نوع مقاله: پژوهشی

روش جدید رمزگذاری تصویر با استفاده از بلوک‌بندی و نگاشت آشوب

دلاور زارعی[۱]، دانشجوی مقطع دکتری، محمدعلی بالافر[۲]، دانشیار، محمدرضا فیضی درخشی[۳]، استاد

۱- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - d.zareai@tabrizu.ac.ir
۲- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - balafarila@tabrizu.ac.ir
۳- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - mfeizi@tabrizu.ac.ir

چکیده: رمزگذاری یکی از قدرتمندترین ابزارهایی است که امنیت اطلاعات را در حوزه ارتباطات و فناوری اطلاعات تضمین می‌کند. رمزگذاری تصویر از سایر رمزگذاری‌ها متفاوت است. این تفاوت به دلیل ویژگی‌های ذاتی تصاویر است. آخرین تلاش‌ها در زمینه‌ی رمزگذاری تصاویر بر پایه‌ی آشوب بوده است. در این مقاله، یک الگوریتم جدید رمزگذاری مبتنی برآشوب برای رمزگذاری تصویر ارائه شده است. در روش پیشنهادی به جای رمزگذاری یک تصویر در هر مرحله، چهار تصویر به صورت هم‌زمان رمزگذاری می شود. به این ترتیب که چهار تصویر استاندارد با همدیگر ترکیب شده و یک تصویر واحد از ترکیب آن‌ها به وجود می‌آید. رمزگذاری هم‌زمان چهار تصویر باعث پیچیده‌تر شدن الگوریتم رمزگذاری پیشنهادی، افزایش امنیت و همچنین گستردگی تغییر مقدار سطح خاکستری هر پیکسل خواهد شد. از نگاشت لجستیک آشوب برای تولید کلید و همچنین جابجایی بلوک‌های تصویر و تغییر مکان آن‌ها استفاده می شود. در نهایت تصویر حاصل با کلید رمزگذاری، XOR شده و تصویر رمزگذاری شده تولید می‌گردد. با توجه به ترکیب چهار تصویر و رمزگذاری هم‌زمان آن‌ها و بررسی تعداد زیادی از معیارهای ارزیابی تصویر ازجمله معیار آنتروپی اطلاعات که مقدار آن در الگوریتم پیشنهادی ما عدد۷/۹۹۹۴ به دست آمده است و به مقدار ایده‌آل ۸ بسیار نزدیک است، نشان می‌دهد که الگوریتم پیشنهادی ما از عملکرد خوبی برخوردار است.

واژه‌های کلیدی: امنیت اطلاعات، رمزگذاری تصویر، نگاشت لجستیک آشوب، بلوک‌بندی تصویر.

A New Method of Image Encryption Using Image Blocking and Chaos Mapping

Delavar Zareai, PhD Student[1], Mohammad-Ali Balafar, Associate Professor[2], Mohammad-Reza Feizi-Derakhshi, Professor[3]

1- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: d.zareai@tabrizu.ac.ir
2- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: balafarila@tabrizu.ac.ir
2- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: mfeizi@tabrizu.ac.ir

Abstract: Encryption is one of the most powerful tools that ensures information security in the field of communication and information technology. Image encryption is different from other encryptions. This difference is due to the inherent characteristics of the images. Recent attempts to encrypt images have been based on chaos. In this paper, a new chaos-based encryption algorithm for image encryption is presented. In the proposed method, instead of encryption one image in each step, four images are encrypted simultaneously. In this way, four standard images are combined and a single image of their combination is created. Simultaneous encoding of four images will cause to complicate the proposed encryption algorithm, increase security, and extend the amount of gray area per pixel. Finally, the resulting image is XORed with encryption key and the encrypted image is generated. Considering the combination of four images and their simultaneous encoding, as well as examining a large number of image evaluation criteria, specifically the information entropy, that has achieved a value equal to 7/9994 in our proposed algorithm, which is really close to the ideal value of 8, shows that the proposed algorithm performs appropriately.

Keywords: Information security, image encryption, chaotic logistics map, image blocking.

نام نویسنده مسئول: محمدعلی بالافر
نشانی نویسنده مسئول: ایران - تبریز - بلوار ۲۹ بهمن - دانشگاه تبریز - دانشکده مهندسی برق و کامپیوتر

۱- مقدمه

بهترین راه برای محرمانه نگه‌داشتن اطلاعات، استفاده از تکنیک‌های مختلف رمزگذاری است[۱]. رمزگذاری و حریم خصوصی داده‌ها دارای چندین هزار سال سابقه است که درگذشته مربوط به مسائل نظامی و مدیریتی دولت بود. امروزه با پیشرفت فناوری، امنیت عملکرد و محرمانه بودن اطلاعات در همه زمینه‌ها موردتوجه قرارگرفته است. با توجه به پیشرفت تکنولوژی در حوزه فناوری اطلاعات و ارتباطات، الگوریتم‌های رمزنگاری توانسته‌اند به طرق مختلف در زندگی روزمره ما ایفای نقش کنند. با توجه به رشد و گسترش شبکه‌های کامپیوتری و به تبع آن شبکه‌های اجتماعی، مردم تصاویر مختلفی را از طریق آن شبکه‌ها به اشتراک گذاشته و یا انتقال می‌دهند[۲]. تصاویر معمولا دارای افزونگی مکانی بالا و همبستگی زیاد در میان پیکسل‌ها هستند. این مسائل باعث می‌شود که استانداردهای رمزگذاری سنتی، زمان زیادی برای رمزنگاری نیاز داشته و کیفیت رمزنگاری نیز پایین باشد. هر یک از طرح‌های رمزگذاری تصویر ارائه شده دارای قدرت و ضعف خاص خود هستند. بنابراین به دلیل افزایش تأثیر الگوریتم های رمزنگاری بر زندگی روزمره و اهمیت ویژه رمزگذاری تصویر در این میان، و با توجه به کاربردها و سخت‌افزارهای جدید و روش‌های مقابله با آن‌ها، نیاز به الگوریتم‌ها و روش‌های بهینه‌تری احساس می‌شود و انجام تحقیقات علمی در زمینه رمزگذاری تصویر هرچه بیشتر ضروری به نظر می‌رسد. رمزنگاری‌های مبتنی بر آشوب به دلیل ویژگی‌های ذاتی سیستم‌های آشوب مانند ساختار ساده، فرسایش و حساسیت بالا به مقادیر اولیه و پارامترهای کنترل، برای رمزگذاری تصویر مناسب هستند[۳]. مقایسه روش‌های رمزگذاری تصویر با استفاده از یک سری معیارهای عملکردی خاص انجام می‌شود. برجسته‌ترین این معیارها NPCR، UACI، KA، HA، CC، IE، NA و ET هستند[۴].

در اکثر مقالات ارائه شده، نتیجه به‌دست‌آمده برای ارزیابی تصویر دارای مشکلاتی بوده است. عمده‌ترین این مشکلات که به‌عنوان معایب مطرح می‌شوند عبارت‌اند از:

- طول کلید رمزگذاری کوتاه هست.
- کلید رمزگذاری حساسیت زیادی نسبت به تغییر حداقل بیت ندارد.
- ضریب همبستگی تصویر رمزگذاری شده در حد مطلوب کاهش نیافته است.
- آنتروپی اطلاعات تصویر رمزگذاری شده خیلی نزدیک به مقدار ایده‌آل عدد ۸ نیست.
- اختلاف تصویر رمزگذاری شده با تصویر اصلی، خیلی زیاد نیست.

سایر معیارهای ارزیابی که به عنوان مشکلات روش‌های رمزگذاری موجود مطرح نشدند، به‌عنوان مزایای این روش‌ها می‌باشند.

در این مقاله، بنیاد روش پیشنهادی ما بر اساس نگاشت آشوب بوده است که در عین حال سعی در برطرف کردن مشکلات روش‌های قبلی داریم و به صورت کامل در بخش‌های بعدی توضیح داده شده است. اهداف کلی مقاله ما عبارت‌اند از:

- اختلاف تصویر رمزگذاری شده با تصویر اصلی، نزدیک به ۱۰۰ درصد باشد.
- شباهت تصویر رمزگشایی‌شده با تصویر اصلی، نزدیک به ۱۰۰ درصد باشد.
- آنتروپی اطلاعات تصویر رمزگذاری شده خیلی نزدیک به عدد ایده‌آل ۸ باشد.

این روش پیشنهادی در حقیقت ادامه روشی است که ما در مقاله[۵] ارائه دادیم. در آن مقاله، رمزگذاری بر روی یک تصویر انجام می‌شد و با استفاده از کلیدهای تولیدشده توسط نگاشت آشوب، حوزه انتقال و جابجایی پیکسل‌ها افزایش پیدا می‌کرد. اما در این روش پیشنهادی، به‌جای این‌که یک تصویر را رمزگذاری کنیم طرحی را ارائه داده‌ایم که قادر به رمزگذاری هم‌زمان چهار تصویر را است. به‌جای کلیدهای استفاده‌شده در مقاله قبلی، ما در اینجا از خود تصاویر برای بزرگ‌تر کردن دامنه انتقال و جابجایی پیکسل‌ها استفاده می‌کنیم. این کار با رمزگذاری هم‌زمان چهار تصویر به جای یک تصویر، نه‌تنها منجر به کاهش زمان رمزگذاری و افزایش سرعت آن می‌شود، بلکه پیچیدگی تصویر رمزگذاری شده را نیز به دلیل مخلوط نمودن پیکسل‌های چهار تصویر با همدیگر افزایش می‌دهد.

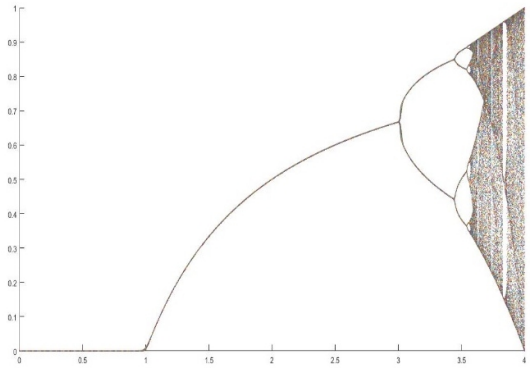
نگاشت لجستیک آشوب

مهم‌ترین ویژگی نگاشت آشوب حساسیت به شرایط اولیه است. اختلافات اندک در شرایط اولیه، نتایج گسترده‌ای را برای چنین سیستم‌های دینامیکی نشان می‌دهد و باعث می‌شود پیش‌بینی طولانی مدت به طورکلی غیرممکن باشد. ویژگی دیگر نگاشت آشوب، تصادفی بودن آن است[۶]. در صورت رعایت شرایط مناسب، نتیجه عملکرد آشوب کاملاً تصادفی است و توالی اعداد شبه تصادفی تولید می‌کند. یکی از پرکاربردترین و ساده‌ترین آشوب‌های غیرخطی، نگاشت لجستیک است. نگاشت لجستیک به‌صورت زیر ارائه‌شده است:

$$X_{n+1} = rX_n(1-X_n) \qquad (۱)$$

هنگامی‌که $r \in (3.57,\ 4)$ است، این نگاشت رفتار آشوب گون دارد. در این معادله $X_n \in (0,\ 1)$ به‌عنوان متغیر نگاشت لجستیک آشوب و r به‌عنوان پارامتر آن نگاشت بوده و n عدد تکرار است.
نمودار دوشاخگی نگاشت لجستیک در شکل ۱ نشان داده شده است. در این شکل نگاشت لجستیک به‌عنوان تابعی از r ترسیم شده است.

این مقاله را به ترتیب زیر ارائه می‌دهیم: در بخش ۲ ما به طور خلاصه مطالعات قبلی در مورد این موضوع را مرور می‌کنیم. در بخش ۳ الگوریتم پیشنهادی را برای رمزگذاری تصویر ارائه کرده و روش رمزگذاری آن را شرح خواهیم داد. در بخش ۴ نیز تحلیل و ارزیابی الگوریتم پیشنهادی و مقایسه آن با سایر الگوریتم‌های مشابه ارائه شده است. سرانجام در بخش ۵ بحث و نتیجه‌گیری آورده شده است.



شکل۱: نمودار دوشاخگی نگاشت لجستیک آشوب

۲- مطالعات مرتبط

محققان، الگوریتم‌های رمزگذاری متنوعی را که مبتنی بر نگاشت‌های آشوب است، در سال‌های گذشته در مطالعات مختلف برای رمزگذاری تصویر معرفی کرده‌اند. خلاصه‌ای از برخی الگوریتم‌های معرفی شده به شرح زیر است:

پریک و همکاران [۷] از دو نگاشت لجستیک و یک کلید خارجی برای رمزگذاری تصویر استفاده کرده‌اند. شرایط اولیه نگاشت‌های لجستیک از کلید خارجی گرفته شده است. کلید مخفی هر بار پس از رمزگذاری بلوکی از تصویر شامل شانزده پیکسل تغییر می‌کند. بنابراین، کشف یک رمز مخفی برای یک مهاجم دشوار است. بااین‌حال این روش، نسبت به تصاویر ورودی حساس نیست.

بهنیا و همکاران [۸] نقشه آشوب یک‌بعدی را با شبکه نقشه همراه برای رمزگذاری تصویر ترکیب نموده‌اند. این ترکیب فضای کلیدی بزرگ و امنیت سطح بالایی را فراهم می‌کند. بااین‌حال، این روش حساسیت کمی نسبت به تصویر ورودی دارد زیرا شرایط اولیه نقشه‌های آشوب به تصویر ورودی وابسته نیستند.

گائو و همکاران [۹] برای کاهش زمان پیش‌بینی نسبت به تکنیک‌های رمزنگاری تصویر مبتنی بر نگاشت‌های آشوب، نگاشت فوق آشوب را در رمزگذاری تصویر پیاده سازی کرده‌اند. در این تکنیک، از تغییر شکل ماتریس استفاده می‌شود تا پیکسل‌های یک تصویر ورودی را تغییر دهد. این روش فضای کلید بهتر و امنیت بالایی را نیز فراهم می‌کند.

میرزائی و همکاران [۱۰] روشی جدید با یک الگوریتم ساده ارائه داده‌اند. روش پیشنهادی آن‌ها از سه دنباله آشوب غیرخطی که به‌عنوان نگاشت‌های لجستیکی سه‌بعدی شناخته می‌شوند، برای رمزگذاری تصویر استفاده می‌کند. از این سه دنباله تصادفی استخراج شده برای تغییر مکان سطر و ستون پیکسل‌های تصویر استفاده می‌شود. سرانجام تغییر مقدار پیکسل‌ها با استفاده از سومین دنباله تصادفی و عمل XOR به صورت ستون به ستون انجام می‌شود.

کوآر و همکاران[۱۱] یک نگاشت فوق آشوب را با استفاده از یک رویکرد بهینه‌سازی تکاملی چند هدفه، بهینه‌سازی کرده‌اند. برای به دست آوردن پارامترهای بهینه یک نگاشت فوق آشوب و فاکتورهای رمزگذاری، از یک بهینه سازی چند منظوره مبتنی بر جستجوی محلی (DLS-MO) استفاده شده است. بعد از آن، با استفاده از پارامترهای بهینه، یک نگاشت فوق آشوب کلیدهای مخفی را توسعه می‌دهد. سپس، از این کلیدهای مخفی برای انجام تغییر مکان و انتشار بر روی یک تصویر ساده برای توسعه تصویر رمزگذاری شده استفاده می‌شود.

کارلا و همکاران[۱۲] معتقد بودند استفاده از دو نگاشت آشوب باعث بهتر شدن امنیت تصویر رمزگذاری می‌شود. لذا در الگوریتم پیشنهادی خود از دو نگاشت آشوب Tent و Logistic استفاده کرده‌اند. رمزگذاری تصویر با استفاده از نگاشت آشوب Tent انجام می‌شود، که بر روی تصویری که با استفاده از نگاشت Logistic رمزگذاری شده است، اعمال می‌گردد. طرح رمزگذاری پیشنهادی آن‌ها به دلیل استفاده از دو نگاشت آشوب به جای یک نقشه، فضای کلیدی نسبتاً بزرگی دارد.

لیو و همکاران[۱۳]، الگوریتم رمز گذاری جدید آشوب برای رمزگذاری تصویر بر اساس نگاشت بهبود یافته Baker و نگاشت Logistic ارائه داده‌اند. با توجه به محدوده آشوب محدود و آسیب‌پذیری یک نگاشت فوق آشوب، آن‌ها از نگاشت آشوب دو بعدی بیکر برای کنترل پارامترهای سیستم و متغیر وضعیت نگاشت آشوب لجستیک استفاده کردند. فرآیند رمزگذاری الگوریتم پیشنهادی آن‌ها از دو قسمت اصلی تشکیل‌شده است: جایگشت و جایگزینی.

گائو و همکاران[۱۴] یک طرح رمزگذاری تصویر را بر اساس مجموعه مندلبرات ارائه داده‌اند. برای بررسی امکان‌پذیر بودن مجموعه مندلبرات تعمیم یافته در طرح رمز گذاری، از ساده‌ترین الگوریتم رمزگذاری یعنی دو دور XOR استفاده‌شده است. در الگوریتم پیشنهادی آن‌ها از کلیدهای یک‌بار مصرف استفاده شده است که مشکل انتقال کلیدهای مخفی را تا حدودی کاهش داده است. فضای کلیدی این طرح نه تنها بزرگ است بلکه به صورت پویا نیز قابل تغییر است.

جواد احمد و همکاران[۲] در مقاله خود روشی را پیشنهاد دادند که در آن ابتدا تصویر ورودی به تعدادی بلوک تقسیم می‌شود و ضرایب همبستگی هر بلوک به‌صورت جداگانه محاسبه می‌گردد. در ادامه بلوکی که ضریب همبستگی بالاتری دارد از بین آن‌ها استخراج می‌شود. سپس با اعداد تصادفی تولید شده توسط skew tent map عمل XOR را انجام می‌دهند. درنهایت مکان پیکسل‌های کل تصویر از طریق دو دنباله تصادفی تولیدشده از یک نگاشت آشوب TD-ERCS جابه‌جا می شوند. سرانجام تصویری که تولید می‌شود تصویر نهایی رمزگذاری شده خواهد بود.

الگوریتمی برای رمزگذاری تصویر در مقاله[۱۵] توسط دیویا و همکاران ارائه شده که مبتنی بر ترکیبی از IWT و DNA و نگاشت آشوب است. الگوریتم پیشنهادی آن‌ها شامل دو مرحله است: مرحله اول شامل دو گام است که برای تغییر مقدار پیکسل‌ها استفاده می‌شود؛ مرحله دوم نیز مرحله جابجایی مکان پیکسل‌ها است. اولین مرحله از

جابجایی مکان پیکسل‌ها، تغییرات بلوک اولیه و به دنبال آن تغییر سطر و ستون به‌عنوان گام دوم مرحله اول است. سپس پیکسل‌هایی که در گام‌های اول و دوم از مرحله اول جابه‌جا شده‌اند دوباره به‌صورت بیتی جابه‌جا می شوند. در مرحله دوم که مرحله تغییر مقدار پیکسل‌ها است عملیات تغییر مقدار بر اساس کدگذاری DNA و عملیات DNA XOR است. درنهایت تصویر حاصل، تصویر رمزگذاری شده در الگوریتم پیشنهادی آن‌ها است.

اخیراً با ترکیب نظریه آشوب و برخی از تئوری‌های میان‌رشته‌ای، تکنیک‌های رمزگذاری تصویر مختلفی پیشنهاد شده است[۱۶]. برای نمونه فناوری رمزگذاری DNA در زیست شناسی، در زمینه رمزگذاری تصاویر نیز به کار رفته است[۱۷]. همچنین با به کارگیری شبکه‌های عصبی، الگوریتم جدید رمزگذاری تصویر طراحی شده است[۱۸]. با بلوغ و توسعه فن آوری کوانتوم، الگوریتم رمزگذاری تصویر همراه با کوانتوم و نظریه آشوب، زمینه جدیدی برای رمزگذاری تصویر شده است[۱۹]. از کاربردهای DCT و DWT در زمینه رمزگذاری تصویر استفاده شده است[۲۰].

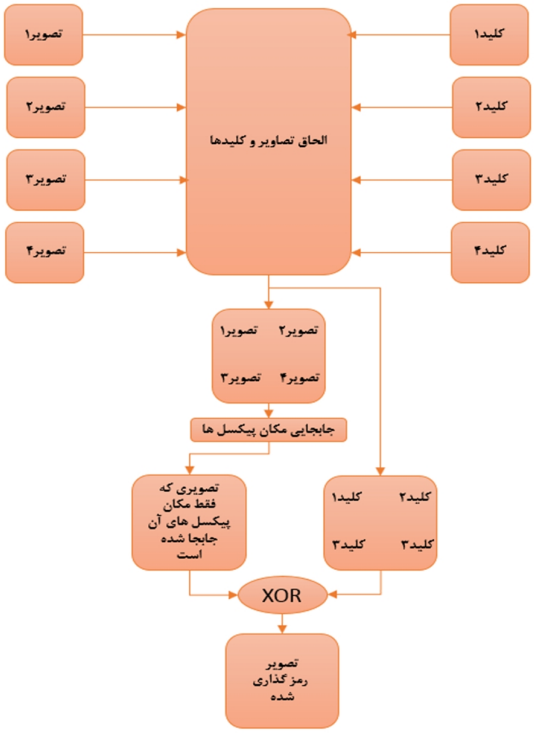
۳- الگوریتم پیشنهادی برای رمزگذاری تصویر

در الگوریتم پیشنهادی ما چهار تصویر به‌صورت هم‌زمان رمزگذاری می شود. با توجه به این‌که تمام تصاویر استاندارد بررسی‌شده در سایر مقالات به شکل مربع یعنی در ابعاد ۲۵۶×۲۵۶ یا در مواردی خیلی کم در ابعاد ۵۱۲×۵۱۲ و یا به‌ندرت در ابعاد ۱۰۲۴×۱۰۲۴ می‌باشند، لذا ما نیز در روش پیشنهادی خود تعداد عکس‌ها را طوری انتخاب کردیم تا شکل مربع بودن تصاویر حفظ شود تا هم بتوانیم جابجایی مکان پیکسل ها را به راحتی انجام دهیم و هم بتوانیم عملکرد الگوریتم پیشنهادی خود را با سایر مقالات مشابه مقایسه کنیم.

اگر تعداد تصاویر بیشتری انتخاب می‌کردیم ناچار بودیم به خاطر این‌که حالت مربع حفظ شود، شانزده تصویر انتخاب کنیم تا درمجموع یک تصویر واحد ۱۰۲۴×۱۰۲۴ تولید شود و چون این اندازه تصویر در سایر مقالات خیلی کم و به ندرت استفاده شده است، در مقایسه به مشکل برمی‌خوردیم. ازاین‌رو از انتخاب تعداد بیشتر از چهار تصویر خودداری کردیم. در مورد تعداد تصاویر کمتر از چهار نیز یک حالت وجود دارد و آن این که تنها می‌توان یک تصویر را انتخاب کرد تا حالت مربعی حفظ شود و این مورد نیز چون شامل روش پیشنهادی ما نمی شد، لذا همان تعداد چهار تصویر بهترین انتخاب بود. هیچ مقاله‌ای تصویری استفاده نکرده که دارای ابعاد غیرمساوی باشند. ما به‌جای این‌که یک تصویر را در هر لحظه رمزگذاری کنیم، چهار تصویر را رمزگذاری می‌کنیم. این شیوه رمزگذاری باعث می‌شود پیکسل‌های چهار تصویر کاملاً با یکدیگر مخلوط شده و هر تصویر بتواند از پیکسل‌های سایر تصاویر نیز استفاده کند. در واقع به‌جای استفاده از کلیدهای اضافی و یا تصاویر کمکی، از خود تصاویر برای رمزگذاری یکدیگر کمک گرفته می‌شود. وقتی از پیکسل‌های سایر تصاویر استفاده می‌شود در حقیقت فضای بزرگ‌تر و پیکسل‌های بیشتری برای انتخاب وجود دارد و این امنیت تصویر رمزگذاری شده ما را بیشتر می‌کند. در عوض هرچقدر انتخاب تعداد پیکسل‌ها و فضای آن‌ها محدودتر باشد، کار مهاجم آسان‌تر و رمزگشایی به‌مراتب راحت‌تر می‌شود. درنهایت در هر بار اجرای الگوریتم، به‌جای یک تصویر، چهار تصویر رمزگذاری می شود که با بررسی معیارهای ارزیابی تصویر در بخش بعدی، نتایج به‌دست‌آمده کیفیت روش پیشنهادی ما را تضمین می‌کنند.

ترتیب چینش تصاویر برای تشکیل یک تصویر واحد هیچ نظم خاصی ندارد. ما در این مقاله هشت تصویر استاندارد انتخاب کرده‌ایم که در اکثر مقالات معتبر از آن‌ها استفاده می شود. به صورت تصادفی آن‌ها را در دو گروه چهارتایی دسته‌بندی کردیم. حالت‌های مختلف این چیدمان در معیارهای مختلف ارزیابی تصاویر بررسی شدند. خروجی حاصل از تغییر چیدمان تفاوت چندانی با سایر حالت‌ها ندارد و در خیلی موارد نیز خروجی آن‌ها کاملاً با هم برابر هستند.

تصویر شکل ۲ بلوک دیاگرام الگوریتم رمزگذاری پیشنهادی و نحوه ترتیب رمزگذاری تصویر را در الگوریتم پیشنهادی نشان می‌دهد. در الگوریتم پیشنهادی بعد از این‌که چهار تصویر با هم الحاق می شوند و یک تصویر واحد ایجاد می‌گردد، تصویر حاصل به بلوک‌هایی (در الگوریتم پیشنهادی ما ۱×۱) تقسیم می‌شود. سپس با استفاده از مرتب‌سازی اعداد تولیدشده توسط نگاشت آشوب، بلوک‌های تصویر بر اساس همان ترتیب جابجایی، جابجا می‌شوند. عملیات الحاق بر روی کلیدهای تولیدشده نیز انجام می‌گردد. درنهایت عمل XOR مابین دو تصویر اعمال و تصویر رمزگذاری شده به دست می‌آید.



شکل ۲: بلوک دیاگرام الگوریتم رمزگذاری پیشنهادی

در الگوریتم پیشنهادی به‌جای این‌که در هر مرحله یک تصویر وارد سیستم رمزگذاری شود هم‌زمان چهار تصویر وارد سیستم شده و عملیات رمزگذاری بر روی این‌ها به‌صورت هم‌زمان اعمال و تصاویر رمزگذاری شده به مقصد ارسال می‌شود. مراحل انجام به ترتیب زیر هست:

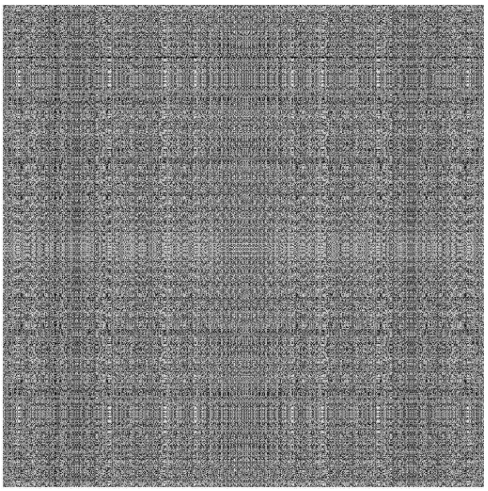
۱- ابتدا چهار تصویر استاندارد در اندازه ۲۵۶×۲۵۶ وارد سیستم رمزگذاری می‌شود.

۲- عملیات الحاق بر روی تصاویر اعمال‌شده و یک تصویر در ابعاد ۵۱۲×۵۱۲ مانند شکل شماره ۳ تولید می‌شود.

شکل۳: الحاق چهار تصویر ورودی و تولید یک تصویر جدید

۳- با استفاده از نگاشت لجستیک آشوب، دو سری از اعداد هرکدام به تعداد ۵۱۲ عدد تولید می شود و یکی از آن‌ها برای جابجایی سطر و دیگری برای جابجایی ستون استفاده می‌شود.

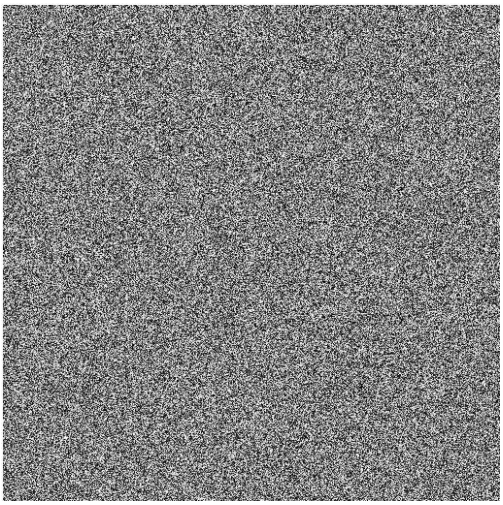
۴- با استفاده از مرتب‌سازی اعداد تولیدشده و ثبت مکان آن‌ها، مکان پیکسل‌ها در تصویر مانند شکل شماره ۴ جابجا می‌شود.



شکل۴: جابجایی مکان پیکسل‌های تصویر

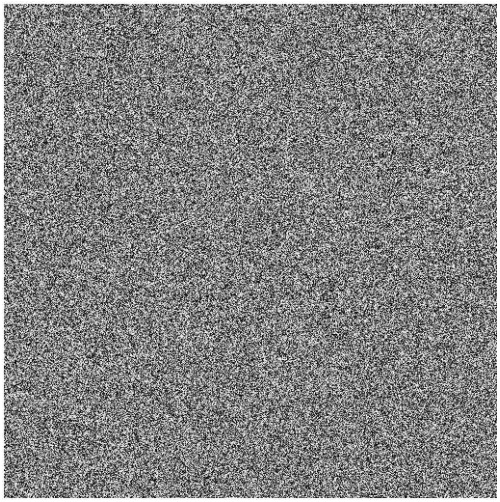
۵- چهار سری دیگر از اعداد تو سط نگا شت لج ستیک آ شوب تولید شده و چهار تصویر کلیدی در ابعاد۲۵۶×۲۵۶ ایجاد می‌گردد.

۶- با الحاق چهار تصویر کلیدی مرحله قبل، یک تصویر کلیدی در ابعاد ۵۱۲×۵۱۲ مانند شکل شماره ۵ تولید می‌شود که به عنوان کلید اصلی از آن استفاده می‌کنیم.



شکل۵: الحاق چهار تصویر کلیدی و تولید یک کلید جدید

در نهایت عمل XOR بین تصویر و کلید اصلی انجام شده و تصویر رمزگذاری شده که شامل چهار تصویر هست مانند شکل شماره ۶ تولید می‌گردد.



شکل۶: تصویر رمزگذاری شده

۴- تحلیل و ارزیابی الگوریتم پیشنهادی

در این بخش با انجام و تحلیل چند آزمایش کارایی الگوریتم نشان داده می‌شود. این آزمایش‌ها در چند بخش انجام خواهد شد:

ابتدا در قسمت عکس‌های آزمایش شده و ارزیابی بصری، تصاویر استانداردی که در این مقاله استفاده شده، به همراه تصاویر رمزگذاری شده آن‌ها و نمودار هیستوگرام آن‌ها نشان داده شده است. سپس تحلیل هیستوگرام صورت گرفته و مقدار خی۲ برای تصاویر مورد آزمایش به دست آمده است. بعد از آن تعداد پیکسل‌های متفاوت در دو تصویر و تغییر شدت متوسط بین آن‌ها توسط NPCR و UACI محاسبه می‌شود. معیارهای آنتروپی و ضریب همبستگی به ترتیب برای محاسبه میزان توزیع مقادیر پیکسل‌ها و نحوه ارتباط پیکسل‌ها در تصاویر اصلی و رمزگذاری شده استفاده شده است. سپس فضای کلید و حساسیت به کلید تحلیل‌شده است. قسمت حملات رمزنگاری از دیگر مواردی است که مقاومت تصاویر در مقابل حملات را بررسی نموده است. در آخر نیز زمان اجرای الگوریتم محاسبه و با الگوریتم‌های مشابه دیگر مقایسه شده است.

عکس‌های آزمایش‌شده

تصاویر ارزیابی شده در مقاله ما شامل هشت تصویر استاندارد هست. این تصاویر به کار گرفته شده عبارت‌اند از:

Lena، Elaine، Couple، Baboon، Boat، Peppers، cameraman، zelda. همه این تصاویر در قالب یک عکس کامل در شکل شماره ۷ نشان داده شده است.

ارزیابی بصری

برای انجام این آزمایش هشت تصویر خاکستری با ابعاد ۲۵۶×۲۵۶ انتخاب شده‌اند. تصاویر در دو دسته چهارتایی گروه‌بندی شده‌اند. گروه اول شامل تصاویر Lena، Elaine، Couple و Peppers هست. گروه دوم تصاویر Baboon، Boat، Cameraman و Zelda را در بردارد. ابعاد هر گروه تصویر ۵۱۲×۵۱۲ هست. شکل شماره ۸ تصاویر اصلی و رمز شده آن‌ها را به همراه هیستوگرام آن‌ها نشان می‌دهد.

تحلیل هیستوگرام

یک الگوریتم رمزنگاری خوب، بایستی تصویر را به‌گونه‌ای در هم بریزد که ویژگی‌های آن به صورت بصری قابل تشخیص نبا شد. همچنین با مقایسه تصویر رمز با تصویر اصلی نبایستی هیچ نوع اطلاعاتی از تصویر رمز، قابل دریافت باشد. حتی با تغییرات شدید در شدت روشنایی پیکسل‌های تصویر اصلی، بایستی تصویر اصلی و تصویر رمز به صورت بصری متمایز باشند. لذا برای اثبات نتیجه آزمون بصری از تحلیل هیستوگرام و آنالیزهای مرتبط مانند آزمون خی ۲ استفاده می‌کنیم. هیستوگرام تصویر نموداری است که توسط آن تعداد پیکسل‌های هر سطح روشنایی در تصویر ورودی مشخص می‌شود. هر یک از پیکسل‌های تصویر خاکستری با ۲۵۶ سطح روشنایی مقداری در بازه ۰ تا ۲۵۵ می‌توانند داشته باشند. X^2 نیز به‌صورت زیر تعریف می‌شود:

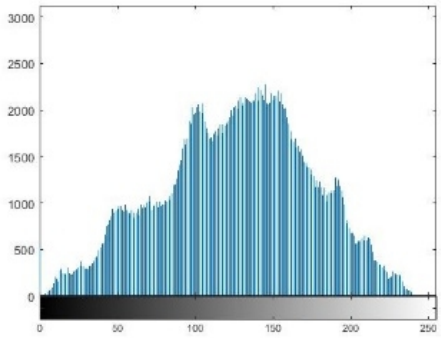
$$X^2 = \sum_{i=0}^{N-1} \frac{(O_i - e_i)^2}{e_i} \quad (۲)$$

در این معادله، N تعداد سطوح رنگ را مشخص می‌کند (در مورد تصویر ما ۲۵۶) ، O_i مشاهدات (فرکانس هر سطح رنگ i) و e_i مقدار توزیع یکنواخت است. این مقدار برای تمام تصاویر در مقیاس خاکستری با اندازه ۲۵۶ × ۲۵۶ برابر۲۵۶ است و برای کلیه تصاویر خاکستری با اندازه ۵۱۲ × ۵۱۲ برابر۱۰۲۴ است. مقادیر X^2 به دست آمده از هشت تصویر آزمایش شده در جدول شماره ۱ نشان داده شده است. مقادیر پایین‌تر خی ۲ نیز نشان دهنده این است که مشاهدات معمولی چقدر به فرضیه‌ای که ساخته‌ایم نزدیک است و مقادیر بالاتر نشان‌دهنده مقدار فاصله از فرضیه هست.

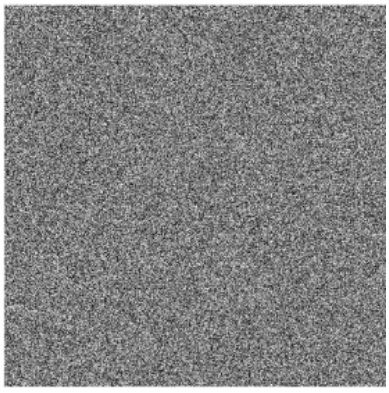
شکل۷. تصاویر استاندارد ارزیابی‌شده در الگوریتم پیشنهادی

الف. تصاویر اصلی (گروه ۱)

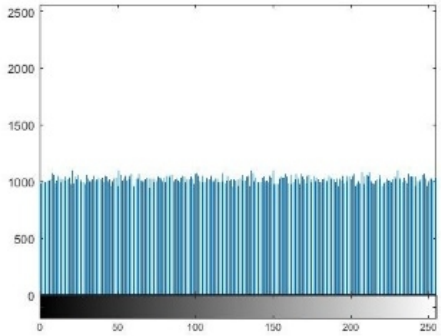
ب. هیستوگرام تصاویر اصلی (گروه ۱)



ج. تصاویر رمزگذاری شده (گروه۱)

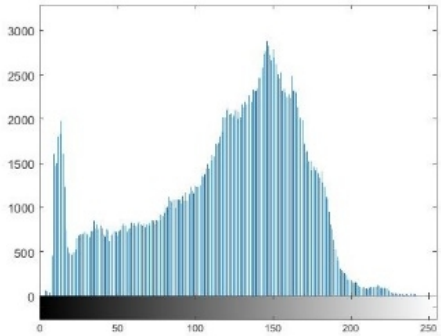


د. هیستوگرام تصاویر رمزگذاری شده (گروه۱)

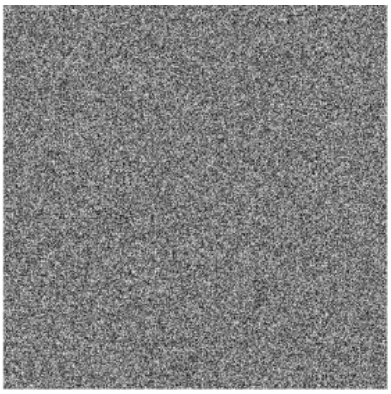


ه. تصاویر اصلی (گروه ۲)

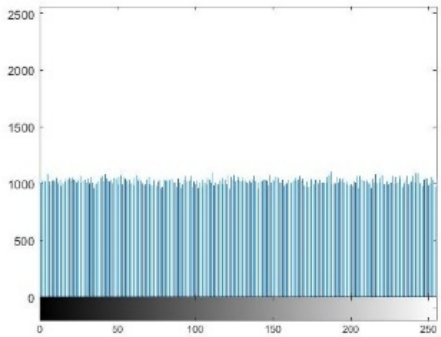
و. هیستوگرام تصاویر اصلی (گروه ۲)



ز. تصاویر رمزگذاری شده (گروه ۲)



ح . هیستوگرام تصاویر رمزگذاری شده (گروه ۲)



شکل۸. دو گروه از تصاویر به همراه تصاویر رمز شده و هیستوگرام آن‌ها

جدول۱. نتایج خی ۲ در الگوریتم پیشنهادی و مقایسه با سایر الگوریتم‌های مشابه

نام تصویر	الگوریتم	اندازه تصویر	خی ۲
Lena	پیشنهادی	۲۵۶×۲۵۶	۲۲۶/۲۴۰۲
	[۱۱]	۲۵۶×۲۵۶	۲۵۵/۱۲
	[۲۱]	۲۵۶×۲۵۶	۲۵۲/۵۳
	[۱۱]	۵۱۲×۵۱۲	۲۴۴/۲۸۱۳
	[۲۲]	۲۵۶×۲۵۶	۲۴۲/۸۲۸۱
Elaine	پیشنهادی	۲۵۶×۲۵۶	۲۲۶/۲۴۰۲
	[۲۳]	۲۵۶×۲۵۶	۲۶۶/۶۸
Couple	پیشنهادی	۲۵۶×۲۵۶	۲۲۶/۲۴۰۲
Peppers	پیشنهادی	۲۵۶×۲۵۶	۲۲۶/۲۴۰۲
	[۱۱]	۲۵۶×۲۵۶	۲۶۰/۳۸
	[۲۱]	۲۵۶×۲۵۶	۲۶۰
	[۲۴]	۵۱۲×۵۱۲	۲۵۵/۸۷۱۲
Zelda	پیشنهادی	۲۵۶×۲۵۶	۲۱۶/۷۶۱۷
Cameraman	پیشنهادی	۲۵۶×۲۵۶	۲۱۶/۷۶۱۷
	[۲۱]	۲۵۶×۲۵۶	۲۴۳
	[۲۴]	۵۱۲×۵۱۲	۲۴۷/۲۳۱۲
Boat	پیشنهادی	۲۵۶×۲۵۶	۲۱۶/۷۶۱۷
	[۱۱]	۲۵۶×۲۵۶	۲۷۲/۴۶
	[۲۴]	۵۱۲×۵۱۲	۲۴۸/۶۷۵۱
	[۲۲]	۵۱۲×۵۱۲	۲۴۸/۰۲۵۴
	[۲۳]	۲۵۶×۲۵۶	۲۲۱/۵۰
Baboon	پیشنهادی	۲۵۶×۲۵۶	۲۱۶/۷۶۱۷
	[۲۱]	۲۵۶×۲۵۶	۲۰۳
	[۲۴]	۵۱۲×۵۱۲	۲۵۶/۴۴۱۲

در مورد الگوریتم پیشنهادی ما، میانگین نتایج ۲۲۱/۵۰۰۹ است که این مقدار در توزیع کاملاً یکنواخت عدد۰ است. به این معنی که برای همه ۲۵۶ سطح رنگ در کل چهار تصویر تجمیع شده، در مشاهدات ۲۲۱ خطا داریم و برای هر سطح رنگ، مقدار به دست‌آمده به طور متوسط کمتر از عدد ۱ است. نتیجه به دست آمده نشان دهنده توزیع یکنواخت سطح رنگ در تصویر رمزگذاری است که نتیجه خیلی خوبی است. با توجه به جدول ۱ و بررسی نتایج آزمون خی ۲ و مقایسه هشت تصویر رمزگذاری شده در الگوریتم پیشنهادی ما با سایر الگوریتم‌های مشابه، همان طور که در جدول نیز مشخص است، از بین هشت تصویر رمزگذاری شده، نتیجه آزمون خی ۲ برای هفت تصویر در الگوریتم پیشنهادی، بهتر از سایر الگوریتم‌ها بوده است. این نشان دهنده برتری الگوریتم پیشنهادی ماست.

(Number of Pixels Change Rate) NPCR

تعداد پیکسل‌هایی را که در دو تصویر یکسان نیستند تعریف می‌کند. این دو تصویر می‌تواند دو تا تصویر با کلیدهای متفاوت رمزگذاری که فقط در یک بیت با هم اختلاف دارند، باشند. مقادیر بالاتر یعنی نزدیک به ۱۰۰ درصد برای NPCR نشان دهنده مقدار تفاوت بین دو تصویر رمزگذاری شده هست. پیکسل‌های دو تصویر رمزگذاری شده که فقط در یک بیت کلید برای رمزگذاری متفاوت هستند با هم نظیر به نظیر مقایسه می‌شوند و درصد تفاوت بین آن‌ها به دست می‌آید. اگر عدد به دست آمده ۱۰۰ درصد باشد یعنی پیکسل‌های دو تصویر کاملاً با هم متفاوت هستند. بر اساس رابطه شماره (۳) مقدار NPCR به دست می آید.

$$NPCR = \frac{1}{M \times N \times K} \times \sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{k=1}^{K} Q(C_{m,n,k}, C'_{m,n,k}) \times 100(\%) \quad (۳)$$

M، N و K در رابطه (۳) اندازه ماتریس تصویر ($K=3$ برای تصویر رنگی و $K=1$ برای مقیاس خاکستری) است. همچنین، C و C' دو تصویری که با کلیدهای متفاوت رمزگذاری شده‌اند، می‌باشند. هر زمان که هر دو پیکسل در یک مکان مشابه، مساوی باشند عملکرد Q برابر با صفر است و در موارد دیگر یک است.

Unified Averaged Changed Intensity (UACI)

به عنوان تغییر شدت متوسط، بین دو تصویر در همان موقعیت تعریف شده است. این معیار فاصله بین دو پیکسل را تعیین می‌کند درحالی‌که NPCR فقط یک معیار برای اندازه‌های نابرابر است. معادله (۴) UACI را تعریف می‌کند.

(۴)

$$UACI = \frac{1}{M \times N \times K \times L} \times \sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{k=1}^{K} |C_{m,n,k} - C'_{m,n,k}| \times 100(\%)$$

در معادله فوق، L بالاترین سطح رنگ است. M، N و K مانند معادله (۳) هستند. نتایج در جدول شماره ۲ نشان داده‌شده است.

جدول۲. مقایسه نتایج به دست آمده در معیارهای NPCR و UACI

نام تصویر	الگوریتم	اندازه تصویر	NPCR	UACI
Lena	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۱۸۵	۳۳/۴۹۰۴
	[۲۵]	۵۱۲×۵۱۲	۹۹/۶۰۳۷	۳۳/۴۷۲۵
	[۱۱]	۲۵۶×۲۵۶	۹۹/۶۹	۳۳/۴۷
	[۲۶]	۲۵۶×۲۵۶	۹۹/۶۳۳۷	۲۸/۸۴۳۲
	[۲۱]	۲۵۶×۲۵۶	۹۹/۶۱	۳۳/۴۹
	[۲۷]	۲۵۶×۲۵۶	۹۹/۶۱۰	۳۳/۴۶۳
	[۲۳]	۲۵۶×۲۵۶	۹۹/۶۰۳۷	۳۳/۴۶۰۶
Elaine	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۱۸۵	۳۳/۴۹۰۴
	[۲۳]	۲۵۶×۲۵۶	۹۹/۶۰۶۷	۳۳/۴۵۰۴
Couple	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۱۸۵	۳۳/۴۹۰۴
Peppers	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۱۸۵	۳۳/۴۹۰۴
	[۱۱]	۲۵۶×۲۵۶	۹۹/۵۹	۳۳/۵۰
	[۲۳]	۲۵۶×۲۵۶	۹۹/۶۰۴۸	۳۳/۴۵۳۹
Zelda	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۰۶۷	۳۳/۵۰۷۰
Cameraman	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۰۶۷	۳۳/۵۰۷۰
	[۲۳]	۲۵۶×۲۵۶	۹۹/۶۰۱۷	۳۳/۴۳۹۹
Boat	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۰۶۷	۳۳/۵۰۷۰
	[۱۱]	۲۵۶×۲۵۶	۹۹/۶۴	۳۳/۴۹
	[۲۲]	۵۱۲×۵۱۲	۹۹/۶۴۱۴	۳۳/۵۴۰۵
	[۲۳]	۲۵۶×۲۵۶	۹۹/۶۱۷۶	۳۳/۴۹۴۶
Baboon	پیشنهادی	۲۵۶×۲۵۶	۹۹/۶۰۶۷	۳۳/۵۰۷۰
	[۲۵]	۵۱۲×۵۱۲	۹۹/۵۹۳۰	۳۳/۴۲۱۰

با توجه به جدول ۲ می‌توان نتیجه گرفته که تفاوت تصویری که با کلید اصلی رمزگذاری شده و تصویری که با کلیدی که فقط در یک بیت با کلید اصلی متفاوت است رمزگذاری شده، در الگوریتم پیشنهادی خیلی نزدیک به عدد ۱۰۰ درصد بوده و این نشان دهنده عملکرد خوب الگوریتم پیشنهادی است. با توجه به دو معیار NPCR و UACI که ارتباط نزدیکی با یکدیگر دارند و نتایج به دست آمده و مقایسه آن‌ها با سایر الگوریتم‌های مشابه و با توجه به این‌که الگوریتم پیشنهادی ما برای تصاویر زیادی تست شده و نتیجه همه آن‌ها تقریباً بهتر از الگوریتم‌های مشابه بوده است، می‌توان نتیجه گرفت که الگوریتم پیشنهادی ما بهتر از سایر الگوریتم‌ها عمل نموده است.

آنتروپی

نظریه اطلاعات یک نظریه ریاضی از مخابرات داده و ذخیره‌سازی است که در سال ۱۹۴۹ توسط شانون معرفی شد[۲۸]. شانون آنتروپی را به‌عنوان معیاری از میزان اطلاعات در منبع معرفی کرد. آنتروپی یک مفهوم علمی و همچنین یک ویژگی فیزیکی قابل‌اندازه‌گیری است که بیشتر با حالت بی‌نظمی، تصادفی یا عدم اطمینان همراه است. امروزه نظریه اطلاعات مدرن با موضوعات تصحیح خطا، فشرده‌سازی اطلاعات، رمزنگاری، و سامانه‌های مخابراتی در ارتباط است. آنتروپی یک تصویر تخمینی از تصادفی بودن آن است. آنتروپی شانون $H(m)$ یک منبع پیام s به‌صورت زیر تعریف می‌شود:

$$H(m)=\sum_{i=0}^{2^{n-1}}P(m_i)\log_2\frac{1}{P(m_i)} \quad (۵)$$

که $p(m_i)$ معرف احتمال سمبل m_i است. به طور کلی یک منبع اطلاعات عملی به ندرت پیام‌های تصادفی تولید می‌کند و میزان آنتروپی آن کوچک‌تر از مقدار ایده‌آل ۸ است. با این وجود هنگامی‌که یک تصویر خاکستری رمزگذاری می شود، آنتروپی آن تصویر بایستی نزدیک به مقدار ایده‌آل ۸ باشد. مقایسه میزان آنتروپی الگوریتم پیشنهادی با سایر الگوریتم‌ها در جدول شماره ۳ نمایش داده‌شده است.

ضریب همبستگی

در یک تصویر معمولی هر پیکسل شباهت زیادی با پیکسل‌های مجاورش دارد. ضریب همبستگی در محورهای افقی، عمودی و مورب رابطه بین دو مقدار مجاور را نشان می‌دهد. روابط ۶ تا ۱۱ چگونگی محاسبه‌ی این معیار را نشان می‌دهد:

$$r_{x,y}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (۶)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x-E(x_i)\right)^2 \quad (۷)$$

$$D(y)=\frac{1}{N}\sum_{i=1}^{N}\left(y-E(x_i)\right)^2 \quad (۸)$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \quad (۹)$$

$$E(y)=\frac{1}{N}\sum_{i=1}^{N}y_i \quad (۱۰)$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \quad (۱۱)$$

که در این روابط x و y مقادیر سطح خاکستری دو پیکسل مجاور است و $r_{x,y}$ ضریب همبستگی است. $E(x)$ مقدار میانگین است، $D(x)$ مقدار واریانس است و $\operatorname{cov}(x,y)$ ، مقدار کوواریانس است.

در تمام الگوریتم‌های رمزگذاری به دنبال روشی هستیم که میزان همبستگی هر پیکسل با پیکسل‌های مجاورش به کمترین میزان خود برسد. کاهش میزان همبستگی نشان‌گر بهبود عملکرد سیستم رمزنگاری است.

مقادیر محاسبه شده این پارامتر برای تصاویر دو گروه که شامل هشت تصویر استاندارد است، مربوط به سه محور با وضعیت سایر الگوریتم‌ها در جدول ۴ مقایسه می‌شود.

شکل ۹ همان تجزیه و تحلیل را برای تصاویر اصلی و رمزگذاری شده نشان می‌دهد.

جدول۳. مقایسه آنتروپی تصاویر مختلف در الگوریتم پیشنهادی با سایر الگوریتم‌ها

نام تصویر	الگوریتم	اندازه تصویر	آنتروپی
Lena	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۲۵]	۵۱۲×۵۱۲	۷/۹۹۹۴
	[۱۱]	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۲۶]	۲۵۶×۲۵۶	۷/۹۹۷۷
	[۲۱]	۲۵۶×۲۵۶	۷/۹۹۷۴
	[۲۷]	۲۵۶×۲۵۶	۷/۹۹۹۳
	[۲۴]	۵۱۲×۵۱۲	۷/۹۹۷۱
	[۲۳]	۲۵۶×۲۵۶	۷/۹۹۶۸
Elaine	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۲۴]	۵۱۲×۵۱۲	۷/۹۹۷۶
	[۲۳]	۲۵۶×۲۵۶	۷/۹۹۹۲
Couple	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
Peppers	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۱۱]	۲۵۶×۲۵۶	۷/۹۹۹۷
	[۲۱]	۲۵۶×۲۵۶	۷/۹۹۷۰
	[۲۴]	۵۱۲×۵۱۲	۷/۹۹۷۰
	[۲۳]	۲۵۶×۲۵۶	۷/۹۹۶۶
Zelda	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
Cameraman	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۲۴]	۵۱۲×۵۱۲	۷/۹۹۷۶
	[۲۳]	۲۵۶×۲۵۶	۷/۹۹۶۹
Boat	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴
	[۱۱]	۲۵۶×۲۵۶	۷/۹۹۹۸
	[۲۴]	۵۱۲×۵۱۲	۷/۹۹۷۴
	[۲۳]	۲۵۶×۲۵۶	۷/۹۹۹۳
Baboon	پیشنهادی	۲۵۶×۲۵۶	۷/۹۹۹۴

	[۲۵]	۵۱۲×۵۱۲	۷/۹۹۹۴

از جدول ۳ می‌توان نتیجه گرفت که میزان آنتروپی در الگوریتم پیشنهادی خیلی نزدیک به عدد ایده‌آل ۸ در تصاویر خاکستری است. ازاین‌رو کیفیت رمزگذاری اثبات می‌شود. الگوریتم پیشنهادی ما هشت تصویر را بررسی نموده است. از بین هشت تصویر بالاترین میزان آنتروپی را در بین شش تصویر (Lena، Elaine، Couple، Zelda، Cameraman، Baboon) دارد. در باقیمانده تصاویر نیز، نتایج خیلی نزدیک به الگوریتم مقایسه شده است. لذا با توجه به تعداد بالای تصاویر در الگوریتم پیشنهادی ما و بالاتر بودن مقدار آنتروپی، می‌توان نتیجه گرفت که الگوریتم پیشنهادی نتایج بهتری نسبت به سایر الگوریتم‌ها ارائه داده است و این نشان‌دهنده برتری الگوریتم پیشنهادی ماست.

فضای کلید

در واقع قسمت اصلی هر الگوریتم رمزگذاری کلیدهای امنیتی هستند، زیرا قدرت الگوریتم به آن بستگی دارد. قوی بودن کلیدهای مخفی باعث مقاومت در برابر انواع حملات می‌شود. فضای بزرگ کلید و حساسیت زیاد از خصوصیات مطلوب کلیدهای محرمانه قوی است[۲۹]. فضای کلید به‌اندازه کلید مخفی بستگی دارد. اگر اندازه بزرگ باشد، تخمین همان کلید برای مهاجم دشوارتر است. فضای کلید مجموع کلیدهای مختلفی است که می‌تواند در سیستم رمزگذاری استفاده شود. یک الگوریتم رمزگذاری باید به تمام کلیدهای رمزگذاری حساس باشد. شرایط اولیه در سیستم نگاشت آشوب می‌توانند به‌عنوان کلیدهای رمزگذاری در رمزگذاری و رمزگشایی تصویر استفاده شوند. ما در این مقاله از نگاشت لجستیک آشوب به تعداد شش بار استفاده می‌کنیم. نگاشت لجستیک آشوب نیز دو تا پارامتر دارد. اگر دقت محاسبه اعداد برای هرکدام از آن‌ها 10^{-15} باشد پس فضای کلید درروش پیشنهادی برابر $(10^{15}\times 10^{15})^6$ خواهد بود. درنتیجه فضای کلید به اندازه کافی بزرگ است که در برابر حملات مقاومت کند. جدول شماره ۵ مقایسه فضای کلید رمزگذاری در الگوریتم پیشنهادی و سایر الگوریتم‌ها را نشان می دهد.

حساسیت نسبت به کلید

حساسیت کلید بدین معناست که اگر مهاجم حتی یک بیت را در کلید اصلی تغییر دهد، تصویر اصلی غیر قابل بازیابی باقی بماند. بدین معنی که تغییر یک بیت در کلید خصوصی، بایستی یک تصویر رمز کاملاً متفاوت در زمان رمزگذاری و یا یک تصویر رمزگشایی شده کاملاً متفاوت از تصویر اصلی در زمان رمزگشایی تولید کند. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله تا حدودی تضمین می‌کند. برای آزمودن میزان حساسیت نسبت به کلید طرح رمزنگاری مورد مطالعه، تصاویر گروه دو که شامل تصاویرBaboon، Boat، Cameraman، Zelda هستند مورد آزمایش قرار گرفتند. به این‌ترتیب که با استفاده از کلید رمزگذاری، رمزگذاری بر روی این تصاویر انجام شد و یک بار با کلید صحیح و یک بار نیز با کلید غیر صحیح که تنها در یک بیت با کلید صحیح متفاوت بود، رمزگشایی صورت گرفت. شکل ۱۰ نتایج رمزگشایی با کلید صحیح و کلید غیر صحیح را نشان می‌دهد. با مقایسه دو تصویر مشخص است که حساسیت به کلید تا چه اندازه در الگوریتم پیشنهادی ما بالا بوده است که با تغییر فقط یک بیت در کلید اصلی تصویر رمزگشایی شده کاملاً متفاوتی تولید شده است.

جدول۵. مقایسه فضای کلید الگوریتم پیشنهادی با سایر الگوریتم‌ها

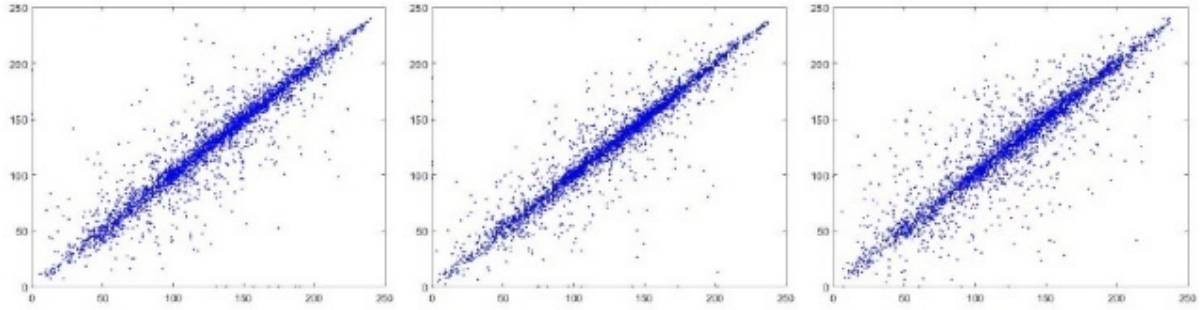
فضای کلید	الگوریتم
10^{180}	پیشنهادی
10^{161}	[۲۱]
4×10^{60}	[۳۰]
10^{48}	[۳۱]
10^{150}	[۳۲]
2.4×10^{112}	[۳۳]
2^{209}	[۳۴]
10^{112}	[۳۵]
10^{89}	[۳۶]
2^{192}	[۲۷]
10^{45}	[۲۵]
10^{98}	[۱۱]
2^{244}	[۲۴]

از بررسی جدول ۵ می‌توان نتیجه گرفت که الگوریتم پیشنهادی ما طول کلید بزرگ‌تری نسبت به سایر الگوریتم‌های مشابه دارد. الگوریتم پیشنهادی ما با دوازده الگوریتم مشابه دیگر مقایسه شده است. طول کلید در الگوریتم پیشنهادی ما از همه آن‌ها بزرگ‌تر است. وقتی طول کلید در الگوریتمی بزرگ‌تر می‌شود مقاومت تصویر در برابر حملات بهتر می‌شود. پس اگر الگوریتم پیشنهادی را با سایر الگوریتم‌ها مقایسه کنیم به این نتیجه می‌رسیم که الگوریتم پیشنهادی ما با داشتن طول کلید بزرگ‌تر باعث مقاومت بیشتر در مقابل حملات بی‌رحمانه به فضای کلید می‌شود. درنتیجه کارایی الگوریتم ما اثبات می‌شود.

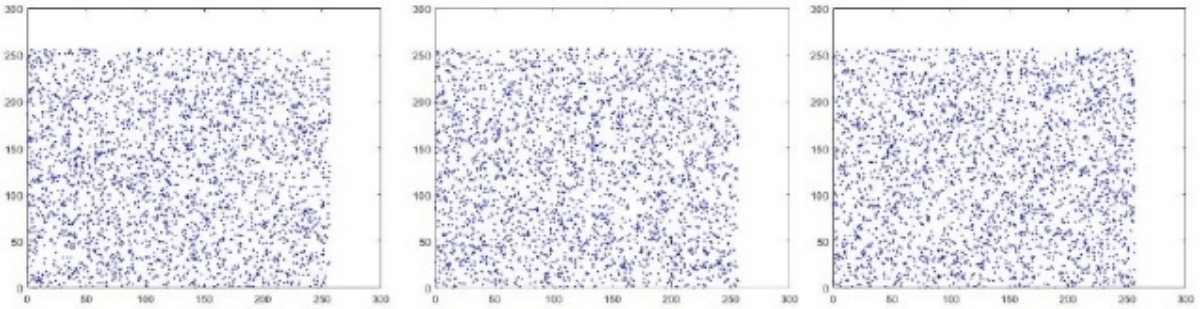
حملات رمزنگاری

همان‌طور که در شکل شماره ۱۱ مشخص است در دو حالت، اعمال حملات بر روی تصاویر رمزگذاری شده گروه اول که شامل تصاویر Lena، Elaine، Couple، Peppers است بررسی‌شده است. در حالت اول نویز فلفل و نمک بر روی تصویر رمزگذاری شده اعمال شده که شکل ۱۱.د نتیجه رمزگشایی آن را نشان می‌دهد. در حالت دیگر دو قسمت از تصویر رمزگذاری شده با مقدار صفر مقداردهی شده است. یا به عبارتی دیگر دو قسمت از تصویر، برش داده شده است. شکل ۱۱.ج نیز نتیجه رمزگشایی این حالت را نشان می‌دهد. نتیجه رمزگشایی در هر دو حالت مقدار دهی با صفر و اعمال نویز فلفل و نمک مشخص‌کننده تصاویر اصلی هستند که ماهیت اصلی تصویر کاملاً مشخص است. لذا نتایج به‌دست‌آمده نشان‌دهنده مقاومت تصویر در برابر حملات است.

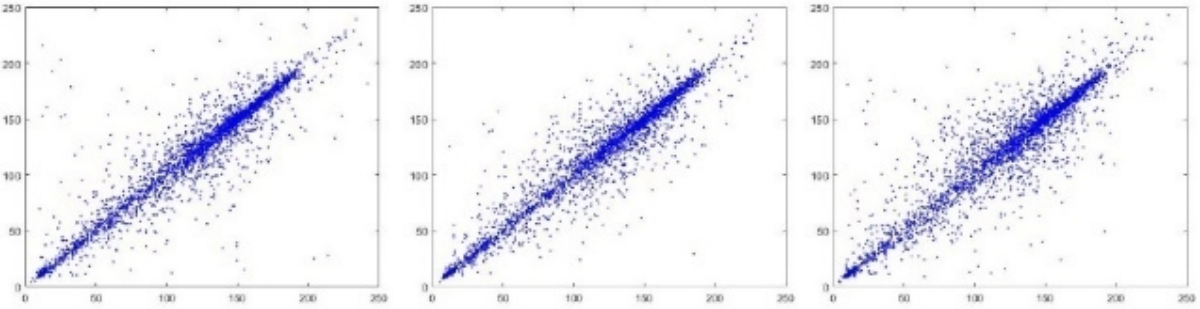
الف .تصاویر اصلی- افقی(گروه ۱) ب. تصاویر اصلی- عمودی(گروه ۱) ج. تصاویر اصلی- مورب(گروه ۱)



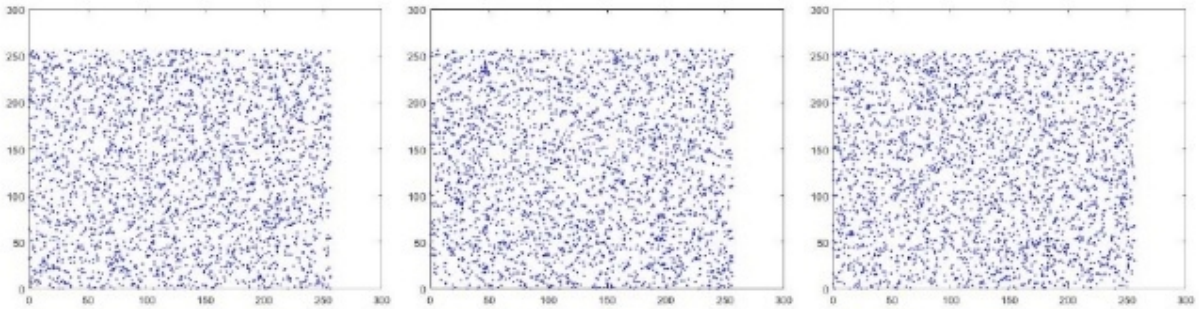
د. تصاویر رمزگذاری شده – افقی (گروه ۱) ه. تصاویر رمزگذاری شده – عمودی (گروه ۱) و. تصاویر رمزگذاری شده – مورب (گروه ۱)



ز. تصاویر اصلی – افقی (گروه ۲) ح. تصاویر اصلی – عمودی (گروه ۲) ط. تصاویر اصلی – مورب (گروه ۳)



ی. تصاویر رمزگذاری شده – افقی (گروه ۲) ک. تصاویر رمزگذاری شده – عمودی (گروه ۱) ل. تصاویر رمزگذاری شده – مورب (گروه ۱)



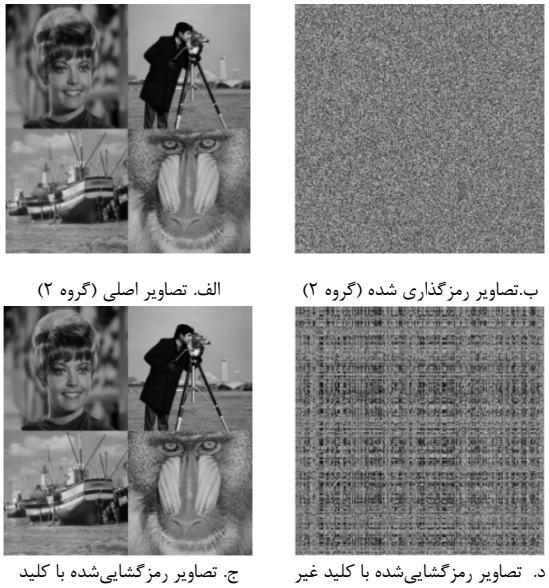
شکل۹. مقایسه ضریب همبستگی تصاویر در الگوریتم پیشنهادی و سایر الگوریتم‌ها

جدول۴. ضریب همبستگی تصاویر مختلف در الگوریتم پیشنهادی و سایر الگوریتم‌های مشابه

نام تصویر	اندازه تصویر	الگوریتم	تصویر افقی	تصویر عمودی	تصویر مورب	تصویر رمز افقی	تصویر رمز عمودی	تصویر رمز مورب
Lena	۲۵۶×۲۵۶	پیشنهادی	۰/۹۴۰۹	۰/۹۵۱۵	۰/۹۰۳۱	-۰/۰۰۱۱	-۰/۰۰۰۷	۰/۰۰۰۷
	۵۱۲×۵۱۲	[۲۵]	۰/۹۷۰۹	۰/۹۸۴۷	۰/۹۵۸۷	-۰/۰۰۰۷	۰/۰۰۰۱	-۰/۰۰۱۰
	۲۵۶×۲۵۶	[۱۱]	۰/۹۶۴۸	۰/۸۳۴۱	۰/۹۰۲۱	۰/۰۰۴۰	۰/۰۰۱۵	۰/۰۰۳۰
	۲۵۶×۲۵۶	[۲۶]	-	-	-	۰/۰۸۲۷	-۰/۰۲۵۴	-۰/۰۶۲۶
	۲۵۶×۲۵۶	[۲۱]	۰/۹۶۶۳	۰/۹۷۸۹	۰/۹۸۴۳	-۰/۰۰۳۶	-۰/۰۰۲۸	-۰/۰۰۲۱
	۲۵۶×۲۵۶	[۲۷]	۰/۹۷۷۴	۰/۹۸۸۱	۰/۹۶۹۸	-۰/۰۰۸۸	۰/۰۰۱۶	-۰/۰۲۵۴
	۲۵۶×۲۵۶	[۲۴]	۰/۹۳۶۵	۰/۹۶۸۲	۰/۹۱۳۲	-۰/۰۰۲۸	-۰/۰۰۰۴	۰/۰۰۴۰
	۲۵۶×۲۵۶	[۲۲]	-	-	-	۰/۰۰۰۹	۰/۰۱۳۴	-۰/۰۰۳۰
	۲۵۶×۲۵۶	[۲۳]	۰/۹۲۹۸	۰/۹۱۵۵	۰/۹۱۶۸	-۰/۰۰۰۵	۰/۰۰۱۲	۰/۰۰۰۷
Elaine	۲۵۶×۲۵۶	پیشنهادی	۰/۹۴۰۹	۰/۹۵۱۵	۰/۹۰۳۱	-۰/۰۰۱۱	-۰/۰۰۰۷	۰/۰۰۰۷
	۲۵۶×۲۵۶	[۲۴]	۰/۹۶۴۲	۰/۹۶۹۹	۰/۹۴۱۵	-۰/۰۰۴۵	۰/۰۰۱۹	-۰/۰۰۰۵
	۲۵۶×۲۵۶	[۲۳]	۰/۹۶۷۹	۰/۹۶۲۵	۰/۹۶۶۶	-۰/۰۰۱۶	-۰/۰۰۲۷	-۰/۰۰۱۷
Couple	۲۵۶×۲۵۶	پیشنهادی	۰/۹۴۰۹	۰/۹۵۱۵	۰/۹۰۳۱	-۰/۰۰۱۱	-۰/۰۰۰۷	۰/۰۰۰۷
Peppers	۲۵۶×۲۵۶	پیشنهادی	۰/۹۴۰۹	۰/۹۵۱۵	۰/۹۰۳۱	-۰/۰۰۱۱	-۰/۰۰۰۷	۰/۰۰۰۷
	۲۵۶×۲۵۶	[۱۱]	۰/۹۶۲۵	۰/۸۲۵۴	۰/۸۶۳۸	۰/۰۱۵۲	۰/۰۰۱۱	۰/۰۱۱۷
	۲۵۶×۲۵۶	[۲۴]	۰/۹۳۶۵	۰/۹۳۶۳	۰/۸۹۴۴	-۰/۰۰۱۹	-۰/۰۰۱۵	۰/۰۰۱۳
	۲۵۶×۲۵۶	[۲۳]	۰/۹۴۱۰	۰/۹۲۶۱	۰/۹۳۱۸	-۰/۰۰۱۱	۰/۰۰۱۴	-۰/۰۰۴۰
Zelda	۲۵۶×۲۵۶	پیشنهادی	۰/۹۳۳۹	۰/۹۴۳۹	۰/۸۹۸۲	۰/۰۰۰۹	۰/۰۰۰۸	-۰/۰۰۲۷
Cameraman	۲۵۶×۲۵۶	پیشنهادی	۰/۹۳۳۹	۰/۹۴۳۹	۰/۸۹۸۲	۰/۰۰۰۹	۰/۰۰۰۸	-۰/۰۰۲۷
	۲۵۶×۲۵۶	[۲۴]	۰/۹۴۶۰	۰/۹۶۸۱	۰/۹۲۲۲	-۰/۰۰۴۲	۰/۰۰۵۲	۰/۰۰۷۸
	۲۵۶×۲۵۶	[۲۳]	۰/۹۱۰۳	۰/۹۲۸۳	۰/۹۱۷۵	-۰/۰۰۰۶	۰/۰۰۰۰	-۰/۰۰۳۴
Boat	۲۵۶×۲۵۶	پیشنهادی	۰/۹۳۳۹	۰/۹۴۳۹	۰/۸۹۸۲	۰/۰۰۰۹	۰/۰۰۰۸	-۰/۰۰۲۷
	۲۵۶×۲۵۶	[۱۱]	۰/۹۶۵۶	۰/۸۹۳۹	۰/۹۱۸۵	۰/۰۰۰۴	۰/۰۰۱۲	۰/۰۰۲۳
	۲۵۶×۲۵۶	[۲۳]	۰/۹۳۷۲	۰/۹۳۸۲	۰/۹۰۵۲	-۰/۰۰۱۹	۰/۰۰۰۳	-۰/۰۰۳۳
Baboon	۲۵۶×۲۵۶	پیشنهادی	۰/۹۳۳۹	۰/۹۴۳۹	۰/۸۹۸۲	۰/۰۰۰۹	۰/۰۰۰۸	-۰/۰۰۲۷
	۵۱۲×۵۱۲	[۲۵]	۰/۸۶۲۷	۰/۷۵۲۲	۰/۷۲۱۸	-۰/۰۰۲۰	۰/۰۰۱۶	-۰/۰۰۰۲

از مقایسه نتایج به‌دست‌آمده در شکل ۹ و همچنین جدول شماره ۴، می‌توان اثبات کرد که همبستگی پیکسل‌های تصویر در سه حالت افقی، عمودی و مورب در تصویر رمزگذاری شده کاملاً به هم ریخته است. این نتایج اگر با نتایج ضریب همبستگی تصویر اصلی مقایسه شود مشخص خواهد کرد که پیکسل‌ها در سه جهت افقی، عمودی و مورب در تصویر اصلی چقدر به یکدیگر وابسته بوده و ارتباط نزدیکی به هم دارند. وقتی ارتباط پیکسل‌ها از یکدیگر کم شد یا اصلاً ارتباطی با همدیگر نداشتند شناسایی تصویر اصلی برای مهاجم به مراتب سخت‌تر خواهد شد. از آنجا که پیکسل‌ها هیچ نوع ارتباطی با همدیگر نداشته و یا خیلی کم با یکدیگر در ارتباط هستند می‌توان نتیجه گرفت که الگوریتم پیشنهادی ما یک الگوریتم کارا و مؤثر در رمزگذاری تصویر است.

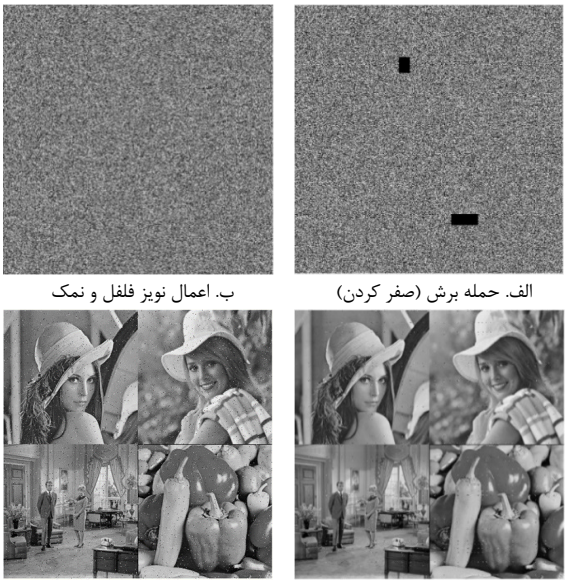
از مقایسه نتایج به‌دست‌آمده در شکل ۱۰ می‌توان نتیجه گرفت که اگر فقط یک بیت کلید را تغییر دهیم نمی‌توان تصویر رمزگذاری شده را رمزگشایی کرد. تصویری که با کلید غیر صحیح رمزگشایی شده است هیچ اطلاعاتی در خصوص تصویر اصلی ارائه نمی‌دهد. پس حساسیت



الف. تصاویر اصلی (گروه ۲) ب.تصاویر رمزگذاری شده (گروه ۲)

ج. تصاویر رمزگشایی‌شده با کلید صحیح د. تصاویر رمزگشایی‌شده با کلید غیر صحیح

شکل ۱۰ : نتایج رمزگشایی با کلید صحیح و غیر صحیح در الگوریتم پیشنهادی



الف. حمله برش (صفر کردن) ب. اعمال نویز فلفل و نمک

ج. تصاویر رمزگشایی‌شده (الف) د. تصاویر رمزگشایی‌شده (ب)

شکل۱۱ : نتایج اعمال دو نوع حمله بر روی تصویر رمزگذاری شده در الگوریتم پیشنهادی

بیشتری نسبت به کلید داشته باشد مقاومت بهتری نیز در مقابل حملات خواهد داشت. پس نتیجه می‌گیریم الگوریتم پیشنهادی ما در مقابل حملات مهاجم مقاومت بیشتری دارد.

همچنین نتیجه اعمال نویز فلفل و نمک و حمله برش در شکل ۱۱ نشان داده شده است. اگر تصاویر رمزگشایی‌شده در دو حالت گفته شده را با تصویر اصلی مقایسه کنیم، شاهد تفاوت چندانی در تصویر رمزگشایی شده با تصویر اصلی نخواهیم بود. لذا می‌توان نتیجه گرفت که تصویر رمزگذاری شده در برابر انواع حملات مقاومت بیشتری دارد.

زمان اجرا

زمان مورد نیاز برای اجرای یک روش رمزگذاری تصویر زمان اجرا گفته می‌شود. که تجمیع زمان کامپایل و اجرا است. برای اجرای عملی رمزگذاری تصویر، زمان اجرا باید حداقل باشد. این زمان به طورکلی در ثانیه، میلی ثانیه یا دقیقه اندازه‌گیری می‌شود[۳۷]. نتایج الگوریتم پیشنهادی ما توسط یک سیستم‌عامل ویندوز ۷ بر روی یک سیستم با مشخصات Intel(R) Core (TM) i7 CPU (Q720 ۱/۶۰GHz) با ۴ گیگا بایت حافظه اصلی به دست آمده است. جدول شماره ۶ مقایسه پیچیدگی الگوریتم پیشنهادی با سایر الگوریتم‌های مشابه را نشان می دهد.

با توجه به این‌که چهار تصویر در هر بار اجرا، رمزگذاری شده است به همین دلیل نتیجه زمان اجرا تقسیم بر چهار شده و زمان اجرای رمزگذاری یک تصویر به صورت تقریبی به دست آمده است. لذا نتیجه به دست آمده برای زمان اجرا در الگوریتم پیشنهادی در مقایسه با نتایج دیگر، مطلوب ارزیابی می‌شود.

جدول۶. مقایسه پیچیدگی الگوریتم پیشنهادی با سایر روش‌ها

نام تصویر	الگوریتم	اندازه تصویر	زمان اجرا(ثانیه)
Lena	پیشنهادی	۲۵۶×۲۵۶	۰/۱۹۹
	[۳۸]	۲۵۶×۲۵۶	۰/۱۰۲
		۵۱۲×۵۱۲	۰/۲۸۱
		۱۰۲۴×۱۰۲۴	۰/۷۱۷
	[۲۵]	۵۱۲×۵۱۲	۱/۱۰۴
	[۲۶]	۲۵۶×۲۵۶	۰/۰۶۰
	[۲۲]	۲۵۶×۲۵۶	۰/۲۰۱
Elaine	پیشنهادی	۲۵۶×۲۵۶	۰/۱۹۹
Couple	پیشنهادی	۲۵۶×۲۵۶	۰/۱۹۹
Peppers	پیشنهادی	۲۵۶×۲۵۶	۰/۱۹۹
Zelda	پیشنهادی	۲۵۶×۲۵۶	۰/۲۰۵
Cameraman	پیشنهادی	۲۵۶×۲۵۶	۰/۲۰۵
Boat	پیشنهادی	۲۵۶×۲۵۶	۰/۲۰۵
Baboon	پیشنهادی	۲۵۶×۲۵۶	۰/۲۰۵

۵- بحث و نتیجه‌گیری

در این مقاله، یک روش جدید برای رمزگذاری تصاویر خاکستری با استفاده از نگاشت لجستیک آشوب و بلوک‌بندی تصویر ارائه شد. در روش پیشنهادی از نگاشت لجستیک آشوب برای تولید کلید و همچنین جابجایی مکان پیکسل‌های تصویر استفاده شده است. در روش پیشنهادی ما، با انجام آزمایش های مختلف بر روی دو گروه چهارتایی از تصاویر استاندارد خاکستری و نمایش نتایج آن‌ها نشان داده شد که الگوریتم پیشنهاد شده از کارایی مناسب برخوردار است. نتایج به دست آمده از آزمون بصری و تحلیل هیستوگرام تصاویر رمزگذاری شده توسط الگوریتم پیشنهادی نشان دادند که هیچ‌گونه الگو و ناحیه بافت قابل‌تشخیص و هیچ شباهت آماری بین ظاهر تصویر اصلی و تصویر رمز شده وجود ندارد. سایر نتایج آزمایش‌ها ازجمله آزمون مربع خی، حساسیت به کلید، تحلیل فضای کلید، آنتروپی، ضریب همبستگی، میزان تمایز بین تصویر اصلی و تصویر رمز و همچنین بررسی انجام برخی حملات به تصویر اصلی و تصویر رمز شده نیز کارایی الگوریتم پیشنهادی را تائید می‌کنند. مقایسه‌های انجام شده با مقالات ارائه شده در سال‌های اخیر، نشان می‌دهد که روش پیشنهادی به مراتب دارای عملکرد بهتری بوده و مقاومت بیشتری در مقابل انواع حملات را دارد.

علیرغم همه مزایایی که برای الگوریتم پیشنهادی مطرح شد، با این حال هیچ‌کدام از معیارهای ارزیابی تصویر هنوز هم به حالت ایده‌آل کامل نرسیده‌اند. پس فعلاً می‌توان الگوریتم‌های بهتری از الگوریتم پیشنهادی ما ارائه داد. مثلاً آنتروپی اطلاعات در الگوریتم پیشنهادی ما عدد ۷/۹۹۹۴ است که می‌توان با ارائه الگوریتم‌های بهتر این عدد را به عدد ایده‌آل ۸ رساند. یا معیار ارزیابی دیگر اگر بخواهیم مطرح کنیم معیار NPCR است که مقدار ایده‌آل آن ۱۰۰ درصد است ولی نتیجه‌ای که در الگوریتم پیشنهادی ما به دست آمده است عدد ۹۹/۶۱۸۵ است که علیرغم این‌که از اکثر الگوریتم‌های دیگر نتیجه بهتری ارائه داده است

ولی هنوز هم به مقدار ایده‌آل ۱۰۰ درصد نرسیده است. معیار ارزیابی مهم‌تر دیگر معیار طول کلید است که در الگوریتم پیشنهادی ما طول کلید عدد 10^{180} محاسبه شده است که بهترین فضای کلید را در میان الگوریتم‌هایی که تاکنون مطرح شده‌اند ارائه کرده است. لذا با در نظر گرفتن سایر معیارهای ارزیابی تصویر که در اینجا مطرح نشد و با توجه به این‌که تقریباً هیچ‌کدام از آن‌ها در هیچ مقاله‌ای به حالت ایده‌آل صد در صد نرسیده‌اند پس همچنان می‌توان در آینده الگوریتمی بهتر از الگوریتم پیشنهادی ما ارائه داد تا تمام معیارهای ارزیابی تصویر رمزگذاری شده به حالت ایده‌آل برسند.

مراجع

[1] S. Som and S. Sen, "A non-adaptive partial encryption of grayscale images based on chaos", Procedia Technology, vol. 10, pp. 663-671, 2013/01/01/ 2013.

[2] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption", Multidimensional Systems and Signal Processing, vol. 30, no. 2, pp. 943-961, 2019/04/01 2019.

[3] G. Gu and J. Ling, "A fast image encryption method by using chaotic 3D cat maps", Optik, vol. 125, no. 17, pp. 4700-4705, 2014/09/01/ 2014.

[4] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques", Archives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15-43, 2020/01/01 2020.

[5] D. Zareai, M. Balafar, and M. R. Feizi Derakhshi, "A new grayscale image encryption algorithm composed of logistic mapping, Arnold cat, and image blocking", Multimedia Tools and Applications, vol. 80, no. 12, pp. 18317-18344, 2021/05/01 2021.

[6] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map", Chaos, Solitons & Fractals, vol. 26, no. 1, pp. 117-129, 2005/10/01/ 2005.

[7] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, vol. 24, no. 9, pp. 926-934, 2006/09/01/ 2006.

[8] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps", Chaos, Solitons & Fractals, vol. 35, no. 2, pp. 408-419, 2008/01/01/ 2008.

[9] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos", Physics Letters A, vol. 372, no. 4, pp. 394-400, 2008/01/21/ 2008.

[10] A. Shokouh Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map", Pattern Analysis and Applications, vol. 22, no. 1, pp. 243-257, 2019/02/01 2019.

[11] M. Kaur and D. Singh, "Multi objective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption", Multidimensional Systems and Signal Processing, vol. 32, no. 1, pp. 281-301, 2021/01/01 2021.

[12] M. Kalra, S. Katyal, and R. Singh, "A tent map and logistic map based approach for chaos-based image encryption and decryption", Innovations in Computer Science and Engineering: Springer, 2019, pp. 159-165.

[13] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map", Multimedia Tools and Applications, vol. 78, no. 15, pp. 22023-22043, 2019/08/01 2019.

[14] W. Gao, J. Sun, W. Qiao, and X. Zhang, "Digital image encryption scheme based on generalized Mandelbrot-Julia set", Optik, vol. 185, pp. 917-929, 2019/05/01/ 2019.

[15] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain", Medical & Biological Engineering & Computing, vol. 59, no. 3, pp. 589-605, 2021/03/01 2021.

[16] H. Liu, F. Wen, and A. Kadir, "Construction of a new 2D Chebyshev-Sine map and its application to color image encryption", Multimedia Tools and Applications, vol. 78, no. 12, pp. 15997-16010, 2019/06/01 2019.

[17] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations", Optics and Lasers in Engineering, vol. 88, pp. 197-213, 2017/01/01/ 2017.

[18] P. Mani, R. Rajan, L. Shanmugam, and Y. Hoon Joo, "Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption", Information Sciences, vol. 491, pp. 74-89, 2019/07/01/ 2019.

[19] H. Liu, B. Zhao, and L. J. E. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling", Entropy, vol. 21, no. 4, p. 343, 2019.

[20] A. M. Shaheen, T. R. Sheltami, T. M. AlKharoubi, and E. Shakshuki, "Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT", Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 12, pp. 4733-4750, 2019/12/01 2019.

[21] A. Firdous, A. U. Rehman, and M. M. S. J. I. A. Missen, "A gray image encryption technique using the concept of water waves, chaos and hash function", IEEE, vol. 9, pp. 11675-11693, 2021.

[22] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion", Nonlinear Dynamics, vol. 103, no. 2, pp. 2043-2061, 2021/01/01 2021.

[23] M. Wang, X. Wang, T. Zhao, C. Zhang, Z. Xia, and N. Yao, "Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme", Information Sciences, vol. 544, pp. 1-24, 2021/01/12/ 2021.

[24] F. Musanna, D. Dangwal, and S. Kumar, "Novel image encryption algorithm using fractional chaos and cellular neural network", Journal of Ambient Intelligence and Humanized Computing, 2021/03/06 2021.

[25] X. Wang and S. Gao, "A chaotic image encryption algorithm based on a counting system and the semi-tensor product", Multimedia Tools and Applications, vol. 80, no. 7, pp. 10301-10322, 2021/03/01 2021.

[26] M. Dua, A. Suthar, A. Garg, and V. Garg, "An ILM-cosine transform-based improved approach to image encryption", Complex & Intelligent Systems, vol. 7, no. 1, pp. 327-343, 2021/02/01 2021.

[27] B. Bouteghrine, C. Tanougast, and S. Sadoudi, "Novel image encryption algorithm based on new 3-d chaos map", Multimedia Tools and Applications, vol. 80, no. 17, pp. 25583-25605, 2021/07/01 2021.

[28] C. E. J. T. B. s. t. j. Shannon, "Communication theory of secrecy systems", IEEE, vol. 28, no. 4, pp. 656-715, 1949.

[29] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps", Signal Processing: Image Communication, vol. 29, no. 5, pp. 618-627, 2014/05/01/ 2014.

[30] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function", Multimedia Tools and Applications, vol. 75, no. 17, pp. 10631-10648, 2016/09/01 2016.

[31] R. Aqeel ur, X. Liao, A. Kulsoom, and S. Ullah, "A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps", Multimedia Tools and Applications, vol. 75, no. 18, pp. 11241-11266, 2016/09/01 2016.

[32] A. ur Rehman, D. Xiao, A. Kulsoom, M. A. Hashmi, and S. A. Abbas, "Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules", Multimedia Tools and Applications, vol. 78, no. 7, pp. 9355-9382, 2019/04/01 2019.

[33] R. Aqeel ur, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos", Optik - International Journal for Light and Electron Optics, vol. 153, pp. 117-134, 2018/01/01/ 2018.

[34] A. ur Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules", Multimedia Tools and Applications, vol. 74, no. 13, pp. 4655-4677, 2015/07/01 2015.

[35] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence", Multimedia Tools and Applications, vol. 72, no. 1, pp. 57-70, 2014/09/01 2014.

[36] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," Multimedia Tools and Applications, vol. 75, no. 11, pp. 6303-6319, 2016/06/01 2016.

[37] A. A. Abd El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," AEU - International Journal of Electronics and Communications, vol. 67, no. 2, pp. 136-143, 2013/02/01/ 2013.

[38] M. Asgari-Chenaghlu, M. A. Balafar, and M. R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," Signal Processing, vol. 157, pp. 1-13, 2019/04/01/ 2019.