. رمزنگاری تصویر در روش پیشنهادی در سه مرحلهٔ جداگانه صورت می‌گیرد. در مرحلهٔ نخست تصویر بلوک‌بندی می‌شود و سپس مقادیر روشنایی پیکسل‌ها با استفاده از اتوماتای سلولی برگشت‌پذیر جایگزین می‌شوند. درهم‌ریزی تصویر در مرحلهٔ دوم با اتوماتای دیگری انجام می‌شود و سپس در مرحلهٔ نهایی بلوک‌های تصویر در کنار یکدیگر قرار می‌گیرند و عمل جایگزینی پیکسل‌ها با استفاده از اتوماتای سلولی برگشت‌پذیر صورت می‌پذیرد. بدیهی است مراحل رمزگشایی تصویر با توجه به برگشت‌پذیری اتوماتای پیشنهادی به‌صورت معکوس قابل اجرا است. نتایج آزمایش‌ها نشان می‌دهد روش پیشنهادی می‌تواند تصویر را به‌گونه‌ای رمز کند که تصویر رمزشده از لحاظ بصری قابل درک نباشد. هم‌چنین روش پیشنهادی با استفاده از معیارهای کمی از جمله ضرایب همبستگی، NPCR، UACI، MAE و آنتروپی با روش‌های دیگر مورد بررسی قرار گرفت و ارزیابی شد. در بیش‌تر موارد، روش پیشنهادی نتایج مطلوب‌تری نسبت به روش‌های دیگر داشته است.

واژگان کلیدی: رمزنگاری تصویر، اتوماتای سلولی، اتوماتای سلولی برگشت‌پذیر

۱- مقدّمه

پیشرفت سریع ارتباطات، شبکه‌های رایانه‌ای و توسعهٔ سیستم‌های چندرسانه‌ای دیجیتال موجب تحولی عظیم در زندگی بشر شده است. این تحول علاوه بر مزایای فراوان مشکلاتی مانند سوء استفاده از رسانه دیجیتال به همراه داشته است. برای حل این مشکل، روش‌هایی جهت حفظ امنیت اطلاعات پیشنهاد شده است. رمزنگاری یکی از روش‌های متداول برای حفظ امنیت اطلاعات است (ویل و همکاران،۲۰۰۴) .

رمزنگاری محتویات رسانه را با استفاده از کلید و عملیات ریاضی برگشت‌پذیر تغییر می‌دهد. در مقصد رمزگشایی رسانه توسط کلید با عملیات معکوس رمزنگاری صورت می‌گیرد. کلید رمزنگاری به‌عنوان عنصر اصلی در عملیات رمزنگاری محسوب می‌شود؛ به‌طوری‌که بدون داشتن کلید حتی با دانستن الگوریتم عملیات رمزگشایی امکان‌پذیر نیست.

تصاویر دیجیتال امروزه در بین رسانه‌های دیجیتال، کاربرد و اهمیت زیادی دارند. تصاویر دیجیتال می‌توانند دربرگیرنده اطلاعات تجاری، نظامی، سیاسی و یا پزشکی باشند و لذا محرمانگی این اطلاعات تصویری، اهمیت زیادی دارد.

الگوریتم‌های رمزنگاری متن مانند RSA[1] و DES[2] برای رمزکردن تصویر کارآمد نیستند؛ زیرا تصویر به‌دلیل حجم زیاد و وابستگی پیکسل‌های آن با متن تفاوت دارد. بنابراین روش‌های رمزنگاری ویژه‌ای برای تصویر ارائه شده است (گودانگ و همکاران،۲۰۰۷).

از روش‌های مهم رمزنگاری برای تصویر جابه‌جایی[3] و جایگزینی[4] پیکسل‌ها را می‌توان نام برد. روش جابه‌جایی، چیدمان پیکسل‌ها را در تصویر تغییر می‌دهد. در این روش طبق یک رابطهٔ برگشت‌پذیر، موقعیت پیکسل‌ها تغییر

[1] Rivest-Shamir-Adleman(RSA)
[2] Data Encryption Standard(DES)
[3] Scrambling
[4] Substitution

می‌کند و تصویر رمزشده به دست می‌آید و در مقصد چیدمان نخستینِ پیکسل‌ها بازیابی می‌شوند (مهرنهاد و لطیف، ۲۰۱۵).

در روش جایگزینی، سطح روشنایی پیکسل‌ها برای رمزنگاری تصویر توسط عملیات منطقی و محاسباتی با استفاده از یک رابطهٔ ریاضی تغییر می‌کند و سپس در مقصد معکوس عملیات رمزنگاری انجام و مقادیر پیکسل‌ها بازیابی می‌شوند (گوان و همکاران، ۲۰۰۵؛ پاریک و همکاران،۲۰۰۶).

در رمزنگاری پیچیدگی عملیات و نحوهٔ پیاده‌سازی سخت‌افزاری و نرم‌افزاری اهمیت دارد. اتوماتای سلولی با ویژگی‌های ذاتی خود مانند امکان پردازش موازی، یک‌ریختی، غیرقابل‌پیش‌بینی‌بودن رفتار آن و پیاده‌سازی ساده، گزینهٔ مناسبی برای رمزنگاری تصویر است.

اتوماتای سلولی در دههٔ ۴۰ میلادی توسط *Von Newmann* ارائه شد (ون نیومن،۱۹۹۶). بعد از آن پژوهش‌های گسترده‌ای بر روی اتوماتای سلولی صورت گرفت. در سال‌های اخیر از اتوماتای سلولی در رمزنگاری (جین و واو، ۲۰۱۲؛ اسلامی و همکاران، ۲۰۱۰)، پردازش تصویر (روزین، ۲۰۱۰؛ کافمن و پیچ، ۲۰۱۰) و امنیت اطلاعات (اسلامی و زارع پور احمدآبادی،۲۰۱۰) استفاده شده 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 (روزینگ و هولیانگ، ۲۰۰۸). در سال ۲۰۱۳ میلادی توسط *FaselQadir* و همکارانش روش قبل با اندکی تغییر مورد استفاده قرار گرفت (ابدو و همکاران، ۲۰۱۳). شایان ذکر است روش‌های درهم‌ریزی تصویر به‌دلیل عدم تغییر هیستوگرام امنیت بالایی ندارند.

در سال ۲۰۱۲ میلادی روشی توسط *Jin* برای رمزنگاری تصویر با استفاده از اتوماتای سلولی به روش جایگزینی پیکسل‌ها معرفی شد (جین، ۲۰۱۲).این روش دارای خاصیت تناوبی بود. تناوبی‌بودن به این معنی است که با استفاده از چندین قانون متوالی به‌صورت چرخشی می‌توان به تصویر اصلی دست یافت. درنتیجه با اجرای یک تناوب کامل الگوریتم رمزگشایی انجام می‌شود.

در سال ۲۰۱۳ میلادی روشی بر مبنای جایگزینی پیکسل‌ها توسط *Abdo* و همکارانش ارائه شد. در این روش از اتوماتای سلولی با استفاده از خاصیت تناوبی استفاده شد (ابدو و همکاران، ۲۰۱۳). در این روش حلقه‌هایی از قوانین برگشت‌پذیر تشکیل و سپس با استفاده از عدد تصادفی حلقه‌ای از قوانین انتخاب و بر روی تصویر اعمال می‌شود تا تصویر رمزشده به‌دست آید. در هر دو روش مذکور با توجه به تناوبی‌بودن الگوریتم احتمال حمله و رمزگشایی تصویر وجود دارد.

در سال ۲۰۱۳ میلادی، روشی بر مبنای جابه‌جایی و جایگزینی پیکسل‌ها توسط *Wang* و همکارش ارائه شد (ونگ و لوان، ۲۰۱۳) . در بخش جایگزینی از اتوماتای سلولی برگشت‌پذیر استفاده شد. در این روش تنها بر روی چهار بیت پرارزش جایگزینی صورت گرفته و چهار بیت کم‌ارزش جابه‌جا می‌شوند. بنابراین احتمال تصادفی‌بودن در این روش نسبت به روش‌هایی که بر روی هشت بیت عمل جایگزینی صورت می‌گیرد، کم‌تر است.

در سال ۲۰۱۴ روش بلاک‌بندی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر توسط *Mohamed* نیز ارائه شد (محمد،۲۰۱۴). در این روش با تقسیم پیکسل‌های تصویر به بلاک‌های متعدد درچهل مرحله به رمز تصویر پرداخته است.

در این مقاله رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر ارائه می‌شود. در این روش برای افزایش امنیت رمزنگاری از ترکیب دو روش جابه‌جایی و جایگزینی پیکسل‌ها استفاده شده است. ساختار تعریف‌شده شامل سه اتوماتا است که تصویر اصلی طی سه مرحله رمز می‌شود. لازم به ذکر است، ساختار پیشنهادی برگشت‌پذیر است و با انجام هر یک از مراحل به‌صورت معکوس، رمزگشایی تصویر انجام می‌شود.

ساختار مقاله به شکل زیر است. در بخش دوم به معرفی اتوماتای سلولی برگشت‌پذیر پرداخته می‌شود. در بخش بعد روش پیشنهادی توضیح و سپس در بخش چهارم نتایج حاصل از اجرای الگوریتم نشان داده می‌شود. ارزیابی روش در بخش پنجم صورت می‌گیرد و در بخش پایانی نتیجه‌گیری لازم ارائه می‌شود.

۲- اتوماتای سلولی

اتوماتای سلولی یک مدل ریاضی برای سامانه‌های پویای 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 چهار مؤلفه به شکل $CA=\{C,S,V,F\}$ است. مؤلفه C نشان‌دهنده سلول اتوماتا و S نشان‌دهندهٔ حالت سلول است. در بیش‌تر کاربردها سلول‌ها دارای دو حالت صفر و یک می‌باشند. مؤلفه V نشان‌دهندهٔ ابعاد اتوماتا و نوع همسایگی و مؤلفه F قوانین انتقال اتوماتای سلولی است. در هر زمان سلول وضعیت خود را بر اساس قانون انتقال مشخص‌شده، تغییر می‌دهد. قوانین انتقال چگونگی تغییر حالت سلول را مشخص می‌کنند. این تغییر بستگی به حالت فعلی سلول و حالت سلول‌های همسایگانش دارد (ون نیومن، ۱۹۹۶).

قوانین اتوماتا برای تمام سلول‌ها می‌تواند یکسان و یا متفاوت باشد. اگر قوانین برای تمام سلول‌های اتوماتا یکسان باشد، اتوماتا یک‌نواخت و در غیر این صورت غیریک‌نواخت نامیده می‌شود (انصاری و میبدی، ۲۰۰۷). اگر سلول‌های اتوماتا به‌طور هم‌زمان به‌روزرسانی شوند، اتوماتای سلولی همگام و در غیر این صورت ناهمگام نام دارد (بیگی و میبدی،۲۰۰۸)

نمونه‌ای از اتوماتای سلولی، شامل همسایگی یک‌بعدی و حالت مرزی تناوبی با قانون انتقال ۳۰ در شکل (۱) نشان داده شده است. سطر نخست هشت حالت ممکن برای سلول‌ها با همسایگی شعاع یک و سطر دوم حالت بعدی هر سلول را نشان می‌دهد. بدیهی است عدد ۳۰ به‌صورت دودویی در ردیف دوم قرار داده شده است. به‌عنوان مثال در جدول (۱) اگر پیکسل سیاه با 1 و پیکسل سفید با 0 نشان داده شود و بردار نخستینِ ورودی اتوماتا به‌صورت [1 1 1 0 1 0 1 0] در نظر گرفته شود. برای اجرای قانون شماره ۳۰ و همسایگی سه‌تایی برای تعیین حالت بعدی بدین شیوه عمل می‌شود. با توجه به همسایگی سه تایی، سه پیکسل اول [1 1 0] انتخاب می‌شود. با توجه به قانون شکل (۱) حالت بعدی 1 در نظر گرفته می‌شود. به همین ترتیب برای سه پیکسل بعد [1 0 1] قانون اعمال شده و حالت بعدی سلول 0 می‌شود. این روند برای پیکسل‌های بعدی ادامه دارد. برای پیکسل نخست و آخر نیز حالت مرزی تناوبی در نظر گرفته می‌شود. روند کلی تا سه مرحله در جدول (۱) نشان داده شده است.

۲-۱- اتوماتای سلولی برگشت‌پذیر

اتوماتای سلولی به‌صورت ذاتی خاصیت برگشت‌پذیری ندارد؛ به‌طوری‌که تنها تعداد محدودی از قوانین برگشت‌پذیر هستند. برای داشتن یک الگوریتم مناسب رمزنگاری باید دقت کرد که عملیات ریاضی رمز برگشت‌پذیر باشد. رمزنگاری با استفاده از این قوانین محدود، امنیت مناسبی ندارد. بنابراین در این مقاله سعی شد از اتوماتای سلولی برگشت‌پذیر استفاده شود.

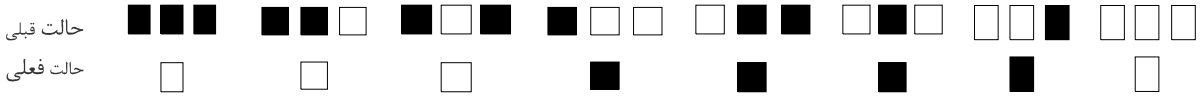
در اتوماتای سلولی برگشت‌پذیر، با داشتن هر حالت فعلی می‌توان به حالت نخستینِ آن دسترسی پیدا کرد. به این معنی که اتوماتای برگشت‌پذیر بر مبنای محاسبات دقیق می‌تواند عقب‌گرد کند و بنابراین تمام مراحل قابل‌ردیابی و بازگشت‌پذیر است (توفولی و مارگولس، ۱۹۹۰؛ ونگ و لوان، ۲۰۱۳).

در اتوماتای سلولی برگشت‌پذیر برای تعیین حالت بعدی اتوماتا به وضعیت فعلی و یک لحظه قبل از آن یعنی t و $t-1$ احتیاج است. 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 نخست مربوط به 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 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 نخست 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 نخستین حاصل می‌شود. در شکل (۳) مراحل برگشت‌پذیری با رنگ خاکستری نشان داده شده است.

۳- روش پیشنهادی برای رمزنگاری تصویر

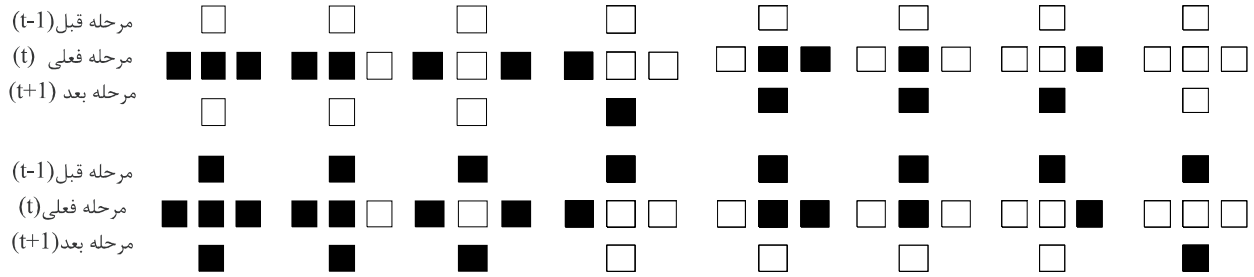
روش پیشنهادی برای رمز تصویر بر اساس عملکرد اتوماتای سلولی برگشت‌پذیر است. در این روش از سه اتوماتای سلولی یک‌بعدی استفاده می‌شود. الگوریتم رمزنگاری در زیر توضیح داده شده است.



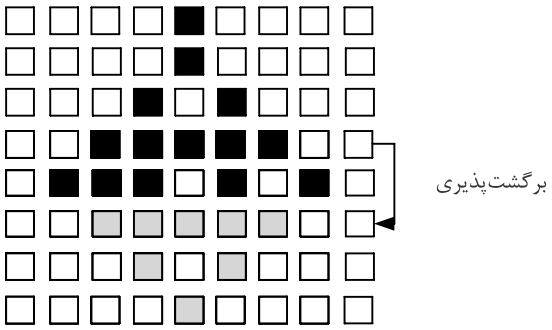
(شکل- ۱): اتوماتای سلولی با قانون ۳۰

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

سطر نخست	
دسته‌بندی سه‌تایی پیکسل‌ها	
حالت بعدی	
خروجی مرحله نخست	
دسته‌بندی سه‌تایی پیکسل‌ها	
حالت بعدی	
خروجی مرحله دوم	
دسته‌بندی سه‌تایی پیکسل‌ها	
حالت بعدی	
خروجی مرحله سوم	



(شکل- ۲): اتوماتای سلولی برگشت‌پذیر با قانون ۳۰



(شکل- ۳): عملکرد اتوماتای سلولی برگشت‌پذیر

۱- ابتدا دو سطر از تصویر ورودی خوانده می‌شود.

۲- K پیکسل از دو سطر انتخاب می‌شود. عدد K توسط کاربر قابل تنظیم است و می‌تواند به‌عنوان کلید در الگوریتم رمزنگاری استفاده شود.

۳- پیکسل‌های مذکور در هر سطر به‌صورت باینری در کنار یکدیگر قرار داده می‌شوند.

۴- این رشته دودویی به دو قسمت مساوی تقسیم می‌شود. (در جدول (۲) با توجه به اینکه k=۲ تعیین شده است تقسیم رشته دودویی به دو قسمت مساوی همان مقادیر دودویی پیکسل‌ها می‌شود.)

۵- دو رشتهٔ دودویی تولیدشده به‌عنوان ورودی اتوماتا در نظر گرفته می‌شود و رمزنگاری اعداد توسط اتوماتا در مرحله نخست صورت می‌گیرد. خروجی این مرحله شامل اعداد در دو زمان t و $t-1$ می‌باشد.

۶- در مرحله دوم رمزنگاری، مکان دو رشته دودویی خروجی مرحله نخست در زمان $t-1$ با یکدیگر جابه‌جا می‌شوند.سپس درهم‌ریزی بیت‌های رمزشده در خروجی اتوماتا در زمان t توسط عدد تصادفی تولیدی با اتوماتای سلولی دوم انجام می‌شود.

۷- رشته‌های بیتی در کنار یکدیگر قرار می‌گیرند.

۸- در مرحله بعد داده تصویر تولیدشده پس از مرحله دوم به‌عنوان ورودی به اتوماتای سوم وارد می‌شود.

۹- در مرحله آخر دو خروجی برای دو زمان t و $t-1$ تولید می‌شوند که مقادیر رمزشده پیکسل‌های خوانده شده می‌باشند. این مقادیر همان‌طور که در جدول (۲) نشان داده شده است، در ماتریس رمز ذخیره می‌شوند.

در مرحلهٔ رمزگشایی مراحل بالا به‌صورت معکوس اعمال می‌شود. با استفاده از تصویر رمزشده و کلیدی که به‌عنوان ماتریس رمزشده در زمان $t-1$ داده شده است، تصویر را طبق الگوریتم رمز به‌صورت معکوس، می‌توان رمزگشایی کرد. یک گام از اجرای قدم‌های ۱ تا ۹ همراه با یک مثال در جدول (۲) نشان داده شده است.

۴- نتایج حاصل از اجرای الگوریتم

نتایج حاصل از اجرای الگوریتم بر روی تصویرهای cameraman و boats با اندازه ۲۵۶×۲۵۶ با کلیدهای متفاوت در ادامه نشان داده شده است. شکل‌های (۴) الی (۶) تصویر اصلی، تصویر رمزشده و تصویر رمزگشایی‌شده با قوانین ۳۰، ۹۸ و ۱۵۳ را به‌ترتیب نشان می‌دهد. برای نشان دادن حساسیت الگوریتم به کلید در شکل (۷) سعی شده است که تصویر رمزشده با قانون ۹۸ را با کلید دیگری رمزگشایی کرد. همان‌گونه که مشاهده می‌شود، رمزگشایی به‌صورت صحیح انجام نشده و تصویر به‌طورکامل نامفهوم است. در شکل‌های (۸ الی ۱۰) این الگوریتم بر روی تصویر boats اعمال شده و نتایج نشان داده شده است.

۵- تحلیل و ارزیابی روش پیشنهادی

در مراجع گذشته برای ارزیابی روش پیشنهادی چندین آزمون پیشنهاد شده است (ونگ و لوان، ۲۰۱۳؛ ابدو و همکاران، ۲۰۱۳؛ جین، ۲۰۱۲). در این مقاله سعی شده است تا آزمون‌های معرفی‌شده بر روی روش پیشنهادی به همراه دو روش Jin و Abdo بررسی شود.

۵-۱- تحلیل آماری

طبق نظریه شانون با استفاده از تحلیل‌های آماری[1] می‌توان بسیاری از مسائل رمز را حل کرد. الگوریتم رمز باید به‌گونه‌ای باشد که دشواری تحلیل‌های آماری را بیش‌تر کند. تحلیل هیستوگرام و ضرایب همبستگی از مواردی است که برای ارزیابی تحلیل‌های آماری استفاده می‌شود. (ونگ و لوان، ۲۰۱۳).

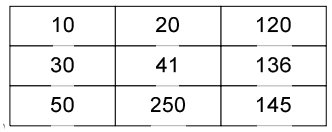
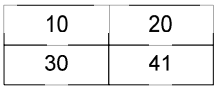
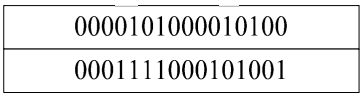
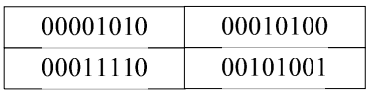
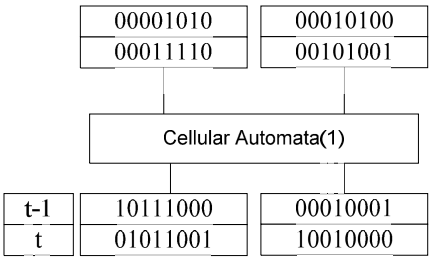
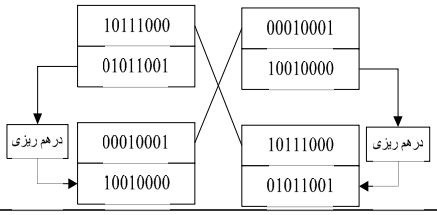
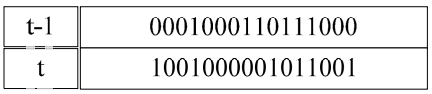
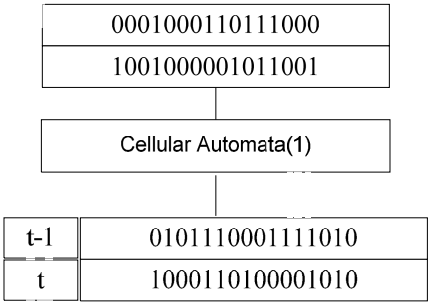
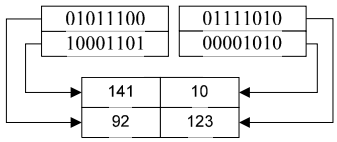
۵-۱-۱ تحلیل هیستوگرام

یک الگوریتم رمزنگاری در صورتی مناسب است که تصویر به‌گونه‌ای رمز شود که هیچ‌گونه اطلاعاتی از تصویر اصلی در آن دیده نشود؛ به عبارتی در رمزنگاری باید تصویر به‌صورت بصری قابل تشخیص نباشد. با توجه به این‌که نتیجهٔ آزمون بصری برای بینندگان مختلف متفاوت است، می‌توان از تحلیل هیستوگرام استفاده کرد. تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از ترسیم تعداد مشاهدات هر شدت روشنایی بیان می‌کند.

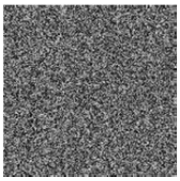
هیستوگرام تصاویر اصلی و رمز شده دو تصویر cameraman و boats در شکل (۱۱ و ۱۲) به ترتیب نشان داده شده است. همان‌طور که در شکل دیده می‌شود، هیستوگرام تصاویر رمزشده یکنواخت می‌باشد که این نشان‌دهنده کارایی الگوریتم رمزنگاری پیشنهادی می‌باشد.

[1] Statistical Analysis

(جدول- ۲): مثالی از عملکرد روش پیشنهادی

ماتریس اولیه		
مرحله نخست رمزنگاری	قدم ۱ و ۲ (k=2)	
	قدم ۳	
	قدم ۴	
	قدم ۵ (مرحله اجرای اتوماتا)	
مرحله دوم رمزنگاری	قدم ۶	
	قدم ۷	
مرحله سوم رمزنگاری	قدم ۸ (مرحله اجرای اتوماتا)	
	قدم ۹	

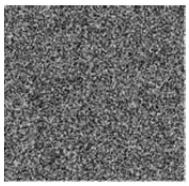

الف) تصویر اصلی


ب) تصویر رمزشده


ج) تصویر رمزگشایی‌شده

(شکل- ۴): نتایج خروجی الگوریتم پیشنهادی با قانون ۳۰

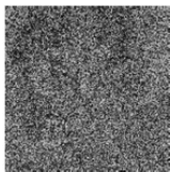

الف) تصویر اصلی


ب) تصویر رمزشده


ج) تصویر رمزگشایی‌شده

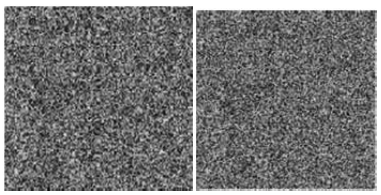
(شکل- ۵): نتایج خروجی الگوریتم پیشنهادی با قانون ۹۸


الف) تصویر اصلی


ب) تصویر رمزشده

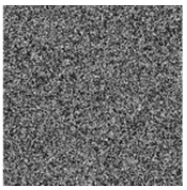

ج) تصویر رمزگشایی‌شده

(شکل- ۶): نتایج خروجی الگوریتم پیشنهادی با قانون ۱۵۳


الف) تصویر رمزشده با قانون ۹۸ ب) تصویر رمزگشایی با قانون ۱۵۰

(شکل- ۷): نتایج خروجی الگوریتم در رمزگشایی با کلید نادرست

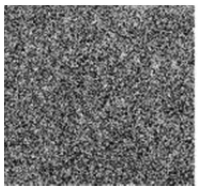

الف) تصویر اصلی


ب) تصویر رمزشده


ج) تصویر رمزگشایی‌شده

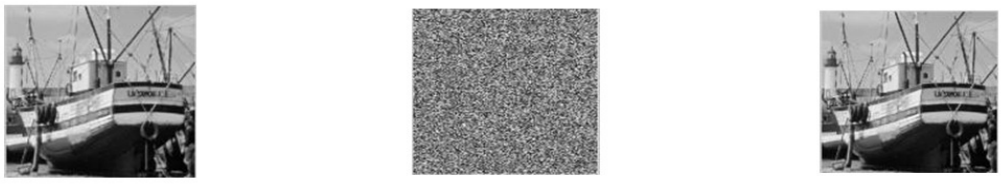
(شکل- ۸): نتایج خروجی الگوریتم پیشنهادی با قانون ۳۰


الف) تصویر اصلی


ب) تصویر رمزشده

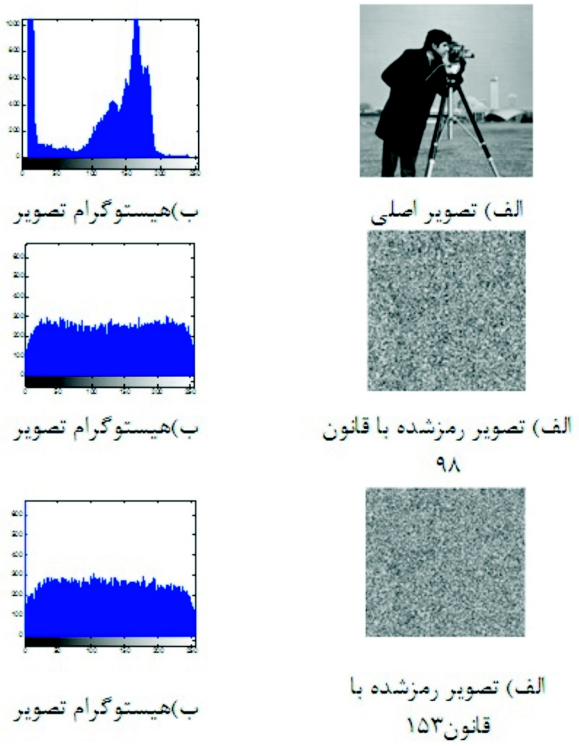

ج) تصویر رمزگشایی‌شده

(شکل- ۹): نتایج خروجی الگوریتم پیشنهادی با قانون ۹۸



الف) تصویر اصلی ب) تصویر رمزشده ج) تصویر رمزگشایی‌شده

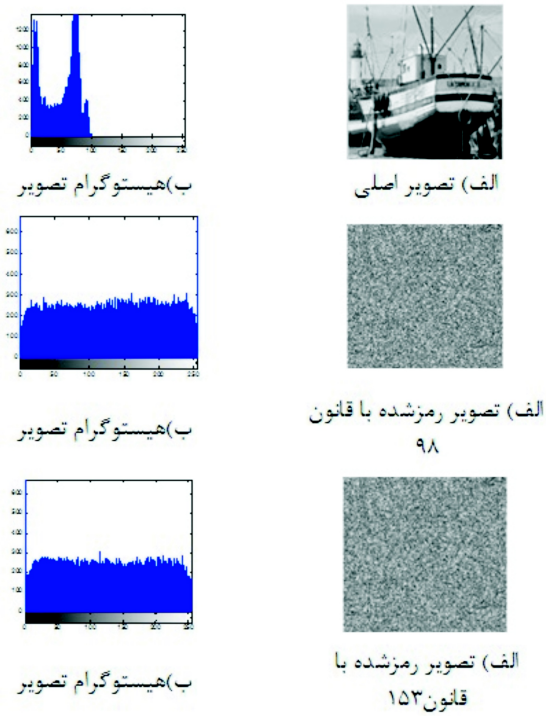
(شکل- ۱۰): نتایج خروجی الگوریتم پیشنهادی با قانون ۱۵۳



الف) تصویر اصلی
ب)هیستوگرام تصویر
الف) تصویر رمزشده با قانون ۹۸
ب)هیستوگرام تصویر
الف) تصویر رمزشده با قانون۱۵۳
ب)هیستوگرام تصویر

(شکل- ۱۱): نتایج هیستوگرام تصاویر رمزشده cameraman

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2 \qquad (۴)$$



الف) تصویر اصلی
ب)هیستوگرام تصویر
الف) تصویر رمزشده با قانون ۹۸
ب)هیستوگرام تصویر
الف) تصویر رمزشده با قانون۱۵۳
ب)هیستوگرام تصویر

(شکل- ۱۲): نتایج هیستوگرام تصاویر رمزشده boats

۵-۱-۲- تحلیل ضرایب همبستگی

یکی دیگر از معیارهای ارزیابی برای تحلیل آماری، همبستگی است. هرچه همبستگی پیکسل‌های همسایه در تصویر رمزشده کم‌تر باشد، عملکرد الگوریتم مطلوب‌تر است (ونگ و لوان، ۲۰۱۳). برای مطالعه همبستگی پیکسل‌ها در راستای افقی، عمودی و قطری از رابطه ۱ استفاده می‌شود.

$$r_{xy} = \frac{\mathrm{Cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۱)$$

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))(y_j - E(y)) \qquad (۲)$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N} x_i \qquad (۳)$$

در این روابط x و y روشنایی دو پیکسل همسایه در تصویر و N تعداد پیکسل‌های انتخاب‌شده از تصویر است.

مقادیر تابع همبستگی در سه راستای عمودی، افقی و قطری برای تصویر cameraman و تصاویر رمزشده آن با قانون ۹۸ و ۱۵۳ با چهار الگوریتم معرفی‌شده توسط Jin، *Abdo*، Wang، Mohamed و الگوریتم پیشنهادی در جداول (۳ و ۴) به‌ترتیب آورده 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): معیار همبستگی برای تصویر cameraman با قانون ۹۸

تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز روش Jin	-۰/۰۳۶۹	-۰/۰۳۸۳	۰/۰۱۱۴
تصویر رمز روش Abdo	۰/۰۱۲۲	۰/۰۱۴۹	-۰/۰۱۷۸
تصویر رمز روش Wang	-۰/۰۱۱۶	-۰/۰۱۷۶	۰/۰۰۶۸
تصویر رمز روش Mohamed	-0..204	0.0337	0.0113
تصویر رمز روش پیشنهادی	۰/۰۱۲۱	۰/۰۱۱۵	-۰/۰۰۰۰۶۷

(جدول- ۴): معیار همبستگی برای تصویر cameraman با قانون ۱۵۳

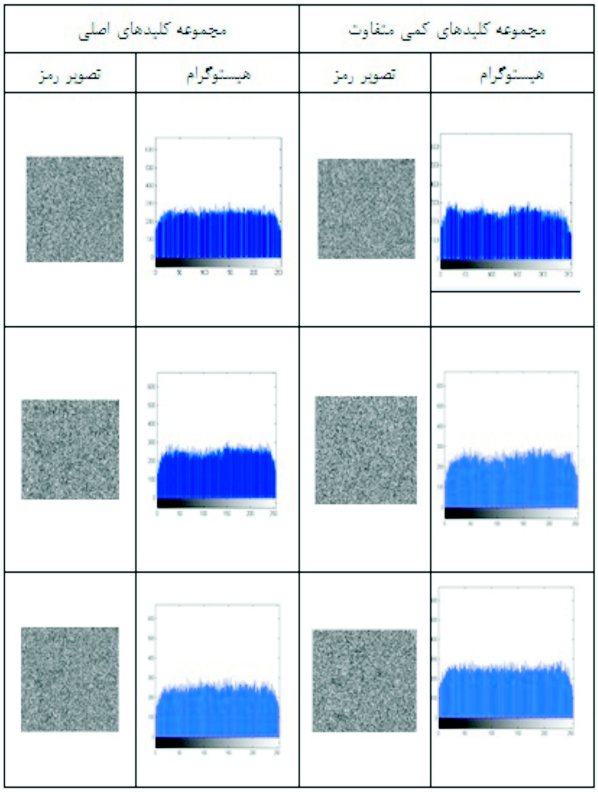
تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۴۸۹	۰/۹۵۳۶	۰/۹۲۱۲
تصویر رمز روش Jin	-۰/۰۶۳۲	-۰/۰۶۴۱	۰/۰۴۱۰
تصویر رمز روش Abdo	-۰/۰۶۰۴	-۰/۰۶۳۵	۰/۰۴۳۲
تصویر رمز روش Wang	-۰/۰۲۱۹	-۰/۰۲۲۷	۰/۰۰۱۷
تصویر رمز روش Mohamed	0.1541	0.2562	0.1368
تصویر رمز روش پیشنهادی	-۰/۰۱۶۶	-۰/۰۰۵۲	-۰/۰۰۱۵

۵-۲-تحلیل حساسیت نسبت به کلید

حساسیت نسبت به کلید ، یکی دیگر از ویژگی‌های ضروری برای یک الگوریتم رمزنگاری مطلوب است. به این معنی که تغییر یک بیت در کلید خصوصی ، بایستی یک تصویر رمز به‌طورکامل متفاوت تولید کند. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله جستجوی جامع[1] تا حدی تضمین می‌کند.

برای ارزیابی ویژگی حساسیت نسبت به کلید ابتدا تصویر اصلی با کلید محرمانه اصلی رمزنگاری می‌شود؛ سپس کلید را کمی تغییر داده و تصویر اصلی دوباره رمزنگاری می‌شود.درصورتی‌که مقایسه این دو تصویر رمز به‌صورت بصری امکان‌پذیر نباشد، الگوریتم رمزنگاری نسبت به کلید حساسیت بالایی دارد. در جدول (۵) نتیجه آزمون حساسیت نسبت به کلید نشان داده شده است. به‌منظور تشخیص تفاوت بین تصاویر رمز هیستوگرام تصاویر رمز ترسیم شده است تا مقایسه آن‌ها آسان‌تر شود.

(جدول-۵): تحلیل حساسیت نسبت به کلید



۵-۳-تمایز تصویر اصلی و رمزشده

یک خاصیت ایده‌آل برای تصویر رمز، حساس‌بودن 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 رابطه بین تصویر اصلی و رمز آشکار شود. با این کار می‌توان کلید را شناسایی کرد.

سه معیار UACI[3]، MAE[4]، NPCR[5] برای آزمودن اثر تغییر یک پیکسل ورودی بر روی تصویر رمزشده است. هر چه این سه معیار بیش‌تر باشند، الگوریتم رمزنگاری عملکرد مطلوب‌تر دارد (کانسو و قبله، ۲۰۱۲).

[1]Brute-Force Attack

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

رابطه ۵ مربوط به محاسبهٔ متوسط خطای مطلق است (جلفایی و میرقدیر، ۲۰۱۰). در این رابطه $C(i,j)$ و $P(i,j)$ به‌ترتیب مقادیر پیکسل‌های تصویر رمز و تصویر اصلی است.

رابطهٔ۶ محاسبه $NPCR$ را نشان می‌دهد که نرخ پیکسل‌های تغییریافته تصویر رمز به ازای یک بیت تغییر در تصویر اصلی است (کانسو و قبله، ۲۰۱۲). نحوهٔ محاسبهٔ $UACI$ در رابطه ۸ نشان داده شده است.

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i,j) - P(i,j)| \qquad (۵)$$

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \qquad (۶)$$

$$D(i,j) = \begin{cases} 0 & if \quad C_1(i,j) = C_2(i,j) \\ 1 & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (۷)$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{C(i,j) - \bar{C}(i,j)}{255} \qquad (۸)$$

در جدول (۶) مقادیر توابع ارزیابی برای الگوریتم‌های *معرفی‌شده توسط* Jin، Abdo ، Wang و Mohamed با الگوریتم پیشنهادی با قانون ۱۵۳ نشان داده شده است.

همان‌طور که در جدول مشاهده می‌شود، این مقادیر برای روش پیشنهادی نسبت به دو روش معرفی شده توسط Jin و Abdo بیش‌ترین مقدار را دارد؛ یعنی به‌ازای تغییر یک پیکسل در تصویر ورودی بیش‌ترین میزان تغییر در خروجی ایجاد شده است. در مقایسه با روش Wang نیز برای UACI و NPCR بیش‌ترین مقادیر را دارد.

(جدول- ۶): معیارهای ارزیابی برای تصویر cameraman با قانون ۱۵۳

الگوریتم	UACI	NPCR	MAE
تصویر رمز روش Jin	۱۵/۰۱۵۱	۴۹/۳۰۵۷	۳۹/۵۷۷۲
تصویر رمز روش Abdo	۱۳/۸۲۴۶	۴۹/۴۲۳۲	۳۸/۶۳۵۹
تصویر رمز روش Wang	۹/۶۵۴۲	۴۹/۲۷۰۶	۷۴/۴۲۵۱
تصویر رمز روش Mohamed	*15.0241*	۵۰.۰۲۵۳	*40.8497*
تصویر رمز روش پیشنهادی	۱۷/۳۳۴۸	۵۰/۲۰۴۵	۴۴/۷۱۴۷

۵-۴-تحلیل آنتروپی

آنتروپی یکی دیگر از مشخصه‌های مهم تصادفی‌بودن الگوریتم است. آنتروپی طبق رابطه ۹ محاسبه می‌شود که در آن S تصویر رمزشده و $P(S_i)$ تعداد رخدادهای S_i است. در حالت ایده‌آل برای یک تصویر رمزشده که هر پیکسل آن ۸ بیتی باشد، این مقدار باید به ۸ نزدیک باشد (ونگ و لوان، ۲۰۱۳). در جدول (۷) مقادیر آنتروپی نشان داده شده است.

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \log_2^{\frac{1}{P(s_i)}} \qquad \text{رابطه (۹)}$$

(جدول- ۷) : مقادیر آنتروپی برای روش‌های مختلف

روش‌ها	روش Jin	روش Abdo	روش Wang	روش Mohamed	روش پیشنهادی
آنتروپی	۷/۹۳۲۲	۷/۴۲۵۹	۷/۲۲۹۲	7/9253	۷/۹۵۵۶

۵-۵-تحلیل فضای کلید

به‌منظور جلوگیری از حمله جست‌وجوی جامع، فضای کلید الگوریتم رمزنگاری باید به حد کافی بزرگ باشد. فضای کلید الگوریتم شامل تعداد کل کلیدهای قابل‌استفاده در الگوریتم رمزنگاری است. هرچه اندازه فضای کلید رمزنگاری بزرگ‌تر باشد، زمان آزمایش کلیه کلیدها بیشتر می‌شود و در نتیجه نسبت به حمله جست‌وجوی جامع مقاوم‌تر است. سازمان NIST حداقل طول ممکن برای برقراری امنیت محاسباتی در برابر حمله‌های جست‌وجوی جامع را تا سال ۲۰۱۵، ۸۰ بیت پیش‌بینی کرده است (ونگ و لوان، ۲۰۱۳). در الگوریتم پیشنهادی از چهار اتوماتای سلولی که شامل دو اتوماتا به‌صورت هم‌زمان در مرحله نخست، یک اتوماتا در مرحله دوم و یک اتوماتای دیگر در مرحله سوم استفاده می‌شود. با توجه به این‌که در هر اتوماتا از 2^8 قانون می‌توان استفاده کرد، فضای کلید $۴۲۹۴۹۶۷۲۹۶ = 2^{32} = 2^8 \times 2^8 \times 2^8 \times 2^8$ است؛ بنابراین ساختار پیشنهادی نسبت به حمله جست‌وجوی جامع مصون است. فضای کلید روش پیشنهادی نسبت به روش معرفی‌شده توسط Wang که برابر با 2^{280} می‌باشد، کم‌تر است.

۵-۶-تحلیل اجرایی

عملکرد یک سامانه رمزنگاری بر اساس عوامل مختلفی ازجمله قابلیت اطمینان در برابر حمله‌های مختلف، پیچیدگی محاسباتی و زمان رمزنگاری ارزیابی می‌شود. در بخش‌های قبل مشاهده شد که الگوریتم پیشنهادی در برابر

حمله‌های مختلف عملکرد خوبی داشته است. در این بخش نیز پیچیدگی محاسباتی و زمان اجرای الگوریتم بحث می‌شود. الگوریتم پیشنهادی در سه مرحله انجام می‌گیرد و شامل عملیات مختلف از جمله تولید اعداد تصادفی، محاسبات خطی اتوماتای سلولی، شیفت‌دادن و XOR بیتی است. تمام این عملیات، پیاده‌سازی مستقیم دارند. بنابراین الگوریتم پیشنهادی از نظر محاسباتی کارآمد است.

زمان اجرای الگوریتم نیز یکی دیگر از عوامل ارزیابی است. الگوریتم پیشنهادی به‌طور متوسط دارای زمان اجرای ۵۷/۸۱۸۳ ثانیه است که نسبت به الگوریتم Wang با زمان اجرای ۱۵۸/۴۵۲ ثانیه، رضایت‌بخش است.

پیاده‌سازی تمام الگوریتم‌ها بر روی سامانه CORE i3 و RAM 2GB صورت گرفته است.

۶-نتیجه‌گیری

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

روش پیشنهادی با استفاده از اتوماتای سلولی برگشت‌پذیر به رمزنگاری تصویر می‌پردازد. در این مقاله ساختار جدیدی برای رمزنگاری تصویر معرفی شد که در سه مرحله به رمزنگاری تصویر می‌پردازد. بدیهی است با توجه به برگشت‌پذیری اتوماتای سلولی مراحل رمزگشایی قابل‌اجرا است. نتایج اعمال این الگوریتم بر روی تصویر با روش‌های *معرفی‌شده* توسط Jin، Abdo ، Wang و Mohamed توسط توابع ارزیابی مانند *UACI*، *MAE*، *NPCR* مقایسه شده است.نتایج نشان می‌دهد که این روش، توانایی بهتری برای رمزنگاری اطلاعات نسبت به روش‌های مورد بررسی دارد.

اتوماتای سلولی به‌دلیل گستردگی و انواع مختلف آن کاربرد زیادی در رمزنگاری دارد. در کارهای بعدی اتوماتای سلولی برگشت‌پذیر را با اتوماتای سلولی ترکیبی به‌طور هم‌زمان می‌توان به کار برد و الگوریتم‌های رمزنگاری جدیدی تولید کرد.

۷- مراجع

Abdo, A., et al. (2013). "A cryptosystem based on elementary cellular automata." Communications in No-nlinear Science and Numerical Simulation 18(1): 136-147.

Asnaashari, M. and M. Meybodi (2007). "Irregular cellular learning automata and its application toclust-ering in sensor networks."Proceedings of 15th Confe-rence on Electrical Engineering, Tehran, Iran.

Beigy, H. and M. R. Meybodi (2008). "Asynchronous cellular learning automata." Automatica 44(5): 1350-1357.

Eslami, Z., et al. (2010). "Secret image sharing based on cellular automata and steganography." Pattern Reco-gnition 43(1): 397-404.

Eslami, Z. and J. Zarepour Ahmadabadi (2010). "A verifiable multi-secret sharing scheme based on cellular automata." Information Sciences 180(15): 2889-2894.

Guan, Z.H., et al. (2005). "Chaos-based image encr-ption algorithm." Physics Letters A 346(1): 153-157.

Guodong Ye, et al. (2007). "Image encryption algorithm of double scrambling based on ASCII code of matrix element." International Conference on Computational Intelligence and Security:843-847.

Jin, J. (2012). "An image encryption based on elementry cellular automata." Optics & Laser Technology50(12): 1836-1843.

Jin, J. and Z.h. Wu (2012). "A secret image sharing based on neighborhood configurations of 2-d cellular automata." Optics & Laser Technology 44(3): 538-548.

Jolfaei, A. and A. Mirghadri (2010). " Image encryption using salsa20." International Journal of Computer Scie-nce Issues 7(5).

Kanso, A. and M. Ghebleh (2012). "A novel image encryption algorithm based on a 3D chaotic map." Communications in Nonlinear Science and Numerical Simulation 17(7): 2943-2959.

Kauffmann, C. and N. Piché (2010). "Seeded ND medical image segmentation by cellular automaton on GPU." International Journal of Computer Assisted Radi-ology and Surgery 5(3): 251-262.

Mehrnahad, Z. and A. latif (2015). " A new image encryption method with Hybrid and reversible cellular automata." ADST Journal 5(4): 257-267.

Mohamed, F. K. (2014)."A parallel block-based encry-ption schemafor digital images using reversible cellular automata"; an International Journalof Science and Technology 17(2): 85-94.

Pareek, N.K., et al. (2006). "Image encryption using chaotic logistic map." Image and Vision Computing 24(9): 926-934.

Rosin, P. L. (2010). "Image processing using3-state cellular automata." Computer Vision and Image Understanding 114(7): 790-802.

RuisongYe. and L. Huiliang (2008). "A novel image scrambling and watermarking scheme based on

cellular automata." International Symposium on Electronic Commerce and SecurityS938-941.

Toffoli, T. and N. H. Margolus (1990). "Invertible cellular automata: A review." Physica D: Nonlinear Phenomena 45(1): 229-253.

Ville, V. D., et al. (2004). "Image scrambling without bandwidth expansion." IEEE Transactions on Circuits and Systems for Video Technology14(6): 892-897.

Von Neumann, J. (1966). "Theory of self-reproducing automata." University of Illinois Press.

Wang, X. and D. Luan (2013). "A novel image encr-yption algorithm using chaos and reversible cellular automata."Communications in Nonlinear Science and Numerical Simulation 18(11): 3075-3085.

Zhenwei, S., et al. (2008). "A block location scram-bling algorithm of digital image based on Arnold transformation." The 9th International Conference for Young Computer Scientists:2942-2947.

زینب مهرنهاد مدرک کارشناسی خود را در رشتهٔ مهندسی کامپیوتر (گرایش نرم‌افزار) و کارشناسی ارشد را در مهندسی کامپیوتر (گرایش هوش مصنوعی و رباتیک) در سال‌های ۱۳۹۱ ۱۳۹۴ از دانشگاه یزد گرفت. زمینهٔ پژوهشی مورد علاقه ایشان شامل پردازش تصاویر، رمزنگاری تصاویر است.

نشانی رایانامهٔ ایشان عبارت است از:

z-mehrnahad@stu.yazd.ac.ir

علی‌محمد لطیف دارای دکترای مهندسی کامپیوتر گرایش هوش مصنوعی از دانشگاه صنعتی اصفهان بوده و مدرک کارشناسی ارشد خود را در رشتهٔ مهندسی برق الکترونیک از دانشگاه صنعتی امیرکبیر و کارشناسی خود را در رشته مهندسی برق الکترونیک از دانشگاه صنعتی اصفهان اخذ کرده است. وی هم‌اکنون عضو هیئت علمی گروه مهندسی کامپیوتر دانشگاه یزد است. زمینهٔ پژوهشی مورد علاقهٔ ایشان شامل پردازش تصاویر دیجیتال، رمزنگاری تصاویر و پنهان‌نگاری است.

نشانی رایانامهٔ ایشان عبارت است از:

alatif@yazd.ac.ir