ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۶ / تابستان ۱۳۹۶ / ص ۹۲- ۷۶

ارائه یک الگوریتم جدید جهت رمزنگاری نامه های محرمانه الکترونیکی

سمیه حق طلبی [۱]، رضا صبور [۲]

[۱] گروه کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، سپیدان، ایران.

[۲] گروه کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، سپیدان، ایران.

نام نویسنده مسئول:
رضا صبور

چکیده

رشد و گسترش روزافزون شبکه های کامپیوتری، خصوصا" اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است و حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام ها ومبادلات تجاری ایفا می نماید. انتقال اطلاعات حساس بر روی یک شبکه مستلزم بکارگیری مکانیزمی است تا عملا" امکان رمزگشائی و دستیابی به داده اولیه توسط افراد غیر مجاز را سلب نمایند.

در این مقاله یک الگوریتم سریع رمزنگاری تصاویر با جایگشت و پخش ترکیبی پیشنهاد و تجزیه و تحلیل شده است. تجزیه وتحلیل های تئوری و آزمونهای تجربی، هر دو تایید می‌کنند که روش پیشنهادی دارای امنیت وسرعت بالایی است. باتوجه به اینکه ازیک کلید با اندازه بزرگ برای رمزنگاری استفاده شده، بنابراین تصویر رمز شده هیچ اطلاعاتی ازتصویراصلی نشان نمی‌دهد. همچنین دارای خواص اغتشاش و انتشار خوبی است بنابراین همبستگی پیکسل های همسایه درتصویراصلی کاهش یافته و تصویر رمز شده یک هیستوگرام متعادل دارد.

واژگان کلیدی: رمزنگاری،آشوب، کلید رمزنگاری، جایگشت، پخش، همبستگی پیکسل.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۶ ، تابستان ۱۳۹۶، ص ۹۲- ۷۶

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

همانطور که می‌دانید رمزنگاری، علم حفاظت اطلاعات محرمانه در هنگام ذخیره یا انتقال داده ها تحت هرشرایط ناامن است. تکنیک های رمزنگاری موجود اغلب بر اساس نظریه اعداد و یا مفاهیم جبری می باشند. یکی از ویژگیهای مهم سیستم های بیولوژیکی نظم در بی نظمی یا آشوب است که عمدتاً به دلیل تعاملات سیستمی و پیچیده میان اجزاء و نیز ماهیت غیر خطی سیستم های بیولوژیکی بوجود می آید. تغییرات ناگهانی در سیستم‌های غیر خطی ممکن است باعث بروز رفتاری شود که به آن آشوب گفته می شود. واژه آشوب در مورد سیستم‌هایی به کار می رود که دارای رفتارهایی با تظاهرات رندم گونه یا غیر پریودیک و نویزی است. آشوب ابزار دیگری است که امیدهای فراوانی را در حصول امنیت مطلوب در رمزنگاری ایجاد نموده است. در نهایت رفتار آشوبناک یک رفتار دقیق از سیستم غیرخطی است که به ظاهر تصادفی به نظر می‌رسد. هر چند این ظاهر تصادفی منشأ تصادفی ندارد و نتیجه ای از یک پردازش قطعی و تعریف شده است. خصوصیت مهم آشوب، حساسیت بسیار زیاد آن به وضعیت ابتدایی سیستم است.

آشوب یک پدیده موجود در سیستم های غیر خطی قطعی است، که حساسیت بالایی به شرایط اولیه نشان می_دهد و رفتار شبه تصادفی دارد. پس از اکتشاف آشوب توسط ادوارد لورنز ، در سال ۱۹۶۳، امروزه تئوری آشوب یک شاخه از مطالعات علمی شده است.

در اوایل ۱۹۹۰ ارتباطات امن به عنوان کاربردی بالقوه در مطالعات بر روی تئوری آشوب مطرح شد. این موضوع برمبنای طرح اصول همگام سازی آشوبناک توسط پیکورا وکارول بود. این امر باعث جلب توجه سایر مهندسین پردازش سیگنال وارتباطات و دانشمندان برای کار بر روی این موضوع شد.

از خواص آشوب می‌توان به دینامیک بودن، ارگودیک ، حساسیت آن به شرایط اولیه سیستم و پارامترهای سیستم اشاره نمود که در واقع برای بکارگیری در ایجاد یک طرح ارتباطی امن بر پایه آشوب، از ویژگیهای اساسی هستند. در مورد این موضوع، مدارات سخت افزاری زیادی نیز پیشنهاد و ساخته شده اند. بر این اساس علاقه به سیستم های مبتنی بر آشوب، به عنوان یک گزینه جایگزین برای طرحهای موجود مانند ECC، RSA وغیره، در رمزنگاری در چندین سال گذشته افزایش یافته است.

یک رفتار آشوبناک، می‌تواند یا در قالب سیستم‌های یک بعدی و دو بعدی در ساده ترین حالت خودشبیه سازی شود(که توسط نگاشت‌های گسسته نمایش داده می‌شود) و یا در قالب سیستم های فیزیکی با ابعاد زیاد شبیه سازی شود که با سه یا بیشتر معادله دیفرانسیل مرتبه اول مستقل و یا با دو یا بیشتر رابطه دیفرانسیل مرتبه اول وابسته معمولی توصیف می شود.

۱- تاریخچه رمزنگاری مبتنی بر آشوب

علم آشوب سومین انقلاب بعد از نظریه نسبیت ومکانیک کوانتومی درقرن ۲۱ نامگذاری شده است. آشوب پدیده‌ای است که در سیستم‌های غیر خطی تعریف پذیر رخ می‌دهد که حساسیت زیاد به شرایط اولیه و رفتار شبه تصادفی از خود نشان می دهند. درسال‌های اخیر طرح‌های رمزنگاری زیادی پیشنهاد شده‌اند که دراین میان روش‌های مبتنی برآشوب[1] امیدوار کننده‌تر می‌باشند.

فردریچ[2] ساخت یک تکنیک رمزنگاری بلوکی متقارن مبتنی بر نگاشت بیکر استاندارد دوبعدی[3] را نشان داد. سه گام در روش فردریچ وجود دارد: ۱) انتخاب یک نگاشت آشوبناک و توسعه آن با معرفی برخی پارامترها، ۲) گسسته سازی نگاشت آشوبناک به یک شبکه مربعی متناهی از نقاطی که نشان دهنده پیکسل‌ها هستند، ۳) بسط نگاشت گسسته شده به سه بعدی و ترکیب آن با یک مکانیزم ساده پخش.

اسکارینگر[4] یک تکنیک رمزنگاری تصویر مبتنی بر جریان کولموگروف آشوبناک طراحی کرد که در آن کل تصویر به عنوان یک بلوک در نظر گرفته می‌شود که از طریق یک سیستم آشوبناک با کلید کنترل شده جایگزین می‌شود، به علاوه یک شیفت رجیستر مولد اعداد شبه تصادفی نیز برای برهم زدن داده‌ها بکار گرفته می‌شود.

ین[5] و گوأ[6] یک روش رمزنگاری مبتنی بر نگاشت آشوبناک لوجستیک به نامBRIE پیشنهاد کردند. اصل اساسی BRIE چرخش بیتی پیکسل‌هاست، که بوسیله یک دنباله دودویی شبه تصادفی آشوبناک کنترل می‌شود. کلید مخفی BRIE شامل دو عدد صحیح و یک شرط اولیه نگاشت لوجستیک است.

1- CHAOS
2 -FRIDRICH
3 -TWO-DIMENSIONAL STANDARD BAKER MAP
4 -SCHARINGER
5 -YEN
6 -GUO

ISSN: 2745-3673
http://www.Rcsj.ir

ین و گواُ همچنین یک روش رمزنگاری به نام CKBA[7] پیشنهاد کردندکه در آن یک دنباله دودویی به عنوان یک کلید با استفاده از یک سیستم آشوبناک تولید می‌شود. پیکسل‌های تصویر با توجه به دنباله دودویی تولید شده دوباره مرتب می‌شوند و سپس با کلید انتخاب شده XOR و XNOR می‌شوند.

بعدها لی[8] و ژنگ[9] با اشاره به برخی از نقص‌های اشاره شده در طرح های رمزنگاری مذکور ین و گواُ در سال ۱۹۹۹ و ۲۰۰۰ ، همچنین در مورد برخی از پیشرفت های ممکن طرحهای آنها بحث کردند.

چن[10] و همکاران یک رمزنگاری متقارن پیشنهاد کردند که در آن نگاشت آشوبناک دوبعدی برای طراحی یک روش رمزنگاری تصویر بلادرنگ امن به نگاشت سه بعدی تعمیم داده می‌شود. این روش یک 3D Cat Map را به منظور برهم زدن مکان پیکسلهای تصویر و نگاشت آشوبناک دیگری را نیز به منظور برهم زدن رابطه بین تصویر اصلی و رمز شده استفاده می‌کند.

ان کی پاریک[11] و همکاران در تحقیقات خود با استفاده از سیگنال‌های آشوبناک یک تصویر رنگی را رمزنگاری کردند. آنها در روش پیشنهادی خود از دو نگاشت آشوبناک مدل لوجستیکی و کلیداصلی به طول 81 بیت استفاده کرده‌اند.

فویان سان[12] و همکارانش یک الگوریتم رمزنگاری تصویر مبتنی بر آشوب مکانی پیشنهادکردند، ایده اساسی در این الگوریتم رمزنگاری پیکسل به پیکسل تصویر با استفاده از نگاشت آشوب مکانی است سپس پیکسل‌ها در جهات مختلف برهم زده می‌شوند که نیاز به دو دور برای رمزنگاری تصویر دارد.

هواکیان یانگ[13] و همکارانش یک روش احراز هویت و رمزنگاری مبتنی بر آشوب پیشنهاد کردند، که در آن به طور خاص یک تابع درهمساز کلیددار برای تولید یک مقدار ۱۲۸ بیتی درهمساز ازهر دو تصویر اصلی و کلیدهای درهمساز مخفی معرفی می‌شود. مقدار درهمساز نقش کلید را برای رمزنگاری ورمزگشایی بازی می‌کند در حالی که کلیدهای درهمساز مخفی برای احراز هویت تصویر رمزگشایی شده استفاده می‌شوند.

نانران[14] و همکارانش ازسه تکنیک رمزنگاری برای افزایش مشکل امنیت داده چندرسانه ای درموبایل وایمکس که درآنهاازالگوریتم AES[15] استفاده می‌شود پیشنهادشده است. پس ازبررسی ومقایسه های انجام شده بین این سه الگوریتم مشخص شده است که هنگامی که ازترکیب نگاشت‌های هنون وبیکردریک تکنیک استفاده شود سرعت افزایش می یابد و در مقابل حملات آماری و دیفرانسیل مقاوم ترخواهند بود.

نارندرا[16] و همکارانش یک روش براساس ترکیب پویای توابع آشوب وتکنیک بازیابی مرحله‌ای درحوزه فوریه پیشنهاد شده است که تصویرتوسط توابع آشوب به تصویر خاص تبدیل می‌شود وکلید نیز به کمک تکنیک بازیابی مرحله‌ای استخراج می‌شود. طرح پیشنهاد شده می تواند زمان انتشار را کاهش دهد و کلید با فضای بزرگتری تولید کند وبرای رمزنگاری چند تصویری نیز توسعه پیدا کند.

۲- روش پیشنهادی

روش پیشنهادی شامل تولید کلیدمحرمانه و جایگشت و پخش می‌باشد و عملکرد آنها به شرح زیر است:

۲-۱- تولید کلید محرمانه

امروزه سیستم های آشوب به دلیل رفتار شبه تصادفی، برای تولیدجملات تصادفی بیشتر مورد توجه قرار گرفته اند. یکی از معروفترین سیگنالهایی که رفتار آشوب گونه دارد و برای تولید اعداد تصادفی متقارن بسیار مناسب می‌باشد سیستم آشوب لجستیک است.

اگر برای سیستم لجستیکی معادله (۴-۱) مقدار پارامتر کنترل a = 3.59 یا بیشتر انتخاب شود تعداد حالات نوسان سیستم به بیشمار حالت رسیده و بعد از آن سیستم در مد آشوب قرار خواهد گرفت.

$$x_{n+1} = rx_n(1 - x_n) \qquad (۱)$$

7- CHAOTIC KEY BASED ALGORITHM
8 -LI
9 -ZHENG
10 -CHEN
11 -N.K. PAREEK
12 -Fuyan Sun
13 - Huaqian Yang
14 -Nanrun
2- Advanced Encryption Standard
16 -Narendra

ISSN: 2745-3673
http://www.Rcsj.ir

$$i = \lfloor (A_i * M) + 1 \rfloor \quad i=1,2,\ldots,10 \qquad (۲)$$

$$j = \lfloor (B_i * N) + 1 \rfloor \quad j=1,2,\ldots,10 \qquad (۳)$$

در یک الگوریتم رمزنگاری کارآمد، کلید محرمانه باید کاملاً متاثر از تصویر اولیه بوده تا الگوریتم رمزنگاری در مقابل حملات Diffrential و Know plain-text مقاوم عمل کند. بنابراین ما به کمک مقادیر i وj بدست آمده به کمک دو آرایه A وB موقعیت ۱۰پیکسل از تصویر را برای تولید کلید انتخاب می‌کنیم و به معادل باینری آن تبدیل کردیم و در آرایه ۸۰ بیتیC قرار دادیم و به کمک رابطه (۴-۴) مقدار کلید را محاسبه کردیم:

$$k = \sum_{i=0}^{79} (b_i * 2^i) \qquad (۴)$$

در رابطهٔ فوق bi بیت i اُم از آرایه ۸۰ بیتی می باشد.

۲-۲ جایگشت و پخش

از رابطه $x_0 = \frac{k}{2^{80}}$ جهت محاسبه مقادیر اولیه دو نگاشت Cubic و Sine استفاده کرده ایم که توسط روابط (۴-۵) و (۴-۶) تعریف می‌شوند و برای تولید اعداد تصادفی بکاربرده شده اند.

برای اینکه این سیستم ها در مد آشوب قرار بگیرند باید مقدار پارامتر کنترل آنها به ترتیب برابر a=2.59 و a=0.99 انتخاب شود.

$$x_{n+1} = a \times x_n \times (1 - x_n^2) \qquad (۵)$$

$$z_{n+1} = a \times \sin(\pi \times z_n) \qquad (۶)$$

توسط نگاشت Cubic به تعداد سطرها عدد تصادفی تولید می شود و در Pm ریخته می شود.

توسط نگاشت Sine به تعداد ستونها عدد تصادفی تولید می شود و در PN ریخته می شود.

برای از بین بردن ارتباط بین پیکسل های مجاور تصویر ما از سطر یک شروع می کنیم آنرا با مقادیر تصادفیPm که تولید شده XOR می کنیم تا مقادیر پیکسل ها تغییر کند. سپس به اندازه y1 که از رابطه (۴-۶) بدست می‌آید شیفت چرخشی به پایین می دهیم. اینکار را تا زمانی که همه سطر های تصویر پیمایش شود انجام می دهیم.

$$y_1 = (2r_i + c_j) mod\ M \qquad (۷)$$

i=0,1,2,…,M
j=0,1,2,…,N

ri شماره سطر و cj شماره ستون مورد نظر می باشند.

سپس از ستون یک شروع می کنیم آنرا با مقادیر تصادفیPN که تولید شده XOR می کنیم تا مقادیر پیکسل ها تغییر کند. سپس به اندازه y2 که از رابطه (۴-۷) بدست می‌آید شیفت چرخشی به راست می دهیم. اینکار را تا زمانی که همه ستون های تصویر پیمایش شود انجام می دهیم. به این ترتیب ما همزمان هم مقدار پیکسل ها را برای از بین بردن ارتباط بین تصویر اصلی و رمزنگاری شده تغییر دادیم که باعث می شود هر تغییر کوچکی در یک پیکسل تصویر تقریباً در کل پیکسل های تصویر جریان پیدا کند و هم آنها را جابجا کردیم. نتیجه اینکار یعنی تغییر و جابجایی پیکسل های تصویر یک تصویر رمزنگاری شده می باشد.

$$y_2 = (r_i + c_j) mod\ N \qquad (۸)$$

i=0,1,2,…,M
j=0,1,2,…,N

۲-۳ رمزگشایی

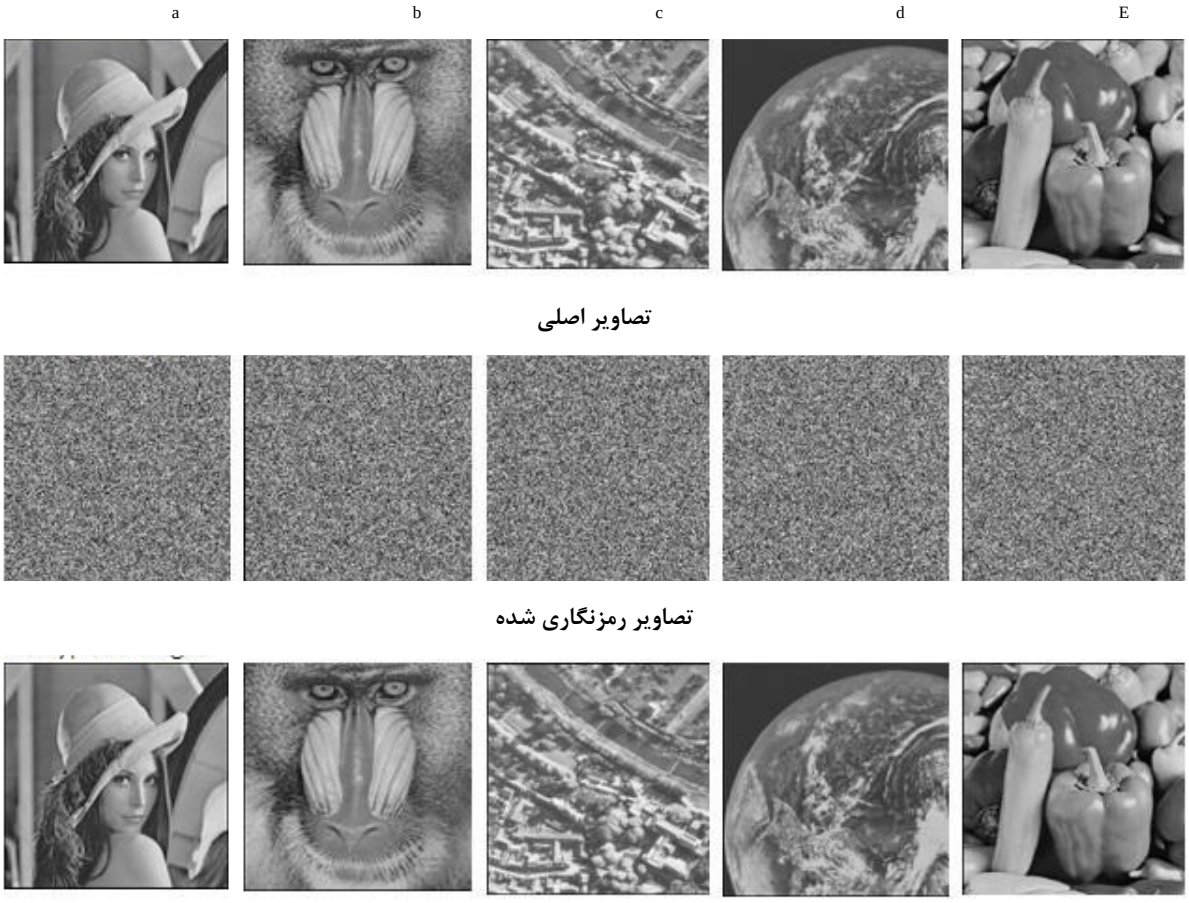
فرایند رمزگشایی تصویر عکس فرایند رمزنگاری است. یعنی از آخرین ستون به سمت اولین ستون آنرا با مقادیر تصادفیPN که تولید شده XOR می کنیم تا مقادیر آن تغییر کند و به اندازه x1 شیفت چرخشی به چپ می دهیم. اینکار را تا زمانی که همه ستون های تصویر پیمایش شود یعنی رسیدن به اولین ستون انجام می دهیم.

ISSN: 2745-3673
http://www.Rcsj.ir

سپس ازآخرین سطر شروع کرده آنرا با مقادیر تصادفیPm که تولید شده XOR می کنیم تا مقادیر آن تغییر کند سپس به اندازه x2 شیفت چرخشی به بالا می دهیم. اینکار را تا زمانی که همه سطر های تصویر پیمایش شود یعنی رسیدن به اولین سطر انجام می دهیم.

$$x_1 = (y_1 - y_2) mod\, M \quad (۹)$$

$$x_2 = (-y_1 + 2y_2) mod\, M \quad (۱۰)$$



شکل (۱). تصاویر اصلی، تصاویر رمزگشایی شده و رمزگشایی شده با الگوریتم پیشنهادی
(a) Lena (b) Mandrill (c) Aerial (d) Earth from Space (e) Pepper

۴-۲ تحلیل نتایج

یک روش رمزنگاری موفق باید در برابر انواع حملات مقاوم باشد، در این بخش روش پیشنهادی را از نظر کارایی و مقاومت در برابر حملات مورد تجزیه و تحلیل قرار می دهیم، از جمله تجزیه و تحلیل فضای کلید، تحلیل حساسیت، تجزیه و تحلیل آماری، تحلیل هیستوگرام، تحلیل ضریب همبستگی، حملات دیفرانسیلی و در بخش پایانی تجزیه و تحلیل سرعت را انجام می‌دهیم.

شبیه سازی ها توسط یک دستگاه کامپیوتر شخصی به زبان Matlab تحت ویندوز ۷، پردازنده Core(TM) i3 @2.40GHz وRAM ۴ گیگابایت بر روی ۱۰۰ تصویر استاندارد به عنوان تصاویر بدون رمز صورت گرفته و اجرا شده است.

تصاویر استاندارد از آدرس زیر دانلود شده اند:

USC-SIPI Image Database, http://sipi.usc.edu/database/database.php

۴-۲ -۱ تحلیل فضای کلید

تنها راه حل موجود برای مقابله با روش تحلیل رمز Brute force بوجودآوردن یک فضای بسیار بزرگ برای حالات ممکن کلید اصلی است که امتحان کردن تمامی آنها با استفاده از قویترین رایانه های امروزی جهان مقدور نباشد.

ISSN: 2745-3673
http://www.Rcsj.ir

با توجه به اینکه ما از یک کلید بزرگ با اندازه ۲۸۰ استفاده کرده ایم، فضای کلید الگوریتم پیشنهادی به اندازه ای بزرگ هست که نیاز کلی در برابرحمله Brute force را برآورده می کند.

۲-۴-۲ تحلیل حساسیت

حساسیت به کلید اصلی در فرایند رمزنگاری ایجاب می کند که کلیدهای بسیار مشابه (که فقط در یک بیت اختلاف دارند) تصاویری بسیار متفاوت با یکدیگر تولید کنند. در طی فرایند رمزگشایی در صورتیکه تصویر با یک کلید بسیار نزدیک به کلید اصلی (که فقط در یک بیت با کلید اصلی متفاوت است) رمزگشایی شود، باید تصویر حاصل از این عمل نه تنها به تصویر اصلی هیچ شباهتی نداشته باشد، بلکه تصویری شبیه به تصویر رمزشده را حاصل نماید.

ما ازکلیدزیربرای رمزگشایی تصاویر استفاده کردیم. تصاویر رمزگشایی شده نامفهومی برای تصاویرHouse و Lena بدست می آید که نتایج آن در شکل های (۲) و (۳) نشان داده شده است و بیان کننده حساسیت بالای کلید الگوریتم می باشد.

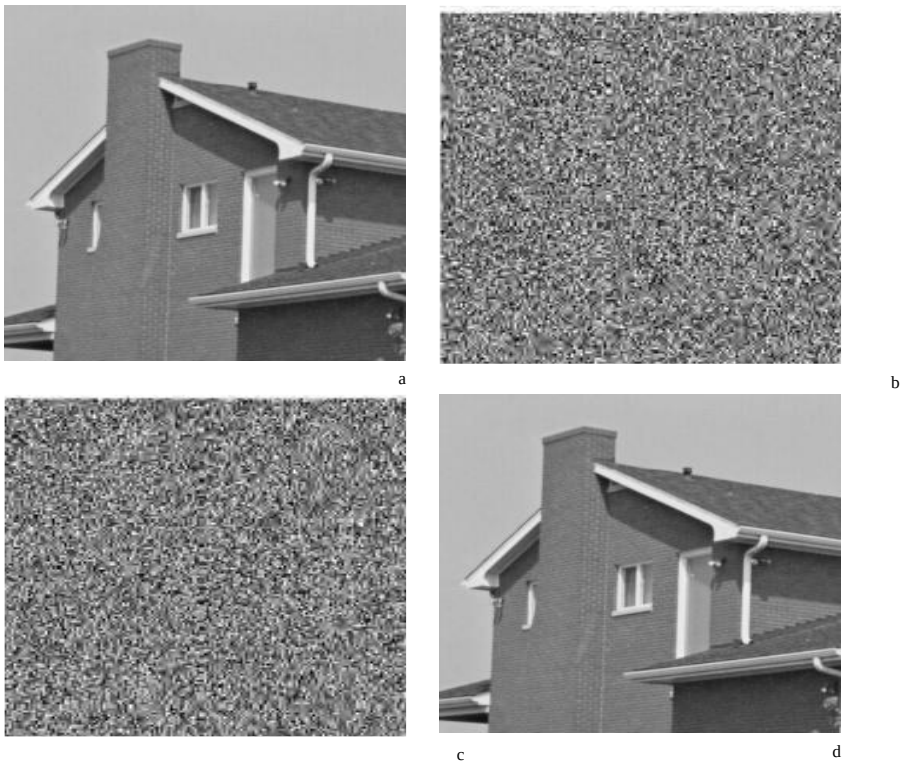
K = 1,208,925,820,740,529,081,548,800

جدول (۱). اختلاف بین پیکسل های در تصاویر پنهانی شده با کلید مشابه با یک بیت اختلاف

تصویر	درصد اختلاف بین دو تصویر پنهانی شده
Paper	۹۹,۵۷۸
Lena	۹۹,۵۰۲
Baboon	۹۹,۵۱۱

شکل (۲): رمزنگاری و رمزگشایی تصویرLena256×256 (a): تصویر اولیه (b) : تصویر رمزشده
(c) : تصویر رمزگشایی شده با کلید اشتباه (d): تصویر رمزگشایی شده با کلید صحیح

ISSN: 2745-3673
http://www.Rcsj.ir



a b c d

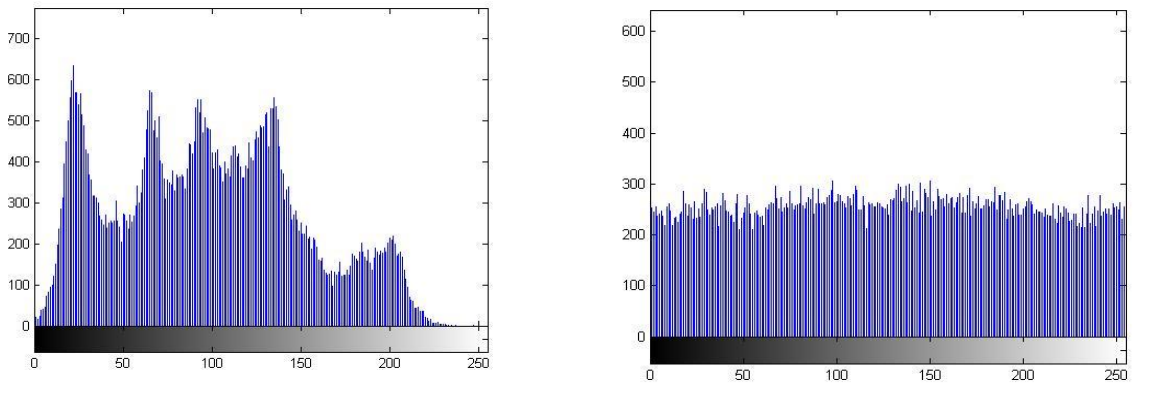
شکل (۳): رمزنگاری و رمزگشایی تصویر House256×256 (a) : تصویر اولیه (b): تصویر رمزشده
(c) : تصویر رمزگشایی شده با کلید اشتباه (d) : تصویر رمزگشایی شده با کلید صحیح

۲-۴-۳ تحلیل آماری

برای بررسی کیفیت رمزگذاری و استحکام آن ازطریق حملات آماری ، هیستوگرام و ضریب همبستگی (correlation coefficient) بین تصویر اصلی و تصویر رمزشده محاسبه می شود.

۲-۴ -۳-۱ تحلیل هیستوگرام

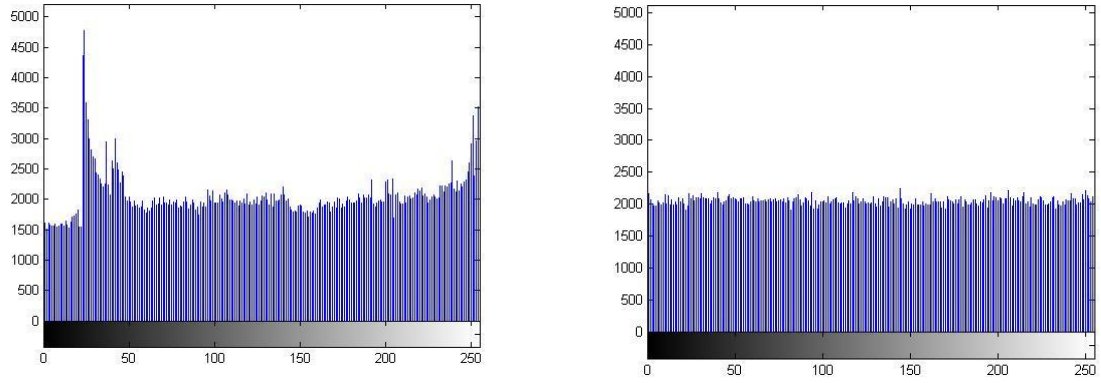
برای تحلیل آماری، تصویرLena را رمزنگاری می کنیم و سپس نمودار هیستوگرام تصویر اصلی و تصویر رمز شده را به ترتیب (a) و (b) در شکل (۴) و (۵) نشان می دهیم. با یک نگاه به هیستوگرام هر دو تصویر می توان ادعا کرد که هیستوگرام تصویر رمز شده تقریباً مسطح است، که دلالت بر یک ویژگی آماری خوب دارد و نشان از موفقیت در برابر حملات آماری نفوذگران است.



a b

شکل (۴): (a): هیستوگرام تصویر اولیه Lena 256×256 (b) : هیستوگرام تصویر رمزشده Lena 256×256

ISSN: 2745-3673
http://www.Rcsj.ir



a b

شکل (۵): (a): هیستوگرام تصویر اولیه House 512 × 512 (b) : هیستوگرام تصویر رمزشده House 512 × 512

۲-۴ -۳-۲ تحلیل ضریب همبستگی[1]۱۷

ضریب همبستگی معیاری برای اندازه گیری همبسته بودن تصویراصلی و تصویر رمزگذاری شده است. اگرآنها به شدت به هم وابسته باشند ضریب همبستگی برابر یک است ، یعنی تصویر رمزگذاری شده همانند تصویر اصلی است و فرایند رمزگذاری درپنهان کردن جزئیات تصویر اصلی شکست خورده است . اگرضریب همبستگی برابرصفرباشد، آنگاه تصویراصلی و تصویررمزگذاری شده آن کاملاً متفاوت هستند. بنابراین، موفقیت فرایند رمزگذاری به معنی ارزش های کوچکتر از ضریب همبستگی می باشد. ضریب همبستگی توسط معادله زیرمحاسبه می شود :

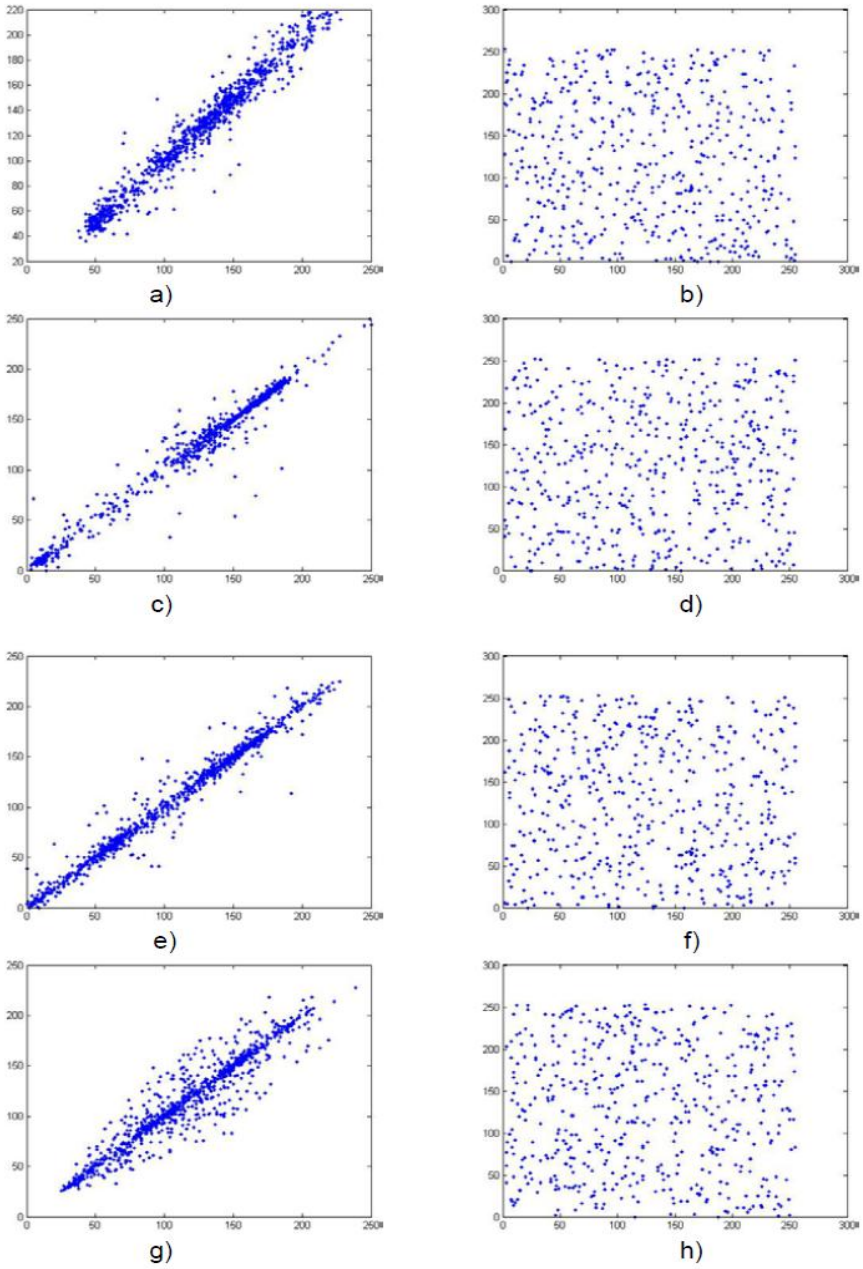
$$Cov(x,y) = E[(x-E(x))(y-E(y))] = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x))(y_i - E(y))] \quad (۱۰)$$

$$rxy = \frac{cov(x*y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (۱۱)$$

x و y مقادیر دو پیکسل مجاور در تصویر هستند. $E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$ و $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$. در هر آزمون ۱۰۰۰زوج پیکسل مجاور انتخاب شده است، یعنی۱۰۰۰ = r. همبستگی دو پیکسل مجاور افقی و عمودی و قطری در تصویر ساده و تصویر رمز شده در شکل (۶) نشان داده شده است.

[1]- Correlation Coefficient analysis

ISSN: 2745-3673
http://www.Rcsj.ir



شکل (۶): همبستگی دو پیکسل مجاور در تصویر ساده و تصویر رمزداربا استفاده از طرح پیشنهادی:

(a) تصویر ساده Lena، (b) تصویر رمزشده Lena ،(c) تصویر ساده Camera Man، (d) تصویر رمزشدهCamera Man

(e) تصویر ساده Pepper، (f) تصویر رمزشده Pepper ، (g)تصویر ساده Barbara، (h) تصویر رمزشدهBarbara

ISSN: 2745-3673
http://www.Rcsj.ir

جدول (۲). نتایج ضرایب همبستگی دو پیکسل مجاور در تصویر ساده و تصویر رمزدار

تصویر	چهت مجاورت	ضریب همبستگی تصویراصلی	ضریب همبستگی تصویر رمزنگاری شده
Girl	Horizontal	۰,۸۳۸۱۸	-۰,۰۰۵۶۹
	Vertical	۰,۸۷۵۲۴	۰,۰۰۲۵۳
	Diagonal	۰,۸۱۱۳۲	۰,۰۰۳۸۳
House	Horizontal	۰,۸۹۸۳۲	-۰,۰۰۳۰۴
	Vertical	۰,۹۲۲۰۶	۰,۰۰۵۰۲
	Diagonal	۰,۸۳۶۰۵	-۰,۰۰۵۳۱
Mandrill	Horizontal	۰,۶۴۴۲۳	۰,۰۰۱۲۸
	Vertical	۰,۷۱۶۰۶	۰,۰۰۵۱۳
	Diagonal	۰,۶۲۳۱۳	-۰,۰۰۹۸۲
Lena	Horizontal	۰,۹۶۰۵۵	-۰,۰۰۰۵۷
	Vertical	۰,۹۴۱۸۲	۰,۰۰۴۰۴
	Diagonal	۰,۹۴۳۸۱	۰,۰۰۲۶۱
Peppers	Horizontal	۰,۹۷۴۰۵	-۰,۰۰۱۴۲
	Vertical	۰,۹۸۰۰۳	-۰,۰۰۱۸۲
	Diagonal	۰۹۵۷۷۱	۰,۰۰۳۲۳
Man	Horizontal	۰,۹۶۸۴۲	-۰,۰۰۱۵۴
	Vertical	۰,۹۶۹۶۱	۰,۰۰۲۹۱
	Diagonal	۰,۹۸۷۳۶	-۰,۰۰۱۰۶
Airport	Horizontal	۰,۹۲۷۶۳	۰,۰۰۰۲۱
	Vertical	۰,۹۴۱۸۵	-۰,۰۰۵۶۴
	Diagonal	۰,۸۴۱۶۸	۰,۰۰۸۹۵
San Diego	Horizontal	۰,۸۲۲۰۴	-۰,۰۰۷۱۳
	Vertical	۰,۸۴۳۷۱	۰,۰۰۰۶۶
	Diagonal	۰,۷۷۳۵۸	-۰,۰۰۶۶۵
Stockton	Horizontal	۰,۶۸۱۰۳	۰,۰۰۰۲۱
	Vertical	۰,۷۲۵۷۹	-۰,۰۰۸۳۶
	Diagonal	۰,۶۳۶۱۳	-۰,۰۰۱۸۶
Washington, D.C	Horizontal	۰,۹۰۱۰۲	-۰,۰۰۲۶۱
	Vertical	۰,۹۳۵۸۷	۰,۰۰۱۳۱
	Diagonal	۰,۸۸۴۰۲	۰,۰۰۳۳۳

اندازه ضرایب همبستگی تصویر بدون رمز نزدیک به یک است، در حالی که در تمام آزمایش های انجام شده، مقادیر بدست آمده در تصویر رمزدارنزدیک به صفر است. این مقادیر ثابت می کنند که از طریق فرایند رمزگذاری همبستگی قوی ذاتی موجود در تصاویر ساده با موفقیت حذف شده است به طوری در تصویر رمزدار پیکسل های همسایه عملاً ارتباطی ندارند.

ISSN: 2745-3673
http://www.Rcsj.ir

۲-۴-۴ حملات دیفرانسیلی

در صورتی که یک تغییر کوچک در تصویر بدون رمز باعث تفاوت معنی داری در تصویررمزدار شود حمله دیفرانسیلی بی اثرخواهد شد. مقادیر نرخ تغییر تعداد پیکسل (NPCR) و شدت در حال تغییر میانگین واحد (UACI) جهت سنجش میزان مقاومت یک سیستم رمزنگاری، در مقابل حملات known plain-text و Diffrential بکار می روند و طبق رابطه زیر محاسبه می شوند:

$$NPCR = \frac{\sum_{r,c} D(r,c)}{W \times H} \times 100\% \quad (۱۲)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{r,c} \frac{|C_1(r,c) - C_2(r,c)|}{255}\right] \times 100\% \quad (۱۳)$$

که c1 و c2 دو تصویر رمزدار هستند که فقط در یک پیکسل از تصویر بدون رمز با هم متفاوت هستند. مقادیر پیکسل های (r,c) از تصویر c1 و c2 به ترتیب با c1(r,c) و c2(r,c) مشخص شده اند. H و W به ترتیب طول و عرض تصویر رمزدار هستند.

```
If C1(r,c) = C2(r,c) then
  D(r,c) = 0
Else
  D(r,c)=1
End
```

مقادیر UACI و NPCR الگوریتم پیشنهادی برای پایگاه داده ای از تصاویر در جدول (۳) بیان شده است. بزرگی این مقادیر بیانگر حساسیت الگوریتم به تصویر اولیه می باشد.

جدول (۳). مقادیر UACI و NPCR سیستم رمزنگاری پیشنهادی برای پایگاه داده ای از تصاویر.

UACI(%)	NPCR(%)	تصویر
۳۳,۱۰	۹۹,۲۴	Girl
۳۲,۹۶	۹۸,۸۷	House
۳۳,۱۱	۹۹,۱۲	Mandrill
۳۳,۱۲	۹۹,۲۲	Lena
۳۳,۱۴	۹۹,۱۵	Peppers
۳۳,۱۸	۹۹,۱۶	Man
۳۳,۱۱	۹۹,۱۸	Airport
۳۲,۸۴	۹۹,۱۴	San Diego
۳۳,۱۵	۹۹,۲۱	Stockton
۳۲,۸۷	۹۹,۱۹	Washington, D.C

مقادیر بدست آمده در آزمون های انجام شده ازشاخص NPCR بین ٪۹۸,۸۷ و ٪۹۹,۲۳ و شاخص UACI بین ٪۳۲,۱۷ و ٪۳۳,۱۸ می باشد، که خیلی به یک نزدیک است و تایید می کند طرح رمزمگاری پیشنهادی در مقابل حملات دیفرانسیلی مقاوم است.

۲-۴-۵ آنتروپی

آنتروپی یکی از خصوصیات برجسته برای تصادفی بودن است. در تصویر اصلی بدلیل وجود وابستگی بین پیکسل ها به ندرت مقادیر به صورت تصادفی است به همین دلیل مقدار آنتروپی کمتر از ۸ می باشد. آنتروپی بیانگر توزیع مقادیر خاکستری در یک تصویر می‌باشد و بیشترین مقدار آن در یک تصویر با ۲۵۶ سطح خاکستری، برابر با ۸ (مقدار ایده آل: زمانی که همه پیکسل ها به صورت تصادفی توزیع شده باشند) بوده و طبق معادله (۴-۱۳) محاسبه می‌گردد که در آن m مقدار سطح خاکستری و p(m) احتمال m می‌باشد. مقادیر آنتروپی تصاویر رمزشده و اصلی در جدول ... نشان داده شده است

$$H(m_i) = -\sum_{i=1}^{l} p(m_i) log_2 p(m_i) \qquad l = 0.1.2. \ldots .255 \quad (۱۳)$$

ISSN: 2745-3673
http://www.Rcsj.ir

با توجه به جدول (۴) مشاهده می شود که آنتروپی در روش پیشنهادی برای تصاویر مختلف در ۲۰ تکرار مختلف حداکثر برابر ۷,۹۹۹۸۲۳ به دست آمده است که بسیار نزدیک به مقدار ایده آل یعنی ۸ می باشد
مقادیر جدول (۴) پس از ۵۰ بار تکرار الگوریتم بدست آمده اند.

جدول (۴).نتایج مربوط به آنتروپی تصویر ساده و تصویر رمزدار

تصویر	آنتروپی	
	تصویراصلی	تصویر رمزنگاری شده
Girl	۶,۴۱۵۴۷۹	۷,۹۹۹۸۱۷
House	۶,۴۰۰۶۷	۷,۹۹۹۶۱۵
Mandrill	۷,۶۴۴۴۴۰	۷,۹۹۹۲۸۲
Lena	۷,۲۷۱۸۶۵	۷,۹۹۰۱۴۶
Peppers	۷,۲۹۷۷۹۵	۷,۹۸۴۴۱۶
Man	۷,۵۲۳۷۳۷	۷,۹۹۹۸۲۶
Airport	۶,۸۳۰۳۳۰	۷,۹۹۹۸۱۶
San Diego	۵,۶۶۲۶۵۶	۷,۹۹۹۸۲۱
Stockton	۶,۰۷۰۷۹۱	۷,۹۹۹۸۲۳
Baboon	۷,۲۲۲۲۶۰	۷,۹۹۱۴۲۷

مقادیر بدست آمده بسیار نزدیک به ۸ می باشد، که به این معنی است که نشت اطلاعات در فرایند رمزنگاری قابل چشم پوشی می باشد و سیستم در مقابل حملات آنتروپی امن است.

جدول (۴-۵). مقایسه آنتروپی بدست آمده در روش های مختلف

روش	تصویر	آنتروپی
الگوریتم پیشنهادی	Paper	۷,۹۸۴۴
	Lena	۷,۹۹۰۱
	Baboon	۷,۹۹۱۴
روش ارائه شده در [16]	Paper	۷,۹۸۱۸
	Lena	۷,۹۸۰۳
	Baboon	۷,۹۸۴۸
روش ارائه شده در [30]	Paper	۷,۹۷۳۱
	Lena	۷,۹۶۷۰
	Baboon	۷,۹۷۹۴

۲-۴-۶ زمان اجرا

به غیر از در نظر گرفتن امنیت، یک عامل مهم در بررسی کارایی ایک سیستم رمزنگاری سرعت آن است. یک الگوریتم رمزنگاری و رمزگشایی باید به اندازه کافی سریع باشد تا بتواند نیازهای کاربردهای بلادرنگ را برآورده کند. زمان اجرای واقعی یک الگوریتم وابسته به عوامل بسیاری از جمله مهارت برنامه نویسی ، زبان برنامه نویسی، محیط اجرا، و غیره است. بنابراین، ما سرعت سیستم رمزنگاری پیشنهادی را با سایر سیستم های رمزنگاری در رمزنگاری یک تصویرمقایسه کردیم .

بر این اساس، ما الگوریتم پیشنهادی را بر روی تصاویر استاندارد با اندازه های متفاوت اجرا کردیم. خلاصه میانگین سرعت به دست آمده در جدول نشان داده شده است:

ISSN: 2745-3673
http://www.Rcsj.ir

جدول (۶). میانگین سرعت فرایند رمزنگاری و رمزگشایی

اندازه تصویر (پیکسل)	اندازه تصویر (مگابایت)	میانگین زمان (ثانیه)	میانگین سرعت (مگابایت برثانیه)
۲۵۶×۲۵۶	۰,۰۹	۰,۰۴۵	۲,۲۲۲
۵۱۲×۵۱۲	۰,۳۵	۰,۱۹۵	۱,۸۴۶
۷۲۰×۵۷۶	۰,۲۹۹	۰,۲۹۷	۱,۰۰۷
۱۰۲۴×۱۰۲۴	۱,۴۷	۰,۷۶۲	۱,۹۳۷
۳۰۰۰×۴۰۰۰	۱۷,۱۷۵	۸,۵۷۵	۲,۰۰۳

همانطور که مشاهده می کنید میانگین سرعت طرح پیشنهادی حدود ۳ مگابایت بر ثانیه دارد، که سریع تر از الگوریتم های ارائه شده در [16] ,[30] ,[32] می باشد، بنابراین برای رمزنگاری بلادرنگ مناسب است.

جدول (۷). زمان اجرای سیستم رمزنگاری پیشنهادی و سایر روشها برای تعدادی تصاویر(زمان رمزنگاری بر اساس میلی ثانیه).

شاخص	[16]	[30]	[32]	الگوریتم پیشنهادی
NPCR	۹۹,۴۸	۹۹,۸۵	۹۹,۶۱	۹۹,۱۴
UACI	۳۰,۸۷	۳۳,۵۸	۳۳,۷۲	۳۳,۰۵
Horizontal	۰,۳۴۲	۰,۰۱۷۷۶	-۰,۰۰۴۳	۰,۰۰۳۹
Vertical	۰,۳۵۲	۰,۰۴۹۱۲	۰,۰۰۴۹	۰,۰۰۵۹
Diagonal	۰,۲۹۸	۰,۰۰۳۴۸	۰,۰۰۵۷	۰,۰۰۰۴
Speed (MB/s)	۱,۶۵	۰,۴۵	۲,۴	۱,۸۰۳

با توجه به نتایج شبیه سازی، مشاهده می‌کنیم که طرح رمزنگاری تصویر ارائه شده نتایج مشابه یا بهتر از دیگر طرح ها داردو به اندازه کافی برای برنامه های Real-Time سریع می باشد. تصویر رمزشده کاملاً با تصویر اصلی متفاوت بوده و هیچگونه ارتباطی با آن ندارد و در مقابل انواع حملات تفاضلی و متن اصلی معلوم و ... پایداری مناسبی از خود نشان می دهد. مقدار بالای آنتروپی (۷,۹۹۱۳) در این روش کارایی بالای روش پیشنهادی را نشان می‌دهد.

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه گیری

رشد و گسترش روزافزون شبکه های کامپیوتری، خصوصا" اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است و حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام ها ومبادلات تجاری ایفا می نماید. انتقال اطلاعات حساس بر روی یک شبکه مستلزم بکارگیری مکانیزمی است تا عملا" امکان رمزگشائی و دستیابی به داده اولیه توسط افراد غیر مجاز را سلب نمایند. بر خلاف پیام های متنی داده های تصویری ویژگی های خاص خود را همانند حجیم بودن , اضافات زیاد و همبستگی زیاد بین نقاط تصویر دارند که با عث می شود که اجرای روشهای رمزنگاری سنتی روی تصاویر بسیارسخت و کند باشد. تصاویر مخابره شده ممکن است کاربرد هایی چون کاربرد تجاری, نظامی و یا حتی کاربرد های پزشکی داشته باشند که در صورت حفظ امنیت آنها و جلوگیری از دسترسی های غیر مجاز به این تصاویر رمز نگاری آنها را قبل از ارسال روی شبکه ضروری می کندولی به دلیل ویژگی های تصاویر خصوصا حجم زیاد داده های تصویری و وید ئویی استفاده از الگوریتم های کلاسیک رمز نگاری متن مانند:RSA , DES و.... در این موارد نا کار آمد , چون اولا رمز کردن حجم زیاد داده های تصویری به این طریق بسیار وقت گیر خواهد بود و خصوصا در کاربرد های بلادرنگ عملی نیست و دومین مشکلی که این الگوریتم‌ها دارند طول کلید آنهاست که با توجه به حجم داده های رمز شده استفاده از کلید های با طول محدود باعث ضربه پذیری روش در برابر حملات متن رمز شده می گردد. رمز نگاری تصویر در سیستم هایی که اطلاعات آنها به صورت تصاویرتبادل می‌شود مهمترین رکن می‌باشد.

در این طرح یک الگوریتم سریع رمزنگاری تصاویر با جایگشت و پخش ترکیبی پیشنهاد و تجزیه و تحلیل شده است. طرح پیشنهادی دارای سیستم کلید خصوصی متقارن است. فضای کلید آن به اندازه کافی بزرگ است. فایل اصلی و رمزگذاری شده هم اندازه هستند. تصویر رمزشده کاملاً با تصویر اصلی متفاوت بوده و هیچگونه ارتباطی با آن ندارد و در مقابل انواع حملات تفاضلی و متن اصلی معلوم و ... پایداری مناسبی از خود نشان می دهد.

معیارهایی مانند هیستوگرام، فضای کلید، ضرایب همبستگی پیکسل‌های مجاور و میزان تفاوت تصویر رمز با تصویر اصلی در این سیستم محاسبه شده است. تجزیه وتحلیل های تئوری و آزمونهای تجربی، هر دو تایید می‌کنند که طرح پیشنهادی دارای امنیت وسرعت بالایی است. باتوجه به اینکه ازیک کلید با اندازه بزرگ برای رمزنگاری استفاده شده، بنابراین تصویر رمز شده هیچ اطلاعاتی ازتصویراصلی نشان نمی‌دهد. و همچنین دارای خواص اغتشاش و انتشار خوبی است بنابراین همبستگی پیکسل های همسایه درتصویراصلی کاهش یافته و تصویررمزشده یک هیستوگرام متعادل دارد.

پیشنهادات

درجاهایی که نیاز به طراحی یک روش رمزنگاری تصویر بلادرنگ نباشد برای پیدا کردن بهترین مقدار پارامترهای اولیه استفاده ازالگوریتم های تکاملی می‌تواند روش خوبی باشد. بنابراین، مطالعه و بررسی این مباحث در تحقیقات آینده قابل انجام و با اهمیت خواهد بود.

استفاده از داده کاوی و استفاده از شروط آن برای جابجایی و غیر قابل پیش بینی کردن محل پیکسل های تصویر مثلاً شرط هایی نظیر زوج یا فرد بودن پیکسل.

تشکر و قدردانی

مقاله حاضر مطالعه ای در قالب طرح تحقیقاتی مصوب و با حمایت معاونت پژوهشی دانشگاه آزاد اسلامی واحد سپیدان انجام شد. نویسندگان مقاله برخود لازم می دانند که مراتب تشکر صمیمانه خود را از حمایتهای معاونت پژوهشی دانشگاه آزاد اسلامی واحد سپیدان که ما را در انجام و ارتقاء کیفی این پژوهش یاری دادند ، اعلام نماید .

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Arumugam, A.S., and Krishnan N. (2010) Biometric Encryption and Bio-Fusion Authentication using Combined Arnold Transition and Permutation Matrices. International Journal of Engineering Science and Technology, 2(10), 5357-5369.
[2] Chengqing Li, Shujun Li, Kwok-Tung Lo. (2011) Breaking a modified substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simul. 16 (2); 837–843.
[3] Chengqing Li, Michael Z.Q. Chen, Kwok-Tung Lo. (2011) Breaking an image encryption algorithm based on chaos, Internat. J. Bifur. Chaos 21 (7); 2067–2076.
[4] Eslami Z, Zarepour Ahmadabadi J. (2010) A verifiable multi-secret sharing scheme based on cellular automata.Inf Sci;180: 2889–94.
[5] Guodong Ye. (2010) Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett, (31), pp. 347–354.
[6] Huaqian, Y., Kwok-Wo, W., Xiaofeng, L., Wei, Z., and Pengcheng, W. (2010) A fast image encryption and authentication scheme based on chaotic maps. Elsevier, Commun Nonlinear Sci Numer Simulat (15), pp. 3507-3517.
[7] Ismail IA, Amin M,Diab H. (2010) A digital image encryption algorithm based a composition of two chaotic Logisti cmaps.Int J Network Secur, (11), pp. 1–10.
[8] Mohamed, M.A., Zaki, F.W., and El-mohandes, A.M. (2013) Enhanced Diffusion Encryption for Transmission over Mobile WiMax Networks. International Journal of computer Science, 10(2), pp.1694-0784.
[9] Nanrun, Z.,Yixian, W., Lihua, G., Xiubo, C., and YixianYang. (2012) Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Elsevier, Optics & Laser Technology, (44) pp. 2270-2281.
[10] Narendra, K. P., Vinod, P., and Krishan, K.Sud. (2013) Diffusion–substitution based gray image encryption scheme**.** Elsevier, Digital Signal Processing, (23), pp. 894–901.
[11] Osama, M., Abu, Z., Nawal, A., Nigm, E. M., and Osama, S. F . (2013) A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security. International Journal of Computer Applications, 61(5), pp.0975- 8887.
[12] Pareek N,Patidar V,Sud K. (2003) Discrete chaotic cryptography using external key.Phys Lett A, (309), pp. 75–82.
[13] Payal, M., and Rajender, S. C. (2013) A New And Secure Chaos Based Multimedia Encryption Scheme. International Journal of Engineering Research and Applications, 3(4), pp.2063-2068.
[14] Raja Kumar, R., Sampath, Dr.A., and Indumathi, Dr.P. (2011) Enhancement and Analysis of Chaotic Image Encryption Algorithms . Computer Science & Information Technology, (02), pp.143–153.
[15] Ramesh Kumar, y., Singh, Dr. B. K., Sinha, S.K., and Pandey, K. K. (2013) A New Approach of Colour Image Encryption Based on Henon like Chaotic Map. Journal of Information Engineering and Applications, 3(6).
[16] Riaz F, Hameed I. Shafi, Kausar R and Ahmed A. (2012). "Enhanced image encryption techniques using modified advanced encryption standard", Communications in Computer and Information Science, vol. 281, pp. 385-39.
[17] Saraswathi P.V. and Venkatesulu M., (2012) "A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal", Journal of Computer Science, vol. 8, no. 9, pp. 1541-1546,.
[18] Şerbănescu A. and Rîncu C.I., (2008) Systemes et signaux face au chaos. Applications aux communications. Bucharest: Military Technical Academy Press.
[19] Sharma, M., and Kowar, M. K. (2010) Image Encryption Techniques UsingChaotic Schemes: a Review. International Journal of EngineeringScience and Technology, 2(6), pp. 2359-2363.
[20] Shen J, Jin X, Zhou C.A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. Lect Notes Comput Sci, (3768), pp. 270–80.

ISSN: 2745-3673
http://www.Rcsj.ir

[21] Shubo Liu, Jing Sun, Zhengquan Xu. (2009) An improved image encryption algorithm based on chaotic system, J. Comput, (4), pp. 1091–1100.
[22] Sivakumar T. and Venkatesan R., (2014) "A novel approach for image encryption using dynamic SCAN pattern", IAENG International Journal of Computer Science, vol. 41, no. 2, pp. 91-101.
[23] SunF,Liu S,Li Z,Lu Z. (2008) A novel image encryption scheme based on spatial chaos map.Chaos Solitons Fractals, (38), pp. 631–40.
[24] Tong X.J. and Cui M.G., (2010) "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation", Science in China Series F: Information Sciences, vol. 53, no. 1, pp. 191-202.
[25] Wang J, Jiang G. and Lin B., (2012) "Cryptanalysis of an image encryption scheme with a pseudorandom permutation and its improved version", Journal of Electronics (China), vol. 29, no. 1-2, pp. 82-93.
[26] Wang X. and He G., (2011) "Cryptanalysis on a novel image encryption method based on total shuffling scheme", Optics Communications, vol. 284, no. 24, pp. 5804–5807.
[27] Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan J.P. and Natarajan P, (2013) "Local Shannon entropy measure with statistical tests for image randomness", Information Sciences, vol. 222, pp. 323-342.
[28] Xing-Yuan, C. Feng, W. Tian. (2010) A new compound mode of confusion and diffusion for block encryption of image based on chaos", Elsevier, Commun Nonlinear Sci Number Simulat, pp.2479-2485.
[29] Yang, K. W. Wong, X. Liao, W. Zhang, P. (2010) A fast image encryption and authentication scheme based on chaotic map, Elsevier, Commun Nonlinear Sci Number Simulat, pp. 3507-3517.
[30] Ye R. (2011) A novel chaos-based image encryption scheme with an efficient permutation–diffusion mechanism.Opt Commun, (284), pp. 5290–8.
[31] Yong, W., Kwok-Wo, W., Xiaofeng, L., and Guanrong C. (2011) A new chaos-based fast image encryption algorithm. Elsevier, Applied Soft Computing, (11), pp. 514-522.
[32] Yoon, J.W., and Kim, H. (2010) An image encryption scheme with a pseudorandom permutation based on chaotic maps. Elsevier, Commun Nonlinear Sci Numer Simulat , (15), pp. 3998–4006
[33] Zhang Q,Guo L,Wei X. (2010) Image encryption using DNA addition combining with chaotic maps.Math Comput Model, (52), pp.2028–35.
[34] Zhang G, Liu Q. (2011) A novel image encryption method based on total shuffling scheme. Opt Commun, (284), pp.2775–80.
[35] USC-SIPI Image Database, http://sipi.usc.edu/database/database.php, last accessed: 01 February 2016.