ارائه الگوریتم جدید رمزنگاری تصویر رنگی مبتنی بر نگاشت آشوب کوانتومی و شبکه تزویج (NCML)

الهه وافری[1]، کاوه کنگرلو[2]، رضا صباغی‌ندوشن[3]

۱. کارشناسی ارشد برق الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکزی

۲. استادیار گروه برق، دانشگاه آزاد اسلامی واحد تهران مرکزی

۳. استادیار گروه برق، دانشگاه آزاد اسلامی واحد تهران مرکزی، r_sabbaghi@iauctb.ac.ir

تاریخ دریافت: ۹۲/۹/۱۸ تاریخ پذیرش: ۹۳/۵/۵

چکیده

در این مقاله یک الگوریتم رمزنگاری تصویر رنگی با استفاده از نگاشت آشوب کوانتومی سه‌بعدی و شبکه‌های تزویج آشوب نزدیکترین همسایه ارائه شده است. الگوریتم شامل سه بخش است: در طبقه اول رشته کلیدهای رمزنگاری توسط نگاشت آشوب کوانتومی سه بعدی و شبکه‌های تزویج آشوب نزدیکترین همسایه، تأمین می‌شود. در طبقه دوم ابتدا موقعیت سطرهای مؤلفه‌های رنگی بصورت تصادفی تغییر و سپس بیت‌های هر پیکسل تصویر رنگی بصورت تصادفی شیفت چرخشی داده می‌شود. در این مرحله بیت‌های هر پیکسل حداقل یک و حداکثر هفت بیت شیفت داده می شوند. در طبقه سوم مؤلفه‌های رنگی جایگشت شده، با استفاده از رشته-کلیدهای شبه تصادفی بهم تزویج می‌شوند. به منظور بالابردن امنیت الگوریتم ارائه شده، برای تولید مقادیر اولیه نگاشت آشوب از کلید۱۲۸ بیتی استفاده می‌شود. تبدیلات بکار رفته در تولید کلید به گونه‌ای است که تک تک بیت ها به شرایط اولیه وابسته باشند. رمزنگاری تصویر بر خلاف روش‌های دیگر که مقادیر مناسب آزمون‌ها در تعداد تکرارهای بیشتری حاصل می‌شود تنها با یک‌بار اجرای الگوریتم صورت گرفته که سبب افزایش سرعت فرایند رمزنگاری شده است. نتایج شبیه‌سازی گویای مقاومت الگوریتم در مقابل انواع حملات آماری، حساسیت و حملات جامع فضای کلید است.

کلیدواژه

رمزنگاری تصویر، نگاشت آشوب کوانتومی سه‌بعدی، شبکه تزویج آشوب نزدیکترین همسایه، امنیت

مقدمه

با توجه به رشد چشمگیر فناوری اطلاعات و شبکه ارتباطات جهانی و نیز افزایش انتقال داده‌های دیجیتال در بستر اینترنت در عصر حاضر، نیاز به حفظ امنیت داده‌ها بویژه داده‌های تصویری با توجه به کاربردهای خاص آن بیش از پیش نمایان است. از این‌رو، رمزنگاری[1] به عنوان ابزاری برای حفظ امنیت داده‌های مورد مبادله و مصون ماندن آنها از دست کاربران غیرمجاز، مطرح شده است. در سالیان اخیر الگوریتم‌های رمزنگاری تصویر بسیاری بر پایه‌ی یکی از روش‌های استفاده از: نگاشت آشوب، تبدیل فوریه کسری، اتوماتای سلولی[2]، دنباله‌های DNA و... ارائه شده است[۵-۱]که در این میان الگوریتم‌های رمزنگاری مبتنی بر تئوری آشوب[3] با توجه به ویژگی‌های خوب این توابع همچون حساسیت به مقادیر اولیه، رفتار شبه تصادفی و قطعی بودن نگاشت در عین رفتار تصادفی آن، موجب شده که بیش از سایر شیوه‌ها نظر محققین را به خود معطوف نمایند[۶]،[۷]،[۱۰]. چنانچه برای نخستین بار در سال ۱۹۸۹ از تابع آشوب در رمزنگاری استفاده شده است[۷]. در این مقاله با استفاده از نگاشت آشوب کوانتومی سه‌بعدی و شبکه‌های تزویج آشوب نزدیکترین همسایه الگوریتمی ارائه می‌شود که به منظور برقرای امنیت بیشتر، از دو مشخصه‌ی مطلوب روش‌های رمزنگاری سنتی، جایگشت[4] و پراکندگی[5] بهره برده است. در ادامه ابتدا توضیح کوتاهی پیرامون نگاشت آشوب کوانتومی و شبکه‌های تزویج نزدیکترین همسایه بیان شده و سپس ضمن بررسی الگوریتم پیشنهادی، به تحلیل نتایج شبیه‌سازی و ارزیابی امنیت طرح، پرداخته شده است. در نهایت جمع‌بندی کار بیان شده است.

مفاهیم پایه‌ای در سیستم رمز پیشنهادی

نگاشت آشوب کوانتومی[6]

نگاشت لجستیک[7]، یک نگاشت خاص و مهم با میزان پراکندگی بسیار بالا است[۸]. با کوپلاژ مسیرهای کوانتومی در نوسانگرهای هارمونیکی، نگاشت لجستیک کوانتومی پراکنده توسط گوگین

1. Encryption
2.Cellular Automata
3.Chaotic Theory

4.Confusion
5.Diffusion
6.Quantum chaotic map
7.Logistic Map

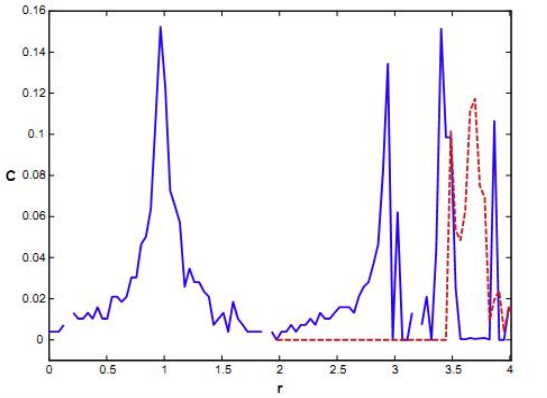
پیشنهاد و معرفی شد[۹]. به منظور مطالعه اثرات تصحیحات کوانتومی، مقدار $a=< a > + \delta a$ که در آن δa یک اعوجاج کوانتومی در حد $< a >$ است، بیان می‌شود. نگاشت آشوب کوانتومی با کمترین تصحیحات بصورت معادله (۱) توصیف می‌شود [۸]:

$$\begin{aligned} X_{n+1} &= r(X_n - |X_n|^2) - ry_n \\ y_{n+1} &= -y_n e^{-z\beta} + e^{-\beta} r\left[(2 - X_n - X_n^*)y_n - X_n Z_n^* - X_n^* Z_n\right] \\ Z_{n+1} &= -Zne^{-2\beta} + e^{-\beta} r\left[2(1 - X_n^*)Z_n - 2X_n y_n - X_n\right] \end{aligned} \quad (۱)$$

که درآن $X =< a >, y =< \delta a + \delta a >, z = \delta a \delta a >$ پارامتر β پراکندگی و r پارامتر قابل تنظیم است. همچنین متغیرهای x_n ،y_n و z_n اعداد مختلط با مقدار X_n^*, y_n^*, Z_n^* هستند. در معادله فوق، اگر مقادیر اولیه بصورت اعداد حقیقی درنظرگرفته شوند، تمامی دنباله‌های تولیدی بصورت اعداد حقیقی خواهند بود.

چنانچه حد پراکندگی β عدد بزرگی باشد ($\beta \to \infty$)، با درنظر گرفتن تصحیحات کوانتومی $y_n, z_n \to 0$، نگاشت سه بعدی کوانتومی به یک نگاشت یک بعدی لجستیک تبدیل می‌شود.

با وجود اینکه مدارات آشوبی بصورت نگاشت‌های زمان گسسته غیرمتناوب، در طبیعت هستند. به دلیل دقت محدود کامپیوترهای دیجیتالی، این مدارات در حوزه تناوبی قرار می‌گیرند اما میانگین دوره تناوب یک مدار در نگاشت سه بعدی بسیار طولانی‌تر از نگاشت یک بعدی است.



شکل ۱. پیچیدگی آماری، نمودار خط ممتد: میزان پراکندگی پیچیدگی نگاشت لجستیک کوانتومی بر حسب پارامتر کنترلی r، نمودارخط چین: میزان پراکندگی پیچیدگی نگاشت لجستیک بر حسب پارامتر کنترلیr[۸].

نمودار شکل (۱) پیچیدگی آماری نگاشت لجستیک کوانتومی را در مقایسه با نگاشت لجستیک، بر حسب پارامتر کنترلی r نشان می‌دهد. از مشاهده این نمودار می‌توان دریافت که نگاشت لجستیک کوانتومی، پیچیدگی رفتاری بیشتری دارد و بنابراین در برابر حملات جامع فضای کلید[۸] مقاومت بیشتری از خود نشان می‌دهد[۸].

شبکه‌های تزویج آشوب نزدیکترین همسایه[۹]

یک سیستم آشوب وابسته به زمان و مکان با نزدیکترین همسایه بصورت معادله (۲) توصیف می‌شود[۱۰]:

$$Z_{n+1}(j) = (1-\delta) f(Z_n(j)) + \delta f(Z_n(j+1)) \quad (۲)$$

که در آن n=۱،۲،۳،... اندیس زمان، j=۱،۲،...،T اندیس حالت شبکه تزویج، f یک نگاشت آشوب و ε ϵ (۰،۱) ضریب ثابت شبکه تزویج است. شرایط مرزی متناوب $z_n(j+T) = z_n(j)$ برای سیستم ارائه شده صادق است.

الگوریتم پیشنهادی

بلوک دیاگرام الگوریتم رمزنگاری طرح شده در شکل (۲) آورده شده است.

جزئیات الگوریتم رمزنگاری مبتنی بر فرآیند پراکندگی کلی نگاشت آشوب کوانتومی به صورت زیر توصیف می‌گردد:

تولید شرایط و مقادیر اولیه (تولید کلید رمزنگاری)

در سیستم‌های رمزنگاری مبتنی بر نگاشت آشوب کوانتومی، این پارامترها و مقادیر اولیه تابع آشوب هستند که کلید رمزنگاری را تشکیل می‌دهند. سیستم رمزنگاری پیشنهادی از یک کلید رمز خارجی متقارن (K) با طول ۱۲۸ بیت استفاده می‌کند که حاوی پارامترها و مقادیر اولیه تابع آشوب است. این کلید خارجی بصورت رابطه (۳) بیان می‌شود:

$$K = K_1, K_2, K_3, \ldots, K_{16} \quad (۳)$$

که در آن K_i بیانگر یک بلوک ۸ بیتی از کلید خواهد بود. به منظور افزایش حساسیت کلید به تغییرات جزئی و اثر اعمال آن روی تمامی پیکسل‌ها، فرآیندهایی بر روی آن انجام گرفته و برای تصویری با ابعاد W×H مقادیر اولیه بصورت رابطه (۴) خواهد بود:

$$\begin{aligned} X_o &= \left(\left((K_1 \oplus \ldots \oplus K_4) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) / 256 \\ X_o^* &= \left(\left((K_6 \oplus \ldots \oplus K_6) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) / 256 \\ y_o &= \left(\left((K_2 \oplus \ldots \oplus K_{12}) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) / 256 \\ Z_o &= \left(\left((K_{12} \oplus \ldots \oplus K_{16}) + \sum_{i=1}^{i=16} K_i\right) \bmod 256\right) / 256 \\ Z_o^* &= (X_o + X_o^* + y_o + Z_o) \bmod 1 \end{aligned} \quad (۴)$$

8.Brute force Attack

9.Nearest-Neighbouring Coupled-Map Lattices

شکل ۲. بلوک دیاگرام الگوریتم رمزنگاری

در بیان علت تلفیق دو مفهوم فوق در الگوریتم ارائه شده باید اشاره کرد که با توجه به اینکه در نگاشت آشوب کوانتومی، (رابطه ۱) چنانچه β عدد بزرگی باشد(چون در توان منفی e قرار دارد)، متغیرهای z،y می‌توانند به سمت صفر میل کنند و در اینصورت نگاشت سه بعدی لجستیک کوانتومی به نگاشت یک بعدی لجستیک که فضای کلید کوچکتری داشته و از پیچیدگی[10] و شدت تصادفی بودن[11] پایین‌تری نیز برخوردار است تبدیل خواهد شد[۸] و از سوی دیگر در نگاشت آشوب کوانتومی پس از چندین بار (مثلا ۵۰۰ بار) تکرار نگاشت، مقدارy، کوچک و کوچکتر شده و در نهایت به صفر می‌رسد که این نیز به نوبه‌ی خود می‌تواند منجر به کاهش پیچیدگی در تولید کلید رمزنگاری و نهایتاً کاهش حساسیت الگوریتم به کلید رمز شود، لذا برای کاهش اثرات نامطلوب یادشده، در الگوریتم پیشنهادی پس از تولید پارامترهای اولیه‌ی نگاشت آشوب کوانتومی، متغیرهای x_n، y_n و z_n توسط شبکه تزویج آشوب نزدیکترین همسایه بهم کوپلاژ شده و سپس رشته کلید رمزنگاری تولید می‌شود تا از پیچیدگی رشته کلید تصادفی اطمینان حاصل نموده و نیز از صفرشدن y و z طی دورهای بعدی اجتناب گردد.

مراحل الگوریتم رمزنگاری پیشنهادی

گام اول: اعمال کلید رمز خارجی ۱۲۸ بیتی و قرار دادن n=۰، H ×W=L، r= ۳/۹، β= ۴/۹ [۸] و تولید مقادیر اولیه طبق رابطه (۴).

گام دوم: اعمال مقادیر اولیه به رابطه (۱) و مقداردهی اولیه نگاشت آشوب. از آنجایی‌که مقادیر اولیه اعدادی حقیقی هستند در هر دور تکرار، سه رشته کلید x_{n+1}، y_{n+1} و z_{n+1} حقیقی بدست می‌آید. به‌منظور افزایش پیچیدگی مابین رشته‌کلیدهای تولیدی، با استفاده از رابطه (۲)، سه رشته‌کلید تولیدی بصورت زیر بهم کوپلاژ می‌شوند.

$$\begin{aligned} X_{n+1}^{coupl} &= (1-\varepsilon)X_n + \varepsilon y_n \\ Y_{n+1}^{couple} &= (1-\varepsilon)Y_n + \varepsilon Z_n \\ Z_{n+1}^{couple} &= (1-\varepsilon)Z_n + \varepsilon X_n \end{aligned} \qquad (۵)$$

سپس مقادیر بدست آمده در بازه [۰ ۲۵۵] بصورت رابطه(۶) نگاشت و ذخیره می‌شوند:

$$\begin{aligned} X_{n+1}^{keyster} &= \mathrm{mod}(round(X_{n+1}^{coupl} \times L),256) \\ Z_{n+1}^{keyster} &= \mathrm{mod}(round(Z_{n+1}^{coupl} \times L),256) \\ Y_{n+1}^{keyster} &= \mathrm{mod}(round(Y_{n+1}^{coupl} \times L),256) \end{aligned} \qquad (۶)$$

10.Complexity
11.Randomness

مقدار n= n+1 و گام دوم تا برقراری n < L ادامه می‌یابد.

گام سوم: در این فرآیند، تصویر رنگی با اندازه W×H فراخوانی شده و در ماتریس P با ابعاد ۳W×H قرار می‌گیرد. تعداد سطرهای این ماتریس ۳W و تعداد ستونهای آن H است.

گام چهارم: از گام دوم، W عضو از $X_{n+1}^{keyster}$ ، $Y_{n+1}^{keyster}$ و $Z_{n+1}^{keyster}$ برداشته می‌شود و در یک بردار سطری با نام m و اندازه ۱×۳W قرار داده می‌شود. سپس مقادیر موجود در بردار m بصورت صعودی منظم شده و در بردار 'm قرار می‌گیرند. با پیداکردن عناصر نظیر به نظیر 'm در m، ماتریس سطری index با مقادیر تصادفی بدست می‌آید که در بازه [۳W ۱] قرار دارند. با استفاده از عناصر ماتریس index ردیف‌های ماتریس P بصورت تصادفی جایگشت و در ماتریس 'P ذخیره می‌شوند.

گام پنجم: در این مرحله ماتریس 'P به سه زیرماتریس، $r\_per_{W\times H}$, $g\_per_{W\times H}$, $b\_pre_{W\times H}$ تقسیم می‌شود و سپس با استفاده از رابطه (۷) مقادیر $X_{n+1}^{keyster}$ ، $Y_{n+1}^{keyster}$ و $Z_{n+1}^{keyster}$ به پیمانه ۷ سنجیده می‌شوند تا تعداد شیفتهای چرخشی برای بیت‌های هر پیکسل مشخص گردد.

$$\begin{aligned} csr &= \mathrm{mod}(X_{n+1}^{keystr},7)+1 \\ csg &= \mathrm{mod}(Y_{n+1}^{keystr},7)+1 \\ csb &= \mathrm{mod}(Z_{n+1}^{keystr},7)+1 \end{aligned} \qquad (۷)$$

طبق رابطه (۸) بیت‌های هر پیکسل، با استفاده از مقادیر csr، csg و csb که در محدوده‌ی بین یک تا هفت قرار دارند، به‌سمت چپ شیفت چرخشی داده می‌شوند.

$$\begin{aligned} &r\_per_n = bitxor(bi\tan d(bitshift(r\_per_n, csr),256), \\ &bitshift(r\_per_n, csr-8)) \\ &g\_per_n = bitxor(bi\tan d(bitshift(g\_per_n, csg),256), \\ &bitshift(g\_per_n, csg-8)) \\ &\_per_n = bitxor(bi\tan d(bitshift(b\_per_n, csb),256), \\ &bitshift(b\_per_n, csb-8)) \end{aligned} \qquad (۸)$$

سپس n=n+1 قرار گرفته و این روند ادامه می‌یابد تا تمامی پیکسل‌ها شیفت داده شوند.

گام ششم: عملکرد فرآیند انتشار بدین ترتیب است که مقدار هر پیکسل به ترتیبی تغییر یابد که تغییر کوچک یک پیکسل روی تمامی پیکسل‌ها گسترش یابد. بدین منظور، در الگوریتم ارائه شده برای رمز هر پیکسل علاوه بر رشته کلید تولیدی و پیکسل ورودی، از مجموع اطلاعات رمزنشده بعد پیکسل رمزشده و مجموع اطلاعات رمزشده قبل پیکسل رمزشده استفاده می‌شود. بنابراین ابتدا پارامترهای n=1 ,rc=0 ,rci=0 ,gc=0 ,gci=0 ,bc=0 ,xrgb=0 bci=0 و sr=sum(r_per) ,sg=sum(g_per) ,sb=sum(b_per) مقداردهی اولیه می‌شوند و سپس مجموع پیکسل‌های رمزنشده‌ی بعد پیکسل nام برای هر سه مؤلفه‌ی قرمز، سبز و آبی از رابطه زیر محاسبه می‌شود:

$$\begin{aligned} sr &= sr - r\_per_n \\ sg &= sg - g\_per_n \\ sb &= sb - b\_per_n \end{aligned} \qquad (۹)$$

سپس مقادیر sr,sg,sb، تحت نگاشت غیر خطی Sbox [۲۳]قرار می‌گیرند. این عمل باعث می‌شود خروجی این معادله برای پیکسل‌هایی که مقدار نزدیک بهم دارند، مقادیر دور از هم یافته و همبستگی پیکسل‌های رمز کاهش یابد.

$$\begin{aligned} rr &= sbox(\mathrm{mod}(sr,256)+1) \\ gg &= sbox(\mathrm{mod}(sg,256)+1) \\ bb &= sbox(\mathrm{mod}(sb,256)+1) \\ ss &= rr+gg+bb \end{aligned} \qquad (۱۰)$$

مقادیر رمزشده‌ی پیکسل nام طبق رابطه زیر بدست می‌آید.

$$\begin{aligned} c\_r_n &= \mathrm{mod}((r\_per_n)+ss+X_n+xrgb+(rci),256) \\ c\_g_n &= \mathrm{mod}((g\_per_n)+ss+Y_n+c\_r_n+(gci),256) \\ c\_b_n &= \mathrm{mod}((b\_per_n)+ss+Z_n+c\_g_n+(bci),256) \end{aligned} \qquad (۱۱)$$

در معادله فوق برای بدست آوردن مقدار رمز شده پیکسل nام (C_r_n, C_g_n, C_b_n)، از مقادیر رمزنشده پیکسل nام (r_per_n, g_per_n, b_per_n)، مجموع نگاشت شده پیکسل‌های رمزنشده بعد پیکسل nام (ss)، مقادیر رشته کلید تولید شده (x_n,y_n,z_n)، مجموع پیکسل‌های رمزشده قبل پیکسل nام (xrgb) و مجموع مقادیر نگاشت شده پیکسل‌های رمزشده قبل پیکسل nام (rci,gci,bci) استفاده شده است.

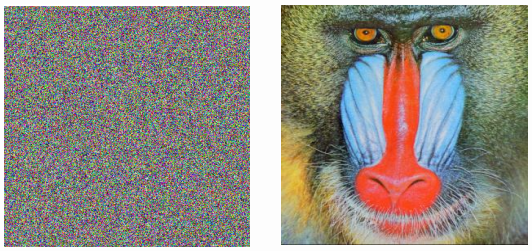
(منظور از نگاشت شده در عبارات فوق، یعنی تابع تحت نگاشت غیرخطی Sbox قرار داده شده است.)

$$\begin{aligned} rc &= rc + c\_r_n \\ gc &= gc + c\_g_n \\ bc &= bc + c\_b_n \\ xrgb &= rc + gc + bc \end{aligned} \qquad (۱۲)$$

$$\begin{aligned} rci &= sbox(\mathrm{mod}(rc,256)+1) \\ gci &= sbox(\mathrm{mod}(gc,256)+1) \\ bci &= sbox(\mathrm{mod}(bc,256)+1) \end{aligned} \qquad (۱۳)$$

سپس مقدار n=n+1 قرار می‌گیرد و تا برقراری n ≤ L، این مرحله تکرار می‌شود.

گام هفتم: درآخرین گام، مقادیر ماتریس‌های C_r_n, C_g_n, C_b_n به ترتیب به ماتریس‌های $enc\_r_{W\times H}$, $enc\_g_{W\times H}$, $enc\_b_{W\times H}$ انتقال داده می‌شوند و تصویر رنگی رمزشده نهایی بدست می‌آید.
شکل(۳) تصویر استاندارد و تصویر رمزشده آنرا نشان می‌دهد.



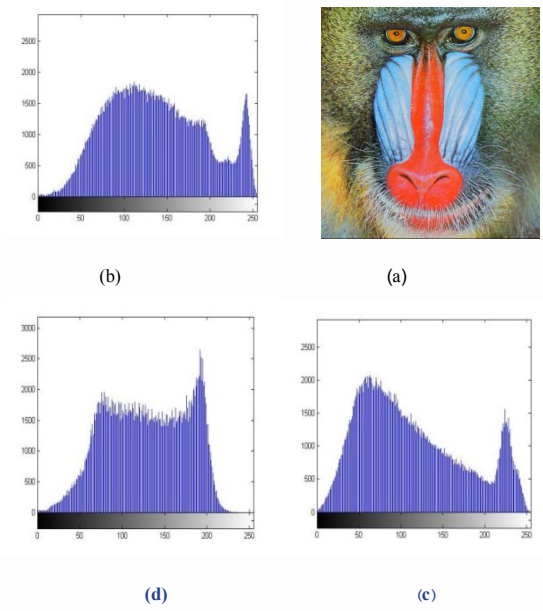
(b) (a)

شکل۳. (a) تصویراصلی بابون (۵۱۲×۵۱۲) ، (b) تصویر رمزشده

الگوریتم رمزگشایی مشابه الگوریتم رمزنگاری است با این تفاوت که فرآیند انجام گرفته در این الگوریتم عکس رمزنگاری بوده و تمامی مراحل از انتها به ابتدا انجام می‌شود.

نتایج شبیه سازی

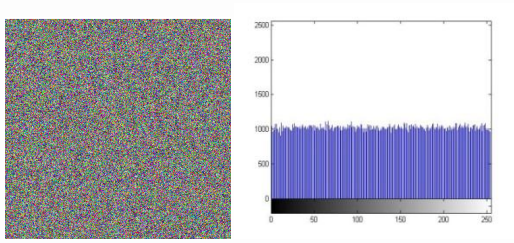
طرح پیشنهادی جهت ارزیابی و مقایسه میزان کارایی آن با سایر روش‌های ارائه شده، بر روی تعدادی از تصاویر استاندارد پایگاه داده CVG-UGR انجام شده است. شکل‌های۴، ۵ و ۶ نتایج اعمال الگوریتم بر تصویر استاندارد بابون با ابعاد ۵۱۲×۵۱۲ را نشان می‌دهد.
یک روش رمزنگاری بهینه باید در برابر انواع حملات از جمله حملات کشف رمز، حملات آماری و حملات جامع فضای کلید از امنیت و کارایی کافی برخوردار باشد که برای بررسی این مورد در ادامه به ارزیابی الگوریتم پیشنهادی پرداخته شده‌است.



(b) (a)

(d) (c)

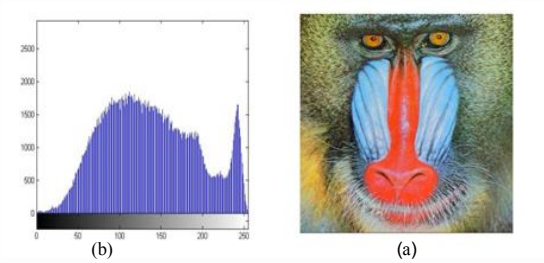
شکل۴. (a) تصویراصلی، (b),(c),(d) به ترتیب هیستوگرام مؤلفه قرمز، سبز و آبی



(b) (a)

(d) (c)

شکل ۵. (a) تصویر رمزشده،(b) ،(c) و (d) به ترتیب هیستوگرام مؤلفه قرمز، سبز و آبی



(b) (a)

(d) (c)

شکل۶ . (a) تصویر رمزگشایی شده،(b) ،(c) و (d) به ترتیب هیستوگرام مؤلفه قرمز، سبز و آبی

تحلیل فضای کلید

یک الگوریتم رمزنگاری باید به کلید رمزنگاری حساس باشد. از نقطه‌نظر رمزنگاری، اندازه فضای کلید باید بزرگتر از 2^{100} باشد تا سطح امنیت بالایی را فراهم نموده و الگوریتم در برابر حملات رمزنگاری مقاوم باشد[۱۱]،[۱۲]. سازمان NIST[12] حداقل طول کلید ممکن برای برقراری امنیت محاسباتی در برابر حملات جستجوی جامع فضای کلید را تا سال ۲۰۱۵، ۸۰ بیت پیش بینی کرده است[۱۳]. از آنجایی‌که این الگوریتم از یک کلید رمز خارجی

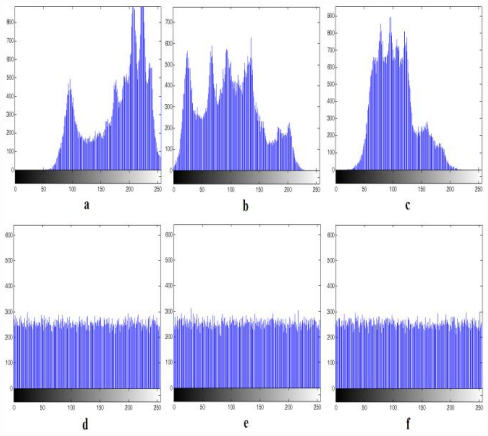
12.National Institute of Standards and Technology

۱۲۸ بیتی استفاده می‌کند، لذا فضای کلیدی برابر با $۲^{۱۲۸}\approx ۳/۴۰۲۸\times ۱۰^{۳۸}$ خواهد داشت که بسیار بزرگتر از $۲^{۱۰۰}$ است. بنابراین الگوریتم در برابر کلیه‌ی حملات جامع فضای کلید مقاوم است.

تحلیل هیستوگرام

اگر توزیع سطوح خاکستری یک تصویر رمزشده یکنواخت نباشد، با حمله‌ی فقط متن رمزشده[۱۳] می‌توان تصویر اصلی را با در اختیار داشتن تصویر رمزشده و بدون نیاز به کلید آشکارسازی نمود. بنابراین یک الگوریتم رمزنگاری خوب باید به‌گونه‌ای عمل کند که هیستوگرام تصویر رمزشده دارای ظاهری تصادفی و یکنواخت بوده و مهاجم از این باب به هیچ اطلاعاتی دست پیدا نکند [۵]، [۱۴]، [۱۵].

در شکل (۷) هیستوگرام سه مؤلفه‌ی قرمز، سبز و آبی تصویر استاندارد لنا به همراه هیستوگرام متناظر تصویر رمزشده آن توسط الگوریتم پیشنهادی، نشان داده شده است. همانطور که مشاهده می‌شود هیستوگرام تمامی تصاویر رمزشده کاملاً یکنواخت بوده و متفاوت از هیستوگرام تصاویر اصلی است. این بدان معنی است که مهاجمان با بررسی هیستوگرام تصاویر رمزشده هیچگونه اطلاعاتی در مورد تصاویر اصلی بدست نخواهند آورد.



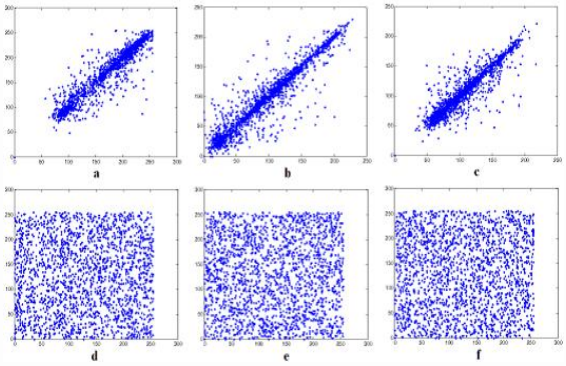
شکل ۷. تحلیل هیستوگرام تصویر لنا، (a)،(b) و (c) به ترتیب هیستوگرام مؤلفه‌های قرمز، سبز و آبی تصویر اصلی،(d)،(e) و (f) به ترتیب هیستوگرام تصاویر رمزشده

تحلیل همبستگی پیکسل‌های مجاور[۱۴]

برای ارزیابی همبستگی میان دو پیکسل مجاور در یک تصویر، ابتدا به صورت کاملاً تصادفی ۴۰۹۶ زوج از پیکسل‌های مجاور هم انتخاب و سپس ضریب هم‌بستگی هر زوج با استفاده از روابط زیر محاسبه می‌شود[۹]:

$$E(X)=\frac{1}{N}\sum_{i=1}^{N}X_i$$
$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(X_i-E(X))(y_i-E(y)) \qquad (۱۴)$$
$$D(X)=\frac{1}{N}\sum_{i=1}^{N}(X_i-E(X))(y_i-E(y))$$
$$r(x,y)=\frac{\operatorname{cov}(x,y)}{\sqrt{D(X)}\sqrt{D(Y)}}$$

x و y مقدار سطح خاکستری دو پیکسل مجاور و N تعداد پیکسل‌های مجاور انتخاب شده از تصویر جهت محاسبه همبستگی است. حداکثر ضریب همبستگی برابر عدد یک و بیانگر وجود همبستگی بالا بین پیکسل‌های مجاور است. یک الگوریتم رمزنگاری خوب باید تصویر را به‌گونه‌ای رمز نماید که ضرایب همبستگی بین پیکسل‌های مجاور در تصویر رمزشده بسیار کوچک و نزدیک به صفر باشد تا حمله‌کننده با تحلیل فوق به هیچگونه اطلاعات درخوری دسترسی نیابد. توزیع همبستگی پیکسل‌های مجاور برای راستای افقی در تصویر اصلی و تصویر رمزشده در شکل (۸) نشان داده شده است.



شکل ۸. تحلیل همبستگی پیکسلهای مجاور در راستای افقی: (a)،(b) و (c) به ترتیب توزیع همبستگی پیکسلهای مجاور مؤلفه قرمز، سبز و آبی در تصویر اصلی لنا،(d)،(e) و (f) به ترتیب توزیع همبستگی پیکسل‌های مجاور مؤلفه قرمز، سبز و آبی در تصویر رمزشده

از مشاهده شکل به وضوح می‌توان دریافت که همبستگی پیکسل‌های مجاور پس از رمزنگاری به میزان قابل توجهی کاهش یافته است. همچنین میانگین ضرایب همبستگی سه مؤلفه‌ی قرمز، سبز و آبی در سه راستای افقی، عمودی و قطری در تصویر اصلی و تصویر رمزشده در جدول (۱) و نتایج مقایسه ضرایب همبستگی روش ارائه شده با سایر روش‌ها در جدول (۲) آورده شده است.

13.Cipher text-Only-Attack
14.Correlation of Two Adjacent Pixels

جدول ۱. ضرایب همبستگی دو پیکسل مجاور در راستای افقی، عمودی و قطری برای تصویر اصلی لنا و تصویر رمزشده آن

جهت	تصویر اصلی	تصویر رمزشده
افقی	۰,۹۶۵۶۸۴	۰,۰۰۲۳۵۱
عمودی	۰,۹۷۸۶۵۲	۰,۰۰۱۲۳۶
قطری	۰,۹۵۳۷۸۶	۰,۰۰۰۳۶۱

جدول ۲. مقایسه ضرایب همبستگی الگوریتم ارائه شده برای تصویر لنا با الگوریتم‌های دیگر

جهت	افقی	عمودی	قطری
تصویر اصلی	۰,۹۶۵۶۸۴۳	۰,۹۷۸۶۵۲۳	۰,۹۵۳۷۸۵۶
الگوریتم ارائه شده	۰,۰۰۲۳۵۰	۰,۰۰۱۲۳۵	۰,۰۰۰۳۶۰
مرجع [۱۲]	۰,۰۰۰۵۵۰	۰,۰۰۰۸۳۹	۰,۰۰۱۱۲۴
مرجع [۴]	۰,۰۰۰۵۹۵	۰,۰۰۱۸۵۱	۰,۰۰۱۸۵۱
مرجع [۱۱]	۰,۰۰۴۹۱۴	۰,۰۱۲۸۷۸	۰,۰۰۷۵۳۹
مرجع [۸]	۰,۰۰۶۵۰۰	۰,۰۰۵۵۰۰	۰,۰۰۸۲۰۰
مرجع [۱۴]	۰,۰۰۵۳۴۳	۰,۰۰۸۴۶۰	۰,۰۰۳۵۵۷

تحلیل حساسیت الگوریتم

الگوریتم رمزنگاری تصویر باید به کوچکترین تغییرات در تصویر اصلی و کلید رمز حساس باشد تا بتواند در مقابل حملات تفاضلی[15] مقاومت نماید. بدین منظور تحلیل حساسیت الگوریتم برای تصویر اصلی و کلید انجام گرفته و نتایج در ادامه آورده شده است.

حساسیت الگوریتم نسبت به تصویر اصلی

برای ارزیابی حساسیت، ابتدا تصویر اصلی رمز می‌گردد. سپس یک پیکسل از تصویر اصلی به صورت کاملاً تصادفی تغییر داده می‌شود. تصویر حاصل مجدداً رمزشده و در نهایت دو تصویر رمزشده با توجه به روابط (۱۶) و(۱۷) با هم مقایسه می‌شوند.

بررسی تأثیر تغییر یک پیکسل در تصویر اصلی بر روی تصویر رمزشده از طریق محاسبه‌ی دو معیار اندازه‌گیری[16] NPCR و UACI[17] انجام می‌گیرد. NPCR متوسط تعداد پیکسل‌هایی از تصویر رمزشده را نشان می‌دهد که در اثر تغییر یک پیکسل از تصویر اصلی تغییر کرده‌اند. برای دو تصویر رمزشدهی C_1 و C_2 که تصاویر اولیه آنها تنها در یک پیکسل با یکدیگر اختلاف دارند ابتدا آرایه دو بعدی D(i, j) طبق رابطه (۱۵) محاسبه می‌شود[۴]:

$$D(i,j)=\begin{cases}1 & c_1(i,j)\neq c_2(i,j)\\ 0 & c_1(i,j)=`c_2(i,j)\end{cases} \qquad (۱۵)$$

15.Differential Attack
16.Number of Pixels Change Rate
17.Unified Average Changing Intensity

$C_1(i,j)$ و $C_2(i,j)$ به‌ترتیب مقدار سطح خاکستری پیکسل در مختصات (i,j) تصاویر رمزشده‌ی C_1 و C_2 را نشان می‌دهد.

سپس NPCR طبق رابطه‌ی زیر محاسبه می‌شود:

$$NPCR=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\% \qquad (۱۶)$$

پارامترهای M و N ابعاد تصویر اصلی را نشان می‌دهد.

UACI میانگین اختلاف شدت روشنایی میان دو تصویر مطابق رابطه‌ی زیر بدست می‌آید:

$$UACI=\frac{1}{M\times N}\left[\frac{\sum i,j\left|C_{1(i,j)}-C_{2(i,j)}\right|}{2^L-1}\right]\times 100 \qquad (۱۷)$$

پارامتر L تعداد بیت‌های مورد استفاده برای نمایش تصویر بوده که در اینجا برابر عدد ۸ است.

این آزمون برای هر تصویر به دفعات تکرار شده و نتایج حاصل در جدول(۳) آورده شده است. با توجه به نتایج شبیه سازی، سیستم رمز ارائه شده عملکرد بالایی در مقابل این آزمون با مقادیر NPCR > ۹۹/۶۰۹۲ و UACI > ۳۳/۴۶۰۶ از خود نشان داده است.

جدول ۳. تحلیل حساسیت الگوریتم به تصویر اصلی

تصویر استاندارد	آزمون	حداقل	حداکثر	میانگین
بابون	NPCR	۰,۹۹۵۸۵۶	۰,۹۹۶۳۲۹	۰,۹۹۶۰۷۶
	UACI	۰,۳۳۳۶۶۶	۰,۳۳۵۲۷	۰,۳۳۴۶۰۱
لنا	NPCR	۰,۹۹۵۹۵۴	۰,۹۹۶۳۰۵	۰,۹۹۶۰۷۸
	UACI	۰,۳۳۳۸۰	۰,۳۳۵۳۳۴	۰,۳۳۴۵۸۵
هواپیما	NPCR	۰,۹۹۵۸۸۵	۰,۹۹۶۳۰۴	۰,۹۹۶۱۰۲
	UACI	۰,۳۳۵۶۲۲	۰,۳۳۵۶۲۲	۰,۳۳۳۸۷۴
قایق	NPCR	۰,۹۹۵۸۷۶	۰,۹۹۶۳۵۱	۰,۹۹۶۰۸۴
	UACI	۰,۳۳۳۶۹۱	۰,۳۳۵۰۱	۰,۳۳۴۵۲۱

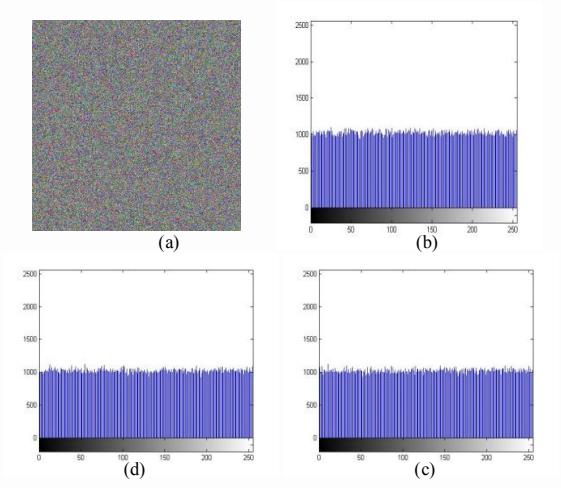
جدول (۴)، به مقایسه‌ی مقادیر NPCR و UACI الگوریتم ارائه شده و مراجع دیگر می‌پردازد. همانطور که نتایج شبیه سازی نشان می‌دهد روش پیشنهادی عملکرد قابل قبولی داشته و به نتایج رضایت بخشی دست یافته است.

جدول ۴. مقایسه مقادیر حساسیت به متن اصلی الگوریتم ارئه شده برای تصویر لنا با الگوریتم‌های دیگر

الگوریتم	میانگین NPCR	میانگین UACI
الگوریتم ارائه شده	۰,۹۹۶۰۸۶	۰,۳۳۴۶۲۷۰
مرجع [۱۲]	۰,۹۹۶۸۲۸	۰,۳۳۴۸۹۸
مرجع [۱۱]	۰,۹۹۶۰۲۸	۰,۳۳۴۲۸۹
مرجع [۱۰]	۰,۹۹۶۱۱۰	۰,۳۳۴۶۳۰۰
مرجع [۵]	۰,۹۹۶۵۰۰	۰,۳۳۴۸۰۰
مرجع [۱۴]	۰,۲۱۴۸۰۰	۰,۰۲۵۱۰۰

حساسیت الگوریتم نسبت به کلید رمز

برای تحلیل حساسیت الگوریتم پیشنهادی نسبت به کلید، ابتدا تصویر اصلی با ابعاد ۵۱۲ ×۵۱۲ توسط کلید «۲۱۵، ۲۱۳، ۶۵، ۱۵۷، ۲۳۸، ۱۳۸، ۲۲۲، ۶۷، ۸۱، ۳۰، ۲۴۰، ۱۶۵، ۲۲،۱۶۳، ۳۹، ۱۶۵» رمزشده و سپس با تغییر کم ارزش‌ترین بیت آخرین حرف کلید یعنی «۲۱۵, ۲۱۳, ۶۵, ۱۵۷, ۲۳۸, ۱۳۸, ۲۲۲, ۶۷, ۸۱, ۳۰, ۲۴۰, ۱۶۵, ۲۲, ۱۶۳, ۱۳۹, ۱۶۴» همان تصویر مجدداً رمز می‌گردد. سرانجام دو تصویر رمزشده با هم مقایسه می‌شوند. این آزمون نشان می‌دهد که اگرچه دو کلید تنها در یک بیت با هم اختلاف دارند، اما یک تفاوت ۹۹/۶۱ درصد برحسب مقادیر سطح خاکستری پیکسل‌ها در دو تصویر رمزشده وجود خواهد داشت. تبدیل‌های استفاده شده در معادلات رمزگذاری و رمزگشایی به گونه‌ای طراحی شده است که پارامترها و شرایط اولیه حتی به تغییر یک بیت بسیار حساس هستند و در نتیجه الگوریتم پیشنهادی می‌تواند در مقابل حملات حساسیت بخوبی مقاومت کند.



شکل۹. (a) تصویر رمزگشایی شده با کلید نادرست(بابون)،(b)(c)(d) به ترتیب هیستوگرام مؤلفه‌های قرمز، سبز و آبی

شکل (۹) تصویر رمزگشایی شده‌ی بابون با کلید نادرست بهمراه هیستوگرام سه مؤلفه‌ی رنگ آنرا نشان می‌دهد.

مقایسه‌ای از حساسیت به کلید رمزنگاری برای الگوریتم ارائه شده و الگوریتم‌های دیگر از جمله روش مرجع [۱۶] که عملکرد ایده‌آل‌تری نسبت به سایر روش‌ها دارد در جدول (۵) نشان داده شده است.

جدول ۵. مقایسه مقادیر حساسیت الگوریتم ارائه شده به کلید رمز برای تصویر لنا با الگوریتم‌های دیگر

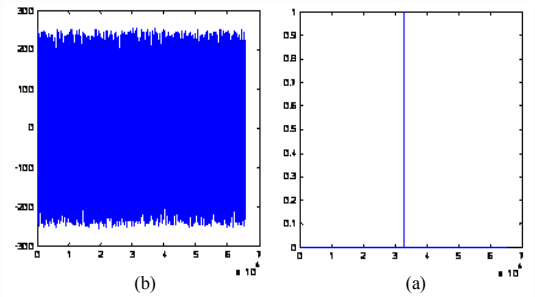
الگوریتم	میانگین مقادیر
الگوریتم ارائه شده	۰,۵۰۰۰۲۹
مرجع [۱۲]	۰,۵۰۰۱۲۲۸۷
مرجع [۱۱]	۰,۴۹۸۲۰۱۰۱
مرجع [۸]	۰,۴۹۹۹
مرجع [۱۸]	۰,۴۹۹۹۱

معیار بهمنی[18]

الگوریتم رمزنگاری به تصویر ورودی بسیار حساس خواهد بود اگر تغییر یک بیت از تصویر اصلی، تصویر رمزشده‌ای بوجود آورد که ۵۰ درصد بیت‌های آن تغییر کرده باشد. برای انجام این آزمون دو تصویر اصلی ورودی که تنها در یک بیت با هم اختلاف دارند، رمز می‌شوند و سپس میزان تغییر بیت‌ها برای تصاویر رمزشده محاسبه می‌شود. در حالت ایده‌آل نرخ تغییر بیت‌ها برای تصاویر رمزشده برابر ۵۰ درصد است. این آزمون بر روی تصاویر مختلف انجام گرفته و نرخ تغییر بیت‌ها برابر با ۵۰/۰۰۰۱۹۰۷۳ درصد بدست آمده است.

تفاوت میان دو مؤلفه تصویر اصلی و تصویر رمزشده‌ی آنها با اختلاف یک بیت، در شکل (۱۰) نشان داده شده است.

جدول(۶) نتایج مقایسه آزمون معیار بهمنی در الگوریتم ارائه شده با دیگر الگوریتم‌ها را نشان می‌دهد.



شکل ۱۰. (a) اختلاف دو تصویر اصلی، (b) اختلاف تصاویر رمزشده‌ی آنها

18.Avalanche criterion

جدول ۶. مقایسه مقادیر معیار بهمنی الگوریتم ارائه شده برای تصویر لنا با الگوریتم‌های دیگر

الگوریتم	میانگین NPCR	میانگین UACI
الگوریتم ارائه شده	۰,۹۹۶۰۷۹۱	۰,۳۳۴۶۳۰۰
مرجع [۱۶]	۰,۹۹۶۳۸۸۶	۰,۳۳۴۱۸۸۶
مرجع [۱۱]	۰,۸۱۴۰۳۳۲	۰,۲۷۲۴۷۵۴
مرجع [۱۲]	۰,۹۹۶۰۹۸۱	۰,۳۳۴۶۲۹۴
مرجع [۱۷]	۰,۹۹۶۰۲۴۴	----

تحلیل بی نظمی[19] اطلاعات

آنتروپی یا بی‌نظمی معیاری برای بیان تصادفی بودن منبع اطلاعات است که نخستین بار در سال ۱۹۴۹ توسط شانون[20] معرفی شد[۱۹] و برای محاسبه آن از رابطه (۱۸) استفاده می‌شود:

$$H(s)=-\sum_{i=0}^{N-1}P(S_i),\log_2,P(S_i) \qquad (۱۸)$$

که در آن N برابر با تعداد سطوح خاکستری استفاده شده در تصویر (در تصاویر ۸ بیتی N= ۲۵۶) و $P(s_i)$ احتمال وقوع سطح خاکستری iام در تصویر است. در یک تصویرکاملاً تصادفی یا به عبارت دیگر در تصویری با ۲۵۶ سطح خاکستری، با این فرض که همه مقادیر سطح خاکستری احتمال برابر داشته باشند، مقدار بی‌نظمی برابر با ۸ خواهد بود که این مقدار به عنوان ایده‌آل در نظر گرفته می‌شود. نتایج مربوط به مقایسه آنتروپی الگوریتم ارائه شده و مراجع دیگر در جدول (۷) آمده است و از مشاهده آن می‌توان دریافت که در فرآیند رمزنگاری، نشت اطلاعات بسیار جزئی و طرح ارائه شده در مقابل حمله‌ی بی‌نظمی به میزان کافی مصونیت دارد.

جدول ۷. مقایسه مقادیر آنتروپی الگوریتم ارائه شده برای تصویر لنا با الگوریتم‌های دیگر

الگوریتم	مؤلفه قرمز	مؤلفه سبز	مؤلفه آبی
الگوریتم ارائه شده	۷,۹۹۹۳۳۰	۷,۹۹۹۳۵۱	۷,۹۹۹۲۵۱
مرجع [۱۶]	۷,۹۹۹۷۸۵	۷,۹۹۹۷۷۸	۷,۹۹۹۷۸۰
مرجع [۱۱]	۷,۹۹۷۲۴۲	۷,۹۹۶۸۳۳	۷,۹۹۷۱۵۴
مرجع [۱۲]	۷,۹۹۹۲۷۱	۷,۹۹۹۲۳۶	۷,۹۹۹۱۰۶

آزمون‌های شبه تصادفی بودن

جهت اطمینان از امنیت یک سیستم رمزنگاری تصویر، آزمون‌های آماری بسیاری برای ارزیابی تصادفی بودن خروجی سیستم رمزنگار وجود دارد که هریک وجود یا عدم وجود یک الگوی معین را در خروجی سیستم مشخص می‌کند، چنانچه اگر الگویی یافت شود بدان معنا است که دنباله‌ی خروجی غیر تصادفی است. اخیراً NIST مجموعه‌ای از آزمون‌های آماری مختلف جهت ارزیابی تصادفی بودن دنباله‌ی دودویی تولید شده توسط مولدهای اعداد شبه تصادفی سخت افزاری یا نرم افزاری را ارائه کرده است.ENT، DIEHARD وNIST از جمله‌ی این آزمون‌ها است[۲۰]،[۲۱]، [۲۲].

برای آنکه نتایج به مقدار واقعی نزدیک باشد، دنباله تصویرهای رمزشده باید بالای صد میلیون بیت باشد. بدین منظور، تصاویر رمزشده با مقادیر کلیدهای ورودی مختلفی بدست می‌آیند و سپس روی این تصاویر رمزشده آزمون‌های موردنظر پیاده‌سازی می‌شوند. در انجام این آزمایش‌ها، از ۱۲۵ دنباله تصویر رمزشده با ۱۰۰۰۰۰۰ بیت استفاده شده است. بیت صحت رنگ[21] در تصاویر اصلی و رمز شده، ۲۴ است. نتایج این ارزیابی در جداول (۱۰-۸) آورده شده است. در تمام این آزمون‌ها، اگر P-مقدار محاسبه شده کوچکتر از ۰/۰۱ باشد، دنباله غیرتصادفی و در غیر اینصورت، دنباله تصادفی است و نشان از موفقیت آن آزمون دارد. توصیف ریاضی مجموعه آزمون‌های آماری NIST با عنوان NIST SP 800-22 قبلاً انجام گرفته است[۲۰]. نتایج بدست آمده حاکی از آن است که الگوریتم مورد مطالعه تمامی آزمون‌های ذکرشده را با موفقیت گذرانده است. بنابراین تصاویر رمزشده کاملاً بصورت شبه تصادفی هستند.

نتیجه‌گیری

در این مقاله روشی برای رمزنگاری تصاویر رنگی مبتنی بر نظریه آشوب کوانتومی و شبکه تزویج نزدیکترین همسایه به همراه تلفیقی از جایگشت و پراکندگی، به گونه‌ای ارائه شده است که ضمن برقراری امنیت و دقت کافی، از حساسیت بالایی نیز برخوردار باشد و در برابر انواع حملات تفاضلی، آماری، حساسیت و حملات جامع فضای کلید امنیت کافی داشته باشد.

استفاده از توابع آشوب کوانتومی برای ایجاد دنباله‌های شبه‌تصادفی از یک سو و وابسته کردن رشته کلیدهای تولیدی به هم با استفاده از شبکه تزویج (NCML) از سوی دیگر باعث می‌شود که از ترکیب این دو تابع، الگوریتم ارائه شده حساسیت به کلید رمز بالایی نسبت به سایر روش‌ها داشته باشد. از دیگر مشخصه‌های روش پیشنهادی آنست که رمزنگاری تصویر با یک‌بار تکرار انجام می‌گیرد در صورتی که در بعضی روش‌ها، مقادیر مناسب برای آزمون‌ها در تعداد تکرارهای بیشتری حاصل می‌شود و این به مفهوم سرعت عمل بیشتر در فرایند رمزنگاری است.

با توجه به اینکه کارت ملی بعنوان ابزاری برای شناسایی و تأیید

19.Entropy
20.Shannon
21.Bit True Color

هویت افراد مورد استفاده قرار می‌گیرد و حفظ امنیت اطلاعات آن ضروری به‌نظر می‌رسد، استفاده از الگوریتم رمزنگاری فوق به منظور اجتناب از جعل هویت پیشنهاد می‌شود.

جدول ۸. نتایج آزمون DIEHARD روی تصویر لنا

نام آزمون	میانگین نتایج	نتیجه*
Birthday spacing	۰,۵۷۶۷۸۲	موفقیت آمیز
Overlapping permutation	۰,۷۱۵۰۸	موفقیت آمیز
Binary rank 31*31	۰,۳۹۷۳۴۴	موفقیت آمیز
Binary rank 32*32	۰,۳۲۲۱۴۷	موفقیت آمیز
Binary rank 6*8	۰,۰۶۰۹۳۵	موفقیت آمیز
Bitstream	۰,۵۴۳۲۳۲	موفقیت آمیز
OPSO	۰,۳۹۷۹۲۶	موفقیت آمیز
OQSO	۰,۳۸۵۰۳۹	موفقیت آمیز
DNA	۰,۵۷۴۱۴۵	موفقیت آمیز
Count the ones 01	۰,۳۷۹۹۷۸	موفقیت آمیز
Count the ones 02	۰,۶۰۳۱۶	موفقیت آمیز
Parking lot	۰,۱۳۸۶۸۷	موفقیت آمیز
Minimum distance	۰,۳۷۱۰۴۵	موفقیت آمیز
3DS spheres	۰,۲۴۸۵۶۳	موفقیت آمیز
Squeeze	۰,۳۶۳۰۳۶	موفقیت آمیز
Overlapping sum	۰,۲۰۰۵۱۰	موفقیت آمیز
Runs	۰,۳۰۸۶۴۶	موفقیت آمیز
Craps	۰,۲۲۶۴۶۷	موفقیت آمیز

جدول ۹. نتایج آزمون ENT روی تصویر لنا

نام آزمون	مقدار میانگین	نتیجه
Entropy	۷,۹۹۹۹۸۲	موفقیت آمیز
Arithmetic mean	۱۲۷,۴۶۵۸	موفقیت آمیز
Monte Carlo	۳,۱۴۲۷۹۸۲۵۰	موفقیت آمیز
Chi square	۲۹۱,۵۸	موفقیت آمیز
SCC	۰,۰۰۰۶۱۶	موفقیت آمیز

جدول ۱۰. نتایج آزمون NIST SP 800-22 روی تصویر لنا

نام آزمون		مقدار p	نتیجه*
Frequency		۰,۵۴۲۵۶۶	موفقیت آمیز
Block-frequency		۰,۸۵۵۵۳۴	موفقیت آمیز
Runs(M=10000)		۰,۲۹۳۲۳۵	موفقیت آمیز
Long runs of ones		۰,۷۴۸۲۲۹	موفقیت آمیز
Rank		۰,۱۵۱۶۱۶	موفقیت آمیز
Spectral DFT		۰,۰۶۵۱۶۲	موفقیت آمیز
No overlapping templates		۰,۴۱۸۹۶۸	موفقیت آمیز
Overlapping templates		۰,۶۲۸۴۴۳	موفقیت آمیز
Universal (L=7, Q=1280,K=141577)		۰,۳۸۵۲۵۷	موفقیت آمیز
Lempel ziv complexity		۰,۴۵۶۳۵۵۷	موفقیت آمیز
Linear complexity		۰,۷۴۸۲۲۹	موفقیت آمیز
Serial	مقدار اولp	۰,۱۳۱۵۰۰	موفقیت آمیز
Serial	مقدار دومp	۰,۵۴۲۵۶۶	موفقیت آمیز
Approximate entropy		۰,۷۱۴۶۶۰	موفقیت آمیز
Cumulative sums forward		۰,۷۹۶۵۸۰	موفقیت آمیز
Cumulative sums reverse		۰,۶۶۳۱۳۰	موفقیت آمیز
Random excursions	X=-4	۰,۷۵۲۳۶۱	موفقیت آمیز
	X=-3	۰,۸۶۵۶۹۷	موفقیت آمیز
	X=-2	۰,۳۰۲۲۹۱	موفقیت آمیز
	X=-1	۰,۷۰۱۸۷۹	موفقیت آمیز
	X=1	۰,۸۶۵۶۹۷	موفقیت آمیز
	X=2	۰,۸۶۵۶۹۷	موفقیت آمیز
	X=3	۰,۷۲۷۳۴۶	موفقیت آمیز
	X=4	۰,۴۲۵۸۱۷	موفقیت آمیز
Random excursions variant (state x)	X=-9	۰,۶۵۰۱۳۲	موفقیت آمیز
	X=-8	۰,۸۶۵۶۹۷	موفقیت آمیز
	X=-7	۰,۳۰۲۲۹۱	موفقیت آمیز
	X=-6	۰,۹۴۷۵۵۷	موفقیت آمیز
	X=-5	۰,۰۹۴۴۲۷	موفقیت آمیز
	X=-4	۰,۴۹۶۸۴۱	موفقیت آمیز
	X=-3	۰,۲۳۵۲۸۵	موفقیت آمیز
	X=-2	۰,۶۲۴۱۰۷	موفقیت آمیز
	X=-1	۰,۲۳۵۲۸۵	موفقیت آمیز
	X=1	۰,۳۴۰۴۶۱	موفقیت آمیز
	X=2	۰,۶۷۶۰۹۷	موفقیت آمیز
	X=3	۰,۷۲۷۳۴۶	موفقیت آمیز
	X=4	۰,۹۴۷۵۵۷	موفقیت آمیز
	X=5	۰,۷۵۲۳۶۱	موفقیت آمیز
	X=6	۰,۳۴۰۴۶۱	موفقیت آمیز
	X=7	۰,۷۰۱۸۷۹	موفقیت آمیز
	X=8	۰,۴۷۲۵۸۴	موفقیت آمیز
	X=9	۰,۱۵۷۰۳۱	موفقیت آمیز

* چنانچه در متن اشاره شده است مقادیر نتایج بالاتر از ۰/۰۱ بر موفقیت آمیز بودن آزمون دلالت دارد.

مرجع‌ها

[1] J. C. Yen and J. I. Guo, "A new chaotic Key-based design for image encryption and decryption," Proceedings of the IEEE International Conference on Circuits and Systems, Vol. 4, pp. 49-52, 2000.

[2] M. Mohsen, G. Zied, Z. Medien, and T. Rached, "Design of reconfigurable image encryption processor using 2-D cellular automata generator," Journal of International Journal of Computer Science and Applications, Vol. 6, No, 4, pp. 43-62, 2009.

[3] C. H. Yuen and K. W. Wong, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1," Journal of Applied Soft Computing, Vol. 11, pp. 5092-5098, 2011.

[4] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Journal of Chaos, Solitons & Fractals, Vol. 21, Issue 3, pp. 749-761, 2004.

[5] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," Journal of Signal Processing, Vol. 90, pp. 2714-2722, 2010.

[6] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," Journal of Optics Communications, Vol. 283, pp. 3259–3266, 2010.

[7] R. Matthews, "On the derivation of chaotic image encryption algorithm," Cryptologia, Vol. 13, No.1, pp. 29-42, 1989.

[8] A. Akhshani, A. Akhavan, S.-C. Lim, Z. Hassan, "An image encryption scheme based on quantum logistic map," Communications in Nonlinear Science and Numerical Simulation, Vol. 17, pp. 4653-4661, 2012.

[9] M.E Goggin, B. Sundaram, P.W. Milonni, "Quantum logistic map," Physical Review A (Atomic, Molecular, and Optical Physics), Vol. 41, pp.5705-5708, 1990.

[10] Y.Wang, K.W. Wong, X.Liao, G. Chen,"A new chaos-based fast image encryption algorithm," Applied Soft Computing, Vol. 11, pp. 514-522, 2011.

[11] S. Mazloom, A. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos, Solitons and Fractals Vol. 42, pp. 1745-1754, 2009.

[12] S. M. Seyedzadeh, S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, "Signal Processing, Vol. 92, pp. 1202-1215, 2012.

[13] Http://csrc.nist.gov/rng.html.

[14] L. Zhang, X. Liao, X. Wang, "An image encryption approach based on chaotic maps, Chaos," Solitons & Fractals, Vol. 24, pp. 759-765, 2005.

[15] K. W. Wong, B. Kwok, W. Law, "A fast image encryption scheme based on chaotic standard map," Phys. Lett. A, vol. 372, pp. 2645-2652, 2008.

[16] A. Ahmed, Abd El-Latif, Li Li, N. Wang, Qi Han, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces " , Signal Processing, 93, pp.2986–3000, 2013.

[17] H. S. Kwok and W. K. S. Tang, "A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation," Journal of Chaos, Solitons & Fractals, Vol. 32, pp. 1518-1529, 2007.

[18] A. Akhshani, A. Akhavan, S. Behnia "An image encryption approach using quantum chaotic map," proc. od the Second Intl. Conf. on Advances in Computer and Information Technology - ACIT, ISBN: 978-981-07-6261-2doi:10.3850/978-981-07-6261-2-36,2013.

[19] C. E. Shannon, "Communication Theory of Secrecy System," The Bell System Technical Journal, Vol. 28, No. 4, pp. 656-715, 1949.

[20] A. Rukhin, et al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22, 2010. http://www.csrc.nist.gov/groups/ST/toolkit/rng/documentation-software.html.

[21] G. Marsaglia, Diehard, a Battery of Tests for Random Number Generators, 1997, http://www.stat.fsu.edu/pub/diehard/.

[22] J. Walker, ENT Test suite, 1998, http://www.fourmilab.ch/random/.

[23] Announcing the advanced encryption standard (AES), Federal Information Processing Standards Publication 197, 2001.