Semnan University

Journal of Modeling in Engineering

Journal homepage: https://modelling.semnan.ac.ir/

ISSN: 2783-2538



Research Article

A New Binary Encoding Method using a Hybrid DNA and Genetic Algorithm Approach

Mohammad-Reza Pourmir [a], **Najme Ghanbari** [b,*]

[a] *Department of Computer Engineering, Faculty of Engineering, University of Zabol, Zabol, Iran*
[b] *Department of Electrical Engineering, Faculty of Engineering, University of Zabol, Zabol, Iran*

UNCORRECTED PROOF

PAPER INFO

Paper history:

Received: 2022-03-13
Revised: 2022-05-12
Accepted: 2022-10-19

Keywords:
DNA Sequencing,
Cryptography,
Bit Exchange,
Encoding,
Transformation,
Mutation,
Replication,
Genetic Algorithm.

ABSTRACT

In this paper a new genetic coding technique is proposed. The proposed method is unpredictable and more reliable than other methods. In the proposed method any digital data is converted to binary form and then goes through the steps of DNA sequencing, transformation, encoding, reproduction, mutation and finally transformation. The main steps of the proposed method are repeated several times (three or more times) and the encrypted data is transmitted as text or image files. On the other hand, in the proposed model the receiver is used to decrypt and transform the transmitted data into the original data. This technique often converts text to image and image to text. This increases the security and accuracy of data transmission. By employing multiple key sequences to increase propagation rate and uncertainty, the decryption process becomes significantly more difficult and intricate. This approach facilitates the development of a comprehensive encryption system. Experimental results show that the proposed method includes multi-layered defense steps based on multi-stage and genetic operations. This technique provides higher security against various attacks. The decrypted information is more suitable for use due to its fundamental differences from confidential information.

DOI: https://doi.org/10.22075/jme.2024.31282.2495

© 2024 Published by Semnan University Press.
This is an open access article under the CC-BY 4.0 license.(https://creativecommons.org/licenses/by/4.0/)

*** Najme Ghanbari.**
E-mail address: n.ghanbari@uoz.ac.ir

How to cite this article:

مقاله پژوهشی

یک روش رمزگذاری باینری جدید با استفاده از روش ترکیبی DNA و الگوریتم ژنتیک

محمدرضا پورمیر[۱]، نجمه قنبری[۲،*]

اطلاعات مقاله

دریافت مقاله: ۱۳۹۵/۰۳/۲۰
بازنگری مقاله: ۱۳۹۵/۰۶/۲۰
پذیرش مقاله: ۱۳۹۵/۰۷/۱۵

واژگان کلیدی:
توالی‌یابی DNA،
رمزنگاری،
تبادل بیت،
رمزگذاری،
تغییر شکل،
جهش،
تکثیر،
الگوریتم ژنتیک،

چکیده

در این مقاله یک تکنیک جدید رمزگذاری ژنتیکی پیشنهاد می‌شود.روش پیشنهادی غیرقابل پیش بینی بوده و نسبت به سایر روش‌ها قابل اعتمادتر می‌باشد.در روش پیشنهادی هر نوع داده دیجیتال ابتدا به شکل باینری تبدیل شده و سپس مراحل توالی‌یابی DNA، تغییر شکل، رمزگذاری، تولید مثل، جهش و در نهایت تغییر شکل را طی می‌کند. مراحل اصلی روش پیشنهادی چندین بار (سه بار یا بیشتر) تکرار شده و داده‌های رمزگذاری شده به صورت فایل‌های متنی یا تصویری منتقل می‌شوند. از طرف دیگر در مدل پیشنهادی از گیرنده به منظور رمزگشایی و تغییر شکل داده‌های انتقال‌یافته به داده‌های اصلی استفاده می‌شود. این تکنیک اغلب متن را به تصویر و تصویر را به متن تبدیل می‌کند. این کار موجب افزایش امنیت و دقت در انتقال داده‌ها می‌شود. استفاده از توالی‌های کلیدی متعدد برای افزایش میزان انتشار و عدم قطعیت، فرآیند رمزگشایی داده‌های رمزگذاری‌شده را دشوار و پیچیده‌تر کرده و امکان ایجاد یک سیستم رمزگذاری کامل را فراهم می‌کند. نتایج تجربی نشان می‌دهد که روش پیشنهادی شامل مراحل دفاعی چندلایه مبتنی بر عملیات‌های چندمرحله‌ای و ژنتیکی می‌باشد. این تکنیک در برابر حملات مختلف امنیت بالاتری را فراهم می‌کند. اطلاعات رمزگشایی شده به دلیل تفاوت‌های اساسی با اطلاعات محرمانه برای استفاده مناسب‌تر هستند.

DOI: https://doi.org/10.22075/jme.2024.31282.2495

© 2024 Published by Semnan University Press.
This is an open access article under the CC-BY 4.0 license.(https://creativecommons.org/licenses/by/4.0/)

UNCORRECTED PROOF

۱-مقدمه

در دنیای امروز داده‌ها به عنوان ارزشمندترین محتوا در جهان شناخته می‌شوند. روزانه میلیون‌ها داده در قالب متن، تصویر، ویدئو و غیره تولید می‌شود که از میان آنها تصاویر نقش مهمتری را در ارتباطات روزمره ایفا می‌کنند. به عنوان مثال تصاویر پزشکی، نظامی و غیره بسیار محرمانه هستند و انتقال ایمن این تصاویر به دلیل آسیب‌پذیری داده‌ها یک چالش بزرگ محسوب می‌شود. از این رو محققان به توسعه الگوریتم‌های رمزنگاری پرداخته‌اند. به عنوان مثال در [۱] یک سیستم رمزگذاری نامتقارن مبتنی بر الگوریتم منحنی بیضی و رمزگذاری اسکن نوری پیشنهاد شده است. در [۲] نیز با استفاده از حالت‌های قطبش دوتایی نور یک سیستم رمزگذاری تصاویر معرفی شده است. در [۳] یک معیار از رمزگذارهای طبقه‌بندی شده به منظور کاربرد در طبقه-بندی‌کننده باینری پیشنهاد شده است. رمزنگاری DNA (اسید دئوکسی ریبونوکلئیک بیولوژیکی) یکی از فناوری‌هایی است که به عنوان الگوریتم‌های شکست‌ناپذیر شناخته شده و عملکرد خوبی را از خود نشان داده است. این فناوری به سرعت در حال رشد است و به طراحی و پیاده‌سازی الگوریتم‌های پیچیده‌تر و مقاوم‌تر در برابر حملات هکرها کمک می‌کند. از مزایای محاسبات DNA می‌توان به سرعت بالاتر، حداقل ذخیره‌سازی مورد نیاز و مصرف انرژی کمتر اشاره کرد. رمزنگاری DNA در تکنیک‌های رمزنگاری شناخته‌شده به کار می‌رود. در این

استناد به این مقاله: نحوه استناد فارسی در اینجا درج گردد.

تکنیک‌ها ویژگی‌های منحصر به فرد DNA مورد استفاده قرار می‌گیرد. امروزه چندین سیستم رمزنگاری DNA به عنوان رویکردهای الگوریتمی یا به عنوان بخش‌های جدایی‌ناپذیر از برنامه‌های حفظ حریم خصوصی داده‌ها پیشنهاد شده‌اند.رویکردهای الگوریتمی که عملیات بیولوژیکی و ریاضی را ترکیب می‌کنند، توسط تحقیقات محدودی برای برآورده‌کردن نیازهای بهینه‌سازی سیستم مورد مطالعه قرار گرفته‌اند. همچنین سیستم‌های رمزنگاری DNA امنیت چندلایه‌ای را در برنامه‌های کاربردی فراهم می‌کنند. در ادامه به مرور تکنیک‌های رمزنگاری DNA پرداخته و روش‌های پیشنهادی توسط محققان اخیر مورد بررسی قرار می‌گیرد. در [۴] با استفاده از تکنیک ژنتیک و توابع منطقی-ریاضی یک روش جدید امنیت داده برای رایانش ابری پیشنهاد شده است. در [۵] برای تخمین پارامترهای سیستم های دینامیکی یک روش با استفاده از الگوریتم ژنتیک مبتنی بر DNA ترکیبی پیشنهاد شده است. همچنین یک روش با استفاده از الگوریتم ژنتیک مبتنی بر DNA برای تخمین پارامتر در واکنش هیدروژناسیون در [۶] ارائه شده است. در [۷] یک الگوریتم رمزگذاری جدید برای ملودی‌ها و نت‌های موسیقی با استفاده از DNA معرفی شده است. در [۸] نیز یک روش جدید درهم‌سازی کلید با استفاده از DNA برای رمزگذاری تصاویر معرفی شده که برخی محدودیت‌های روش DNA در آن مرتفع شده است. در [۹] برای شناسایی مناطق کدکننده پروتئین‌ها یک نمایش دوتایی جدید برای نمایش DNA با استفاده از تبدیل موجک گابور ارائه شده است. به کمک یادگیری عمیق یک روش رمزگذاری جدید DNA مبتنی بر فرکانس جدید برای پیش‌بینی تقویت‌کننده‌های DNA انسان و موش در [۱۰] پیشنهاد شده است. این روش دارای دو سناریو و چهار مرحله می‌باشد. در [۱۱] با استفاده از رمزگذاری پرتوگردابی یک روش رمزگذاری جدید برای تصاویر نامتقارن نوری به کمک DNA معرفی شده است. در واقع رمزگذاری تصاویر نوری بر اساس DNA از طریق گرداب‌های نوری انجام و در این روش دو سطح امنیت حاصل شده است. در [۱۲] یک روش رمزگذاری ترکیبی کوتاه‌تر با استفاده از DNA برای ذخیره‌سازی کارآمد داده معرفی شده است. در [۱۳] مروری بر روی روش‌های رمزگذاری DNA از سال ۲۰۱۸ به بعد انجام شده است. در [۱۴] یک روش برای رمزگشاهای موثر برای کدهای DNA و در [۱۵] روشی به منظور رمزگذاری اطلاعات غیربیولوژیکی به منظور ذخیره طولانی مدت آنها در DNA ارائه شده است. ارتباط نوری تصویر رمزگذاری DNA ایمن با استفاده از کلید مخفی پویا و Hyperchaos غیرمنحط در [۱۶] انجام شده است. در [۱۷] با استفاده از مدل ترکیبی CNN-DLSTM پیش‌بینی تقویت‌کننده‌ها در داده‌های توالی DNA صورت گرفته است. در این روش‌ها معمولا عملیات بیولوژیکی و ریاضی با هم ادغام می‌شود. اکثر مقالات مورد بررسی در این مرجع بر اساس اصول ریاضی نبوده و تجزیه و تحلیل امنیتی جامعی را ارائه نداده اند. برای چند دهه الگوریتم های رمزگذاری سنتی مانند RSA[1]، AES[2] و DES[3] ستون فقرات ارتباطات دیجیتالی ایمن بوده‌اند. این الگوریتم‌ها بر پایه‌ی اصول ریاضی ابداع شده‌اند و به دلیل قابلیت اطمینان و قدرت رمزنگاری بالای خود مورد اعتماد هستند. الگوریتم RSA یکی از متداول‌ترین تکنیک‌های رمزگذاری نامتقارن است، هرچند هزینه محاسباتی بالایی دارد. در سالهای اخیر الگوریتم های ژنتیک (GA[4]) به عنوان یک راهکار امیدوارکننده برای رفع محدودیت‌های روشهای سنتی رمزنگاری مورد توجه قرار گرفته اند. با الهام از اصول انتخاب طبیعی و ژنتیک، این الگوریتم‌ها قادر به پیمایش کارآمد فضاهای جستجوی گسترده هستند که آنها را به گزینه ای مناسب برای مسائل پیچیده رمزنگاری تبدیل می کند. با این حال هیچ روش رمزگذاری نمی‌تواند امنیت دائمی را تضمین کند. بنابراین انتخاب الگوریتم مناسب باید براساس سطح امنیت مورد نیاز، منابع محاسباتی موجود و الزامات خاص برنامه انجام شود. الگوریتم‌های ژنتیکی در رمزگذاری تصویر عملکرد قوی دارند و مقاومت خوبی در برابر حملات بیرحمانه نشان داده‌اند. مدل‌های مبتنی بر این الگوریتم‌ها همچنین در برابر حملات مبتنی بر آنتروپی و دیفرانسیل مستحکم هستند، که نشان‌دهنده پتانسیل آن‌ها برای ایجاد روش‌های رمزگذاری ایمن است. توانایی این الگوریتم‌ها در تطبیق پویا با شرایط در حال تغییر ، آن‌ها را انعطاف‌پذیرتر

[1] Rivest–Shamir–Adleman

[2] Advanced Encryption Standard

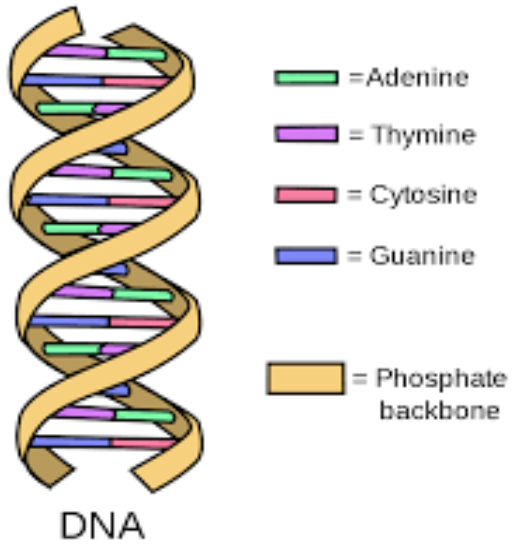
[3] Data Encryption Standard

[4] genetic algorithm

UNCORRECTED PROOF

و پاسخگوتر از روش‌های استاتیک سنتی می‌کند. الگوریتم ژنتیک (GA) و الگوریتم تکاملی تفاضلی (DE[5]) نمونه‌هایی از محاسبات تکاملی هستند. الگوریتم‌های ژنتیکی از فرآیند تولیدمثل ژنتیکی استفاده می‌کنند، در حالی‌که تکامل تفاضلی در واقع زیرمجموعه‌ای از فضای وسیع‌تر الگوریتم‌های ژنتیکی به شمار می‌آید. هر دو الگوریتم به دنبال یافتن بهترین راه‌حل از مجموعه‌ای از گزینه‌ها براساس یک معیار مشخص هستند. بهترین راه‌حل، راه‌حلی است که کمترین مقدار (یا بیشترین مقدار در صورت ماکزیمم‌سازی) را برای آن معیار ارائه دهد. معیار معمولاً به عنوان تابع جریمه یا تابع برازندگی تعریف می‌شود و می‌تواند بسته به مسئله مورد نظر شامل انرژی مصرف‌شده، سود، هزینه یا جریمه باشد. الگوریتم ژنتیک معمولاً برای هر مسئله به صورت سفارشی طراحی می‌شود، به این معنا که عملگرهای ژنتیکی بر اساس نوع نمایش راه‌حل انتخاب می‌شوند. مجموعه‌ای از عملگرها برای بردارهایی با مقادیر حقیقی، آرایه‌های بیتی، جایگشت‌ها و غیره وجود دارد. تکامل تفاضلی مجموعه‌ای از بردارهای حقیقی را تکامل داده و به همین دلیل برای تنظیم پارامترها در مدل‌های شبیه‌سازی مانند رگرسیون غیرخطی کاربرد دارد. مطالعات نشان داده‌اند که DE در حوزه‌های خاص عملکرد بهتری دارد. با این حال وقتی مسئله‌ای وجود دارد که DE برای آن مناسب نیست، الگوریتم ژنتیک می‌تواند گزینه بهتری باشد، زیرا GA تطبیق‌پذیری بیشتری داشته و انواع مختلف نمایش داده‌ها را مدیریت می‌کند. مکانیزم جستجوی اصلی DE بر پایه جهش تفاضلی است. این در حالی است که GA برای ترکیب راه‌حل‌ها به شدت بر عملگر تقاطع تکیه دارد. DE معمولاً برای مسائل عددی به‌ویژه مسائل با ابعاد بالا، ساده‌تر و کارآمدتر از GA در نظر گرفته می‌شود و جهش تفاضلی آن می‌تواند تنوع بیشتری در فرآیند جستجو ایجاد کند.

DNA (اسید دئوکسی ریبونوکلئیک بیولوژیکی) یک بیومولکول اسید نوکلئیک است که از واحدهای کوچکتری به نام نوکلئوتید تشکیل شده است. نوکلئوتیدها اطلاعات ژنتیکی موجودات زنده را در خود ذخیره می‌کنند. علاوه براین برخی از نوکلئوتیدها نقش مهمی در تنظیم زمان و شدت بیان ژن‌ها ایفا می‌کنند. یک نوکلئوتید DNA از سه جزء اصلی تشکیل شده است: یک قند پنج کربنی به نام دئوکسی‌ریبوز[6]، یک گروه فسفات، و یک باز نیتروژنی. در نوکلئوتیدهای DNA چهار نوع باز نیتروژنی وجود دارد: آدنین، گوانین، سیتوزین و تیمین. دانشمندان نوکلئوتیدها را با استفاده از حرف اول باز نیتروژنی آن‌ها یعنی آدنین(A)، گوانین (G)، سیتوزین (C) و تیمین(T) مشخص می‌کنند. نوکلئوتیدها به یکدیگر متصل می‌شوند و این اتصال ، بین قند دئوکسی‌ریبوز یک نوکلئوتید و گروه فسفات نوکلئوتید بعدی می‌باشد. این آرایش یک زنجیره متناوب از ساختار قند و گروه فسفات را ایجاد می‌کند که به عنوان ستون فقرات قند- فسفات شناخته می‌شود. نوکلئوتیدها به هر ترتیبی می‌توانند به هم متصل شوند، به این معنی که هر دنباله‌ای از بازهای نیتروژنی امکان‌پذیر است. شکل (۱) ساختار DNA را با توصیف اجزای اصلی نشان می‌دهد.



شکل ۱- توصیف اجزای اصلی ساختار DNA

در تحقیقات اخیر برای تامین محرمانگی داده‌ها و ایجاد الگوریتم‌های قوی از محاسبات DNA استفاده شده است. در زیست‌شناسی مولکولی، سخت‌افزار و بیوشیمی از محاسبات DNA به جای محاسبات الکترونیکی تراشه‌های الکترونیکی استفاده می‌شود. به جای استفاده از ارقام باینری صفر و یک که در روشهای سنتی به کار می‌روند، محاسبات DNA از چهار باز نیتروژنی برای نمایش داده‌ها و رمزگذاری اطلاعات ژنتیکی استفاده می‌کنند. این چهار پایگاه عبارتند از: A برای آدنین، G برای گوانین، C برای سیتوزین، و Tبرای تیمین (ادلمان،۱۹۹۴) [۱۸]. توانایی ایجاد

[5] Differential Evolution

[6] Deoxyribose

UNCORRECTED PROOF

توالی‌های کوتاه از DNA مصنوعی که به عنوان ورودی برای الگوریتم‌های رمزگذاری استفاده می‌شوند، منجر به معرفی روش‌های جدید رمزنگاری شده است. به همین دلیل در سال‌های اخیر تحقیقات در حوزه DNA توجه محققان بیشتری را به خود جلب کرده است.

نوآوری‌های اصلی مقاله به شرح زیر است:

- ارائه یک روش رمزنگاری مبتنی بر توالی‌های DNA با فضای کلید گسترده معادل ۲۵۶ بیت که مقاومت بالایی در برابر حملات brute-force دارد.
- استفاده از الگوریتم ژنتیک برای تولید خروجی‌های تصادفی و غیرقابل‌پیش‌بینی بدون همبستگی آشکار با داده‌های ورودی.
- ترکیب چندین سطح رمزگذاری DNA شامل تلاقی (crossover)، چرخش (rotation) و جهش (mutation) برای افزایش امنیت و مقاومت در برابر تحلیل‌های آماری و حملات پیشرفته.
- کاهش پیچیدگی محاسباتی از طریق طراحی مناسب عملگرهای ژنتیک به گونه‌ای که کارایی الگوریتم حفظ شود.
- ارائه چارچوبی قابل تعمیم برای رمزگذاری انواع داده‌ها شامل متن، تصویر و سیگنال با قابلیت انعطاف‌پذیری بالا در مدیریت داده‌های غیرعددی و گسسته.

۲-الگوریتم پیشنهادی

رمزنگاری DNA یکی از نمونه‌های اولیه و مهم در رمزنگاری مدرن به شمار می‌رود. DNA یک اسید نوکلئیک حاوی دستورالعمل‌ها و اطلاعات ژنتیکی است که از چهار باز نیتروژنی آدنین (A)، سیتوزین (C)، گوانین (G) و تیمین (T) تشکیل می‌شود. قابلیت پردازش موازی در مقیاس بالا از مهم‌ترین مزایای رمزنگاری مبتنی‌بر DNA است. ازاین‌رو رویکردهای رمزنگاری بیومولکولی بر پایه‌ی DNA طراحی شده و توسعه یافته‌اند. نسل جدید سیستم‌های کلید مبتنی‌بر DNA با هدف بهبود محاسبات از طریق ماتریس بسط کلید مبتنی‌بر DNA و طرح تولید سریع کلیدهای تصادفی معرفی شده است. این روش یک تکنیک نوین و منحصربه‌فرد مبتنی‌بر شبیه‌سازی بیولوژیکی برای رمزگذاری و رمزگشایی DNA ارائه می‌دهد. در این روش متن ساده به دو بخش تقسیم شده و هر بخش با استفاده از یک جدول رمزگذاری اختصاصی به دنباله‌های DNA ترجمه می‌شود. سپس با اعمال معیارهای پیشنهادی متن رمز نهایی تولید می‌گردد. در این مقاله یک الگوریتم جدید رمزنگاری DNA مبتنی‌بر تولید کلید متقارن ایمن پیشنهاد شده است. این الگوریتم شامل سه مرحله‌ی رمزگذاری، تولید کلید تصادفی و رمزگشایی می‌باشد. در مرحله‌ی نخست متن ورودی ابتدا به کد ASCII و سپس برای رمزگذاری به کد DNA تبدیل می‌شود. رمز اولیه حاصل از این فرآیند با استفاده از توالی‌های DNA تولیدشده توسط کلید تصادفی به رمز نهایی تبدیل می‌شود. همچنین یک تکنیک رمزگذاری ژنتیکی مبتنی‌بر DNA ارائه شده است که در آن اطلاعات محرمانه ابتدا به داده‌های باینری و سپس به توالی‌های DNA تبدیل می‌شوند. مدل پیشنهادی شامل یک الگوریتم تکراری است که هر اجرای آن یک تکرار نامیده می‌شود و تعداد این تکرارها می‌تواند سه یا بیشتر باشد. این تکنیک شامل چهار عملیات تکراری شامل رمزگذاری، روش‌های تغییرشکل و عملیات ژنتیکی است که برای تضمین امنیت و محرمانگی اطلاعات به‌کار می‌روند. علاوه بر این استفاده از یک کلید متقارن امکان رمزگذاری انواع قالب‌های داده‌ای نظیر متن، اسناد Word، تصاویر پیکسلی، صدا و ویدئو را فراهم می‌کند. نتایج مطالعات تجربی نشان می‌دهند که اطلاعات بازسازی‌شده نسخه‌ای استاندارد از اطلاعات محرمانه هستند. به عبارت دیگر نتایج تجربی نشان می‌دهد که روش پیشنهادی در شرایط ارزیابی‌شده، مقاومت قابل توجهی در برابر حملات آماری و حملات تفاضلی دارد. در ادامه مراحل روش پیشنهادی به تفصیل شرح داده می‌شود.

۲-۱- مرحله رمزگذاری

در این مرحله پس از خواندن داده‌های محرمانه و با توجه به نوع آن‌ها، اطلاعات لازم استخراج می‌شود. برای ترجمه مقادیر ASCII موجود در یک فایل متنی و تقسیم‌بندی آن‌ها به داده‌های باینری هشت‌بیتی هر دو بیت مجاور به یکی از چهار باز، آدنین (A)، سیتوزین (C)، گوانین (G) و تیمین (T) در DNA تبدیل می‌شوند. این فرآیند در جدول (۱) نشان داده شده است. به عبارت دیگر در صورت وجود متن در فایل داده‌ها ، این متن به صورت باینری هشت‌بیتی خوانده شده و سپس هر دو بیت مجاور به یکی از بازهای مذکور تبدیل می‌شوند.

UNCORRECTED PROOF

جدول ۱- DNA و نمایش بیت‌ها

بیت ها	DNA
00	A
01	C
10	G
11	T

یک فرم باینری مانند پیام، تصویر، ویدئو یا سیگنال می‌تواند نمایانگر هر نوع داده‌ای باشد. داده‌های باینری به کلاس‌های هشت‌بیتی تقسیم می‌شوند و هر یک از چهار باز آدنین(A)، سیتوزین(C)، گوانین (G) و تیمین (T) در DNA به یک جفت بیت مجاور اختصاص می‌یابد. به عبارت دیگر می‌توان رشته‌ی بیتی مربوط به داده‌های محرمانه را به‌عنوان یک فایل باینری در نظر گرفت و این فایل را به گروه‌هایی از بایت‌ها با اندازه‌ی دلخواه تقسیم کرد. به عنوان مثال رشته‌ی بیتی از داده‌های محرمانه را به شکل زیر داریم:

10 10 00 01 11 10 00 10 00 11

در این مرحله داده‌های فوق به یک توالی پایه‌ی DNA تبدیل می‌شوند و نتیجه‌ی این تبدیل به شکل زیر به دست می‌آید:

GGACTGCGAT

۲-۲- مرحله رمزگذاری

الگوریتم‌های رمزنگاری به دو دسته کلید متقارن و نامتقارن تقسیم می‌شوند. در الگوریتم‌های متقارن یک کلید مشترک میان فرستنده و گیرنده تبادل می‌شود. درحالیکه طرح‌های رمزنگاری نامتقارن از دو کلید مرتبط ریاضی استفاده می‌کنند. این کلیدها دارای دو نوع عمومی و خصوصی می‌باشند. مزیت اصلی الگوریتم‌های رمزنگاری متقارن سرعت بالای فرآیند رمزگذاری است. این ویژگی باعث می‌شود که رمزنگاری متقارن برای حجم‌های بالای داده مناسب‌تر باشد. به همین دلیل در روش پیشنهادی مقاله که مبتنی‌بر DNA می‌باشد، از کلید متقارن استفاده می‌شود.

رمزگذاری با استفاده از کلید متقارن پس از تبدیل داده‌های باینری به توالی‌های DNA انجام می‌شود. اگر داده‌های کلیدی و توالی‌های DNA به صورت باینری نمایش داده شوند، یک عملیات OR انحصاری (XOR) روی عناصر این توالی‌ها اعمال شده و نتیجه‌ی حاصل دوباره به توالی DNA تبدیل می‌شود. به عنوان مثال توالی DNA تولیدشده در مرحله‌ی قبل به صورت زیر است:

10 10 00 01 11 10 00 1000 11

اکنون توالی کلید ، به شکل زیر در نظر گرفته می‌شود:

00 10 11 11 11 11 00 1110 01

که بعد از عملیات OR انحصاری نتیجه زیر حاصل شده است:

10 00 11 10 00 01 00 0110 10

۲-۳-مرحله تغییر شکل[7]

یک الگوریتم ساده ژنتیک پس از مرحله‌ی رمزگذاری شامل سه عملگر تکثیر[8] (تولید مثل)، تلاقی[9] و جهش[10] است. فرآیند تغییرشکل برای تولید مواد ژنتیکی جدید به‌کار می‌رود و این مواد به‌صورت نسل‌های بعدی در قالب جمعیت کروموزوم‌ها منتقل می‌شوند. در این مرحله تعداد و طول کروموزوم‌های اولیه برای هر تکرار تعیین و این مقادیر می‌توانند ثابت یا متغیر باشند.

برای ایجاد کروموزوم‌های والد (جمعیت اولیه کروموزوم‌ها) با طول از پیش تعیین‌شده، تغییرشکل داده‌ها از طریق تراز کردن توالی‌های DNA و در ردیف‌ها انجام می‌گیرد. به عنوان مثال داده‌های حاصل از مرحله‌ی رمزگذاری به صورت زیر درنظر گرفته می‌شود:

GCCCGCACCGGAACAACGGGCGTTC
CGTCCGACCCCTTTCAACTATCAGTC
TTGTCAGGCTACCGATTATCAATGCG
CT

و جمعیت کروموزوم‌های به دست آمده به صورت زیر است:

GCCCGCACCGGAACAACGGGCGTTC
CGTCCGACCCCTTTCAACTATCAGTC

[7] Reshaping

[8] Replication

[9] Crossover

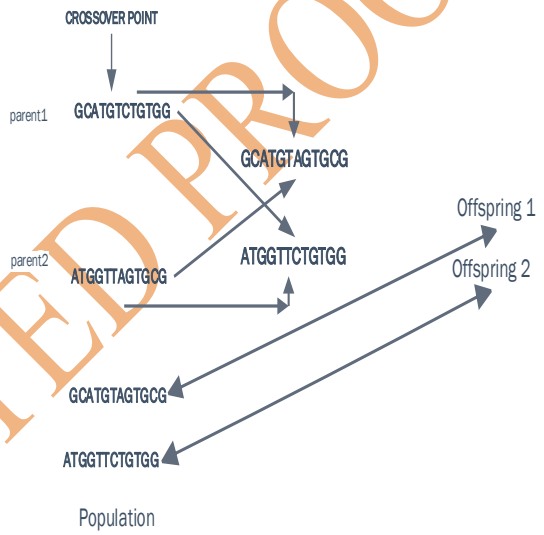
[10] Mutation

UNCORRECTED PROOF

TTGTCAGGCTACCGATTATCAATGCG CT

۲-۴-مرحله تلاقی یا Crossover

مرحله بعدی عملیات تلاقی است. در این مرحله دو روش برای ایجاد کروموزوم‌های والد وجود دارد. این روش‌ها می‌توانند به صورت متوالی در تکرارهای روش پیشنهادی مورد استفاده قرار گیرند. در روش اول والدین از استخر جفت‌گیری انتخاب شده و سپس یک نقطه تقاطع تک‌نقطه‌ای بین اولین و آخرین بیت کروموزوم‌های والد مشخص می‌شود. با تعویض بخش‌های ابتدایی والد اول و والد دوم دو فرزند جدید تولید می‌گردد.



شکل ۲- ایجاد دوفرزند با تعویض سر دو والد

در این روش فرزندان شامل بخش‌هایی از کدهای DNA هر دو والد هستند. نمونه‌ی این فرآیند در شکل (۲) نشان داده شده است. دومین روش تلاقی، روش چرخش است. در این روش پس از تراز کردن توالی‌های DNA در ردیف‌ها برای اعضای جمعیت کروموزومی، با استفاده از یک مقدار از پیش‌تعریف‌شده چرخشی به سمت چپ یا راست اعمال می‌شود. با فرض داده‌های محرمانه زیر خواهیم داشت:

0 1101 1010 0101 0101 111

اعمال چرخش تلاقی:

0 1010 1111 0110 1101 001

و اعمال تلاقی تک نقطه‌ای:

دو والد:

11 0110 0100 1001 0010 11

10 0100 0111 1011 1110 01

و دو فرزند:

11 0110 0100 1011 1110 01

10 0100 0111 1001 0010 11

به عبارت دیگر با تعویض بخش ابتدایی دو والد، دو فرزند جدید ایجاد می‌شود.

۲-۵-مرحله جهش Mutation

پس از فرآیند crossover بعضی کروموزوم‌ها در معرض جهش قرار گرفته و عناصر موجود در رشته دستخوش تغییر می‌شوند. برای انجام جهش دو روش مورد استفاده قرار می‌گیرد. در روش نخست داده‌ها به یک بردار باینری تبدیل شده و دو نقطه‌ی جهش بین بیت اول و بیت آخر تعیین می‌شود. سپس بیت‌های واقع در این نواحی مکمل می‌شوند. به عبارت دیگر جهش باعث تغییر بیت از صفر به یک و یا از یک به صفر می‌گردد. در روش دوم مطابق جدول (۲)، ابتدا هر چهار بیت به دو باز DNA تبدیل می‌شوند (برای مثال ۱۰۱۰ به CG تبدیل می‌شود) و رشته‌ی حاصل به یک بردار DNA تبدیل می‌گردد. سپس دو نقطه بین اولین و آخرین موقعیت تعیین شده و مقادیر موجود در این نواحی میان رشته‌های DNA جابه‌جا می‌شوند.

جدول۲- روش دوم برای انجام فرآیند جهش

DNA	Bits	DNA	Bits	DNA	Bits	DNA	Bits
TA	0000	GA	0100	CA	1000	AA	1100
TC	0001	GC	0101	CC	1001	AC	1101
TG	0010	GG	0110	CG	1010	AG	1110
TT	0011	GT	0111	CT	1011	AT	1111

مثال زیر نحوه انجام فرآیند جهش در روش پیشنهادی را نشان می‌دهد. فرض می‌شود رشته بیت قبل از جهش به صورت زیر باشد:

قبل از جهش:

11 0110 0100 1001 0010 11

بعد از جهش:

11 0101 1011 0110 1010 11

UNCORRECTED PROOF

و اعمال تغییر جهش:

قبل از جهش:

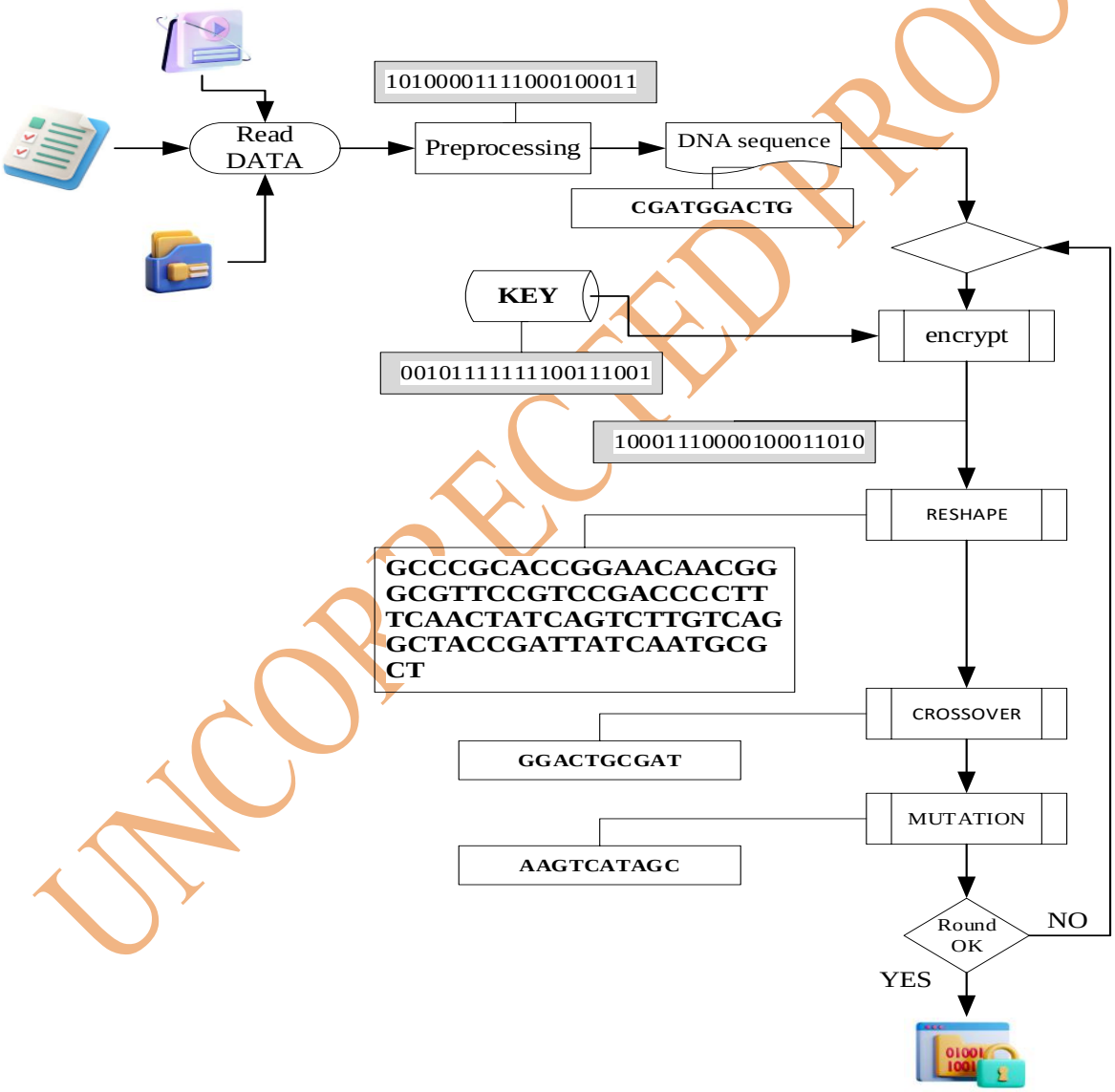
GGACTGCGAT

و بعد از جهش :

AAGTCATAGC

احتمال انجام عملیات رمزگذاری و تغییر شکل داده‌ها برای انتقال به دور بعدی تلاقی و جهش برابر با ۱۰۰٪ است. تعداد دورها وابسته به تعداد تکرارهای مساله بوده و از قبل تعیین می‌شود.

داده‌های رمزگذاری‌شده به‌صورت فایل متنی یا تصویر و در قالب داده‌های باینری قابل انتقال هستند. در سمت گیرنده داده‌های باینری، دریافت شده و به توالی‌های DNA تبدیل می‌گردند. سپس این توالی‌ها به فرمت اصلی بازتولید شده و عملیات رمزگشایی، تلاقی و جهش معکوس بر روی آن‌ها اعمال می‌شود. مراحل الگوریتم پیشنهادی در شکل (۳) نشان داده شده است.



شکل ۳-مراحل روش پیشنهادی رمزگذاری باینری

UNCORRECTED PROOF

برای هر نوع فایل داده و فرمت، مجموعه‌ای گسترده از تبدیل‌ها وجود دارد. از این رو مرحله پیش‌پردازش در توضیحات قبلی پیچیده و چالش‌برانگیز است. برای حل این مشکل تعمیم الگوریتم پیشنهادی به مقادیر ASCII، خواندن پیکسل‌های تصویر، جداسازی اجزا یا فریم‌ها و درنظر گرفتن ویژگی‌های فایل ویدیویی پیشنهاد می‌شود. دراین مرحله خواندن و پیش‌پردازش داده‌ها جایگزین عملیات پیچیده‌ی اولیه می‌شود. به نظر می‌رسد نیاز نوظهوری برای تعیین قدرت رمزنگاری به‌صورت عینی و نه صرفاً ذهنی و با توصیف‌های کیفی مانند «ضعیف»، «خوب» یا «قوی» وجود دارد. منطقی به نظر می‌رسد که برخی ویژگی‌های الگوریتم‌های رمزنگاری شناسایی شوند که این ویژگی‌ها می‌توانند به صورت مقادیر عددی عینی یا مقادیر ذهنی و صفتی بیان گردند. معیارهای استخراج شده می‌توانند برای ارزیابی و مقایسه الگوریتم‌های رمزنگاری و همچنین تعیین ارزش حفاظتی محصولات حاوی این الگوریتم‌ها مورد استفاده قرار گیرند. ویژگی‌های الگوریتم رمزگذاری که برای توسعه این معیارها در نظر گرفته شده‌اند، می‌توانند به شکل زیر بیان شوند:

- نوع کلید: متقارن (کلید مخفی یا یک کلید) یا نامتقارن (کلید عمومی یا دو کلید). هرچند به‌طور دقیق این ویژگی ممکن است یک معیار کامل برای سنجش امنیت نباشد اما نوع کلیدی که الگوریتم استفاده می‌کند برای کاربران اهمیت دارد و ارزش مشخص شدن را دارد. از آنجا که حملات میانبر می‌توانند بر روی الگوریتم‌های نامتقارن اعمال شوند، طول کلیدهای بسیار زیاد برای این الگوریتم‌ها مورد نیاز است. با افزایش طول کلید الگوریتم‌های دوکلیدی نسبت به الگوریتم‌های تک‌کلیدی به‌طور محسوسی کندتر عمل می‌کنند. این محدودیت استفاده مؤثر از الگوریتم‌های نامتقارن را به حوزه‌هایی با نیاز به مدیریت کلید محدود می‌کند، در حالی که الگوریتم‌های متقارن با مدیریت کلید ساده‌تر کارایی بالاتری دارند.
- محرمانه بودن پیام، یکپارچگی پیام، احراز هویت و امضای دیجیتال (مانند نوع الگوریتم) ممکن است به‌طور مستقل یک معیار کامل برای سنجش نباشند اما برای کاربران نهایی اهمیت دارند و ارزش بررسی و مشخص شدن را دارند.
- پیچیدگی: این ویژگی شامل پیچیدگی الگوریتم در رمزگذاری، رمزگشایی و تنظیم کلید است. این موارد می‌توانند به‌صورت تعداد عملیات مورد نیاز مانند عملیات روی بیت‌ها، ضرب مدولار و توان مدولار مشخص شوند. لازم به ذکر است که تعداد عملیات ثابت است و تنها سرعت اجرای الگوریتم ممکن است تغییر کند.
- بررسی عملکرد الگوریتم در برابر بهترین روش‌های شناخته‌شده حمله از جمله حملات brute force، factoring، تحلیل خطی (linear) و تحلیل تفاضلی (differential cryptanalysis).
- قدرت: ارزیابی میزان قدرت الگوریتم بر اساس عواملی مانند طول کلید، پیچیدگی الگوریتم و بهترین روش‌های شناخته‌شده حمله.

عملکرد رمزنگاری شامل تبدیل (رمزگذاری) اطلاعات با استفاده از کلیدهای مخفی به‌منظور تأمین محرمانگی و صحت اطلاعات است. یک سیستم رمزنگاری از فرآیندهای مربوط به محرمانگی، یکپارچگی، احراز هویت یا ترکیبی از آن‌ها تشکیل می‌شود. در یک الگوریتم رمزنگاری ، کلید تبدیل‌ها را پارامتردهی کرده و تبدیل‌های مرتبط با محرمانگی برای رمزگذاری و رمزگشایی به کار می‌روند. عملکرد رمزگذاری، داده‌های قابل فهم (متن ساده یا متن شفاف) را به داده‌های غیرقابل فهم تبدیل کرده و تابع رمزگشایی، متن رمز را به حالت اولیه (متن ساده) بازمی‌گرداند. الگوریتم‌های رمزنگاری، توابع ریاضی مورد استفاده در فرآیند رمزگذاری و رمزگشایی بوده و کارکرد هر سیستم رمزنگاری را تعیین می‌کنند. عملکردهای اصلی الگوریتم‌های رمزگذاری شامل تأمین محرمانگی و حفاظت

UNCORRECTED PROOF

از یکپارچگی پیام (احراز هویت و صحت) هستند. بطور مثال الگوریتم RSA می‌تواند برای رمزگذاری، رمزگشایی، تولید امضا و تأیید امضا به‌کار رود. همچنین الگوریتم امضای دیجیتال (DSA)، الگوریتم هش ایمن (SHA) و الگوریتم امضاکننده‌ی الگامال از طریق عملکردهای تولید و تأیید امضا، یکپارچگی پیام را تضمین می‌کنند. در سیستم‌های رمزنگاری متقارن ، امنیت تابعی از طول کلید است. هر چه طول کلید بیشتر باشد الگوریتم در برابر حمله‌ی جست‌وجوی فراگیر (Brute Force) مقاوم‌تر خواهد بود. از این رو، طول کلید معمولاً به‌عنوان نخستین معیار برای انتخاب الگوریتم رمزنگاری درنظر گرفته می‌شود. طول کلید یک معیار عددی و عینی است که معمولاً به‌صورت تعداد بیت بیان می‌شود. مفهوم «مراحل حمله» نیز به عنوان تعداد گام‌های لازم برای انجام بهترین حمله‌ی شناخته‌شده تعریف می‌شود. این عدد بدون نیاز به اجرای عملی حمله (که ممکن است امکان‌پذیر نباشد)، زمان مورد نیاز برای یک حمله‌ی موفق را بر اساس توان محاسباتی یک پردازنده‌ی مشخص تخمین می‌زند.

دانستن الگوریتم نباید امکان شکستن متن رمز را فراهم کند. آگاهی از الگوریتم نباید موجب کاهش قدرت رمزنگاری شود، هرچند می‌تواند منابع موردنیاز برای شکستن سیستم را به‌طور قابل توجهی کاهش دهد. الگوریتم DES سال‌هاست که به‌صورت عمومی منتشر شده، با این حال امنیت آن همچنان بر پیچیدگی ساختار الگوریتم و استفاده از یک کلید مخفی استوار است. در نهایت، وقوع یک حمله‌ی متنِ ساده و شناخته‌شده علیه هر کلید نباید ممکن باشد. برای تعیین قدرت یک الگوریتم باید بهترین روش‌های شناخته‌شده‌ی حمله و زمان موردنیاز برای اجرای این حملات با توجه به فناوری فعلی در نظر گرفته شود. در ادامه معیارهای ذکرشده در مورد مدل پیشنهادی بررسی و نتایج حاصل ارائه می‌شود. برای سهولت ارزیابی یک چک‌لیست پیشنهادی از ویژگی‌ها جهت استفاده رمزنگاران باتجربه ارائه شده است. در این روش توصیه می‌شود هنگام تخصیص مقادیر مربوط به قدرت الگوریتم که تا حدی نیازمند قضاوت کارشناسی است، مجموعه‌ای از معیارهای پذیرفته‌شده مانند موارد زیر مورد توجه قرار گیرد.

- بدون در اختیار داشتن کلید، استخراج متن ساده از متن رمزشده باید غیرممکن باشد.
- نباید هیچ حمله‌ی متن ساده‌ای وجود داشته باشد که از حمله‌ی جست‌وجوی کامل (Brute Force) کارآمدتر باشد.
- آگاهی از الگوریتم نباید موجب کاهش قدرت رمزنگاری شود.
- بین بیت‌های ورودی و یا بیت‌های کلید با بیت‌های خروجی نباید هیچ‌گونه وابستگی یا هم‌بستگی وجود داشته باشد.
- الگوریتم باید شامل ترکیبی از عملیات جایگزینی و جایگشت باشد به‌گونه‌ای که این عملیات ماهیتی غیرقابل معکوس‌سازی بدون کلید را داشته باشد.
- الگوها یا گروه‌های تکرارشونده‌ی بیت‌ها در متن ساده و همچنین در متن رمزشده کاملا پنهان و غیرقابل تشخیص باشند.
- هر کلید معتبر باید منجر به تولید یک متن رمز قوی شود. هرچند این ویژگی در برخی الگوریتم‌های مطرح مانند DES و بسیاری از الگوریتم‌های کلید عمومی همواره صدق نمی‌کند.
- طول متن رمز باید با طول متن ساده برابر باشد.

ما موارد فوق را در ادامه و در بررسی روش پیشنهادی به‌تفصیل بیان می‌کنیم تا بتوان معیارهای ارائه‌شده توسط رمزنگاران را با دقت بیشتری در مورد روش پیشنهادی ارزیابی کرد. هر الگوریتم رمزنگاری دارای نقاط قوت و ضعف بوده و مجموعه معیارهای فوق می‌تواند به‌عنوان مبنایی برای شناسایی این نقاط مورداستفاده قرار گیرد. قدرت یک الگوریتم مبتنی بر رمزگذاری DNA ، به میزان مقاومت الگوریتم در برابر انواع مختلف حملات رمزنگاری همراه با حفظ عملکرد قابل قبول اشاره دارد. در رمزنگاری DNA داده‌ها در قالب توالی‌هایی از نوکلئوتیدها کدگذاری شده و سپس با استفاده از عملیات بیولوژیکی یا محاسباتی دست‌کاری می‌شوند. قدرت در الگوریتم‌های مبتنی بر DNA به چند عامل اصلی بستگی دارد که عبارت‌اند از:

UNCORRECTED PROOF

- تعریف اندازه فضای کلید: هرچه فضای کلید بزرگ‌تر باشد حملات جست‌وجوی فراگیر (Brute-Force) دشوارتر یا غیرممکن می‌شوند و در نتیجه الگوریتم از قدرت بالاتری برخوردار است.
- آنتروپی بالا در تولید کلید: افزایش آنتروپی، غیرقابل پیش‌بینی بودن کلید را تضمین می‌کند. در رمزنگاری DNA اغلب از توالی‌های تصادفی DNA یا جهش‌های الهام‌گرفته از فرآیندهای بیولوژیکی برای افزایش ویژگی غیرقابل پیش‌بینی استفاده می‌شود.
- مقاومت در برابر حملات شناخته‌شده: فضای کلید بزرگ امکان جست‌وجوی جامع (Brute-Force) را محدود کرده و مقاومت الگوریتم را در برابر حملات شناخته‌شده افزایش می‌دهد.
- پیچیدگی رمزگذاری-رمزگشایی: الگوریتم‌های رمزنگاری DNA از نگاشت پویای باینری به DNA استفاده می‌کنند، به‌طوری که نگاشت در هر دور رمزگذاری تغییر می‌کند. این الگوریتم‌ها عملیات DNA مانند مکمل، معکوس، جایگزینی و پیوند را به‌کار می‌گیرند و برای کنترل تحولات از نقشه‌های آشفته یا الگوریتم‌های ژنتیک بهره می‌برند.
- امنیت چندلایه: ترکیب چندین سطح رمزگذاری DNA برای افزایش مقاومت الگوریتم در برابر حملات مختلف.
- یک الگوریتم رمزگذاری DNA باید از فضای کلید معادل ۲۵۶ بیت استفاده کند، فاقد سوگیری آماری قابل شناسایی بوده و در برابر حملات متن ساده مقاوم باشد. در این صورت الگوریتم از نظر امنیت رمزنگاری قوی محسوب می‌شود.

۳-نتایج تجربی ارزیابی روش پیشنهادی و تجزیه و تحلیل آن

الگوریتم‌های ژنتیک آشوبگر نیستند و رفتار تصادفی از خود نشان می‌دهند. پیچیدگی این الگوریتم‌ها به پیچیدگی عملگرهای مورداستفاده و نحوه‌ی پیاده‌سازی آن‌ها بستگی دارد. بنابراین با انتخاب و پیاده‌سازی مناسب عملگرها می‌توان پیچیدگی کلی الگوریتم را کاهش داده و در نتیجه هزینه‌ی محاسباتی را نیز کم کرد. یکی از مزایای مهم مدل پیشنهادی کاهش هزینه‌ی محاسباتی است. برای ارزیابی کارایی روش پیشنهادی آزمایش‌هایی بر روی مجموعه‌ای از داده‌های محرمانه‌ی مختلف و در برابر انواع حملات رمزنگاری، حملات ریاضی و حملات brute-force اجرا می‌شود. در حمله‌ی Brute-Force تمامی ترکیب‌های ممکن یک کلید و یا گذرواژه و تا زمان پیدا کردن ترکیب درست امتحان می‌شود. تحلیلگر رمز، تلاش می‌کند به هر داده‌ی رمزگذاری‌شده حمله کرده تا بتواند محتوای آن را بازیابی نماید. یک تکنیک رمزگذاری موفق باید در برابر این نوع حملات مقاوم باشد. از این‌رو ویژگی‌های مشخصی باید برای دستیابی به این مقاومت در نظر گرفته شوند. در روش پیشنهادی هیچ‌گونه هم‌بستگی میان مقادیر داده‌های حساس ، قبل و بعد از رمزگذاری وجود ندارد. فرآیند رمزگذاری به‌گونه‌ای انجام می‌شود که اجزای مختلف داده‌های محرمانه ترکیب شده و هیچ بخشی در جایگاه اصلی خود باقی نماند. این کار افزایش ابهام، پنهان‌سازی الگوها و بهبود امنیت در برابر تحلیل‌های آماری و حملات مبتنی بر الگو را به همراه دارد.

۳-۱-تجزیه و تحلیل فضای کلیدی

مدل پیشنهادی دارای فضای کلیدی گسترده‌ای است که انجام حملات brute-force را غیرممکن می‌سازد. این ویژگی ناشی از وجود کلیدهای مخفی DNA و ترکیبات متنوع توالی‌های باینری است. در نتیجه روش پیشنهادی در برابر حملات brute-force از مقاومت بالایی برخوردار است.

۳-۲-تلاش مهاجم

مهاجم تلاش می‌کند تا اطلاعاتی از داده‌های رمزگذاری‌شده استخراج کند که با بررسی تغییرات ورودی و تأثیر آن بر خروجی بتواند پیوندی بین داده‌های رمز شده و داده‌های اصلی برقرار کرده و در نهایت کلید رمز را کشف نماید. در

UNCORRECTED PROOF

صورتی که داده‌های رمزگذاری‌شده به صورت متنی باشند مهاجم ممکن است تغییر کوچکی در متن ایجاد و اثر آن را بر متن ساده مشاهده نماید. با این حال حتی اگر هکر فایل را رمزگشایی کند، متن دیگری دریافت می‌کند که باعث سردرگمی او می‌شود و نمی‌تواند با اطمینان تشخیص دهد که اطلاعات واقعی در توالی DNA هستند یا در قالب متن قرار دارند. به دلیل ویژگی‌های تصادفی در رمزنگاری، رمزگشایی برای مهاجم بسیار دشوار است. یافته‌های تجربی نشان می‌دهد که روش پیشنهادی قادر است بر بسیاری از حملات موجود غلبه کند. خروجی این روش به صورت توالی DNA است که پیش‌بینی راز اصلی را بسیار پیچیده می‌سازد. بنابراین روش پیشنهادی در برابر برخی حملات جدید از سطح بالاتری از محافظت برخوردار است (جدول (۳)).

نتایج جدول (۳) نشان می‌دهد که روش پیشنهادی با استفاده از فضای کلید با ۲۵۶ بیت و تولید توالی‌های DNA ،غیرقابل‌پیش‌بینی بوده و ترکیب عملیات ژنتیکی منجر به سطح بالاتری از امنیت و مقاومت در برابر حملات مختلف از جمله brute-force و تحلیل‌های شناخته‌شده را در مقایسه با الگوریتم‌های کلاسیک مانند DES، RC5 و RSA ارائه می‌دهد. این ویژگی‌ها باعث می‌شوند که روش پیشنهادی نه تنها پیچیدگی پیش‌بینی رمز را افزایش دهد، بلکه توانایی مقابله با حملات جدید و پیشرفته را نیز بهبود بخشد. علاوه بر این در الگوریتم پیشنهادی طول متن رمزشده با طول متن ساده برابر بوده و اعمال عملیات تصادفی و چندلایه، اطمینان از محرمانگی، یکپارچگی و استحکام داده‌ها را فراهم آورده و برتری قابل‌توجهی نسبت به روش‌های رمزنگاری سنتی دارد. درجدول (۴) نیز مقایسه‌ای بین روش‌های اخیر رمزنگاری مبتنی بر DNA ([۲۱-۱۹]) و روش پیشنهادی این مقاله ارائه شده است. همان‌طور که در جدول (۴) دیده می‌شود این روش‌ها محدود به کاربردهای خاصی مانند داده‌های سبک IoT یا رمزگذاری تصویر هستند و در پیاده‌سازی پیچیده‌اند. در مقابل روش پیشنهادی با بهره‌گیری از الگوریتم ژنتیک و فضای کلید گسترده ، قادر به رمزگذاری انواع داده‌ها شامل متن، تصویر و سیگنال بوده و خروجی آن غیرقابل پیش‌بینی و مقاوم در برابر حملات مدرن است. این ویژگی‌ها انعطاف‌پذیری و امنیت بالاتر روش پیشنهادی را نسبت به روشهای اخیر نشان می‌دهند.

متریک / الگوریتم	Algorithm Strength	Key Length	Attack
DES	الگوریتم نسبتا قوی	56-bit key	مقاوت بیشتر نسبت به الگوریتم های ساده، اما در برابر brute-force آسیب‌پذیر
RC5	الگوریتم قوی و سبک	64-bit	مقاوم در برابر بسیاری از حملات، بسته به پیکربندی
RSA	وابسته به اندازه کلید	1024- bit	مقاوم در برابر اغلب حملات کلاسیک اما مستعد حملات زمانبندی
روش پیشنهادی	قوی در رمزنگاری و تولید خروجی غیرقابل پیش‌بینی	Uses a 256-bit equivalent key space	استفاده از فضای کلیدبزرگ مانع جستجوی جامع شده و مقاومت در برابر brute-force را تضمین می‌کند

جدول ۳- مقایسه روشهای رمزنگاری براساس ویژگی‌های الگوریتم و مقاومت در برابر حملات

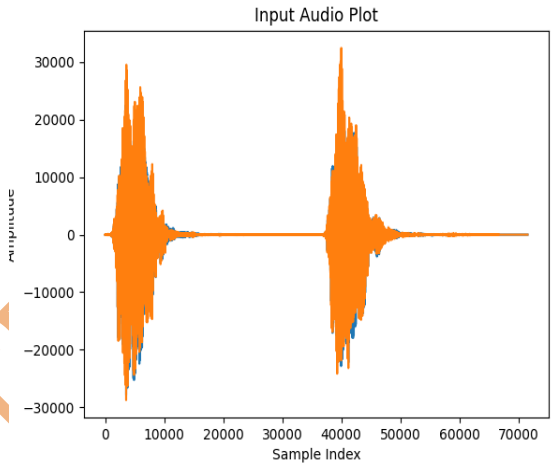
مرجع و موضوع رویکرد کلیدی	نقاط قوت مطالعه	محدودیت‌ها -خلأ موجود	تمایز و نوآوری پژوهش حاضر
[19] DNA-PRESENT: light encryption, Improvement diffusion and confusion	امنیت بالا و اثر avalanche قابل توجه	تمرکز بر IoT محیط و داده‌های سبک	روش پیشنهادی عمومی‌تر و مقاوم‌تر برای انواع داده‌ها (متن، تصویر، سیگنال)
[20] A novel DNA tree-based chaotic image encryption algorithm	امنیت بالا برای تصاویر و رمزگذاری تصویر با نقشه آشوب	محدود به تصاویر، پیچیدگی پیاده‌سازی بالا	استفاده از الگوریتم ژنتیک و فضای کلید بزرگ‌تر، انعطاف برای داده‌های مختلف

UNCORRECTED PROOF

انعطاف‌پذیری برای انواع داده‌ها و فضای کلید وسیع‌تر	مناسب داده‌های سبک و پایش بیمار. عمومی نیست	رمزگذاری ترکیبی DNA + نقشه آشوب برای داده‌های IoT	[21] A hybrid logistic DNA-based encryption system for securing IoT patient monitoring systems

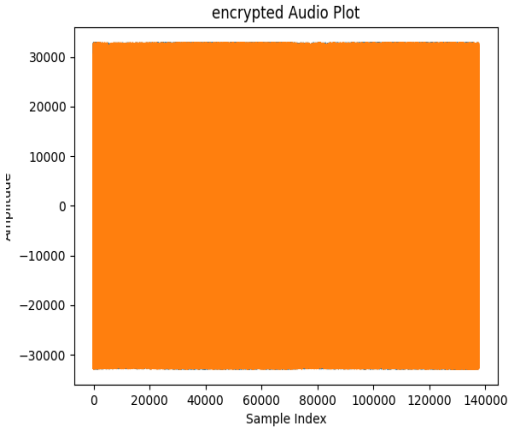
جدول ۴- مقایسه روش پیشنهادی با پژوهش‌های جدید رمزنگاری مبتنی بر DNA

همچنین برای ارزیابی عملکرد روش پیشنهادی یک فایل صوتی مورد استفاده قرار گرفته است. (شکل ۴)

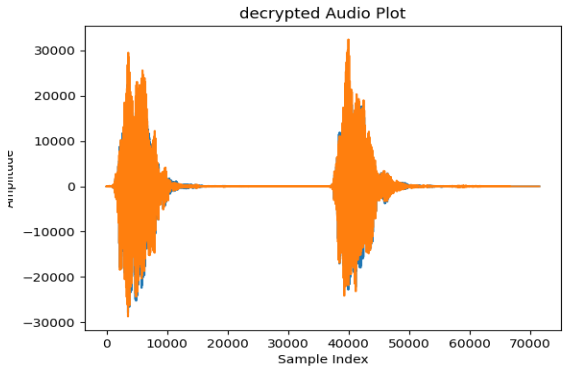


شکل ۴- نمایشی از فایل صوتی مورد بررسی جهت ارزیابی روش پیشنهادی

نتایج حاصل از رمزگذاری و رمزگشایی الگوریتم پیشنهادی روی فایل صوتی در شکل (۵) و شکل (۶) نشان داده شده است.

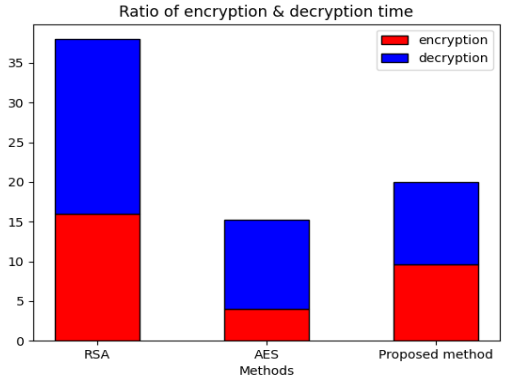


شکل ۵- نمایشی از فایل صوتی رمزگذاری شده توسط روش پیشنهادی



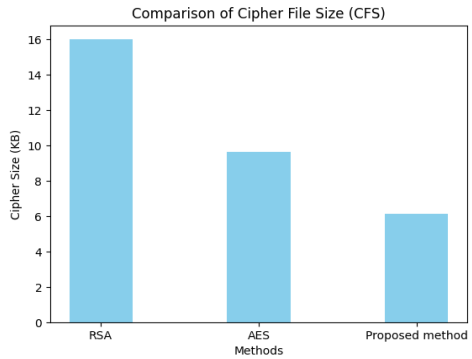
شکل ۶- نمایشی از فایل صوتی پس از رمزگشایی

شکل (۷) به مقایسه زمان اجرای الگوریتم پیشنهادی و الگوریتم‌های سنتی RSA (رمزگذاری نامتقارن) و AES (رمزگذاری متقارن) می‌پردازد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به AES زمان اجرای بیشتری دارد اما نسبت به RSA سریعتر می‌باشد.



شکل۷- مقایسه زمان اجرای الگوریتم پیشنهادی با سایر روشها

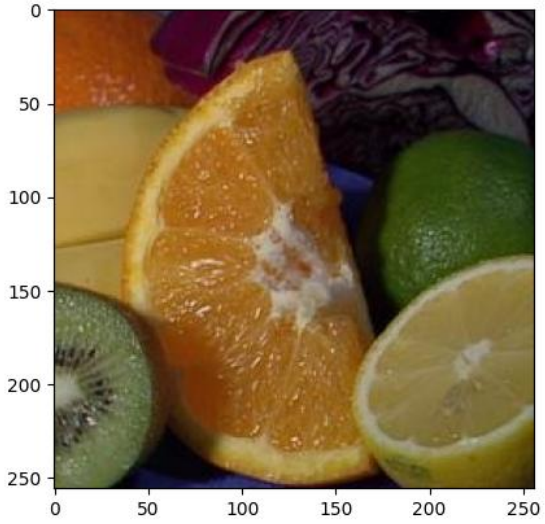
در شکل (۸) اندازه فایل رمزشده پس از رمزگذاری توسط الگوریتم پیشنهادی و الگوریتم‌های سنتی RSA و AES مقایسه شده است. روش پیشنهادی دارای کمترین اندازه است.



شکل ۸- مقایسه اندازه فایل رمز گذاری شده در الگوریتم پیشنهادی با سایر روشها

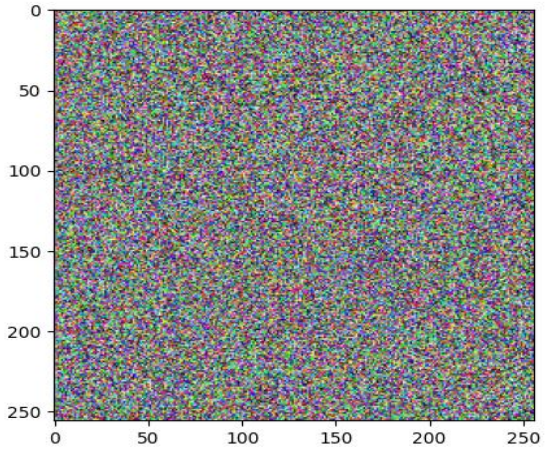
آنتروپی نیز بر اساس تعریف شانون در نظریه اطلاعات معیاری برای سنجش میزان عدم قطعیت یا تصادفی بودن نمادهای تولیدشده توسط یک منبع است. در تصاویر دیجیتال با عمق رنگ ۸ بیت، حداکثر مقدار نظری آنتروپی برابر با ۸ بیت بر پیکسل در نظر گرفته می‌شود که نشان‌دهنده توزیع کاملاً یکنواخت شدت روشنایی است. در این مقاله مقادیر آنتروپی تصویر آزمایشی پیش از رمزگذاری در بازه‌ای بین ۶.۷۴ تا ۷.۵۵ بیت بر پیکسل قرار داشت. پس از اعمال الگوریتم پیشنهادی مقدار آنتروپی در تمامی کانال‌های رنگی به حدود ۷.۹۹۷ بیت بر پیکسل افزایش یافت (جدول (۵)). این افزایش که به طور میانگین حدود ۰.۴ بیت بر پیکسل است، بیانگر آن است که توزیع آماری پیکسل‌های تصویر رمزگذاری‌شده به مقدار نظری ایده‌آل بسیار نزدیک شده است. مقدار بالای آنتروپی نشان‌دهنده بهبود ویژگی‌های تصادفی خروجی بوده و می‌تواند مقاومت الگوریتم را در برابر تحلیل‌های آماری مبتنی بر هیستوگرام و سایر روش‌های آماری سطح پایین تقویت کند. زیرا تصویر رمزگذاری‌شده از نظر توزیع شدت روشنایی رفتاری نزدیک به نویز سفید از خود نشان می‌دهد. همچنین در صورت در نظر گرفتن مقادیر بالای NPCR و UACI حاصل از آزمون‌های حساسیت می‌توان نتیجه گرفت که الگوریتم پیشنهادی نسبت به تغییرات بسیار کوچک در کلید یا داده ورودی واکنش قابل توجهی نشان می‌دهد و موجب ایجاد تغییرات گسترده در توزیع آماری خروجی می‌گردد.

همانطور که قبلا نیز گفته شد، هدف اصلی این مقاله ارائه یک الگوریتم رمزگذاری جدید است که با ترکیب سیستم‌های پویای آشوبناک، شامل قوانین کدگذاری مبتنی بر DNA و نقشه‌های لجستیک موجب ارتقای محرمانگی و یکپارچگی داده‌های دیجیتال شود. به منظور ارزیابی میزان امنیت الگوریتم پیشنهادی عملکرد آن با استفاده از مجموعه‌ای از آزمون‌های آماری مورد بررسی قرار گرفته است. در این ارزیابی شاخص‌هایی نظیر NPCR (نرخ تغییر تعداد پیکسل‌ها)، UACI(میانگین شدت تغییر یکپارچه) و معیار آنتروپی به عنوان معیارهای اصلی تحلیل امنیتی در نظر گرفته شده‌اند. در ادامه به منظور بررسی دقیق‌تر کارایی مدل پیشنهادی، الگوریتم بر روی تصویر نمونه ارائه‌شده در شکل (۹) اعمال شده و عملکرد آن از طریق محاسبه آنتروپی و تحلیل ویژگی‌های آماری تصویر رمزگذاری‌شده ارزیابی شده است.



شکل ۹- تصویر اولیه مورد استفاده در فرآیند رمزگذاری

تصویر حاصل از رمزگذاری به صورت شکل (۱۰) نمایش داده شده است.



شکل ۱۰- تصویر حاصل پس از اعمال الگوریتم رمزگذاری

Entropy analysis	آنتروپی
Original Red	۷.۵۵۲۱۳۱
Original Blue	۷.۳۳۷۵۹۱
Original Green	۶.۷۴۵۹۶۳
cipher Red	۷.۹۹۷۰۶۸
Cipher Blue	۷.۹۹۷۳۹۵
Cipher Green	۷.۹۹۷۱۷۷

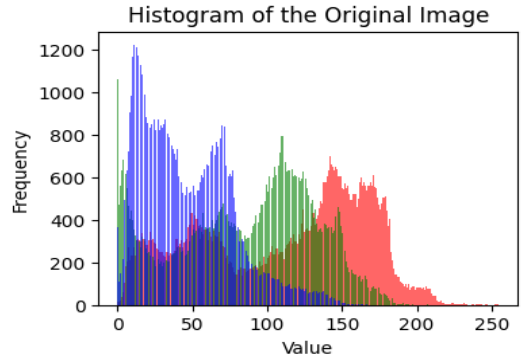
جدول ۵- نتایج تحلیل آنتروپی تصاویر قبل و بعد از رمزگذاری

همبستگی بین پیکسل‌های همسایه در یک تصویر یکی از مهم‌ترین آزمون‌های آماری است که میزان اثربخشی الگوریتم رمزگذاری را نشان می‌دهد. تصاویر اصلی معمولاً همبستگی بسیار بالایی (معمولاً بالای ۰.۹) در جهت‌های افقی، عمودی و مورب دارند. این مقادیر در تصاویر رمزگذاری شده به طور چشمگیری کاهش یافته‌اند. در آزمایش‌های انجام شده میانگین همبستگی تصاویر رمزگذاری شده بین ۰.۰۰۰۲ تا ۰.۰۱۲ گزارش شد که نشان می‌دهد روابط ساختاری و آماری پیکسل‌ها به شدت کاهش یافته و تقریباً از بین رفته‌اند. نتایج دقیق آنالیز همبستگی نیز در جدول (۶) ارائه شده است.

correlation analysis	vertical	horizontal
red	0.9635233504	0.97625097326
green	0.9547757226	0.93415979937
blue	0.9337957302	0.87543910774
Cipher red	0.00028831290	0.01264217461
Cipher green	-0.0070999258	0.00837660251
Cipher blue	0.00598340105	0.007650086031

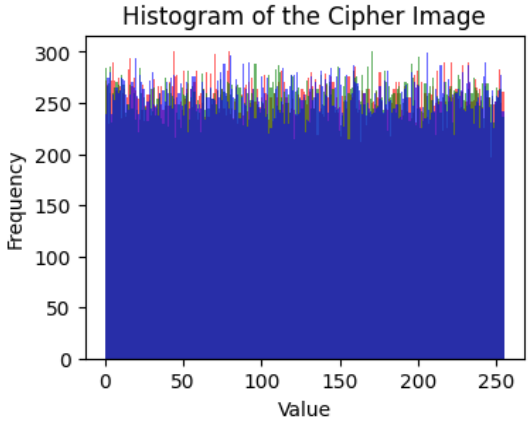
جدول ۶- نتایج ارزیابی ضرایب همبستگی

تحلیل هیستوگرام یکی از مهم‌ترین ابزارهای بصری برای بررسی توزیع آماری تصاویر رمزگذاری شده است. در حالی که تصاویر اصلی معمولاً دارای پیک‌های برجسته و چگالی‌های ساختاری قابل تشخیص در کانال‌های R-G-B هستند، هیستوگرام تصاویر رمزگذاری شده تقریباً یکنواخت و مسطح دیده می‌شوند. این امر نشان می‌دهد که ویژگی‌های آماری تصویر تغییر یافته و با روش‌های تحلیل معمولی قابل تفسیر نیستند. هیستوگرام تصویر اولیه و تصویر رمزگذاری شده به ترتیب در شکل‌های (۱۱) و (۱۲) نشان داده شده‌اند.



شکل ۱۱- هیستوگرام تصویر اولیه پیش از رمزگذاری

هیستوگرام تصویر رمزگذاری شده در شکل (۱۲) نشان داده شده است.



شکل ۱۲- هیستوگرام تصویر پس از رمزگذاری

آزمون کای-اسکوئر هیستوگرام یکی از معیارهای مهم در ارزیابی امنیت تصاویر رمزگذاری شده است. این آزمون میزان یکنواختی هیستوگرام را اندازه‌گیری می‌کند. هرچه مقدار کای-اسکوئر کمتر باشد هیستوگرام یکنواخت‌تر بوده و سیستم رمزگذاری تصویر امن‌تر خواهد بود. در این مقاله واریانس و مقدار کای-اسکوئر محاسبه شد که نتایج آن به صورت زیر است.

UNDER PEER REVIEW

var of red 3090.297

var of green 3090.297

var of blue 3090.297

var of cipher red 5491.023

var of cipher green 5460.184

var of cipher blue 5478.391

همچنین مقدار کای-اسکوئر (Chi-Square) به صورت زیر به دست آمد:

Chi Square of Cipher Red 265.5703125

Chi Square of Cipher Green 235.359375

Chi Square of Cipher Blue 256.5078125

معیارهای استاندارد برای سنجش مقاومت یک الگوریتم رمزگذاری در برابر حملات تفاضلی NPCR و UACI هستند. NPCR (نرخ تغییر پیکسل‌ها) نشان می‌دهد چه درصدی از پیکسل‌ها در اثر رمزگذاری تغییر می‌کنند، حتی اگر تنها یک بیت در تصویر ورودی تغییر کند. به صورت مشابه UACI (میانگین شدت تغییر یکپارچه) نیز میانگین تفاوت شدت پیکسل‌ها را بین دو تصویر رمزگذاری شده اندازه‌گیری می‌کند (بر حسب درصد و در بازه ۰ تا ۲۵۵). این دو معیار امکان ارزیابی عددی الگوریتم رمزگذاری را فراهم می‌کنند تا مشخص شود آیا الگوریتم دارای «اثر بهمن» است یا خیر. به این معنا که حتی یک تغییر کوچک در ورودی بتواند تغییرات گسترده و قابل توجهی در خروجی ایجاد کند.

در یک الگوریتم رمزگذاری امن مقدار NPCR باید بسیار بالا (تقریباً ۱۰۰٪) و مقدار UACI از نظر تئوری حداقل ۳۳٪ باشد. نزدیک شدن به این مقادیر نشان می‌دهد که حتی یک تغییر یک بیتی می‌تواند تقریباً تمامی پیکسل‌های تصویر رمزگذاری شده را تحت تأثیر قرار دهد و به‌طور متوسط حدود یک سوم تفاوت روشنایی ایجاد کند. در آزمایش‌های انجام شده الگوریتم ما عملکرد بسیار خوبی در معیارهای NPCR و UACI از خود نشان داد. در این مقاله

تحلیل‌های NPCR و UACI با مقایسه تصویر رمزگذاری شده و تصویر اصلی آن انجام شد. این ارزیابی‌ها بر روی یک تصویر آزمایشی متفاوت و با استفاده از خروجی حاصل از یک بار اجرای الگوریتم رمزگذاری انجام شد. نتایج ارائه شده در جدول (۷) نشان می‌دهد که مقادیر NPCR بالای ۹۹.۱۰٪ و مقادیر UACI تقریباً ۳۳٪ هستند.

	NPCR	UACI	PSNR
Red	99.23858	33.539	8.242
Blue	99.601745	33.614	8.233
Green	99.601745	33.581	8.258

جدول ۷- نتایج آزمون‌های NPCR، UACIو PSNR

طبق انتظار روش پیشنهادی هم بر روی داده‌های متنی و هم داده‌های صوتی عملکرد موفقی داشته است. تجزیه و تحلیل های تجربی روش پیشنهادی عمدتا برای داده‌های صوتی انجام شده است. بررسی‌های انجام‌شده نشان می‌دهد که روش پیشنهادی در مقایسه با بسیاری از الگوریتم‌های مرسوم سرعت بالاتر و کارایی بهینه‌تری دارد. با این وجود برای اطمینان کامل از تأمین الزامات امنیتی و تحقق اصول سه‌گانه امنیت اطلاعات (محرمانگی(Confidentiality) ، یکپارچگی (Integrity) ودسترس‌پذیری(Availability)) لازم است تجزیه و تحلیل امنیتی بیشتری بر روی روش پیشنهادی انجام شود.

درادامه نمونه‌ای از عملیات رمزگذاری و رمزگشایی مبتنی برالگوریتم پیشنهادی برروی متن و کلید داده شده به شکل زیر ارائه می‌شود.

متن:

Encryption is a way to conceal information by altering it so that it appears to be random data. Encryption is essential for security on the Internet.

کلید:

Key: 128
01111001010011110100111101110000011010000010000010100101101111101001100101010110000010001000100010011010111010001101100011010100101111000

UNCORRECTED PROOF

عملیات رمزگذاری و رمزگشایی مبتنی بر الگوریتم پیشنهادی:

Initial DNA sequence:

CACCCGTGCGATCTAGCTGCCTAACTCA
CGGCCGTTCGTGAGAACGGCCTATAGA
ACGACAGAACTCTCGACCTGCAGAACT
CACGTTAGAACGATCGTTCGTGCGATC
GCCCGACCGTAAGAACGGCCGTGCGCG
CGTTCTAGCGTCCGACCTCACGGCCGTT
CGTGAGAACGAGCTGCAGAACGACCGT
ACTCACGCCCTAGCGGCCGTGCGCTAG
AACGGCCTCAAGAACTATCGTTAGAAC
TCACGGACGACCTCAAGAACGGCCTCA
AGAACGACCTAACTAACGCCCGACCTA
GCTATAGAACTCACGTTAGAACGAGCG
CCAGAACTAGCGACCGTGCGCACGTTC
GTCAGAACGCACGACCTCACGACAGTG
AGAACACCCGTGCGATCTAGCTGCCTA
ACTCACGGCCGTTCGTGAGAACGGCCT
ATAGAACGCCCTATCTATCGCCCGTGCT
CACGGCCGACCGTAAGAACGCGCGTTC
TAGAGAACTATCGCCCGATCTCCCTAG
CGGCCTCACTGCAGAACGTTCGTGAGA
ACTCACGGACGCCAGAACAGCCGTGCT
CACGCCCTAGCGTGCGCCCTCAAGTG

Final DNA sequence:

CCCAATATGTAATCAGGATCACGCGGA
GAGACGGCGTATCATGAAGACAGACGG
ATCAACGAGAAAAACATCCACTTAAAT
GCGGCATCGGCATTTTCCCATGGCACG
GGTGCCTACCGTTCGCCGAGGCTTTAA
ATCCAATTTTGTGAGCTCCCGCTCCATA
TTAAAAAACAGGAATGGGGAATTGAAC
GCGCAGGATCCACGGAGACCGGATTAC
CGTGAAAACTCCTGCAGCCATACTGAG
GCTCTCCACTCGAACAAGCGCTATATGT
GTGAACATCTAACTCGAGCCAAGGGGT
GACTGCCTCGATGGAACCGTATACATTT
CTGTGATTGCAGAGTCTATACCCCGCTG
TTCAGATTCGGAGTGGTGCGACTTACG
AGCGATATCCAGAAGGCATCACTGCAC
TTATATGGCGATCACCCGCGATGGAAT
CCGCTCTGGATCGCCCTAAACACACAG
AGTTCAGCAGCGATTGTCTCCGTGGAT
ACCGGGAAGAATACCTCTTCTACCTTTT
CGTAGATGGGCTGCCATACTGGCAATC
GGGCATAGGACCGTTGGACGGGCGAGC
ATTACACCGCGTCCGCAACCCCCA

Total execution time: 0.20404839515686035

Encrypted text:
CCCAATATGTAATCAGGATCACGCGGA
GAGACGGCGTATCATGAAGACAGACGG
ATCAACGAGAAAAACATCCACTTAAAT
GCGGCATCGGCATTTTCCCATGGCACG
GGTGCCTACCGTTCGCCGAGGCTTTAA
ATCCAATTTTGTGAGCTCCCGCTCCATA
TTAAAAAACAGGAATGGGGAATTGAAC
GCGCAGGATCCACGGAGACCGGATTAC
CGTGAAAACTCCTGCAGCCATACTGAG
GCTCTCCACTCGAACAAGCGCTATATGT
GTGAACATCTAACTCGAGCCAAGGGGT
GACTGCCTCGATGGAACCGTATACATTT
CTGTGATTGCAGAGTCTATACCCCGCTG
TTCAGATTCGGAGTGGTGCGACTTACG
AGCGATATCCAGAAGGCATCACTGCAC
TTATATGGCGATCACCCGCGATGGAAT
CCGCTCTGGATCGCCCTAAACACACAG
AGTTCAGCAGCGATTGTCTCCGTGGAT
ACCGGGAAGAATACCTCTTCTACCTTTT
CGTAGATGGGCTGCCATACTGGCAATC
GGGCATAGGACCGTTGGACGGGCGAGC
ATTACACCGCGTCCGCAACCCCCA

Initial DNA sequence:

CCCAATATGTAATCAGGATCACGCGGA
GAGACGGCGTATCATGAAGACAGACGG
ATCAACGAGAAAAACATCCACTTAAAT
GCGGCATCGGCATTTTCCCATGGCACG
GGTGCCTACCGTTCGCCGAGGCTTTAA
ATCCAATTTTGTGAGCTCCCGCTCCATA
TTAAAAAACAGGAATGGGGAATTGAAC
GCGCAGGATCCACGGAGACCGGATTAC
CGTGAAAACTCCTGCAGCCATACTGAG
GCTCTCCACTCGAACAAGCGCTATATGT
GTGAACATCTAACTCGAGCCAAGGGGT
GACTGCCTCGATGGAACCGTATACATTT
CTGTGATTGCAGAGTCTATACCCCGCTG
TTCAGATTCGGAGTGGTGCGACTTACG
AGCGATATCCAGAAGGCATCACTGCAC
TTATATGGCGATCACCCGCGATGGAAT
CCGCTCTGGATCGCCCTAAACACACAG
AGTTCAGCAGCGATTGTCTCCGTGGAT
ACCGGGAAGAATACCTCTTCTACCTTTT
CGTAGATGGGCTGCCATACTGGCAATC
GGGCATAGGACCGTTGGACGGGCGAGC
ATTACACCGCGTCCGCAACCCCCA

Decrypted text:

Encryption is a way to conceal information by altering it so that it appears to be random data. Encryption is essential for security on the Internet.

INCORRECTED PROOF

۴-نتیجه گیری

روش پیشنهادی در این مقاله بر اساس چندین تکرار و فعالیت‌های ژنتیکی طراحی شده و یک تکنیک رمزگذاری پایدارتر ارائه می‌دهد. عملیات روش پیشنهادی شامل رمزگذاری، چرخش (rotation)، تلاقی (crossover)، جهش (mutation) و تغییرشکل‌های مختلف است که موجب بهبود استانداردهای رمزگذاری می‌شود. همچنین ارتباط کم بین داده‌های ورودی و خروجی رمزگذاری‌شده احتمال تحلیل و شکستن رمز را کاهش می‌دهد و مراحل دفاعی چندلایه امنیت داده‌ها را افزایش می‌دهد. با استفاده از فضای کلید گسترده و تولید توالی‌های DNA غیرقابل پیش‌بینی روش پیشنهادی امنیت و مقاومت بالاتری نسبت به الگوریتم‌های سنتی مانند DES، RC5 و RSA فراهم می‌کند. همچنین در مقایسه با روش‌های اخیر رمزنگاری مبتنی بر DNA که معمولاً محدود به داده‌های سبک IoT یا رمزگذاری تصویر هستند و پیچیدگی پیاده‌سازی بالایی دارند، روش پیشنهادی انعطاف‌پذیری بیشتری دارد و قادر است انواع داده‌ها شامل متن، تصویر و سیگنال را رمزگذاری کند. با وجود مزایای قابل توجه مانند مقاومت بالا در برابر حملات و تولید خروجی غیرقابل پیش‌بینی، روش پیشنهادی دارای پیچیدگی نسبی محاسباتی و نیازمند مدیریت کلیدها و توالی‌های DNA است که ممکن است برای داده‌های بسیار بزرگ یا سیستم‌های با منابع محدود نیازمند بهینه‌سازی باشد. در کارهای آینده می‌توان با بهینه‌سازی پیاده‌سازی، بهره‌گیری از پردازش موازی و انتخاب هوشمندانه عملگرها کارایی الگوریتم را افزایش و محدودیت‌های عملیاتی آن را کاهش داد بدون آنکه امنیت و قدرت رمزنگاری آن تحت تأثیر قرار گیرد. استانداردسازی روش و کاهش انتقال داده‌ها نیز می‌تواند کاربردپذیری آن را در سیستم‌های عملی بهبود بخشد. همچنین در کارهای آینده بهینه‌سازی انتخاب توالی‌های DNA و مدیریت کلیدها می‌تواند عملکرد و امنیت روش پیشنهادی را در محیط‌های داده‌ای پیچیده و بزرگ افزایش دهد ([۲۲،۲۳]). همچنین در آینده می‌توان از روش انتخاب ویژگی مبتنی بر BGSA که در [۲۴] ارایه شده است، به‌عنوان جایگزینی برای PCA استفاده و نتیجه را ارزیابی کرد.

تقدیر و تشکر

این کار با حمایت از پژوهانه دانشگاه زابل با شماره IR-UOZ-GR-5366 انجام شده است.

تعارض منافع

در انتشار این مقاله هیچ تعارض منافعی وجود ندارد.

مراجع

[1] Chang, X., W. Li, A. Yan, P. W. M. Tsang, and T.-C. Poon. "Asymmetric cryptosystem based on optical scanning cryptography and elliptic curve algorithm." *Scientific Reports* 12, no. 1 (2022): 7722.
[2] Shikder, A., and N. K. Nishchal. "Image encryption using binary polarization states of light beam." *Scientific Reports* 13, no. 1 (2023): 14028.
[3] Matteucci, F., V. Arzamasov, and K. Böhm. "A benchmark of categorical encoders for binary classification." In *Proceedings of the Neural Information Processing Systems Conference (NeurIPS)*, 2023, 1–21. Available online: GitHub/EncoderBenchmarking.
[4] Naseri, H., and A. Izadi Mazidi. "A new data security algorithm for cloud computing based on genetic techniques and logical-mathematical functions." *18th National Conference on Applied Research in Electrical, Computer and Biomedical Engineering*, Shirvan, 2023. Available online: civilica.com/doc/1944290. (in Persian)
[5] Dai, K., and N. Wang. "A hybrid DNA based genetic algorithm for parameter estimation of dynamic systems."*Chemical Engineering Research and Design* 90, no. 12 (2012): 2235–2246.
[6] Chen, X., and N. Wang. "A DNA based genetic algorithm for parameter estimation in the hydrogenation reaction."*Chemical Engineering Journal* 150, no. 2 (2009): 527–535.
[7] Kiryanova, O. Y., R. R. Garafutdinov, I. M. Gubaydullin, and A. V. Chemeris. "A novel approach to encode melodies in DNA." *BioSystems* 237 (2024): 105136.
[8] Uddin, M., F. Jahan, M. K. Islam, and M. Rakib Hassan. "A novel DNA-based key scrambling technique for image encryption." *Complex & Intelligent Systems* 7, no. 6 (2021): 3241–3258.

UNCORRECTED PROOF

[9] Raman Kumar, M., and N. K. Vaegae. "A new numerical approach for DNA representation using modified Gabor wavelet transform for the identification of protein coding regions." *Biocybernetics and Biomedical Engineering* 40, no. 2 (2020): 836–848.
[10] Alakuş, T. B. "A novel repetition frequency-based DNA encoding scheme to predict human and mouse DNA enhancers with deep learning." *Biomimetics* 8, no. 2 (2023): 218.
[11] Rao, S. K., R. Kumar, N. K. Nishchal, and A. Alfalou. "Optical asymmetric image encryption using DNA through vortex beam encoding." *Discover Applied Sciences* 6, no. 11 (2024): 591.
[12] Preuss, I., M. Rosenberg, Z. Yakhini, and L. Anavy. "Efficient DNA-based data storage using shortmer combinatorial encoding." *Scientific Reports* 14, no. 1 (2024): 7731.
[13] Turab, N., M. Abu Alhija, H. Owida, and J. Al-Nabulsi. "A survey on DNA cryptographic techniques, challenges and future trends." (2022): 7178.
[14] Houghten, S., and S. Banik. "Effective decoders for DNA codes." *BioSystems* 211 (2022): 104583.
[15] Garafutdinov, R. R., D. A. Chemeris, A. R. Sakhabutdinova, O. Y. Kiryanova, C. I. Mikhaylenko, and A. V. Chemeris. "Encoding of non-biological information for its long-term storage in DNA." *BioSystems* 215–216 (2022): 104664.
[16] Wen, H., et al. "Secure DNA-Coding Image Optical Communication Using Non-Degenerate Hyperchaos and Dynamic Secret-Key." *Mathematics* 10, no. 17 (2022): 1–18.
[17] Kaur, A., A. P. S. Chauhan, and A. K. Aggarwal. "Prediction of enhancers in DNA sequence data using a hybrid CNN-DLSTM model." *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 20, no. 2 (2023): 1327–1336.
[18] Adleman, L. M. "Molecular computation of solutions to combinatorial problems." *Science* 266, no. 5187 (1994): 1021–1024.
[19] Wang, X., Y. Li, and Z. Chen. "DNA-PRESENT: An Improved Security and Low-Latency, Lightweight Cryptographic Solution for IoT." *Sensors* 24, no. 24 (2024): 7900.
[20] Zhang, H., J. Liu, and P. Kumar. "A novel DNA tree-based chaotic image encryption algorithm." *Journal of Information Security and Applications* 73 (2024): 103448.
[21] Patel, R., M. Singh, and K. Roy. "A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems." *Computers & Electrical Engineering* 105 (2023): 108597.
[۲۲] Ghanbari, N., H. Zahiri, and H. Shahraki. "Clustering of Fuzzy Data Sets Based on Particle Swarm Optimization with Fuzzy Cluster Centers." *International Journal of Industrial Engineering & Production Research* 33, no. 2 (2022): 1–12.
[۲۳] Ghanbari, N., S. H. Zahiri, and H. Shahraki. "Clustering of Triangular Fuzzy Data Based on Heuristic Methods." *Journal of Electrical and Computer Engineering Innovations* 12, no. 1 (2024): 1–14.
[24] Ghanbari, N., Razavi, S. M., and Nabavi Karizi, S. H. "An Intelligent BGSA Based Method for Feature Selection in a Persian Handwritten Digits Recognition System." Nashriyyah-i Muhandisi-i Barq va Muhandisi-i Kampyutar-i Iran 9, no. 1 (2011): 29–36. https://www.rimag.ir/fa/Article/28000/FullText.

UNCORRECTED PROOF