مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال پنجم، شماره ۴، زمستان ۱۳۹۳؛ ص ۲۷۳-۲۶۳

یک روش ترکیبی جدید برای رمزنگاری تصویر با اتوماتای سلولی ترکیبی و برگشت‌پذیر

زینب مهرنهاد[۱]، علی‌محمد لطیف[۲*]

۱-دانشجوی کارشناسی ارشد، ۲- استادیار، دانشکده مهندسی برق و کامپیوتر دانشگاه یزد

(دریافت: ۹۳/۱۰/۲۱، پذیرش: ۹۴/۰۲/۰۸)

چکیده

یکی از راه‌های حفاظت و امنیت اطلاعات در پدافند غیرعامل، رمزنگاری می‌باشد. در این مقاله یک روش جدید برای رمزنگاری تصویر با استفاده از اتوماتای سلولی ترکیبی و برگشت‌پذیر ارائه شده است. با توجه به این‌که اطلاعات اصلی تصویر در ۴ بیت پرارزش قرار دارد، ابتدا اتوماتای سلولی ترکیبی بر روی ۴ بیت بالای تصویر اعمال می‌شود و آن‌ها را رمز می‌کند. سپس در مرحله بعد، اتوماتای سلولی برگشت‌پذیر بر روی کل پیکسل‌های تصویر اعمال شده و در پایان بیت‌های تصویر با استفاده از اتوماتای سلولی درهم‌ریزی می‌شوند. به منظور بررسی کارآمدی الگوریتم پیشنهادی با استفاده از آزمون‌های استاندارد، الگوریتم پیشنهادی با چند الگوریتم دیگر مقایسه شده است. نتایج تجربی نشان می‌دهد روش پیشنهادی از لحاظ معیارهای کمی نتایج مطلوبی دارد.

کلید واژه‌ها: رمزنگاری تصویر، اتوماتای سلولی ترکیبی، اتوماتای سلولی برگشت‌پذیر، امنیت.

A New Image Encryption Method with Hybrid and Reversible Cellular Automata

Z. Mehrnahad, A. Latif[*]

Department of Electrical and Computer Engineering, Yazd University

(Received: 11/01/2015; Accepted: 28/04/2015)

Abstract

Cryptography is one of the most important ways of information security in passive defence. In this paper, a new image encryption method using reversible and hybrid cellular automata is presented. Since four most significant bits of each pixel have main information of an image, a hybrid cellular automata encrypts this bitst. Then, a reversible cellular automata are applied to whole of the pixels and finally, cellular automata scrambles the image bits. Using a series of standard tests, the suggested method was compared with some other methods to assess the efficiency of the algorithm. The experimental results show that the suggested algorithm has satisfactory performance in terms of quantitative assessment from some other schemes.

Keywords: Image Encryption, Hybrid Cellular Automata, Reversible Cellular Automata, Security Ortho-Photo.

[*]Corresponding Author E-mail: alatif@yazd.ac.ir

۱. مقدمه

از زمانی که انسان‌ها قادر به ارتباط با یکدیگر شدند، امکان ارتباط بصری به صورت پنهان و ایمن خواسته بشر بوده است. گسترش روزافزون اینترنت و رشد سریع فناوری، انسان‌ها را به سوی مبادله اطلاعات سوق داده است. امنیت رسانه‌های دیجیتال یک نیاز مهم است و این نیاز روزبه‌روز افزایش می‌یابد. در این راستا رمزنگاری یکی از راه‌های پیشنهادی امنیت رسانه‌های دیجیتالی است [۱].

در رمزنگاری اطلاعات به‌گونه‌ای رمز می‌شوند که برای شخص ثالث قابل فهم نباشد. در این روش ابتدا فرستنده با کلید و عملیات ریاضی برگشت‌پذیر به رمز کردن تصویر می‌پردازد. گیرنده با داشتن کلید رمزنگاری، تصویر را رمزگشایی می‌کند. بدیهی است کلید رمزنگاری بین فرستنده و گیرنده مشترک بوده و به عنوان عنصر اصلی در رمزنگاری به‌کار می‌رود.

تصویر به عنوان یکی از رسانه‌های دیجیتال مورد توجه بشر بوده است. تصاویر دیجیتال ممکن است شامل اطلاعات تجاری، سیاسی و نظامی باشند؛ بنابراین حفظ محرمانگی آن‌ها مهم است. در تصاویر دیجیتال برای هر پیکسل چند بیت در نظر گرفته می‌شود که این باعث افزایش حجم فایل تصویری می‌گردد. همچنین پیکسل‌های مجاور تصویر دارای همبستگی در چند جهت می‌باشند. این ویژگی‌های تصویر باعث شده است تا الگوریتم‌های رمزنگاری متن روی تصویر قابل استفاده نباشد. به همین دلیل الگوریتم‌های جدیدی برای رمزنگاری تصویر ارائه شده است [۱].

رمزنگاری تصویر با دو روش جابه‌جایی[1] و جایگزینی[2] پیکسل‌ها صورت می‌گیرد. در روش جابه‌جایی چیدمان پیکسل‌ها در تصویر تغییر می‌کند. در این روش طبق یک رابطه برگشت‌پذیر موقعیت پیکسل‌ها تغییر می‌کند و تصویر رمز شده به‌دست می‌آید و در مقصد چیدمان اولیه پیکسل‌ها بازیابی می‌شود. روش‌هایی مانند تبدیل آرنولد، تبدیل منحنی هیلبرت، دنباله بی‌نظم از این قبیل هستند [۵-۲]. در روش جایگزینی، سطح روشنایی پیکسل‌ها توسط عملیات منطقی و محاسباتی با یک رابطه ریاضی تغییر می‌کند و سپس در مقصد معکوس عملیات رمزنگاری انجام می‌شود و مقادیر پیکسل‌ها بازیابی می‌شوند [۶ و ۷].

روش‌های رمزنگاری با توجه به ماهیت تصویر، زمان و توان محاسباتی پردازنده، نحوه پیاده‌سازی سخت‌افزاری و نرم‌افزاری، باید کارایی و ایمنی مناسبی داشته باشند. تاکنون ابزارها و روش‌های ویژه‌ای مطرح شده‌اند تا سامانه‌های رمزنگاری را امن‌تر کنند [۸]. یکی از ابزارها اتوماتای سلولی است. در این مقاله روش جدیدی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر[3] و اتوماتای سلولی ترکیبی[4] ارائه می‌شود.

اتوماتای سلولی با ویژگی‌های ذاتی خود مانند امکان پردازش موازی، یک ریختی[5]، غیر قابل پیش بینی بودن رفتار آن و پیاده‌سازی ساده گزینه مناسبی برای رمزنگاری تصویر است. اتوماتای سلولی در دهه ۴۰ میلادی توسط ون نیومن ارائه شد [۹]. بعد از آن تحقیق‌های گسترده‌ای بر روی اتوماتای سلولی صورت گرفت. در سال‌های اخیر از اتوماتای سلولی در رمزنگاری [۱۰ و ۱۱]، پردازش تصویر [۱۲ و ۱۳] و امنیت اطلاعات [۱۴] استفاده فراوانی شده است.

ریوسنگ [۱۵] روشی بر مبنای جابه‌جایی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی معرفی کرده است. او ابتدا با استفاده از اتوماتای سلولی دنباله‌ای از اعداد تصادفی تولید کرد و سپس درهم-ریزی تصویر را با استفاده از این اعداد انجام داد. این روش توسط فاسل غدیر و همکارانش[۱۶] با اندکی تغییر در الگوریتم مورد استفاده قرار گرفت. با توجه به این‌که روش‌های درهم‌ریزی تصویر، هیستوگرام تصویر را تغییر نمی‌دهد، این روش‌ها به‌تنهایی دارای امنیت بالایی نیستند.

جین [۱۷] روشی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی به روش جایگزینی پیکسل‌ها معرفی کرد. در این روش از اتوماتای سلولی با استفاده از خاصیت تناوبی استفاده شد. تناوبی بودن به این معنی که با استفاده از چندین قانون متوالی به صورت چرخشی می‌توان به تصویر اصلی دست یافت. در نتیجه رمزگشایی با اجرای یک تناوب کامل الگوریتم انجام می‌شود.

عبدو و همکارانش [۱۸] روشی بر مبنای جایگزینی پیکسل‌ها ارائه کردند. در این روش ابتدا حلقه‌هایی از قوانین برگشت‌پذیر تشکیل می‌شود و سپس با استفاده از عدد تصادفی یکی از حلقه‌ها انتخاب می‌گردد و قوانین حلقه بر روی تصویر اعمال می‌شود تا تصویر رمز شده به‌دست آید. بدیهی است در هر دو روش مذکور با توجه به تناوبی بودن الگوریتم احتمال حمله و رمزگشایی تصویر وجود دارد.

روشی بر مبنای جابه‌جایی و جایگزینی پیکسل‌ها توسط وانگ و همکارش[۱۹] ارائه شد. در مرحله جایگزینی از اتوماتای سلولی برگشت‌پذیر استفاده شد. در این روش جابه‌جایی تنها بر روی ۴ بیت کم‌ارزش و جایگزینی بر روی ۴ بیت پرارزش صورت گرفت. بنابراین احتمال تصادفی بودن در این روش نسبت به روش‌هایی که فقط عمل جایگزینی بر روی کل بیت‌ها صورت می‌گیرد، کم‌تر است.

روش بلاک‌بندی برای رمزنگاری تصویر با استفاده از اتوماتای سلولی برگشت‌پذیر نیز ارائه شده است [۲۰]. در این روش با تقسیم پیکسل‌های تصویر به بلاک‌های متعدد در ۴۰ مرحله به رمز تصویر پرداخته است. این روش دارای مراحل طولانی است.

در روش پیشنهادی از دو روش جابه‌جایی و جایگزینی استفاده شده است. اطلاعات اصلی در تصویر در ۴ بیت پرارزش وجود دارد. برای صرفه‌جویی در زمان در مرحله اول رمزنگاری با اتوماتای سلولی

[1] Scrambling
[2] Substitution
[3] Reversible Cellular Automata
[4] Hybrid Cellular Automata
[5] Isomorphic

ترکیبی، جایگزینی بر روی ۴ بیت پرارزش انجام شده است. در مرحله دوم رمزنگاری ۴ بیت رمز شده در کنار ۴ بیت کم‌ارزش پیکسل مربوطه که هنوز عملی بر روی آن‌ها صورت نگرفته، قرار می‌گیرند و تصویر جدیدی به‌دست می‌آید؛ سپس با استفاده از اتوماتای سلولی برگشت‌پذیر عمل جایگزینی و جابه‌جایی به ترتیب بر روی پیکسل‌های تصویر جدید صورت می‌گیرد.

۲. روش تحقیق

در این بخش ابتدا ابزارها و عناصری که در الگوریتم پیشنهادی برای رمزنگاری استفاده شده است، معرفی می‌شوند. سپس الگوریتم پیشنهادی توضیح داده می‌شود.

۲-۱. اتوماتای سلولی برگشت‌پذیر

اتوماتای سلولی یک مدل ریاضی برای سامانه‌های دینامیکی گسسته است که از تعدادی سلول تشکیل شده است. این سلول‌ها در کنار یکدیگر یک شبکه را تشکیل می‌دهند و در طول زمان طبق قوانین داده شده در اتوماتا تغییر می‌کنند.

اتوماتای سلولی با ۴ مؤلفه به شکل $CA=\{C,S,V,F\}$ تعریف می‌شود. مؤلفه C نشان دهنده سلول اتوماتا و S نشان دهنده حالت سلول می‌باشد که برای ساده‌ترین حالت می‌توان $S=\{0,1\}$ را تعریف کرد. مؤلفه V نشان دهنده نوع و تعداد همسایگی یک سلول می‌باشد که در تعیین حالت بعدی سلول استفاده می‌شود. مؤلفه F قوانین انتقال اتوماتای سلولی می‌باشد. در هر زمان سلول وضعیت خود را بر اساس شماره قانون انتقال، تغییر می‌دهد. قوانین انتقال چگونگی تغییر حالت سلول را مشخص می کنند. این تغییر بستگی به حالت فعلی سلول و حالت سلول‌های همسایگانش را دارد [۹ و ۲۱].

اتوماتای سلولی در ابعاد مختلفی دسته‌بندی می‌شود. اتوماتای سلولی یک بعدی، دوبعدی و سه‌بعدی نمونه‌هایی از این دسته‌بندی هستند. در این مقاله از اتوماتای سلولی یک بعدی استفاده شده است. برای هر سلول همسایگی راست و چپ آن در نظر گرفته شده است.

در اتوماتای سلولی شرایط مرزی به صورت رابطه (۱) تعریف می‌شود. در این مقاله شرایط مرزی دوره‌ای[1] در نظر گرفته شده است.

$$S_{i,j}^{t}=S_{u,v}^{t} \Leftrightarrow i\equiv u(\mathrm{mod}\, r) \text{ and } \ j\equiv v(\mathrm{mod}\, c) \qquad (۱)$$

که در آن، i ، j ، u و v مختصات سلول در فضای دوبعدی $r\times c$ و S حالت سلول در زمان t است.

همسایگی‌های معمول اتوماتای سلولی در شکل (۱) نشان داده شده است که در الگوریتم پیشنهادی همسایگی von newman در نظر گرفته شده است. تابع انتقال F بر روی سلول C در زمان t به صورت رابطه (۲) تعریف می‌شود:

$$F:C^{t}\rightarrow C^{t+1} \qquad (۲)$$

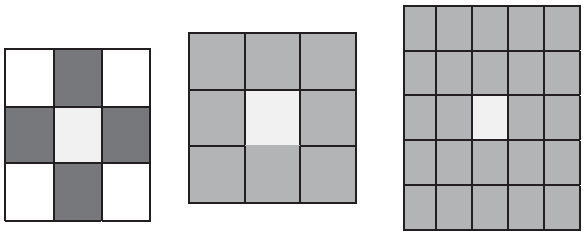
که طبق همسایگی استفاده شده حالت سلول مورد نظر و سلول راست و چپ آن در زمان t در نظر گرفته می‌شود:

$$F:S_{i,j}^{t+1}=f(S_{i,j-1}^{t},S_{i,j}^{t},S_{i,j+1}^{t}) \qquad (۳)$$

در الگوریتم پیشنهادی علاوه بر حالت سلول مورد نظر در زمان t، زمان t-1 نیز در نظر گرفته شده است. بنابراین تابع انتقال به صورت زیر تغییر داده می‌شود:

$$F:S_{i,j}^{t+1}=f(S_{i,j-1}^{t},S_{i,j}^{t},S_{i,j+1}^{t},S_{i,j}^{t-1}) \qquad (۴)$$

رابطه (۴) اتوماتای سلولی را برگشت‌پذیر می‌کند [۲۱]. عملکرد تابع انتقال در اتوماتای سلولی برگشت‌پذیر در جدول (۱) نشان داده شده است. در ستون اول حالت یک سلول با دو سلول همسایه راست و چپ در زمان t نشان داده شده است. در ستون دوم حالت سلول در زمان t-1 نشان داده شده است. در این زمان سلول دو حالت صفر یا یک دارد. برای تعیین حالت بعدی از شماره قانون اتوماتای سلولی که به صورت باینری نوشته شده است، استفاده می‌شود. شماره قانون‌ها برای دو حالت $S_{i,j}^{t-1}=0$ و $S_{i,j}^{t-1}=1$ مخالف[2] یکدیگر هستند. در ستون دوم و سوم جدول دو قانون ۲۲ و ۲۳۳ به صورت باینری نوشته شده است. در مرحله رمزگشایی تصویر، حالت سلول‌ها در زمان t-1 به بعد از زمان t انتقال داده می‌شود و مانند قبل اتوماتا اجرا می‌شود. در این حالت دیده می‌شود که مراحل رمزنگاری مرحله به مرحله برگشت داده می‌شوند و حالت اولیه سلول به دست می‌آید. این موضوع در شکل (۲) نشان داده شده است.



الف: مدل پیشرفته Moore — ب: مدل Moore — ج: مدل Von neumann

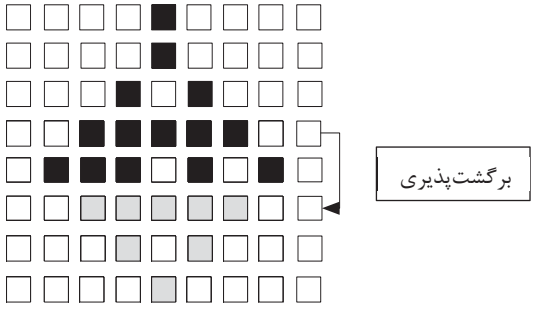
شکل ۱. انواع همسایگی اتوماتای سلولی

جدول ۱. عملکرد قوانین اتوماتای سلولی برگشت‌پذیر

$S_{i,j-1}^{t}S_{i,j}^{t}S_{i,j+1}^{t}$	$S_{i,j}^{t+1}$	
	$S_{i,j}^{t-1}=0$	$S_{i,j}^{t-1}=1$
000	0	1
001	1	0
010	1	0
011	0	1
100	1	0
101	0	1
110	0	1
111	0	1

[1] Periodic Boundry

[2] Opposite



شکل ۲. عملکرد اتوماتای سلولی برگشت‌پذیر

۲-۲. اتوماتای سلولی ترکیبی

اتوماتای سلولی ترکیبی عملکردی مشابه اتوماتای سلولی معمولی دارد. تنها تفاوت آن داشتن قوانین مختلف برای هر سلول است. در این نوع اتوماتا می‌توان شماره قانون متفاوتی را برای هر سلول در نظر گرفت و با توجه به آن حالت بعدی هر سلول را تعیین کرد. به طور مثال برای یک سلول قانون ۳۰ تعیین کننده حالت‌های بعدی و برای سلول دیگری قانون ۹۰ تعیین‌کننده حالت بعدی است. بنابراین برای یک پیکسل از تصویر که ۸ بیت دارد، از ۸ قانون اتوماتا برای تعیین حالت بعدی هر بیت استفاده می‌شود. لازم به ذکر است، اگر قوانین برای تمام سلول‌های اتوماتا یکسان باشد، اتوماتا یکنواخت و در غیر این صورت غیریکنواخت نامیده می‌شود [۲۲]. اتوماتای سلولی ترکیبی را به نام اتوماتای سلولی غیریکنواخت نیز می‌شناسند.

۲-۳. الگوریتم پیشنهادی

الگوریتم پیشنهادی شامل دو مرحله مجزای رمزنگاری می‌باشد. مراحل رمزنگاری به صورت جداگانه در ادامه توضیح داده شده است.

مرحله اول رمزنگاری: ابتدا ۴ بیت پرارزش پیکسل‌های تصویر به عنوان ورودی به اتوماتای سلولی ترکیبی داده شده است. در اتوماتای سلولی ترکیبی برای هر بیت با تابع معرفی‌شده در رابطه (۵)، شماره قانونی تولید و هر بیت با قانون متناظرش رمز می‌شود.

$$f(a_{n+1}) = -2(a_n)^2 + 1 \qquad a_n \in (-1,+1) \qquad (۵)$$

در این تابع، a_0 به عنوان کلید در نظر گرفته می‌شود. سپس به تعداد بیت‌های تصویر، عدد تولید می‌شود که شماره قانون مربوطه برای هر بیت از پیکسل‌های تصویر خوانده شده است. قدم‌های مرحله اول رمزنگاری در الگوریتم پیشنهادی در شکل (۳) به صورت خلاصه نشان داده شده است.

مرحله دوم رمزنگاری: در مرحله دوم ۴ بیت کم‌ارزش‌تر تصویر در کنار ۴ بیت پرارزش که در مرحله اول رمز شدند، قرار می‌گیرند و ۸ بیت را تشکیل می‌دهند. این مقادیر در ماتریس جدیدی ذخیره می‌شوند و تصویر تولید می‌شود. این مرحله شامل قدم‌های زیر است:

۱. ابتدا دو سطر از تصویر جدا می‌شود (قدم ۱ در شکل (۴)).

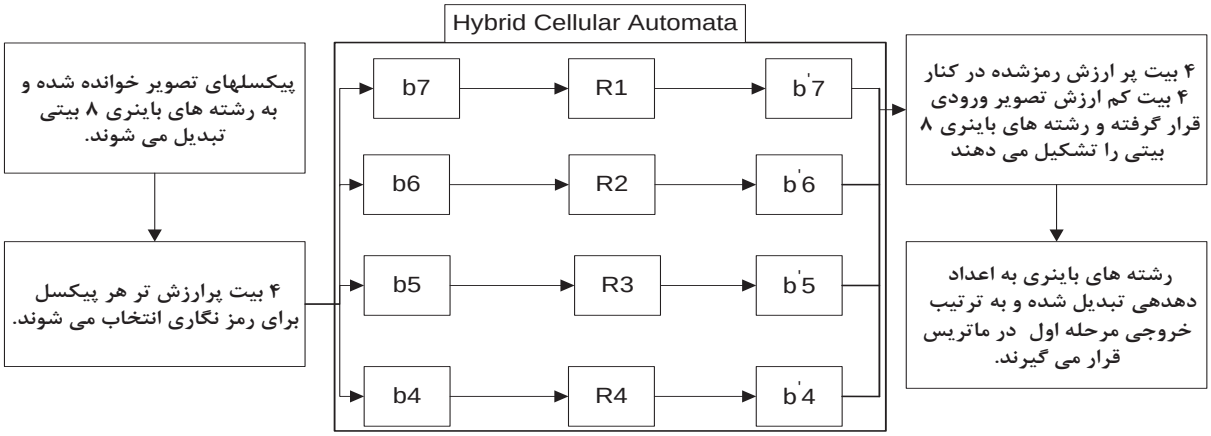
۲. از هر سطر دو پیکسل جدا می‌شود و به صورت رشته باینری نوشته می‌شوند (قدم ۲ در شکل (۴)).

۳. دو رشته باینری ستون اول از دو سطر به عنوان ورودی برای اتوماتای سلولی در زمان $t\text{-}1$ و t در نظر گرفته می‌شوند و با شماره قانون‌هایی که به عنوان کلید هستند، رمز می‌شوند. دو رشته باینری ستون دوم از دو سطر نیز به همین ترتیب رمز می‌شوند. خروجی در دو زمان $t\text{-}1$ و t به‌دست می‌آید (قدم ۳ در شکل (۴)).

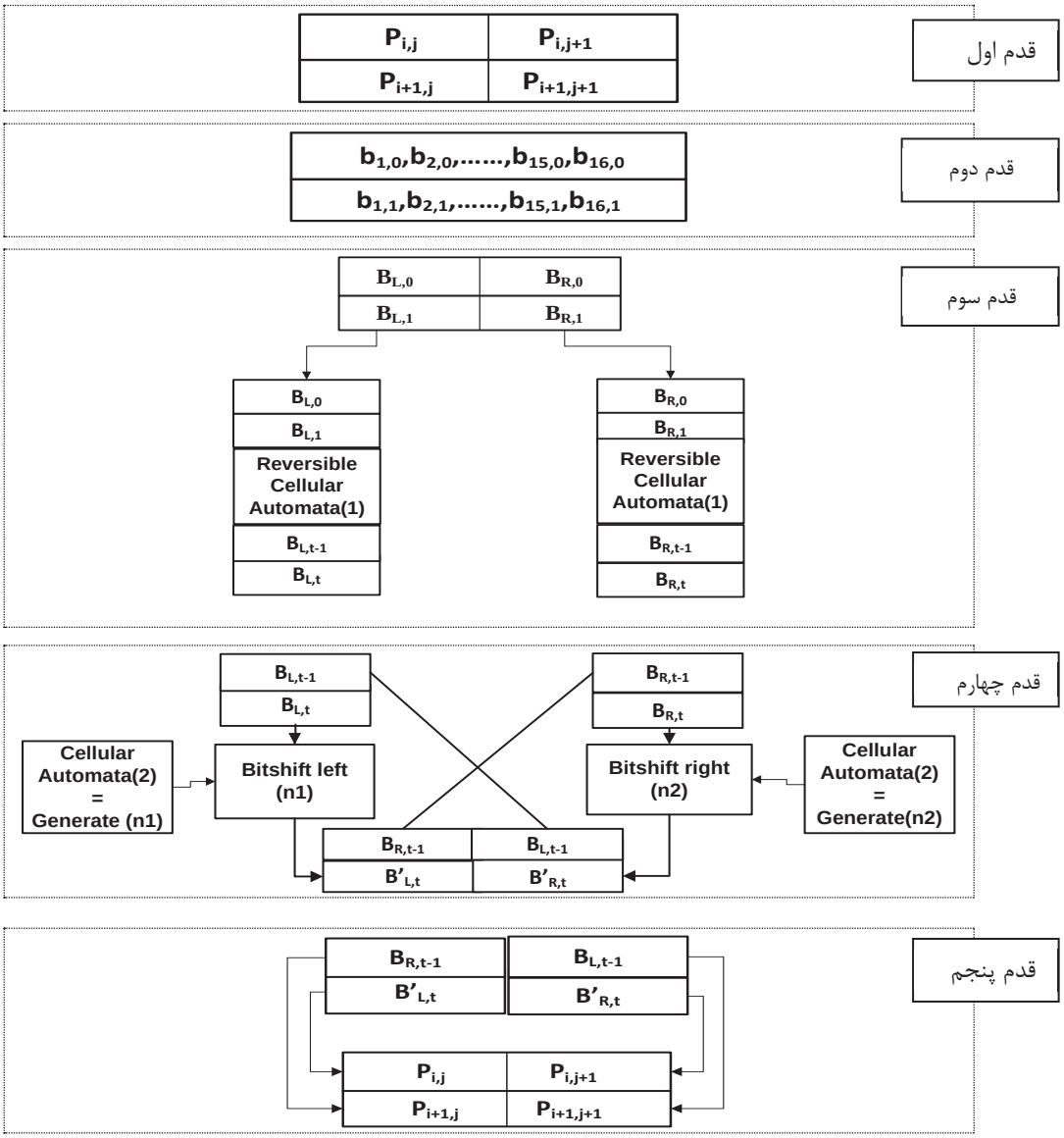
۴. مکان رشته‌های باینری رمز شده در $t\text{-}1$ با یکدیگر جابه‌جا می‌شوند. رشته‌های باینری در t با عدد تصادفی ایجاد شده توسط اتوماتای سلولی دیگری، شیفت داده می‌شوند. به این ترتیب جابه‌جایی بیت‌ها صورت می‌گیرد (قدم ۴ در شکل (۴)).

۵. این مقادیر همان‌طور که در شکل (۴) نشان داده شده است، در ماتریس رمز ذخیره می‌شوند (قدم ۵ در شکل (۴)).

در مرحله رمزگشایی مراحل فوق به صورت معکوس اعمال می‌شود. در تصویر رمزشده نحوه قرارگیری پیکسل‌ها مانند شکل (۲) است که برگشت‌پذیری اتوماتا را ممکن می‌سازد. قدم‌های ۱ تا ۴ از مرحله دوم رمزنگاری در شکل (۴) نشان داده شده است.



شکل ۳. مرحله اول رمزنگاری در الگوریتم پیشنهادی



شکل ۴. گام‌های مرحله دوم رمزنگاری

۳. نتایج حاصل از اجرای الگوریتم

نتایج حاصل از اجرای الگوریتم بر روی تصویرهای cameraman و boats با اندازه ۲۵۶×۲۵۶ و با کلیدهای متفاوت در ادامه نشان داده شده است. شکل (۵) تصویر اصلی، تصویر رمزشده و تصویر رمزگشایی شده با کلیدهای مختلف برای تابع اتوماتای سلولی و تولید قوانین اتوماتای سلولی ترکیبی در مرحله اول و قوانین ۳۰ و ۹۸ و ۱۳۵ به عنوان کلید اتوماتای سلولی برگشت‌پذیر در مرحله دوم را به ترتیب نشان می‌دهد. برای نشان دادن حساسیت الگوریتم به کلید در شکل (۶) سعی شده است که تصویر رمز شده با قانون ۳۰ را با کلید دیگری رمزگشایی کرد. همان‌گونه که مشاهده می‌شود رمزگشایی به صورت صحیح انجام نشده و تصویر نامفهوم است.

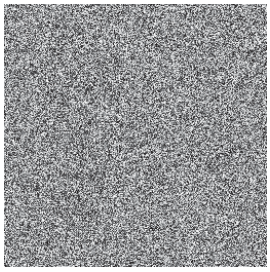
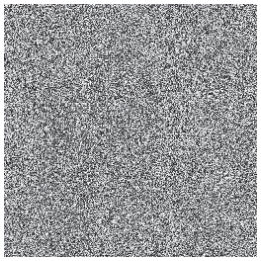
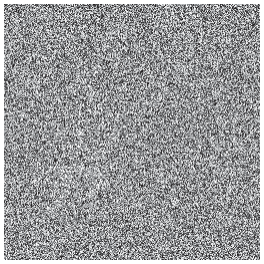
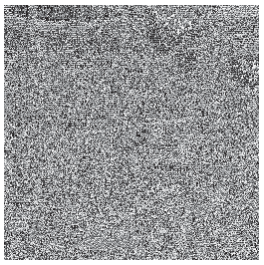
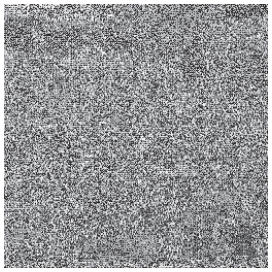
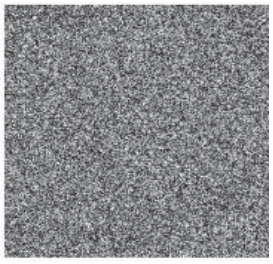
۴. تحلیل و ارزیابی الگوریتم

در مراجع گذشته برای ارزیابی روش پیشنهادی چندین آزمون پیشنهاد شده است [۱۹-۱۷]. در این مقاله سعی شده است تا آزمون‌های معرفی شده بر روی روش پیشنهادی به همراه سه روش معرفی شده در [۱۹-۱۷] بررسی شود.

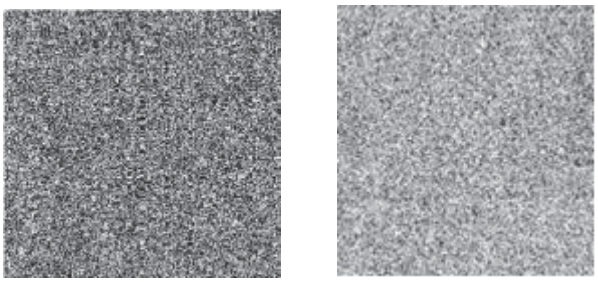
۴-۱. تحلیل آماری

با استفاده از تحلیل‌های آماری[1] می‌توان بسیاری از مسائل رمزنگاری را آشکار کرد. الگوریتم رمز باید به گونه‌ای باشد که دشواری تحلیل‌های آماری را بیشتر کند. تحلیل هیستوگرام و ضرایب همبستگی از مواردی است که برای ارزیابی تحلیل‌های آماری استفاده می‌شود [۱۹].

[1] Statistical Analysis

قانون	X_0	تصویر اصلی	تصویر رمزشده	تصویر رمزگشایی‌شده
R=۱۳۵	۰/۴۵			
R=۹۸	۰/۵۰			
R=۳۰	۰/۵۵			
R=۱۳۵	۰/۴۵			
R=۹۸	۰/۵۰			
R=۳۰	۰/۵۵			

شکل ۵. نتایج رمزنگاری تصاویر با الگوریتم پیشنهادی



(الف) (ب)

شکل ۶. نتیجه رمزگشایی با کلید نادرست، الف) تصویر رمزشده با x_0= ۰/۵۵ و قانون ۳۰، ب) تصویر رمزگشایی با x_0= ۰/۴۵ و قانون ۳۵

تحلیل هیستوگرام: یک الگوریتم رمزنگاری در صورتی مناسب است که تصویر را به گونه‌ای رمز کند که هیچ‌گونه اطلاعاتی از تصویر اصلی در آن دیده نشود. به عبارتی ویژگی‌های تصویر به صورت بصری نباشد. با توجه به این‌که نتیجه آزمون بصری برای بینندگان مختلف متفاوت است، تحلیل هیستوگرام پیشنهاد شده است. تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از ترسیم تعداد مشاهدات هر شدت روشنایی بیان می‌کند.

هیستوگرام تصاویر اصلی و رمز شده دو تصویر cameraman و boats در شکل‌های (۷ و ۸) به ترتیب نشان داده شده است. همان‌طور که در شکل دیده می‌شود، هیستوگرام تصاویر رمزشده یکنواخت می‌باشد که این نشان دهنده کارایی الگوریتم رمزنگاری پیشنهادی می‌باشد.

تحلیل ضرایب همبستگی: ضریب همبستگی یکی از معیارهای ارزیابی در تحلیل آماری است. هرچه همبستگی پیکسل‌های همسایه در تصویر رمز شده کمتر باشد، عملکرد الگوریتم مطلوب‌تر است [۱ و ۱۹]. برای مطالعه همبستگی پیکسل‌ها در راستای افقی، عمودی و قطری از رابطه (۶) استفاده می‌شود.

$$r_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۶)$$

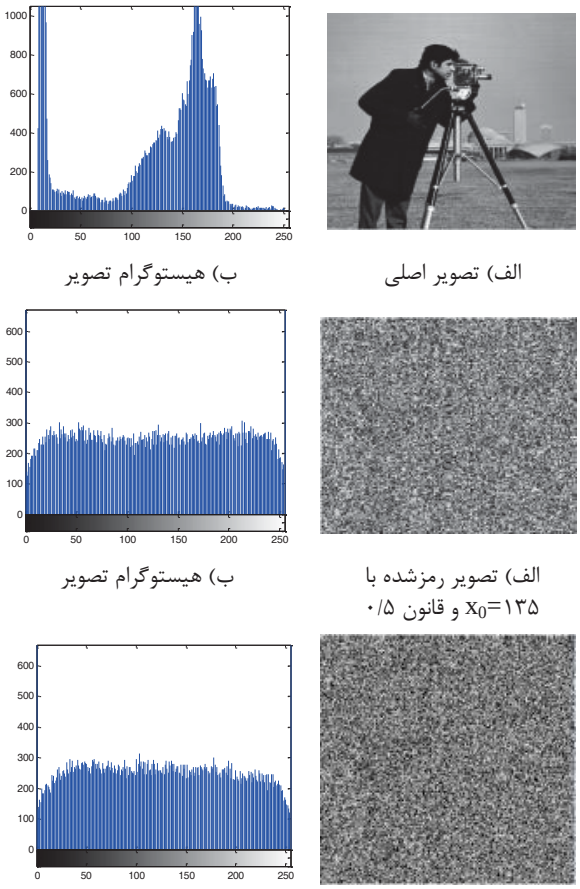
$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))(y_j - E(y)) \qquad (۷)$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N} x_i \qquad (۸)$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2 \qquad (۹)$$

در این روابط، x و y روشنایی دو پیکسل همسایه در تصویر و N تعداد پیکسل‌های تصویر می‌باشد. مقادیر تابع همبستگی در سه راستای عمودی، افقی و قطری برای تصویر cameraman و تصاویر رمز شده آن با قانون ۹۸ و ۱۳۵ با سه الگوریتم معرفی شده در [۱۹-۱۷] و الگوریتم پیشنهادی در جدول‌های (۲ و ۳) به ترتیب آورده شده است.

با توجه به اعداد جدول همان‌طور که انتظار می‌رود، همبستگی پیکسل‌های تصویر اصلی زیاد است. در تصاویر رمز شده این میزان کمتر شده و پیکسل‌ها وابستگی کمتری نسبت به یکدیگر دارند. در روش پیشنهادی مقدار همبستگی نسبت به دو روش دیگر کمتر بوده است.



الف) تصویر اصلی ب) هیستوگرام تصویر

الف) تصویر رمزشده با x_0=۱۳۵ و قانون ۰/۵ ب) هیستوگرام تصویر

الف) تصویر رمزشده با x_0=۹۸ و قانون ۰/۵ ب) هیستوگرام تصویر

شکل ۷. نتایج هیستوگرام تصاویر رمزشده cameraman

جدول ۲. معیار همبستگی برای تصویر cameraman با کلید x_0= ۰/۴۵ و قانون ۱۳۵

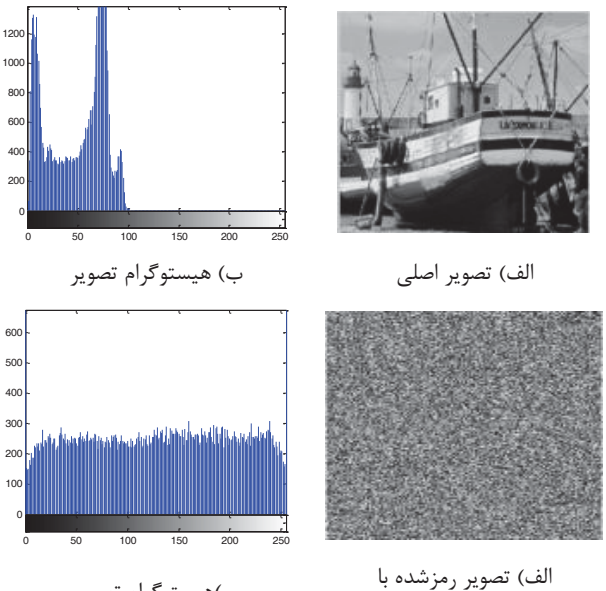
تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز مرجع [۱۷]	۰/۰۱۱۱	۰/۰۱۶۵	۰/۰۵۳۶
تصویر رمز مرجع [۱۸]	-۰/۰۰۳۸	-۰/۰۰۶۵	۰/۰۰۳۴
تصویر رمز مرجع [۱۹]	-۰/۰۲۱۹	-۰/۰۱۲۹	۰/۰۰۲۷
تصویر رمز مرجع [۲۰]	۰/۰۵۵۷	۰/۰۱۰۴	۰/۰۰۷۲
تصویر رمز روش پیشنهادی	-۰/۰۰۱۱	-۰/۰۰۰۰۴۳	۰/۰۰۲۶

۴-۲. تحلیل فضای کلید

به منظور جلوگیری از حمله جست‌وجوی جامع[1]، فضای کلید

[1] Brute Force Attack

الگوریتم رمزنگاری باید به حد کافی بزرگ باشد. فضای کلید الگوریتم شامل تعداد کل کلیدهای قابل‌استفاده در الگوریتم رمزنگاری است. هرچه اندازه فضای کلید رمزنگاری بزرگ‌تر باشد، زمان آزمایش کلیدها بیشتر می‌شود و در نتیجه نسبت به حمله جست و جوی جامع مقاوم‌تر است.



الف) تصویر اصلی ب) هیستوگرام تصویر

الف) تصویر رمزشده با x_0=۱۳۵ و قانون ۰/۵ ب)هیستوگرام تصویر

الف) تصویر رمزشده با x_0=۹۸ و قانون ۰/۵ ب) هیستوگرام تصویر

شکل ۸. نتایج هیستوگرام تصاویر رمزشده boats

جدول ۳. معیار همبستگی برای تصویر cameraman با کلید x_0= ۰/۴۵ و قانون ۹۸

تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی	۰/۹۴۸۹	۰/۹۵۳۶	۰/۹۲۱۲
تصویر رمز مرجع [۱۷]	-۰/۰۳۶۹	-۰/۰۳۸۳	۰/۰۱۱۴
تصویر رمز مرجع [۱۸]	۰/۰۱۲۲	۰/۰۱۴۹	-۰/۰۱۷۸
تصویر رمز مرجع [۱۹]	-۰/۰۱۱۶	-۰/۰۱۷۶	۰/۰۰۶۸
تصویر رمز مرجع [۲۰]	-۰/۰۰۳۸	۰/۰۳۱۴	-۰/۰۰۰۰۳۶
تصویر رمز روش پیشنهادی	۰/۰۰۱۵	۰/۰۱۴۰	-۰/۰۰۰۰۲۴

سازمان NIST حداقل طول ممکن برای برقراری امنیت محاسباتی در برابر حمله‌های جست و جوی جامع را تا سال ۲۰۱۵ میزان ۸۰ بیت پیش‌بینی کرده است [۱ و ۱۹]. در الگوریتم پیشنهادی از ۳ اتوماتای سلولی که شامل یک اتوماتای سلولی ترکیبی در مرحله اول، یک اتوماتا در مرحله دوم برای جایگزینی پیکسل‌ها و یک اتوماتای دیگر برای تولید عدد تصادفی استفاده می‌شود. کلید اولیه تابع معرفی شده در رابطه (۵) که تولید کننده قانون اتوماتای سلولی ترکیبی است با دقت 10^{-3} است. در اتوماتای سلولی ترکیبی از 2^4 قانون برای هر پیکسل و دو اتوماتای دیگر از 2^8 قانون می‌توان استفاده کرد. فضای کلید برای روش پیشنهادی برابر با $10^3 \times (2^4)^{m\times n} \times 2^8 \times 2^8$ که در آن $m\times n$ اندازه تصویر است، می‌باشد. بنابراین ساختار پیشنهادی نسبت به حمله جست و جوی جامع مصون است.

۴-۳. تحلیل آنتروپی

آنتروپی به عنوان یکی از مشخصه‌های مهم تصادفی بودن الگوریتم به شمار می‌رود. آنتروپی طبق رابطه (۱۰) محاسبه می‌شود. در این رابطه که در آن S تصویر رمز شده و $P(S_i)$ تعداد رخدادهای S_i می‌باشد. در حالت ایده‌آل در یک تصویر رمز شده که هر پیکسل آن ۸ بیتی می‌باشد، این مقدار باید به ۸ نزدیک باشد [۱۹]. در جدول (۴) مقادیر آنتروپی نشان داده شده است.

$$H(S)=\sum_{i=0}^{2^n-1} P(S_i)\log_2\frac{1}{P(S_i)} \qquad (۱۰)$$

جدول ۴. مقادیر آنتروپی برای روش‌های مختلف

روش‌ها	روش [۱۷]	روش [۱۸]	روش [۱۹]	روش [۲۰]	روش پیشنهادی
آنتروپی	۷/۸۸۴۸	۷/۷۱۳۳	۷/۲۳۳۹	۷/۹۲۵۳	۷/۹۵۸۴

۴-۴. تمایز تصویر اصلی و رمزشده

یک خاصیت ایده‌آل برای تصویر رمز، حساس بودن نسبت به تغییرهای جزئی در تصویر اصلی است. در حمله‌های تفاضلی[1]، مهاجم تلاش می‌کند با ایجاد یک تغییر کوچک در تصویر، تغییر حاصل در تصویر رمز را مشاهده کند و به این ترتیب رابطه بین تصویر اصلی و رمز آشکار شود.

سه معیار UACI[2]، MAE[3]، NPCR[4] برای آزمودن اثر تغییر یک پیکسل ورودی بر روی تصویر رمز شده می‌باشد. هر چه این سه معیار بیشتر باشند، الگوریتم رمزنگاری عملکرد مطلوب‌تر دارد [۲۳ و ۲۴]. رابطه (۱۱) مربوط به محاسبه متوسط خطای مطلق می‌باشد [۱]. در این رابطه C(i,j) و P(I,j) به ترتیب مقادیر پیکسل‌های تصویر رمز و تصویر اصلی می‌باشد.

رابطه (۱۲) محاسبه NPCR را نشان می‌دهد که نرخ پیکسل‌های تغییر یافته تصویر رمز به ازای یک بیت تغییر در تصویر اصلی می‌باشد [۱۷ و ۱۸]. نحوه محاسبه UACI در رابطه (۱۴) نشان داده شده است.

[1] Differential Attack
[2] Unified Average Changing Intensity (UACI)
[3] Mean Absolute Error (MAE)
[4] Number of Pixel Change Rate (NPCR)

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i,j) - P(i,j)| \quad (۱۱)$$

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \quad (۱۲)$$

$$D(i,j) = \begin{cases} 0 & if \quad C_1(i,j) = C_2(i,j) \\ 1 & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \quad (۱۳)$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{C(i,j) - \bar{C}(i,j)}{255} \quad (۱۴)$$

در جدول (۵) مقادیر توابع ارزیابی برای الگوریتم‌های معرفی شده در [۱۹-۱۷] با الگوریتم پیشنهادی با قانون ۱۳۵ نشان داده شده است. همان‌طور که در جدول مشاهده می‌شود، این مقادیر برای روش پیشنهادی نسبت به دو روش معرفی‌شده در [۱۷ و ۱۸] بیشترین مقدار را دارد. یعنی به ازای تغییر یک پیکسل در تصویر ورودی بیشترین میزان تغییر در خروجی ایجاد شده است. در مقایسه با روش [۱۹] نیز برای UACI و NPCR بیش‌ترین مقادیر را دارد.

۴-۵. تحلیل حساسیت نسبت به کلید

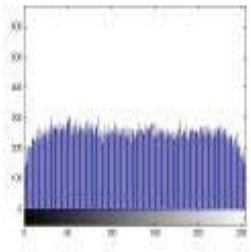
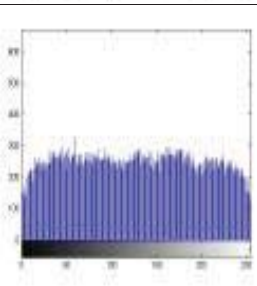
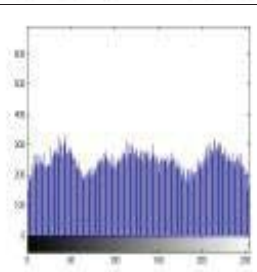
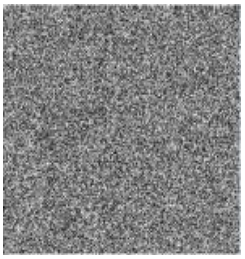
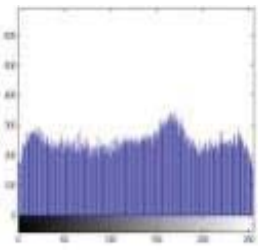
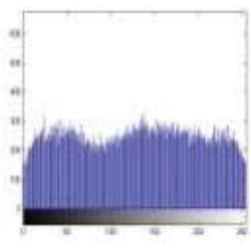
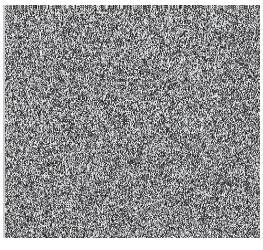
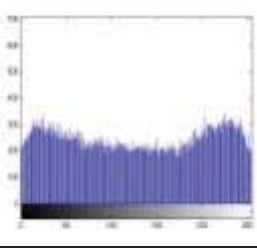
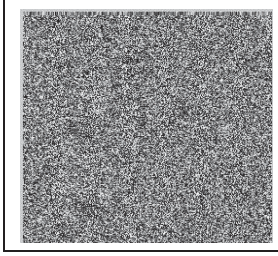
حساسیت نسبت به کلید، یکی از ویژگی‌های ضروری برای یک الگوریتم رمزنگاری مطلوب است. حساسیت نسبت به کلید به این معنی است که با تغییر یک بیت در کلید خصوصی، یک تصویر رمز متفاوت تولید شود. حساسیت بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله جستجوی جامع تضمین می‌کند.

برای ارزیابی ویژگی حساسیت نسبت به کلید، ابتدا تصویر اصلی با کلید محرمانه اصلی رمزنگاری می‌شود، سپس کلید را کمی تغییر داده و تصویر اصلی دوباره رمزنگاری می‌شود. در صورتی‌که مقایسه این دو تصویر رمز به صورت بصری امکان‌پذیر نباشد، الگوریتم رمزنگاری نسبت به کلید حساسیت بالایی دارد. در جدول (۶) نتیجه آزمون حساسیت نسبت به کلید نشان داده شده است. هیستوگرام هر تصویر نیز به منظور تشخیص تفاوت بین تصاویر رمز ترسیم شده است تا مقایسه آن‌ها آسان‌تر شود.

جدول ۵. مقادیر توابع ارزیابی برای تصویر cameraman با کلید x_0=۰/۴۵ و قانون ۱۳۵

الگوریتم	UACI	NPCR	MAE
تصویر رمز [۱۷]	۱۳/۵۲۸۰	۴۹/۱۵۰۱	۳۸/۱۰۹۱
تصویر رمز [۱۸]	۱۵/۶۰۶۹	۴۶/۱۱۳۶	۳۸/۰۱۷۳
تصویر رمز [۱۹]	۹/۵۴۶۵	۴۹/۴۷۸۱	۷۴/۵۲۱۷
تصویر رمز [۲۰]	۱۶/۲۸۸۷	۴۹/۳۵۴۶	۴۴/۲۷۳۶
تصویر رمز روش پیشنهادی	۱۶/۳۵۳۷	۴۹/۷۳۹۱	۴۴/۲۹۶۷

جدول ۶. تحلیل حساسیت نسبت به کلید

مجموعه کلیدهای اصلی	
هیستوگرام	تصویر رمز
	
	
	
	
	
	

۴-۶. ارزیابی زمانی و پیچیدگی محاسباتی

عملکرد یک سامانه رمزنگاری بر اساس عوامل مختلفی از جمله قابلیت اطمینان در برابر حمله‌های مختلف، پیچیدگی محاسباتی و زمان رمزنگاری ارزیابی می‌شود. در بخش‌های قبل مشاهده شد که الگوریتم پیشنهادی در برابر حمله‌های مختلف عملکرد خوبی داشته است. در این بخش نیز پیچیدگی محاسباتی و زمان اجرای الگوریتم بحث می‌شود. الگوریتم پیشنهادی در دو مرحله انجام می‌گیرد و شامل عملیات‌های مختلف از جمله تولید اعداد تصادفی، محاسبات خطی اتوماتای سلولی، شیفت دادن و XOR بیتی می‌باشد. تمام این عملیات‌ها، پیاده‌سازی مستقیم دارند. بنابراین الگوریتم پیشنهادی از نظر محاسباتی کارآمد است. زمان اجرای الگوریتم نیز یکی دیگر از عوامل ارزیابی است. الگوریتم پیشنهادی به طور متوسط دارای زمان اجرای ۳۲۳/۸۱۸۳ ثانیه است.

۵. نتیجه‌گیری

با توجه به خاصیت تصادفی بودن اتوماتای سلولی و امکان تولید الگوهای پیچیده، اتوماتای سلولی گزینه خوبی برای سامانه‌های رمزنگاری است. در این مقاله الگوریتم جدیدی با استفاده از اتوماتای سلولی معرفی شد. اتوماتای سلولی شامل انواع مختلفی است که در الگوریتم پیشنهادی از دو نوع اتوماتای سلولی ترکیبی و اتوماتای سلولی برگشت‌پذیر استفاده شده است. ساختار جدید برای رمزنگاری تصویر شامل دو مرحله رمزنگاری تصویر می‌باشد. بدیهی است با توجه به برگشت‌پذیری اتوماتای سلولی مراحل رمزگشایی قابل اجرا است.

به‌منظور بررسی کارآمدی روش پیشنهادی از آزمون‌های مختلف استفاده شده است. در این آزمون‌ها الگوریتم رمز پیشنهادی با سه الگوریتم رمز معرفی‌شده در [۲۰-۱۷] مقایسه شد و نتایج بهتری در اکثر آزمایش‌ها به‌دست آمد. طبق تحلیل آماری که شامل تحلیل هیستوگرام و ضرایب همبستگی است، مشاهده شد که در ساختار پیشنهادی هیچ‌گونه تشابه آماری و ظاهری بین تصویر اصلی و رمزشده نیست. همچنین در تصویر رمز شده میزان همبستگی بین پیکسل‌ها به طور قابل ملاحظه‌ای کاهش می‌یابد. در تحلیل هیستوگرام مشاهده شد که هیستوگرام تصاویر رمز تقریباً یکنواخت است. در تحلیل فضای کلید نشان داده شد که با استفاده از اتوماتای سلولی برگشت‌پذیر و اتوماتای سلولی ترکیبی از قوانین متعدد و مختلفی برای هر پیکسل استفاده شده است که این فضای کلید بزرگ عمل رمزگشایی و شناسایی کلید را مشکل‌تر می‌سازد. بنابراین الگوریتم پیشنهادی از فضای کلید مناسبی برخوردار است و نسبت به حمله‌های جامع مصون است. یکی دیگر از معیارهای ارزیابی، تمایز تصویر اصلی و رمز شده است. مطابق با نتایج به‌دست آمده، مشاهده شد که روش پیشنهادی نسبت به تغییرات ورودی حساسیت بالایی از خود نشان می‌دهد. در تحلیل حساسیت نسبت به کلید، نشان داده شد که الگوریتم رمز پیشنهادی نسبت به تغییرات کلید حساس است. همچنین پیچیدگی محاسباتی و ارزیابی زمانی نیز بر روی الگوریتم اعمال شدو نتایج رضایت بخشی را در بر داشت.

۶. مراجع

[1] Jolfaei, A.; Mirghadri, A. "A Novel Chaotic Image Encryption Scheme Using Chaotic Maps"; Advanced Defence Sci. & Tech. 2011, 2, 111-124.

[2] Gao, H.; Zhang, Y.; Liang, S.; Li, D. "A New Chaotic Algorithm for Image Encryption"; Chaos Soliton Fract. 2006, 29, 393-399.

[3] JH, l.; Lu JA, l.; C, Sh. "Chaotic Time Series Analysis and Its Application"; Publishing House of Wuhan University, Wuha, 2002, 57-66.

[4] Ding, A.; Yan, W. Q.; Qi, D. X. "Digital Image Scrambling Technology Based on Arnold Transformation"; Comput. Aided Des. 2001, 4, 338-341.

[5] Chen, J. X.; Zhu, Z. L.; Fu, C.; Yu, H.; Zhang, L. B. "A Fast Chaos-Based Image Encryption Scheme with a Dynamic State Variables Selection Mechanism"; Communications in Nonlinear Science and Numerical Simulation 2015, 20, 846-860.

[6] Pareek, N. K.; Patidar, V.; Sud, K. K. "Image Encryption Using Chaotic Logistic Map"; Image Vision Comput. 2006, 24, 926-934.

[7] Guan, Z. H.; Huang, F.; Guan, W. "Chaos-Based Image Encryption Algorithm"; Phys. Lett. A. 2005, 346, 153-157.

[8] Guardeno, D. A. "Framework for the Analysis and Design of Encryption Strategies Based on Discrete-Time Chaotic Dynamical Systems"; 2009, Doctoral Thesis, Universidad Politecticnica De Madrid.

[9] Von Neumann, J. "Theory of Self-Reproducing Automata"; Univ. of Illinois Press, 1966.

[10] Jin, J.; Wu, Z. H. "A Secret Image Sharing Based on Neighborhood Configurations of 2-D Cellular Automata"; Opt. Laser Technol. 2012, 44, 538-548.

[11] Eslam, Z.; Razzagh, S.; Zarepour Ahmadabadi, J. "Secret Image Sharing Based on Cellular Automata and Steganography"; Pattern Recogn. 2010, 43, 397-404.

[12] Rosin, P. L. "Image Processing Using 3-State Cellular Automata"; Computer Vision Image Understanding. 2010, 114, 790-802.

[13] Kauffmann, C.; Piche, N. "Seeded ND Medical Image Segmentation by Cellular Automaton on GPU"; Int. J. Comput. Assist Radiol. Surg. 2010, 5, 251-262.

[14] Eslami, Z.; Zarepour Ahmadabadi, J. "A Verifiable Multi- secret Sharing Scheme Based on Cellular Automata"; Inform. Sci. 2010, 180, 2889-2894.

[15] Ruisong, Y.; Huiliang, L. "A Novel Image Scrambling and Watermarking Scheme Based on Cellular Automata"; International Symposium on Electronic Commerce and Security. 2008, 938-941.

[16] Qadir, F.; Peer, M.; Khan, K. "Digital Image Scrambling Based on Two Dimensional Cellular Automata"; International Journal of Communication Networks and Information Security. 2013, 5, 36-41.

[17] Jin, J. "An Image Encryption Based on Elementary Cellular Automata"; Opt. Laser Eng. 2012, 50, 1836-1843.

[18] Abdo, A.; Lian, S.; Ismail, L.; Amin, M.; Diab, H. "A Cryptosystem Based on Elementary Cellular Automata"; Commun. Nonlinear Sci. Numer. Simul. 2013, 18, 136-147.

[19] Wang, X.; Luan, D. "A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata"; Commun. Nonlinear Sci. Numer. Simul. 2013, 18, 3075-3085.

[20] Mohamed, F. K. "A Parallel Block-Based Encryption Schema for Digital Images Using Reversible Cellular Automata"; Int. J. Eng. Sci. and Tech. 2014, 17, 85-94.

[21] Wolframe, S. "Theory and Application of Cellular Automata"; Singapore: World Scientific Publishing, 1986.

[22] Esnaashari, M.; Meybodi, M. "A Novel Clustering Algorithm for Wireless Sensor Networks Using Irregular Cellular Learning Automata"; In Int. Symposium on Telecommunications, 2008, 330-336.

[23] Kanso, A.; Ghebleh, M. "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map"; Commun. Nonlinear Sci. Numer. Simul. 2012, 17, 2943-2959.

[24] Jolfaei, A.; Mirghadri, A. "Survey: Image Encryption Using Salsa20"; International Journal of Computer Science Issues. 2010, 7, 213-220.