

مروری بر روش های رمزنگاری تصویر

۱- ناهید ابراهیمی زاده

۲- علی نودهی

دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران استادیار، گروه مهندسی کامپیوتر، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران

ali.nodehi84@gmail.com

nahid.ebrahimizade@gmail

چکیده - امنیت داده های تصویری در عصر دیجیتال به یکی از چالش های اساسی تبدیل شده است. رمزنگاری تصاویر از طریق تبدیل اطلاعات تصویر به قالبی تصادفی و غیرقابل درک، به عنوان راهکاری موثر برای محافظت از این داده ها در برابر دسترسی های غیرمجاز در نظر گرفته می شود. در این پژوهش به بررسی و ارزیابی روش های مختلف رمزنگاری تصاویر پرداخته شده است. هدف اصلی این پژوهش، یافتن روشی ایمن و کارآمد برای رمزنگاری تصاویر با توجه به ویژگی های مختلف آن ها، از جمله اندازه، نوع و میزان حساسیت اطلاعات است. برای ارزیابی عملکرد روش های مختلف، معیارهای امنیتی مختلفی همچون مقاومت در برابر حملات، حساسیت به تغییرات در کلید رمزنگاری و کیفیت تصویر پس از رمزگشایی در نظر گرفته شده است. نتایج این پژوهش نشان می دهد که ترکیب الگوریتم های درهم ساز با روش های رمزنگاری مبتنی بر آشوب، می تواند به بهبود امنیت و کارایی سیستم های رمزنگاری تصویر کمک کند. همچنین، با توجه به نتایج حاصل از این پژوهش، پیشنهاداتی برای طراحی سیستم های رمزنگاری تصویر ایمن تر ارائه شده است.

کلید واژه- کدگذاری DNA، رمزنگاری مبتنی بر آشوب، رمزنگاری تصویر، امنیت داده، الگوریتم های رمزنگاری

1- مقدمه

هوشمند را فراهم می کند که به صورت خودکار اجرا می شوند و به کاهش خطاهای انسانی کمک می کنند [۱].

رمزنگاری مبتنی بر آشوب به واسطه ویژگی های منحصر به فردی مانند حساسیت شدید به تغییرات کوچک در داده های ورودی و رفتار بسیار پیچیده و غیرقابل پیش بینی، توجه بسیاری از محققان را به خود جلب کرده است. این روش رمزنگاری به دلیل قابلیت ایجاد الگوهای تصادفی و پیچیده، پتانسیل بالایی برای ایجاد سیستم های امنیتی قوی دارد [۲]. تابع تبدیل آرنولد دارای ویژگی های مهمی از جمله ارگودیسیتی بالا و قابلیت ایجاد برش در تصویر است که آن را برای تحلیل رمز کاربردی می سازد. با این حال، این تابع برای استفاده در رمزنگاری مناسب نیست، زیرا تنها جایگاه پیکسل ها را تغییر می دهد و مقدار آن ها را دست نخورده باقی می گذارد. در نتیجه، هیستوگرام تصویر تغییری نمی کند و این مسئله مانعی برای کاربرد مؤثر آن در رمزنگاری ایجاد می کند [۳]. به دلیل مصرف انرژی بسیار کم، تراکم بالای اطلاعات و قابلیت پردازش موازی گسترده، رمزنگاری مبتنی بر DNA در سال های اخیر به یکی از

با گسترش روزافزون فناوری اطلاعات و تبادل گسترده داده های تصویری، اهمیت حفاظت از این داده ها در برابر دسترسی های غیرمجاز بیش از پیش احساس می شود. رمزنگاری به عنوان ابزاری قدرتمند برای تأمین امنیت اطلاعات، از طریق تبدیل داده ها به شکلی نامفهوم، از این داده ها در برابر تهدیدات مختلف محافظت می کند. در حوزه تصاویر، رمزنگاری نقش حیاتی در حفظ یکپارچگی و محرمانگی اطلاعات تصویری ایفا می کند. روش های نوینی مانند تبدیلات آرنولد، فناوری بلاک چین، سیستم های آشوبناک و کدگذاری DNA، به عنوان رویکردهای نوآورانه در رمزنگاری تصاویر مورد توجه قرار گرفته اند و به طور فزاینده ای در سیستم های امنیتی پیچیده مورد استفاده قرار می گیرند. در صنایع مختلف، از بلاک چین برای مدیریت زنجیره تأمین، ردیابی محصولات و کنترل کیفیت استفاده می شود. با استفاده از بلاک چین، می توان به طور دقیق تاریخچه هر محصول را ردیابی کرده و از اصالت آن اطمینان حاصل کرد. همچنین، بلاک چین امکان ایجاد قراردادهای

مراحل اولیه در MD5 شامل عملیات بولی بیتی، جمع اعداد صحیح و سپس چرخش یا انتقال بیت‌ها هستند [۶]. الگوریتم هش SHA که یک تابع هش رمزنگاری است، از MD5 متمایز بوده و امنیت بالاتری ارائه می‌دهد. از کاربردهای متداول آن می‌توان به ذخیره‌سازی کلمات عبور و امضاهای دیجیتال اشاره کرد. نتیجه‌ی هش ۲۵۶ بیتی تولید شده به ورودی تابع بستگی دارد. این الگوریتم از چهار بخش اصلی تشکیل می‌شود: ۱. اضافه کردن بیت‌های پرکننده: فرآیند با افزودن بیت‌های پرکننده به داده ورودی شروع می‌شود. ۲. افزودن بیت‌های طول: بیت‌های اضافی که طول پیام اصلی را نشان می‌دهند، به آن اضافه می‌شوند. ۳. مقداردهی اولیه بافر: در این مرحله، بافر به‌عنوان جزئی از الگوریتم مقداردهی می‌شود. ۴. الگوریتم فشرده‌سازی: در نهایت، الگوریتم فشرده‌سازی بر ورودی تکمیل‌شده اعمال شده و نتیجه نهایی هش را تولید می‌کند [۶]. با انجام این چهار مرحله، الگوریتم SHA یک فرایند هش امن و قابل اعتماد ایجاد می‌کند که آن را برای انواع مختلف کاربردهای رمزنگاری مناسب می‌سازد. الگوریتم SHA-256 به منظور تنظیم شرایط اولیه و پیکربندی‌های کنترل استفاده می‌شود. هش ۲۵۶ بیتی که توسط این الگوریتم شناخته‌شده تولید می‌شود، معادل یک عدد مبنای شانزده ۶۴ رقمی است. نکته جالب این است که حتی اگر دو تصویر تنها یک بیت با هم تفاوت داشته باشند، هش‌های آنها کاملاً متفاوت خواهد بود. این ویژگی قدرت رمزنگاری SHA-256 را افزایش می‌دهد و آن را برای کاربردهایی که تغییرات کوچک در داده‌ها باید منجر به تولید هش‌های کاملاً متفاوت شوند، بسیار مناسب می‌سازد [۷]. روش‌های رمزنگاری تصویر مبتنی بر نقشه‌های فوق آشوب ممریستور چهاربعدی از ویژگی‌های غیرخطی و رفتار غیرقابل پیش‌بینی این سیستم‌ها برای ایجاد کلیدهای رمزنگاری قوی استفاده می‌کنند. این نقشه‌ها با بهره‌گیری از جاذب‌های آشوبی چندگان، فضای کلید گسترده‌ای فراهم کرده و حساسیت بالایی به شرایط اولیه و پارامترها دارند که امنیت روش را در برابر حملات brute-force افزایش می‌دهد. در این

مباحث اصلی در حوزه تحقیقات رمزنگاری تبدیل شده است. پژوهش‌ها نشان می‌دهند که فناوری DNA علاوه بر تقویت سیستم‌های رمزنگاری، به شکل مؤثری مانع از حملات انتخاب متن آشکارا می‌شود. با این وجود، روش‌های رمزنگاری تصویری مبتنی بر DNA برخلاف مزایای خود با چالش‌هایی نیز مواجه‌اند. به ویژه، اصول رمزنگاری DNA در ترکیب با نگاشت‌های آشوبی با بُعد پایین، به دلیل قابلیت پیش‌بینی بیشتر، می‌توانند آسیب‌پذیری سیستم را افزایش دهند. برای حل این مشکلات در عملیات رمزنگاری، از توالی‌های آشوبی متفاوتی که از نگاشت‌های آشوبی با بُعد بالا بهره می‌برند، استفاده شده است. در این رویکرد، پارامترهای اولیه سیستم آشوبی توسط تصویر متن آشکار تعیین می‌گردند. در نتیجه، سیستم‌های رمزنگاری متنوعی به منظور رفع این چالش‌ها توسعه یافته‌اند [۴]. الگوریتم هش MD5 به راحتی قابل پیاده‌سازی است و می‌تواند برای پیام‌هایی با طول‌های مختلف یک "اثر انگشت" یا خلاصه پیام یکتا تولید کند. الگوریتم‌های هش، از جمله MD5، هر ورودی را با هر طولی که باشد، به یک مقدار ثابت تبدیل می‌کنند که طول آن وابسته به نوع الگوریتم استفاده شده است. MD5 که بخشی از خانواده الگوریتم‌های خلاصه پیام ۲ به شمار می‌آید، به عنوان نسخه‌ای بهبودیافته از الگوریتم پیشین خود، یعنی MD4، توسعه یافته است. تابع فشرده‌سازی در خانواده هش MD به ساختاری منسجم مجهز است که شامل توسعه پیام و اجرای متوالی چندین عملیات یا مرحله مرتبط می‌شود. معمولاً این فرآیندها بین سه تا پنج دور را شامل می‌شوند [۵]. گسترش پیام در الگوریتم MD5 به بهبود انتشار کلمات پیام کمک می‌کند و تضمین می‌نماید که هر بخش پیام چندین بار به کار گرفته شود. برای افزایش انتشار، از گسترش بازگشتی پیام استفاده می‌شود، به طوری که ورودی هر مرحله پیوند قوی با پیام اصلی دارد. بنابراین، هر تغییر کوچک در پیام می‌تواند مراحل متعددی را تحت تأثیر قرار داده و یک هش یا خلاصه پیام منحصر به فرد ایجاد کند.

¹ chosen-plaintext attacks

² Message Digest

کنند[۱۹]. الگوریتم‌های رمزنگاری تصویر مبتنی بر درخت مرکل و دنباله DNA به دلیل ویژگی‌های خاص خود، برای امنیت تصاویر بسیار مناسب هستند. درخت مرکل یک ساختار داده‌ی درختی مبتنی بر هش است که تغییر کوچک در هر گره برگ آن منجر به تغییرات بزرگ در گره ریشه می‌شود. این ویژگی حساسیت کلید را افزایش می‌دهد و امنیت کلیدهای رمزنگاری را تضمین می‌کند. استفاده از درخت مرکل در فرآیند تولید پارامترهای رمزنگاری باعث می‌شود که حتی تغییرات کوچک در کلید منجر به تولید کلیدهای کاملاً متفاوت شود[۲۱].

کارهای مرتبط در بخش دوم ساختار مقاله گنجانده شده است. ارزیابی تجربی در بخش سوم مطرح شده و سپس نتیجه‌گیری ارائه می‌شود. بخش بعدی به بررسی جدیدترین مدل‌هایی می‌پردازد که به‌طور خاص برای رمزنگاری تصاویر طراحی شده‌اند. این بخش اطلاعاتی در مورد نحوه عملکرد این مدل‌ها ارائه می‌دهد و ویژگی‌ها، نقاط قوت و ضعف آنها را شرح می‌دهد.

2- کارهای مرتبط

عبدالله و همکارانش یک روش مبتنی بر بلاک‌چین برای رمزنگاری تصاویر به نام BDIE-AOFOLS ارائه کرده‌اند که در آن از بهینه‌سازی محاسباتی سیستم لورنز مرتبه کسری بهره گرفته شده است. آنها همچنین یک روش نوآورانه برای رمزگشایی تصاویر رنگی رمزنگاری شده با استفاده از BDIE-AOFOLS توسعه داده‌اند. این روش برای محافظت از تصاویر از سه فرآیند کلیدی استفاده می‌کند: تولید کلید بهینه، رمزنگاری تصویر و فناوری بلاک‌چین. ابتدا تصاویر با استفاده از تکنیک FOLS رمزنگاری می‌شوند. سپس برای تکمیل فرآیند تولید کلید بهینه و به‌دست آوردن بالاترین مقدار PSNR، از الگوریتم AOA استفاده می‌شود. در نهایت، فناوری بلاک‌چین برای اطمینان از امنیت و حفظ مقادیر پیکسلی تصاویر رمزنگاری شده به کار گرفته می‌شود[۱]. تحقیقات شارکوی و همکارانش مدلی را ارائه می‌دهد که

روش‌ها، سیگنال‌های آشوبی تولیدشده توسط مدارهای ممریستوری به‌عنوان منبع تولید اعداد شبه‌تصادفی برای عملیات رمزنگاری، از جمله تولید جعبه‌های جانشین^۳، استفاده می‌شوند. پیاده‌سازی این سیستم‌ها بر روی سخت‌افزارهایی نظیر FPGA علاوه بر افزایش بازدهی، موجب کاهش مصرف توان و زمان اجرا می‌شود و آن‌ها را برای کاربردهای بلادرنگ مناسب می‌سازد[۱۸]. الگوریتم‌های رمزنگاری تصویر مبتنی بر الگوریتم ژنتیک و رمزنگاری منحنی بیضوی^۴ به دلیل ویژگی‌های منحصر به فردشان برای امنیت داده‌های تصویری بسیار مناسب هستند. رمزنگاری منحنی بیضوی به دلیل بهره‌گیری از خواص ریاضی پیچیده منحنی‌های بیضوی، امنیت بالایی را با کلیدهای کوتاه‌تر فراهم می‌کند. امنیت ECC بر حل مسئله‌ی لگاریتم گسسته منحنی بیضوی^۵ استوار است که یک مسئله بسیار پیچیده محاسباتی است. استفاده از ECC برای رمزنگاری مقادیر پیکسلی تصاویر، به ویژه با توجه به کارایی بالا و مصرف منابع کم، آن را برای کاربردهای تصویر مناسب می‌سازد. الگوریتم ژنتیک به عنوان یک روش بهینه‌سازی، برای بهبود فرآیند تولید کلید در رمزنگاری تصویر استفاده می‌شود. با شبیه‌سازی فرآیند تکامل طبیعی، GA مجموعه‌ای از کلیدهای احتمالی را ایجاد و بر اساس معیارهای خاصی (مانند نزدیکی به نقاط هدف روی منحنی بیضوی) بهینه‌سازی می‌کند. این فرآیند نه تنها امنیت کلیدها را افزایش می‌دهد بلکه امکان انعطاف‌پذیری بیشتری را در فضای کلید فراهم می‌آورد. در این الگوریتم‌ها، الگوریتم ژنتیک برای بهینه‌سازی فرآیند تولید کلیدهای ECC استفاده می‌شود، که باعث ایجاد کلیدهای قوی‌تر و غیرقابل پیش‌بینی‌تر می‌شود. این ترکیب موجب افزایش مقاومت در برابر حملات مختلف از جمله حملات آماری و bruteforce می‌شود. این ویژگی‌ها باعث شده است که این الگوریتم‌ها برای رمزنگاری تصاویر مناسب باشند و امنیت بالایی در انتقال داده‌های حساس تصویری فراهم

³ S-box

⁴ ECC

⁵ ECDLP

¹⁰LDCML (نقشه تفاوت لجستیک با حلقه) و دنباله‌های کدگذاری شده با DNA طراحی شده است. در این روش، ابتدا از تکنیک هش SHA-256 به همراه یک کلید مشخص برای تنظیم مقادیر و پیکربندی‌های اولیه سیستم LDCML استفاده می‌شود. فرآیند آشوبی تولیدشده توسط الگوریتم LDCML در ابتدا تصویر اصلی را به‌طور کامل غیرقابل خواندن می‌سازد. سپس، ماتریس حاصل از مرحله اول درهم‌سازی به یک ماتریس DNA تبدیل شده، کدگذاری می‌شود و در نهایت به صورت یک ساختار "C" بازچیدمان می‌گردد. برای تکمیل این فرآیند، یک قانون از پیش تعیین‌شده به ماتریس DNA اعمال می‌شود تا با افزودن دنباله آشوبی اضافی تولیدشده توسط سیستم LDCML، عملیات تبدیل انجام گیرد. ماتریس DNA به‌دست‌آمده از مرحله دوم درهم‌سازی برای پراکنده‌سازی و تولید تصویر رمزنگاری‌شده نهایی مورد استفاده قرار می‌گیرد. نتایج ارزیابی‌های امنیتی و آزمایش‌های شبیه‌سازی نشان‌دهنده امنیت بالای این الگوریتم و توانایی آن در مقابله با حملات رایج است [۸].

ابراهیم زارعی زفره روشی نوآورانه برای رمزنگاری تصاویر معرفی کرده است که ترکیبی از توابع درهم ساز، سیستم‌های آشوبی و محاسبات DNA را در یک طراحی ترکیبی به کار می‌گیرد. این روش به‌گونه‌ای طراحی شده است که تغییر یک بیت در تصویر اصلی یا کلید مخفی، تأثیر قابل توجهی بر شرایط ابتدایی و تنظیمات کنترل سیستم‌های آشوبی خواهد داشت. برای تحقق این امر، از توابع هش SHA256 و MD5 که از تصویر اصلی و کلید خصوصی استخراج می‌شوند، استفاده می‌شود. نتایج تجربی نشان می‌دهند که روش پیشنهادی امنیت بالاتری نسبت به روش‌های رمزنگاری تصویر پیشین ارائه می‌دهد و به اندازه کافی سریع است تا در کاربردهای عملی مورد استفاده قرار گیرد [۹]. وقاس خان و یونگ‌چنول بیون یک سیستم بلاک‌چین خصوصی و مجاز برای رمزنگاری تصاویر پیشنهاد داده‌اند که امنیت تصاویر را ارتقا می‌بخشد. با توجه به این

هدف آن حفظ قدرت کلید قوی در حین بهبود رمزنگاری تصاویر است. این مدل از سیستم فرا آشوب ممریستور^۶ برای ساخت ماتریس‌های X، Y، Z و W استفاده کرده و کلیدی ایجاد می‌کند که از ترکیب الگوریتم‌های هش SHA-256 و MD5 به‌دست می‌آید. پس از تولید کلید، تصویر منبع تحت تبدیل آرنولد قرار می‌گیرد. سپس تصاویر با استفاده از پنج نقشه آشوبی ترکیب می‌شوند. پس از آن، تصویر در ماتریس‌های کدگذاری شده با DNA و رمزگشایی شده از DNA توزیع می‌شود. دوازده معیار برای ارزیابی عملکرد مدل پیشنهادی بر روی نه تصویر پرترفدار اعمال می‌شود [۳]. چرف آویساوی و همکارانش روشی امن و کارآمد برای رمزنگاری و رمزگشایی تصاویر پزشکی معرفی کرده‌اند که از الگوریتم‌های هش (SHA-256، MD5)، نقشه‌های آشوب یک‌بعدی و ⁷DNA بهره می‌برد. این روش ابتدا یک کلید حساس و قوی تولید می‌کند که برای تبدیل تصویر اصلی به داده‌های تصویر از یک تابع هش استفاده می‌شود. سپس، تصویر پزشکی ابتدا با چرخش و جابه‌جایی دو بیت مهم‌تر آن پردازش می‌شود تا توالی‌های اضافی کدگذاری شده DNA کاهش یابند و پس‌زمینه سیاه تصویر کم شود. در مرحله بعد، با استفاده از نقشه لجستیک، قوانین DNA به‌طور پویا برای هر مقدار پیکسل ۲ بیتی انتخاب می‌شود که شامل کدگذاری و رمزگشایی DNA است. همچنین، فرایند آشفستگی و پخش^۸ با استفاده از عملیات XOR و نقشه خیمه^۹ انجام می‌گیرد. با اینکه این سیستم تنها روی تعداد محدودی از مجموعه‌های داده استاندارد آزمایش شده است و مقایسه‌های جامع مشکل است، نتایج نشان می‌دهند که فضای کلید گسترده است و نسبت به تغییرات کوچک حساس است [۲].

زینگ یوان وانگ و همکارانش روشی نوین برای رمزنگاری تصاویر ارائه داده‌اند که بر مبنای نقشه آشوبی

⁶ memristor

⁷ Deoxyribonucleic acid

⁸ Confusion-diffusion

⁹ Tent map

¹⁰ Logistic Difference Chaotic Map with Loop

تحلیل‌های آماری، ارزیابی حساسیت به نویز و بررسی مقاومت در برابر حملات تفاضلی تأیید شده است. این تحقیق می‌تواند به عنوان الگویی مؤثر برای توسعه سامانه‌های رمزنگاری بلادرنگ در حوزه‌هایی مانند کاربردهای پزشکی، نظامی و صنعتی مورد استفاده قرار گیرد [۱۸].

سانجی کومار و دیپمالا شارما در این مقاله یک روش نوین برای رمزنگاری تصاویر ارائه کرده‌اند که از ترکیب نقشه آشوب آرنولد، رمزنگاری منحنی بیضوی^{۱۵} و الگوریتم ژنتیک^{۱۶} استفاده می‌کند. در این روش، نقشه آشوب آرنولد برای جابجایی موقعیت پیکسل‌ها، ECC برای رمزنگاری مقادیر پیکسل با کلیدهای عمومی و خصوصی، و الگوریتم ژنتیک برای بهینه‌سازی فرآیند تولید کلید به کار گرفته شده‌اند. این ترکیب منحصربه‌فرد موجب افزایش سطح امنیت، بهبود تصادفی‌سازی و مقاومت بالا در برابر حملات رمزنگاری می‌شود. تحلیل‌های آماری نشان‌دهنده پراکندگی بالا و همبستگی نزدیک به صفر در تصویر رمزنگاری شده است که نشان‌دهنده استحکام الگوریتم پیشنهادی است. نتایج تجربی کارایی این روش را در رمزنگاری تصاویر حساس و محافظت از آنها در برابر دسترسی غیرمجاز و حملات احتمالی تأیید می‌کند [۱۹]. زینگ‌یوان وانگ و پنگ‌بو لیو یک مدل جدید مبتنی بر شبکه جفت‌شده‌ی نقشه‌های کاملاً آشوبی پیشنهاد داده‌اند که با بهره‌گیری از ویژگی‌های سیستم‌های آشوبی همچون حساسیت بالا به شرایط اولیه و رفتار غیرخطی پیچیده، برای رمزنگاری تصاویر به کار رفته است. نویسندگان ابتدا ساختار و ویژگی‌های نظری این شبکه جدید را معرفی کرده و سپس با استفاده از آن، یک الگوریتم رمزنگاری تصویر طراحی کرده‌اند. در این الگوریتم، داده‌های تصویری با اعمال تبدیل‌های آشوبی چندلایه و جفت‌شده به شکلی کارآمد و ایمن رمزگذاری می‌شوند. بررسی‌های عددی و آزمایش‌های شبیه‌سازی، کارایی بالای روش پیشنهادی را در تأمین

که بلاک‌چین از رمزنگاری غیرقابل شکستن استفاده می‌کند، هیچگونه آسیب‌پذیری امنیتی در محیط اینترنت اشیاء صنعتی^{۱۱} وجود ندارد. این روش از بلاک‌چین برای ذخیره‌سازی ایمن مقادیر پیکسلی رمزنگاری‌شده تصویر بهره می‌برد و بدین ترتیب حریم خصوصی و امنیت داده‌های تصویری حفظ می‌شود. مقاومت روش رمزنگاری پیشنهادی در برابر حملات موجود با استفاده از معیارهای مختلف سنجیده می‌شود. مقادیر انتروپی به دست آمده نشان‌دهنده مقاومت در برابر حملات از نوع جستجوی فراگیر^{۱۲} است، چرا که این مقادیر نزدیک به مقدار بهینه هشت قرار دارند. نتایج رمزنگاری‌شده نشان‌دهنده کارایی بالای این روش در جلوگیری از نشت داده‌ها و تأمین امنیت اطلاعات است. با این حال، همچنان برخی محدودیت‌ها از جمله سرعت تراکنش و توان پردازشی وجود دارند. برخی از دستگاه‌های IIoT مانند حسگرهایی که به شبکه متصل هستند به عنوان گره‌های بلاک‌چین، ممکن است به اندازه کافی حافظه یا قدرت پردازشی نداشته باشند. اگرچه خدمات وب ممکن است در رفع این مشکل کمک کنند، اما نیاز به تحقیقات بیشتر برای غلبه بر این چالش‌ها وجود دارد [۱۰]. ویجایاکومار و آهیلا در این مقاله، یک روش نوآورانه برای رمزنگاری تصاویر ارائه داده‌اند که بر مبنای نگاشت‌های فوق آشوبی چهاربعدی مبتنی بر میمریستور طراحی شده است. این روش با بهره‌گیری از جعبه جایگشتی (S-box) مبتنی بر آشوب و استفاده از اتوماتای سلولی، امنیت فرآیند رمزنگاری را بهبود می‌بخشد. پیاده‌سازی این الگوریتم بر روی سخت‌افزار FPGA نتایجی برجسته از جمله نرخ تغییر پیکسل 13 معادل 99.97٪، میانگین شدت تغییر^{۱۴} 33.4٪، و توان عملیاتی 163.84 Mbps را به همراه داشته است. این روش همچنین با مصرف توان کم و استفاده بهینه از منابع سخت‌افزاری، برتری خود را نسبت به الگوریتم‌های رمزنگاری متداول نشان می‌دهد. کارایی روش پیشنهادی با

¹¹ IIoT¹² Brute force¹³ NPCR¹⁴ UACI¹⁵ ECC¹⁶ GA

در این روش، نقشه‌های آشوبی چهاربعدی با تولید مقادیر تصادفی پیچیده و حساس به شرایط اولیه، امنیت بالایی را برای سیستم رمزنگاری فراهم می‌کنند. همچنین، استفاده از توالی‌های DNA به عنوان لایه‌ای اضافی در فرآیند رمزنگاری، پیچیدگی بیشتری به الگوریتم اضافه می‌کند و قابلیت مقاومت در برابر حملات مختلف را افزایش می‌دهد. این طرح شامل مراحل رمزنگاری و رمزگشایی است که به صورت خاص برای تصاویر رنگی طراحی شده‌اند و شامل جداسازی کانال‌های رنگی، اعمال عملیات آشوبی، و استفاده از کدگذاری DNA در هر کانال می‌شود. تحلیل‌های امنیتی و آزمایش‌های عددی ارائه شده در این مقاله نشان می‌دهند که روش پیشنهادی از مقاومت بالایی در برابر حملات آماری، حملات بازگشتی و سایر حملات رایج برخوردار بوده و می‌تواند به عنوان یک چارچوب مؤثر در حفاظت از داده‌های تصویری رنگی به کار رود [۲۳].

در این مقاله یک الگوریتم جدید و ایمن برای رمزنگاری تصاویر ارائه شده است که بر اساس ترکیب تکنیک‌های حسگر فشرده^{۱۷} و کدگذاری DNA طراحی شده است. این روش با بهره‌گیری از ویژگی کاهش ابعاد و فشرده‌سازی در حسگری فشرده، ضمن کاهش حجم داده‌های پردازشی، امنیت بالایی در برابر تحلیل‌های رمزنگاری فراهم می‌کند. همچنین، استفاده از کدگذاری DNA به عنوان یک لایه اضافی در فرآیند رمزنگاری، پیچیدگی و غیرقابل پیش‌بینی بودن الگوریتم را افزایش می‌دهد. الگوریتم پیشنهادی شامل سه مرحله اصلی است: فشرده‌سازی تصویر با حسگری فشرده، اعمال تبدیلات آشوبی و رمزنگاری مبتنی بر توالی‌های DNA.

تحلیل‌های امنیتی و شبیه‌سازی‌های عددی در این پژوهش نشان می‌دهند که روش پیشنهادی در برابر حملات مختلف، از جمله حملات تفاضلی و آماری، مقاوم است و عملکرد مطلوبی از نظر پیچیدگی محاسباتی و سرعت ارائه می‌دهد. این مطالعه چارچوبی مؤثر برای رمزنگاری تصاویر با حفظ

امنیت داده‌ها و مقاومت در برابر حملات مختلف نشان داده‌اند. این مقاله می‌تواند به عنوان یک پیشرفت نوآورانه در حوزه ترکیب سیستم‌های آشوبی و امنیت اطلاعات مورد استفاده قرار گیرد [۲۰]. در این مقاله یینگ سو و همکاران روشی را معرفی کرده‌اند که از تکنیک‌های پیشرفته‌ای نظیر جابه‌جایی سه‌بعدی در فضای تصویر، انتشار داده‌ها، درخت مرکب و کدهای DNA بهره می‌برد. این روش نوین با ترکیب خصوصیات غیرخطی سیستم‌های آشوبی و ویژگی‌های توزیع و انسجام ارائه شده توسط درخت مرکب، امنیت بالایی را در انتقال داده‌های تصویری فراهم می‌کند.

نویسندگان با استفاده از کدهای DNA، تبدیل‌های پیچیده و چندلایه‌ای را بر روی پیکسل‌های تصویر اعمال کرده‌اند تا حساسیت به داده‌های اولیه و مقاومت در برابر حملات تقویتی افزایش یابد. نتایج شبیه‌سازی نشان‌دهنده عملکرد برتر این روش در مقایسه با تکنیک‌های رمزنگاری مشابه در زمینه کارایی و امنیت است. این پژوهش در راستای تقویت امنیت تصاویر دیجیتال و کاربردهای آن در حوزه‌هایی مانند ارتباطات امن و ذخیره‌سازی اطلاعات ارزشمند است [۲۱].

در این مقاله نویسندگان یک روش نوین برای رمزنگاری تصاویر معرفی کرده‌اند که بر پایه‌ی ترکیب نقشه‌های آشوبی یک‌بعدی و کدگذاری تصادفی DNA توسعه یافته است. این روش با بهره‌گیری از خواص حساسیت بالا به شرایط اولیه در سیستم‌های آشوبی و ویژگی‌های منحصر به فرد کدگذاری DNA، امنیت و پیچیدگی فرآیند رمزنگاری را بهبود می‌بخشد. الگوریتم پیشنهادی ابتدا با تولید مقادیر آشوبی مبتنی بر یک نقشه‌ی یک‌بعدی به ایجاد کلیدهای رمزنگاری می‌پردازد و سپس با استفاده از تکنیک‌های کدگذاری DNA، تصویر اصلی را به صورت تصادفی و غیرقابل پیش‌بینی رمزگذاری می‌کند. نتایج شبیه‌سازی و تحلیل‌های امنیتی در این پژوهش نشان‌دهنده‌ی مقاومت بالای این طرح در برابر حملات مختلف و کارایی مناسب آن برای کاربردهای عملی در زمینه‌ی حفاظت از داده‌های تصویری است. این مطالعه می‌تواند به عنوان الگویی مؤثر برای توسعه روش‌های پیشرفته‌تر رمزنگاری با ترکیب مفاهیم آشوب و زیست‌محاسباتی به کار رود [۲۲]. سیمیاو وانگ و همکارانش در این مقاله یک روش پیشرفته برای رمزنگاری تصاویر رنگی پیشنهاد داده‌اند که از ترکیب نقشه‌های آشوبی چهاربعدی و توالی‌های DNA بهره می‌برد.

¹⁷ Compressive Sensing

کیفیت و امنیت بالا ارائه می‌کند [۲۴].

3- ارزیابی تجربی

بخش‌های بعدی شامل معیارهای عملکرد، نتایج ارزیابی‌های تجربی و تفسیر یافته‌ها در برخی کارهای مرتبط هستند.

3-1- تحلیل کلید

کلیدهای رمزنگاری برای حفاظت از محرمانگی داده‌ها در رمزنگاری تصاویر از اهمیت بالایی برخوردارند. در ارزیابی قدرت یک کلید، دو عامل حساسیت کلید و فضای کلید مورد توجه قرار می‌گیرند. حساسیت کلید به این معناست که حتی کوچک‌ترین تغییر در کلید رمزنگاری منجر به غیرقابل بازیابی شدن تصویر رمزنگاری شده گردد. بنابراین، یک الگوریتم رمزنگاری موثر باید از حساسیت بالا و فضای کلید وسیع برخوردار باشد [۱۱].

3-2- تحلیل فضای کلید

یک الگوریتم رمزنگاری قدرتمند باید دارای فضای کلید بزرگ و حساس به تغییرات مقدار کلید باشد [۱۲]. به منظور مقابله با حملات جستجوی فراگیر^{۱۸}، فضای کلید باید حداقل برابر با 2^{100} باشد [۲-۳].

3-3- تحلیل حملات آماری

برای ارزیابی مقاومت الگوریتم پیشنهادی در برابر حملات آماری و تحلیل همبستگی بین پیکسل‌های مجاور در تصاویر رمزنگاری شده از محاسبه آنتروپی اطلاعات و بررسی هیستوگرام استفاده می‌شود.

1-1-1- تحلیل هیستوگرام

برای تحلیل توزیع شدت پیکسل‌های یک تصویر، از هیستوگرام استفاده می‌شود. در فرآیند رمزنگاری تصویر،

ضروری است که هیستوگرام تصویر رمزنگاری شده به طور کامل با هیستوگرام تصویر اصلی تفاوت داشته باشد. معمولاً توزیع شدت پیکسل‌ها در تصویر اصلی یکنواخت نیست، در حالی که هیستوگرام تصویر رمزنگاری شده باید توزیع یکنواختی را نشان دهد [۱۱]. تحلیل هیستوگرام اطمینان حاصل می‌کند که مقادیر به‌طور مناسب توزیع شده و تصویر اصلی به‌طور مؤثری مخفی می‌ماند [۳].

$$\text{var}(Z) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (z_i - z_j)^2 \quad (1)$$

در این معادله، مقادیر هیستوگرام با Z نشان داده می‌شوند و تعداد پیکسل‌هایی که دارای مقادیر خاکستری معادل i و j هستند، به صورت (Z_i, Z_j) بیان می‌شود. در یک سیستم رمزنگاری مؤثر، واریانس تصویر رمزنگاری شده باید به طور ایده‌آل کمتر از واریانس تصویر اصلی باشد. این رابطه تأکید می‌کند که هدف اصلی در رمزنگاری، دستیابی به واریانس پایین در هیستوگرام تصویر رمزنگاری شده است که نشان‌دهنده توزیع یکنواخت‌تر و ایمن‌تر مقادیر پیکسل‌ها می‌باشد.

1-1-2- تحلیل ضرایب همبستگی^{۱۹}

ضریب همبستگی ارتباط بین پیکسل‌های مختلف یک تصویر دیجیتال را نشان می‌دهد. در تصاویر ساده، پیکسل‌های مجاور معمولاً در ابعاد قطری، افقی و عمودی همبستگی بالایی دارند. برای مقابله با حملات آماری، رمزنگاری تصویر باید ارتباط بین پیکسل‌های مجاور در تصویر رمزنگاری شده را به میزان زیادی کاهش دهد.

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

(۳)

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (4)$$

(۴)

¹⁹ Analysis of Correlation Coefficients(CCA)

¹⁸ Brute force

1-1-4- نسبت سیگنال به نویز اوج²¹

PSNR تفاوت مقادیر پیکسل‌ها در تصاویر اصلی و رمزنگاری شده را نشان می‌دهد. در یک تصویر رمزنگاری شده، مقدار PSNR کمتر خواهد بود، زیرا عدد بالاتر PSNR به معنای کیفیت بهتر تصویر است. مقدار ایده آل PSNR برای تصاویر رمزنگاری شده کمتر از ۱۰ دسی بل می‌باشد [۱۶]. برای محاسبه PSNR، از فرمول زیر استفاده می‌شود:

(۷)

$$PSNR = 10 \times \log_{10} \frac{M \times N \times 255^2}{\sum_{m=1}^M \sum_{n=1}^N |C1(i,j) - C2(i,j)|^2}$$

1-1-5- خطای میانگین مربعات²²

این معیار برای ارزیابی ویژگی‌های انتشار در یک تصویر رمزنگاری شده به کار می‌رود. طبق تئوری، انتظار می‌رود مقدار این معیار بیش از ۱۰,۰۰۰ باشد [۳]. محاسبه MSE بر اساس رابطه زیر به دست می‌آید.

(۸)

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - C(i,j))^2$$

$I(i, j)$ مقدار پیکسل‌های تصویر اصلی و $C(i, j)$ مقدار پیکسل‌های تصویر رمزگذاری شده را نشان می‌دهند، که در اینجا M و N ابعاد تصویر است.

1-1-6- تحلیل حملات تفاضلی

تحلیل حملات تفاضلی به منظور ارزیابی این موضوع انجام می‌شود که چگونه تغییرات کوچک در یک پیکسل در تصویر رمزگذاری شده می‌تواند تصویر اصلی را تحت تأثیر قرار دهد. این تحلیل مستلزم آن است که تصویر اولیه و

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$

(۵)

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

حروف x و y به ترتیب نمایانگر میانگین واریانس و مقادیر خاکستری دو پیکسل مجاور هستند، در حالی که کوواریانس با نمادهای $D(x)$ ، $\text{cov}(x, y)$ و N نشان داده می‌شود. زمانی که ضریب همبستگی به مقدار صفر نزدیک باشد، این امر نشان‌دهنده آن است که تصویر رمزنگاری شده ارتباطات کمتری بین پیکسل‌های مجاور خود دارد که این ویژگی به عنوان یک نتیجه مطلوب در نظر گرفته می‌شود.

1-1-3- تحلیل آنتروپی اطلاعات

آنتروپی به عنوان معیاری برای ارزیابی بی‌نظمی و توزیع مقادیر خاکستری در یک تصویر، نقش مهمی در یک سیستم رمزنگاری ایفا می‌کند. هر چه مقدار آنتروپی اطلاعات^{۲۰} افزایش یابد، توزیع مقادیر پیکسل‌های خاکستری به یکنواختی بیشتری خواهد رسید [۱۵].

برای محاسبه آنتروپی از فرمول زیر استفاده می‌شود:

$$H(x) = - \sum_{i=1}^L p(x_i) \log_2 p(x_i) \quad (۶)$$

در اینجا $p(x_i)$ نمایانگر احتمال وقوع مقدار x_i توسط منبع اطلاعات x است. بیشترین مقدار آنتروپی برای یک تصویر خاکستری با عمق ۸ بیت برابر ۸ است. به این ترتیب، هر چه مقدار آنتروپی به ۸ نزدیک‌تر شود، سیستم رمزنگاری بزرگ‌تر و تصادفی‌تر خواهد شد.

²¹ PSNR

²² Mean Square error(MSE)

²⁰ Information Entropy(IE)

در اینجا $C1(i,j)$ و $C2(i,j)$ تصاویر رمزنگاری شده را نشان می‌دهند که هم قبل و هم بعد از تغییر پیکسل‌های تصویر اصلی هستند.

4- نتیجه گیری

تحقیق حاضر به بررسی روش‌های مختلف رمزنگاری تصویر پرداخته است، نتایج به‌دست‌آمده نشان داد که ترکیب الگوریتم‌های درهم ساز مانند SHA-256 و MD5 با روش‌های رمزنگاری مبتنی بر آشوب کارایی و امنیت بالاتری نسبت به استفاده از هر روش به صورت مستقل ارائه می‌دهد. تحلیل دقیق شاخص‌های امنیتی همچون مقاومت در برابر حملات آماری، حساسیت به تغییرات کلید رمزنگاری و کیفیت تصویر پس از رمزگشایی، مؤید کارایی روش‌های پیشنهادشده در این پژوهش بود.

با این وجود، برای کاربردهای واقعی و پیچیده‌تر، نیاز به توجه بیشتر به عواملی مانند سرعت اجرای الگوریتم‌ها، مصرف منابع محاسباتی و انعطاف‌پذیری در مواجهه با داده‌های متنوع وجود دارد. از این رو، ترکیب روش‌های درهم ساز قوی با الگوریتم‌های سبک‌تر و بهینه‌تر می‌تواند مسیری مناسب برای پژوهش‌های آتی باشد.

در پایان، این تحقیق پیشنهاد می‌کند که طراحی سیستم‌های رمزنگاری تصویر باید به گونه‌ای باشد که علاوه بر دستیابی به امنیت بالا، کارایی و انعطاف لازم را در مواجهه با نیازهای مختلف کاربران فراهم آورد. استفاده از روش‌های ترکیبی و بهره‌گیری از ویژگی‌های الگوریتم‌های مبتنی بر آشوب، رویکردی نویدبخش برای بهبود سیستم‌های رمزنگاری تصویر در آینده است.

5- مراجع

1. M. A. Alohali et al., "Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments," *Sustain.*, vol. 15, no. 6, 2023, doi: 10.3390/su15065133.
2. I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly correlated key-medical image for DNA-chaos based encryption," *IET Image*

تصویر تغییر یافته با یک کلید محرمانه یکسان رمزگذاری شوند. دو شاخص متداول برای ارزیابی حملات تفاضلی عبارتند از نرخ تغییر پیکسل‌ها^{۲۳} و شدت تغییرات میانگین یکپارچه^{۲۴}. این شاخص‌ها اطلاعات ارزشمندی درباره واکنش الگوریتم رمزنگاری به تغییرات کوچک در تصویر ورودی فراهم می‌کنند و به تحلیل کلی امنیت سیستم کمک می‌کنند.

7-1-1- نرخ تغییر پیکسل‌ها

نرخ تغییر تعداد پیکسل‌ها درصد پیکسل‌های متفاوت بین دو تصویر رمزگذاری شده را مشخص می‌کند. مقدار بالاتر NPCR نشان می‌دهد که روش رمزنگاری می‌تواند در برابر حملات تفاضلی مقاومت بیشتری داشته باشد [۱۱]. برای محاسبه NPCR می‌توان از فرمول زیر استفاده کرد [۱۷].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100\% \quad (9)$$

در این فرمول، N نشان‌دهنده تعداد کل پیکسل‌های تصویر است و "تعداد پیکسل‌های متفاوت" با استفاده از تابع $D(i,j)$ محاسبه می‌شود

$$D(i,j) = \begin{cases} 0 & \text{if } C1(i,j) = C2(i,j) \\ 1 & \text{if } C1(i,j) \neq C2(i,j) \end{cases}$$

اصطلاحات $C1(i,j)$ و $C2(i,j)$ به نسخه‌های رمزنگاری شده اصلی و تغییر یافته تصاویر اشاره دارند. در همین حال، $D(i,j)$ تفاوت مقادیر پیکسل‌ها بین تصاویر رمزنگاری شده اصلی و نسخه‌های تغییر یافته آن‌ها را نشان می‌دهد.

۲-۴-۳- سیستم شدت تغییرات میانگین یکپارچه

تفاوت شدت متوسط بین دو تصویر رمزنگاری شده را می‌توان با استفاده از سیستم شدت تغییرات متوسط یکپارچه محاسبه کرد [۱۱]. این سیستم تعریف زیر را دارد [۳]:

$$UACI = \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255 \times N} \times 100\% \quad (10)$$

²³ NPCR (Number of Pixel Change Rate)

²⁴ UACI (Unified Average Changing Intensity)

- 22787–22808, 2018, doi: 10.1007/s11042-017-5534-8.
14. X. Liu and T. Zhu, "Deep learning for constructing microblog behavior representation to identify social media user's personality," *PeerJ Comput. Sci.*, vol. 2016, no. 9, 2016, doi: 10.7717/peerj-cs.81.
 15. . P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimed. Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, 2016, doi: 10.1007/s11042-015-2573-x.
 16. . S. Chirakkarottu and S. Mathew, "A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography," *SN Appl. Sci.*, vol. 2, no. 1, 2020, doi: 10.1007/s42452-019-1685-8.
 17. Belazi, A., Abd El-Latif, A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 128, 155-170.
 18. Vijayakumar, M., & Ahilan, A. (2024). An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. *Ain Shams Engineering Journal*, 15(4), 102620.
 19. Kumar, S., & Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review*, 57(4), 87.
 20. Wang, X., & Liu, P. (2021). A new full chaos coupled mapping lattice and its application in privacy image encryption. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(3), 1291-1301.
 21. Su, Y., Wang, X., Xu, M., Zou, C., & Liu, H. (2023). A three-dimensional (3d) space permutation and diffusion technique for chaotic image encryption using Merkel tree and dna code. *Sensing and Imaging*, 24(1), 5.
 22. Liang, Q., & Zhu, C. (2023). A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. *Optics & Laser Technology*, 160, 109033.
 23. Wang, S., Peng, Q., & Du, B. (2022). Chaotic color image encryption based on 4D chaotic maps and DNA sequence. *Optics & Laser Technology*, 148, 107753.
 24. Bao, W., & Zhu, C. (2022). A secure and robust image encryption algorithm based on Process., vol. 15, no. 12, pp. 2770–2786, 2021, doi: 10.1049/ipr2.12261.
 3. N. H. Sharkawy, Y. M. Afify, W. Gad, and N. Badr, "Gray-Scale Image Encryption Using DNA Operations," *IEEE Access*, vol. 10, pp. 63004–63019, 2022.
 4. Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, "Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation," *Opt. Lasers Eng.*, vol. 143, no. April, p., 2021, 106626 doi: 10.1016/j.optlaseng.2021.106626.
 5. R. Rivest, "The MD5 message-digest algorithm," 1992.
 6. V. Mekathoti and B. Nithya, A Survey on Congestion Control Algorithms of Wireless Body Area Network, vol. 735 LNEE. 2021.
 7. H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. with Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010, doi: 10.1016/j.camwa.2010.03.017.
 8. X. Wang, W. Xue, and J. An, "Image encryption algorithm based on LDCML and DNA coding sequence," *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 591–614, 2021, doi: 10.1007/s11042-020-09688-7.
 9. E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimed. Tools Appl.*, vol. 79, no. 33–34, pp. 24993–25022, 2020, doi: 10.1007/s11042-020-09111-1.
 10. P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, 2020, doi: 10.3390/e22020175.
 11. U. Zia et al., "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, 2022, doi: 10.1007/s10207-022-00588-5.
 12. A. Soni and A. Kumar Acharya, "A Novel Image Encryption Approach using an Index based Chaos and DNAEncoding and its Performance Analysis," *Int. J. Comput. Appl.*, vol. 47, no. 23, pp. 1–6, 2012, doi:10.5120/7493-9944.
 13. . J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimed. Tools Appl.*, vol. 77, no. 17, pp.

compressive sensing and DNA coding.
Multimedia Tools and Applications, 81(11),
15977-15996.