نشریه علمی "پدافند الکترونیکی و سایبری"
سال هشتم، شماره ۳، پاییز ۱۳۹۹، ص ۱۵۰-۱۳۹

علمی– پژوهشی

الگوریتم رمزنگاری تصویر مبتنی بر گروه جایگشت S_n و توابع آشوب

ابراهیم زارعی زفره

استادیار، گروه علوم کامپیوتر، دانشگاه خوانسار، خوانسار، ایران

(دریافت: ۹۸/۰۸/۲۴، پذیرش: ۹۸/۱۱/۱۲)

چکیده

در این مقاله، یک الگوریتم رمزنگاری تصویر جدید با استفاده از گروه جایگشت S_n و توابع آشوب ارائه شده است. الگوریتم پیشنهادی شامل سه مرحله می‌باشد: (۱) با اعمال توابع درهم‌ساز بر روی اطلاعات تصویر اصلی و کلید رمز خارجی ۲۵۶ بیتی، یک کلید رمز محرمانه ۲۵۶ بیتی استخراج می‌گردد که با کمک آن شرایط اولیه و پارامترهای مربوط به توابع آشوب تولید می‌شود؛ (۲) در مرحله انتشار، با انجام یک جایگشت سطری و یک جایگشت ستونی مبتنی بر توابع آشوب، موقعیت پیسکل‌ها در تصویر اصلی جابه‌جا می‌شود به‌طوری که همبستگی بین پیکسل‌های مجاور به شدت کاهش می‌یابد؛ (۳) در مرحله اغتشاش، مقدار سطح روشنایی هر پیکسل با انجام جایگشت در سطح بیت با کمک گروه جایگشت S_8 و توابع فوق آشوب تغییر می‌یابد؛ سپس با انجام تبدیل در سطح بیت به وسیله جعبه‌های جایگزینی S_8Sbox و عملگر XOR، امنیت الگوریتم پیشنهادی افزایش می‌یابد. نتایج تجربی و تحلیل‌های امنیتی نشان می‌دهد که $NPCR >$ ٪۹۹/۶۰، $UACI >$ ٪۳۳/۴۰، آنتروپی بزرگ‌تر ۷/۹۹ و ضرایب همبستگی برای تصویر رمز نزدیک به صفر می‌باشد. همچنین الگوریتم رمزنگاری تصویر پیشنهادی مقاومت بالایی در برابر حملات متداول همانند حملات جستجوی کامل، برش و نویز از خود نشان می‌دهد.

کلیدواژه‌ها: رمزنگاری تصویر، گروه جایگشت، توابع آشوب، جعبه جایگزینی، انتشار، اغتشاش

۱- مقدمه

با توجه به رشد سریع فناوری اطلاعات در عصر حاضر و گسترش استفاده از داده‌های چندرسانه‌ای در شبکه‌های ارتباطی و اطلاعاتی، نیاز به طرح‌هایی برای محافظت در برابر کپی و توزیع غیر مجاز اطلاعات بسیار ضروری می‌باشد [۱]. تصاویر دیجیتال یکی از انواع پر کاربرد و با اهمیت داده‌های چندرسانه‌ای است که می‌تواند دربر گیرنده اطلاعات تجاری، نظامی، سیاسی و یا پزشکی باشند؛ بنابراین حفظ محرمانگی این اطلاعات اهمیت بسیار بالایی دارد. روش‌های متنوعی از جمله پنهان‌نگاری[1]، نهان‌نگاری[2] و رمزنگاری[3] برای حفظ محرمانگی تصویر و جلوگیری از دسترسی‌های غیر مجاز به محتوای تصویر وجود دارد.

رمزنگاری تصویر یکی از کارآمدترین و رایج‌ترین روش‌های محافظت از تصویر می‌باشد. به دلیل برخی ویژگی‌های درونی تصاویر، همانند افزونگی داده‌ها، حجم زیاد داده‌ها و همبستگی قوی بین پیکسل‌های مجاور، رمزنگاری تصویر متفاوت از رمزنگاری متن است، بنابراین سامانه‌های رمزنگاری سنتی همانند DES، AES و Blowfish برای رمزنگاری تصاویر مناسب نیستند و نیاز به روش‌های رمزنگاری با کارایی بالا از لحاظ امنیت و سرعت برای تصاویر ضروری می‌باشد [۲ و ۳]. بنابراین روش‌های متنوعی برای رمزنگاری تصویر بر پایه توابع آشوب، اتوماتای سلولی، محاسبات DNA و غیره پیشنهاد گردید.

توابع آشوب به دلیل ویژگی‌های ذاتی از جمله حساسیت شدید به شرایط اولیه و پارامترهای آن، غیر قابل پیش‌بینی بودن و رفتار تصادفی، موجب شده تا محققان زیادی برای رمزنگاری به این سامانه‌ها روی آورند [۴]. الگوریتم‌های رمزنگاری تصویر مبتنی بر توابع آشوب، شامل دو قسمت جایگشت پیکسل‌ها (تغییر مکان) و جایگزینی پیکسل‌ها (تغییر مقدار سطح روشنایی) می‌باشند [۵]. متهوس نخستین بار در سال ۱۹۸۹ از سامانه آشوب برای رمزنگاری استفاده نمود و فریدریچ در سال ۱۹۹۷ اولین سامانه آشوب را در رمزنگاری تصویر استفاده نمود [۶]. در ده‌های اخیر الگوریتم‌های رمزنگاری تصویر مختلفی مبتنی بر توابع آشوب توسط محققین در زمینه رمزنگاری گسترش یافت [۷ و ۸].

میرقدری و جلفایی [۹]، یک الگوریتم رمزنگاری تصویر با استفاده از توابع آشوب ارائه دادند که شامل سه مرحله است. در مرحله اول (اغتشاش)، مقدار پیکسل‌های تصویر با استفاده از یک

* رایانامه نویسنده مسئول: zarei@khansar-cmc.ac.ir

[1] Steganography
[2] Watermarking
[3] Cryptography

ماتریس جانشنی مبتنی بر نگاشت هنون[1] تغییر می‌یابد. در مرحله دوم (انتشار)، پیکسل‌های تصویر با استفاده از ماتریس‌های جایگشت سطری، ستونی و قطری مبتنی بر نگاشت بیکر[2] جابه‌جا می‌شوند. در مرحله سوم، تصویر حاصل از مرحله قبل با یک دنباله کلید مبتنی بر نگاشت بیکر، یای انحصاری[3] می‌شوند. الگوریتم فوق به اختصار SPK^r نامیده شد که r بیانگر تعداد دورهای تکرار عملیات رمزنگاری می‌باشد.

وو و همکاران [۱۰]، یک الگوریتم رمزنگاری تصویر بر اساس شبکه جابه‌جایی- جایگزینی شامل سه مرحله انتشار، اغتشاش و تبدیل مبتنی بر تابع آشوب دوبعدی لجستیک[4] ارائه نمودند.

نوروزی و همکاران [۱۱]، یک الگوریتم رمزنگاری تصویر بر اساس توابع فوق آشوب ارائه نمودند که شامل سه مرحله می‌باشد: (۱) رمزنگاری سطرها و ستون‌های تصویر اصلی؛ (۲) رمزنگاری زیر- تصویرهای تصویر اصلی (۳) تغییر مقدار چهار بیت با ارزش‌تر هر پیکسل تصویر به‌جای هشت بیت هر پیکسل.

اسد و فرج‌الله [۱۲]، یک روش رمزنگاری بر مبنای توابع آشوب ارائه دادند که شامل r دور تکرار عملیات رمزنگاری فوق‌الذکر می‌باشد: (۱) تکرار r_d مرتبه عمل اغتشاش به وسیله یک ماتریس دودویی با اندازه ۳۲×۳۲؛ (۲) سپس تکرار r_p مرتبه عمل انتشار روی هر پیکسل تصویر به وسیله یک جایگشت بیتی با کمک تابع آشوب دوبعدی.

موروگن و همکاران [۱۳]، یک الگوریتم رمزنگاری تصویر مبتنی بر توابع آشوب ارائه نمودند به‌طوری که از نگاشت آشوب هنون برای عمل انتشار و از نگاشت آشوب لورنز[5] برای عمل اغتشاش استفاده می‌کند.

بلزی و همکاران [۱۴]، یک جعبه جایگزینی بر اساس تابع آشوب لجستیک- سینوس ارائه نمودند. سپس یک الگوریتم رمزنگاری بر اساس شبکه جابه‌جایی- جایگزینی آشوبی و جعبه جایگزینی ارائه نمودند.

مندل و همکاران [۱۵]، یک الگوریتم رمزنگاری تصویر بر اساس تابع آشوب دوبعدی بیکر ارائه نمودند. در الگوریتم فوق، ابتدا پیکسل‌های تصویر اصلی بر اساس دنباله اعداد تصادفی تولید شده با تابع آشوب دوبعدی بیکر جابه‌جا شده و سپس مقدار پیکسل با تصویر کلید رمزنگاری با کمک یای انحصاری تغییر می‌یابد.

فرج‌الله‌زاده و مطیعی [۱۶]، یک الگوریتم رمزنگاری متقارن با استفاده از توابع آشوب ارائه دادند به‌طوری که از نگاشت آرنولد[6] برای عمل انتشار و از نگاشت سه‌بعدی لجستیک درهم آمیخته برای عمل اغتشاش استفاده می‌کند.

با توجه به خواص مناسب سامانه‌های آشوب در طراحی جعبه‌های جایگزینی، در سال‌های اخیر استفاده از توابع آشوب به‌منظور تولید جعبه‌های جایگزینی مورد توجه محققین در زمینه رمزنگاری قرار گرفته است و تحقیقات زیادی در این زمینه در حال انجام است [۱۷ و ۱۸]. در این مقاله، یک الگوریتم رمزنگاری تصویر با استفاده از گروه جایگشت S_n، توابع آشوب و جعبه‌های جایگزینی S_8Sbox ارائه شده است.

در ادامه مقاله، در بخش ۲ مفاهیم مقدماتی بیان می‌شود. در بخش ۳، الگوریتم رمزنگاری پیشنهای تشریح و سپس در بخش ۴، نتایج حاصل از تحلیل امنیت و ارزیابی الگوریتم رمزنگاری پیشنهای بیان می‌گردد. در بخش پایانی نیز نتیجه‌گیری ارائه می‌شود.

۲- مفاهیم مقدماتی

در این بخش، ابتدا مفاهیم مقدماتی سازنده الگوریتم پیشنهادی شامل توابع آشوب و گروه‌های جایگشت معرفی می‌شود.

۲-۱- توابع آشوب

توابع آشوب با برخورداری از امتیازات منحصر به فردی از جمله حساسیت شدید به شرایط اولیه و پارامترهای آن، غیر قابل پیش‌بینی بودن، رفتار تصادفی، یک روش ایده‌آل برای رمزنگاری تصویر محسوب می‌شوند [۴]. توابع آشوب یک‌بعدی به دلیل سادگی پیاده‌سازی و پیچیدگی محاسباتی کم، به‌طور گسترده در رمزنگاری تصویر استفاده می‌شوند. تابع آشوب لجستیک، یک سامانه آشوب یکبعدی به‌صورت زیر می‌باشد:

$$x_{i+1} = ax_i(1 - x_i), x_i \in (0,1) \quad (۱)$$

زمانی که $a \in [3.89, 4]$ باشد، دنباله تصادفی تولید شده در بازه $(0,1)$ خواهد بود [۱۹]. تابع آشوب لجستیک، انتخاب مناسبی برای انجام فرآیند جایگشت در زمان اجرای پایین می‌باشد.

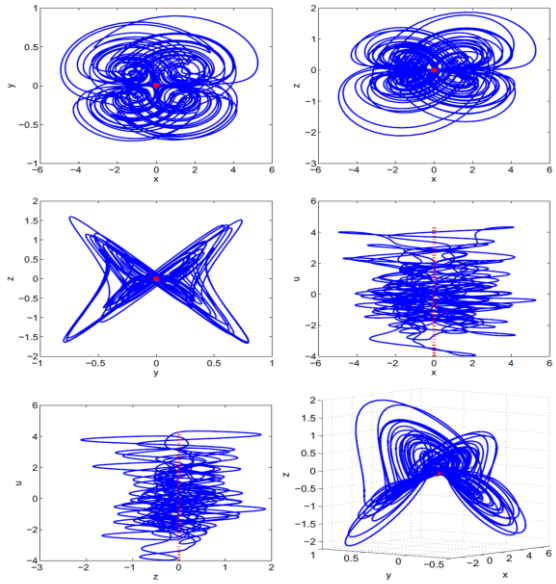
توابع فوق‌آشوب با داشتن حداقل دو نمای لیاپانوف مثبت و به دلیل محرمانگی قوی‌تر، پیچیدگی بیشتر، فضای کلید بزرگ‌تر و رفتار غیر خطی پیچیده‌تر نسبت به دیگر توابع آشوب، مقاومت بیشتری در برابر دسترسی‌های غیر مجاز دارند؛ بنابراین برای ساخت ماتریس کلید مناسب‌تر می‌باشند. در این مقاله، از تابع

[1] Henon
[2] Baker
[3] XOR
[4] Logistic
[5] Lorenz
[6] Arnold

فوق آشوب مرجع [۲۰] استفاده خواهد شد که به‌صورت زیر می‌باشد:

$$\begin{aligned} x_{i+1} &= ax_i + by_iz_i \\ y_{i+1} &= cy_i + dx_iz_i - ky_i(m + 3nu_i^2) \\ z_{i+1} &= ez_i + fx_iy_i + gx_iu_i \\ u_{i+1} &= -y_i \end{aligned} \quad (۲)$$

زمانی که پارامترهای $a = 0.35$، $b = -10$، $c = -0.6$، $d = 0.3$، $e = -1.6$، $f = 2$، $g = 0.1$، $m = 0.1$ و $n = 0.01$ باشد، آنگاه سامانه رفتار آشوبناک پیچیده از خود نشان می‌دهد [۲۰ و ۲۱]. شکل (۱) تصویر برخی نمودارهای جاذب ایجاد شده در صفحات مختلف را نشان می‌دهد.



شکل (۱): تصویر برخی نمودارهای جاذب در صفحات مختلف برای تابع فوق آشوب [۲۰] با پارامترهای $a = 0.35$، $b = -10$، $c = -0.6$، $d = 0.3$، $e = -1.6$، $f = 2$، $g = 0.1$، $m = 0.1$، $n = 0.01$ و $k = 0.2$. (تصویر از مرجع [۲۰]).

۲-۲- گروه جایگشت

گروه‌های جایگشتی، دسته‌ای از گروه‌های متناهی هستند که کاربردهای فراوانی در رمزنگاری، کدگذاری، علوم فیزیک، رایانه، برق و غیره دارند.

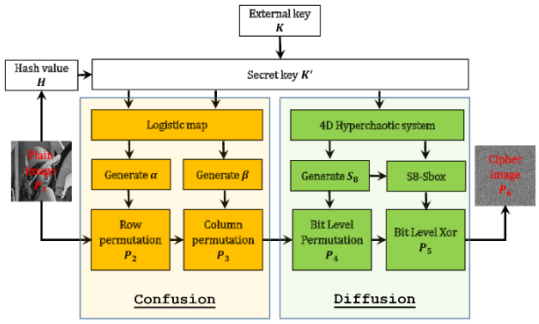
فرض‌کنید I_n یک مجموعه از n شی با برچسب‌های $1, 2, \dots, n$ باشد. در این صورت هر نگاشت یک‌به‌یک و پوشا از مجموعه I_n به مجموعه I_n را یک جایگشت گویند. به‌طور کلی، یک جایگشت α روی مجموعه $I_n=\{1, 2, ..., n\}$ را می‌توان به‌صورت زیر نمایش داد:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$$

مجموعه تمام جایگشت‌ها روی مجموعه I_n با S_n نمایش داده می‌شود و تعداد آن $|S_n| = n!$ است [۲۲]. در الگوریتم رمزنگاری پیشنهادی از گروه جایگشت S_n، به‌ویژه S_8 برای عملیات جایگشت در سطح بیت و تولید S_8Sbox استفاده می‌شود.

۳- الگوریتم رمزنگاری پیشنهادی

شکل (۲) دیاگرام الگوریتم رمزنگاری تصویر پیشنهادی را نشان می‌دهد. در ادامه مراحل رمزنگاری تشریح خواهد شد.



شکل (۲): دیاگرام الگوریتم رمزنگاری تصویر پیشنهادی.

۳-۱- تولید کلید محرمانه

الگوریتم رمزنگاری تصویر پیشنهادی دارای کلید رمز خارجی ۲۵۶ بیتی به نام K می‌باشد که به‌صورت تصادفی تولید شده و از طریق یک کانال ارتباطی امن قبل از عملیات رمزنگاری و رمزگشایی بین طرفین به اشتراک گذاشته می‌شود. کلید K به بلوک‌های ۸ بیتی در قالب دهدهی تقسیم شده و به‌صورت زیر نشان داده شده است:

$$K = [k_1, k_2, \dots, k_{32}] \quad (۳)$$

فرض کنید تصویر اصلی P_1 به‌صورت یک ماتریس دوبعدی $M \times N$ می‌باشد. با استفاده از ترکیب توابع درهم‌ساز MD5 و SHA256، اطلاعات تصویر و کلید K، مقدار درهم H با رابطه (۴) محاسبه و سپس به بلوک‌های ۸ بیتی در قالب دهدهی تقسیم می‌شود.

$$\begin{aligned} H &= SHA256(MD5(P_1), MD5(K)) \\ H &= [h_1, h_2, \dots, h_{32}] \end{aligned} \quad (۴)$$

با ترکیب کلید K و مقدار درهم H به وسیله عملگر XOR، کلید محرمانه K' به‌صورت زیر به‌دست می‌آید:

$$\begin{aligned} K' &= k'_1, k'_2, \dots, k'_{32} \\ k'_i &= k_i \oplus h_i \ , i = 1,2, \dots, 32 \end{aligned} \quad (۵)$$

با تغییر یک بیت از تصویر اصلی یا کلید K، مقدار درهم H و

کلید محرمانه K' به‌طور کامل تغییر خواهد کرد، بنابراین الگوریتم پیشنهادی نسبت به کوچک‌ترین تغییر در کلید K و تصویر اصلی حساس خواهد.

۳-۲- مرحله انتشار

در یک تصویر دیجیتال، هر پیکسل از تصویر در مجاورت با حداقل هشت پیکسل همسایه است؛ بنابراین همبستگی بالایی بین پیکسل‌های مجاور وجود دارد. در مرحله انتشار به‌منظور کاهش همبستگی بالای بین پیکسل‌های مجاور در تصویر اصلی، بدون تغییر مقدار سطح روشنایی پیکسل‌ها، مکان آن‌ها تغییر می‌یابد. باید توجه داشت که با کمک انتشار، هیستوگرام تصویر اصلی و تصویر رمز شده کاملاً مشابه یکدیگر می‌باشند؛ بنابراین رمزنگاری تنها با استفاده از انتشار، امنیت چندانی نخواهد داشت.

در الگوریتم پیشنهادی، نخست تمام سطرها و سپس تمام ستون‌های تصویر اصلی با استفاده از یک جایگشت سطری و یک جایگشت ستونی مبتنی بر تابع آشوب لجستیک تعویض می‌شوند. گام‌های اساسی این مرحله عبارتند از:

۱) دریافت تصویر اصلی P_1 به‌صورت یک ماتریس دوبعدی $M \times N$؛

۲) محاسبه پارامتر کنترل u و مقدار اولیه x_0 برای تابع آشوب لجستیک با استفاده از رابطه (۶)؛

$$u = 3.89 + ((k'_1 \oplus k'_2 \oplus \cdots \oplus k'_8) / 256) \times 0.01$$
$$x_0 = (k'_9 \oplus k'_{10} \oplus \cdots \oplus k'_{16}) / 256 \qquad (۶)$$

۳) تکرار N مرتبه تابع آشوب لجستیک و به‌دست آوردن بردار تصادفی R؛

۴) انجام عمل مرتب‌سازی صعودی بردار R با استفاده از تابع $[f_R, l_R] = Sort(R)$، که در آن بردار f_R شامل دنباله مرتب شده و l_R شامل مقادیر شاخص f_R؛

۵) تولید جایگشت سطری α با استفاده از رابطه (۷) و انجام عمل جایگشت سطری بر روی تصویر اصلی و تولید تصویر P_2؛

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & N \\ l_R(1) & l_R(2) & l_R(3) & \cdots & l_R(N) \end{pmatrix} \qquad (۷)$$

۶) تکرار M مرتبه تابع آشوب لجستیک و به‌دست آوردن بردار تصادفی C؛

۷) انجام عمل مرتب‌سازی صعودی بردار C با استفاده از تابع $[f_C, l_C] = Sort(C)$، که در آن بردار f_C شامل دنباله مرتب شده و l_C شامل مقادیر شاخص f_C؛

۸) تولید جایگشت ستونی β با استفاده از رابطه (۸) و انجام عمل جایگشت ستونی بر روی تصویر P_2 و تولید تصویر P_3؛

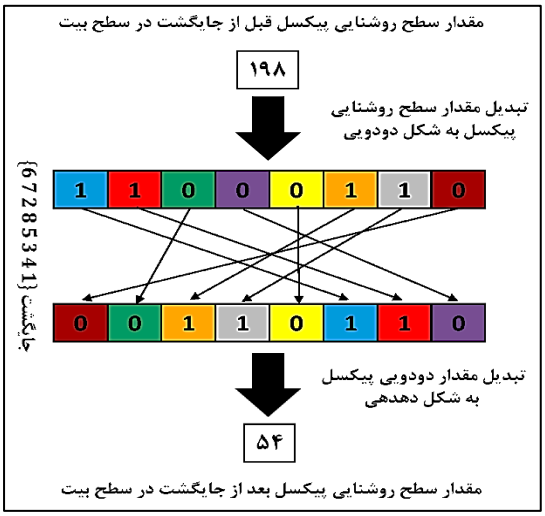
$$\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & M \\ l_C(1) & l_C(2) & l_C(3) & \cdots & l_C(M) \end{pmatrix} \qquad (۸)$$

۹) در نظر گرفتن تصویر P_3 به‌عنوان خروجی مرحله انتشار.

۳-۳- مرحله اغتشاش

در مرحله اغتشاش، مقدار سطح روشنایی پیکسل‌های تصویر تغییر می‌یابد، به‌طوری که هیستوگرام تصویر رمز شده یکنواخت و متمایز از هیستوگرام تصویر اصلی خواهد بود؛ در نتیجه امنیت الگوریتم رمزنگاری با اغتشاش در مقایسه با انتشار بالاتر خواهد بود. در الگوریتم رمزنگاری پیشنهادی، مرحله اغتشاش شامل دو بخش جایگشت در سطح بیت و تبدیل در سطح بیت می‌باشد. به‌منظور کاهش زمان اجرای الگوریتم پیشنهادی و کاهش پیچیدگی عملیات در سطح بیت، مرحله اغتشاش به‌صورت موازی انجام می‌شود.

یک تصویر دیجیتال از واحدهای کوچکی به نام پیکسل تشکیل شده است. سطح روشنایی هر پیکسل می‌تواند مقداری بین ۰ تا ۲۵۵ داشته باشد. این محدوده به‌صورت کد دودویی و در قالب هشت بیتی قابل نمایش می‌باشد. بنابراین با کمک گروه جایگشت S_8، می‌توان مقدار سطح روشنایی هر پیکسل تصویر را تغییر داد که به آن جایگشت در سطح بیت گویند. شکل (۳)، مثالی از جایگشت در سطح بیت را نشان می‌دهد.



شکل (۳): مثالی از جایگشت در سطح بیت

فرآیند انجام جایگشت در سطح بیت به‌صورت زیر می‌باشد:

۱) دریافت تصویر P_3 حاصل از مرحله انتشار و تبدیل آن به تصویر دودویی؛

۲) تولید تمام جایگشت‌های $I_8 = \{1,2,\dots,8\}c$ و ذخیره آن در ماتریسی به نام S_8 با اندازه ۸×۴۰۳۲۰. در واقع، هر سطر ماتریس S_8 بیانگر یک جایگشت می‌باشد؛

۳) محاسبه مقادیر اولیه x_0، y_0، z_0 و u_0 برای تابع فوق آشوب [۲۰] با رابطه (۹)؛

$$\begin{aligned} x_0 &= (k'_1 \oplus k'_2 \oplus \cdots \oplus k'_8) \,/\, 256 \\ y_0 &= (k'_9 \oplus k'_{10} \oplus \cdots \oplus k'_{16}) \,/\, 256 \\ z_0 &= (k'_{17} \oplus k'_{18} \oplus \cdots \oplus k'_{24}) \,/\, 256 \\ u_0 &= (k'_{25} \oplus k'_{26} \oplus \cdots \oplus k'_{32}) \,/\, 256 \end{aligned} \quad (۹)$$

۴) تولید دنباله تصادفی V با طول $M \times N$ به وسیله تابع فوق آشوب؛

۵) به‌دست آوردن دنباله اعداد صحیح D از ۰ تا ۴۰۳۲۰ با استفاده از رابطه (۱۰)؛

$$D_i = \lfloor V_i \times 40320 \rfloor \quad (۱۰)$$

۶) استفاده از اعداد تولید شده در مرحله ۵ به‌عنوان شاخص ماتریس S_8 برای انجام عمل جایگشت در سطح بیت و تولید تصویر P_4.

پس از انجام جایگشت در سطح بیت، به‌منظور بهبود امنیت بیشتر الگوریتم پیشنهادی، تبدیل در سطح بیت با کمک جعبه‌های جایگزینی S_8Sbox و عملگر XOR انجام می‌شود. فرآیند انجام تبدیل در سطح بیت به‌صورت زیر می‌باشد:

۱) دریافت تصویر دودویی P_4 حاصل از مرحله جایگشت در سطح بیت؛

۲) تولید S_8Sbox به‌صورت زیر:

a) تکرار 64 مرتبه تابع فوق آشوب و به‌دست آوردن بردار تصادفی V با طول ۲۵۶حاصل از الحاق x_iها، y_iها، z_iها و u_iها؛

b) انجام عمل مرتب‌سازی صعودی بردار V با استفاده از تابع $[f_V, l_V] = Sort(V)$، که بردار f_V شامل دنباله مرتب شده و l_V شامل مقادیر شاخص f_V؛

c) ساخت یک Sbox با اندازه ۱۶×۱۶ شامل ۲۵۶ مقدار متمایز از ۰ تا ۲۵۵ با تغییر آرایش بردار l_V به صورت یک ماتریس ۱۶×۱۶ و ذخیره آن به‌عنوان Sbox. شکل (۴) نمونه‌ای از Sbox تولید شده را نشان می‌دهد؛

d) تبدیل هر عنصر Sbox به معادل دودویی آن در قالب ۸ بیتی؛

e) اعمال هر جایگشت از S_8 به هر عنصر از Sbox؛

$$f: S_8 \times Sbox \rightarrow S_8Sbox$$

و تولید ۴۰۳۲۰ تا Sbox جدید و ذخیره آن در ماتریس سه‌بعدی S_8Sbox با اندازه ۱۶×۱۶×۴۰۳۲۰.

۳) تولید سه دنباله تصادفی U، V و W با طول $M \times N$ به وسیله تابع فوق آشوب [۲۰]؛

۴) به‌دست آوردن دنباله اعداد صحیح A از 0 تا 40320، B از ۰ تا ۱۶ و C از ۰ تا ۱۶ به وسیله رابطه (۱۱)؛

$$\begin{aligned} A_i &= \lfloor U_i \times 40320 \rfloor \\ B_i &= \lfloor V_i \times 16 \rfloor \\ C_i &= \lfloor W_i \times 16 \rfloor \end{aligned} \quad (۱۱)$$

۵) استفاده از اعداد تولید شده در مرحله ۴ به‌عنوان شاخص ماتریس سه‌بعدی S_8Sbox برای انجام عمل تبدیل در سطح بیت و تبدیل تصویر دودویی حاصل به تصویر دسیمال با رابطه (۱۲)؛

$$\begin{aligned} P_5 &= P_4 \oplus S_8Sbox\ (A, B, C) \\ P_6 &= Bin2Dec(P_5) \end{aligned} \quad (۱۲)$$

۶) ارسال تصویر P_6 به‌عنوان تصویر رمز شده به خروجی.

217	23	174	29	185	230	1	209	161	25	88	110	78	16	197	241
121	86	141	223	168	93	7	117	66	247	182	221	207	68	235	254
175	123	250	126	74	246	39	166	20	4	227	176	129	21	48	3
194	107	75	167	219	64	136	56	201	240	65	147	111	43	35	205
150	96	8	72	151	244	113	238	82	53	34	22	248	203	128	218
32	95	104	231	27	18	183	198	41	105	164	140	214	97	232	112
40	159	92	181	47	132	192	253	236	190	189	170	14	17	63	249
57	114	33	62	215	125	188	234	134	171	216	142	135	70	106	73
245	191	173	233	124	42	163	31	143	77	51	24	213	9	76	187
184	91	200	165	154	6	204	60	177	101	226	130	102	225	13	145
229	0	148	108	196	71	144	85	127	87	156	122	37	52	224	61
15	90	152	26	100	131	81	222	58	79	193	59	158	138	228	45
115	208	5	38	210	206	89	50	36	153	98	46	195	49	180	116
12	19	251	146	83	10	169	172	237	55	109	160	252	69	118	94
137	133	54	103	119	157	179	44	80	211	84	28	243	139	155	120
11	202	212	242	30	220	178	99	149	239	162	199	67	255	186	2

شکل (۴): نمونه Sbox تولید شده

شکل (۵) یک مثال از نحوه‌ی کارکرد الگوریتم رمزنگاری پیشنهادی برای یک تصویر با اندازه ۳×۳ را نشان می‌دهد.

۳-۴- الگوریتم رمزگشایی

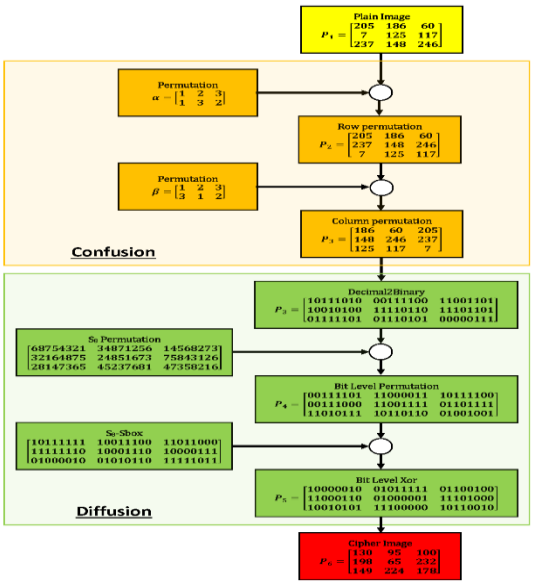
شکل (۶)، فرآیند رمزگشایی الگوریتم پیشنهادی را نشان می‌دهد که معکوس فرآیند رمزنگاری است. به عبارت دیگر با استفاده از نگاشت‌های آشوب مشابه، به‌کارگیری مقادیر اولیه یکسان برای آن و با انجام معکوس فرآیند رمزنگاری بر روی تصویر رمز شده، تصویر اصلی بازیابی خواهد شد.

۴- تحلیل امنیت و ارزیابی الگوریتم پیشنهادی

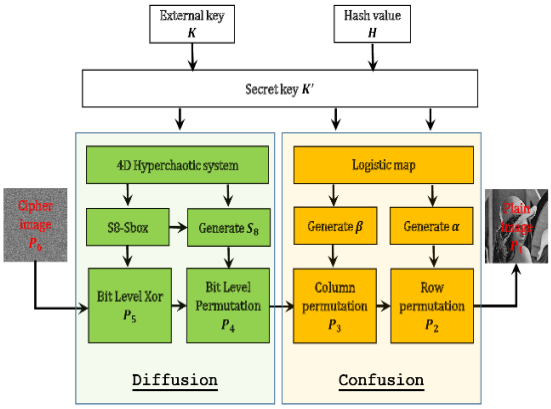
شکل (۷) نتایج حاصل از اجرای الگوریتم رمزنگاری پیشنهادی بر روی تصویرهای Lena، Peppers و Boat با اندازه ۲۵۶×۲۵۶ را نشان می‌دهد. تصاویر رمز شده شبیه به تصاویر نویزدار هستند به‌طوری که هیچ اطلاعات مفید در مورد تصویر اصلی را نمی‌توان از آن‌ها پیدا کرد.

یک الگوریتم رمزنگاری مناسب باید در برابر انواع حملات از جمله حملات کشف رمز، حملات آماری، حملات تفاضلی و غیره

از امنیت کافی برخوردار باشد. در ادامه، تعدادی آزمون و روش ارزیابی استاندارد برای بررسی امنیت و کارایی الگوریتم پیشنهادی بیان شده است.



شکل (۵): یک مثال از الگوریتم رمزنگاری پیشنهادی



شکل (۶): دیاگرام الگوریتم رمزگشایی تصویر پیشنهادی

۴-۱- تحلیل فضای کلید

اندازه فضای کلید، مجموع تمام کلیدهای مختلفی است که در الگوریتم رمزنگاری می‌توان استفاده کرد. از دیدگاه رمزنگاری، اندازه فضای کلید باید بزرگ‌تر از $2^{100} \approx 10^{30}$ باشد به‌طوری که الگوریتم رمزنگاری سطح امنیتی بالایی را تأمین کند. از آنجایی که الگوریتم پیشنهادی از یک کلید رمز خارجی ۲۵۶ بیتی استفاده می‌کند، بنابراین فضای کلید آن 2^{256} می‌باشد که بسیار بزرگ‌تر از 2^{100} است. همچنین، اگر سریع‌ترین رایانه، 2^{80} محاسبه را در هر ثانیه انجام دهد [۱۳]، آنگاه زمان لازم برای حمله جستجوی جامع برابر است با

$$\frac{2^{256}}{2^{80} \times 365 \times 24 \times 60 \times 60} \cong 3.0372 \times 10^{45}\ years$$

بنابراین، فضای کلید الگوریتم پیشنهادی به اندازه کافی بزرگ است که در برابر حمله جستجوی جامع از نظر محاسباتی مقاوم باشد.

۴-۲- تحلیل حساسیت به کلید

یکی از ویژگی‌های ضروری برای تضمین امنیت یک الگوریتم رمزنگاری قوی، حساسیت شدید نسبت به کلید رمز است. همان‌طور که در شکل (۸) نشان داده شده است، فقط با استفاده از کلید رمز صحیح key_1، تصویر رمز به درستی قابل رمزگشایی است و با تغییر حتی یک بیت در کلید رمز key_1، تصویر رمز قابل رمزگشایی نیست. بنابراین الگوریتم پیشنهادی حساسیت شدیدی نسبت به کلید رمز دارد.

۴-۳- تحلیل هیستوگرام

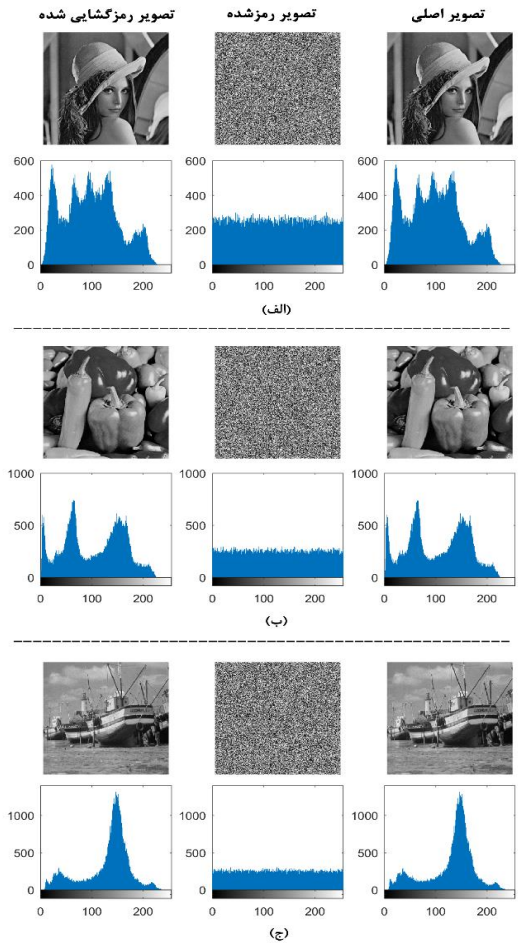
هیستوگرام یک تصویر، بیانگر فراوانی پیکسل‌ها برای هر مقدار شدت روشنایی می‌باشد. برای جلوگیری از حملات آماری، هیستوگرام تصویر رمز باید متفاوت از هیستوگرام تصویر اصلی و نسبتاً یکنواخت باشد. شکل (۷) هیستوگرام‌های تصاویر اصلی Lena، Peppers، Boat و تصاویر رمز شده مربوطه را نشان می‌دهد. نمودار هیستوگرام حاصل از تصویر رمز شده، به خوبی یکنواخت بوده و هیچ‌گونه اطلاعات مفیدی از آن قابل استخراج نیست، که این بیانگر کارایی بالای الگوریتم رمزنگاری پیشنهادی می‌باشد.

۴-۴- تحلیل ضرایب همبستگی

در یک تصویر دیجیتال، پیکسل‌های همجوار به هم وابسته هستند. یک الگوریتم رمزنگاری خوب باید همبستگی بین پیکسل‌های همجوار در راستای افقی، عمودی و قطری را کاهش دهد. هر چه همبستگی پیکسل‌های همجوار در تصویر رمز شده کمتر باشد، کارایی الگوریتم رمزنگاری مطلوب‌تر است. برای این منظور، به‌طور تصادفی ۱۰۰۰۰ جفت از پیکسل‌های مجاور در راستای افقی، عمودی و قطری از تصویر اصلی و تصویر رمز انتخاب شده و ضریب همبستگی آن‌ها از رابطه (۱۳) محاسبه گردید.

$$\begin{aligned} r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \\ E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \end{aligned} \qquad (۱۳)$$

که در آن، x و y مقادیر روشنایی دو پیکسل مجاور در تصویر، N تعداد پیکسل‌های مجاور می‌باشد. جدول (۱) نتایج حاصل از ضرایب همبستگی برای تصاویر اصلی Lena، Peppers، Boat و تصاویر رمز شده مربوطه را نشان می‌دهد. شکل (۹) نیز نتایج گرافیکی همبستگی برای تصاویر اصلی Lena و رمز شده را نشان می‌دهد. نتایج بیانگر کاهش بسیار شدید همبستگی بین جفت پیکسل‌های مجاور در راستای افقی، عمودی و قطری است.

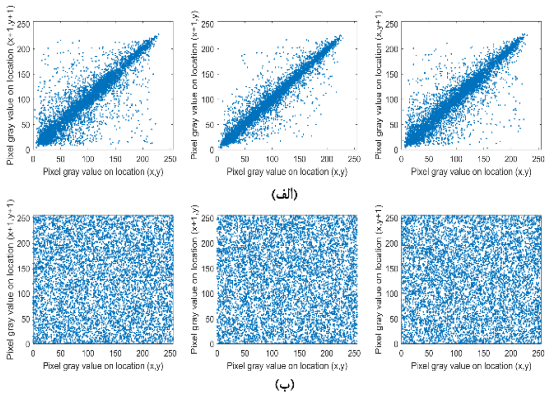


شکل (۷): نتایج اجرای الگوریتم پیشنهادی برای تصویرهای (الف) Lena، (ب) Peppers و (ج) Boat .

شکل (۸): تحلیل حساسیت به کلید. (الف) تصویر Lena، (ب) تصویر رمز با کلید key_1، (ج) تصویر رمزگشایی شده با کلید key_1 و (د) تصویر بازیابی شده با کلید key_2 متمایز با کلید key_1 در یک بیت

جدول (۱): ضرایب همبستگی پیکسل‌های مجاور در راستای افقی، عمودی و قطری با الگوریتم رمزنگاری تصویر پیشنهادی.

تصویر	افقی	عمودی	قطری
تصویر Lena	۰/۹۲۳۳	۰/۹۵۸۳	۰/۹۰۱۸
تصویر رمز Lena	۰/۰۰۳۴	-۰/۰۱۵۶	-۰/۰۱۰۷
تصویر Peppers	۰/۹۵۵۸	۰/۹۶۰۳	۰/۹۲۸۱
تصویر رمز Peppers	۰/۰۰۴۵	۰/۰۰۲۸	۰/۰۱۶۷
تصویر Boat	۰/۸۴۶۰	۰/۹۱۴۳	۰/۷۹۲۹
تصویر رمز Boat	۰/۰۳۶۴	۰/۰۱۹۴	-۰/۰۰۹۹



شکل (۹): همبستگی پیکسل‌های مجاور در راستای افقی، عمودی و قطری (الف) تصویر اصلی Lena و (ب) تصویر رمز شده Lena .

۴-۵- تحلیل آنتروپی

آنتروپی یک معیار مهم در تشخیص تصادفی بودن الگوریتم است که از رابطه (۱۴) محاسبه می‌شود.

$$H(s) = \sum_{i=0}^{2^N-1} p(s_i) \log_2 \frac{1}{p(s_i)} \qquad (۱۴)$$

که در آن، $p(s_i)$ احتمال وقوع سطح خاکستری s_i و 2^N تعداد سطوح خاکستری ممکن است. مقدار ایده‌آل آنتروپی در یک تصویر کاملاً یکنواخت با ۲۵۶ سطح خاکستری، برابر ۸ خواهد بود که به معنای وجود بیشترین بی‌نظمی در میان پیکسل‌های تصویر است. بنابراین، هر چه مقدار آنتروپی در یک الگوریتم به ۸ نزدیک‌تر باشد، الگوریتم رمزنگاری تصادفی‌تر و دارای امنیت بالاتری است. در جدول (۲) مقادیر آنتروپی نشان داده شده است.

جدول (۲): مقادیر آنتروپی

تصویر استاندارد	آنتروپی تصویر اصلی	آنتروپی تصویر رمز شده
Lena	۷/۵۸۹۶	۷/۹۹۷۴
Peppers	۷/۵۶۹۷	۷/۹۹۷۲
Boat	۷/۱۹۵۷	۷/۹۹۷۲

۴-۶- آزمون شبه تصادفی بودن

به‌منظور ارزیابی امنیت سامانه‌های رمزنگاری تصویر، آزمون‌های آماری بسیاری وجود دارد. آزمون آماری NIST SP 800-22 یک مجموعه آزمون آماری به‌منظور ارزیابی تصادفی بودن دنباله دودویی تولید شده حاصل از مولدهای اعداد تصادفی، وارسی دنباله کلید مورد استفاده در سامانه رمزنگاری و نیز تصویر رمز شده تولید شده به وسیله الگوریتم رمزنگاری است [۲۳].

آزمون NIST SP 800-22 برای یافتن الگوی معین در خروجی سامانه رمزنگاری، نیاز به یک دنباله دودویی با حداقل 10^6 بیت دارد [۱۵]. نتیجه این آزمون با P- مقدار بیان شده است. اگر P- مقدار محاسبه شده بزرگ‌تر از ۰/۰۱ باشد، دنباله تصادفی و بیانگر موفقیت آمیز بودن آزمون می‌باشد. جدول (۳) نتایج ارزیابی آزمون آماری NIST بر روی تصویر رمز شده Lena را نشان می‌دهد. دنباله‌های دودویی ایجاد شده توسط الگوریتم پیشنهادی با موفقیت تمام آزمایش‌های NIST پشت سر گذاشته است.

۴-۷- تمایز تصویر اصلی و تصویر رمز شده

یک الگوریتم رمزنگاری امن باید حساسیت شدید نسبت به تغییرات جزئی در تصویر اصلی داشته باشد. در حملات تفاضلی، فرد مهاجم تلاش می‌کند با ایجاد یک تغییر بسیار کوچک در تصویر اصلی و مشاهده تغییرات حاصل در تصویر رمز شده، ارتباط معناداری بین تصویر اصلی و تصویر رمز پیدا نماید. اگر یک تغییر بسیار کوچک در تصویر اصلی موجب تغییرات چشمگیری در تصویر رمز شده گردد، آنگاه الگوریتم در مقابل حملات تفاضلی مقاوم خواهد بود. دو معیار مهم در تحلیل حملات تفاضلی NPCR (نرخ پیکسل‌های تغییر یافته در تصویر رمز شده به ازای یک بیت تغییر در تصویر اصلی) و UACI (متوسط اختلاف شدت سطح روشنایی دو تصویر رمز شده) می‌باشند که از رابطه (۱۵) محاسبه می‌شود:

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \qquad (۱۵)$$

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

جدول (۳): نتایج آزمون NIST برای تصویر رمز شده Lena

نام آزمون		P-مقدار	نتیجه
Frequency		۰/۴۴۹۶	قبول
Block Frequency		۰/۲۲۵۵	قبول
Run		۰/۶۷۰۵	قبول
Longest Run of Ones		۰/۱۹۵	قبول
Rank		۰/۳۷۰۵	قبول
Spectral DFT		۰/۸۹۷۷	قبول
Non-Overlapping Template		۰/۸۰۶۸	قبول
Overlapping Template		۰/۱۴۰۱	قبول
Universal		۰/۸۱۰۹	قبول
Linear Complexity		۰/۲۹۳۴	قبول
Serial	مقدار اول p	۰/۳۰۴۰	قبول
Serial	مقدار دوم p	۰/۸۵۹۳	قبول
Approximate Entropy		۰/۰۴۲۲	قبول
Cummulative Sums (Forward)		۰/۵۷۰۹	قبول
Cummulative Sums (Reverse)		۰/۸۰۳۹	قبول
Random Excursions	x = -4	۰/۵۰۳۵	قبول
	x = -3	۰/۸۷۷۸	قبول
	x = -2	۰/۹۳۰۴	قبول
	x = -1	۰/۶۵۰۳	قبول
	x = 1	۰/۶۶۹۱	قبول
	x = 2	۰/۱۰۳۱	قبول
	x = 3	۰/۶۵۰۳	قبول
	x = 4	۰/۸۰۶۰	قبول
Random Excursions Variant	x = -9	۰/۳۰۶۳	قبول
	x = -8	۰/۳۶۱۳	قبول
	x = -7	۰/۳۹۹۳	قبول
	x = -6	۰/۳۴۹۸	قبول
	x = -5	۰/۳۲۱۰	قبول
	x = -4	۰/۵۴۲۲	قبول
	x = -3	۰/۸۸۹۷	قبول
	x = -2	۰/۷۷۴۵	قبول
	x = -1	۰/۷۰۹۸	قبول
	x = 1	۰/۱۹۲۷	قبول
	x = 2	۰/۳۳۳۶	قبول
	x = 3	۰/۲۲۲۳	قبول
	x = 4	۰/۱۷۳۹	قبول
	x = 5	۰/۲۹۱۷	قبول
	x = 6	۰/۳۱۲۶	قبول
	x = 7	۰/۲۳۵۲	قبول
	x = 8	۰/۱۹۴۶	قبول
	x = 9	۰/۲۹۲۳	قبول
مقادیر نتایج بالاتر از ۰/۰۱ بر موفقیت آمیز بودن آزمون دلالت دارد.			

به‌طوری که H و W به ترتیب طول و عرض تصاویر، C_1 و C_2 تصاویر رمز شده قبل و بعد از تغییر دادن یک پیکسل از تصویر اصلی می‌باشد. مقادیر مورد انتظار NPCR و UACI به ترتیب ۹۹/۶۰۹۴ و ۳۳/۴۶۳۵ می‌باشد. نتایج حاصل از مقادیر NPCR و UACI برای تصاویر اصلی Lena، Peppers و Boat در جدول (۴) نشان می‌دهد یک تغییر بسیار کوچک در تصویر اصلی موجب تغییرات چشمگیری در تصویر رمز شده است.

جدول (۴): مقادیر NPCR و UACI.

تصویر استاندارد	NPCR	UACI
Lena	۹۹/۶۲۱۶	۳۳/۴۸۱۵
Peppers	۹۹/۶۰۹۴	۳۳/۶۲۰۶
Boat	۹۹/۶۱۵۴	۳۳/۵۴۱۳

۴-۸- تحلیل حملات برش و حملات نویزی

یک الگوریتم رمزنگاری خوب باید در مقابل حملات برش (حذف بخشی از اطلاعات تصویر رمز شده) و حملات نویز (تغییر برخی از مقادیر شدت پیکسل‌های تصویر رمز شده) مقاوم باشد. نسبت پیک سیگنال به نویز (PSNR) بین تصویر اصلی و تصویر رمزگشایی شده به‌عنوان معیاری برای تحلیل مقاومت الگوریتم در حملات برش و نویز در نظر گرفته می‌شود و از رابطه (۱۶) محاسبه می‌شود.

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\big(P(i,j)-D(i,j)\big)^2$$
$$PSNR = 10\times\log\frac{MAX_P^2}{MSE} \qquad (16)$$

به‌طوری که M و N به ترتیب طول و عرض تصاویر، P و D تصویر اصلی و تصویر رمزگشایی شده و MAX_P^2 مربع حداکثر مقدار پیکسل‌های تصویر می‌باشد. نتایج حاصل از جدول (۵) و شکل (۱۰) برای حمله برش و جدول (۶) و شکل (۱۱) برای حمله نویز، بیانگر مقاومت خوب الگوریتم پیشنهادی در برابر حملات برش و نویز است.

۴-۹- تحلیل اجرایی

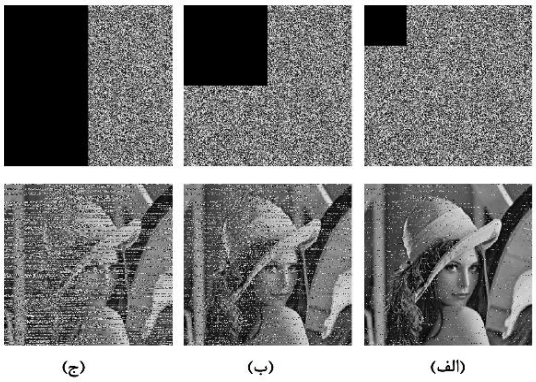
مستقل از ملاحظات امنیتی، یک سامانه رمزنگاری به‌منظور استفاده در پردازش‌های بلادرنگ باید از لحاظ زمان اجرای ارزیابی شود. زمان اجرای فرآیند رمزنگاری و رمزگشایی به فاکتورهای مختلفی همانند ساختار پردازنده، اندازه حافظه، سامانه عامل، زبان برنامه‌نویسی و غیره وابسته است [۲۴]. الگوریتم رمزنگاری پیشنهادی با استفاده MATLAB بر روی ماشینی با پردازنده Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz و حافظه 16 گیگا بایت اجرا گردید. به‌منظور افزایش دقت در محاسبه زمان اجرا، الگوریتم پیشنهادی بر روی چندین تصویر با اندازه‌های مختلف ۱۰ مرتبه اجرا و میانگین زمان اجرای بر حسب ثانیه در جدول (۷) ارائه شد.

۴-۱۰- مقایسه الگوریتم پیشنهادی با سایر الگوریتم‌ها

جدول (۸) خلاصه نتایج مقایسه الگوریتم رمزنگاری پیشنهادی با الگوریتم‌های موجود در مراجع [۹، ۱۰، ۱۳، ۱۶] از لحاظ آنتروپی، ضریب همبستگی، حملات تفاضلی، برش و نویز و همچنین زمان اجرای را نشان می‌دهد.

جدول (۵): نتایج حمله برش

تصویر استاندارد	نرخ برش		
	۱/۱۶	۱/۴	۱/۲
Lena	۲۰/۸۳۲۸	۱۴/۶۹۸۰	۱۱/۵۷۴۴
Peppers	۲۰/۴۹۹۷	۱۴/۶۲۴۳	۱۱/۵۱۱۳
Boat	۲۱/۴۵۶۳	۱۵/۲۶۱۵	۱۲/۲۹۱۰



(الف) (ب) (ج)

شکل (۱۰): حمله برش با نرخ (الف) ۱/۱۶، (ب) ۱/۴ و (ج) ۱/۲

جدول (۶): نتایج حمله نویز

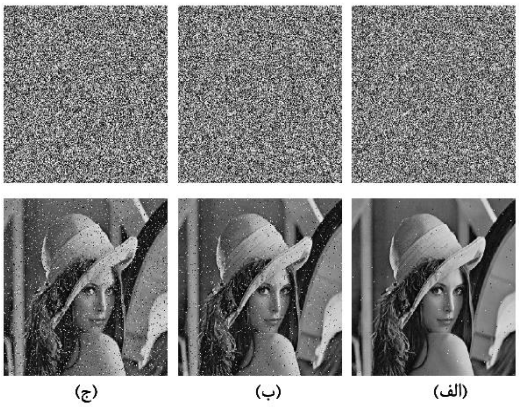
تصویر استاندارد	چگالی نویز فلفل و نمک		
	۰/۰۰۵	۰/۰۵	۰/۱
Lena	۳۱/۵۲۰۳	۲۱/۵۰۹۹	۱۸/۶۳۱۲
Peppers	۳۱/۷۶۵۸	۲۱/۵۰۶۷	۱۸/۳۷۶۷
Boat	۳۲/۸۷۳۹	۲۲/۴۷۰۵	۱۹/۳۷۰۶

جدول (۷): زمان اجرای الگوریتم پیشنهادی به ثانیه

اندازه تصویر	تصویر استاندارد	زمان رمزنگاری	زمان رمزگشایی
۲۵۶×۲۵۶	Lena	۰/۵۱۹۷	۰/۴۹۲۱
	Peppers	۰/۵۱۲۸	۰/۴۸۹۴
	Boat	۰/۵۱۸۳	۰/۴۹۳۴
۵۱۲×۵۱۲	Lena	۱/۰۱۰۸	۱/۰۰۷۳
	Peppers	۱/۰۳۵۴	۱/۰۲۴۰
	Boat	۱/۰۴۶۷	۱/۰۳۸۳
۱۰۲۴×۱۰۲۴	Lena	۳/۷۳۳۴	۳/۶۸۷۷
	Peppers	۳/۶۷۰۱	۳/۶۵۹۰
	Boat	۳/۶۶۲۶	۳/۶۵۱۳

جدول (۸): نتایج مقایسه الگوریتم پیشنهادی با چند الگوریتم دیگر

تصویر اندازه	معیار		الگوریتم					
			[۹] SPK[1]	[۹] SPK[5]	[۱۰] Yue	[۱۳] Murugan	[۱۶] Farajollah	Our
Lena ۲۵۶×۲۵۶	آنتروپی		۷/۹۹۷۰	۷/۹۹۷۱	۷/۹۹۶۹	۷/۹۹۷۱	۷/۹۹۷۲	۷/۹۹۷۴
	ضریب همبستگی	افقی	-۰/۰۱۴۳	۰/۰۰۳۸	۰/۰۱۷۰	-۰/۰۲۶۶	-۰/۰۰۴۷	۰/۰۰۳۴
		عمودی	۰/۰۰۷۴	-۰/۰۰۱۵	۰/۰۱۱۶	۰/۰۰۵۵	۰/۰۰۱۲	-۰/۰۱۵۶
		قطری	-۰/۰۳۰۰	-۰/۰۰۴۳	-۰/۰۲۶۵	۰/۰۰۰۸	۰/۰۰۷۶	-۰/۰۱۰۷
	حمله تفاضلی	NPCR	۰/۰۰۱۵	۰/۰۰۱۵	۹۹/۵۸۳۴	۹۹/۶۰۶۳	۹۹/۶۲۳۷	۹۹/۶۲۱۶
		UACI	۰/۰۰۰۹	۰/۰۰۱۱	۳۳/۲۳۶۰	۳۳/۵۱۵۳	۳۳/۴۱۳۰	۳۳/۴۸۱۵
	PSNR حمله برش با نرخ برش	۱/۱۶	۲۰/۵۹۰۵	۲۰/۵۶۳۷	۸/۵۷۳۹	۲۰/۶۰۴۷	۲۰/۶۱۴۸	۲۰/۸۳۲۸
		۱/۴	۱۴/۵۰۵۴	۱۴/۵۶۱۲	۸/۵۶۱۱	۱۴/۵۹۵۱	۱۴/۵۹۰۴	۱۴/۶۹۸۰
		۱/۲	۱۱/۵۱۰۲	۱۱/۵۵۹۶	۸/۵۶۲۰	۱۱/۵۷۸۱	۱۱/۵۶۲۲	۱۱/۵۷۴۴
	PSNR حمله نویز با چگالی	۰/۰۰۵	۳۱/۱۹۶۵	۳۲/۳۴۶۵	۸/۵۶۸۲	۳۱/۵۵۷۷	۳۱/۷۳۵۶	۳۱/۵۲۰۳
		۰/۰۵	۲۱/۳۳۷۶	۲۱/۴۷۶۵	۸/۵۸۵۱	۲۱/۷۰۶۷	۲۱/۵۰۵۸	۲۱/۵۰۹۹
		۰/۱	۱۸/۴۶۹۴	۱۸/۶۲۶۷	۸/۵۶۳۹	۱۸/۵۳۵	۱۸/۶۳۰۴	۱۸/۶۳۱۲
	زمان اجرا (ثانیه)	رمزنگاری	۰/۱۱۴۴	۰/۵۷۴۳	۱۰/۳۲۷۸	۲/۵۹۰۹	۰/۸۸۷۵	۰/۵۱۹۷
		رمزگشایی	۰/۱۲۰۶	۰/۵۶۸۷	۱۰/۴۴۴۳	۱/۵۴۳۵	۰/۸۲۱۲	۰/۴۹۲۱
Lena ۵۱۲×۵۱۲	آنتروپی		۷/۹۹۹۱	۷/۹۹۹۲	۷/۹۹۹۳	۷/۹۹۹۳	۷/۹۹۹۲	۷/۹۹۹۳
	ضریب همبستگی	افقی	۰/۰۲۶۲	۰/۰۰۶۸	۰/۰۱۴۷	-۰/۰۰۷۵	-۰/۰۰۱۴	۰/۰۰۱۰
		عمودی	-۰/۰۰۶۰	-۰/۰۲۰۰	۰/۰۱۴۲	-۰/۰۰۹۱	۰/۰۱۸۴	۰/۰۰۶۴
		قطری	۰/۰۱۸۴	۰/۰۰۳۲	-۰/۰۰۵۱	۰/۰۱۶۴	۰/۰۰۳۰	۰/۰۱۰۲
	حمله تفاضلی	NPCR	۰/۰۰۰۴	۰/۰۰۰۴	۹۹/۶۱۸۹	۹۹/۶۰۶۷	۹۹/۵۸۶۱	۹۹/۶۰۱۷
		UACI	۰/۰۰۰۲	۰/۰۰۰۲	۳۳/۵۳۹۷	۳۳/۴۳۷۳	۳۳/۳۷۹۰	۳۳/۴۳۴۷
	PSNR حمله برش با نرخ برش	۱/۱۶	۲۰/۴۷۷۲	۲۰/۵۸۴۱	۸/۵۶۹۱	۲۰/۵۸۰۷	۲۰/۵۷۴۹	۲۰/۷۴۹۴
		۱/۴	۱۴/۴۵۳۸	۱۴/۵۷۷۱	۸/۵۷۴۷	۱۴/۵۸۴۴	۱۴/۵۳۸۸	۱۴/۶۶۳۸
		۱/۲	۱۱/۴۸۰۱	۱۱/۵۶۳۶	۸/۵۵۶۷	۱۱/۵۷۰۸	۱۱/۵۲۳۸	۱۱/۶۲۵۵
	PSNR حمله نویز با چگالی	۰/۰۰۵	۳۱/۰۷۶۷	۳۱/۶۳۶۰	۸/۵۵۳۴	۳۱/۶۳۶۰	۳۱/۵۴۹۰	۳۱/۷۹۲۳
		۰/۰۵	۲۱/۴۷۳۷	۲۱/۵۰۴۶	۸/۵۶۳۸	۲۱/۶۶۹۵	۲۱/۵۴۳۹	۲۱/۶۴۶۶
		۰/۱	۱۸/۳۵۱۸	۱۸/۳۹۴۷	۸/۵۷۵۱	۱۸/۵۷۰۹	۱۸/۵۹۰۴	۱۸/۵۹۲۳
	زمان اجرا (ثانیه)	رمزنگاری	۰/۴۳۵۶	۲/۱۱۶۹	۴۷/۷۹۷۲	۷/۳۷۲۷	۳/۲۷۰۹	۱/۰۱۰۸
		رمزگشایی	۰/۴۲۰۳	۲/۱۰۷۸	۴۶/۰۵۹۴	۶/۳۸۵۱	۳/۱۳۶۰	۱/۰۰۷۳
Lena ۱۰۲۴×۱۰۲۴	آنتروپی		۷/۹۹۹۵	۷/۹۹۹۸	۷/۹۹۹۸	۷/۹۹۹۸	۷/۹۹۹۸	۷/۹۹۹۸
	ضریب همبستگی	افقی	-۰/۰۰۷۸	۰/۰۰۵۵	۰/۰۱۱۵	۰/۰۰۰۲	۰/۰۱۰۹	-۰/۰۰۷۵
		عمودی	۰/۰۰۵۱	۰/۰۰۳۲	-۰/۰۰۴۴	۰/۰۱۲۰	۰/۰۲۰۱	۰/۰۰۵۳
		قطری	۰/۰۰۵۲	۰/۰۰۵۲	۰/۰۰۷۲	-۰/۰۰۸۵	-۰/۰۰۳۶	-۰/۰۱۰۸
	حمله تفاضلی	NPCR	۰/۰۰۰۱	۰/۰۰۰۱	۹۹/۶۰۱۹	۹۹/۶۱۵۵	۹۹/۵۹۹۰	۹۹/۶۱۵۴
		UACI	۰/۰۰۰۱	۰/۰۰۰۱	۳۳/۴۵۴۲	۳۳/۴۶۸۳	۳۳/۴۴۵۴	۳۳/۵۰۰۷
	PSNR حمله برش با نرخ برش	۱/۱۶	۲۰/۵۱۳۵	۲۰/۶۰۰۹	۸/۵۶۳۵	۲۰/۶۴۱۴	۲۰/۶۰۸۱	۲۰/۶۱۰۹
		۱/۴	۱۴/۴۵۶۳	۱۴/۵۷۸۱	۸/۵۶۴۰	۱۴/۶۱۳۱	۱۴/۵۷۵۱	۱۴/۵۹۷۲
		۱/۲	۱۱/۴۷۰۸	۱۱/۵۷۴۳	۸/۵۶۴۵	۱۱/۵۸۶۰	۱۱/۵۶۳۰	۱۱/۶۱۵۲
	PSNR حمله نویز با چگالی	۰/۰۰۵	۳۱/۴۹۷۶	۳۱/۵۲۷۸	۸/۵۸۴۳	۳۱/۶۸۷۳	۳۱/۶۷۵۷	۳۱/۳۱۰۸
		۰/۰۵	۲۱/۴۵۰۴	۲۱/۵۷۳۴	۸/۵۵۳۷	۲۱/۵۹۱۹	۲۱/۵۹۳۰	۲۱/۵۳۴۶
		۰/۱	۱۸/۴۴۶۹	۱۸/۵۱۴۴	۸/۵۶۲۰	۱۸/۵۷۷۷	۱۸/۵۶۳۰	۱۸/۵۴۷۴
	زمان اجرا (ثانیه)	رمزنگاری	۲/۳۷۷۸	۱۱/۹۲۰۷	۲۰۷/۱۶۵۸	۱۲۷/۶۳۳۳	۱۳/۴۰۸۴	۳/۷۳۳۴
		رمزگشایی	۲/۴۱۷۹	۱۲/۱۴۵۲	۲۱۳/۰۶۲۶	۱۱۵/۱۴۴۹	۱۳/۲۶۰۷	۳/۶۸۷۷



شکل (۱۱): حمله نویز با چگالی (الف) ۰/۰۰۵، (ب) ۰/۰۵ و (ج) ۰/۱

الگوریتم پیشنهادی و الگوریتم‌های مراجع [۹، ۱۰، ۱۳، ۱۶] مقادیر قابل قبولی از لحاظ آنتروپی و ضریب همبستگی دارند.

از لحاظ حساسیت تصویر رمز شده به تغییرات جزئی در تصویر اصلی (NPCR و UACI)، الگوریتم مرجع [۹] به اندازه کافی حساس نیست، زیر تغییر یک پیکسل تصویر اصلی، تأثیری در دیگر پیکسل‌ها ندارد. الگوریتم پیشنهادی و الگوریتم‌های مراجع [۱۰، ۱۳، ۱۶] حساسیت قابل توجهی به تغییرات جزئی در تصویر اصلی دارند.

الگوریتم پیشنهادی و الگوریتم‌های مراجع [۹، ۱۳، ۱۶] بر خلاف الگوریتم مرجع [۱۰] مقامت بالایی در برابر حملات برش و نویز دارند.

به‌منظور مقایسه زمان اجرا، تمام الگوریتم‌ها با استفاده MATLAB بر روی یک ماشین یکسان برای چندین تصویر با اندازه‌های مختلف، ۱۰ مرتبه اجرا و میانگین زمان اجرای فرآیند رمزنگاری و رمزگشایی بر حسب ثانیه محاسبه شد. نتایج بیانگر این است که با بزرگ شدن اندازه تصویر، الگوریتم پیشنهادی زمان اجرای کمتری در مقایسه با الگوریتم‌های مراجع [۹، ۱۰، ۱۳، ۱۶] دارد.

به‌طور کلی با در نظر گرفتن تمام معیارهای آنتروپی، ضریب همبستگی، حملات تفاضلی، برش و نویز و نیز زمان اجرای، الگوریتم پیشنهادی عملکر قابل قبولی داشته و به نتایج رضایت بخشی دست یافته است.

۵- نتیجه‌گیری

در این مقاله، یک الگوریتم رمزنگاری تصویر با استفاده از گروه جایگشت S_n و توابع آشوب ارائه گردید. برای اثبات کارایی الگوریتم پیشنهادی، آنالیز امنیت و کارایی آن از لحاظ تحلیل فضای کلید، تحلیل حساسیت نسبت کلید، تحلیل هیستوگرام، تحلیل همبستگی، تحلیل آنتروپی، حملات تفاضلی، برش و نویز مورد بررسی قرار گرفت.

با توجه به تحلیل فضای کلید و تحلیل حساسیت به کلید، الگوریتم رمزنگاری تصویر پیشنهادی نه تنها فضای کلید به اندازه کافی بزرگ دارد که نسبت به حمله جستجوی جامع از نظر محاسباتی مقاوم است، بلکه حساسیت شدیدی به کوچک‌ترین تغییر در کلید رمز دارد.

نتایج تحلیل هیستوگرام نشان داد که هیستوگرام حاصل از تصویر رمز، به خوبی یکنواخت بوده و هیچگونه اطلاعات مفیدی از آن قابل استخراج نیست. همچنین نتایج تحلیل همبستگی نشان داد که مقادیر ضرایب همبستگی بین پیکسل‌های همسایه در راستای افقی، عمودی و قطری بعد از عمل رمزنگاری به‌طور قابل ملاحظه‌ای کاهش یافته و به مقدار صفر نزدیک می‌باشند.

نتایج آزمون تصادفی بودن نشان داد که دنباله‌های دودویی ایجاد شده توسط الگوریتم پیشنهادی تمام آزمون‌های NIST را با موفقیت می‌گذراند.

در آزمایش سنجش میزان تمایز بین تصور اصلی و تصویر رمز، مقادیر $NPCR >$ ٪۹۹/۶۰ و $UACI <$ ٪۳۳/۴۰ نشان داد که الگوریتم پیشنهادی حساسیت شدیدی به کوچک‌ترین تغییر در تصویر اصلی دارد، بنابراین در مقابل حملات تفاضلی مقاوم می‌باشد. همچنین مقدار آنتروپی محاسبه شده در الگوریتم پیشنهادی بزرگ‌تر از ۷/۹۹ بود که نزدیک به مقدار آنتروپی ایده‌آل ۸ می‌باشد.

الگوریتم رمزنگاری پیشنهادی در برابر حملات برش و نویز مقاوم بوده و همچنین از لحاظ زمان اجرا، عملکر قابل قبولی دارد.

۶- مراجع

[1] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image Encryption Algorithm Based on Multiple Mixed Hash Functions and Cyclic Shift," OPT. LASER ENG., vol. 107, pp. 370-379, 2018.

[2] Q. Zhang, L. Guo, and X. Wei, "A Novel Image Fusion Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System," OPTIK, vol. 124, no. 18, pp. 3596-3600, 2013.

[3] M. Ahmadipari and M. Moradi, "A New Approach for Grayscale Image Encryption Using Beness Interconnection Networks and Logistic Map Chaos Function," Electronic and Cyber Defense, vol. 6, no. 1, pp. 37-46, 2017. (In Persian)

[4] M. Khan and T. Shah, "A Novel Image Encryption Technique Based on Hénon Chaotic Map and S_8 Symmetric Group," Neural Comput. Appl., vol. 25, no. 7-8, pp. 1717-1722, 2014.

[5] P. K. Sharma, M. Ahmad, and P. M. Khan, "Cryptanalysis of Image Encryption Algorithm Based on Pixel Shuffling and Chaotic S-box Transformation," In Int. Symposium on Security in Computing and Communication, Springer, pp. 173-181, 2014.

[6] S. Xu, Y. Wang, Y. Guo, and C. Wang, "A Novel Image Encryption Scheme Based on a Nonlinear Chaotic Map," IJIGSP, vol. 2, no. 1, p. 61, 2010.

[7] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadipour, "A Novel Parallel Image Encryption with Chaotic Windows Based on Logistic Map," Comput. Electr. Eng., vol. 62, pp. 384-400, 2017.

[8] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based Chaotic System for Image Encryption," Inform. Sciences, vol. 480, pp. 403-419, 2019.

[9] A. Mirghadri and A. Jolfaei, "A Novel Image Encryption Scheme Using Chaotic Maps," J. of Passive Defence Science and Technology, 2011. (In Persian)

[10] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image Encryption Using the Two-dimensional Logistic Chaotic Map," J. Electron. Imaging, vol. 21, no. 1, p. 013014, 2012.

[11] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A Novel Image Encryption Based on Row-Column, Masking and Main Diffusion Processes with Hyper Chaos," Multimed. Tools Appl., vol. 74, no. 3, pp. 781-811, 2015.

[12] S. El Assad and M. Farajallah, "A New Chaos-based Image Encryption System," Signal Process-Image, vol. 41, pp. 144-157, 2016.

[13] B. Murugan and A. G. N. Gounder, "Image Encryption Scheme Based on Block-based Confusion and Multiple Levels of Diffusion," IET. COMPUT. VIS., vol. 10, no. 6, pp. 593-602, 2016.

[14] A. Belazi, M. Khan, A. El-Latif, and S. Belghith, "Efficient Cryptosystem Approaches: S-boxes and Permutation–substitution-based Encryption," Nonlinear Dynam., vol. 87, no. 1, pp. 337-361, 2017.

[15] B. Mondal, P. Kumar, and S. Singh, "A Chaotic Permutation and Diffusion Based Image Encryption Algorithm for Secure Communications," Multimed. Tools Appl., vol. 77, no. 23, pp. 31177-31198, 2018.

[16] A. Farajollahzadeh and F. Motiei, "Image Encryption Based Using Three-dimensional Logistic Chaotic Map," 5th Int. Conf. on Electrical and Computer Engineering, 2018. (In Persian)

[17] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "Construction of S8 Liu J S-boxes and their Applications," Comput. Math Appl., vol. 64, no. 8, pp. 2450-2458, 2012.

[18] F. Özkaynak, V. Çelik, and A. B. Özer, "A New S-box Construction Method Based on the Fractional-order Chaotic Chen System," Signal Image Video P, vol. 11, no. 4, pp. 659-664, 2017.

[19] X. Wang and C. Liu, "A Novel and Effective Image Encryption Algorithm Based on Chaos and DNA Encoding," Multimed. Tools Appl., vol. 76, no. 5, pp. 6229-6245, 2017.

[20] J. Ma, Z. Chen, Z. Wang, and Q. Zhang, "A Four-wing hyper-Chaotic Attractor Generated from a 4-D Memristive System with a Line Equilibrium," Nonlinear Dynam., vol. 81, no. 3, pp. 1275-1288, 2015.

[21] F. ul Islam and G. Liu, "Designing S-box Based on 4D-4wing Hyperchaotic System," 3D Res, vol. 8, no. 1, p. 9, 2017.

[22] T. W. Hungerford, "Abstract Algebra: An Introduction," Cengage Learning, 2012.

[23] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Booz-Allen and Hamilton Inc. Mclean Va, 2001.

[24] P. Ping, F. Xu, Y. Mao, and Z. Wang, "Designing Permutation–substitution Image Encryption Networks with Henon Map," Neurocomputing, vol. 283, pp. 53-63, 2018.

Journal of Electronical & Cyber Defence
Vol. 8, No. 3, 2020, Serial No. 31

An Image Encryption Algorithm Based on the Sn Permutation Group and Chaotic Functions

E. Zarei Zefreh*
Department of Computer Science, University of Khansar, Khansar, Iran
(Received: 15/11/2019, Accepted: 01/02/2020)

ABSTRACT

In this paper, an image encryption algorithm is proposed based on the Sn permutation group and chaotic functions. The proposed algorithm consists of three steps. In the first step, by applying the hash functions to the plain image information and using the 256-bit external key, a 256-bit secret key is extracted and used to calculate the initial values and parameters of the chaotic functions. In the second step known as the confusion step, the pixel positions of the plain image are rearranged using a row and column level permutation based on the chaotic functions, such that the correlation between adjacent pixels of the plain image is significantly reduced. In the third step or the diffusion step, the gray value of each pixel is changed based on a bit level permutation using the S8 permutation group and the chaotic functions. Finally, by applying the bit level transform using the S8Sbox and XOR operation, the security of the proposed image encryption algorithm is increased. The experimental results and security analysis show that the NPCR is , the UACI is , entropy is and the correlation coefficients of the encrypted images are close to 0. Also, the proposed image encryption algorithm has high resistance against common attacks such as the exhaustive search, cropping and noise attacks.

Keywords: Image Encryption, Permutation Group, Chaotic Functions, S-box, Confusion, Diffusion.

* Corresponding Author Email: zarei@khansar-cmc.ac.ir