

رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت پذیر

زینب مهرنهاد و علی محمد لطیف

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

چکیده

در این مقاله یک ساختار جدید برای رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت پذیر ارائه شده است. رمزنگاری تصویر در روش پیشنهادی در سه مرحله جداگانه صورت می گیرد. در مرحله نخست تصویر بلوک بندی می شود و سپس مقادیر روشنایی پیکسل ها با استفاده از اتوماتای سلولی برگشت پذیر جایگزین می شوند. در هر مرحله تصویر در مرحله دوم با اتوماتای دیگری انجام می شود و سپس در مرحله نهایی بلوک های تصویر در کنار یکدیگر قرار می گیرند و عمل جایگزینی پیکسل ها با استفاده از اتوماتای سلولی برگشت پذیر صورت می پذیرد. بدیهی است مراحل رمزگشایی تصویر با توجه به برگشت پذیری اتوماتای پیشنهادی به صورت معکوس قابل اجرا است. نتایج آزمایش ها نشان می دهد روش پیشنهادی می تواند تصویر را به گونه ای رمز کند که تصویر رمز شده از لحاظ بصری قابل درک نباشد. همچنین روش پیشنهادی با استفاده از معیارهای کمی از جمله ضرایب همبستگی، NPCR، UACI، MAE و آنتروپی با روش های دیگر مورد بررسی قرار گرفت و ارزیابی شد. در بیش تر موارد، روش پیشنهادی نتایج مطلوب تری نسبت به روش های دیگر داشته است.

واژگان کلیدی: رمزنگاری تصویر، اتوماتای سلولی، اتوماتای سلولی برگشت پذیر

۱- مقدمه

پیشرفت سریع ارتباطات، شبکه های رایانه ای و توسعه سیستم های چند رسانه ای 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، روش هایی جهت حفظ امنیت اطلاعات پیشنهاد شده است. رمزنگاری یکی از روش های متداول برای حفظ امنیت اطلاعات است (ویل و همکاران، ۲۰۰۴).

رمزنگاری محتویات رسانه را با استفاده از کلید و عملیات ریاضی برگشت پذیر تغییر می دهد. در مقصد رمزگشایی رسانه توسط کلید با عملیات معکوس رمزنگاری صورت می گیرد. کلید رمزنگاری به عنوان عنصر اصلی در عملیات رمزنگاری محسوب می شود؛ به طوری که بدون داشتن کلید حتی با دانستن الگوریتم عملیات رمزگشایی امکان پذیر نیست.

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

الگوریتم های رمزنگاری متن مانند^۱ RSA و^۲ DES برای رمز کردن تصویر کارآمد نیستند؛ زیرا تصویر به دلیل حجم زیاد و وابستگی پیکسل های آن با متن تفاوت دارد. بنابراین روش های رمزنگاری ویژه ای برای تصویر ارائه شده است (گودانگ و همکاران، ۲۰۰۷).

از روش های مهم رمزنگاری برای تصویر جابه جایی^۳ و جایگزینی^۴ پیکسل ها را می توان نام برد. روش جابه جایی، چیدمان پیکسل ها را در تصویر تغییر می دهد. در این روش طبق یک رابطه برگشت پذیر، موقعیت پیکسل ها تغییر

^۱ Rivest-Shamir-Adleman (RSA)

^۲ Data Encryption Standard (DES)

^۳ Scrambling

^۴ Substitution

می‌کند و تصویر رمزشده به دست می‌آید و در مقصد چیدمان نخستین 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 رابطه 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 نحوه پیاده‌سازی سخت‌افزاری و نرم‌افزاری اهمیت دارد. اتوماتای سلولی با ویژگی‌های ذاتی خود مانند امکان پردازش موازی، یک‌ریختی، غیرقابل پیش‌بینی بودن رفتار آن و پیاده‌سازی ساده، گزینه مناسبی برای رمزنگاری تصویر است.

اتوماتای سلولی در دهه 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 به دلیل 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. تناوبی بودن به این معنی است که با استفاده از چندین قانون متوالی به صورت چرخشی می‌توان به تصویر اصلی دست یافت. در نتیجه 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 به دست آید. در هر دو روش مذکور با توجه به تناوبی بودن 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 پردازش جایگزینی صورت گرفته و چهار بیت کم‌ارزش جابه‌جا می‌شوند. بنابراین احتمال تصادفی بودن 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 در چهل 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 تعریف شده 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 به صورت 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 می تواند دارای ابعاد مختلفی باشد.

اتوماتای سلولی دارای چهار مؤلفه به شکل $CA = \{C, S, V, F\}$ است. مؤلفه C نشان دهنده سلول اتوماتا و S نشان دهنده حالت سلول است. در بیش تر کاربردها سلول ها دارای دو حالت صفر و یک می باشند. مؤلفه V نشان دهنده ابعاد اتوماتا و نوع همسایگی و مؤلفه F قوانین انتقال اتوماتای سلولی است. در هر زمان سلول وضعیت خود را بر اساس قانون انتقال مشخص شده، 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 (ون نیومن، ۱۹۹۶).

قوانین اتوماتا برای تمام سلول ها می تواند یکسان و یا متفاوت باشد. اگر قوانین برای تمام سلول های اتوماتا یکسان باشد، اتوماتا یک نواخت و در غیر این صورت غیر یک نواخت نامیده می شود (انصاری و میبیدی، ۲۰۰۷). اگر سلول های اتوماتا به طور هم زمان به روز رسانی شوند، اتوماتای سلولی همگام و در غیر این صورت ناهمگام نام دارد (بیگی و میبیدی، ۲۰۰۸).

نمونه ای از اتوماتای سلولی، شامل همسایگی یک بعدی و حالت مرزی تناوبی با قانون انتقال ۳۰ در شکل (۱) نشان داده شده است. سطر نخست هشت حالت ممکن برای سلول ها با همسایگی شعاع یک و سطر دوم حالت بعدی هر سلول را نشان می دهد. بدیهی است عدد ۳۰ به صورت دودویی در ردیف دوم قرار داده شده است. به عنوان مثال در جدول (۱) اگر پیکسل سیاه با ۱ و پیکسل سفید با ۰ نشان داده شود و بردار نخستین ورودی اتوماتا به صورت $[0\ 1\ 1\ 0\ 1\ 0\ 1\ 1]$ در نظر گرفته شود. برای اجرای قانون شماره ۳۰ و همسایگی سه تایی برای تعیین حالت بعدی بدین شیوه عمل می شود. با توجه به همسایگی سه تایی، سه پیکسل اول $[0\ 1\ 1]$ انتخاب می شود. با توجه به قانون شکل (۱) حالت بعدی ۱ در نظر گرفته می شود. به همین ترتیب برای سه پیکسل بعد $[1\ 1\ 0]$ قانون اعمال شده و حالت بعدی سلول ۰ می شود. این روند برای پیکسل های بعدی ادامه دارد. برای پیکسل نخست و آخر نیز حالت مرزی تناوبی در نظر گرفته می شود. روند کلی تا سه مرحله در جدول (۱) نشان داده شده است.

۲-۱- اتوماتای سلولی برگشت پذیر

اتوماتای سلولی به صورت ذاتی خاصیت برگشت پذیری ندارد؛ به طوری که تنها تعداد محدودی از قوانین برگشت پذیر

هستند. برای داشتن یک الگوریتم مناسب رمزنگاری باید دقت کرد که عملیات ریاضی رمز برگشت پذیر باشد. رمزنگاری با استفاده از این قوانین محدود، امنیت مناسبی ندارد. بنابراین در این مقاله سعی شد از اتوماتای سلولی برگشت پذیر استفاده شود.

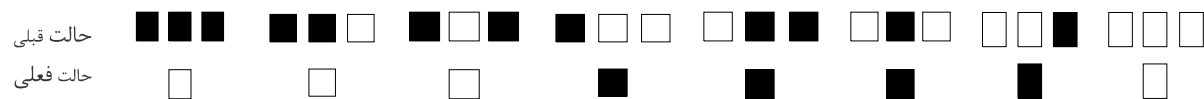
در اتوماتای سلولی برگشت پذیر، با داشتن هر حالت فعلی می توان به حالت نخستین آن دسترسی پیدا کرد. به این معنی که اتوماتای برگشت پذیر بر مبنای محاسبات دقیق می تواند عقب گرد کند و بنابراین تمام مراحل قابل ردیابی و بازگشت پذیر است (توفولی و مارگولس، ۱۹۹۰؛ ونگ و لوان، ۲۰۱۳).

در اتوماتای سلولی برگشت پذیر 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 می توان 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 می توان حالت سلول را برای لحظه بعد تعیین کرد. در این روش دو قانون برای اتوماتا در نظر گرفته می شود. 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.

نمونه ای از عملکرد اتوماتای سلولی برگشت پذیر 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 سلول ها مشخص می شود. سطرها بعدی را می توان به همین ترتیب تولید کرد. برای برگشت پذیری اتوماتا سطر چهارم (زمان $t-1$) را بعد از سطر پنجم (زمان t) قرار داده و قوانین اتوماتای برگشت پذیر طبق شکل (۲) اعمال می شود. به این ترتیب برگشت پذیری صورت می گیرد و بردار نخستین حاصل می شود. در شکل (۳) مراحل برگشت پذیری با رنگ خاکستری نشان داده شده است.

۳- روش پیشنهادی برای رمزنگاری تصویر

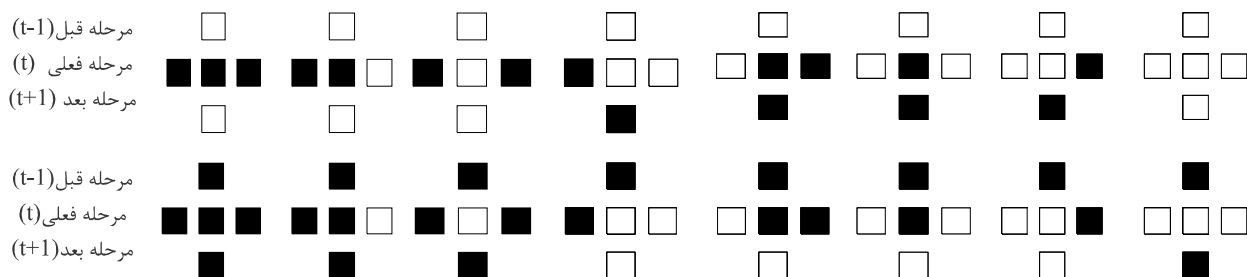
روش پیشنهادی برای رمز تصویر بر اساس عملکرد اتوماتای سلولی برگشت پذیر است. در این روش از سه اتوماتای سلولی یک بعدی استفاده می شود. الگوریتم رمزنگاری در زیر توضیح داده شده است.



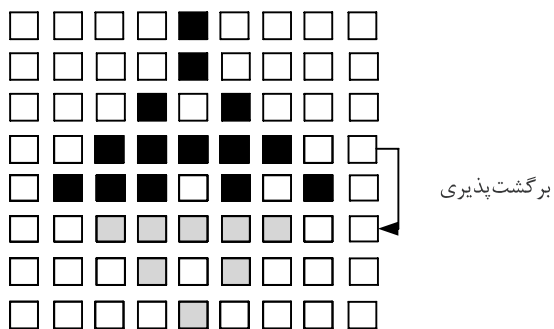
(شکل - ۱): اتوماتای سلولی با قانون ۳۰

(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

می‌دهد. برای نشان دادن حساسیت الگوریتم به کلید در شکل (۷) سعی شده است که تصویر رمز شده با قانون ۹۸ را با کلید دیگری رمزگشایی کرد. همان گونه که مشاهده می‌شود، رمزگشایی به صورت صحیح انجام نشده و تصویر به طور کامل نامفهوم است. در شکل های (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 آزمون های معرفی شده بر روی روش پیشنهادی به همراه دو روش Jin و Abdo بررسی شود.

۵-۱- تحلیل آماری

طبق نظریه شانون با استفاده از تحلیل های آماری^۱ می‌توان بسیاری از مسائل رمز را حل کرد. الگوریتم رمز باید به گونه ای باشد که دشواری تحلیل های آماری را بیش تر کند. تحلیل هیستوگرام و ضرایب همبستگی از مواردی است که برای ارزیابی تحلیل های آماری استفاده می‌شود. (ونگ و لوان، ۲۰۱۳).

۵-۱-۱ تحلیل هیستوگرام

یک الگوریتم رمزنگاری در صورتی مناسب است که تصویر به گونه ای رمز شود که هیچ گونه اطلاعاتی از تصویر اصلی در آن دیده نشود؛ به عبارتی در رمزنگاری باید تصویر به صورت بصری قابل تشخیص نباشد. با توجه به این که نتیجه آزمون بصری برای بینندگان مختلف متفاوت است، می‌توان از تحلیل هیستوگرام استفاده کرد. تحلیل هیستوگرام چگونگی توزیع پیکسل ها 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. همان طور که در شکل دیده می‌شود، هیستوگرام تصاویر رمز شده یکنواخت می‌باشد که این نشان دهنده کارایی الگوریتم رمزنگاری پیشنهادی می‌باشد.

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 به عنوان کلید در الگوریتم رمزنگاری استفاده شود.
۳- پیکسل های مذکور در هر سطر به صورت باینری در کنار یکدیگر قرار داده می‌شوند.

۴- این رشته دودویی به دو قسمت مساوی تقسیم می‌شود. (در جدول (۲) با توجه به اینکه $k=2$ تعیین شده است تقسیم رشته دودویی به دو قسمت مساوی همان مقادیر دودویی پیکسل ها می‌شود).

۵- دو رشته دودویی تولید شده به عنوان 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 بیت های رمز شده در خروجی اتوماتا در زمان t توسط عدد تصادفی تولیدی با اتوماتای سلولی دوم انجام می‌شود.

۷- رشته های بیتی در کنار یکدیگر قرار می‌گیرند.
۸- در مرحله بعد داده تصویر تولید شده پس از مرحله دوم به عنوان ورودی به اتوماتای سوم وارد می‌شود.

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

در مرحله رمزگشایی مراحل بالا به صورت معکوس اعمال می‌شود. با استفاده از تصویر رمز شده و کلیدی که به عنوان ماتریس رمز شده در زمان $t-1$ داده شده است، تصویر را طبق الگوریتم رمز به صورت معکوس، می‌توان رمزگشایی کرد. یک گام از اجرای قدم های 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 256×256 با کلیدهای متفاوت در ادامه نشان داده شده است. شکل های (۴) الی (۶) تصویر اصلی، تصویر رمز شده و تصویر رمزگشایی شده با قوانین ۳۰، ۹۸ و ۱۵۳ را به ترتیب نشان

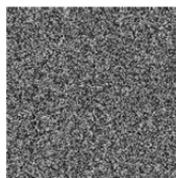
¹Statistical Analysis

(جدول - ۲): مثالی از عملکرد روش پیشنهادی

ماتریس اولیه		<table><tr><td>10</td><td>20</td><td>120</td></tr><tr><td>30</td><td>41</td><td>136</td></tr><tr><td>50</td><td>250</td><td>145</td></tr></table>	10	20	120	30	41	136	50	250	145
10	20	120									
30	41	136									
50	250	145									
مرحله نخست رمزنگاری	قدم ۱ و ۲ (k=2)	<table><tr><td>10</td><td>20</td></tr><tr><td>30</td><td>41</td></tr></table>	10	20	30	41					
	10	20									
	30	41									
	قدم ۳	<table><tr><td>0000101000010100</td></tr><tr><td>0001111000101001</td></tr></table>	0000101000010100	0001111000101001							
0000101000010100											
0001111000101001											
قدم ۴	<table><tr><td>00001010</td><td>00010100</td></tr><tr><td>00011110</td><td>00101001</td></tr></table>	00001010	00010100	00011110	00101001						
00001010	00010100										
00011110	00101001										
قدم ۵ (مرحله اجرای اتوماتا)	<table><tr><td>00001010</td><td>00010100</td></tr><tr><td>00011110</td><td>00101001</td></tr></table> Cellular Automata(1) <table><tr><td>t-1</td><td>10111000</td><td>00010001</td></tr><tr><td>t</td><td>01011001</td><td>10010000</td></tr></table>	00001010	00010100	00011110	00101001	t-1	10111000	00010001	t	01011001	10010000
00001010	00010100										
00011110	00101001										
t-1	10111000	00010001									
t	01011001	10010000									
مرحله دوم رمزنگاری	قدم ۶	<table><tr><td>10111000</td><td>00010001</td></tr><tr><td>01011001</td><td>10010000</td></tr></table> درهم ریزی <table><tr><td>00010001</td><td>10111000</td></tr><tr><td>10010000</td><td>01011001</td></tr></table> درهم ریزی	10111000	00010001	01011001	10010000	00010001	10111000	10010000	01011001	
	10111000	00010001									
01011001	10010000										
00010001	10111000										
10010000	01011001										
قدم ۷	<table><tr><td>t-1</td><td>0001000110111000</td></tr><tr><td>t</td><td>1001000001011001</td></tr></table>	t-1	0001000110111000	t	1001000001011001						
t-1	0001000110111000										
t	1001000001011001										
مرحله سوم رمزنگاری	قدم ۸ (مرحله اجرای اتوماتا)	<table><tr><td>0001000110111000</td></tr><tr><td>1001000001011001</td></tr></table> Cellular Automata(1) <table><tr><td>t-1</td><td>0101110001111010</td></tr><tr><td>t</td><td>1000110100001010</td></tr></table>	0001000110111000	1001000001011001	t-1	0101110001111010	t	1000110100001010			
	0001000110111000										
1001000001011001											
t-1	0101110001111010										
t	1000110100001010										
قدم ۹	<table><tr><td>01011100</td><td>01111010</td></tr><tr><td>10001101</td><td>00001010</td></tr></table> 141 10 92 123	01011100	01111010	10001101	00001010						
01011100	01111010										
10001101	00001010										



(ج) تصویر رمزگشایی شده



(ب) تصویر رمز شده

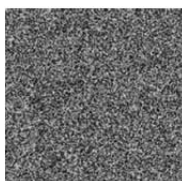


(الف) تصویر اصلی

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



(ج) تصویر رمزگشایی شده



(ب) تصویر رمز شده



(الف) تصویر اصلی

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



(ج) تصویر رمزگشایی شده



(ب) تصویر رمز شده



(الف) تصویر اصلی

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



(الف) تصویر رمز شده با قانون ۹۸ (ب) تصویر رمزگشایی با قانون ۱۵۰

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



(ج) تصویر رمزگشایی شده



(ب) تصویر رمز شده

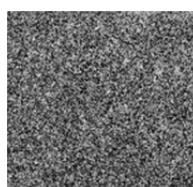


(الف) تصویر اصلی

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



(ج) تصویر رمزگشایی شده



(ب) تصویر رمز شده



(الف) تصویر اصلی

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



الف) تصویر اصلی



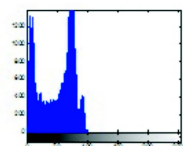
ب) تصویر رمز شده



ج) تصویر رمز گشایی شده

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

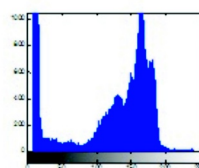
$$D(x) = \frac{1}{N} \sum_{j=1}^N (x_j - E(x))^2 \quad (۴)$$



الف) تصویر اصلی



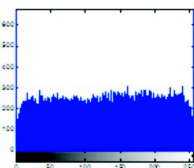
ب) هیستوگرام تصویر



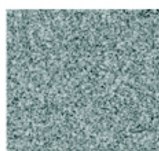
الف) تصویر اصلی



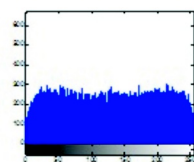
ب) هیستوگرام تصویر



الف) تصویر رمز شده با قانون ۹۸

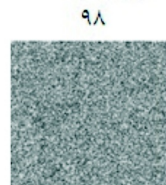


ب) هیستوگرام تصویر

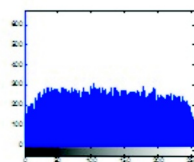


الف) تصویر رمز شده با قانون ۹۸

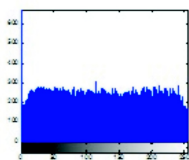
ب) هیستوگرام تصویر



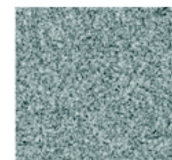
الف) تصویر رمز شده با قانون ۱۵۳



ب) هیستوگرام تصویر



الف) تصویر رمز شده با قانون ۱۵۳



ب) هیستوگرام تصویر

(شکل - ۱۱): نتایج هیستوگرام تصاویر رمز شده cameraman

(شکل - ۱۲): نتایج هیستوگرام تصاویر رمز شده boats

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

مقادیر تابع همبستگی در سه راستای عمودی، افقی و قطری برای تصویر cameraman و تصاویر رمز شده آن با قانون ۹۸ و ۱۵۳ با چهار الگوریتم معرفی شده توسط Wang, Abdo, Jin, Mohamed و الگوریتم پیشنهادی در جداول (۳ و ۴) به ترتیب آورده 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

۵-۱-۲- تحلیل ضرایب همبستگی

یکی دیگر از معیارهای ارزیابی برای تحلیل آماری، همبستگی است. هرچه همبستگی پیکسل‌های همسایه در تصویر رمز شده 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.

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

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

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

معرفی شده نسبت به دو روش مورد بررسی عملکرد بهتری دارد.

(جدول-۳): معیار همبستگی برای تصویر cameraman با قانون ۹۸

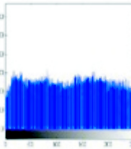
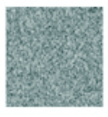
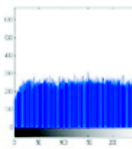
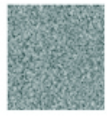
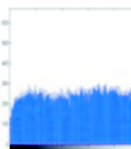
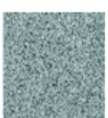
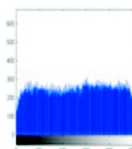
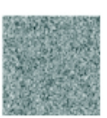
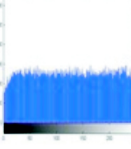
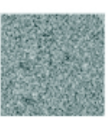
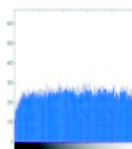
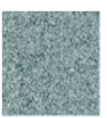
تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز روش Jin	-۰/۰۳۶۹	-۰/۰۳۸۳	۰/۰۱۱۴
تصویر رمز روش Abdo	۰/۰۱۲۲	۰/۰۱۴۹	-۰/۰۱۷۸
تصویر رمز روش Wang	-۰/۰۱۱۶	-۰/۰۱۷۶	۰/۰۰۶۸
تصویر رمز روش Mohamed	-۰/۰۲۰۴	۰/۰۰۳۳۷	۰/۰۱۱۳
تصویر رمز روش پیشنهادی	۰/۰۱۲۱	۰/۰۱۱۵	-۰/۰۰۰۰۶۷

(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	۰/۰۱۵۴	۰/۰۲۵۶۲	۰/۰۱۳۶۸
تصویر رمز روش پیشنهادی	-۰/۰۱۶۶	-۰/۰۰۵۲	-۰/۰۰۱۵

حساسیت بالایی دارد. در جدول (۵) نتیجه آزمون حساسیت نسبت به کلید نشان داده شده است. به منظور تشخیص تفاوت بین تصاویر رمز هیستوگرام تصاویر رمز ترسیم شده است تا مقایسه آنها آسان تر شود.

(جدول-۵): تحلیل حساسیت نسبت به کلید

مجموعه کلیدهای کمی متفاوت		مجموعه کلیدهای اصلی	
هیستوگرام	تصویر رمز	هیستوگرام	تصویر رمز
			
			
			

۵-۳- تمایز تصویر اصلی و رمز شده

یک خاصیت ایده آل برای تصویر رمز، حساس بودن نسبت به تغییرهای جزئی در تصویر اصلی است. در حمله های تفاضلی^۲، مهاجم تلاش می کند 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 می توان کلید را شناسایی کرد.

سه معیار^۳ $UACI$ ،^۴ MAE ،^۵ $NPCR$ برای آزمودن اثر تغییر یک پیکسل ورودی بر روی تصویر رمز شده است. هر چه این سه معیار بیش تر باشند، الگوریتم رمزنگاری عملکرد مطلوب تر دارد (کانسو و قبله، ۲۰۱۲).

۵-۲- تحلیل حساسیت نسبت به کلید

حساسیت نسبت به کلید، یکی دیگر از ویژگی های ضروری برای یک الگوریتم رمزنگاری مطلوب است. به این معنی که تغییر یک بیت در کلید خصوصی، بایستی یک تصویر رمز به طور کامل متفاوت تولید کند. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله جستجوی جامع^۱ تا حدی تضمین می کند.

برای ارزیابی ویژگی حساسیت نسبت به کلید ابتدا تصویر اصلی با کلید محرمانه اصلی رمزنگاری می شود؛ سپس کلید را کمی تغییر داده و تصویر اصلی دوباره رمزنگاری می شود. در صورتی که مقایسه این دو تصویر رمز به صورت بصری امکان پذیر نباشد، الگوریتم رمزنگاری نسبت به کلید

^۱Brute-Force Attack

^۲Differential Attack

^۳Unified Average Changing Intensity (UACI)

^۴Mean Absolute Error (MAE)

^۵Number of Pixel Change Rate (NPCR)

۵-۴- تحلیل آنتروپی

آنتروپی یکی دیگر از مشخصه‌های مهم تصادفی بودن الگوریتم است. آنتروپی طبق رابطه ۹ محاسبه می‌شود که در آن S تصویر رمز شده و $P(S_i)$ تعداد رخ دادهای S_i است. در حالت ایده‌آل برای یک تصویر رمز شده 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.

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

(جدول - ۷) : مقادیر آنتروپی برای روش‌های مختلف

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

۵-۵- تحلیل فضای کلید

به منظور جلوگیری از حمله جست‌وجوی جامع، فضای کلید الگوریتم رمزنگاری باید به حد کافی بزرگ باشد. فضای کلید الگوریتم شامل تعداد کل کلیدهای قابل استفاده در الگوریتم رمزنگاری است. هرچه اندازه فضای کلید رمزنگاری بزرگ‌تر باشد، زمان آزمایش 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 به صورت هم‌زمان در مرحله نخست، یک اتوماتا در مرحله دوم و یک اتوماتای دیگر در مرحله سوم استفاده می‌شود. با توجه به این که در هر اتوماتا از 2^8 قانون می‌توان استفاده کرد، فضای کلید $2^8 \times 2^8 \times 2^8 \times 2^8 = 2^{32} = 4294967296$ است؛ بنابراین ساختار پیشنهادی نسبت به حمله جست‌وجوی جامع مصون است. فضای کلید روش پیشنهادی نسبت به روش معرفی شده توسط Wang که برابر با 2^{28} می‌باشد، کم‌تر است.

۵-۶- تحلیل اجرایی

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

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

رابطه ۶ محاسبه NPCR را نشان می‌دهد که نرخ پیکسل‌های تغییر یافته تصویر رمز به ازای یک بیت تغییر در تصویر اصلی است (کانسو و قبله، ۲۰۱۲). نحوه محاسبه UACI در رابطه ۸ نشان داده شده است.

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

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

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

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

در جدول (۶) مقادیر توابع ارزیابی برای الگوریتم‌های معرفی شده 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

Asnaashari, M. and M. Meybodi (2007). "Irregular cellular learning automata and its application to clustering in sensor networks." Proceedings of 15th Conference 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 Recognition* 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 encryption 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 elementary cellular automata." *Optics & Laser Technology* 50(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 Science 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 Radiology and Surgery* 5(3): 251-262.

Mehrshad, 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 encryption schema for digital images using reversible cellular automata." *an International Journal of 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 using 3-state cellular automata." *Computer Vision and Image Understanding* 114(7): 790-802.

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

حمله های مختلف عملکرد خوبی داشته است. در این بخش نیز پیچیدگی محاسباتی و زمان اجرای الگوریتم بحث می شود. الگوریتم پیشنهادی در سه مرحله انجام می گیرد و شامل عملیات مختلف از جمله تولید اعداد تصادفی، محاسبات خطی اتوماتای سلولی، شیف دادن و XOR بیتی است. تمام این عملیات، پیاده سازی مستقیم دارند. بنابراین الگوریتم پیشنهادی از نظر محاسباتی کارآمد است.

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

پیاده سازی تمام الگوریتم ها بر روی سامانه CORE i3 و RAM 2GB صورت گرفته است.

۶- نتیجه گیری

اتوماتای سلولی یک ابزار مفید برای رمزنگاری است. با توجه به خاصیت تصادفی بودن اتوماتای سلولی، تصویر را به خوبی و با کیفیت بالا می توان رمز کرد. اتوماتای سلولی برگشت پذیر نیز این قابلیت را دارد تا بتوان روش های رمزنگاری برگشت پذیر بر روی تصویر را معرفی کرد.

روش پیشنهادی با استفاده از اتوماتای سلولی برگشت پذیر به رمزنگاری تصویر می پردازد. در این مقاله ساختار جدیدی برای رمزنگاری تصویر معرفی شد که در سه مرحله به رمزنگاری تصویر می پردازد. بدیهی است با توجه به برگشت پذیری اتوماتای سلولی مراحل رمزگشایی قابل اجرا است. نتایج اعمال این الگوریتم بر روی تصویر با روش های معرفی شده توسط Wang، Abdo، Jin و Mohamed توسط توابع ارزیابی مانند $NPCC$ ، MAE ، $UACI$ مقایسه شده است. نتایج نشان می دهد که این روش، توانایی بهتری برای رمزنگاری اطلاعات نسبت به روش های مورد بررسی دارد.

اتوماتای سلولی به دلیل گستردگی و انواع مختلف آن کاربرد زیادی در رمزنگاری دارد. در کارهای بعدی اتوماتای سلولی برگشت پذیر را با اتوماتای سلولی ترکیبی به طور هم زمان می توان به کار برد و الگوریتم های رمزنگاری جدیدی تولید کرد.

۷- مراجع

Abdo, A., et al. (2013). "A cryptosystem based on elementary cellular automata." *Communications in Nonlinear Science and Numerical Simulation* 18(1): 136-147.

cellular automata." International Symposium on Electronic Commerce and Security 938-941.

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 Technology 14(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 encryption 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 scrambling 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 رشته مهندسی کامپیوتر

(گرایش نرم افزار) و کارشناسی ارشد

را در مهندسی کامپیوتر (گرایش

هوش مصنوعی و رباتیک) در

سال‌های ۱۳۹۱ تا ۱۳۹۴ از دانشگاه یزد گرفت. زمینه پژوهشی مورد علاقه ایشان شامل پردازش تصاویر، رمزنگاری تصاویر است.

نشانی رایانامه ایشان عبارت است از:

z-mehrnahad@stu.yazd.ac.ir



علی محمد لطیف دارای دکترای

مهندسی کامپیوتر گرایش هوش

مصنوعی از دانشگاه صنعتی اصفهان

بوده و مدرک کارشناسی ارشد خود

را در رشته 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. زمینه پژوهشی مورد علاقه

ایشان شامل پردازش تصاویر دیجیتال، رمزنگاری تصاویر و

پنهان نگاری است.

نشانی رایانامه ایشان عبارت است از:

alatif@yazd.ac.ir