دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۲ (۲۴-۳۳)
https://monadi.isc.org.ir

ارائه‌شده در بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه تربیت مدرس و پژوهشگاه ارتباطات و فناوری اطلاعات، ۲۵ و ۲۶ مهرماه ۱۴۰۳

رمزنگاری تصویر IEPS: رمزنگاری بر مبنا نگاشت آشوبی PWLCM و تابع چکیده‌ساز SHA-512★

سید حسام‌الدین هاشمی و محمدحسن مجیدی*

گروه مهندسی مخابرات، دانشکده مهندسی برق و کامپیوتر، دانشگاه بیرجند، بیرجند، ایران

اطلاعات مقاله

کلمات کلیدی:
رمزنگاری آشوبی تصویر
رمزنگاری تصویر IEPS
نگاشت آشوبی PWLCM
تابع چکیده‌ساز SHA-512

نوع مقاله: پژوهشی

چکیده

با رشد روزافزون اینترنت و گسترش ابزار تصویر برداری، بخش عظیمی از اطلاعاتی که با آن سر و کار داریم را تصاویر دیجیتال تشکیل داده‌اند. گاها این تصاویر حاوی اطلاعات سرّی می‌باشد که برای حفظ امنیت این اطلاعات می‌توان از سیستم‌های رمزنگاری تصویر استفاده کرد. این مقاله یک روش رمزنگاری تصویر آشوبی معرفی کرده است که می‌تواند به خوبی از اطلاعات موجود در تصویر محافظت کند. سیستم رمزنگاری IEPS یک طرح رمزنگاری تصویر بر مبنا نگاشت آشوبی PWLCM و تابع چکیده‌ساز SHA-512 می‌باشد. این طرح شامل دو عملیات جابجایی و جایگزینی در پیکسل‌های تصویر می‌باشد. در مرحله جابجایی از نگاشت آشوبی PWLCM استفاده شده است و برای جایگزینی پیکسل‌ها از ویژگی‌های تابع چکیده‌ساز SHA-512 بهره‌برداری شده است. نتایج آزمایش نشان داد، الگوریتم رمزنگاری PWLCM به خوبی می‌تواند اطلاعات درون تصویر را از رمز کند و عملکرد مناسبی در برابر تحلیل‌های مختلف از قبیل معیار آنتروپی، معیار هیستوگرام، معیار حساسیت به کلید، مقاومت در برابر حملات تفاضلی از خود نشان داده است.

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

امروزه تصاویر دیجیتال به دلیل توسعه اینترنت و ابزار ضبط و ویرایش آنها بسیار مورد توجه قرارگرفته‌اند [۱]. حفظ امنیت برخی از این تصاویر به دلیل وجود اطلاعات سری بسیار مهم می‌باشد [۲]. رمزنگاری تصویر یک راهکار مناسب جهت حفظ امنیت تصاویر می‌باشد. همبستگی زیاد اطلاعات میان پیکسل‌های مجاور در تصاویر دیجیتال باعث شده است، استفاده از روش‌های مرسوم رمزنگاری مانند AES [۱] و DES [۲] به طور معمول ناکارآمد باشد [۳]. از این رو تحقیق و توسعه روش‌های رمزنگاری تصاویر تبدیل به موضوع مهم در حوزه امنیت اطلاعات دیجیتال شده است. الگوریتم‌های رمزنگاری تصویر به صورت معمول شامل دو مرحله جایگزینی و جابجایی می‌باشد. در مرحله جایگزینی، مقدار هر پیکسل با مقدار جدید تغییر می‌کند و در مرحله جابجایی محل پیکسل‌ها تغییر می‌کند. وجود هر دو مرحله در طراحی یک سیستم رمزنگاری ضروری می‌باشد [۴]. نگاشت‌های آشوبی به دلیل خواص شبه‌تصادفی خود یک ابزار مناسب برای طراحی سیستم‌های رمزنگاری می‌باشد [۵].

در [۶] یک روش رمزنگاری تصویر با استفاده از دنباله آشوبی و تبدیل ویولت در تصویر معرفی شده است که می‌تواند اطلاعات درون تصویر را به خوبی محافظت کند. در این روش از یک نگاشت آشوبی لوجستیک برای تولید دنباله آشوبی استفاده شده است. همچنین عملیات رمزنگاری در حوزه ویولت نیز صورت گرفته است. در [۷] یک روش رمزنگاری برای تصاویر رنگی بر اساس نگاشت آشوبی KAA با چندین نگاشت آشوبی پیشنهاد شده است. در این روش برهم‌ریزی پیکسل‌ها با استفاده

★از کمیته علمی بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول.
آدرس‌های رایانامه: hashemi_h@birjand.ac.ir (سید حسام‌الدین هاشمی)، m.majidi@birjand.ac.ir (محمدحسن مجیدی)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] Advanced Encryption Standard [2] Data Encryption Standard

از دو کلید انجام می‌شود، کلید اول با استفاده از نگاشت آشوبی دو بعدی لوجستیک ایجاد می‌شود. کلید دوم با استفاده از نگاشت آشوبی برنولی تولید می‌شود. در [۸] نیز یک روش رمزنگاری تصویر بر اساس نگاشت آشوبی دوبعدی سالمون ارائه شده است. نگاشت آشوبی سالمون به دلیل داشتن ضرایب لیاپانوف گسترده‌تر نسبت به سایر روش‌ها، مورد استفاده قرارگرفته است. در [۹] یک روش رمزنگاری بر اساس توابع بسل معرفی شده است. نگاشت بسل معرفی شده در این روش دارای سه پارامتر کنترلی می‌باشد که می‌تواند چگالی و همبستگی پیکسل‌ها را بر هم ریزد. نتایج شبیه سازی تاکید بر امنیت بالا این روش دارد. طرح جدیدی جهت رمزنگاری تصویر با استفاده از چندجمله‌ای آشوبی PWQPCM [۱] معرفی شده است. همچنین از یک طرح S-Box جهت جابجایی و جانشینی تصاویر در این روش استفاده شده است [۱۰].

هدف از این مقاله معرفی یک روش رمزنگاری تصاویر دیجیتال است که علاوه بر حفظ امنیت محتوا تصویر، بتواند در مقابل حملات مختلف موجود در این حوزه مقاوم باشد. از این رو سیستم رمزنگاری IEPS [۲] جهت رمزنگاری تصاویر دیجیتال معرفی شده است که از نگاشت آشوبی PWLCM [۳] و خواص تابع چکیده‌ساز SHA-512 استفاده می‌کند.

در بخش ۲ این مقاله، ادبیات موضوع اشاره شده است، در این بخش نگاشت‌های آشوب و تابع چکیده‌ساز مورد استفاده بحث شده است. در بخش ۳ روش پیشنهادی رمزنگاری IEPS معرفی شده است، در بخش ۴ عملکرد طرح پیشنهادی را مورد بررسی و ارزیابی قرار داده‌ایم و در بخش ۵ نتیجه‌گیری این مقاله آورده شده است.

۲ ادبیات موضوع

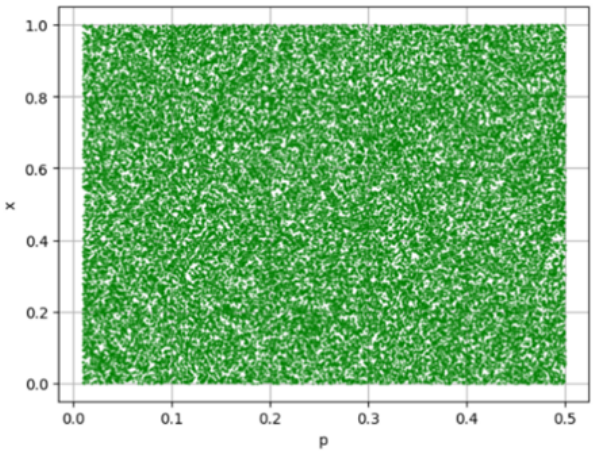
در این بخش به صورت خلاصه با ابزار مورد استفاده در سیستم رمزنگاری IEPS آشنا خواهیم شد. در ابتدا به صورت خلاصه با تابع چکیده‌ساز SHA-512 و سپس نگاشت آشوب‌ناک PWLCM معرفی خواهد شد.

۱.۲ تابع چکیده‌ساز SHA-512

توابع چکیده‌ساز یک دسته از توابع ریاضی هستند که در کاربردهای مختلف رمزنگاری و مخابرات امن استفاده می‌شوند. خروجی یک تابع چکیده‌ساز همیشه دارای طول ثابت برای هر پیام با طول دلخواه می‌باشد. خانواده توابع چکیده‌ساز SHA [۴] یک دسته از توابع چکیده‌ساز محبوب است که توسط آژانس امنیت ملی آمریکا توسعه یافته است. الگوریتم‌های SHA-256 و SHA-512 به ترتیب دارای ۲۵۶ و ۵۱۲ بیت اطلاعات در خروجی می‌باشند که فضای جستجوی مناسب و امنی برای کاربردهای مختلف ایجاد کرده است [۱۱].

توابع SHA-256 از بلاک‌هایی با سایز ۵۱۲ بیت و ۶۴ دور محاسبه

[1] Piece-Wise Quadratic Polynomial Chaotic Map [2] Image Encryption Based on PWLCM and SHA512 [3] Piecewise Linear Chaotic Map [4] Secure Hashing Algorithm



شکل ۱. نگاشت PWLCM با مقادیر مختلف r

به دست می‌آید، درحالی که SHA-512 از بلاک‌هایی با سایز ۱۰۲۴ و ۸۰ دور به دست می‌آید. به علاوه در SHA-512 از یک کلمه داخلی با سایز ۶۴ بیت استفاده می‌کند. تابع SHA-256 از ۶۴ ثابت $K_0, K_1, \ldots, K_{63}$ که هرکدام ۳۲ بیت است، تشکیل شده است. همچنین در این تابع از ۸ ثبت‌کننده برای ذخیره‌سازی اطلاعات واسط با نام‌های $H_0, H_1, \ldots, H_7$ این مقادیر در [۱۲] اشاره شده است.

۲.۲ نگاشت آشوبی PWLCM

ساختار آشوب در لغت به معنی درهم‌ریختگی و بی‌نظمی می‌باشد. در حوزه ریاضیات نگاشت‌های آشوب‌ناک معادلاتی غیرخطی هستند که رفتار شبه تصادفی از خود نشان می‌دهند. هرچند در ظاهر خروجی این معادلات تصادفی به نظر می‌رسد ولی این خروجی کاملا قطعی می‌باشد [۱۳]. نگاشت‌های آشوب‌ناک بسیار به ورودی آنها حساس هستند بدین معنی که با کوچکترین تغییر در ورودی، خروجی سیستم کاملاً تغییر خواهد کرد. نگاشت آشوب‌ناک خطی قطعه‌ای PWLCM به صورت سه زیرمعادله خطی (۱) تعریف می‌شود [۱۴].

$$x_{n+1} = f(x_n, p) = \begin{cases} \frac{x_n}{p}, & 0 \le x_n \le p \\ \frac{x_n - p}{0.5 - p}, & 0 \le x_n \le p \\ f(1 - x_n, p) & 0.5 \le x_n \le 1 \end{cases} \quad (1)$$

در این رابطه x_n متغیر محاسبه شده در دور n است و x_0 مقدار اولیه تابع است. عدد ثابت p یک پارامتر کنترل سیستم آشوب‌ناک است که مقادیری بین ۰ تا ۰٫۵ را اختیار می‌کند. شکل ۱ مقدار x_{1000} با یک مقدار اولیه تصادفی و pهای مختلف را نشان می‌دهد. همانطور که مشاهده می‌شود نگاشت آشوب‌ناک PWLCM دارای محدوده آشوبی و رفتار پیچیده تری نسبت به نگاشت آشوبی لوجستیک دارد.

۳ روش پیشنهادی

در این روش ابتدا تصویر با استفاده از تابع آشوب‌ناک PWLCM برهم ریخته خواهد شد و سپس مقادیر پیکسل‌ها با مقادیر جدید و با استفاده از تابع چکیده‌ساز SHA-512 جایگزین می‌شود. این سیستم رمزنگاری شامل دو مرحله رمزنگاری و رمزگشایی می‌باشد که در ادامه شرح داده خواهند شد.

۱.۳ رمزنگاری

در طراحی سیستم رمزنگاری IEPS نیاز به دو عملیات جابجایی و جایگزینی می‌باشد.

در عملیات جابجایی با استفاده از تابع آشوب PWLCM و $SubKey_1$ و $SubKey_2$ محل قرار گیری پیکسل‌ها به صورت زیر تغییر می‌کند. $SubKey_1$ و $SubKey_2$ مقادیر اعشاری بین ۰ تا ۱ هستند.

(آ) با استفاده از تابع آشوب PWLCM و مقدار اولیه $SubKey_1$، M دنباله آشوبی $S_1, S_2, \ldots, S_M$ با طول N تولید می‌شود.

(ب) در هر سطر از تصویر I پیکسل‌ها بر اساس جایگاه مرتب شده دنباله‌های آشوبی S_i جابجا می‌شوند و تصویر برهم‌ریخته P_1 ایجاد می‌شود.

(ج) با استفاده از تابع آشوب PWLCM و مقدار اولیه $SubKey_2$، N دنباله آشوبی $O_1, O_2, \ldots, O_N$ با طول M تولید می‌شود.

(د) در هر ستون از تصویر برهم‌ریخته P_1 پیکسل‌ها بر اساس جایگاه مرتب شده دنباله‌های آشوبی O_i جابجا می‌شوند و تصویر برهم‌ریخته P_2 ایجاد می‌شود.

شکل ۲ فرایند یک دور جابجایی یک تصویر آشکار را نشان می‌دهد.

در عملیات جایگزینی، از خواص تابع چکیده‌ساز SHA-512 برای تغییر مقادیر پیکسل‌ها به صورت زیر استفاده شده است.

۱) تصویر P_2 را به بلاک‌هایی با اندازه ۱۶ × ۱۶ تقسیم می‌کنیم. نتیجه این اقدام ایجاد بلاک‌های $B_1, B_2, \ldots, B_{\frac{M}{16},\frac{N}{16}}$ می‌باشد.

$$B_{1,1}, B_{1,2}, \ldots, B_{\frac{M}{16},\frac{N}{16}} = Blocks(P_2) \qquad (۲)$$

۲) هر بلاک را به زیر بلاک‌هایی با اندازه ۸ × ۸ تقسیم می‌کنیم. نتیجه این اقدام ایجاد ۴ زیربلاک به صورت زیر است.

$$SB_1, SB_1, SB_3, SB_4 = Blocks(B_{i,j}) \qquad (۳)$$

۳) اطلاعات زیربلاک اول از طریق رابطه (۴) با مقادیر جدید رمز می‌شود.

$$SB'_1 = (SB_1 + SHA512(SubKey_3)) \pmod{256} \qquad (۴)$$

۴) اطلاعات سه زیر بلاک بعدی از طریق رابطه (۵) رمز می‌شود ($m \in \{2, 3, 4\}$).

$$SB'_m = (SB_m + SHA512(SB'_{m-1})) \pmod{256} \qquad (۵)$$

۵) زیربلاک‌های رمزشده را مانند یک بلاک با ابعاد ۱۶ کنار هم قرار می‌دهیم و بلاک رمزشده B' ایجاد می‌شود.

$$B'_{i,j} = Blocks^{-1}(SB'_1, SB'_2, SB'_3, SB'_4) \qquad (۶)$$

۶) بلاک‌های رمزشده را مانند یک تصویر با ابعاد $M \times N$ کنار هم قرار می‌دهیم و تصویر رمزشده C ایجاد می‌شود.

$$C = Blocks^{-1}(B'_{1,1}, B'_{1,2}, \ldots, B'_{\frac{M}{16},\frac{N}{16}}) \qquad (۷)$$

از آنجایی که خروجی تابع SHA-512 یک رشته بیت با ۵۱۲ بیت اطلاعات است که شامل ۶۴ بایت اطلاعات می‌باشد، می‌توان آن را به صورت یک تصویر هشت بیتی ۸ × ۸ نظیر کرد و آن را با بلاک‌های ۸ × ۸ بیتی جمع و یا تفریق کرد. از این رو اندازه بلاک‌ها به صورت هوشمندانه ۸ × ۸ انتخاب شده است. از طرفی تابع mod به منظور جمع و تفریق در پیمانه ۲۵۶ انتخاب شده است که باعث می‌شود همه مقادیر پس از محاسبات به یک عدد بین ۰ تا ۲۵۵ تبدیل شوند و در نهایت بتوان آن را به صورت یک مقدار ۸ بیتی متناظر دانست. شکل ۳ شمای کلی فرایند جایگزینی را نشان می‌دهد.

شکل ۴ شمای کلی طرح رمزنگاری IEPS را نشان می‌دهد. برای افزایش امنیت فرایند جابجایی و جایگزینی را به تعداد n دور تکرار می‌کنیم. همانطور که در تصویر مشاهده می‌شود، اطلاعات هر زیربلاک مانند یک زنجیر درون اطلاعات زیربلاک‌های بعدی قرار می‌گیرد و این فرایند باعث می‌شود با کوچکترین تغییر در تصویر اصلی، تصویر رمزشده آن با تصویر دیگر کاملاً متمایز باشد.

الگوریتم IEPS برای تصاویر رنگی را می‌توان با سه بار تکرار برای هرکانال رنگی به صورت جداگانه انجام داد.

۲.۳ رمزگشایی

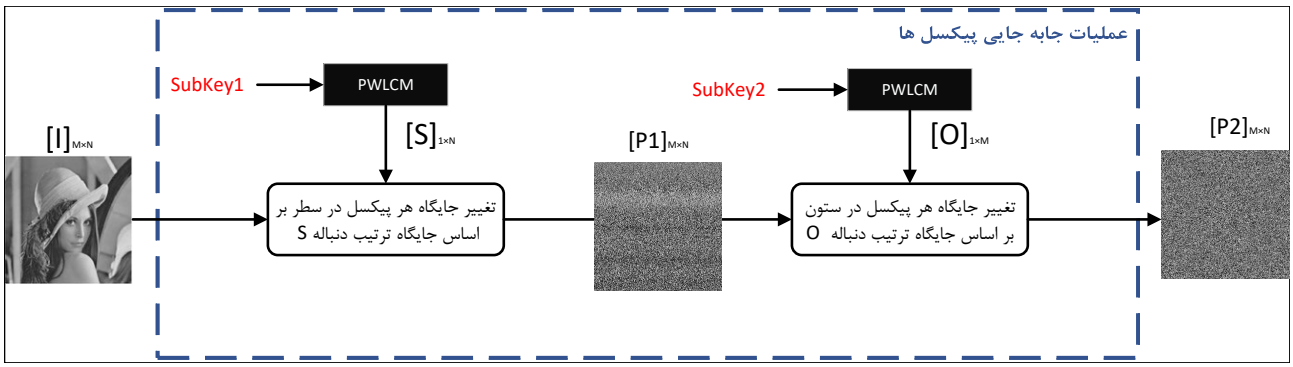
در مرحله رمزگشایی IEPS، فرایند معکوس جایگزینی به صورت زیر انجام می‌شود.

۱) تصویر C را به بلاک‌هایی با اندازه ۱۶ × ۱۶ تقسیم می‌کنیم. تا بلاک‌های رمزشده $B'_1, B'_2, \ldots, B'_{\frac{M}{16},\frac{N}{16}}$ ایجاد شوند.

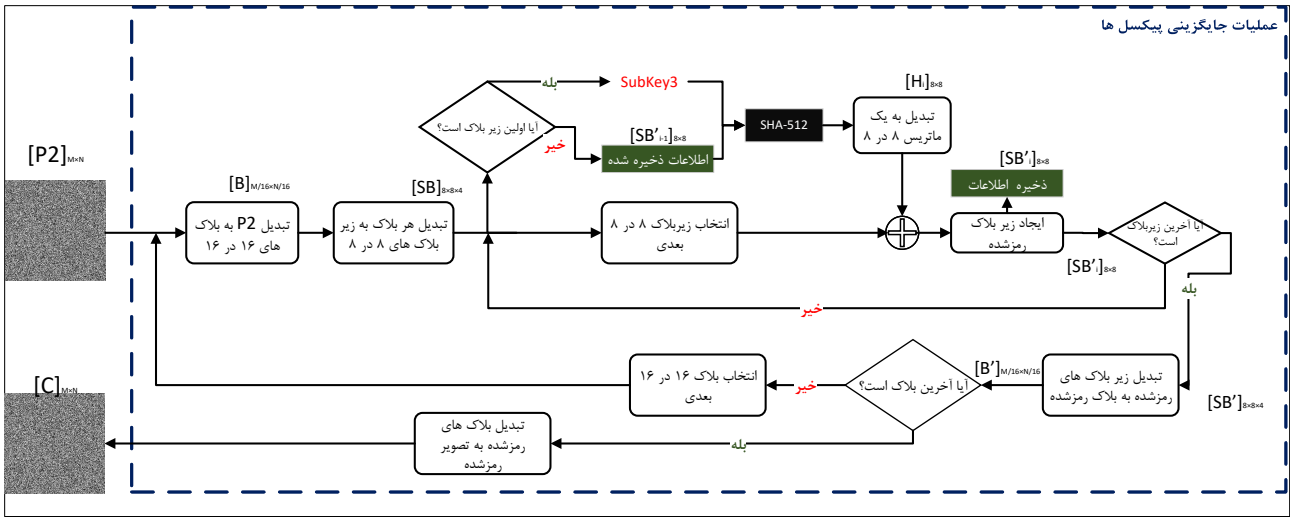
$$B'_{1,1}, B'_{1,2}, \ldots, B'_{\frac{M}{16},\frac{N}{16}} = Blocks(C) \qquad (۸)$$

۲) هر بلاک را به زیر بلاک‌هایی با اندازه ۸ × ۸ تقسیم می‌کنیم. نتیجه این اقدام ایجاد ۴ زیربلاک رمزشده به صورت زیر است.

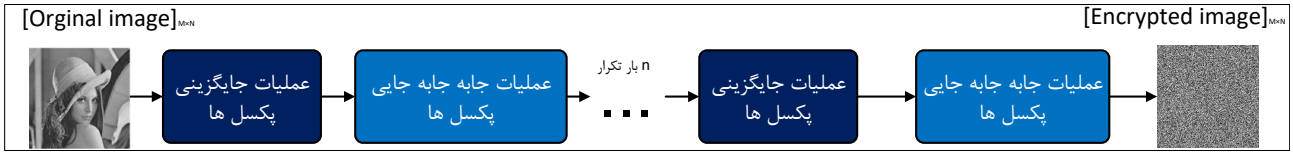
$$SB'_1, SB'_2, SB'_3, SB'_4 = Blocks(B'_{i,j}) \qquad (۹)$$



شکل ۲. فرایند جابجای پیکسل‌ها در طرح رمزنگاری IEPS



شکل ۳. فرایند جایگزینی پیکسل‌ها در طرح رمزنگاری IEPS



شکل ۴. فرایند رمزنگاری در طرح IEPS

۳) اطلاعات زیربلاک اول از طریق رابطه (۱۰) با مقادیر جدید رمزگشایی می‌شود.

$$SB_1 = (SHA512(SubKey_3) - SB'_1) \pmod{256} \quad (10)$$

۴) اطلاعات سه زیر بلاک بعدی از طریق رابطه زیر رمزگشایی می‌شوند ($m \in \{2,3,4\}$).

$$SB_m = (SHA512(SB_{m-1}) - SB'_m) \pmod{256} \quad (11)$$

۵) زیربلاک‌های رمزگشایی شده را به یک بلاک با ابعاد 16×16 تبدیل می‌کنیم و بلاک آشکار B ایجاد می‌شود.

$$B_{i,j} = Blocks^{-1}(SB_1, SB_2, SB_3, SB_4) \quad (12)$$

۶) بلاک‌های آشکار را مانند یک تصویر با ابعاد $M \times N$ کنار هم قرار می‌دهیم و تصویر آشکار P_2 ایجاد می‌شود.

$$P_2 = Blocks^{-1}(B_{1,1}, B_{1,2}, \ldots, B_{\frac{M}{16},\frac{N}{16}}) \quad (13)$$

همچنین در این مرحله، برای معکوس جابجایی از طریق مراحل زیر انجام خواهد شد.

(آ) با استفاده از تابع آشوب PWLCM و مقدار اولیه $SubKey_2$، N دنباله آشوبی $O_1, O_2, \ldots, O_N$ با طول M تولید می‌شود.

(ب) در هر ستون از تصویر برهم‌ریخته P_2 پیکسل‌ها بر اساس معکوس جایگاه مرتب شده دنباله‌های آشوبی O_i جابجا می‌شوند و تصویر برهمریخته P_1 ایجاد می‌شود.

(ج) با استفاده از تابع آشوب PWLCM و مقدار اولیه $SubKey_1$، M دنباله آشوبی $S_1, S_2, \ldots, S_M$ با طول N تولید می‌شود.

(د) در هر سطر از تصویر برهم‌ریخته P_1 پیکسل‌ها بر اساس جایگاه مرتب‌شده دنباله‌های آشوبی S_i جابجا می‌شوند و تصویر آشکار I رمزگشایی می‌شود.

فرایند رمزگشایی تصویر رمزشده C با ابعاد $M \times N$ با فرض عدم تغییر در فایل رمزشده در فرایند ارسال به صورت معکوس فرایند رمزگشایی و n دور تکرار به ترتیب با عملیات معکوس جایگزینی و معکوس جابجایی انجام می‌شود. شکل ۵ شمای کلی طرح رمزگشایی IEPS را نشان می‌دهد.

۴ شبیه‌سازی و ارزیابی طرح رمزنگاری IEPS

برای بررسی عملکرد رمزنگاری IEPS، سیستم فوق را بر اساس معیارهای استاندارد جهت بررسی عملکرد سیستم رمزنگاری تصاویر مورد ارزیابی قرار داده‌ایم. شکل ۶ عملکرد طرح رمزنگاری پیشنهادی را برای دو تصویر سیاه و سفید و رنگی نشان می‌دهد.

همانطور که مشاهده می‌شود، طرح پیشنهادی به خوبی توانسته است ساختار تصویر را بر هم بزند، به گونه‌ای که از تصویر رمزشده نتوان هیچگونه اطلاعات قابل فهمی استخراج کرد. با این حال برای بررسی عملکرد تمایز از معیارهای MSE و PSNR استفاده می‌شود. برای محاسبه MSE از رابطه (۱۴) استفاده می‌شود.

$$MSE = \frac{1}{M \times N \times O} \sum_{x=1}^{M} \sum_{y=1}^{N} \sum_{z=1}^{O} \left[\left(I_{(x,y,z)} - I'_{(x,y,z)} \right)^2 \right] \quad (۱۴)$$

که در آن M و N ابعاد تصویر و O تعداد کانال‌های تصویر می‌باشد. برای تصاویر سیاه و سفید مقدار O برابر یک و برای تصاویر رنگی (RGB) مقدار آن برابر سه می‌باشد. $I_{(x,y,z)}$ و $I'_{(x,y,z)}$ به ترتیب پیکسل‌های تصویر اصلی و نهان‌نگاشته در موقعیت x، y و کانال z می‌باشد. MSE از مجموع مربعات پیکسل‌های تغییریافته محاسبه می‌شود و PSNR مطابق رابطه (۱۵) محاسبه می‌شود.

$$PSNR = 10 \log_{10} \left(\frac{\max^2}{MSE} \right) \quad (۱۵)$$

در این رابطه max بیشترین مقدار ممکن برای پیکسل‌ها در تصویر می‌باشد که برای تصاویر ۸ بیتی این مقدار ۲۵۵ می‌باشد.

جدول ۱. معیار MSE و PSNR میان تصویر اصلی و رمزشده

روش رمزنگاری	معیار MSE	معیار PSNR
تصویر سیاه و سفید لنا	۸۶۷۸٫۳۸	۲۰٫۱۳۹۳
تصویر رنگی دریا	۱۰۹۵۷٫۸	۱۷٫۸۰۷۱

جدول ۲. تحلیل آنتروپی در تصویر اصلی و رمزشده

روش رمزنگاری	تصویر اصلی	تصویر رمزنگاری شده
روش مرجع [۳] تصویر لنا	۷٫۶۳۴۳	۷٫۹۸۱۲
روش مرجع [۴] تصویر لنا	۷٫۶۳۴۳	۷٫۹۹۷۲
روش مرجع [۵] تصویر لنا	۷٫۶۳۴۳	۷٫۹۹۷۵
روش مرجع [۷] تصویر لنا	۷٫۶۳۴۳	۷٫۹۹۷۱
روش IEPS تصویر لنا	۷٫۶۳۴۳	۷٫۹۹۸۱
روش IEPS تصویر رنگی (میانگین سه کانال)	۷٫۰۱۹۳	۷٫۹۹۹۱
روش IEPS میانگین صد تصویر سیاه و سفید	۶٫۸۸۴۳	۷٫۹۹۸۴
روش IEPS میانگین صد تصویر رنگی	۶٫۷۸۵۴	۷٫۹۹۹۱

نتایج مقایسه میزان شباهت تصویر اصلی و تصویر رمز شده در جدول ۱ ارائه شده است. مشاهده می‌شود مقدار MSE و PSNR میان تصویر اصلی و رمز شده بسیار زیاد است و نتایج تاکید می‌کند که تصویر رمزشده هیچ شباهتی به تصویر اصلی ندارد و مشابه یک نویز عمل کرده است.

۱.۴ تحلیل آنتروپی

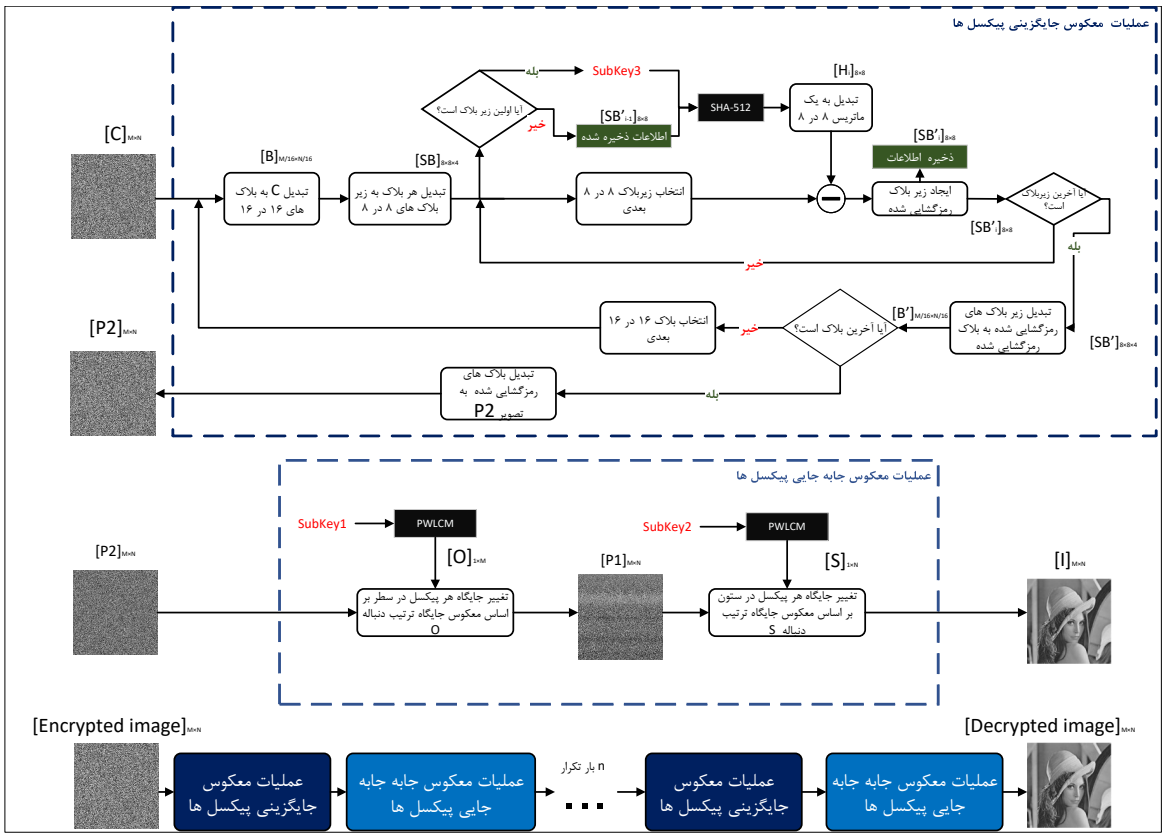
برای بررسی اینکه چه میزان اطلاعات درون تصویر رمزشده موجود است از تحلیل آنتروپی استفاده شده است. برای محاسبه آنتروپی از رابطه (۱۶) استفاده شده است.

$$H(s) = \sum_{i=0}^{2^N - 1} p(s_i) \log_2 \frac{1}{p(s_i)} \quad (۱۶)$$

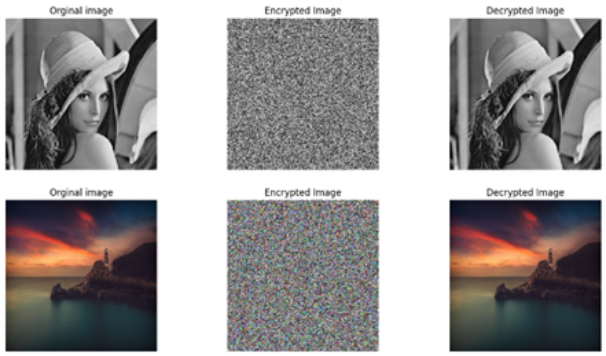
در رابطه فوق $p(s_i)$ احتمال وقوع یکی سطح خاکستری s_i می‌باشد و 2^N تعداد سطوح خاکستری می‌باشد که در تصاویر ۸ بیتی این مقدار ۲۵۶ می‌باشد. در تصاویر ۸ بیتی بیشترین مقدار آنتروپی ۸ بیت است.

برای بررسی عملکرد سیستم رمزنگاری آنتروپی اطلاعات برای تصاویر فوق و همچنین میانگین صد تصویر سیاه و سفید و میانگین صد تصویر رنگی محاسبه شده است.

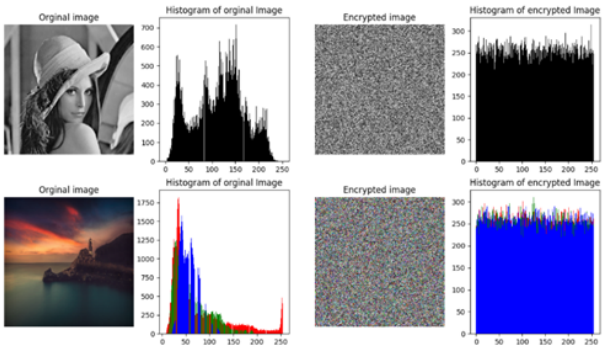
همانطور که در جدول ۲ مشاهده می‌شود، در تصاویر رنگی و سیاه و سفید آنتروپی تصویر رمزشده بسیار نزدیک به ۸ است که نشان دهنده عملکرد مثبت روش پیشنهادی در برهم‌ریزی اطلاعات تصویر می‌باشد. همچنین روش پیشنهادی نسبت به روش‌های مختلف رمزنگاری تصویر بررسی و ارزیابی شده است که نشان می‌دهد، روش معرفی شده در معیار آنتروپی عملکرد بهتری نسبت به سایر روش‌ها دارد.



شکل ۵. شمای کلی برای رمزگشایی در طرح رمزنگاری IEPS



شکل ۶. عملکرد طرح رمزنگاری IEPS دو تصویر رنگی و سیاه و سفید



شکل ۷. تحلیل هیستوگرام سیستم رمزنگاری IEPS

۲.۴ تحلیل آماری تصویر رمزنگاری شده

یک سیستم رمزنگاری خوب باید همه اطلاعات آماری درون تصویر را از بین ببرد. از این رو توزیع رخداد هر روشنایی در تصویر رمز شده باید به صورت یکنواخت باشد. شکل ۷ تحلیل هیستوگرام دو تصویر سطح خاکستری لنا و تصویر رنگی دریا را نشان می‌دهد. مشاهده می‌شود، در هر دو مورد هیستوگرام تصویر رمزشده به صورت یکنواخت تبدیل شده است.

به جهت بررسی عملکرد روش رمزنگاری IEPS در برهم‌ریزی همبستگی میان پیکسل‌ها، همبستگی میان پیکسل‌ها در راستا افقی، عمودی و مورب در تصویر رمزشده محاسبه شده است. همبستگی از طریق روابط (۱۷) محاسبه می‌شود.

$$r_{xy} = \frac{\sigma_{xy}}{\sqrt{\sigma_x}\sqrt{\sigma_y}} \qquad (۱۷)$$

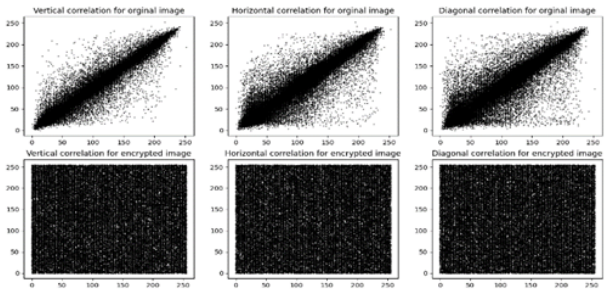
که در آن σ_{pq} واریانس مشترک[1] تصویر x و y می‌باشد، که از طریق رابطه (۱۸) محاسبه می‌شود.

$$\sigma_{pq} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}(p_{x,y,z}-\mu_p)(q_{x,y,z}-\mu_q)}{MNO} \qquad (۱۸)$$

[1] Covariance

جدول ۳. عملکرد طرح رمزنگاری IEPS در برهم‌ریزی همبستگی

روش رمزنگاری	همبستگی در راستای افقی	همبستگی در راستای عمودی	همبستگی در راستای مورب
روش مرجع [۶] (رنگی)	۰٫۰۳۲۱	۰٫۰۳۰۱	۰٫۰۰۲۱
روش مرجع [۷] (رنگی)	۰٫۰۱۴۴	۰٫۰۰۱۵	۰٫۰۰۸۱
روش مرجع [۸] (رنگی)	۰٫۰۲۱۲	۰٫۰۰۱۷	۰٫۰۰۱۲
روش مرجع [۱۰] (سیاه و سفید)	۰٫۰۰۲۸۷	۰٫۰۰۱۰	۰٫۰۰۴۴
روش IEPS (سیاه و سفید)	۰٫۰۰۲۶	۰٫۰۰۱۳	۰٫۰۰۱۱
روش IEPS (رنگی)	۰٫۰۰۰۸	۰٫۰۰۱۱	۰٫۰۰۰۵
روش IEPS میانگین ۱۰۰ تصویر	۰٫۰۰۱۵	۰٫۰۰۱۳	۰٫۰۰۱۲



شکل ۸. بررسی همبستگی تصویر رمزشده (سیاه و سفید)

در رابطه (۱۸) μ_p و σ_q به ترتیب برابر با میانگین و واریانس شدت روشنایی پیکسل‌های تصویر x می‌باشد و از طریق روابط زیر محاسبه می‌شود.

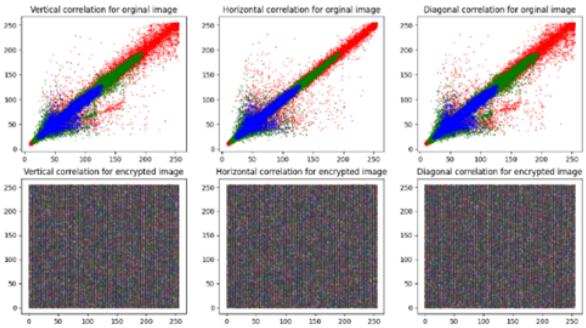
$$\mu_p = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}(p_{x,y,z})}{MNO} \quad (۱۹)$$

$$\sigma_p = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}(p_{x,y,z}-\mu_p)^2}{MNO} \quad (۲۰)$$

انتظار می‌رود در یک سیستم رمزنگاری خوب مقدار ضرایب همبستگی در راستا افقی، عمودی و مورب نزدیک به صفر باشد. جدول ۳ میانگین همبستگی میان پیکسل‌ها در تصاویر فوق و در ۱۰۰ تصویر تصادفی رمز شده برای روش IEPS و سایر روش‌های رمزنگاری تصویر نشان می‌دهد. میانگین مقدار همبستگی در راستا افقی، عمودی و مورب برای صد تصویر به ترتیب برابر با ۰٫۰۰۱۵، ۰٫۰۰۱۳ و ۰٫۰۰۱۲ می‌باشد. نتایج تاکید می‌کنند روش IEPS به خوبی می‌تواند اطلاعات پیکسل‌های مجاور را از بین ببرد. شکل ۸ و شکل ۹ همبستگی تصویر در راستا افقی، عمودی و مورب را برای دو تصویر سطح خاکستری لنا و رنگی دریا نشان می‌دهد.

۳.۴ عملکرد در مقابل حملات تفاضلی

همچنین برای بررسی طرح پیشنهادی نسبت به حملات تفاضلی، معیارهای NPCR و UACI ارائه شده است. برای محاسبه معیار NPCR از معادله (۲۱) استفاده شده است.



شکل ۹. بررسی همبستگی تصویر رمزشده (رنگی)

جدول ۴. بررسی معیار UACI و NPCR

روش رمزنگاری	UACI	NPCR
روش مرجع [۶]	۳۳٫۱۲۰۰	۹۹٫۷۵۷
روش مرجع [۷]	۳۳٫۴۶۵۷	۹۹٫۶۲۵
روش مرجع [۸]	۳۳٫۴۷۹۸	۹۹٫۶۰۹
روش مرجع [۱۰]	۳۳٫۸۸۷۱	۹۹٫۶۳۳
روش IEPS تصاویر سیاه و سفید	۳۳٫۴۸۰۳	۹۹٫۶۰۵
روش IEPS رنگی دریا	۳۳٫۴۴۸۹	۹۹٫۶۱۳
روش IEPS میانگین ۱۰۰ تصویر سیاه و سفید	۳۳٫۴۱۴۵	۹۹٫۶۴۳
روش IEPS میانگین ۱۰۰ تصویر رنگی	۳۳٫۴۲۴۳	۹۹٫۶۳۱

$$NPCR = \frac{100}{M \times N \times K}\sum_{k=0}^{K}\sum_{j=0}^{N}\sum_{i=0}^{M} D(i,j,k) \quad (۲۱)$$

که در آن از طریق معادله (۲۲) محاسبه می‌شود.

$$D(i,j,k) = \begin{cases} 0 & \text{if } C_1(i,j,k) = C_2(i,j,k) \\ 1 & \text{if } C_1(i,j,k) \neq C_2(i,j,k) \end{cases} \quad (۲۲)$$

و برای محاسبه UACI نیز از طریق معادله (۲۳) استفاده شده است.

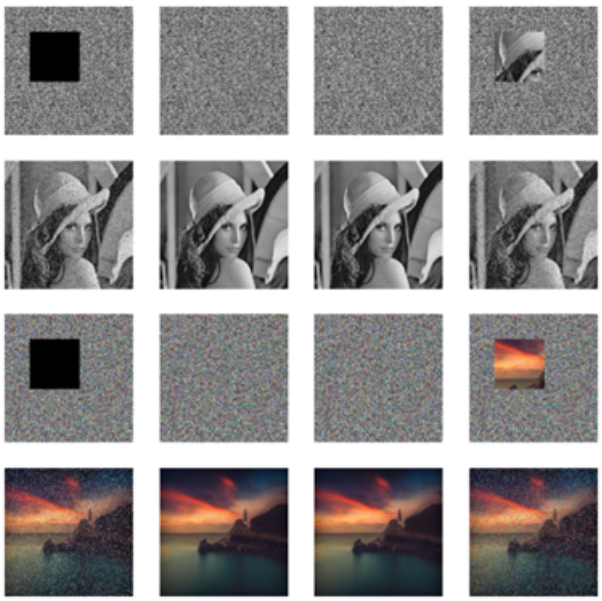
$$UACI = \frac{1}{M \times N \times K}\sum_{k=0}^{K}\sum_{j=0}^{N}\sum_{i=0}^{M} \frac{|C_1(i,j,k) - C_2(i,j,k)|}{255} \quad (۲۳)$$

در روابط فوق C_1 و C_2 دو تصویر رمزشده هستند، که تصویر آشکار آنها فقط در یک پیکسل و به اندازه یک بیت باهم تفاوت دارند.

نتایج این آزمایش در جدول ۴ نشان داده شده است. همانطور که از نتایج آزمایش مشخص است، طرح پیشنهادی به دلیل تغییر در ساختار پیکسل‌ها به خوبی می‌تواند در مقابل حملات تفاضلی عملکرد مناسبی از خود نشان دهد.

۴.۴ مقاومت تصویر رمزشده در برابر تغییرات

طرح پیشنهادی در مقابل برخی تغییرات از جمله، برش، نویز جمع‌شونده گوسی، نویز نمک و فلفل و کپی کردن بخشی از تصویر مورد ارزیابی قرار



شکل ۱۰. بررسی عملکرد روش IEPS در مقابل حملات مختلف

جدول ۵. تحلیل حساسیت به کلید میان دو تصویر رمزشده با کلید متفاوت

روش رمزنگاری	فضای کلید
روش مرجع [۶]	∞
روش مرجع [۷]	$۱۰^{۱۴۴}$
روش مرجع [۸]	$۲^{۵۶}$
روش مرجع [۱۰]	$۳^{۵۲}$
روش IEPS	∞

گرفته است. شکل ۱۰ نتایج آزمایشات را نشان می‌دهد. سطر اول و سوم تصویر رمزشده مخدوش شده برای تصویر سیاه و سفید و رنگی می‌باشد و سطر دوم و چهارم، تصاویر رمزگشایی می‌باشد. مشاهده می‌شود طرح پیشنهادی به دلیل برهم‌ریزی پیکسل‌ها به خوبی توانسته است در مقابل این تغییرات مقاوم باشد و اطلاعات تصویر اصلی را حفظ کند.

۵.۴ امنیت کلید سیستم رمزنگاری

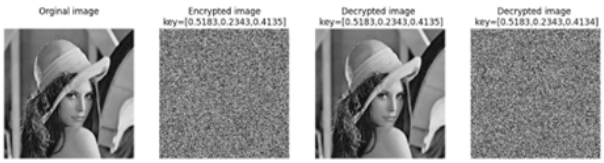
یکی از ویژگی‌های مهم سیستم‌های رمزنگاری تصویر، امنیت کلید آن است. سیستم رمزنگاری معرفی شده مجموعا دارای ۳ زیرکلید است، که ۲ زیرکلید اعداد اعشاری بین صفر و یک هستند و یک زیرکلید می‌تواند هر مقداری اختیار کند که در تابع SHA-512 مورد استفاده قرار میگیرید. لذا فضای کلید طرح پیشنهادی بینهایت می‌باشد. جدول ۵ فضای کلید طرح پیشنهادی را در مقایسه با چهار روش رمزنگاری تصویر جدید نشان می‌دهد.

در گام بعدی حساسیت به کلید را برای سیستم رمزنگاری IEPS با دو روش بررسی شده است. در آزمایش اول، یک تصویر را با دو کلید متفاوت که تنها ۰٫۰۰۰۱ اختلاف دارند رمزنگاری کرده‌ایم و اختلاف میان

جدول ۶. تحلیل حساسیت به کلید میان دو تصویر رمزشده با کلید متفاوت

روش IEPS	معیار MSE	معیار PSNR
تصویر رمز شده با کلید متفاوت	۱۰۹۱۳٫۲۲	۱۷٫۸۴۷۹

شکل ۱۱. بررسی حساسیت به کلید در عملیات رمزنگاری



شکل ۱۲. بررسی حساسیت نسبت به کلید در رمزگشایی

تصاویر را محاسبه کرده‌ایم. شکل ۱۱ نتایج این آزمایش را نشان می‌دهد. برای بررسی دقیق‌تر MSE و PSNR را برای دو تصویر رمزشده محاسبه کرده‌ایم. جدول ۶ نتایج محاسبه PSNR و MSE میان دو تصویر رمزشده را نشان می‌دهد. مشاهده می‌شود، تصاویر رمزشده کاملا با هم متمایز هستند و هیچ اطلاعات مفیدی قابل برداشت نیست.

در آزمایش دوم برای رمزگشایی یک تصویر رمزشده تنها ۰٫۰۰۰۱ اختلاف در کلید ایجاد کرده‌ایم. شکل ۱۲ نتایج عملکرد روش پیشنهادی رمزنگاری را نشان می‌دهد. تصویر اول از سمت چپ تصویر اصلی است، تصویر دوم تصویر رمزنگاری شده است، تصویر سوم تصویر رمزگشایی با کلید صحیح است و تصویر آخر تصویر رمزگشایی با کلید اشتباه است. همانطور که مشاهده می‌شود، با کلید اشتباه، تصویر رمزگشایی نشده است و هیچ اطلاعات با اهمیتی آشکار نشده است.

۶.۴ تحلیل سرعت اجرای الگوریتم

سرعت عملکرد سیستم رمزنگاری IEPS، از طریق یک پردازنده Core-i7 نسل ۸ مورد ارزیابی قرار گرفت. جدول ۷ میانگین سرعت سیستم رمزنگاری IEPS و سایر روش‌ها را نشان می‌دهد. مشاهده می‌شود فرایند رمزنگاری و رمزگشایی در تصاویر رنگی حدوداً ۰٫۵ ثانیه زمان می‌برد، که در مقایسه با سایر روش ها از سرعتی مناسبی برخوردار است.

۵ نتیجه‌گیری

در این مقاله، یک روش رمزنگاری تصویر آشوبی مبتنی بر نگاشت PWLCM و تابع چکیده‌ساز SHA-512 با نام IEPS معرفی شده است. از

جدول ۷. سرعت اجرا (میلی ثانیه) طرح رمزنگاری IEPS

روش IEPS	رمزنگاری	رمزگشایی
روش مرجع [۷] تصاویر رنگی	۲۷۵۰٫۹۶	۲۶۳۷٫۱۱
روش مرجع [۸] تصاویر	۶۹۳٫۲۱۴	۷۰۱٫۳۲۱
روش مرجع [۱۰] تصاویر سیاه و سفید	۸۸۸٫۰۱۰	۱۰۸۴٫۱۹
میانگین ۱۰۰ تصویر سیاه و سفید	۱۹۸٫۰۷۹	۱۹۶٫۲۹۲
میانگین ۱۰۰ تصویر رنگی	۵۴۸٫۸۲۳	۵۱۷٫۶۶۰

نگاشت آشوبی PWLCM به جهت برهم‌ریزی مکان پیکسل‌ها و از خواص تابع چکیده‌ساز جهت جایگزین کردن مقادیر پیکسل‌ها با مقادیر جدید استفاده شده است. نتایج نشان داد، طرح پیشنهادی می‌تواند اطلاعات درون تصویر را امن نگاه دارد و آنتروپی تصویر رمزشده را تا حد زیادی نزدیک به ۸ کرده است. به دلیل استفاده از SHA-512 خروجی اطلاعات متناسب با سایز زیربلاک‌های ایجاد شده است، لذا عملیات جمع و تفریق ماتریسی با سرعت بالایی قابل اجراست همچنین این رویکرد باعث شده است محدودیتی در طول سایز کلید وجود نداشته باشد و فضا کلید سیستم IEPS نامحدود باشد. نتایج نشان داد، طرح پیشنهادی در برابر حملات و تحلیل‌های آماری مقاوم است و همبستگی میان پیکسل‌ها را به صورت کامل از بین می‌برد. معیارهای UACI و NPCR نشان داد، طرح پیشنهادی در برابر حملات تفاضلی نیز مقاوم است.

۶ سپاسگزاری

از انجمن رمز ایران بابت برگزاری کنفرانس که فرصت هم‌اندیشی میان محققان را فراهم کرده است، کمال تشکر و قدردانی داریم.

مراجع

[1] Xiao, Di, Liao, Xiaofeng, and Wei, Pengcheng. Analysis and improvement of a chaos-based image encryption algorithm. *Chaos, Solitons & Fractals*, 40(5):2191–2199, 2009.

[۲] فاتح، منصور، رجبلو، و پور، علی. مروری بر نهان‌نگاری تصویر مبتنی بر مخفی‌سازی در کم‌ارزش‌ترین بیت و دسته‌بندی پیکسل و ارائه روشی جدید در این حوزه. دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۵(۲):۶۳–۷۱، ۲۰۱۷.

[3] Kumari, Manju, Gupta, Shailender, and Sardana, Pranshul. A survey of image encryption algorithms. *3D Research*, 8:1–35, 2017.

[4] Wen, Heping and Lin, Yiting. Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding. *Expert Systems with Applications*, 237:121514, 2024.

[5] SaberiKamarposhti, Morteza, Ghorbani, Amirabbas, and Yadollahi, Mehdi. A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos, Solitons & Fractals*, 178:114361, 2024.

[6] Pourasad, Yaghoub, Ranjbarzadeh, Ramin, and Mardani, Abbas. A new algorithm for digital image encryption based on chaos theory. *Entropy*, 23(3):341, 2021.

[7] Alexan, Wassim, Elkandoz, Marwa, Mashaly, Maggie, Azab, Eman, and Aboshousha, Amr. Color image encryption through chaos and kaa map. *Ieee Access*, 11:11541–11554, 2023.

[8] Lai, Qiang, Hu, Genwen, Erkan, Uğur, and Toktas, Abdurrahim. A novel pixel-split image encryption scheme based on 2d salomon map. *Expert Systems with Applications*, 213:118845, 2023.

[9] Toktas, Abdurrahim, Erkan, Uğur, Gao, Suo, and Pak, Chanil. A robust bit-level image encryption based on bessel map. *Applied Mathematics and Computation*, 462:128340, 2024.

[10] Zhu, Shenli, Deng, Xiaoheng, Zhang, Wendong, and Zhu, Congxu. Secure image encryption scheme based on a new robust chaotic map and strong s-box. *Mathematics and Computers in Simulation*, 207:322–346, 2023.

[11] Gueron, Shay, Johnson, Simon, and Walker, Jesse. Sha-512/256. in *2011 Eighth International Conference on Information Technology: New Generations*, pp. 354–358. IEEE, 2011.

[12] Rijmen, Vincent and Oswald, Elisabeth. Update on sha-1. in *Topics in Cryptology–CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings*, pp. 58–71. Springer, 2005.

[13] Li, Lizong. A novel chaotic map application in image encryption algorithm. *Expert Systems with Applications*, p. 124316, 2024.

[14] Li, Shujun, Chen, Guanrong, and Mou, Xuanqin. On the dynamical degradation of digital piecewise linear chaotic maps. *International journal of Bifurcation and Chaos*, 15(10):3119–3151, 2005.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 2 (pp. 24–33)
https://monadi.isc.org.ir

Presented at the ISCISC 2024 in Tarbiat Modares University & Research Institute for Information and Communication Technology, Tehran, Iran

IEPS image encryption: Encryption based on PWLCM and SHA-512 hash function★

Seyed Hesam Odin Hashemi and Mohammad-Hassan Majidi *

Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran

ARTICLE INFO.

Keywords:
Image encryption
IEPS image encryption
PWLCM chaotic map
SHA-512 hash function

Type: Research paper

ABSTRACT

With the ever-increasing growth of the Internet and the expansion of imaging tools, digital images are a huge part of the information we work with. This information often contains sensitive data that requires protection. This paper presents a chaotic image encryption method that effectively safeguards the information contained within digital images. The IEPS encryption system is an image encryption scheme based on a Piecewise linear chaotic map (PWLCM) and the SHA-512 hashing function. This design incorporates two operations: permutation and substitution of image pixels. In the permutation stage, the PWLCM map is employed, and the features of the SHA-512 are utilized to substitute the pixels. The experimental results demonstrate that the PWLCM encryption algorithm successfully encrypts the information within the image and exhibits robust performance against various analyses, including the entropy, histogram, key sensitivity criterion, and resistance to differential attacks.

© 2024 ISC

★ The ISCISC 2024 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: hashemi_h@birjand.ac.ir (Seyed Hesam Odin Hashemi), m.majidi@birjand.ac.ir (Mohammad-Hassan Majidi)
© 2024 ISC. All rights reserved.