این مقاله در قالب نهایی آن در مجله
ماشین‌بینایی و پردازش‌تصویر چاپ خواهد شد
تاریخ انتشار برخط: آبان‌ماه ۱۳۹۹

http://jmvip.sinaweb.net
www.ismvip.ir

رمزنگاری جدید تصاویر خاکستری بر اساس استاندارد رمزنگاری پیشرفته و دنباله DNA

امیرحسین رزمی[۱]، کوروش منوچهری کلانتری[۲]، علیرضا هدایتی[۳]

چکیده

یک تصویر دیجیتال نمایش بصری از چیزی است که بصورت الکترونیکی ایجاد و کپی یا ذخیره شده‌است. امنیت تصاویر با توجه به استفاده گسترده از تصاویری که در شبکه یا در دیسک ذخیره می‌شوند، نگرانی مهمی در امنیت اطلاعات امروز است. بدلیل آنکه رسانه‌های عمومی غیرقابل اعتماد و در برابر حملات آسیب‌پذیر می‌باشند؛ رمزگذاری تصویر موثرترین راه برای محرمانگی و محافظت از حریم خصوصی تصاویر در رسانه‌های عمومی غیرقابل اعتماد است.

در این مقاله یک الگوریتم جدید رمزنگاری تصویر براساس استاندارد رمزنگاری پیشرفته و دنباله DNA برای تصاویر خاکستری ارائه می‌شود. ما نحوه رمزگذاری و رمزگشایی داده‌ها در دنباله DNA براساس جایگزینی کدون‌ها و چگونگی انجام مراحل مختلف استاندارد رمزنگاری پیشرفته مبتنی‌بر DNA را توضیح می‌دهیم. الگوریتم در نرم‌افزار MATLAB 2012b پیاده‌سازی می‌شود و برای ارزیابی اثربخشی آن از معیارهای مختلف عملکرد استفاده می‌شود. تجزیه و تحلیل تئوری و تجربی نشان می‌دهد که الگوریتم پیشنهادی کارآیی بهتری در سرعت و دقت دارد. علاوه بر این، تجزیه و تحلیل امنیتی ثابت می‌کند الگوریتم پیشنهادی مقاومت بیشتری نسبت به نویز و حملات شناخته شده از خود نشان می‌دهد؛ به طوری که شکست‌ناپذیری الگوریتم پیشنهادی ۳۷,۴۸% بهتر از الگوریتم‌های مورد قیاس می‌باشد.

کلیدواژه‌ها

رمزنگاری تصویر، استاندارد رمزنگاری پیشرفته، دنباله DNA، دقت، سرعت، شکست‌ناپذیری

۱ مقدمه

با نگاهی به تاریخ، از زمان ایران و یونان باستان تا دوره نقاشی‌های داوینچی، تلاش انسان در جهت پنهان نمودن اطلاعات بصری مشهود بوده است. شاید نخستین تلاش بشر برای رمزنگاری تصویر را بتوان در نقاشی تصویر پادشاه فردریک سوم و همسرش مشاهده کرد که با استفاده از یک سیلندر شیشه‌ای در مرکز نقاشی، رمزگشایی می‌شود.

تصاویر ممکن است کاربردهای تجاری، نظامی یا حتی پزشکی داشته باشند که برای حفظ امنیت آنها و جلوگیری از دسترسی‌های غیرمجاز به این تصاویر، رمزنگاری آنها قبل از ارسال روی شبکه ضروری است. به این ترتیب فقط عوامل مجاز در صورت داشتن کلید صحیح قادر به رمزگشایی آنها می‌باشند [۱].

تصویر، یک داده حجیم دوبعدی است که کوچکترین واحد آن یک پیکسل است. هر پیکسل از یک تصویر دیجیتال، معرف میزان روشنایی آن نقطه از تصویر است. با توجه به حساسیت چشم انسان در تشخیص سطوح روشنایی از یکدیگر، کل محدوده روشنایی قابل نمایش به ۲۵۶ سطح تقسیم‌بندی می‌شود. بنابراین

این مقاله در مردادماه سال ۹۸ دریافت، در مردادماه ۹۹ بازنگری و در شهریورماه همان سال پذیرفته شد.

[۱] دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی، واحد تهران مرکزی
رایانامه: ami.razmi.eng@iauctb.ac.ir
[۲] گروه مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر، واحد دانشگاهی گرمسار
رایانامه: kmanochehri@aut.ac.ir
[۳] گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی، واحد تهران مرکزی
رایانامه: hedayati@iauctb.ac.ir

نویسنده مسئول: کوروش منوچهری

سطح روشنایی هر پیکسل می‌تواند مقداری بین ۰ تا ۲۵۵ داشته باشد. تصویر خاکستری به تصویری گفته می‌شود که شدت نور هر پیکسل آن می‌تواند از مشکی تا سفید تغییر کند. رنگ سفید با مقدار ۲۵۵ و رنگ سیاه با مقدار ۰ نشان داده می‌شود و سایر سطوح خاکستری مقادیری بین ۰ و ۲۵۵ دارد. هر چقدر عدد به ۲۵۵ نزدیک‌تر باشد، پیکسل مورد نظر روشن‌تر دیده می‌شود و هرچقدر به ۰ نزدیک‌تر باشد پیکسل مورد نظر تاریک‌تر دیده می‌شود [۲].

با توجه به ویژگی‌های ذاتی داده‌های چندرسانه‌ای، وجود محدودیت در توان محاسباتی پردازنده، پهنای‌باند شبکه انتقال داده و زمان محاسباتی، بایستی از طرح‌های رمزنگاری کارآمد متناسب با شرایط استفاده کرد [۳]. برای غلبه بر مشکلات رمزنگاری تصویر، پژوهشگران تلاش کرده‌اند تا طرح‌های رمزنگاری خاصی برای داده‌های چندرسانه‌ای ابداع کنند. پژوهشگران در طی پژوهش‌های به عمل آمده، ثابت کرده‌اند که طرح‌های جدید از نقطه نظر علم رمزنگاری، دارای یکسری مزایا و معایب می‌باشند [۳].

این مقاله متمرکز بر الگوریتم جدید رمزنگاری تصویر براساس استاندارد رمزنگاری پیشرفته و دنباله DNA برای تصاویر خاکستری است. در بخش ۲، مفاهیم اولیه، کارهای پیشین و الگوریتم‌های مورد قیاس (رمزنگاری تصویر براساس نگاشت آشوبی لجستیک ۲بعدی و دنباله DNA، نگاشت آشوبی لجستیک ۳بعدی، نگاشت آشوبی هنون-سین ۲بعدی و دنباله DNA) بررسی می‌شود. در بخش ۳، الگوریتم پیشنهادی و نحوه اجرای آن مطرح می‌گردد. در بخش ۴، الگوریتم پیشنهادی بوسیله تعدادی از آزمون‌های استاندارد از قبیل آنتروپی، هیستوگرام و غیره ارزیابی شده و سپس با الگوریتم‌های مورد نظر مقایسه می‌شود. در انتها در بخش ۵، جمع‌بندی و نتیجه گیری ارائه می‌شود.

۲ مروری بر تحقیقات گذشته

کلمه رمزنگاری (Cryptography) برگرفته از لغات یونانی Kryptos به مفهوم محرمانه و Graphien به معنای نوشتن است. رمزنگاری مطالعه‌ی فرآیند رمزگذاری و رمزگشایی می‌باشد. با تبدیل هنر رمزنگاری به علم رمزنگاری، روش‌های فراوانی برای رمزنگاری و پنهان‌سازی اطلاعات در قالب روش‌های کلاسیک تدوین و توسعه پیدا کرده‌اند. رمزنگاری تصویر به دلیل برخی ویژگی‌های ذاتی آن، هم‌چون هم‌بستگی زیاد میان پیکسل‌ها متفاوت از رمزنگاری متن می‌باشد؛ لذا روشهای کلاسیک رمزنگاری متن برای این منظور چندان کارآمد نیستند.

در سال ۱۹۸۹، برای اولین بار در رمزنگاری تصویر از سیتم‌های آشوب استفاده شده‌است [۴]. Yen و همکارش، الگوریتم رمزنگاری مبتنی‌بر کلید آشوبگون معرفی کردند که در آن یک دنباله دودویی توسط سیستم آشوب تولید می‌گردد و به عنوان کلید رمزنگاری بکار می‌رود؛ همچنین پیسکل‌های تصویر مطابق با دنباله‌های دودویی تولید شده، مرتب می‌شوند و با کلید رمزنگاری XOR و XNOR می‌شود [۵]. دارا و منوچهری، طرحی را پیشنهاد کردند که از نگاشت آشوبی لجستیک برای تولید S-box در استاندارد رمزنگاری پیشرفته استفاده می‌شود [۶].

با گسترش محاسابت DNA و پتانسیل زیاد آن در رمزنگاری، اخیرا استفاده از DNA در رمزنگاری تصویر مرسوم شده‌است. ناصر و همکارانش رمزنگاری تصویر براساس DNA را پیشنهاد کردند که در آن الگوریتم، پیکسل‌های تصویر اصلی با استفاده از قوانین کدگذاری DNA به دنباله‌های DNA تبدیل می‌شود؛ سپس عملگرهایی مانند جمع، تفریق روی آن دنباله‌ها اعمال می‌گردد؛ همچنین آنها از نگاشت آشوبی لجستیک ۲بعدی در طرح پیشنهادی خود استفاده کردند [۷]. در [۸]، Zhang و همکارش روشی پیشنهاد کردند که در آن از نگاشت آشوبی کوانتوم و قوانین کدگذاری DNA برای رمزنگاری تصویر استفاده می‌شود. در ادامه الگوریتم‌های مورد قیاس به منظور ارزیابی و مقایسه با الگوریتم پیشنهادی شرح داده می‌شود.

۲-۱ رمزنگاری تصویر براساس نگاشت آشوبی و دنباله DNA

ابتدا بهتر است علت انتخاب الگوریتم‌های رمزنگاری مورد نظر برای مقایسه شرح داده شود. هدف از انتخاب آنها برای مقایسه آن است که، دو الگوریتم رمزنگاری از ۲ نسخه متفاوت نگاشت آشوبی لجستیک استفاده می‌نماید که یکی از الگوریتم‌ها از دنباله DNA استفاده می‌کند و دیگری خیر. بدین صورت می‌توان تاثیر نسخه‌های نگاشت آشوبی و استفاده یا عدم‌استفاده از دنباله DNA را در الگوریتم رمزنگاری سنجید. همچنین می‌توان تاثیر تغییر نگاشت آشوبی لجستیک به هنون-سین را نیز ارزیابی کرد.

آشوب، همانطور که از نامش پیداست، رفتاری به ظاهر تصادفی و بی‌نظم است که در بسیاری از پدیده‌های دنیای واقعی رخ می‌دهد [۹]. از دهه ۱۹۹۰ تاکنون، سامانه‌های دینامیک آشوبی به صورت گسترده در طراحی استراتژی‌های جدید برای رمزنگاری اطلاعات استفاده شده‌اند. اکثر الگوریتم‌های رمزنگاری تصویر بایستی شامل دو مرحله تکرارشونده باشد: انتشار و اغتشاش . این بدین صورت حاصل می‌شود که تمام پیکسل‌های تصویر به صورت کلی با استفاده از یک نگاشت آشوبی دوبعدی یا سه‌بعدی جایگشت یابند. پیکسل انتقال یافته به مکان جدید در واقع یک جانشانی از پیکسل اولیه می‌باشد. این معماری اساس یکسری از سامانه‌های رمزنگاری مبتنی‌بر آشوب چندبعدی را تشکیل می‌دهد.

۲-۱-۱ رمزگذاری تصویر با استفاده از نگاشت آشوبی لجستیک ۲بعدی و DNA

متداولترین و ساده‌ترین سیستم آشوبی به نگاشت لجستیک معروف می‌باشد و اولین بار توسط Robert May معرفی

شده‌است. نگاشت آشوبی لجستیک ۲بعدی را می‌توان طبق رابطه (۱) تعریف کرد [۱۰].

$$\begin{cases} x_{i+1} = x_i u_1 (1 - x_i) + \lambda_1 y_i^2 \\ y_{i+1} = y_i u_2 (1 - y_i) + \lambda_2 (x_i^2 + x_i y_i) \end{cases} \quad (۱)$$

در رابطه (۱)، $3.4 < u_1 < 2.75$، $3.45 < u_2 < 2.75$، $0.21 < \lambda_1 < 0.15$، $0.15 < \lambda_2 < 0.13$ و $x_i, y_i \in (0,1]$ می‌باشد. u_1، u_2، λ_1، λ_2 پارامترهای سیستم و x، x مقادیر اولیه نگاشت می‌باشند.

فرآیند رمزگذاری تصویر براساس نگاشت آشوبی لجستیک ۲بعدی و دنباله DNA به شرح زیر می‌باشد:

گام اول: کلید رمزنگاری به وسیله تابع درهم‌ساز ۲۵۶بیتی از تصویر اصلی محاسبه می‌شود. همچنین پارامترها و مقادیر اولیه سیستم آشوبی u_1، u_2، λ_1، λ_2 و x_0، y_0 نیز در آن دخیل می‌باشند.

گام دوم: تصویر اصلی $P(M \times N)$ با استفاده از قانون رمزگذاری DNA رمزگذاری می‌شود که منجر به تولید ماتریس DNA $P_2(M \times 4N)$ می‌شود.

گام سوم: یک جایگشت مبتنی‌بر موج در سطح DNA بر روی ماتریس P_2 اعمال می‌شود و ماتریس اغتشاش P_3 حاصل می‌شود.

گام چهارم: انتشار در سطح DNA بر روی ماتریس P_3 اعمال می‌شود و ماتریس P_4 به دست می‌آید.

گام پنجم: ماتریس DNA P_4 توسط قانون رمزگشایی DNA، رمزگشایی می‌شود. در نهایت، تصویر رمزگذاری شده تولید می‌شود.

۲-۱-۲ رمزگذاری تصویر با استفاده از نگاشت آشوبی لجستیک ۳بعدی

نگاشت آشوبی لجستیک ۳بعدی را می‌توان طبق رابطه (۲) تعریف کرد [۱۱].

$$\begin{cases} x_{i+1} = \alpha x_i (1 - x_i) + \beta z_i^2 x_i + \gamma z_i^3 \\ y_{i+1} = \alpha y_i (1 - y_i) + \beta y_i^2 y_i + \gamma x_i^3 \\ z_{i+1} = \alpha z_i (1 - z_i) + \beta x_i^2 z_i + \gamma y_i^3 \end{cases} \quad (۲)$$

در رابطه (۲)، $3.81 < \alpha < 0.35$، $0.022 > \beta > 0$، $0.015 > \gamma > 0$ و $x_i, y_i, z_i \in (0,1)$ می‌باشد. α, β, γ پارامترهای سیستم و x, y, z مقادیر اولیه نگاشت می‌باشند.

فرآیند رمزگذاری تصویر براساس نگاشت آشوبی لجستیک ۳بعدی به شرح زیر می‌باشد:

گام اول: تصویر اصلی به عنوان ماتریس P و اندازه آن $m \times n$ در نظر گرفته می‌شود.

گام دوم: پارامترها و مقادیر اولیه سیستم آشوبی مقداردهی می‌شوند.

گام سوم: مقدار درهم‌سازی تصویر اصلی توسط تابع درهم‌ساز محاسبه می‌شود.

گام چهارم: مقادیر اولیه سیستم آشوبی x_0, y_0, z_0 بروزرسانی می‌شوند؛ مقادیر بروزرسانی شده $\overline{x_0}, \overline{y_0}, \overline{z_0}$ فرض می‌شوند.

گام پنجم: بر روی تصویر اصلی P جایگشت اعمال می‌شود و تصویر جایگشت شده A حاصل می‌شود.

گام ششم: پارامتر سیستم آشوبی بر روی تمام سطرها و ستونها قبل از فرآیند انتشار اعمال می‌شود.

گام هفتم: بعد از اعمال انتشار بر روی تصویر جایگشت شده A، تصویر رمزگذاری شده C حاصل می‌شود.

۲-۱-۳ رمزگذاری تصویر با استفاده از نگاشت آشوبی هنون-سین ۲بعدی و DNA

نگاشت هنون یک نگاشت آشوبی دوبعدی معکوس‌پذیر می‌باشد که در سال ۱۹۷۶ توسط هنون معرفی شده‌است. نگاشت آشوبی هنون-سین ۲بعدی طبق رابطه (۳) تعریف می‌شود [۱۲].

(۳)

در رابطه (۳)، پارامترهای نگاشت برابر هستند با $a, b \in (-\infty, +\infty)$ و x, y مقادیر اولیه نگاشت می‌باشند.

فرآیند رمزگذاری تصویر براساس نگاشت آشوبی هنون-سین ۲بعدی و دنباله DNA به شرح زیر می‌باشد:

گام اول: پارامترها و مقادیر اولیه سیستم آشوبی a، b، x_1^0، y_1^0، a_2، b_2، x_2^0، y_2^0 به عنوان کلید رمزنگاری در نظر گرفته می‌شوند.

گام دوم: تصویر اصلی با استفاده از قانون رمزگذاری DNA رمزگذاری می‌شود که منجر به تولید ماتریسی با عنوان ماتریس $I_{m \times n}$ می‌شود؛ سپس I به آرایه‌ای با عنوان P و طول mn تغییر شکل می‌دهد.

گام سوم: توالی P با اعمال فرآیند انتشار در سطح DNA، به توالی جدیدی تبدیل می‌شود.

گام چهارم: توالی جدید تولید شده جایگشت می‌شود تا توالی رمزگذاری C حاصل شود.

گام پنجم: توالی رمزگذاری C باعث تولید I_c با اندازه $m \times n$ می‌شود. I_c ماتریسی می‌باشد که توسط قانون رمزگشایی DNA، رمزگشایی می‌شود. در اصل، I_c همان تصویر رمزگذاری شده می‌باشد.

۳ روش تحقیق

الگوریتم پیشنهادی، یک نسخه جدید از استاندارد رمزنگاری پیشرفته به نام الگوریتم رمزنگاری تصویر براساس استاندارد رمزنگاری پیشرفته و دنباله DNA می‌باشد. در ابتدا بهتر است نحوه رمزنگاری براساس DNA شرح داده شود و سپس به نحوه رمزنگاری تصویر براساس استاندارد رمزنگاری پیشرفته و دنباله DNA پرداخته شود.

DNA از واحدهای ساده‌تری به نام نوکلئوتید ساخته شده‌است که هر نوکلئوتید شامل گوانین[1]، سیتوزین[2]، آدنین[3]، تیمین[4] می‌باشد. در هر رشته DNA، هر سه نوکلئوتید متوالی یک کدون نامیده می‌شود و هر کدون یک اسید آمینه را در یک پروتئین مشخص می‌کند (مانند جدول ۱) [۱۳] تا [۱۶].

جدول ۱: کدون‌ها و اسید آمینه مربوط به آنها

اسید آمینه	کدون
Isoleucine	ATA, ATC, ATT
Leucine	CTA, CTC, CTG, CTT, TTA, TTG
Valine	GTA, GTC, GTG, GTT
Glycine	GGA, GGC, GGG, GGT

برای استفاده از DNA برای رمزنگاری، ابتدا باید اطلاعات دودویی را به فرمت DNA تبدیل کرد. طبق جدول ۲، الفبای DNA از چهار حرف A، C، G، T تشکیل شده‌است [۱۷]. داده ابتدا به بیت و پس از آن به فرمت DNA تبدیل می‌شود. اگر داده یک متن باشد، آنگاه واحد رمزنگاری کاراکتر است و به صورت کد ۷بیتی نمایش داده می‌شود؛ اگر داده یک تصویر باشد، آنگاه واحد رمزنگاری پیکسل است و حداقل بصورت کد ۸بیتی نمایش داده می‌شود. با توجه به اینکه هر حرف DNA با ۲ بیت نمایش داده می‌شود، بدین معنی است که یک کاراکتر یا یک پیکسل در ۴ حرف نمایش داده خواهد شد که برابر با یک بایت است.

جدول ۲: تبدیل دودویی به DNA

DNA	دودویی	۷بیتی	۸بیتی
A	۰۰	۰	۰+۱=۱
C	۰۱	۱	۱+۱=۲
G	۱۰	۲	۱+۲=۳
T	۱۱	۳	۱+۳=۴

آدنین و تیمین و همچنین گوانین و سیتوزین مکمل یکدیگرند. از آنجا که ۰ و ۱ مکمل هم هستند، بنابراین ۰۰ و ۱۱ نیز مکمل هم خواهند بود. به همین صورت ۰۱ و ۱۰ نیز وضعیت مشابه‌ای داشته و مکمل یکدیگر هستند. با استفاده از چهار ترکیب آدنین، سیتوزین، گوانین و تیمین، بیست و چهار حالت مختلف برای رمزنگاری وجود دارد. اما با توجه به این قانون که آدنین و تیمین و همچنین گوانین و سیتوزین مکمل یکدیگرند، تنها هشت حالت که در جدول ۳ آمده‌است، معتبر خواهند بود.

برای یک تصویر خاکستری ۸بیتی، هر پیکسل می‌تواند بصورت دنباله‌های DNA با طول ۴ نشان داده شود. برای مثال اگر سیتوزین، آدنین، تیمین و گوانین به ترتیب برای نمایش مقادیر دودویی ۰۰، ۰۱، ۱۰ و ۱۱ استفاده شوند، آنگاه کد DNA مربوط به پیکسلی با مقدار ۱۷۳ (که معادل دودویی آن ۱۰۱۰۱۱۰۱ است)، برابر با TTGA خواهد شد؛ نحوه نمایش مقدار ۱۷۳ بدین صورت می‌باشد که از سمت راست ۲ بیت ۲ بیت جدا کرده و معادل نوکلئوتید DNA نوشته می‌شود:

$$\frac{10}{T}\frac{10}{T}\frac{11}{G}\frac{01}{A}$$

جدول ۳: حالتهای مجاز برای رمزنگاری

	۱	۲	۳	۴	۵	۶	۷	۸
A	۰۰	۰۰	۰۱	۰۱	۱۰	۱۰	۱۱	۱۱
T	۱۱	۱۱	۱۰	۱۰	۰۱	۰۱	۰۰	۰۰
C	۰۱	۱۰	۰۰	۱۱	۰۰	۱۱	۰۱	۱۰
G	۱۰	۰۱	۱۱	۰۰	۱۱	۰۰	۱۰	۰۱

۱-۳ الگوریتم پیشنهادی

الگوریتم پیشنهادی همانند استاندارد رمزنگاری پیشرفته، یک الگوریتم کلید متقارن است، بدین معنی که از یک کلید رمزنگاری یکسان برای رمزگذاری و رمزگشایی استفاده می‌کند که این کلید رمزنگاری می‌تواند ۱۲۸، ۱۹۲ و ۲۵۶ بیتی باشد [۱۸]. در این مقاله به دلیل افزایش امنیت از کلید رمزنگاری با اندازه ۲۵۶ بیت استفاده می‌شود. همچنین اندازه کلید رمزنگاری مورد استفاده در این الگوریتم، تعداد تکرارهای چرخه‌های تبدیل را نیز تعیین می‌کند. تعداد چرخه‌های تکرار به صورت زیر است:

- ۱۰ چرخه تکرار برای کلیدهای ۱۲۸ بیتی
- ۱۲ چرخه تکرار برای کلیدهای ۱۹۲ بیتی
- ۱۴ چرخه تکرار برای کلیدهای ۲۵۶ بیتی

در اصل الگوریتم پیشنهادی همانند استاندارد رمزنگاری پیشرفته عمل می‌کند؛ تنها تفاوت آنها در این است که داده‌ها در الگوریتم پیشنهادی برمبنای نوکلئوتید می‌باشد.

الگوریتم پیشنهادی شامل ۶ گام رمزگذاری و رمزگشایی، یای انحصاری، جانشین‌سازی بایت‌ها، جابجاسازی سطرها، درهم‌ریزی ستون‌ها و افزودن کلید چرخه می‌باشد که در ادامه به آنها پرداخته می‌شود.

۱-۱-۳ رمزگذاری و رمزگشایی

در این بخش، نشان داده می‌شود که چگونه داده‌های دودویی بدون تغییر آمینواسیدهای یک پروتئین براساس جایگزینی کدون‌ها، به DNA تبدیل می‌شوند.

تبدیل داده‌ها به یک زنجیره نوکلئوتید به منظور ایجاد یک رشته DNA می‌تواند باعث تکثیر و ایجاد وضعیت بد برای گونه شود. برای حل این مشکل، از جایگزینی کدون‌ها در DNA استفاده می‌شود که به سلول‌های زنده آسیب نمی‌رساند. جایگزینی کدون‌ها، تغییر حداقل یک کدون توسط یک کدون متفاوت دیگر در توالی

[1] Guanine (G)
[2] Cytosine (C)
[3] Adenine (A)
[4] Thymine (T)

کدون یک ژن می‌باشد. در الگوریتم پیشنهادی از جایگزینی کدون‌هایی استفاده می‌شود که در آن، توالی‌های اسید آمینه تغییر نمی‌کند؛ بنابراین هیچ تغییری در تولید پروتئین بوجود نمی‌آید.

در الگوریتم پیشنهادی، مقادیر پیکسل‌های تصویر ابتدا به داده‌های دودویی تبدیل و سپس براساس قوانین DNA که در بخش ۳ توضیح داده شده‌است، به دنباله DNA تبدیل می‌شوند. فرض می‌شود، داده‌ها در یک رشته DNA ذخیره شده‌اند. حروف x, y, z (همچنین x'، y' و z') به صورت پیشنهادی برای نوکلئوتید (A، C، G یا T) انتخاب می‌شوند. به این ترتیب با انتخاب دلخواه، کدونی به عنوان xyz یا ($x'y'z'$) نوشته می‌شود. کدون‌هایی که با نوکلئوتید x شروع می‌شوند و نوکلئوتید بعد از آن y می‌باشد، اسید آمینه l را تولید می کنند که در یک آرایه (لیست) $S_{xy}(l)$ گروه‌بندی می‌شوند. این آرایه بر اساس حروف الفبا مرتب می‌شود. به عنوان مثال، فرض کنید که نماد I به اسید آمینه ایزولوسین اشاره دارد، بنابراین طبق جدول ۳، $S_{AT}(I) =$ $\{ATA, ATC, ATT\}$ می‌باشد.

از آنجا که $S_{xy}(l)$ یک آرایه مرتب شده‌است، کدون‌های $S_{xy}(l)$ با صفر شروع می‌شوند. برای مثال، $|ATA| = 0$ و $|ATT| = 2$ در $S_{AT}(I)$ می‌باشد. اگر $xyz \in S_{xy}(l)$ باشد، پس $|xyz|$ موقعیت (یا شاخص) xyz را در $S_{xy}(l)$ نشان می‌دهد. بنابراین، در طول این مقاله، عملیات محاسباتی با توجه به شاخص $|xyz|$ بر روی کدون xyz انجام می‌گیرد.

هنگامیکه یک بیت ۰ یا ۱ است، یک لیست $S_{xy}(l)$ با حداقل دو کدون می‌تواند برای جایگزینی استفاده شود. به عبارت دیگر، یک کدون که هیچ کدون جایگزین برای تولید اسید آمینه یکسان (یعنی تعداد عناصر $S_{xy}(l)$ یک می‌باشد) را بدلیل عدم جایگزینی کدون‌ها نمی‌توان استفاده کرد. بنابراین، این کدون‌ها حذف می‌شوند که به آنها کدون‌های قابل حذف گفته می‌شود.

به آرایه $S_{xy}(l)$ که تنها یک کدون دارد، آرایه قابل حذف گفته می‌شود و کدون آن نیز کدون قابل حذف نامیده می‌شود. کدونی که قابل حذف نباشد، کدون غیرقابل حذف نامیده می‌شود. به عنوان مثال، کدون‌ها ATG و AGG کدون قابل حذف و کدون ATA کدون غیرقابل حذف می‌باشد.

به منظور جایگزینی کدون‌ها، یک نگاشت با نام نگاشت جایگزینی[5] معرفی می‌شود که xyz کدون غیرقابل حذف را به یک xyz' کدون غیرقابل حذف دیگر تبدیل می‌نماید؛ به طوری که هر دو کدون اسید آمینه مشابه تولید می‌کنند. چون ممکن است بیش از یک xyz وجود داشته باشد، نگاشت جایگزینی عملکرد xyz و موقعیت xyz' را در $S_{xy}(l)$ مشخص می‌نماید.

در نگاشت جایگزینی فرض می‌شود که $xyz \in S_{xy}(l)$ و i یک عدد صحیح می‌باشد. نگاشت جایگزینی $SM(xyz, i) = xyz'$ بدین صورت تعریف می‌شود که تعریف می‌شود که $xyz' \in$ $S_{xy}(l)$ و $|xyz'| = |xyz| + i \ (mod\ 2)$. از آنجا که برخی از $S_{xy}(l)$ حاوی بیش از دو کدون هستند، رمزگذاری داده‌های دودویی به یک رشته DNA با استفاده از SM می‌تواند منجر به یک مشکل رمزگشایی شود. بنابراین، قبل از اعمال SM، کدون xyz غیرقابل حذف با اولین کدون در $S_{xy}(l)$ رمزگذاری می‌شود. تابعی که کدون را به کدون شاخص ۰ در $S_{xy}(l)$ کدگذاری می‌کند، نگاشت جایگزینی آغازین[6] می‌گویند. در استاندارد رمزنگاری پیشرفته، حالت یک آرایه‌ای با طول ۱۲۸ بیت (یعنی ۱۶ بایت یا ماتریس ۴×۴ بایت) است. در الگوریتم پیشنهادی، حالت دی‌ان‌ای یک رشته دی‌ان‌ای با ۱۲۸ کدون غیرقابل حذف است. در الگوریتم‌های ۱ و ۲، نشان داده می‌شود که چگونه از دو نگاشت SM و FSM برای رمزگذاری و رمزگشایی داده‌های دودویی با توجه به مفهوم DNA و جایگزینی کدون‌ها استفاده می‌شود.

Algorithm 1 Encoding
Input: $e = (e_{m-1}e_{m-2} \dots e_0)_2$ is a binary data and S is a known part in DNA with m non-omittable codons.
Output: S after storing e in S as replaced Codons.
Begin
1: Let the m non-omittable codons in S be $x_i y_i z_i, i = 0,1, \dots, m-1$.
2: **for** $i = 0$ to m-1 **do**
3: $x_i y_i z_i' = FSM\ (x_i y_i z_i), i.e., |x_i y_i z_i'| = 0$.
4: $x_i y_i z_i = SM(x_i y_i z_i', e_i)$
5: **end for**
The m non-omittable codons in S are exposed to replaced Codons.
End

برای توضیح مراحل الگوریتم ۱، از نمونه زیر استفاده می‌شود: فرض کنید که داده‌های دودویی $e = (110101)_2$ و S = TCC-TCG-TGG-CAA-GCA-ATC-CAG می‌باشد. همچنین e و S ورودی الگوریتم ۱ می‌باشند. توجه داشته باشید که TCC-TCG-TGG-CAA-GCA-ATC-CAG، ۶ کدون غیرقابل حذف در S می‌باشند. با استفاده از نگاشت FSM در ۶ کدون، کدون‌های TCA-TCA-CAA-GCA-ATA-CAA به ترتیب بازیابی می‌شوند. بطوریکه

- هر وقت که $e_0 = 1$، کدون TCA به TCC تبدیل می‌شود.
- هر وقت که $e_1 = 0$، کدون TCA به TCA تبدیل می‌شود.
- هر وقت که $e_2 = 1$، کدون CAA به CAG تبدیل می‌شود.
- هر وقت که $e_3 = 0$، کدون GCA به GCA تبدیل می‌شود.
- هر وقت که $e_4 = 1$، کدون ATA به ATC تبدیل می‌شود.
- هر وقت که $e_5 = 1$، کدون CAA به CAG تبدیل می‌شود.

بنابراین، کدگذاری $e = (110101)_2$ در S = TCC-TCG-TGG-CAA-GCA-ATC-CAG منجر به جایگزینی کدون‌ها TCC-TCA-TGG-CAG-GCA-ATC-CAG می‌شود. توجه داشته باشید که کدون TGG در طول رمزگذاری در نظر گرفته نمی‌شود زیرا TGG یک کدون قابل حذف است.

[5] Substitution Map (SM)

[6] First Substitution Map (FSM)

Algorithm 2 Decoding
Input: S is a known part in DNA that stores $e = (e_{m-1}e_{m-2} \dots e_0)_2$ as replaced Codons.
Output: $e = (e_{m-1}e_{m-2} \dots e_0)_2$
Begin
1: Let the non-omittable codons in S be $x_i y_i z_i, i = 0,1, \dots, m-1$.
2: **for** $i = 0$ to m-1 **do**
3: $e_i = |x_i y_i z_i| (mod\ 2)$
4: **end for**
5: return e.
End

برای توضیح مراحل الگوریتم ۲، از نمونه زیر استفاده می‌شود:
فرض کنید S = TCC-TCA-TGGCAG-GCA-ATC-CA
خروجی رمزگذاری بوسیله الگوریتم ۲ است. کدون‌های غیرقابل حذف TCC-TCACAG-GCA-ATC-CAدر S می‌باشند.
با استفاده از جدول ۱:

- TCC یک است و e_0 نیز یک می‌باشد.
- TCA صفر است و e_1 نیز یک می‌باشد.
- CAG یک است و e_2 نیز یک می‌باشد.
- GCA صفر است و e_3 نیز صفر می‌باشد.
- ATC یک است و e_4 نیز یک می‌باشد.
- CAG یک است و e_5 نیز یک می‌باشد.

بنابراین، خروجی $e = (110101)_2$ است.

۲-۱-۳ یای انحصاری

عملیات یای انحصاری یا XOR در الگوریتم پیشنهادی استفاده می‌شود. در استاندارد رمزنگاری پیشرفته عملیات یای انحصاری بیتی بین دو رشته با طول یکسان انجام می‌شود؛ در حالیکه در الگوریتم پیشنهادی، عمل یای انحصاری بین دو رشته DNA انجام می‌شود. رشته اول DNA به عنوان دنباله‌ای از کدون‌ها در نظر گرفته می‌شود و دومین رشته DNA به عنوان دنباله نوکلئوتیدها در نظر گرفته می‌شود. تعداد کدون‌ها در اولین رشته DNA برابر با تعداد نوکلئوتیدها در رشته دوم است. قبل از انجام عملیات یای انحصاری دومین رشته DNA با یک توالی از ارقام ۰، ۱، ۲ و ۳ (A=0، C=1، G=2 و T=3) با نوکلوئیدها کدگذاری می شود. سپس یای انحصاری بین اولین رشته DNA و توالی رقم‌ها با استفاده از نگاشت جایگزینی انجام می‌گیرد.

در یای انحصاری فرض می‌شود که $S_1 = x_0 y_0 z_0 - \dots - x_n y_n z_n$ یک دنباله از کدون‌ها می‌باشد و S_2 یک توالی نوکلئوتید با توالی رقمی $K_0, K_1, \dots, K_n$ است که

$$k_i = \begin{cases} 0, & if\ x_i = A; \\ 1, & if\ x_i = C; \\ 2, & if\ x_i = G; \\ 3, & if\ x_i = T; \end{cases} \qquad (٤)$$

در الگوریتم پیشنهادی، عملیات یای انحصاری $\oplus_{DNA}$ در دو مرحله استفاده می‌شود: درهم‌ریزی ستون‌ها (بخش ۵-۱-۳) و افزودن کلید چرخه (بخش ۶-۱-۳).

۳-۱-۳ جانشین‌سازی بایت‌ها

این مرحله شامل استفاده از یک جدول جستجو می‌باشد که S-box نامیده می‌شود تا بایت جایگزین شده را برای هر بایت در آرایه حالت ورودی پیدا کند. الگوریتم ۳ برای انجام جانشین‌سازی بایت‌ها در حالت DNA با ۱۶ $S_{i,j}(i,j = 0,1,2,3)$ که هر $S_{i,j}$ شامل ۸ کدون غیرقابل حذف است، ارائه می‌شود.

Algorithm 3 Substitution Bytes
Input: a DNA state $\bar{S}$:
$S_{0,0}, S_{1,0}, S_{2,0}, S_{3,0}, S_{0,1}, S_{1,1}, S_{2,1}, S_{3,1}, \dots, S_{3,3}$,
where each $S_{i,j}$ is 8 non-omittable codons.
Output: perform the substitution on $\bar{S}$
Begin
1: **for** $i = 0$ to 3 **do**
2: **for** $j = 0$ to 0 **do**
3: $d_{i,j}$ = Decoding $(S_{i,j})$
4: Encoding (S-box $(d_{i,j}), S_{i,j}$)
5: **end for**
6: **end for**
End

۴-۱-۳ جابجاسازی سطرها

مرحله جابجاسازی سطرها روی سطرهای حالت اعمال می‌شود. بدین صورت که، بایت‌های هر سطر به وسیله یک آفست معین به صورت چرخشی شیفت می‌یابد. نخستین سطر بدون تغییر باقی می‌ماند. هر بایت از سطر دوم یکی به سمت چپ شیفت می‌یابد. به صورت مشابه، سطرهای سوم و چهارم به ترتیب با آفست‌های دو و سه شیفت می‌یابند. سطر n به تعداد $n-1$ بایت به صورت چرخشی به چپ شیفت می‌یابد. بدین صورت، هر ستون از حالت خروجی در این مرحله ترکیب شده بایت‌های هر ستون از حالت ورودی است. این فرآیند توسط الگوریتم ۴ انجام می‌گیرد. سپس از الگوریتم ۴ برای تعریف گام جابجاسازی سطرها به عنوان الگوریتم ۵ استفاده می‌شود.

Algorithm 4 Swap
Input: S_0 and S_1 are two DNA strands and each one is 8 non-omittable codons with d_0= Decoding (S_0) and d_1= Decoding (S_1).
Output: Changing in S_0 and S_1 such that d_1= Decoding (S_0) and d_0= Decoding (S_1)
Begin
1: **for** $i = 0$ to 1 **do**
2: d_i = Decoding S_i
3: **end for**
4: Decoding (d_1, S_0)
5: Encoding (d_0, S_1)
End

Algorithm 5 Shift Rows
Input: a DNA state $\bar{S}$:
$S_{0,0}, S_{1,0}, S_{2,0}, S_{3,0}, S_{0,1}, S_{1,1}, S_{2,1}, S_{3,1}, \dots, S_{3,3}$, where each $S_{i,j}$ is 8 non-omittable codons.
Output: perform Shift Rows on $\bar{S}$.
1: Swap $(S_{1,0}, S_{1,1})$ ▶shifting second row:
2: Swap $(S_{1,1}, S_{1,2})$
3: Swap $(S_{1,2}, S_{1,3})$
4: Swap $(S_{2,0}, S_{2,2})$ ▶shifting third row:
5: Swap $(S_{2,1}, S_{2,3})$
6: Swap $(S_{3,0}, S_{3,1})$ ▶shifting fourth row:
7: Swap $(S_{3,2}, S_{3,3})$
8: Swap $(S_{3,0}, S_{3,2})$
End

۵-۱-۳ درهم‌ریزی ستون‌ها

در مرحله درهم‌ریزی ستون‌ها، چهار بایت از هر ستون حالت با استفاده از تبدیل خطی معکوس ترکیب می‌شوند. تابع درهم‌ریزی ستون‌ها چهار بایت را به عنوان ورودی در نظر می‌گیرد و چهار بایت را به خروجی می‌دهد، که هر بایت ورودی بر هر چهار بایت خروجی تأثیر می‌گذارد.

به صورت کلی‌تر، هر ستون به عنوان یک چند جمله‌ای روی $GF(2^8)$ تلقی می‌شود. در هم‌ریزی ستون در حالت ورودی S می‌تواند پس از ضرب ماتریس، که در آن اضافه و ضرب در $GF(2^8)$ انجام می‌شود، رخ دهد که طبق رابطه (۵) خواهد بود. فرض کنید j یک شاخص از یک ستون باشد. سپس خروجی در هم‌ریزی ستون‌ها را می‌توان با استفاده از عمل یای انحصاری به صورت رابطه (۶) بیان کرد.

$$\begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix} \times \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \quad (۵)$$
$$= \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

$$\begin{cases} S'_{0,j} = 2S_{0,j} \oplus 3S_{1,j} \oplus S_{2,j} \oplus S_{3,j} \\ S'_{1,j} = S_{0,j} \oplus 2S_{1,j} \oplus 3S_{2,j} \oplus S_{3,j} \\ S'_{2,j} = S_{0,j} \oplus S_{1,j} \oplus 2S_{2,j} \oplus 3S_{3,j} \\ S'_{3,j} = 3S_{0,j} \oplus S_{1,j} \oplus S_{2,j} \oplus 2S_{3,j} \end{cases} \quad (۶)$$

فرض کنید $temp = S_{0,j} \oplus S_{1,j} \oplus S_{2,j} \oplus S_{3,j}$. پس رابطه (۷) بازنویسی می‌شود.

$$\begin{cases} S'_{0,j} = S_{0,j} \oplus temp \oplus 2(S_{0,j} \oplus S_{1,j}) \\ S'_{1,j} = S_{1,j} \oplus temp \oplus 2(S_{1,j} \oplus S_{2,j}) \\ S'_{2,j} = S_{2,j} \oplus temp \oplus 2(S_{2,j} \oplus S_{3,j}) \\ S'_{3,j} = S_{3,j} \oplus temp \oplus 2(S_{3,j} \oplus S_{0,j}) \end{cases} \quad (۷)$$

الگوریتم ۶ و ۷ گام درهم‌ریزی ستون‌ها را شرح می‌دهد.

Algorithm 6 MultBy2 (Multiplication by 2 in GF (2^8))
Input: S is a chain of 8 nucleotides with the digit sequence $(e_7e_6e_5e_4e_3e_2e_1e_0)_2$
Output: S'= 2S.
Begin
1: **if** e_7 = 0 **then**
2: create a chain of nucleotides S' with the digit sequence $(e_7e_6e_5e_4e_3e_2e_1e_0 0)_2$
3: **else**
4: create a chain of nucleotides S' with the digit sequence
$(e_7e_6e_5e_4e_3e_2e_1e_0 0)_2 \oplus (00011011)_2$
5: **end if**
End

Algorithm 7 Mix Columns
Input: a DNA state S':
$S_{0,0}, S_{1,0}, S_{2,0}, S_{3,0}, S_{0,1}, S_{1,1}, S_{2,1}, S_{3,1}, \dots, S_{3,3}$, where each $S_{i,j}$ is 8 non-omittable and $d_{i,j}$ = Decoding $(S_{i,j})$
Output: perform Mix Columns on S'.
Begin
1: **for** $j = 0$ to 3 **do**
2: U_0 is a chain of nucleotides with the digit sequence $(d_{0,j} \oplus d_{1,j})$
3: U_1 is a chain of nucleotides with the digit sequence $(d_{1,j} \oplus d_{2,j})$
4: U_2 is a chain of nucleotides with the digit sequence $(d_{2,j} \oplus d_{3,j})$
5: U_3 is a chain of nucleotides with the digit sequence $(d_{3,j} \oplus d_{0,j})$
6: V_0 = MultBy2(U_0)
7: V_1 = MultBy2(U_1)
8: V_2 = MultBy2(U_2)
9: V_3 = MultBy2(U_3)
10: term is a chain of nucleotides with the digit sequence $(d_{0,j} \oplus d_{1,j} \oplus d_{2,j} \oplus d_{3,j})$
11: $(S_{0,j} \oplus_{DNA} term) \oplus_{DNA} V_0$
12: $(S_{1,j} \oplus_{DNA} term) \oplus_{DNA} V_1$
13: $(S_{2,j} \oplus_{DNA} term) \oplus_{DNA} V_2$
14: $(S_{3,j} \oplus_{DNA} term) \oplus_{DNA} V_3$
15: **end for**
End

۶-۱-۳ افزودن کلید چرخه

برای ساخت کلید چرخه الگوریتم پیشنهادی می‌توان فرض کرد که f_i و g_i بصورت تصادفی از مجموعه‌های {A,G} و {C,T} به ترتیب انتخاب می‌شوند، یعنی $f_i = A$ یا $f_i = G$ با احتمال برابر (به طور مشابه، $g_i = C$ یا $g_i = T$ با احتمال‌های برابر)، $i = 0,1, \dots, 255$. فرض کنید که $r = (e_{255} \dots e_1e_0)_2$ کلید چرخه در الگوریتم پیشنهادی می‌باشد. تابع $L(r)$ به عنوان $x_{255} \dots x_1x_0$ تعریف شده، که

$$x_i = \begin{cases} f_i \ \ if \ x_i = 0 \\ g_i \ \ if \ x_i = 1 \end{cases} \quad (۸)$$

بنابراین اگر $n = (10,12,14)$ باشد و $r_0, r_1, \dots, r_{n-1}$؛ با استفاده از الگوریتم توسعه کلید میتوان کلید چرخه را ایجاد کرد، سپس این کلیدهای چرخه را می‌توان برای ایجاد کلیدهای چرخه دور الگوریتم پیشنهادی $L(r_0), L(r_1), \dots, L(r_{n-1})$ استفاده کرد.

۴ تحلیل و ارزیابی الگوریتم پیشنهادی

برای شبیه‌سازی، ارزیابي الگوریتم پیشنهادی و مقایسه با سامانه‌های رمزنگاری تصویر مورد مطالعه، بایستي از يك‌سری تصویر اصلي استاندارد با اندازه ۲۵۶×۲۵۶ واقع در پایگاه‌داده تصویری USC-SIPI که در دسترس همگان است، استفاده شود. بدین‌علت که ارزیابي‌های صورت گرفته قابل سنجش و تحقیق توسط محققین دیگر نیز باشد. شکل ۱، تصاویر پنتاگون، ساعت،

کشتی، هواپیما، لنا، بابون و تانک را نشان می‌دهد که برای رمزنگاری استفاده شده‌اند [۱۹].

شکل ۱: تصاویر مورد استفاده برای رمزنگاری

جهت ارزیابي يك طرح رمزنگاری تصـوير، تعدادی آزمون و روش ارزیابي استاندارد وجود دارد كه در ادامه به آنها پرداخته خواهد شد.

۴-۱ آنتروپی

آنتروپي بـه معنـای ميزان بي‌نظمي و عدم‌قطعيت در يك سامانه فيزيكي می‌باشد. آنتروپی یک تصویر، تخميني از تصادفي بودن آن مي‌باشد كه به طور معمول برای سنجش ميزان تيزی قله‌های هيستوگرام استفاده می‌شود. آنتروپي شانون H(s) يک منبع پيام s طبق رابطه (۹) محاسبه می‌شود [۲۰].

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

در رابطـــــــه (۹)، $P(s_i)$ معرف احتمال سمبل s_i مي‌باشد. هنگاميكه تصوير رمزگذاری می‌شود، آنتروپي آن بايستي نزديك به مقدار ايده‌آل ۸ باشد. اگر آنتروپي كمتر ۸ باشـد، يك ميزان معيني از پيش‌بيني‌پذيری پديد مي‌آيد كه امنيت سامانه را تهديد مي‌كند. جـدول ۴، نتايج تحليل آنتروپي مربـوط بـه الگـوريتم‌هـای مـورد مطالعه را نشان می‌دهد.

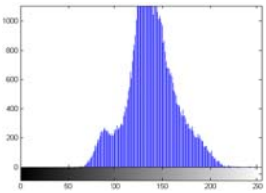
جدول ٤: آنتروپي تصاوير رمزگذاری شده

تصوير	كشتی	تانک	هواپيما	ساعت	پنتاگون	لنا	بابون
الگوريتم پيشنهادی	۷/۹	۷/۹۲	۷/۹۷	۷/۹۱	۷/۹۵	۷/۹۱	۷/۹۹
مرجع [۱۰]	۷/۶۸	۷/۵۹	۷/۴	۷/۳۶	۷/۱۴	۷/۲	۷/۲۵
مرجع [۱۱]	۷/۷۵	۷/۶۳	۷/۵۵	۷/۵۸	۷/۴۲	۷/۳۵	۷/۵۳
مرجع [۱۲]	۷/۸۶	۷/۸۸	۷/۸	۷/۸۴	۷/۶	۷/۴۶	۷/۶۱

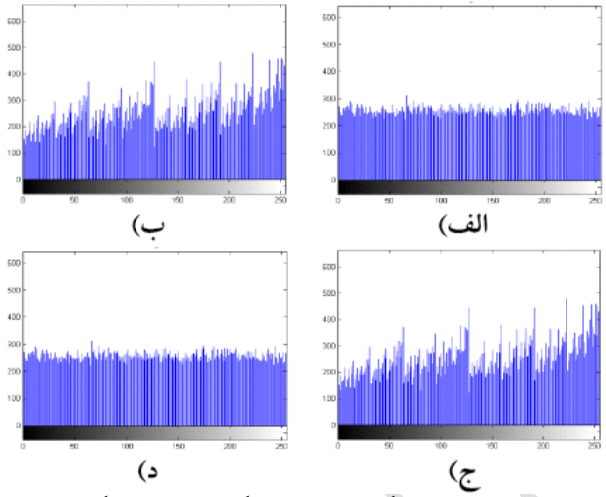
طبق جدول ۴، مقادير بدست آمده نزديک به مقدار ايده‌آل ۸ هســـــــــتند؛ اين بدين معني است كه در روند رمزنگاری، نشت اطلاعات بسيار ناچيز می‌باشد؛ ولی الگوريتم پيشنهادی بدليل آنكه مقادير آنتروپی به دست آمده‌اش به ۸ بيشتر نزديكتر است، در اين آزمون از ديگر الگوريتم‌ها موفق‌تر بوده‌است.

۴-۲ هیستوگرام

تحليل هيستوگرام چگونگي توزيع پيكسل‌ها در تصوير را با استفاده از ترسيم تعداد مشاهدات هر ميزان شدت روشنايي، بيان مي‌كند. توزيع يكنواخت هيستوگرام تصـــوير مي‌تواند نشان‌دهنده كيفيت خوب روش رمزنگاری باشد [۲۱].



شکل ۲: هیستوگرام تصویر اصلی پنتاگون



شکل ۳: هیستوگرام تصاویر رمزگذاری شده پنتاگون

شکل ۲ هیستوگرام تصویر اصلی پنتـاگون را نشـان می‌دهـد. در شکل ۳ الف) هیستوگرام تصـویر رمزگـذاری شـده پنتـاگون بوسـيله الگوريتم پيشنهادی، ب) هيستوگرام تصوير رمزگذاری شده پنتاگون بوسيله مرجع [۱۰]، ج) هيستوگرام تصوير رمزگذاری شده پنتاگون بوسيله مرجع [۱۱] و د) هيستوگرام تصوير رمزگذاری شده پنتاگون بوسـيله مرجـع [۱۲] نشـان داده شده‌اسـت. با مقايسه شـكل ۳، مشخص است كه تصاوير رمزگذاری شده نسبت به تصـاوير اصلي كاملا متمايز هستند و به نظر دارای توزيع پيكسلي تصـــــــادفی يكنواخـت می‌باشـند. در انتهـا می‌تـوان نتيجـه گرفـت، تصـاوير رمزگذاری شـده بوسـيله الگـوريتم پيشـنهادی و مرجـع [۱۲] توزيـع پيكسلي يكنواخت‌تری دارند؛ پس از ديگر الگوريتم‌ها موفق‌تر عمل كرده‌اند.

۴-۳ تمایز بین تصویر اصلی و تصویر رمزگذاری شده

به طور كلي يك خاصيت ايده‌آل برای يك تصوير رمزگذاری شـده، حساس بودن نسبت به تغييرات جزئي در تصوير اصلي، يعني فقط تغيير يك پيكسل مي‌باشد. برای آزمودن اثر تغيير يك پيكسل ورودی بر روی تمام تصوير رمزگـذاری شده، چهـار معيار رايج،

میانگین خطای مطلق[7]، تعداد نرخ تغییرات پیکسل‌ها[8]، میانگین یکپارچه تغییر شدت[9] و محتوا ساختاری[10] استفاده می‌گردد. میانگین خطای مطلق، متوسط خطای مطلق می‌باشد. تعداد نرخ تغییرات پیکسل‌ها، نرخ تعداد پیکسل‌های تغییر یافته است. میانگین یکپارچه تغییر شدت، متوسط‌گیری روی تغییرات شدت روشنایی به صورت یکپارچه که در آن متوسط اختلافات شدت روشنايي دو تصوير اصلي و تصوير رمزگذاری شده سنجيده مي‌شود. فرض کنید $C(i,j)$ و $P(i,j)$ به‌ترتیب نشان‌دهنده سطح خاکستری پیکسل‌های تصویر رمزگذاری شده و اصلی باشد و H ارتفاع و W عرض تصویر می‌باشد، طوری‌که $0 \le i \le H-1$ و $0 \le j \le W-1$. میانگین خطای مطلق بین دو تصویر طبق رابطه (۱۱) محاسبه مي‌شود [۲۲].

$$MAE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} |C(i,j) - P(i,j)| \qquad (۱۱)$$

دو تصویر رمزگذاری شده C و $\bar{C}$ را در نظر بگیرید که تصاویر اصلي متناظر آنها فقط در يك پيكسل متمايزند. تعداد نرخ تغییرات پیکسل‌ها این دو تصویر طبق رابطه (۱۲) محاسبه می‌شود [۲۲].

$$NPCR = \frac{\sum_{i=0}^{H-1} \sum_{j=0}^{W-1} D(i,j)}{H \times W} \times 100\%$$
$$D(i,j) = \begin{cases} 0, & if\ C(i,j) = \bar{C}(i,j) \\ 1, & if\ C(i,j) \neq \bar{C}(i,j) \end{cases} \qquad (۱۲)$$

معیار دیگر میانگین یکپارچه تغییر شدت است که رابطه (۱۳) محاسبه می‌شود [۲۲].

$$UACI = \frac{1}{H \times W} \times \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \left[\frac{|C(i,j) - P(i,j)|}{255} \right] \times 100\% \qquad (۱۳)$$

معیار دیگر محتوا ساختاری می‌باشد. این معیار از تقسیم مجموع مقدار مربع پیکسل تصویر اصلی $f(i,j)$ بر مجموع مقدار مربع پیکسل تصویر رمزگشایی شده $f'(i,j)$ به دست می‌آید. اگر در تصاویر رمزگشایی شده هیچگونه اعوجاج وجود نداشته باشد، محتوا ساختاری برابر با ۱خواهد بود. محتوا ساختاری طبق رابطه (۱۴) محاسبه می‌شود [۲۲].

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} f(i,j)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} f'(i,j)^2} \qquad (۱۴)$$

نتایج آزمون میانگین خطای مطلق الگوریتم‌های مورد مطالعه در جدول ۵ ثبت شده‌است. با مقایسه نتایج حاصل می‌توان نتیجه گرفت، الگوریتم پیشنهادی در این آزمون بهتر عمل کرده‌است.

جدول ۵: میانگین خطای مطلق

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۲۱	۱۶,۹	۲۸,۱	۱۵	۹,۵	۳۱,۱	۳۵	الگوریتم پیشنهادی
۱۷	۱۳	۲۴,۸۹	۱۲,۶	۸	۲۸	۳۲,۳	مرجع [۱۰]
۱۸,۱	۱۵	۲۶	۱۳,۹	۸,۴	۳۰,۲	۳۳,۸	مرجع [۱۱]
۱۹,۸	۱۵,۵	۲۷,۳	۱۴	۸,۹۹	۳۰,۹	۳۴	مرجع [۱۲]

جدول ٦: تعداد نرخ تغییرات پیکسل‌ها

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۹۹,۹%	۹۹,۸%	۹۹,۷%	۹۹,۸%	۹۹,۸%	۹۹,۷%	۹۹,۹%	الگوریتم پیشنهادی
۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	مرجع [۱۰]
۹۹,۵%	۹۹,۶%	۹۹,۵%	۹۹,۷%	۹۹,۶%	۹۹,۵%	۹۹,۶%	مرجع [۱۱]
۹۹,۸%	۹۹,۷%	۹۹,۶%	۹۹,۷%	۹۹,۶%	۹۹,۶%	۹۹,۷%	مرجع [۱۲]

نتایج تعداد نرخ تغییرات پیکسل‌های الگوریتم‌های مورد مطالعه در جدول ۶ ثبت شده‌است. در الگوریتم‌ها، $NPCR >$ 99.5% می‌باشد. به دلیل آنکه تعداد نرخ تغییرات پیکسل‌های الگوریتم پیشنهادی بزرگتر است، پس در این آزمون موفق‌تر بوده‌است.

جدول ۷: میانگین یکپارچه تغییر شدت

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۳۳,۶%	۳۳,۸%	۳۳,۹%	۳۳,۹%	۳۳,۸%	۳۳,۷%	۳۳,۶%	الگوریتم پیشنهادی
۳۳,۴%	۳۳,۴%	۳۳,۵%	۳۳,۴%	۳۳,۵%	۳۳,۴%	۳۳,۴%	مرجع [۱۰]
۳۳,۴%	۳۳,۵%	۳۳,۵%	۳۳,۵%	۳۳,۵%	۳۳,۵%	۳۳,۴%	مرجع [۱۱]
۳۳,۵%	۳۳,۶%	۳۳,۵%	۳۳,۶%	۳۳,۶%	۳۳,۶%	۳۳,۵%	مرجع [۱۲]

نتایج میانگین یکپارچه تغییر شدت الگوریتم‌های مورد مطالعه در جدول ۷ ثبت شده‌است. در الگوریتم‌ها، $UACI >$ 33.4% می‌باشد. با مقایسه نتایج حاصل می‌توان نتیجه گرفت، الگوریتم پیشنهادی بهتر عمل کرده‌است. نتایج محتوا ساختاری الگوریتم‌های مورد مطالعه در جدول ۸ ثبت شده‌است. نتایج به‌دست آمده نشان می‌دهد که مقادیر محتوا ساختاری الگوریتم‌ها به ۱ نزدیک می‌باشند. بدلیل آنکه مقادیر محتوا ساختاری الگوریتم پیشنهادی به ۱ بیشتر نزدیک است؛ پس در این سنجش بهتر عمل کرده‌است.

جدول ۸: محتوا ساختاری

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۱	۱/۱	۰/۹۸	۱/۴	۱/۲	۰/۹	۰/۹۴	الگوریتم پیشنهادی
۰/۷۵	۰/۳	۰/۶۹	۱/۷	۱/۹	۰/۵۹	۰/۷	مرجع [۱۰]
۰/۸	۰/۷	۰/۷۵	۱/۶	۱/۷	۰/۶۲	۰/۷۸	مرجع [۱۱]
۰/۹	۰/۸	۰/۸۳	۱/۳	۱/۵	۰/۷۷	۰/۸	مرجع [۱۲]

۴-۴ تصادفی بودن

امروزه، روش‌های آزمون آماری بسیاری جهت ارزیابي تصادفي بودن خروجي سامانه رمزنگاری وجود دارد که هر يك حضور يا عدم‌حضور يك الگوی مشخص را در خروجي سامانه رمزنگاری

[7] Mean Absolute Error (MAE)
[8] Number of Pixels Change Rate (NPCR)
[9] Unified Average Changing Intensity (UACI)
[10] Structural Content (SC)

تعیین می‌کنـد و اگر يك الگو يافت شود می‌تـوان نتيجه گرفـت كه دنباله خروجي غيرتصادفي است.

يكنواختي حاصل از يك تابع رمزنگاری تصوير را مي‌توان بـــه صورت كمي بـا استفاده از آزمون مربع كای پيرسون ارزيـابی كـرد. آزمون مربع كای پيرسون طبق رابطه (۱۵) محاسبه می‌شود [۲۳].

$$\chi^2_{test} = \sum_{k=1}^{256} \frac{(v_k - e_k)^2}{e_k} \qquad (۱۵)$$

در رابطـه (۱۵)، k تعـداد سـطح خاكسـتری (۲۵۶)، v_k تعداد رخدادهای مشاهده هر سطح خاكستری (۲۵۵-۰) و e_k تعداد رخداد مورد انتظار هر سطح خاكستری مي‌باشد. بـه‌طور مثال، اگر تصوير اصلي دارای ابعاد W×H باشد آنگاه

$$e_k = \frac{H \times W}{256} \qquad (۱۶)$$

اگـــر $\chi^2_{test} < \chi^2$ (255,0.01)، آنگاه نتيجه گرفته مي‌شود كه توزيع هيستوگرام تصوير رمز گذاری شده يكنواخت مي‌باشد.

جدول ۹: آزمون χ^2

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۲۷۵	۲۸۰	۲۹۹/۲	۲۸۹/۳	۲۶۱	۲۶۷/۴	۲۶۸	الگوریتم پیشنهادی
۲۵۹/۷	۲۶۵/۲	۲۶۸/۸	۲۸۸/۴	۲۵۹/۲	۲۶۶/۳	۲۶۳	مرجع [۱۰]
۲۶۴/۱	۲۶۹/۹	۲۲۸/۶	۲۸۸/۱	۲۵۹/۳	۲۶۲/۷	۲۶۰	مرجع [۱۱]
۲۷۰/۶	۲۷۸/۸	۲۶۱,۵	۲۷۰/۹	۲۵۵/۳	۲۵۷/۵	۲۵۶/۸	مرجع [۱۲]

نتايج آزمون مربع خي در جدول ۹ثبت شده‌است. نتايج به دست آمده از جـدول ۹، نشان مي‌دهد كه $\chi^2_{test} < \chi^2$ (255,0.01)، يعني توزيع هيستوگرام تصوير رمزگذاری شده توسط الگوريتم‌هـا يكنواخت مـی‌باشـد. در انتهـا بـا مقايسـه نتـايج حاصـل مـی‌تـوان نتيجـه گرفـت، الگوريتم پيشنهادی بهتر عمل كرده‌است.

۴-۵ فضای كليد رمزنگاری

فضـای كليد رمزنگـاری، تعداد كل كليـدهای مختلفـی است كه مـــــی‌توان در الگوريتم رمزنگاری استفاده كرد [۲۴]. كليـــــد رمزنگاری مراجع [۱۰] تـا [۱۲]، شـامل پارامترهـا و مقـادير اوليـه سيستم آشوبی می‌باشند. اگر دقـت محاسبات $۱۰^{-۱۴}$ فـرض شـود، آنگاه فضای كليد رمزنگاری مراجع [۱۰] تـا [۱۲] بـه ترتيـب برابر هستند بـا $۱۰^{۸۴} = ۶(۱۰^{۱۴})$، $۱۰^{۸۴} = ۶(۱۰^{۱۴})$ و $۱۰^{۱۱۲} = ۸(۱۰^{۱۴})$. از آنجا كه ۴ نوكلئوتيد DNA در كليد رمزنگاری الگـوريتم پيشـنهادی دخيـل هسـتند، پـس $۱۰^{۵۶} = ۴(۱۰^{۱۴})$ در فضـای كليـد رمزنگـاری منظـور مـی‌شـود. فضـای كليـد رمزنگـاری الگـوريتم پيشـنهادی در جدول ۱۰ثبت شده‌است.

جدول ۱۰: فضای كليد رمزنگاری

۲۵۶ بيتی	۱۹۲ بيتی	۱۲۸ بيتی	
$۱۰^{۵۶} \times ۱۰^{۷۷}$	$۱۰^{۵۶} \times ۱۰^{۵۷}$	$۱۰^{۵۶} \times ۱۰^{۳۸}$	الگوريتم پيشنهادی

اگـر فضـای كليـد رمزنگـاری بزرگتـر از $۱۰^{۳۰} \simeq ۲^{۱۰۰}$ باشـد، می‌توان اطمينان داشت كه الگوريتم از فضای كليد رمزنگاری بسيار خوبی بهره‌مند است. پس الگوريتم‌های مورد مطالعه از فضای كليد مناسبی برخوردار می‌باشند. از آنجا كه هرچقدر فضای كليد بزرگتـر باشد، آن الگوريتم قابل اعتمادتر است؛ پس الگوريتم پيشـنهادی بـا كليد رمزنگاری ۲۵۶ بيتی قابل اعتمادتر می‌باشد.

۴-۶ حساسيت نسبت به كليد

حساسيت نسبت به كليد، يـک ويژگـی ضـروری بـرای يـک سـامانه رمزنگاری مطلوب مي‌باشد. بدين معني كه تغيـر يك بيت در كليـد رمزنگـــاری، بايستي يك تصوير رمزگـــذاری شـــده كاملا متفاوت توليد كند. برای آزمودن ميزان حساسيت نسبت به كليد طرح‌هـــای رمزنگاری، تصوير مورد آزمايش يكبار با استفاده از كليد رمزنگـاری اصلي و يكبار با استفاده از كليد رمزنگـاری كـه كمي تغيير يافته، رمزگذاری مي‌شود [۲۴].

از آنجا كه مقايسه دو تصوير از طريق مشاهده كاری دشوار است، لـــــــذا برای مقايسه بهتر مي‌توان درصد تعداد پيكسل‌های متمايز دو تصوير رمزگـذاری شـده با كليدهای متفاوت را محاسبه كرد. هـر چه مقدار اين محاسبه بـه ۱۰۰% نزديك‌تـر باشـد، آنگاه حساسيت نسبت به كليد بيشتر است.

جدول ۱۱: درصد تعداد پيكسل‌های متمايز دو تصوير رمزگذاری شده

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۹۹,۹%	۹۹,۸%	۹۹,۷%	۹۹,۸%	۹۹,۸%	۹۹,۷%	۹۹,۹%	الگوریتم پیشنهادی
۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	۹۹,۵%	مرجع [۱۰]
۹۹,۵%	۹۹,۶%	۹۹,۵%	۹۹,۷%	۹۹,۶%	۹۹,۵%	۹۹,۶%	مرجع [۱۱]
۹۹,۸%	۹۹,۷%	۹۹,۶%	۹۹,۷%	۹۹,۶%	۹۹,۶%	۹۹,۷%	مرجع [۱۲]

نتـايج مربـوط بـه درصد تعداد پيكسل‌های متمايز دو تصوير رمزگـذاری شـده توسـط الگوريتم‌هـای مـورد مطالعـه در جـدول ۱۱ثبت شده‌است. نتايج حاصل، نشان از حساسيت نسبت به كليد الگوريتم‌هـای مـورد مطالعـه می‌باشـد. بـه دليـل آنكـه الگـوريتم پيشنهادی به ۱۰۰% نزديک‌تر مـی‌باشـد، می‌تـوان نتيجـه گرفـت كـه حساسيت بيشتری نسبت بـه كليد از خـود نشـان می‌دهـد و در ايـن آزمون موفق‌تر بوده‌است.

۴-۷ ماكزيمم نسبت سيگنال به نويز

ماكزيمم نسبت سيگنال به نويز معياری برای نمايش ميزان سـيگنال مفيد در مقابل سيگنال مزاحم (يـا نـويز) در سيسـتم‌های الكتريكـی است. اين عدد، نسبت توان سيگنال بـه تـوان نـويز است. در مـورد تصاوير، تصوير اصلی به عنوان سيگنال و تصوير رمزگذاری شده به عنوان نويز در نظر گرفته می‌شود. ماكزيمم نسبت سـيگنال بـه نـويز طبـق رابطـه (۱۷) و ميـانگين خطـای مربعـات طبـق رابطـه (۱۸) محاسبه می‌شود [۲۵].

$$PSNR = 20 \times \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (۱۷)$$

$$MSE = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}[I(i,j) - K(i,j)]^2 \qquad (۱۸)$$

در رابطه (۱۷)، I نشان‌دهنده مقادیر پیکسل تصویر اصلی، K نشان‌دهنده مقادیر پیکسل تصویر رمزگذاری شده، (i,j) موقعیت پیکسل‌ها، W و H نشان‌دهنده ابعاد تصویر می‌باشند. زمانی می‌توان گفت سامانه رمزنگاری موفق عمل کرده‌است که تصویر رمزگذاری شده دارای مقدار میانگین خطای مربعات زیاد و ماکزیمم نسبت سیگنال به نویز کم باشد؛ در واقع مقدار کم ماکزیمم نسبت سیگنال به نویز نشان‌دهنده تفاوت بیشتر بین تصویر اصلی و تصویر رمزگذاری شده می‌باشد.

جدول ۱۲: میانگین خطای مربعات

تصویر	کشتی	تانک	هواپیما	ساعت	پنتاگون	لنا	بابون
الگوریتم پیشنهادی	۱۲۹	۱۲۹,۷	۱۸۲	۱۷۵	۱۲۷/۴	۱۳۰,۷	۱۳۲
مرجع [۱۰]	۱۱۵,۹	۱۲۱	۱۶۹,۱	۱۵۶	۱۲۱,۷	۱۲۲	۱۲۶
مرجع [۱۱]	۱۲۴,۵	۱۲۱,۸	۱۷۲,۲	۱۶۰	۱۲۴,۴	۱۲۶	۱۲۶,۸
مرجع [۱۲]	۱۲۶	۱۲۵,۶	۱۷۷	۱۶۸	۱۲۶,۹	۱۲۸,۱	۱۲۷,۹

جدول ۱۳: ماکزیمم نسبت سیگنال به نویز

تصویر	کشتی	تانک	هواپیما	ساعت	پنتاگون	لنا	بابون
الگوریتم پیشنهادی	۳۰	۲۷/۲	۲۵	۲۶/۶	۲۴	۲۸/۵	۲۷
مرجع [۱۰]	۳۶	۲۹/۱	۲۸/۶	۲۹/۱	۲۸/۳	۳۰/۳	۲۹/۵
مرجع [۱۱]	۳۵/۳	۲۸/۵	۲۷/۹	۲۸/۴	۲۷/۷	۳۰/۱	۲۹/۲
مرجع [۱۲]	۳۲	۲۸	۲۶/۳	۲۷	۲۵/۵	۲۹	۲۸/۱

نتایج میانگین خطای مربعات و ماکزیمم نسبت سیگنال به نویز تصاویر رمزگذاری شده توسط الگوریتم‌ها در جداول ۱۲ و ۱۳ ثبت شده‌است. با مقایسه نتایج، می‌توان نتیجه گرفت که الگوریم پیشنهادی بهتر عمل کرده‌است.

۴-۸ دقت

دقت فرآیند رمزنگاری، بوسیله ماکزیمم کردن انحراف بین نتایج رمزنگاری با تصویر اصلی محاسبه می‌گردد. نخست، نمودار هیستوگرام که نشان‌دهنده توزیع تصویر رمزنگاری شده و تصویر اصلی سطح خاکستری است، تولید شده و سپس تعداد پیکسل‌های هر مقدار مقیاس خاکستری در بازه ۰ تا ۲۵۵ شمرده می‌شود. دوم، اختلاف بین دو مقدار حاصل محاسبه می‌شود. در انتها، سطح زیر منحنی با اضافه کردن این مقادیر به سادگی اندازه گرفته می‌شود. مجموع انحراف D طبق رابطه (۱۹) محاسبه می‌شود [۲۶].

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad (۱۹)$$

در رابطه (۱۹)، h_i ماکزیمم جابجایی بین دو منحنی در مقدار i است. هرچه مقدار D بیشتر (مثبت یا منفی) باشد، تصویر رمزگذاری شده از تصویر اصلی دورتر خواهد بود.

جدول ۱۴: دقت

تصویر	کشتی	تانک	هواپیما	ساعت	پنتاگون	لنا	بابون
الگوریتم پیشنهادی	۵۰۸	۵۳۲	۳۸۲	۸۸۶	۵۴۱	۶۴۹	۷۵۰
مرجع [۱۰]	۴۶۴	۵۲۸	۲۵۹	۴۷۲	۴۶۱	۴۴۱	۲۶۸
مرجع [۱۱]	۴۶۵	۵۱۰	۲۶۰	۴۸۰	۵۰۰	۵۳۲	۳۳۹
مرجع [۱۲]	۴۶۸	۵۰۳	۲۶۳	۴۹۸	۵۰۴	۵۶۸	۵۰۰

نتایج ماکزیمم انحراف الگوریتم‌های مورد مطالعه در جدول ۱۴ ثبت شده‌است. نتایج نشان می‌کند که الگوریتم پیشنهادی ماکزیمم انحراف کمتری نسبت به دیگر الگوریتم‌ها دارد، پس دقت فرآیند رمزنگاری آن بهتر می‌باشد.

۴-۹ سرعت

به طور کلی، سرعت رمزنگاری به ساختار پردازنده، اندازه حافظه، زبان برنامه‌نویسي و همچنین نوع کامپایلر وابسته مي‌باشد. بنابراین مقایسه سرعت رمزنگاری دو طرح رمزنگاری، بدون استفاده از محیط برنامه‌نویسي یکسان، کاری بیهوده است.

به طور معمول برای افزایش دقت در اندازه‌گیری‌های زماني، مجموعه تصویر ۱۰ بار رمزنگاری مي‌شود، سپس میانگین سرعت رمزنگاری آنها ثبت مي‌شود [۲۷]. کارایي الگوریتم‌های مورد مطالعه با استفاده از کد MATLAB بر روی ماشيني با پردازنده Intel Core i5 1.80 GHz و 8 GB of RAM در محیط سیستم‌عامل ویندوز ۱۰، ارزیابی شد. نتایج این ارزیابي بر حسب ثانیه در جدول ۱۵ ثبت شده‌است.

جدول ۱۵: سرعت

تصویر	کشتی	تانک	هواپیما	ساعت	پنتاگون	لنا	بابون
الگوریتم پیشنهادی	۳۷۰/۳	۳۸۵/۱	۳۶۰	۳۹۲/۴	۴۰۰	۴۰۰/۵	۴۶۲
مرجع [۱۰]	۶۲/۵	۶۵/۳	۵۹/۲	۶۸/۴	۶۸/۶	۶۹/۳	۷۰/۵
مرجع [۱۱]	۳۶۳/۱	۳۷۶/۲	۳۵۹/۳	۳۹۰/۵	۳۹۰/۵	۳۹۰/۱	۳۹۰/۲
مرجع [۱۲]	۳۶۱	۳۶۸/۴	۳۴۵	۳۸۶/۳	۳۸۶/۳	۳۸۷	۳۸۸/۱

مطابق نتایج ثبت شده در جدول ۱۵، در این آزمون الگوریتم پیشنهادی توانست از دیگر الگوریتم‌ها موفق‌تر عمل نماید.

۴-۱۰ شکست‌ناپذیری

شکست‌ناپذیری به معنای مقاومت در برابر عوامل خارجی می‌باشد. عوامل خارجی می‌توانند حملاتی به منظور دستیابی برای کلید رمزنگاری باشد و یا نویز باشد که بر ساختار و اجرای سامانه رمزنگاری تاثیر می‌گذارد.

۴-۱۰-۱ حمله

در رمزنگاری، کلید رمزنگاری قطعه معلومات یا پارامتری است که به کاربر اجازه دسترسی به اطلاعات را نمی‌دهد. در واقع الگوریتم رمزنگاری با استفاده از کلید رمزنگاری می‌تواند داده‌های رمزگذاری شده را به صورت اولیه درآورد. در زمان طراحی سامانه‌های رمزگذاری، فرض بر این گذاشته می‌شود که جزئیات

الگوریتم رمزنگاری برای نفوذگر مشخص است. بر اساس این تلقی که به آن اصل Kerckhoffs گفته می‌شود، تنها مخفی بودن کلید رمزنگاری است که امنیت را تأمین می‌کند [۲۸]. تاریخچه رمزنگاری نیز نشان می‌دهد که تلاش برای مخفی نگاه داشتن الگوریتم‌های رمزنگاری با کاربرد گسترده، با دشواری زیادی همراه است. در مقابل، مخفی نگاه داشتن کلید رمزنگاری آسان‌تر است، چون کلید رمزنگاری قطعه کوچکی از اطلاعات است که در صورت لو رفتن به سادگی قابل تغییر است (برخلاف الگوریتم رمزنگاری که تغییر آن آسان نیست). امنیت هر الگوریتم رمزنگاری مستقیما به پیچیده بودن اصولی مربوط است که الگوریتم بر اساس آن بنا شده‌است.؛ اما اساسا امنیت رمزنگاری بر اساس پنهان ماندن کلید رمزنگاری و نه الگوریتم مورد استفاده است.

هر چیزی که مکانیزم امنیت سیستم را دور زده و باعث تخریب گردد را حمله گویند. در بیشتر انواع حمله، مهاجم تمام کلیدهای رمزنگاری ممکن را تولید و روی متن رمزگذاری شده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتم‌های رمزنگاری در برابر این نوع حمله آسیب‌پذیر هستند، اما با استفاده از کلیدهای رمزنگاری طولانی‌تر، می‌توان کار را برای حمله‌کننده مشکل‌تر کرد.

حملات مرسوم به سامانه رمزنگاری تصویر عبارتند از حمله جستجوی جامع، حمله تفاضلی، حمله متن اصلی مشخص، حمله متن اصلی منتخب. در ادامه به این حملات پرداخته می‌شود.

حمله جستجوی جامع

در رمزنگاری، حمله جستجوی جامع یا حمله غیرهوشمندانه، حمله‌ای است که در آن تمام حالات ممکن تا رسیدن به جواب بررسی می‌گردد [۲۹].

برای هر الگوی رمزنگاری می‌توان زمان لازم برای آزمودن کلیه حالات ممکن برای کلید رمزنگاری را محاسبه نمود و معمولا الگوهای رمزنگاری آنچنان طراحی می‌شوند که آزمودن تمامی حالات ممکن در یک زمان قابل قبول غیرممکن یا غیرمؤثر باشد.

طول کلید رمزنگاری، تعیین‌کننده قابل اجرا بودن حمله جستجوی جامع برای رمزگشایی می‌باشد. افزایش طول کلید رمزنگاری می‌تواند استفاده از این روش را به صورت نمایی سخت‌تر کند. کلیدهای رمزنگاریی که به صورت دلبخواه، بی‌معنا یا گمراه‌کننده انتخاب شوند، می‌توانند کاربرد این حمله را به شدت دشوارتر کنند. بدیهي است که جهت جلوگیری از حمله جستجوی جامع، فضای کلید الگوریتم رمزنگاری بایستي به اندازه کافي بزرگ باشد. اگر برای مهاجم آزمون کردن کلیه کلیدهای رمزنگاری ممکن با استفاده از کامپیوترهای مدرن بسیار زمان‌بر باشد، به طور مثال چندین دهه، آنگاه مي‌توان گفت که الگوریتم رمزنگاری نسبت به حمله جستجوی جامع از نظر محاسباتي امن مي‌باشد.

همانطور که در بخش ۴-۵ توضیح داده شد، فضای کلید رمزنگاری الگوریتم پیشنهادی با کلید رمزنگاری ۲۵۶ بیتی، 10^{133} می‌باشد. از آنجا که فضای کلید رمزنگاری مراجع [۱۰] تا [۱۲]، به ترتیب برابر هستند با $10^{84}=(10^{14})^6$، $10^{84}=(10^{14})^6$ و $10^{112}=(10^{14})^8$؛ در نتیجه الگوریتم پیشنهادی به دلیل داشتن فضای کلید رمزنگاری بزرگتر نسبت به دیگر الگوریتم‌ها، بیشتر در برابر حمله جستجوی جامع از خود مقاومت نشان می‌دهد.

حمله تفاضلی

در حمله تفاضلی، مهاجم تلاش مي‌كند كه با ايجاد تغييرات جزئي در تصوير ورودي، تغييرات حاصل در تصوير رمزگذاري شده را مشاهده كند. با اين روش، رابطه معني‌دار بين تصوير اصلي و تصوير رمزگذاري شده آشكار مي‌شود كه اين عمل خود منجر به تسهيل در تشخيص و شناسايي كليد رمزنگاري مي‌شود [۳۰]. براي آزمودن اثر تغيير يك پيكسل ورودي بر روي تمام تصوير رمزگذاري شده به وسيله الگوريتم‌هاي مورد مطالعه، معيارهاي تعداد نرخ تغييرات پيكسل‌ها و ميانگين يكپارچه تغيير شدت (در بخش ۳-۴ كامل شرح داده شده‌است) استفاده مي‌گردد. با توجه به جداول ۶ و ۷، می‌توان نتیجه گرفت که الگوریتم پیشنهادی در برابر حمله تفاضلی مقاومت بیشتری نسبت به دیگر الگوریتم‌ها از خود نشان می‌دهد.

حمله متن اصلی مشخص و حمله متن اصلی منتخب

در حمله متن اصلی مشخص، مهاجم دارای نمونه‌هایی از متن اصلی و نسخه رمزگذاری شده آن (متن رمزگذاری شده) است [۳۱].

در حمله متن اصلی منتخب، فرض می‌شود حمله‌کننده قابلیت انتخاب دلخواه پیام اصلی را دارد و می‌تواند پیام رمزگذاری شده مربوط به آن را به دست آورد [۳۱]. هدف حمله به دست آوردن اطلاعات بیشتری است که می‌تواند امنیت طرح‌های رمزنگاری را کاهش دهد. در بدترین حالت حمله می‌تواند کلید رمزنگاری طرح را فاش نماید.

برای بررسی مقاومت سامانه رمزنگاری نسبت به حمله متن اصلی مشخص و حمله متن اصلی منتخب می‌توان حساسیت نسبت به کلید را بررسی کرد (در بخش ۴-۶ شرح داده شده‌است). با بررسی جدول ۱۱، می‌توان نتیجه گرفت که الگوریتم پیشنهادی حساسیت بیشتری نسبت به کلید رمزنگاری دارد و مقاومت بهتری نسبت به دیگر الگوریتم‌ها در برابر حملات متن اصلی مشخص و متن اصلی منتخب از خود نشان می‌دهد.

۲-۱۰-۴ نویز

نویز به سیگنالی ناخواسته گفته می‌شود که بر سیگنال‌های دیگر اثر نامطلوب می‌گذارد؛ اما در علم پردازش تصویر، نویز به اختلالات ناخواسته به وجود آمده روی تصویر گفته می‌شود؛ به گونه‌ای که بر روی کیفیت تصویر تاثیر منفی می‌گذارد [۳۲].

نویز، ذاتا ماهیتی تصادفی یا اتفاقی دارد، بنابراین در بررسی آن از مفاهیم آمار و احتمال استفاده می‌شود. به منظور بررسی میزان تاثیر نویز در تصویر از معیارهای ماکزیمم نسبت سیگنال به نویز و میانگین خطای مربعات استفاده می‌شود.

نویز نمک و فلفل

اگر تصویری دارای نویز نمک و فلفل باشد، آنگاه نقاط سیاه و سفیدی در اکثر نقاط تصویر خواهد افتاد. این نقاط سیاه و سفید بر روی پیکسل‌های تصویر اصلی می‌افتند و کیفیت تصویر اصلی را پایین می‌آورند [۳۲]. شکل ۴، نویز نمک و فلفل با تراکم نویز ۰/۰۲ برای تصویر اصلی پنتاگون (شکل ۱) را نشان می‌دهد.

شکل ٤: تصویر اصلی پنتاگون حاوی نویز نمک و فلفل

جدول ١٦: میانگین خطای مربعات

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۱۳۲	۱۳۰,۷	۱۲۹/۴	۱۷۵	۱۸۹	۱۲۶,۷	۱۲۸	الگوریتم پیشنهادی
۱۲۶	۱۲۵	۱۲۱,۷	۱۵۶	۱۶۹,۱	۱۲۰	۱۱۲,۹	مرجع [۱۰]
۱۲۶,۸	۱۲۶	۱۲۴,۴	۱۶۰	۱۷۰,۲	۱۲۱,۸	۱۲۰,۵	مرجع [۱۱]
۱۲۷,۹	۱۲۹,۱	۱۲۶,۹	۱۶۸	۱۸۲	۱۲۵,۱	۱۲۶	مرجع [۱۲]

جدول ۱۷: ماکزیمم نسبت سیگنال به نویز

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۲۷	۲۸/۵	۲۳	۲۶/۶	۲۴	۲۷/۲	۳۱	الگوریتم پیشنهادی
۲۹/۵	۳۰/۹	۲۸/۳	۲۸/۸	۲۸/۶	۲۹/۱	۳۶	مرجع [۱۰]
۲۹/۲	۳۰/۱	۲۷/۷	۲۸/۱	۲۷/۹	۲۸/۵	۳۴/۳	مرجع [۱۱]
۲۸/۱	۲۹	۲۵/۵	۲۷	۲۶/۳	۲۸	۳۲	مرجع [۱۲]

نتایج میانگین خطای مربعات و ماکزیمم نسبت سیگنال به نویز تصاویر رمزگذاری شده حاوی نویز نمک و فلفل در جداول ۱۶ و ۱۷ ثبت شده‌است. با مقایسه نتایج، می‌توان نتیجه گرفت که نویز نمک و فلفل تاثیر کمتری بر الگوریتم پیشنهادی دارد.

نویز گاوسی

نویز گاوسی باعث می‌شود تصاویر کم‌رنگ و تار به نظر برسند [۳۲]. شکل ۵، نویز گاوسی با میانگین ۰/۰۲ برای تصویر اصلی هواپیما (شکل ۱) را نشان می‌دهد.

نتایج میانگین خطای مربعات و ماکزیمم نسبت سیگنال به نویز تصاویر رمزگذاری شده حاوی نویز گاوسی در جداول ۱۸ و ۱۹ ثبت شده‌است. با مقایسه نتایج، می‌توان نتیجه گرفت که نویز گاوسی تاثیر کمتری بر الگوریتم پیشنهادی دارد.

در انتها بعد از بررسی نتایج مربوط به حملات و نویزها می‌توان نتیجه گرفت، الگوریتم پیشنهادی شکست‌ناپذیر است یا به عبارت دیگر در برابر عوامل خارجی نسبت به مراجع [۱۰] تا [۱۲]، مقاومت بیشتری از خود نشان می‌دهد.

شکل ٥: تصویر اصلی پنتاگون حاوی نویز گاوسی

جدول ۱۸: میانگین خطای مربعات

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۱۳۹	۱۳۰,۷	۱۳۷/۴	۱۷۵	۱۹۲	۱۳۹,۷	۱۴۰	الگوریتم پیشنهادی
۱۲۶	۱۲۲	۱۲۱,۷	۱۵۶	۱۶۹,۱	۱۲۱	۱۱۵,۹	مرجع [۱۰]
۱۲۶,۸	۱۲۶	۱۳۴,۴	۱۶۰	۱۸۲,۸	۱۲۱,۸	۱۳۴,۵	مرجع [۱۱]
۱۲۷,۹	۱۲۸,۱	۱۳۶,۹	۱۶۸	۱۹۷	۱۳۵,۶	۱۳۶	مرجع [۱۲]

جدول ۱۹: ماکزیمم نسبت سیگنال به نویز

بابون	لنا	پنتاگون	ساعت	هواپیما	تانک	کشتی	تصویر
۲۷	۲۸/۵	۲۸/۳	۲۱/۶	۲۵	۲۷/۹	۳۱	الگوریتم پیشنهادی
۲۹/۵	۳۰/۳	۳۸/۳	۲۹/۱	۲۸/۶	۲۹/۱	۳۸	مرجع [۱۰]
۲۸/۴	۳۰/۱	۳۷/۷	۲۵/۴	۲۷/۹	۲۸/۵	۳۶/۳	مرجع [۱۱]
۲۸/۱	۲۹	۳۲/۵	۲۳	۲۶/۳	۲۸	۳۴	مرجع [۱۲]

۵ نتیجه‌گیری

امروزه، برای رمزنگاری تصویر الگوهای متنوعی پیشنهاد شده‌است که در این میان، ترکیب الگوریتم‌های رمزنگاری با دنباله DNA از محبوبیت ویژه‌ای برخوردار می‌باشد.در این مقاله نیز الگوریتمی بصورت ترکیب الگوریتم استاندارد رمزنگاری پیشرفته و دنباله DNA پیشنهاد شده‌است.

الگوریتم پیشنهادی شامل ۶ گام می‌باشد. در گام اول، نشان داده می‌شود که چگونه داده‌های دودویی بدون تغییر آمینواسیدهای یک پروتئین، به DNA تبدیل می‌شود. در گام دوم عملیات یای انحصاری بین دو رشته DNA مطرح می‌شود. در گام سوم، چهارم، پنجم و ششم به ترتیب جانشین‌سازی بایت‌ها، جابجاسازی سطرها، درهم‌ریزی ستون‌ها و افزودن کلید چرخه بررسی شده‌است. در گام سوم، براساس جدول جستجو، بایتی که قرار است در آرایه حالت جایگزین شود، پیدا می‌شود. در گام چهارم، بایت‌های هر سطر آرایه حالت به وسیله یک آفست معین به صورت چرخشی شیفت می‌یابد. در گام پنجم، چهار بایت از هر ستون حالت با استفاده از تبدیل خطی معکوس ترکیب می‌شوند. در انتها در گام ششم، کلید چرخه مشخص می‌شود.

جهت ارزیابی الگوریتم پیشنهادی از آزمون‌هایی استاندارد از قبیل آنتروپی، هیستوگرام و غیره استفاده شد که نتایج حاصل از این آزمون‌ها از قبیل نزدیک بودن میزان بی‌نظمی به عدد ۸، همگی کارآمدی سیستم رمزنگاری پیشنهادی را به وضوح نشان می‌دهند. نتایج آزمایش‌ها و تحلیل‌های امنیتی نیز نشان می‌دهد که الگوریتم پیشنهادی با کلید رمزنگاری ۲۵۶ بیتی دارای امنیت رمزنگاری قابل قبول‌تر، فضای کلید رمزنگاری بزرگتر و مقاومت بیشتر در برابر عوامل خارجی نسبت به مراجع [۱۰] تا [۱۲] می‌باشد.

بعد از بررسی نتایج حاصل از ارزیابی‌ها، می‌توان نتیجه گرفت که عملکرد سیستم رمزنگاری با تغییر نگاشت آشوبی لجستیک ۲ بعدی به هنون-سین ۲ بعدی، بهبود یافته‌است؛ همچنین حذف دنباله DNA و تغییر نسخه نگاشت آشوبی لجستیک، باعث افزایش عملکرد سیستم رمزنگاری شده‌است.

در انتها شایان ذکر است که الگوریتم پیشنهادی توانسته است پارامترهای دقت، سرعت و شکست‌ناپذیری را نسبت به مراجع [۱۰] تا [۱۲] بهبود ببخشد.

مراجع

[1] Xu, M. "*Cryptanalysis of an Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-chaotic System*." 3D Research, vol.8, no.2, pp.15, Apr.2017.

[2] Qidwai, U., Chen, C.H. "*Digital image processing: an algorithmic approach with MATLAB*." Chapman and Hall/CRC, Oct.2009.

[3] Murugan, C.A., KarthigaiKumar, P. "*Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms*." Mobile Networks and Applications, pp.1-6, May.2018.

[4] Matthews, R. "*On the derivation of a chaotic encryption algorithm*." Cryptologia, vol.8, no.1, pp.29-42, 1989.

[5] Guo, J.I., Yen, J.C. "*A new chaotic key-based design for image encryption and decryption*." In IEEE International Symposium on Circuits and Systems. Emerging Technologies for the 21st Century, Vol.4, pp.49-52, May.2000.

[6] Dara, M., Manochehri, K. "*A novel method for designing s-boxes based on chaotic logistic maps using cipher key*". World applied sciences journal, vol.28, no.12, pp.2003-2009, 2013.

[7] Elamrawy, F., Sharkas, M., Nasser, A.M. "*An image encryption based on DNA coding and 2D Logistic chaotic map*." International Journal of Signal Processing, vol.3, pp.27-32, 2018.

[8] Zhang, J., Huo, D. "*Image encryption algorithm based on quantum chaotic map and DNA coding*." Multimedia Tools and Applications, vol.78, no.11, pp.15605-15621, 2019.

[9] Kulsoom, A., Xiao, D., Abbas, S.A. "*An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules*." Multimedia Tools and Applications, vol.75, no.1, pp.1-23, Jul.2014.

[10] Chai, X., Chen, Y., Broyde, L. "*A novel chaos-based image encryption algorithm using DNA sequence operations*." Optics and Lasers in Engineering, vol.88, pp.197-213, Jan.2017.

[11] Ye, G., Jiao, K., Pan, C., & Huang, X. "*An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map*." Security and Communication Networks, pp.11, Oct.2018.

[12] Wu, J., Liao, X., & Yang, B. "*Image encryption using 2D Hénon-Sine map and DNA approach*." Signal Processing, vol.153, pp.11-23, Jun.2018.

[13] Kaundal, A.K., Verma, A.K. "*DNA based cryptography: a review*." International Journal of Information and Computation Technology, vol.4, no.7, pp.693-698, Aug.2014.

[14] Jain, S., Bhatnagar, V. "*A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography*." Advances in Engineering and Technology Research (ICAETR), International Conference on. IEEE, pp.1-5, Aug.2014.

[15] Babu, E. S., Nagaraju, C., & Prasad, M. K. "*Light-Weighted DNA-Based Cryptographic Mechanism Against Chosen Cipher Text Attacks*." Advanced Computing and Systems for Security, Springer India, vol.395, pp.123-144, 2016.

[16] Ahmed, K., El-Henawy, I. "*Increasing robustness of data encryption standard by integrating DNA cryptography*." International Journal of Computers and Applications, vol.39, no.2, pp.91-105, Apr.2017.

[17] Hossain, E. M. S., Alam, K. M. R., Biswas, M. R., & Morimoto, Y. "*A DNA cryptographic technique based on dynamic DNA sequence table*." Computer and Information Technology (ICCIT), 19th International Conference on. IEEE, pp.270-275, Dec.2016.

[18] Pandya, P. "*Advanced Encryption Standard*." Computer and Information Security Handbook (Third Edition), pp.1185-1195, 2014.

[19] University of Southern California. "SIPI Image Database" Internet:http://sipi.usc.edu/database/database.php?volume=misc, Jan. 2000.

[20] Kumari, M., Shailender, G., & Pranshul, S. "*A Survey of Image Encryption Algorithms*." 3D Research, no.4, pp.1-35, Dec.2017.

[21] Luo, Y., Yu, J., Lai, W., Liu, L. "*A novel chaotic image encryption algorithm based on improved baker map and logistic map*." Multimedia Tools and Applications, vol.8, no.4, pp.35, Dec.2017.

[22] Kaur, M., Kumar, V. "*A Comprehensive Review on Image Encryption Techniques*." Archives of

Computational Methods in Engineering, pp.1-29, Nov.2018.

[23] Pei, B., Zhao, H., Xing, W., Lee, H. S. "*The Exploration of Automated Image Processing Techniques in the Study of Scientific Argumentation*." Cognitive Computing in Technology-Enhanced Learning, pp.175-190, 2019.

[24] Fu, X. Q., Liu, B. C., Xie, Y. Y., Li, W., Liu, Y. "*Image encryption-then-transmission using DNA encryption algorithm and the double chaos*." IEEE Photonics Journal, vol.10, no.3, pp.1-15, Jun.2018.

[25] Chaudhary, V. "*PSNR and Robustness Comparison Between DCT and SVD Based Digital Image Watermarking Against Different Noise and Attacks*." Advances of Science and Technology: 6th EAI International Conference, vol.274, pp.315, 2019.

[26] Usama, M., Khan, M.K., Alghathbar, K., Lee, C., "*Chaos-based secure satellite imagery cryptosystem*." Computers & Mathematics with Applications, vol.60, no.2, pp.326-337, 2010.

[27] Kumari, M., Gupta, S. "*A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher*." 3D Research, vol.9, no.1, p.10, Feb.2018.

[28] Cayre, F., & Bas, P. "*Kerckhoffs-based embedding security classes for woa data hiding*." IEEE Transactions on Information Forensics and Security, vol.3, no.1, pp.1-15, Mar.2008.

[29] Nardo, L.G., Nepomuceno, E.G., Arias-Garcia, J., Butusov, D.N. "*Image encryption using finite-precision error*." Chaos, Solitons & Fractals, vol.123, pp.69-78, 2019.

[30] Akhavan, A., Samsudin, A., Akhshani, A. "*Cryptanalysis of an image encryption algorithm based on DNA encoding*." Optics & Laser Technology, vol.95, pp.94-99, Apr.2017.

[31] Xiong, Y., C. Quan. "*Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting*." Optics & Laser Technology, vol.109, pp.456-464, Aug.2018.

[32] Perry, S. "*Image and Video Noise: An Industry Perspective*." In Denoising of Photographic Images and Video, pp. 207-234. Springer, Cham, 2018.