نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۱، پاییز ۱۳۹۸؛ ص ۲۲- ۹

رمزنگاری تصاویر با استفاده از نظریه آشوب و اتوماتای سلولی

حمید طباطبایی[1*]، سید کاظم شکفته[2]، حسین سلامی[3]، محمدوحید زنگنه‌مقدم[4]

۱- استادیار گروه مهندسی کامپیوتر، واحد قوچان، دانشگاه آزاد اسلامی، قوچان، ۲- مربی گروه مهندسی کامپیوتر، موسسه آموزش عالی غیرانتفاعی- غیردولتی شاندیز، مشهد ۳- مربی گروه مهندسی کامپیوتر، موسسه آموزش عالی فردوس، مشهد ۴- دانشجوی مقطع دکتری گروه مهندسی کامپیوتر، دانشگاه شهید بهشتی

(دریافت: ۹۸/۰۱/۱۷؛ پذیرش: ۹۷/۰۴/۱۸)

چکیده

تفاوت‌های موجود بین داده‌های متنی و داده‌های چندرسانه‌ای مانند تصاویر از جمله حجم زیاد تصاویر و همبستگی پیکسل‌های مجاور موجب شده که روش‌های رمزنگاری سنتی برای رمز کردن این داده‌ها کارایی لازم را نداشته باشند. در این مقاله، با به‌کارگیری نگاشت‌های آشوب و اتوماتای سلولی تک بعدی حافظه‌دار، روش جدیدی برای رمزنگاری تصاویر ارائه شده است که در گام جایگشت، از نگاشت آشوب خطی Piecewise و در گام پخش از نگاشت آشوب لجستیک و اتوماتای سلولی استفاده می‌نماید. ویژگی بارز الگوریتم ارائه‌شده، قابلیت بررسی صحت داده در سطح قالب است که در کاربردهایی مانند کاربردهای نظامی و پزشکی که داده‌های تصویر یا بخشی از آن بسیار حساس هستند دارای اهمیت بالایی است. نتایج بررسی‌های متفاوت از جمله بررسی حساسیت کلید و بررسی‌های آماری نشان‌دهنده‌ی حساسیت بالای روش پیشنهادی است، همچنین بررسی انواع حملات مختلف، نشان داد که روش پیشنهادی مقاومت مناسبی در برابر آنها دارد.

واژگان کلیدی

رمزنگاری تصویر، نظریه آشوب، نگاشت‌های آشوب، اتوماتای سلولی برگشت‌پذیر

۱- مقدمه

یکی از مسایل به‌کارگیری شبکه‌های عمومی مانند اینترنت برای انتقال اطلاعات، عدم امنیت آن‌ها است، به‌طوری که یک فرد سودجو می‌تواند اقدام به سرقت یا دست‌کاری اطلاعات نماید [۱]. رمزنگاری پیام‌ها یکی از راه‌حل‌های مواجهه با این مشکل است. پیام‌ها تنها شامل اطلاعات متنی نیستند بلکه در بسیاری از موارد، اطلاعات حمل شده توسط پیام‌ها، اطلاعات چندرسانه‌ای از جمله تصاویر می‌باشند. هنگامی که در مورد انتقال تصاویری چون نقشه پایگاه نظامی، نقشه‌ی ساختمان یک بانک و یا تصاویر نظامی‌گرفته شده توسط یک ماهواره بحث می‌شود، اهمیت انتقال با امنیت این نوع اطلاعات نیز جایگاه ویژه‌ای می‌یابد. روش‌های رمزنگاری زیادی برای داده‌های متنی وجود دارند [۲]، اما با توجه به تفاوت‌های موجود بین داده‌های متنی و داده‌های تصویری، استفاده از روش‌های رایج رمزنگاری داده‌های متنی برای رمز کردن داده‌های تصویری، به دو دلیل کارا نخواهد بود:

- اندازه داده‌های تصویری به مراتب بالاتر از داده‌های متنی است. بنابراین سیستم‌های رمزنگاری رایج، در صورت استفاده مستقیم برای رمزکردن تصاویر، بسیار زمانبر خواهند بود.
- داده‌های متنی رمزشده بعد از رمزگشایی، باید کاملا همانند متن اصلی باشند، ولی این قید در مورد داده‌های تصویری صادق نیست، روش‌های رمزنگاری تصاویر می‌توانند به گونه‌ای باشند که تصویر رمزگشایی شده تا حدی که مفهوم و محتوای تصویر اصلی تغییر نکند، با تصویر اصلی تفاوت داشته باشد.

با توجه به موارد مطرح شده، روش‌های گوناگون رمزنگاری مخصوص تصاویر به وجود آمدند که از بین آنها می‌توان به الگوریتم‌های مبتنی بر زبان‌های پیمایشی، الگوریتم‌های مبتنی‌بر نظریه آشوب، الگوریتم‌های مبتنی‌بر ساختارهای درختی و سایر روش‌های متقارن اشاره کرد [۳]. یکی از الگوریتم‌های رمزنگاری تصاویر، مبتنی بر اتوماتای سلولی می‌باشد که به سبب پیاده‌سازی سریع، آسان و سرعت بالای آن، در این مقاله مورد استفاده قرار گرفته است [۵-۴]. به‌طور دقیق‌تر با به‌کارگیری نگاشت‌های آشوب و اتوماتای سلولی تک بعدی حافظه‌دار، روش جدیدی برای رمزنگاری تصاویر ارائه شده است که در گام جایگشت، از نگاشت آشوب خطی Piecewise و در گام پخش از نگاشت آشوب لجستیک و اتوماتای سلولی استفاده می‌نماید [۷-۶]. ویژگی بارز

الگوریتم ارائه شده، قابلیت بررسی صحت داده در سطح قالب است که در کاربردهایی مانند کاربردهای نظامی و پزشکی که داده‌های تصویر یا بخشی از آن بسیار حساس هستند دارای اهمیت بالایی است.

ادامه این مقاله به‌صورت زیر می‌باشد. در بخش ۲، ابتدا به مرور برخی تلاش‌های پیشین در حوزه رمزنگاری تصاویر که از اتوماتای سلولی و نظریه آشوب برای این مسئله بهره برده‌اند خواهیم پرداخت. در بخش ۳، با معرفی مقدمات اولیه در مورد نظریه آشوب و اتوماتای سلولی، روش پیشنهادی معرفی خواهند شد و همچنین برخی جزییات پیاده‌سازی سخت افزاری آن نیز بیان خواهد شد.

۲- کارهای پیشین

با توجه به این‌که ارزیابی عملکرد الگوریتم‌های رمزنگاری تصاویر بر پایه نتایج آن‌ها در برابر برخی آزمون‌ها و نیز میزان مقاومتشان در برابر تعدادی از حملات سنجیده می‌شود، در دو زیربخش ابتدایی این بخش، ابتدا این آزمون‌ها و حملات معرفی شده‌اند و سپس در زیربخش سوم برخی الگوریتم‌های موجود که مبتنی‌بر اتوماتای سلولی و نظریه آشوب هستند معرفی شده و ویژگی‌های آن‌ها به اختصار شرح داده شده است.

۲-۱- حملات روی سیستم‌های رمزنگاری تصاویر

بررسی سیستم‌های رمزنگاری داده‌های تصویری با استفاده از برخی حملات که در زیر به‌صورت مختصری شرح داده شده‌اند انجام می‌شوند. در تمامی این حملات فرض بر آن است که مهاجم، اطلاعات کافی راجع به الگوریتم استفاده شده را داراست [۸-۹].

- **حمله فقط تصویر رمزشده[1]**

در این حمله فرض می‌شود که مهاجم فقط دارای یک یا چند تصویر رمزشده است و اطلاعی از کلید خصوصی سیستم رمزنگاری ندارد. به عبارت دیگر در این حمله مهاجم باید تنها کلید خصوصی را از روی تصویر رمزشده مشخص کند. البته مهاجم، روش رمزنگاری استفاده شده به همراه نوع و فرمت تصویر رمزشده را می‌داند [۱۰].

- **حمله تصویر ساده معلوم[2]**

در این حمله فرض می‌شود که مهاجم به تعدادی تصویر و تصویرهای رمزشده معادل آنها تحت یک کلید خصوصی دسترسی دارد. مهاجم بایستی با توجه به این اطلاعات، کلید خصوصی سیستم رمزنگاری را مشخص کند [۱۱].

- **حمله تصویر ساده انتخابی[3]**

در این حمله مهاجم توانایی این را دارد که برای تصویرهای دلخواه خود، تصویرهای رمزشده متناظر با آنها را داشته باشد. این حمله به مراتب خطرناک‌تر از حملات قبلی است زیرا مهاجم می‌تواند تصویرهایی را انتخاب کند که درصورت رمز شدن این تصویرها و به‌دست آوردن تصویرهای رمزشده معادل آنها، اطلاعات بیشتری راجع به کلید خصوصی در اختیارش قرار دهد [۱۲].

- **حمله تفاضلی[4]**

برای امن بودن یک سیستم رمزنگاری تصاویر در برابر حمله تفاضلی، سیستم رمزنگاری باید به گونه‌ای باشد که کوچک‌ترین تغییر در تصویر اصلی باعث تغییرات فراوانی در تصویر رمز شده شود [۱۳]. برای بررسی میزان تغییرات حاصل از یک پیکسل تصویر اصلی در تصویر رمز شده دو معیار NPCR و UACI وجود دارد که به‌صورت زیر تعریف می‌شوند:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times M} \times 100 \qquad (۱)$$

$$UACI = \frac{1}{N \times M}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100 \qquad (۲)$$

که در آن، C_1 و C_2 دو تصویر رمزشده هستند که دو تصویر اصلی مربوط به آنها در یک پیکسل با هم تفاوت دارند و مقدار در مقیاس خاکستری پیکسلی که در موقعیت (i,j) در C_1 و C_2 قرار دارد به‌صورت $C_1(i,j)$ و $C_2(i,j)$ نمایش داده می‌شود. N و M به ترتیب عرض و طول تصویر رمز شده هستند. $D(i,j)$ براساس $C_1(i,j)$ و $C_2(i,j)$ به این صورت مشخص می‌شود که $D(i,j) = 1$ اگر و تنها اگر $C_1(i,j) \neq C_2(i,j)$، در غیر این‌صورت $D(i,j) = 0$ می‌باشد.

۳- آزمون‌های آماری[5]

یکی از روش‌های بررسی میزان امنیت الگوریتم‌های رمزنگاری تصاویر، انجام برخی تحلیل‌های آماری بر روی تصاویر حاصل از این الگوریتم‌هاست. در این زیربخش، به معرفی برخی از این تحلیل‌ها پرداخته شده است [۴-۵]:

[1] Cipher-image only attack
[2] Known plain-image attack
[3] Chosen plain-image attack
[4] Differential attack
[5] Statistical analysis

- **نمودار فراوانی رنگ** [1]

این نمودار برای بررسی فراوانی رنگ‌های یک تصویر مورد استفاده قرار می‌گیرد. نمودار فراوانی رنگ تصویر اصلی و تصویر رمزشده متناظر با آن باید کاملا نسبت به هم متمایز و متفاوت باشد.

- **همبستگی پیکسل‌های مجاور** [2]

فرآیند این تحلیل بدین صورت است که ابتدا ۱۰۰۰۰ جفت از پیکسل‌هایی که به صورت افقی در تصویر مجاور هم هستند را در نظر گرفته و سپس ضریب همبستگی r_{xy} برای هر جفت پیکسل با استفاده از فرمول زیر محاسبه می‌شود [۲۷]:

$$cov(x,y) = E((x - E(x))(y - E(y))) \quad (۳)$$

$$r_{xy} = \frac{cov(x,y)}{sqrtD(x)sqrtD(x)} \quad (۴)$$

که x و y مقادیری در مقیاس خاکستری برای دو پیکسل مجاور و $D(X) = (\frac{1}{N})\sum_{i=1}^{N}(x_i - y_i)$ و $E(X) = (\frac{1}{N})\sum_{i=1}^{N} x_i$ می‌باشد. همچنین عملیات مشابهی برای پیکسل‌هایی که به صورت عمودی و قطری مجاور هم هستند می‌توان انجام داد. نتیجه این آزمون‌ها و ضرایب به‌دست‌آمده برای تصویر رمز شده باید نزدیک به صفر باشد.

- **متفاوت بودن تصویر رمز شده از تصویر اصلی**

برای بررسی این مطلب که تصویر رمز شده چه مقدار با تصویر اصلی تفاوت دارد معیاری با نام PSNR[3] استفاده می‌شود که مهم‌ترین و پرکاربردترین معیار برای اندازه‌گیری کیفیت تصویرهای بازسازی شده در روش‌های رمزنگاری تصاویری که مقادیری از داده‌های تصویری در آنها از بین می‌رود، می‌باشد [18]. علت استفاده از این معیار در سیستم‌های رمزنگاری تصاویر، محاسبه مقدار تفاوت تصویر اصلی و تصویر رمز شده است تا مشخص شود چه مقدار اطلاعات می‌توان از تصویر رمز شده درباره تصویر اصلی کسب کرد. PSNR با استفاده از فرمول زیر بیان می‌شود:

$$PSNR = 20 \times \log_{10}\left(\frac{(2^n - 1)\sqrt{N \times N}}{\sum_{i=1}^{N}\sum_{j=1}^{N}|secretimage(i,j) - encryptedimage(i,j)|^2}\right) \quad (۵)$$

در رابطه فوق، N اندازه یک بعد تصویر مربعی و n تعداد بیت لازم برای نمایش هر پیکسل می‌باشد.

۳-۱- مرور کارهای پیشین

در روش‌های مبتنی‌بر آشوب، طراحی تابعی که قرار است برای پخش استفاده شود، کاری چالش برانگیز است، چرا که این تابع باید به گونه‌ای باشد که مقاومت در برابر حملات تصویر ساده معلوم و تصویر ساده انتخابی حاصل گردد [۲۳-۲۱] و [۲۷]. به‌طور مثال در [۲۷] از یک سیگنال از پیش پردازش شده سیستم آشوب چن به‌عنوان تابع پخش استفاده شده است که بعداً نشان داده شد که ایرادهای اساسی در برابر حملات متن ساده معلوم و تصویر ساده انتخابی دارد [۲۰]. در [۲۱] امنیت روش ارائه‌شده در [۴۸] مورد بررسی قرار گرفت و تعدادی نقص و ضعف کشف شد که عموماً به دلیل یک معماری پخش ضعیف هستند. در [۲۸] لی و چن تابع پخش طرح‌های [۳۲-۲۹] را همزمان مورد بررسی قرار داده و مشکلاتی از قبیل نقص امنیتی در تابع پخش یافتند، بنابراین، بسیار مهم است که یک سیستم رمزنگاری آشوب محور با یک سازوکار پخش قوی ارائه شود. به عنوان مثال ژانگ و همکاران در [۳۳] از عملگرهای موجود روی دنباله DNA برای رمز کردن اطلاعات تصاویر استفاده کردند. آن‌ها سپس نگاشت‌های آشوب را با عمل جمع دنباله DNA ترکیب نمودند تا سیستم رمزنگاری را پیاده سازی کنند. در [۳۴] یک دنباله شبه تصادفی S1 توسط یک نگاشت تولید شده و سپس آن را به یک دنباله طولانی شبه تصادفی S2 توسعه داده و در نهایت با استفاده از آن‌ها یک ماتریس جایگشت تولید کرده‌اند. در [۳۵] در گام رمزنگاری (پخش) از یک سازوکار بازخورد محور و وابسته به ورودی استفاده شده تا پارامترهای فعلی رمزنگاری را با اطلاعات از پیش رمز شده ترکیب کرده و پیکسل‌ها را رمز کنند.

برای یک سیستم رمزنگاری مهم است که به اندازه کافی سریع باشد تا بتواند مقدار عظیم داده تصویر را رمز کند. کاندیدی مناسب برای رفع این نیاز اتوماتای سلولی است. به دلیل پیاده‌سازی سخت‌افزاری ساده، اتوماتای سلولی در رمزنگاری تصویر نیز مورد استفاده قرار گرفته است [۳۷-۳۶]. در این بخش به بررسی چند سیستم رمزنگاری پیشنهاد شده در این زمینه پرداخته شده است.

- **روش ریوسانگ یه**

در این مقاله، یک الگوریتم رمزنگاری تصاویر با یک ساختار بهینه جایگشت-پخش ارائه شده است [۲۲ و ۳۸]. در هر دو مرحله جایگشت و پخش از نگاشت‌های آشوب استفاده شده است. در

[1] Histogram
[2] Correlation of adjacent pixels
[3] Peak Signal to Noise Ratio

مرحله جایگشت، نگاشت آرنولد تعمیم یافته به‌کار گرفته می‌شود تا دنباله آشوب $\{(x_k, y_k), \mathrm{k} = 0,1, \dots\}$ تولید گردد. سپس دنباله مختصات xها $\{x_k, k = 1, \dots, W \times H\}$ که در آن H و W به ترتیب طول و عرض تصویر هستند و دنباله مختصات yها $\{y_k, k = 1, \dots, W \times H\}$ مرتب می‌شوند تا دو مجموعه ترتیب اندیس‌ها به منظور جایگشت تصویر به دست آید. برای بهبود مرحله پخش از یک فرایند دو طرفه پخش استفاده شده است که در آن یک نگاشت تعمیم‌یافته آرنولد و یک نگاشت انتقال برنولی تعمیم‌یافته به‌کار گرفته شده است تا دو دنباله از مقادیر خاکستری شبه تصادفی به‌دست آید. سپس از این دو دنباله برای تغییر مقادیر خاکستری پیکسل‌ها استفاده می‌شود. نکته قابل توجه این است که این دو دنباله نه تنها به پارامترهای کنترل و شرایط اولیه نگاشت‌های آشوب حساس هستند، بلکه شدیدا به تصویر رمز نشده نیز همبستگی دارند و باعث مقاومت این روش در برابر حملات تصویر ساده معلوم و تصویر ساده انتخاب شده می‌شوند.

- **روش اسماعیل و همکاران**

روش اسماعیل و همکاران [۳۵] یک الگوریتم رمزنگاری کلید متقارن است که در آن به طور مستقیم از پارامترهای سیستم و شرایط اولیه نگاشت‌های آشوب به‌عنوان کلید استفاده نشده است؛ بلکه از این پارامترها در تولید یک کلید خارجی استفاده شده است. همچنین در این سیستم از روش بازخورد استفاده شده است.

- **روش ژنگ و همکاران [۳۹]**

روش ژنگ و همکاران، یک طرح رمزگذاری تصویر جدید براساس اتوماتای سلولی دو بعدی متعادل است. در این طرح، یک تصویر تصادفی با همان ابعاد تصویر سری که قرار است رمز شود، اولین بار توسط یک مولد عدد شبه تصادفی تولید می‌شود. سپس، تصویر تصادفی به‌طور متناوب با دو قانون خاص مربوط به اتوماتای سلولی دو بعدی و متعادل تکامل پیدا کرده، در نهایت تصویر رمزشده از عمل XOR بیتی، بیت‌های تصویر تکامل یافته و تصویر سری به‌دست می‌آید. مزیت روش ژنگ و همکارانش دارا بودن فضای بسیار بزرگ کلید، ساختار پیچیده رمزنگاری و سرعت بالای رمزگذاری/رمزگشایی می‌باشد.

- **روش ری و همکاران [۴۰]**

این روش برای رمزنگاری تصاویر دیجیتالی مورد استفاده قرار می‌گیرد. تصویر سری در این روش به یک مشبکه سه بعدی تبدیل می‌شود. پروتکل استفاده شده در این سیستم دارای دو بخش زیر می‌باشد:

- عمل جایگشت در این روش توسط یک نگاشت خاص مبتنی بر نظریه آشوب انجام می‌شود.
- عمل پخش نیز در این سیستم رمزنگاری توسط یک اتوماتای سلولی سه بعدی انجام می‌پذیرد.

نشان داده شد که این روش مقاومت مناسبی در برابر اکثر حملات شناخته شده در زمینه رمزنگاری تصاویر دارد.

- **روش وانگ و همکاران [۴۱]**

روش وانگ یک سیستم رمزنگاری تصاویر، مبتنی‌بر نظریه آشوب و اتوماتای سلولی است. این روش از رفتار آشوب‌گونه و پیچیده یک نگاشت لجستیکی و یک اتوماتای سلولی برگشت‌پذیر استفاده می‌کند. در این روش مقادیر پیکسل‌ها به واحدهایی چهار بیتی تقسیم می‌شود و سپس در گام جایگشت از یک جریان کلید که توسط نگاشت لجستیک مورد نظر تولید شده است، استفاده می‌شود و در گام پخش نیز از اتوماتای سلولی مطرح شده در بالا استفاده می‌گردد. این روش رمزنگاری که جزء روش‌های متقارن محسوب می‌شود، دارای امنیت مناسب بوده و در برابر حملات تفاضلی مقاومت مناسبی از خود نشان می‌دهد.

- **روش ابدو و همکاران [۴۲]**

براساس اتوماتای سلولی ابتدایی، یک الگوریتم رمزنگاری تصویر جدید توسط ابدو و همکارانش ارائه شده است. در این روش از یک نوع خاص اتوماتای سلولی ابتدایی با همسایگی پیوسته و تعداد خاصی قانون حلقوی که توسط جریان کلید مورد استفاده قرار می‌گیرند، استفاده شده است. در این روش از شبکه‌های عصبی و مفاهیم نظریه آشوب برای تولید جریان کلید استفاده شده است که این امر خود باعث افزایش فضای کلید و افزایش امنیت این سیستم در مقابل حملات آماری و تفاضلی شده است.

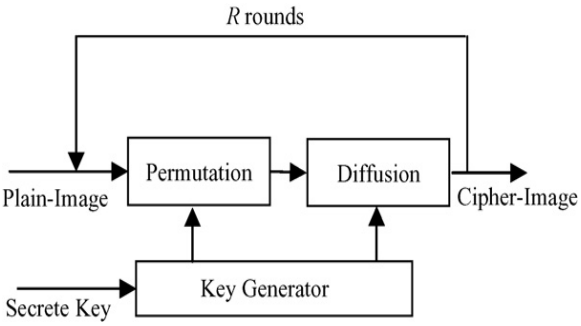
در برخی کارهای پیشین رویکردهای ترکیبی با سایر الگوریتم‌ها مطرح شده است. الگوریتم‌هایی از سایر حوزه‌های علوم کامپیوتر از جمله بیوانفورماتیک [۴۳]، تبدیل موجک [۴۴] و الگوریتم‌های هوش مصنوعی [۴۵ و ۴۶] مورد استفاده قرار گرفته‌اند.

۴- نظریه آشوب و اتوماتای سلولی

نظر به این که روش پیشنهادی بر مبنای نظریه آشوب و اتوماتای سلولی می‌باشد، در این بخش به معرفی مختصری از این دو موضوع خواهیم پرداخت.

۴-۱- سیستم‌های رمزنگاری تصاویر مبتنی بر نظریه آشوب

نظریه آشوب از سال ۱۹۷۰ در بسیاری از تحقیقات علمی مطرح شد. نظریه آشوب برای مطالعه رفتار سیستم‌های پویا که بسیار حساس به وضعیت اولیه بودند، استفاده می‌شد [۲۴-۱۹]. از سال ۱۹۹۰ رابطه نزدیک این نظریه با رمزنگاری مورد توجه قرار گرفت و از آن برای ساخت سیستم‌های رمزنگاری استفاده گردید. برای سیستم‌های رمزنگاری مبتنی‌بر نظریه آشوب فواید و برتری‌هایی نسبت به سیستم‌های رمزنگاری سنتی همچون امنیت بالا، سرعت مناسب و سربار محاسباتی قابل قبول بیان شده است. یک ساختار جایگشت-پخش به صورت شکل (۱) می‌باشد:



شکل (۱): ساختارهای جایگشت-پخش [۱۹]

در زمینه رمزنگاری تصاویر، در قسمت جایگشت، مکان پیکسل‌های مربوط به تصویر جابجا می‌شود ولی مقدار این پیکسل‌ها بدون تغییر باقی خواهد ماند. در قسمت پخش، مقدار پیکسل‌ها تغییر می‌کند به طوری که کوچک‌ترین تغییر در مقدار یک پیکسل در تصویر اصلی باعث تغییر مقادیر زیادی از پیکسل‌ها در تصویر رمز شده خواهد شد. این دو قسمت در ساختار گفته شده تکرار شونده محسوب می‌شوند. از نظریه آشوب به‌عنوان یک نگاشت در هر کدام از این دو قسمت به منظور تغییر مکان و یا تغییر محتوای پیکسل‌ها استفاده می‌شود.

۴-۲- اتوماتای سلولی

اتوماتای سلولی، سیستم‌های پویایی به‌صورت زمان و فضا گسسته هستند [۵-۱]. در حالت کلی یک اتوماتای سلولی، شامل آرایه‌ای نامتناهی از اجزاست که به آن‌ها سلول گویند. هر یک از سلول‌ها در هر زمان دارای یک حالت می‌باشد که از یک مجموعه محدود انتخاب می‌شود. حالت یک سلول با گذشت زمان و براساس قوانین محلّی تغییر می‌کند.

اتوماتای سلولی دودویی تک بعدی حالت متناهی[1] عبارت است از آرایه تک بعدی متناهی از n شیء یکسان که همان سلول‌ها هستند. هر یک از سلول‌ها، در هر زمان یک حالت دارند که از مجموعه $\sigma \in \{0,1\}$، انتخاب می‌شود. سلول‌ها با اندیس شناخته می‌شوند و iامین سلول، که $1 \le i \le n$، به صورت $< i >$ و حالت آن در زمان T با $a_i^{(T)}$ نشان داده می‌شود. حالت سلول‌ها با گذشت زمان، بطور همزمان و با توجه به یک تابع انتقال محلی تغییر می‌کند. حالت بعدی سلول به متغیرهای این تابع بستگی دارد که شامل حالت خود سلول و حالت همسایگان آن سلول در زمان جاری می‌باشد. همسایگی انواعی دارد که معمولاً همسایگی متقارن در نظر گرفته می‌شود. برای سلول $< i >$، همسایگی متقارن به شعاع r به صورت زیر تعریف می‌شود:

$$N = \{< i - r >, \dots, < i >, \dots, < i + r >\} \qquad (۶)$$

تابع گذار محلی[2] برای اتوماتای سلولی با شعاع همسایگی r به صورت زیر می‌باشد:

$$f: (Z_2)^{2r+1} \to (z_2) \qquad (۷)$$

حالت سلول iام در زمان $T+1$ به‌صورت زیر به‌دست می‌آید:

$$a_i^{T+1} = f\left(N_i^{(T)}\right), 0 \le i \le N-1 \qquad (۸)$$

که در آن، $N_i^{(T)} \in (Z_2)^{2r+1}$ بیانگر حالات همسایه‌های $< i >$ در زمان T می‌باشد.

بردار $C^T = \left(a_{0,\dots,}^T a_{N-1}^T\right)$ را پیکربندی[3] اتوماتای سلولی در زمان T، و $C^{(0)}$ را پیکربندی اولیه آن می‌نامند. مجموعه تمام پیکربندی‌های ممکن برای CA به صورت C نشان داده می‌شود. واضح است که $|C| = 2^N$. دنباله $C^0, \dots, C^T, \dots, C^K$ را تکامل[4] CA از مرتبه k گویند. تابع سراسری برای CA به صورت تبدیل خطی $\Phi : C \to C$ می‌باشد که پیکربندی CA را در زمان بعدی مشخص می‌کند، یعنی $C^{T+1} = \Phi(C^T)$.

اگر برای اتوماتای سلولی CA، Φ نگاشتی دوسویی (یک به یک و پوشا) باشد، اتوماتای سلولی دیگری با تابع سراسری Φ^{-1} وجود دارد، که به آن وارون CA گویند. وقتی اتوماتای وارون برای یک CA وجود داشته باشد، آن را وارون‌پذیر گویند و تولید $C^{(T-1)}$ از روی C^T ممکن است، یعنی تکامل به عقب امکان‌پذیر است [۱۶]. اگر تابع گذار محلی برای یک CA با شعاع همسایگی r، به‌صورت زیر باشد:

[1] One-dimensional finite Boolean cellular
[2] Local transition function
[3] Configuration
[4] Evolution

$$a_i^{T+1} = \sum_{j=-r}^{r} a_j a_{i+j}^{(T)} \bmod(2) \quad 0 \le i \le N-1 \qquad (۹)$$

که به‌ازای هر j، $a_j \in \mathbb{Z}_2$، به CA، اتوماتای سلولی خطی از مرتبه r، LCA[1] گویند. از آنجا که در همسایگی متقارن به شعاع r، تعداد $2r+1$ سلول وجود دارد، تعداد کل LCAها برابر 2^{2r+1} می‌باشد. هر یک از LCAها با عدد صحیح w، که آن را شماره قانون می‌نامند، مشخص می‌شوند، w برای LCA رابطه بالا، از طریق رابطه زیر به‌دست می‌آید:

$$W = \sum_{j=-r}^{r} a_j 2^{r+j} \qquad (۱۰)$$

در CAهایی که تاکنون بحث کردیم، حالت هر سلول در زمان $T+1$ فقط به پیکربندی همسایه‌هایش در زمان T بستگی دارد، که به آن‌ها CAهای بدون حافظه[2] گویند. با این وجود می‌توان حالتی را در نظر گرفت که حالت هر سلول در زمان $T+1$ علاوه‌بر حالت همسایه‌ها در زمان T به حالت گروه‌های مختلف از سلول‌ها و در زمان‌های $T-1, T-2, \ldots$ نیز وابسته باشد، به چنین ماشین‌هایی اتوماتای سلولی با حافظه MCA[3] گویند [۲۵-۲۶]

در این مقاله، گونه خاصی از MCA به نام MCA خطی مرتبه tام (LMCA[4]) [۲۶]، با تابع گذار محلی زیر به کار برده شده است و حالت سلول در زمان T+1 به‌صورت زیر محاسبه می‌شود:

$$a_i^{T+1} = f_1(N_i^T) + f_2(N_i^{T-1}) + \cdots + f_t(N_i^{T-t+1}), 0 \le i \le N-1 \qquad (۱۱)$$

که در آن f_i، $0 \le i \le t$، تابع گذار محلی برای LCA با شعاع r می‌باشد. در چنین ماشینی، برای شروع تکامل LMCA به t پیکربندی اولیه، $C^{(0)}, \ldots, C^{(T-1)}$، نیاز است. در این رابطه، N همسایگی متقارن به شعاع r می‌باشد. اما برای این‌که چنین LMCAای وارون‌پذیر باشد، گزاره زیر در نظر گرفته می‌شود:

اگر $f_t\left(N_i^{(T-t+1)}\right) = a_i^{(T-t+1)}$، آن‌گاه LMCA با تابع گذار داده شده در معادله بالا وارون‌پذیر است و وارون آن یک LMCA با تابع گذار محلی زیر می‌باشد:

$$a_i^{(T+1)} = \sum_{m=0}^{t-2} f_{t-m-1}(N_i^{T-m}) + a_i^{(T-t+1)} \, mod(2), \; 0 \le i \le N-1 \qquad (۱۲)$$

۵- روش جدید پیشنهادی

در این بخش، یک الگوریتم رمزنگاری جدید برای تصاویر با استفاده از نگاشت‌های آشوب و یک LMCA تک بعدی ارائه می‌شود. کلیدهای مخفی در این طرح، همان شرایط اولیه نگاشت‌های آشوب می‌باشد. شماره قوانین LMCA نیز می‌تواند به صورت عمومی اعلام شده یا می‌تواند بخشی از کلید باشند. طرح شامل ۴ گام است. گام اول، گام جایگشت می‌باشد که در آن پیکسل‌های تصویر ساده با استفاده از یک نگاشت آشوب بُر می‌خورند. گام دوم، گام رمزنگاری است که در آن اتوماتای سلولی حافظه‌دار تک بعدی به کار گرفته شده است تا پیکسل‌های تصویر بُرخورده را درهم بریزد. گام سوم، گام رمزگشایی است که در آن تصویر ساده از تصویر رمزشده، بازیابی می‌شود. آخرین گام، گام بررسی صحت داده می‌باشد که به منظور کشف هرگونه دستکاری بر روی تصویر در حین انتقال تعبیه شده است. در ادامه جزییات هر یک از این چهار گام بیان شده است.

۵-۱- گام جایگشت

ورودی این گام، تصویر ساده P، و خروجی آن تصویر بُرخورده P` می‌باشد. در این گام، از نگاشت آشوب خطی Piecewise استفاده کرده‌ایم که فرمول آن مطابق زیر است:

$$f(x) = \begin{cases} \dfrac{x}{p} & if\ x \in [0,p) \\ \dfrac{x-p}{0.5-p} & if\ x \in [p,0.5) \\ f(1-x/p) & if\ x \in [0.5,1) \end{cases} \qquad (۱۳)$$

که در آن، $p \in [0, 0.5], x \in [0,1]$ به‌عنوان کلید خصوصی در نظر گرفته می‌شوند. فرایند جایگشت بر مبنای این نگاشت شامل مراحل زیر است:

۱- نگاشت خطی Piecewise را M × N بار تکرار کرده تا مقادیر عددی $\{x_1, \ldots, x_{MN}\}$ به دست آید. در اینجا N, M به ترتیب تعداد سطرها و ستون‌های تصویر P هستند.

۲- مقادیر عددی بالا را به ترتیب صعودی مرتب کرده تا مجموعه $\{\overline{x}_1, \ldots, \overline{x}_{MN}\}$ حاصل گردد.

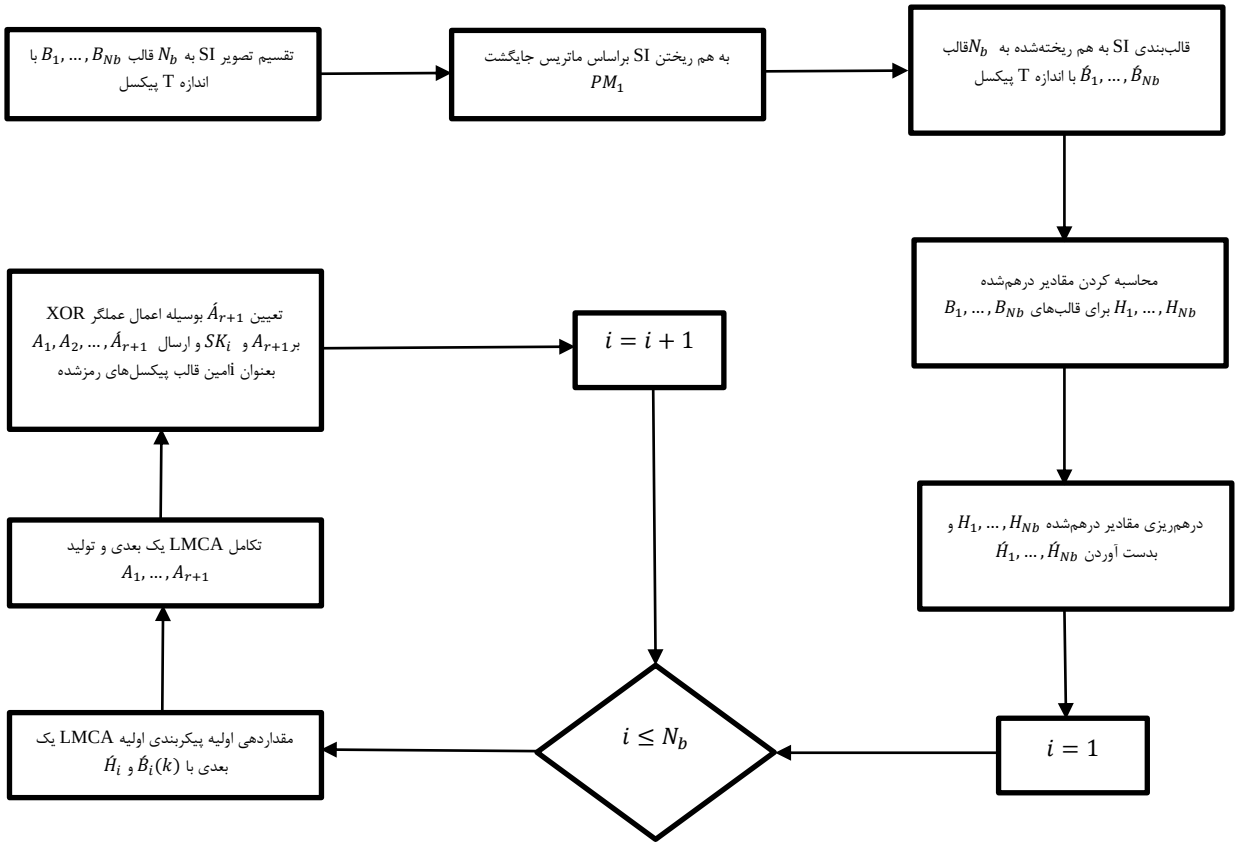
۳- مکان مقادیر $\{\overline{x}_1, \ldots, \overline{x}_{MN}\}$ را در مجموعه $\{x_1, \ldots, x_{MN}\}$ پیدا کرده و مجموعه مکان‌ها $S = \{s_1, s_2, \ldots, s_{MN}\}$ تشکیل می‌شود که در آن $\overline{x}_i$ دقیقا مقدار $\overline{x}_{s_i}$ است.

پیکسل‌های تصویر ساده p را با استفاده از مجموعه S برچسب زده تا تصویر بُرخورده P` به‌دست آید.

[1] Linear Cellular Automata
[2] Memoryless
[3] Memory cellular Automata
[4] Linear Memory cellular automata

۵-۲- گام رمزنگاری

ورودی این مرحله، تصویر بُرخورده P` و خروجی آن، تصویر رمز شده Ψ می‌باشد. فلوچارت کلی رمزنگاری در شکل (۲) نشان داده شده است. این گام به منظور تامین امنیت در مقابل حملات آماری و حمله تفاضلی در نظر گرفته شده است. جریان کلید در این مرحله نه تنها به کلید مخفی بلکه به تصویر ساده نیز وابسته است که موجب می‌شود این طرح در برابر حملات تصویر ساده معلوم و تصویر ساده انتخابی مقاوم باشد.



شکل (۲): فلوچارت رمزنگاری در روش پیشنهادی

در این گام، کلید مخفی، شرایط اولیه نگاشت لجستیک است که طبق فرمول زیر تعریف می‌شود:

$$y_{n+1} = 4y_n \times [1 - y_n] \qquad (۱۴)$$

برخلاف اغلب الگوریتم‌های رمزنگاری تصویر که رمز جریانی هستند، الگوریتم ارائه شده یک الگوریتم رمز قالبی است که در آن تصویر به n_b قالب تقسیم شده و هر قالب به‌طور جداگانه پردازش می‌شود. فرآیند دقیق این گام در زیر آمده است:

تصویر بُرخورده P` را به n_b قالب m پیکسلی تقسیم کرده که در آن $n_b = [\frac{M \times N}{m}]$، و m یک مقدار اختیاری است، البته انتخاب مقادیر بزرگتر منجر به محاسبات کمتر می‌گردد در حالی که انتخاب مقادیر کوچکتر برای m منجر به دقت بیشتر در گام بررسی صحت داده می‌گردد. بنابراین، هنگام انتخاب m باید بین این دو مورد توازن برقرار کرد. برای هر قالب $1 \le i \le n_b, B_i$ مراحل زیر را انجام می‌دهیم:

الف. مقدار درهم‌ریخته[1] قالب را طبق فرمول زیر محاسبه می‌نماییم:

$$H_i = f_h(B_i(1), \dots, B_i(m)) \qquad (۱۵)$$

که در آن، f_h یک تابع درهم‌ساز دلخواه می‌باشد و $B_i(k)$ نمایانگر kامین پیکسل از iامین قالب است.

ب. LMCA معکوس‌پذیر L از مرتبه m+2 توسط محاسبه پیکربندی اولیه $\{C^{(1)}, \dots, C^{(m+2)}\}$مطابق زیر ساخته می‌شود:

[1] Hash

- قرار بده $C^{(1)} = B_i(1), C^{(2)} = B_i(2), \dots, C^{(m)} = B_i(m)$
- قرار بده $C^{(m+1)} = H_i$ که در آن، H_i مقدار درهم‌ریخته قالب است که توسط فرمول (۱۵) محاسبه شده است.
- اگر i=1 (یعنی این قالب اولین قالب است که رمز می‌شود) $C^{(m+2)}$ را برابر با یک عدد دلخواه بین ۰ تا ۲۵۵ قرار داده و در غیر این صورت $C^{(m+2)}$ برابر با $D = B_{i-1}(1) \oplus B_{i-1}(2) \dots \oplus B_{i-1}(m)$ قرارمی‌دهیم که در واقع Xor پیکسل‌های قالب قبلی است.

ج. با شروع از پیکربندهای اولیه $\{C^{(1)}, \dots, C^{(m+2)}\}$ اتومات L را ω بار نمو داده تا پیکربندی‌های جدید $\{A_i(1), A_i(2), \dots., A_i(\mathrm{m}+1), A_i(\mathrm{m}+2)\}$ به‌دست آید. در این جا ω نیز می‌تواند به‌صورت عمومی تعیین شده یا قسمتی از کلید مخفی باشد.

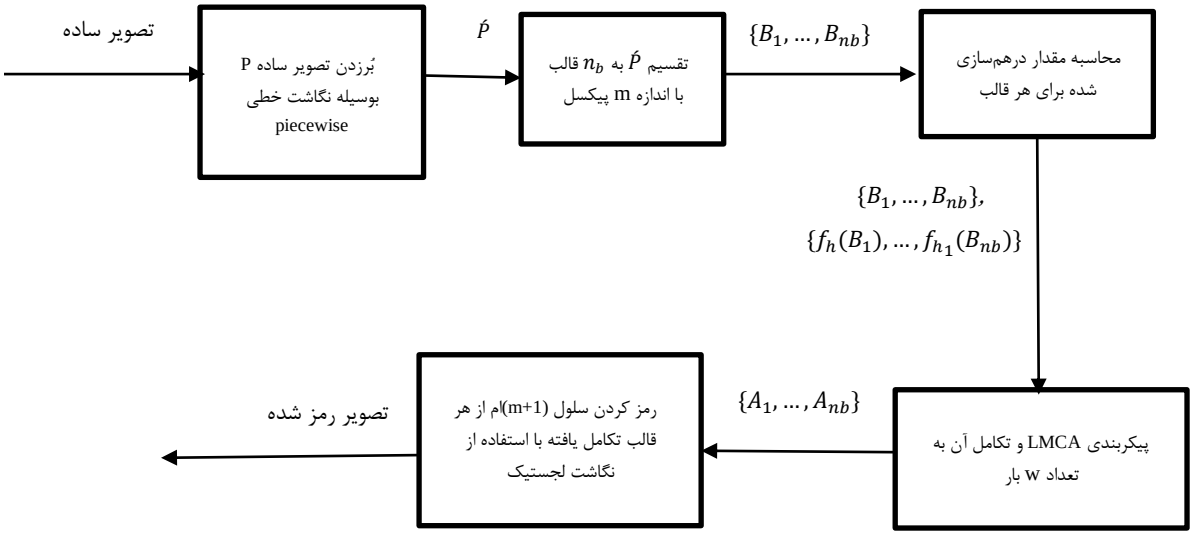
د. (m+1) امین پیکربندی از یک قالب نمو داده شده ($A_i(m+1)$) به‌صورت زیر رمز می‌شود

$k = 1 + \mathrm{mod}(A_i(1), 4)$. محاسبه می‌شود.

- نگاشت لجستیک را k بار تکرار کرده تا مقدار y به دست آید.
- مقدار $d = \lfloor mod(y \times 10^6) \rfloor$ محاسبه می‌شود.
- مقدار جدید $\{\acute{A}_i(\mathrm{m}+1) = A_i(\mathrm{m}+1) \oplus mod(d + A_i(m+2), 256)$ محاسبه می‌شود.

ذ. قالب رمزشده متناظر ψ_i برابر با مقادیر $\{A_i(1), A_i(2), \dots., \acute{A}_i(\mathrm{m}+1), A_i(\mathrm{m}+2)\}$ قرار داده می‌شود.

تصویر رمزشده ψ شامل قالب‌های رمزشده $1 \le i \le n_b, \psi_i$ است که توسط روند توضیح داده شده به‌دست‌آمده و در شکل (۳) نشان داده شده است.



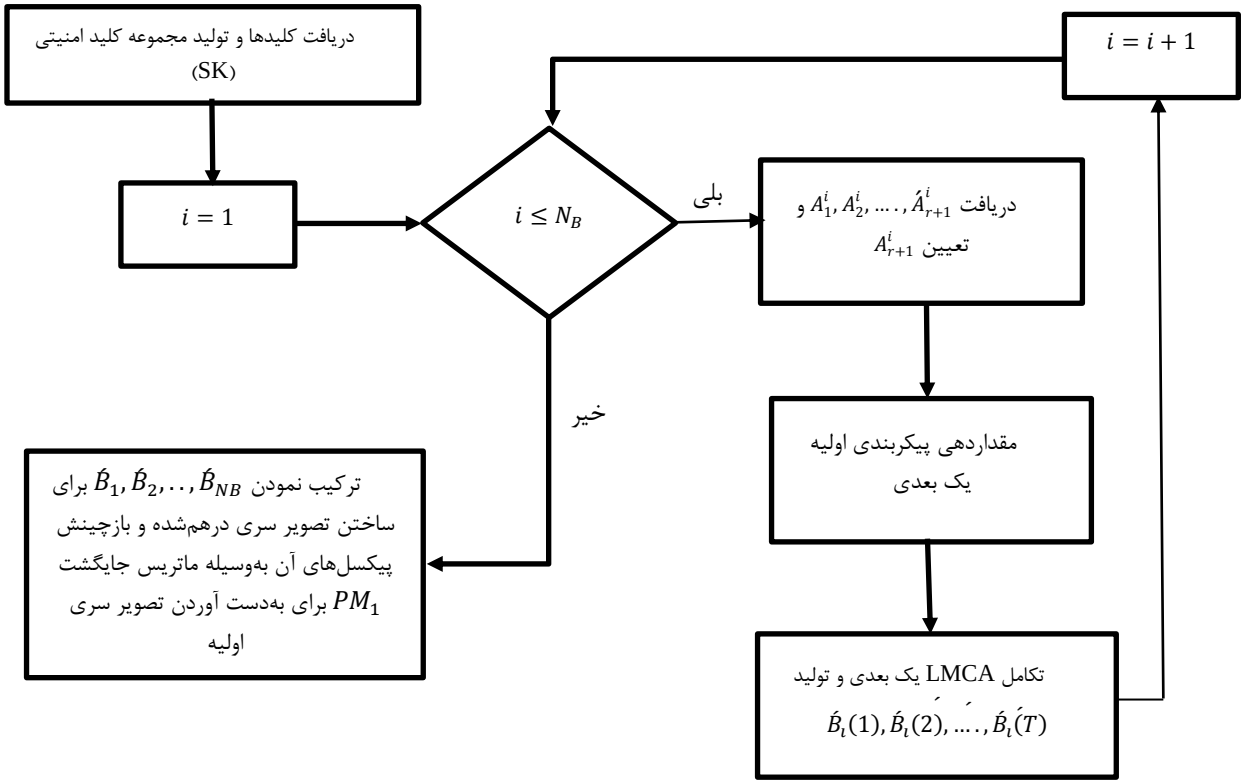
شکل (۳): گام‌های جایگشت و رمزنگاری در روش پیشنهادی

در یک مثال ساده، مراحل رمزگذاری مطرح شده برای یک پیکسل با مقدار دلخواه را تشریح می‌کنیم. با فرض مقدار ۳۷ برای پیکسل مورد نظر که معادل باینری آن برابر است با ۰۱۰۰۱۰۱، مراحل رمزگذاری را آغاز می‌کنیم.

با فرض اندازه ۷ برای هر قالب، مقدار درهم‌ریخته برای این قالب برابر بیت ۱ می‌باشد. همچنین با فرض این که مقدار درهم‌ریخته قالب قبلی باشد، مقدار پیکربندی اولیه برای اتوماتای سلولی مورد نظرمان برابر است با: ۰۱۰۰۱۰۱۱۰ . با فرض این که بعد از تکامل دادن اتوماتای سلولی دلخواه با پیکربندی اولیه ۰۱۰۰۱۰۱۱۰ به مقدار ۱۰۱۰۱۱۰۰۱ برسیم، باید با استفاده از مقدار کلید مخفی متناسب با این قالب (فرض می‌کنیم ۱۰۱۰۱۰۱۰۱ باشد) مقدار رمزشده را محاسبه و ارسال کنیم. این مقدار برابر است با ۰۰۰۰۰۱۱۰۰ که در کنار سایر قالب‌های رمزشده برای گیرنده ارسال می‌شود.

۵-۳- گام رمزگشایی تصویر

ورودی این گام، تصویر برخورده ψ و خروجی آن، تصویر رمز شده p می‌باشد. فلوچارت کلی رمزگشایی در شکل نشان داده شده است.



شکل (۴): فلوچارت رمزگشایی در روش پیشنهادی

الگوریتم رمزگشایی دقیقا مانند الگوریتم رمزنگاری است اما به ترتیب بلعکس. چون LMCA از مرتبه m+2 است برای نمو دادن آن به عقب دقیقا آخرین m+2 پیکربندی لازم است، بنابراین، رمزگشایی تصویر رمزشده بدون داشتن کلید، امکان‌پذیر نیست، زیرا در هر قالب $\psi_i = \{A_i(1), A_i(2), \dots, \acute{A}_i(m+1), A_i(m+$ 2)} یک پیکربندی A`i(m+1) با استفاده از کلید، رمز شده است. روند دقیق این کار به فرم زیر است:

$\psi_i = \{A_i(1), A_i(2), \dots, \acute{A}_i(m+1), A_i(m+2)\},\ n_b \le i \le 1$ ،

در طرف گیرنده، برای هر قالب رمزشده مراحل زیر باید انجام شود:

۱- مقدار $A_i(m+1)$ را با استفاده از فرمول
$A_i(m+1) = \acute{A}_i(m+1) \oplus \mathrm{mod}(d + A_i(m+2), 256)$
محاسبه کرده که در آن مقدار d توسط تکرار نگاشت لجستیک به‌دست می‌آید و این نیز تنها زمانی ممکن است که گیرنده مقدار کلید را بداند.

۲- $\overline{L}$ را ساخته که در واقع همان معکوس L با پیکربندی‌های اولیه است. $\{C^1 = A_i(1), C^2 = A_i(2), \dots, = C^{(m+1)} = A_i(m+1), C^{(m+2)} = A_i(m+2)\}$ و آن را ω بار نمو داده تا مقادیر $\{B_i(1), \dots, B_i(m)\}$ و همچنین مقدار H_i را که بعدا برای بررسی صحت داده استفاده می‌شود، به‌دست آید. پس از رمزگشایی تمام قالب‌ها، گیرنده تصویر برخورد P` را به‌دست می‌آورد. حال باید معکوس عمل جایگشت را انجام دهد تا تصویر ساده P را به دست آید.

در تشریح گام رمزگذاری مثالی مطرح شد که مقدار رمزشده‌ی یک قالب برابر شد با ۰۰۰۰۰۱۱۰۰. در گام رمزگشایی ابتدا با استفاده از مقدار کلید مخفی متناسب با قالب مورد نظر (۱۰۱۰۱۰۱۰۱)، گیرنده با استفاده از عملگر ⊕ مقدار پیکربندی اولیه اتوماتای سلولی را برای تکامل به عقب محاسبه می‌کند که این مقدار برابر است با ۰۱۰۰۱۰۱۱۰. گیرنده با حذف بیت‌های هشتم و نهم به مقدار رمزگشایی شده صحیح یعنی ۰۱۰۰۱۰۱ یا همان ۳۷ می‌رسد. البته برای فرایند بررسی صحت داده به مقدار بیت ۸ ام نیاز می‌باشد که در گام بررسی صحت داده، نحوه استفاده از این مقدار توضیح داده می‌شود.

۵-۴- گام بررسی صحت داده

ورودی این گام، تصویر بُرخورده P`، و خروجی آن کشف این می‌باشد که آیا تصویر دست‌کاری شده است یا نه؟ الگوریتم بررسی صحت داده به فرم زیر است.

تصویر P` را به قالب‌های m پیکسلی $\{B_i, \dots, B_{nb}\}$ تقسیم نموده و برای هر قالب B_i مراحل زیر اجرا می‌شود: $1 \le i \le n_b$

(الف) مقدار $h_i = f_h(B_i(1), \dots, B_i(m))$ را محاسبه کرده که در آن f_h همان تابع درهم‌ساز است و منظور از $B_i(k)$، kامین پیکسل iامین قالب است.

(ب) اگر مقدار H_i که در مرحله ۲ از گام رمزگشایی به‌دست آمده، با مقدار h_i برابر بود، یعنی این قالب دست‌کاری نشده است.

اگر برای هر B_i، $1 \le i \le n_b$ داشته باشیم $h_i = H_i$ آن‌گاه کل تصویر دست نخورده است.

در مثالی که در دو گام رمزگذاری و رمزگشایی برای درک بیشتر روش ارائه‌شده بیان شد، گیرنده برای بررسی صحت مقدار رمزگشایی شده (۰۱۰۰۱۰۱) باید مقدار بیت هشتم، یعنی ۱ را با حاصل جمع بولی بیت‌های مقدار رمزگشایی شده مقایسه کند که درصورت عدم تساوی این دو مقدار صحت داده رمزگشایی شده تایید نمی‌شود.

۶- ارزیابی و بررسی امنیت روش ارائه شده

در این بخش ابتدا بررسی‌های مربوط به کلید را انجام داده و سپس رفتار الگوریتم در مقابل حملات آماری و حمله تفاضلی بررسی خواهد شد. همچنین درباره مقاومت الگوریتم در برابر حملات تصویر ساده معلوم و تصویر ساده انتخابی بحث می‌شود. لازم به ذکر است با توجه به این که داده‌های تصویری با داده‌های متنی متفاوت هستند. استفاده از سیستم‌های رایج و سنتی رمزنگاری داده‌های متنی همچون DSA و RSA به دلایلی چون حجم بالای داده‌های تصویری و یا این که در رمزنگاری داده‌های تصویری برخلاف رمزنگاری داده‌های متنی، نیاز نیست که داده رمزگشایی شده دقیقا همان داده قبل از رمزنگاری باشد، کارا نمی‌باشند. بنابراین، مقایسه سیستم‌های رمزنگاری تصاویر با سیستم‌های رمزنگاری داده‌ای مرسوم نمی باشد.

۶-۱- بررسی‌های مربوط به کلید

- **فضای کلید**

یک سیستم رمزنگاری تصویر خوب، باید دارای فضای کلید نسبتاً بزرگ باشد تا بتواند در مقابل حمله با آزمون و خطا[1] مقاوم باشد. اندازه فضای کلید برابر است با تعداد کل کلیدهایی که می‌توانند در الگوریتم استفاده شوند. در روش ارائه‌شده، کلیدهای مخفی همان شرایط اولیه نگاشت خطی Piecewise، (x)، پارامترهای کنترل نگاشت خطی Piecewise، (p)، و شرایط اولیه نگاشت لجستیک، (y)، هستند. برای امنیت بیشتر، شماره قانون‌های اتوماتای سلولی را نیز می‌توان به‌عنوان کلید در نظر گرفت؛ اما در این بخش آن‌ها حساب نشده‌اند. بنابراین، اندازه کل فضای کلید برابر است با $2^{25} \times 2^{25} \times 2^{25}$ که طبق استاندارد IEEE [۴۷] برای مقابله با حمله آزمون و خطا به اندازه کافی بزرگ است [۱۱].

- **حساسیت کلید**

یک الگوریتم رمزنگاری خوب، باید نسبت به کلید مخفی حساس باشد، بدین معنی که یک تغییر کوچک در کلید منجر به ایجاد یک تغییر اساسی در تصویر رمز شده متناظر شود. برای آزمودن حساسیت پارامتر کلید K، تصویر ساده با $K = p + \Delta\delta, K = p - \Delta\delta, K = p$ رمز شده است در حالی که دیگر پارامترهای کلید بدون تغییر هستند. در این جا $\Delta\delta$ یک مقدار بسیار کوچک است و مقدار انحراف نام دارد. تصاویر رمز شده متناظر به ترتیب با I3,I2,I1 نشان داده شده‌اند. ضریب حساسیت برای پارامتر کلید K طبق فرمول زیر به‌دست می‌آید:

$$Ps(K) = \frac{1}{2 \times H \times W} \sum_{i,j} [N_S(I_1(i,j), I_2(i,j), I_3(i,j)], \quad (۱۶)$$

که در آن، $N_S(x,y) = 1$ اگر $x \neq y$ و در غیر این‌صورت $N_S(x,y) = 0$ خواهد بود. مقادیر بزرگتر برای $P_S(K)$ نمایانگر حساسیت بیشتر برای پارامتر K است.

یک آزمون روی ۴ تصویر Boat, Lake, Lena, Pepper انجام شده است که در آن پارامتر K برابر با شرایط اولیه نگاشت خطی Piecewise در نظر گرفته شده است و مقدار انحراف برابر با 10^{-10} قرار داده شد و تمامی پارامترهای دیگر کلید بدون تغییر ماند. نتایج را می‌توان در جدول (۱) مشاهده کرد که حاکی از آن است که طرح پیشنهادی دارای حساسیت بالا نسبت به کلید می‌باشد.

جدول (۱): نتایج آزمون حساسیت کلید
$\Delta\delta = 10^{-10}, K = 0.123456789$

تصویر	$P_S(K)$
Boat	۰/۹۹۶۶
Lake	۰/۹۹۵۹
Lena	۰/۹۹۶۷
Pepper	۰/۹۹۶۲

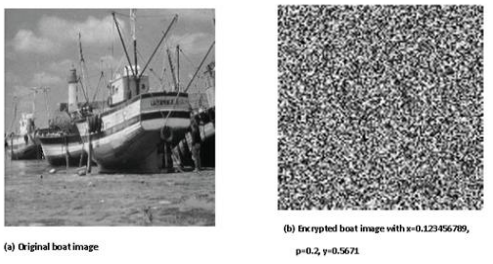
[1] Brute force attack

۶-۲- بررسی‌های آماری

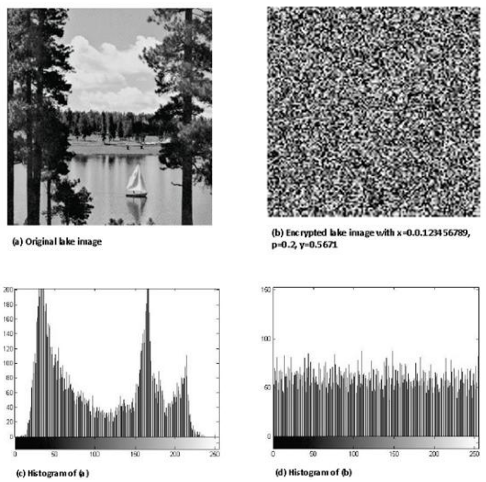
بررسی‌های آماری روی طرح ارائه شده، نمایانگر پراکندگی و اغتشاش بسیار زیاد آن بوده که تصویر رمزشده را در برابر حملات آماری شدیدا مقاوم می‌کند. این ادعا توسط یک آزمون روی نمودار فراوانی رنگ، یک آزمون روی همبستگی پیکسل‌های مجاور و یک آزمون روی آنتروپی تصویر ثابت شده است.

- **نمودار فراوانی رنگ**

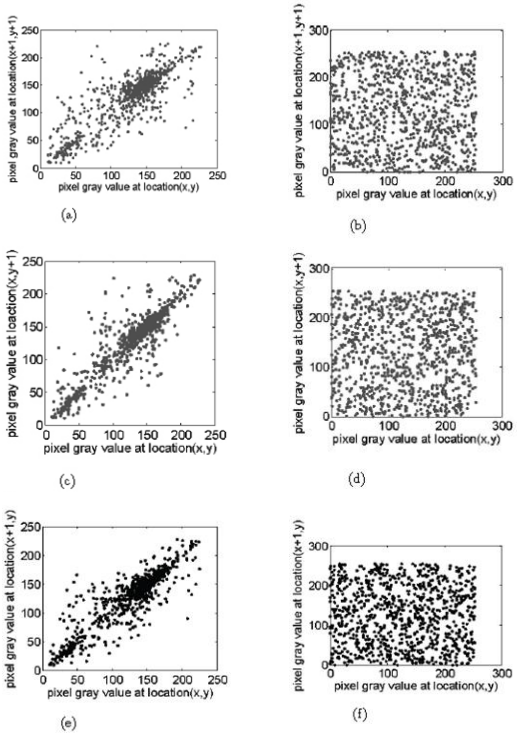
نمودار فراوانی رنگ برای دو تصویر Lake و Boat در شکل‌های (۶-۵) نمایش داده شده است. این شکل‌ها بیان می‌کنند که تصاویر رمزشده دارای فراوانی رنگ نسبتا یکنواخت بوده و بنابراین هیچ گونه اطلاعات مفیدی به مهاجم نمی‌دهند.



شکل (۵): نمودار فراوانی رنگ برای تصویر Boat



شکل (۶): نمودار فراوانی رنگ برای تصویر Lake



شکل (۷): همبستگی پیکسل‌های مجاور در تصویر Lake، ((a),(c),(e) مربوط به تصویر ساده و (b),(d),(f) مربوط به تصویر رمز شده هستند)

- **همبستگی بین پیکسل‌های مجاور**

معمولا همبستگی بسیار زیادی بین پیکسل‌های مجاور در تصاویر وجود دارد. یک الگوریتم رمزنگاری تصویر امن، باید این همبستگی را از بین ببرد تا تصویر رمزشده در مقابل حملات آماری مقاوم باشد. برای آزمون همبستگی بین پیکسل‌های مجاور، به‌صورت تصادفی ۱۰۰۰ زوج از پیکسل‌های مجاور (به طور عمودی، افقی و قطری) انتخاب شده و ضرایب همبستگی هر زوج یکبار قبل از رمزنگاری و یکبار پس از رمزنگاری با استفاده از فرمول‌های زیر محاسبه شده است:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۱۷)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x)(y_i - E(y)) \qquad (۱۸)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x)(y)^2 \qquad (۱۹)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (۲۰)$$

که در آن‌ها، x و y مقادیر خاکستری دو پیکسل مجاور هستند. ضرایب همبستگی تصاویر ساده و تصاویر رمزشده دو تصویر Lake

و Boat به‌ترتیب در شکل‌های (۷) و (۸) نمایش داده شده است. همچنین جدول (۲) نیز نتایج را نشان می‌دهد.

جدول (۱): ضرایب همبستگی پیکسل‌های مجاور در تصویر ساده و تصویر رمز شده متناظر با آن

	تصویر ساده Lake	تصویر رمز شده Lake	تصویر ساده Boat	تصویر رمزشده Boat
افقی	۰/۹۱۸۹	-۰/۰۰۶۳	۰/۹۲۸۳	-۰/۰۰۳۵
عمودی	۰/۹۰۲۸	۰/۰۰۹۵	۰/۹۴۴۴	۰/۰۰۸۹
قطری	۰/۹۲۶۶	۰/۰۰۸۹	۰/۸۹۲۷	-۰/۰۰۱۱

- **حمله آنتروپی اطلاعات**

آنتروپی اطلاعات، بارزترین ویژگی تصادفی بودن است. مقدار آنتروپی برای ۴ تصویر رمزشده توسط طرح ارائه شده، با استفاده از فرمول زیر محاسبه شده و در جدول (۳) نمایش داده شده است و دلالت بر این دارد که این تصاویر، نزدیک به یک منبع تصادفی بوده و در مقابل حمله آنتروپی مقاوم هستند [۴۸].

$$H(m) = -\sum k.p_k \log(p_k) \qquad (۲۱)$$

جدول (۲): نتایج آزمون آنتروپی

تصویر	H(m)
Boat	۷/۹۷۰۶
Lake	۷/۹۷۳۰
Lena	۷/۹۶۹۶
Pepper	۷/۹۷۱۷

- **حمله تفاضلی**

همان‌طور که گفته شده در این حمله، مهاجم یک پیکسل از تصویر ساده را تغییر داده و سعی در یافتن رابطه‌ای معنادار بین تصاویر رمزشده متناظر دارد. برای فهمیدن این که چگونه تغییر یک پیکسل در تصویر ساده روی تصویر رمزشده متناظر تاثیر می‌گذارد دو معیار NCPR و UACI را برای ۴ تصویر محاسبه کرده‌ایم که نتایج در جدول (۴) نمایش داده شده اند.

جدول (۳۰): معیارهای UACI و NPCR برای تصاویر رمز شده با تصاویر ساده دارای اختلاف جزئی

تصویر	NPCR(%)	UACI(%)
Boat	۹۹/۱۰۲۵	۳۳/۱۶۰۰
Lake	۹۹/۱۲۲۰	۳۳/۶۰۶۴
Lena	۹۹/۴۶۰۲	۳۳/۳۱۶۱
Pepper	۹۸/۹۲۰۴	۳۳/۵۷۲۴

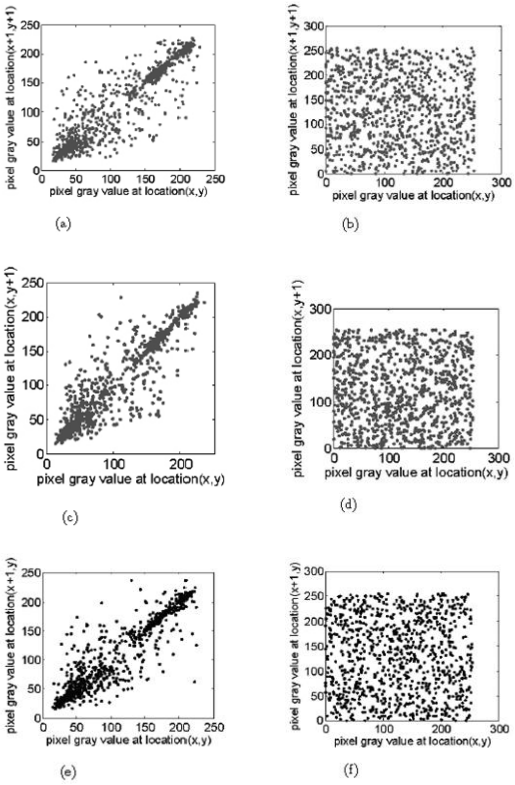
- **مقاومت در برابر حمله تصویر ساده معلوم و حمله تصویر ساده انتخابی**

در الگوریتم ارائه شده گام پخش به گونه‌ای طراحی شده که در آن یک بازخورد از تصویر رمزشده به کار گرفته می‌شود تا تعداد تکرارهای نگاشت لجستیک را در هر بار تغییر دهد. طبق فرمول $k = 1 + \mathrm{mod}(A_i(1),(4))$ که در آن، $A_i(1)$ یک بازخورد از تصویر رمزشده است و k تعداد تکرارهای نگاشت لجستیک است. بنابراین هنگامی‌که تصاویر ساده مختلف رمز می‌شوند، جریان کلید متناظر وابسته به آن تصاویر رمز شده است. مهاجم توسط رمزنگاری یک سری تصاویر خاص هیچ گونه اطلاعات مفیدی به‌دست نمی‌آورد، زیرا اطلاعات حاصله به همان تصاویر انتخاب شده مربوط است. بنابراین طرح ارائه شده در برابر حملات تصویر ساده معلوم و تصویر ساده انتخابی به شدت مقاوم است.

در جمع‌بندی این بخش، در مقایسه با روش‌های قبلی مطرح شده در این مقاله نکات و توضیحات زیر قابل بیان می‌باشد:

- روش ارائه شده در این مقاله در مقایسه با روش اسماعیل و همکاران از فضای کلید به مراتب بزرگتری برخوردار می باشد. همچنین در برابر تمامی روش‌های تحلیل آماری سیستم‌های رمزنگاری تصاویر که در این نوشتار بیان شده‌اند، روش ارائه شده نسبت به روش اسماعیل و همکاران، عملکرد بهتری را ثبت می‌کند.
- در مقایسه با روش‌های وانگ و همکاران، و ژنگ و همکاران، روش ارائه شده به لحاظ بزرگی فضای کلید، عملکرد مشابهی دارد. همچنین روش ارائه شده قابلیت بررسی داده در مقیاس‌های مختلف را فراهم می‌سازد که روش‌های دیگر مطرح شده در این مقاله چنین قابلیتی را ندارند. با توجه به نتایج مربوط به تحلیل وابستگی بین پیکسل‌های مجاور و همچنین نمودار فراوانی رنگ دو روش وانگ و همکاران [۴۱] و ژنگ و همکاران [۳۹]، می‌توان براحتی عملکرد بهتر روش پیشنهادی در این مقاله را مشاهده نمود.

با توجه به فضای کلید بزرگتری که روش پیشنهادی در مقایسه با فضای کلید حاصل از روش ارائه شده در روش ابدو و همکاران [۴۲] داراست، به‌راحتی بالاتر بودن میزان امنیت روش پیشنهادی نسبت به روش ابدو و همکاران قابل مشاده است. نکته دیگر در مقایسه این دو روش این است که برخلاف روش پیشنهادی در این مقاله، روش ابدو و همکاران فاقد پشتیبانی از بررسی صحت داده رمزگشایی شده می‌باشد.



شکل (۸): همبستگی پیکسل‌های مجاور در تصویر Boat، ((a),(c),(e) مربوط به تصویر ساده و (b),(d),(f) مربوط به تصویر رمز شده هستند)

۷- نتیجه‌گیری

در این مقاله، با استفاده از نگاشت‌های آشوب و اتوماتای سلولی تک بعدی حافظه‌دار برای رمزنگاری تصاویر روشی کارا و بهینه ارائه شد که در گام جایگشت از نگاشت آشوب خطی Piecewise و در گام پخش از نگاشت آشوب لجستیک و اتوماتای سلولی استفاده شده است. یک ویژگی بارز الگوریتم ارائه شده این است که قابلیت بررسی صحت داده را در سطح قالب دارد. این ویژگی به خصوص در کاربردهایی اهمیت دارد که داده‌های تصویر یا بخشی از آن بسیار حساس هستند. با این حال‌این برتری، به قیمت افزونگی داده[1] تمام شده، اما به دلیل کم بودن مقدار افزونگی داده (یک پیکسل به ازای هر قالب) و پیاده سازی سریع و آسان اتوماتای سلولی، الگوریتم همچنان کارا بوده و قابل استفاده برای کاربردهای عملی می‌باشد. طرح ارائه شده تمام ویژگی‌های یک سیستم رمزنگاری خوب از جمله فضای کلید بزرگ، مقاومت در برابر حملات آنتروپی، تفاضلی، تصویر ساده معلوم و تصویر ساده انتخابی را داراست. روش پیشنهادی فقط بر تصاویر مقیاس خاکستری اعمال شده است، اما می‌توان توسط آن تصاویر رنگی را نیز به صورت بهینه رمزنگاری کرد.

تقدیر و تشکر: این مقاله مستخرج از طرح پژوهشی با حمایت مالی دانشگاه آزاد اسلامی واحد قوچان می باشد.

[1] Data Extension

۸- منابع

[1] P. H. Bardell, “Analysis of cellular automata used as pseudorandom pattern generators,” in Proceedings. International Test Conference 1990, 1990, pp. 762–768.

[2] K. Cattell and J. C. Muzio, “An Explicit Similarity Transform between Cellular Automata and LFSR Matrices,” Finite Fields Their Appl., vol. 4, no. 3, pp. 239–251, 1998.

[3] R. Díaz Len et al., “Wolfram cellular automata and their cryptographic use as pseudorandom bit generators,” Int. J. Pure Appl. Math., vol. 4, 2003.

[4] C. Fraile Rubio, L. Hernandez Encinas, S. White, Á. Rey, and G. Sánchez, “The Use of Linear Hybrid Cellular Automata as Pseudo Random Bit Generators in Cryptography.,” Neural Parallel Sci. Comp., vol. 12, pp. 175–192, 2004.

[5] P. Guan, “Cellular automaton public-key cryptosystem,” Complex Syst., vol. 1, 1987.

[6] H. Gutowitz, “Cryptography with Dynamical Systems,” Cellular Automata and Cooperative Systems. Springer, Dordrecht, 1993. 237-274.

[7] W. Meier and O. Staffelbach, “Analysis of Pseudo Random Sequences Generated by Cellular Automata,” in Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques, 1991, pp. 186–199.

[8] S. Nandi, B. K. Kar, and P. P. Chaudhuri, “Theory and Applications of Cellular Automata in Cryptography,” IEEE Trans. Comput., vol. 43, no. 12, pp. 1346–1357, Dec. 1994.

[9] S. Wolfram, “Cryptography with Cellular Automata,” in Advances in Cryptology, 1986, pp. 429–432.

[10] I. Ingemarsson, D. Tang, and C. Wong, “A Conference Key Distribution System,” IEEE Trans. Inf. Theor., vol. 28, no. 5, pp. 714–720, Sep. 2006.

[11] K. Bogart, “Basic Algebra,” Am. Math. Mon., vol. 92, no. 10, 1985.

[12] A. Joux, “A One Round Protocol for Tripartite Diffie--Hellman,” in Algorithmic Number Theory, 2000, pp. 385–393.

[13] M. Just and S. Vaudenay, “Authenticated multi-party key agreement,” in Advances in Cryptology --- ASIACRYPT ’96, 1996, pp. 36–49.

[14] G. Marañón, L. H. Encinas, A. H. Encinas, Á. M. del Rey, and G. R. Sánchez, “Graphic Cryptography with Pseudorandom Bit Generators and Cellular Automata,” in Knowledge-Based Intelligent Information and Engineering Systems, 2003, pp. 1207–1214.

[15] L. Hernandez Encinas, Á. Rey, and A. Encinas, “Encryption of Images with 2-dimensional Cellular Automata,” Proc. of 6-th Multiconference on Systemics, Cybernetics and Informatics, 2002, pp. 471-476.

[16] T. Toffoli and N. H. Margolus, "Invertible cellular automata: A review," Phys. D Nonlinear Phenom., vol. 45, no. 1, pp. 229–253, 1990.

[17] C. Schwartz, "A NEW GRAPHICAL METHOD FOR ENCRYPTION OF COMPUTER DATA," Cryptologia, vol. 15, no. 1, pp. 43–46, 1991.

[18] I. N. Herstein, "Topics in Algebra," 1975.

[19] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," Chaos, Solitons & Fractals, vol. 40, no. 5, pp. 2191–2199, 2009.

[20] C. Çokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," Phys. Lett. A, vol. 373, no. 15, pp. 1357–1360, 2009.

[21] D. Arroyo, G. Alvarez, S. Li, C. Li, and J. Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption system," Phys. Lett. A, vol. 372, no. 7, pp. 1034–1039, 2008.

[22] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," Phys. Lett. A, vol. 319, no. 3, pp. 334–339, 2003.

[23] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," Image Vis. Comput., vol. 27, no. 8, pp. 1035–1039, 2009.

[24] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," Image Vis. Comput., vol. 27, no. 9, pp. 1371–1381, 2009.

[25] R. Alonso-Sanz, "Reversible cellular automata with memory: two-dimensional patterns from a single site seed," Phys. D Nonlinear Phenom., vol. 175, no. 1, pp. 1–30, 2003.

[26] R. Alonso-Sanz and M. Martín, "Elementary Cellular Automata with Memory," Complex Syst., vol. 14, no. 2, p. 99–126, 2003.

[27] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," Phys. Lett. A, vol. 346, no. 1, pp. 153–157, 2005.

[28] C. Li and G. Chen, "On the security of a class of image encryption schemes," in 2008 IEEE International Symposium on Circuits and Systems, 2008, pp. 3290–3293.

[29] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[30] Yaobinmao, Guanrongchen, and Shiguolian, "A NOVEL FAST IMAGE ENCRYPTION SCHEME BASED ON 3D CHAOTIC BAKER MAPS," Int. J. Bifurc. Chaos, vol. 14, 2011.

[31] J. Shen, X. Jin, and C. Zhou, "A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation," in Advances in Multimedia Information Processing - PCM 2005, 2005, pp. 270–280.

[32] X. He, Q. Zhu, and P. Gu, "A New Chaos-Based Encryption Method for Color Image," in Rough Sets and Knowledge Technology, 2006, pp. 671–678.

[33] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," Math. Comput. Model., vol. 52, no. 11, pp. 2028–2035, 2010.

[34] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Commun. Nonlinear Sci. Numer. Simul., vol. 15, no. 12, pp. 3998–4006, 2010.

[35] I. Amr Ismail, A. Mohammed, and H. Diab, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic logestic Maps[J]," Int. J. Netw. Secur., vol. 11, 2010.

[36] F. Maleki, A. Mohades, S. M. Hashemi, and M. E. Shiri, "An Image Encryption System by Cellular Automata with Memory." 2008 Third International Conference on Availability, Reliability and Security, Barcelona, pp. 1266–1271, 2008.

[37] R.-J. Chen and J.-L. Lai, "Image security system using recursive cellular automata substitution," Pattern Recognit., vol. 40, no. 5, pp. 1621–1631, 2007.

[38] D. R. Stinson, "Cryptography: Theory and Practice, Third Edition," 2001.

[39] C. Z. S. Y. Q. Zhang Xiaoyan; Wang, "Image Encryption Scheme Based on Balanced Two-Dimensional Cellular Automata," Math. Probl. Eng., pp. 229–253, 2013.

[40] Á. Rey and G. Sánchez, "An image encryption algorithm based on 3D cellular automata and chaotic maps," Int. J. Mod. Phys. C, vol. 26, 2015.

[41] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," Commun. Nonlinear Sci. Numer. Simul., vol. 18, no. 11, pp. 3075–3085, 2013.

[42] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," Commun. Nonlinear Sci. Numer. Simul., vol. 18, no. 1, pp. 136–147, 2013.

[43] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," Signal Process. Image Commun., vol. 52, pp. 6–19, 2017.

[44] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," Signal Processing, vol. 148, pp. 124–144, 2018.

[45] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," Opt. Lasers Eng., vol. 90, pp. 146–154, 2017.

[46] R. Jamali and A. Farzan, "A new image cryptography algorithm using Arnold transformation algorithms and differential evolution," J. Electron. Cyber Def. (in Persian), vol. 6, no. 1, 2018.

[47] J. Nam, S. Kim, and D. Won, "Security Weakness in Ren et al.'s Group Key Agreement Scheme Built on Secure Two-Party Protocols," in Information Security Applications, 2006, pp. 1–9.

[48] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," Phys. Lett. A, vol. 309, no. 1, pp. 75–82, 2003.

Journal of "Innovations of Applied Information and Communication Technologies"

Vol. 1, No. 1, 2019 (Serial No. 1)

Encryption of Images using Chaos Theory and Cellular Automata

H. Tabatabaei*, S. K. Shekofteh, H. Salami, M. V. Zangeneh Moghadam

Islamic Azad University, Quchan Branch

Abstract

The differences between textual and multimedia data, images for instance, the big size of images for one example and the correlation of adjacent pixels for another, have led to insufficient efficiency of traditional methods of cryptography and encrypting those data. This paper introduces a new method for image cryptography, using chaos mappings and 1D memory cellular automata. The method benefits from Piecewise linear chaos mapping in permutation phase and Logistic chaos mapping and cellular automata in broadcast phase. The outstanding characteristic of the introduced proposed algorithm is its capability of data verification in block level that holds a great weight in military and medical functions where image data or part of it is believed to be of great sensitivity. In this paper, the educational board of Cortex-M3 LPC1768 is served for hardware implementation of the proposed method. The results of different studies including key sensitivity assessment and statistical assessments depict the high level of the sensitivity of the proposed method. Furthermore, assessment of various attacks revealed the right level of resistance of the proposed method.

Keywords: Image Encryption, Chaos Theory, Chaos Mapping, Reversible Cellular Automaton

* Corresponding author E-mail: h_tabatabaee@mshdiau.ac.ir