مجله علمی-پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال دوم، شماره ۲، تابستان ۱۳۹۰ :ص ۱۲۴- ۱۱۱

طرح جدید رمزنگاری تصویر با استفاده از نگاشت‌های آشوبی

عبدالرسول میرقدری*[۱]، علیرضا جلفایی[۲]

۱- استادیار، ۲- کارشناس ارشد، دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین(ع)

(دریافت:۱۳۸۹/۱۰/۱، پذیرش: ۱۳۹۰/۰۶/۱۰)

چکیده

امنیت اطلاعات یکی از مسائل با اهمیت پدافندی در مقابله با حمله مهاجمان به حریم اطلاعات با ارزش سازمان‌ها می‌باشد. یکی از ابزارهای قدرتمند پدافند غیرعامل در راستای تامین امنیت اطلاعات و ارتباطات، علم رمزنگاری می‌باشد. در این مقاله، یک الگوریتم جدید برای رمزنگاری تصویر با استفاده از نگاشت‌های آشوبی بیکر و هنون برای حفاظت از تبادل تصاویر دیجیتال به طریقی کارآمد و امن پیشنهاد می‌دهیم. برای بررسی کارایی این طرح، با استفاده از نرم‌افزار MATLAB آن را پیاده‌سازی نموده و به‌منظور بررسی میزان کارآمدی طرح پیشنهادی، آن را با استفاده از یک‌سری آزمون‌ها و مقایسه‌ها می‌سنجیم. این آزمون‌ها عبارتند از: آزمون بصری، تحلیل فضای کلید، تحلیل هیستوگرام، آنتروپی اطلاعات، سنجش کیفیت رمزنگاری، تحلیل همبستگی، تحلیل تفاضلی و تحلیل حساسیت نسبت به کلید. با توجه به نتایج آزمون‌ها و تحلیل‌های صورت گرفته می‌توان نتیجه گرفت که طرح پیشنهادی برای رمزنگاری تصویر، کارآمد می‌باشد.

کلیدواژه‌ها: نظریه آشوب، نگاشت بیکر، نگاشت هنون، امنیت، کارآمدی

A Novel Image Encryption Scheme Using Chaotic Maps

A. Mirghadri,[1*] A. Jolfaei [2]
Faculty and Research Center of Communication and Information Technology, Imam Hossein University
(Received: 12/22/2010, Accepted: 09/01/2011)

Abstract

Information security is one of the most important defensive issues that prevents the intruders' attacks to the privacy of organizations valuable data. Cryptology is one of the most powerful tools of Passive defence that assures the security of communication and information technology. In this paper, we propose a new image encryption scheme using chaotic maps to protect the distribution of digital images in an efficient and secure way. The new encryption scheme is implemented using MATLAB to check its efficiency. Moreover, a series of tests and some comparisons have been performed to justify efficiency of image encryption method. These tests included key space analysis, psychophysical experiments, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis and key sensitivity analysis. Simulation experiment has validated the effectiveness of the proposed system.

Keywords: Chaos Theory, Baker's Map, Henon Map, Security, Efficiency

*Corresponding author E-mail: Amrghdri@ihu.ac.ir

۱. مقدمه

با نگاهی به تاریخ، از زمان ایران و یونان باستان تا دوره نقاشی‌های داوینچی[1]، همواره تلاش انسان در جهت پنهان نمودن اطلاعات بصری مشهود بوده است[۱]. شاید نخستین تلاش بشر برای رمزنگاری تصویر را بتوان در نقاشی تصویر پادشاه فردریک سوم[2] و همسرش مشاهده کرد که با استفاده از یک سیلندر شیشه‌ای در مرکز نقاشی، رمزگشایی می‌شود.

امنیت یکی از ارکان حیاتی موجودات زنده و احساس امنیت یکی از اساسی‌ترین نیازهای نوع بشر است. امروزه با گسترش وسایل ارتباطی و حجم اطلاعات مبادله شده در شبکه‌های رایانه‌ای که از آن به‌عنوان انفجار اطلاعات یاد شده است، بر لبه یک انقلاب بزرگ در زمینه امنیت اطلاعات چندرسانه‌ای قرار گرفته‌ایم. توسعه و پیشرفت‌های صنعت مخابرات چندرسانه‌ای، مفهوم مخابرات تصویری را متحول ساخته است. امنیت رسانه‌های دیجیتال یکی از مسائل مهم و مطرح جامعه رمزنگاری در دنیای امروز می‌باشد. با توجه به کاربرد روزافزون رایانه و گسترش زیر ساخت‌های ارتباطی از جمله شبکه‌های سیار و اینترنت، حفظ محرمانگی و تایید صحت تصاویر روز به روز اهمیت بیشتری می‌یابد.

امروزه به خوبی دریافته‌اند که بیشتر زیر ساخت‌های ارتباطی از نوع شبکه‌های عمومی، برای انتقال مستقیم داده‌های محرمانه مناسب نیستند. بدین‌سبب، اخیراً تلاش‌هایی در راستای حفظ محرمانگی داده‌های چندرسانه‌ای در زیرساخت‌های مخابراتی از جمله شبکه‌های بی‌سیم و اینترنت صورت گرفته است.

تصاویر ممکن است کاربردهای تجاری، نظامی یا حتی پزشکی داشته باشند که برای حفظ امنیت آنها و جلوگیری از دسترسی‌های غیرمجاز به این تصاویر، رمزنگاری آنها قبل از ارسال روی شبکه ضروری می‌باشد. روش‌های متنوعی برای حفظ محرمانگی تصویر و جلوگیری از دسترسی غیر مجاز به محتوای تصویر وجود دارد. یک روش کارآمد برای حفظ محرمانگی داده‌های چندرسانه‌ای، رمزنگاری می‌باشد. به این ترتیب، فقط عوامل مجاز در صورت داشتن کلید صحیح قادر به رمزگشایی آنها می‌باشند.

به‌طور کلی امنیت داده‌های چندرسانه‌ای نسبت به امنیت داده‌های متنی متمایز است، بدین علت که به‌طور معمول محتویات داده‌های چندرسانه‌ای از نظر حافظه حجیم هستند و مجموعه عملیاتی که در آنها به کار می‌روند، از نوع تعاملی[3] می‌باشند که نیازمند پاسخ‌های بلادرنگ هستند.

تصویر، یک داده حجیم دوبعدی است که کوچکترین واحد آن یک پیکسل است. هر پیکسل از یک تصویر دیجیتال، معرف میزان روشنایی آن نقطه از تصویر است. با توجه به حساسیت چشم انسان در تشخیص سطوح روشنایی[4] از یکدیگر، کل محدوده روشنایی قابل نمایش به ۲۵۶ سطح تقسیم‌بندی می‌شود. بنابراین سطح روشنایی هر پیکسل می‌تواند مقداری بین ۰ تا ۲۵۵ داشته باشد. این محدوده توسط یک بایت (۸ بیت) قابل بازنمایی است.

بنابراین، هر پیکسل ۱ بایت، معادل ۸ بیت، می‌باشد. به طور مثال یک تصویر خاکستری با ابعاد ۲۵۶×۲۵۶ پیکسل تقریباً معادل ۶۵ کیلوبایت است. پس یک تصویر با ابعاد کوچک، حجم اطلاعاتی بزرگی دارد. بنابراین با توجه به ویژگی‌های ذاتی داده‌های چندرسانه‌ای، وجود محدودیت در توان محاسباتی پردازنده، پهنای باند شبکه انتقال داده و زمان محاسباتی، بایستی از طرح‌های رمزنگاری کارآمد متناسب با شرایط ذکرشده استفاده کرد.

برای غلبه بر مشکلات رمزنگاری تصویر، پژوهشگران تلاش کرده‌اند تا با استفاده از برخی از نظریه‌های غیرخطی طرح‌های رمزنگاری خاصی برای داده‌های چندرسانه‌ای ابداع کنند[۵-۲]. پژوهشگران در طی پژوهش‌های به‌عمل آمده، ثابت کردند که برخی از طرح‌های جدید از نقطه نظر علم رمزنگاری امن نمی‌باشند[۶]. لذا یکسری پیشنهادها و قوانین مطرح شد تا طراحی سامانه‌های[5] رمزنگاری امن‌تر تسهیل شود[۷].

در این مقاله یک طرح جدید رمزنگاری تصویر با استفاده از نگاشت‌های آشوبی هنون و بیکر ارائه می‌شود که در ادامه به شرح آن می‌پردازیم.

۲. رمزنگاری و نظریه آشوب

مفهوم آشوب یکی از مفاهیم جدید و بنیادی علم نوین است که افق درک ما نسبت به هستی را بسیار گسترش می‌دهد. آشوب، همان‌طور که از نامش پیداست، رفتاری به ظاهر تصادفی و بی‌نظم است که در بسیاری از پدیده‌های دنیای واقعی رخ می‌دهد. پدیده‌های معروفی چون اثر پروانه‌ای[6] از ویژگی‌های خاص آشوب است.

از دهه ۱۹۹۰ تا کنون، سامانه‌های دینامیک آشوبی به‌صورت گسترده در طراحی استراتژی‌های جدید برای رمزنگاری اطلاعات استفاده شده‌اند. در حقیقت، وابستگی به شرایط اولیه و پارامترهای کنترل همگام با ارگادیک[7] بودن نمو آنها، اجازه استفاده از آشوب به عنوان پایه سامانه‌های رمزنگاری جدید (طرح‌های جدید ایجاد اغتشاش و انتشار در تصویر) را می‌دهد. با این وجود، جهت طراحی بهینه یک سامانه رمزنگاری، نه تنها نیازمند درک جامع از علم رمزنگاری می‌باشیم، بلکه بایستی درک کاملی از دینامیک و ساختار درون سامانه‌های آشوبگون داشته باشیم.

[1] Davinci
[2] King Frederik III
[3] Interactive
[4] Level of Intensity (Gray Scale)
[5] System
[6] Butterfly Effect
[7] Ergodic

بنابراین جهت ارائه هرگونه پیشنهادی برای استفاده از نظریه آشوب در مفهوم رمزنگاری بایستی از یکسری قواعد طراحی تبعیت کنیم تا از طراحی دینامیک‌های سامانه‌های غیر آشوب‌ساز اجتناب شود و همچنین از کاربرد بهینه خواص آشوب اطمینان حاصل گردد.

نخستین بار شانون در مقاله[۸] ایده استفاده از آشوب را در رمزنگاری مطرح کرد. شانون هیچ‌گاه به‌طور مستقیم از واژه آشوب استفاده نکرد، ولی بیان کرد که می‌توان تبدیل‌های مخلوط‌کننده خوب موجود در سامانه‌های امن را بر اساس عملیات انبساطی و انقباضی[۱] ساخت. این‌گونه تبدیل‌های مخلوط کننده خوب را می‌توان به‌صورت نگاشت‌های آشوبی در نظر گرفت که در فضای فاز محدودند و نمای لیاپانوف مثبت[۲] دارند.

در مقاله[۹]، پیسارچیک[۳] و همکارانش پیشنهاد کردند که پیکسل‌های تصویر با استفاده از نگاشت‌های آشوبی به صورت یک‌سویه نگاشت شوند تا یک شبکه نگاشت آشوبی[۴] (CML) تشکیل دهند. تصویر رمز شده از طریق تکرار CML همراه با پارامترهای محرمانه سامانه و تعداد دور به‌دست می‌آید. در مقاله[۱۰]، پریک[۵] و همکارانش یک روش رمزنگاری تصویر با استفاده از دو نگاشت لجستیک[۶] و یک کلید خارجی ارائه دادند[۱۰].

کوک[۷] و همکارانش، یک سامانه رمزنگاری تصویر مبتنی بر آشوب سریع با معماری رمز جریانی پیشنهاد کردند[۱۱]. در طرح آنها پیکسل‌های تصویر اصلی[۸] با استفاده از یک دنباله کلید شبه تصادفی تولید شده از یک نگاشت مثلثی[۹] اریب[۱۰] و یک نگاشت ACM[۱۱] چند بعدی پوشانده می‌شود.

در مقاله[۱۲]، فردریچ[۱۲] پیشنهاد کرد که یک طرح رمزنگاری تصویر بایستی شامل دو مرحله تکرار شونده باشد : انتشار[۱۳] و اغتشاش[۱۴]. این بدین صورت حاصل می‌شود که تمام پیکسل‌های تصویر به صورت کلی با استفاده از یک نگاشت آشوبی دوبعدی یا سه‌بعدی جایگشت یابند. پیکسل انتقال یافته به مکان جدید در واقع یک جانشان از پیکسل اولیه می‌باشد. در مرحله انتشار، مقادیر پیکسل‌ها به‌صورت جریانی تغییر می‌کنند، تغییر اعمال شده به یک پیکسل به‌خصوص به جمع آثار تمامی پیکسل‌های قبل وابسته است.

این معماری اساس یکسری از سامانه‌های رمزنگاری مبتنی بر آشوب چندبعدی را تشکیل می‌دهد. به طور مثال چن و همکارانش در مرحله جانشانی از یک ACM سه‌بعدی و یک نگاشت بیکر سه‌بعدی استفاده کردند[۱۳]. گوان[۱۵] و همکارانش از یک نگاشت آشوبی دوبعدی برای جایگشت مکان پیکسل‌ها و از سامانه آشوبی گسسته چن، برای پنهان کردن مقادیر پیکسل‌ها استفاده کردند[۱۴].

لیان[۱۶] و همکارانش از یک نگاشت استاندارد[۱۷] دو بعدی در فاز جانشانی و از یک نگاشت لجستیک در فاز انتشار استفاده کردند[۱۵]. پارامترها و مقادیر اولیه این دو نگاشت آشوبی به وسیله دنباله کلید تولیدی در هر دور مشخص می‌شود. معماری چنین سامانه‌های رمزنگاری بدین صورت است که شامل یک تعداد دور جانشانی و انتشار می‌باشند.

۳. روش تحقیق

در این بخش، در ابتدا عناصر سازنده الگوریتم پیشنهادی تشریح و سپس الگوریتم پیشنهادی برای رمزنگاری تصویر معرفی می‌شود. این الگوریتم از نوع متقارن می‌باشد که در ادامه به شرح آنها می‌پردازیم.

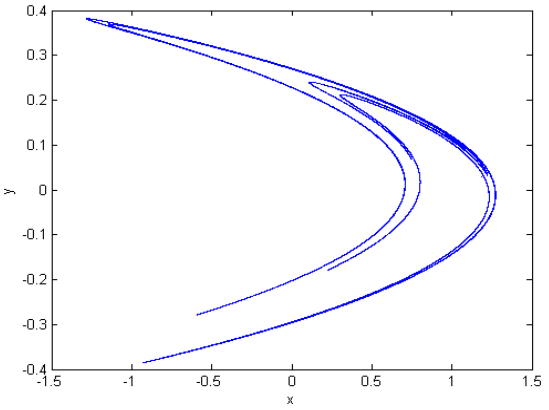
۳-۱. نگاشت هنون

نگاشت هنون یک نگاشت آشوبی دوبعدی معکوس‌پذیر می‌باشد که در سال ۱۹۷۶ توسط هنون معرفی شده است[۱۶]. این نگاشت یک نمونه ساده شده نگاشت پوانکاره برای معادلات لورنز[۱۸] می‌باشد. نگاشت آشوبی هنون به‌عنوان روشی برای تولید دنباله‌های شبه تصادفی معرفی شده است[۱۷]. نگاشت دوبعدی هنون به‌صورت زیر تعریف می‌شود:

$$\begin{cases} x_{n+1} = 1 + y_n - \alpha x_n^2 \\ y_{n+1} = \beta x_n , \end{cases} \qquad (1)$$

به این صورت که (x_0, y_0) نقطه شروع و زوج (x, y) یک حالت دوبعدی سامانه می‌باشد. هنگامی که $\alpha = 1/4$ و $\beta = 0/3$ باشد، سامانه در حالت آشوبی می‌باشد. هنون نشان داد که اگر شرایط اولیه در ناحیه S، که در محدوده‌های (۰/۴۲، ۱/۳۳-)، (۰/۱۳۳، ۱/۳۲)، (۰/۱۴-، ۱/۲۴۵) و (۰/۵-، ۱/۰۶-) تعریف شده است، انتخاب شود آنگاه نقاط حاصل از تکرار نگاشت، یعنی (x_i, y_i) برای $i \le 1$، نیز در محدوده S قرار می‌گیرد[۱۶]. نگاشت هنون، جاذب[۱۹] عجیبی دارد. شکل (۱) دیاگرام فضای حالت این نگاشت را هنگامی که در حالت آشوبی است، نشان می‌دهد. برای هر مقدار (x_i, y_i) در S، دنباله نقاط به این جاذب همگرا می‌شوند و در طول تکرار نگاشت بر روی آن باقی می‌مانند.

[1] Rolled-Out and Folded-Over Operations
[2] Positive Lyapunov Exponent
[3] Pisarchik
[4] Chaotic Map Lattice
[5] Pareek
[6] Logistic Map
[7] Kwok
[8] Plain-Image
[9] Tent
[10] Skewed
[11] Arnold Cat Map (ACM)
[12] Fridrich
[13] Diffusion
[14] Confusion
[15] Guan
[16] Lian
[17] Standard Map
[18] Lorenz
[19] Attractor



شکل۱. دیاگرام فضای حالت نگاشت هنون

۳-۲. نگاشت بیکر

نگاشت آشوبی بیکر یک سامانه دینامیکی گسسته دوبعدی برای تولید آشوب است که سال ۱۹۳۷ توسط ابرهارد هاپف ابداع شد[۱۸و۱۲]. این نگاشت شباهت بسیاری به نگاشت نعل اسب[1] دارد[۱۹]. نگاشت بیکر به صورت زیر تعریف می‌گردد:

$$F:[0,1)\times[0,1)\to[0,1)\times[0,1), \quad (۲)$$

$$F(x,y)=(\sigma(x),g(a,x,y)), \quad (۳)$$

$$\sigma(x)=2x \mod 1,\ 0\le\sigma(x)<1, \quad (۴)$$

$$g(a,x,y)=\left\{\begin{matrix}\frac{1}{2}ay, & 0\le x<\frac{1}{2}\\ \frac{1}{2}(ay+1), & \frac{1}{2}\le x<1\end{matrix}\right\}\mod 1, 0\le g<1 \quad (۵)$$

F(S) در شکل (۲) نمایش داده شده است، به‌طوری که S مربع واحد است. ماهیت هندسی نگاشت به این‌گونه است که ابتدا موجب انبساط افقی و انقباض عمودی سطح می‌شود، سپس سطح را یک برش عمودی می‌دهد و دو تکه سطح را بر روی هم می‌گذارد.

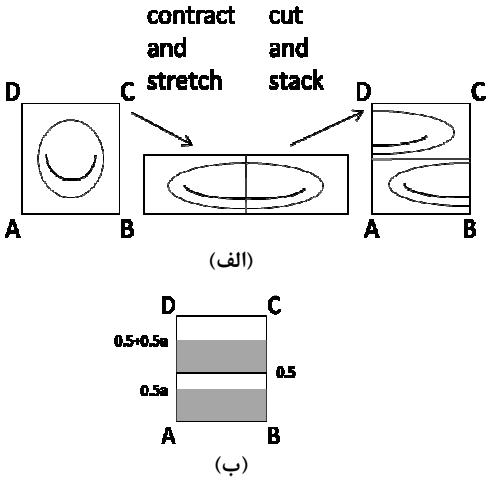
این عمل مشابه تهیه خمیر نان می‌باشد. به همین علت، این نگاشت را نگاشت نانوا می‌گویند (بیکر در زبان انگلیسی به معنای نانوا می‌باشد).

۳-۳. الگوریتم پیشنهادی

جایگشت پیکسلی، جانشانی و xor کردن با یک کلید از ساده‌ترین شکل‌های رمزنگاری است که می‌توان برای رمزنگاری تصویر استفاده کرد. در واقع این سامانه رمزنگاری نوعی درهم‌ریزی[2] می‌باشد.

اگرچه هیچ تعریف مشخصی از درهم‌ریزی وجود ندارد، اما در واقع ساده‌ترین نوع تلاش ممکن برای رمزنگاری می‌باشد که شامل یک جانشانی ساده یا یک ترانهش[3] رمزی ساده می‌باشد که امروزه از نظر امنیتی در پایین‌ترین سطح ممکن قرار دارد.

[1] Horseshoe Map
[2] Scrambling
[3] Transposition



شکل۲. نگاشت بیکر: (الف) ماهیت هندسی نگاشت بیکر، (ب) انقباض ناحیه تحت نگاشت F

درهم‌ریزی پیکسلی دو پیامد مهم دارد که برای رمزنگاری تصویر مناسب است. درهم‌ریزی نه‌تنها مکان پیکسل‌ها را جابه‌جا می‌کند (انتشار)، بلکه مقدار هر پیکسل را نیز تغییر می‌دهد (اغتشاش).

عملیات جایگشت و جانشانی هر دو از مبانی رمزنگاری هستند که تاریخچه آن‌ها به مقاله‌های نخستین ریتر[4] بازمی‌گردد[۲۱و۲۰]. روش‌های ریتر شبیه به پیشنهادهای وُنگ[5] می‌باشد[۲۲]. همچنین در سال ۱۹۷۵، فیستل[6] و همکارانش یک شبکه جانشانی-جایگشتی[7] (SPN) معرفی کردند که در واقع پیاده‌سازی کارآمد و ساده اصول شانون مبتنی بر اغتشاش و انتشار می‌باشد[۲۳].

در سامانه رمزنگاری پیشنهادی، پیکسل‌ها نخست با استفاده از یک ماتریس جانشانی مبتنی بر نگاشت هنون تعویض می‌شوند. سپس، مکان پیکسل‌ها با استفاده از یک واحد جابه‌جا کننده[8] مبتنی بر نگاشت بیکر جابه‌جا می‌شود. در نهایت تصویر نهایی با یک کلید دوری مبتنی بر نگاشت بیکر xor می‌شود.

برای انتشار تغییر صورت گرفته در مقدار پیکسل‌ها در کل تصویر، جابه‌جا کردن مکان پیکسل‌ها بعد از عمل جانشانی مناسب است. برخلاف داده متنی که تنها دو همسایگی دارد، هر پیکسل در تصویر در مجاورت با ۸ پیکسل همسایه است. بنابراین هر پیکسل همبستگی بالایی با پیکسل‌های همسایه خود دارد.

ماتریس جانشانی با استفاده از نگاشت هنون، هم‌اندازه تصویر اصلی به شرح الگوریتم (۱) تولید می‌شود.

[4] Ritter
[5] Wong
[6] Feistel
[7] Substitution Permutation Network (SPN)
[8] Shuffler Unit

الگوریتم ۱. تولید ماتریس جانشانی آشوبی

```
NoIt = number of iterations that is 256
For it1 = 1 to NoIt do
        [x_n, y_n] = Vector generated according
          to a recursive Henon map
        V(it) = x_n+iy_n
        SUB(it) = Euclidean distance of V
End For
For it1 = 1 to NoIt do
        Max = Maximum of vector SUB
        For it2 = 1 to NoIt do
                If SUB(it2) is equal to MAX
        then SUB(it2) = −256+ it1
        End For
End For
Chaotic substitution = Absolute
                value of SUB.
```

این بدان معنی است که می‌توان مقدار هر پیکسل را با استفاده از مقادیر همسایه‌هایش حدس زد[۲۴]. با این وجود، از بین بردن همبستگی بالای بین پیکسل‌های تصویر برای افزایش سطح امنیت تصویر رمز، امری مهم است. بنابراین از یک نگاشت بیکر دوبعدی برای ساخت ماتریس جایگشت آشوبی استفاده می‌گردد.

ماتریس جایگشت همان ماتریس همانی است که جای سطرها یا ستون‌های آن عوض شده است. درایه‌های ماتریس جایگشت فقط شامل ۰ و ۱ می‌باشد به‌گونه‌ای که در هر سطر و هر ستون فقط یک درایه با مقدار ۱ وجود دارد. ویژگی مهم ماتریس جایگشت این است که معکوس آن با ترانهاده‌اش برابر است.

بنابراین برای محاسبه ماتریس معکوس جهت رمزگشایی، نیاز به محاسبات اضافی نمی‌باشد. واحد جابه‌جا کننده شامل یک نگاشت جایگشتی آشوبی است که در سه جهت عمودی، افقی و قطری برای کاهش همبستگی بین پیکسل‌های همسایه اعمال می‌شود. الگوریتم تولید ماتریس جایگشت آشوبی به شرح الگوریتم (۲) است.

با استفاده از ماتریس Pmap، تصویر ورودی در جهت‌های عمودی، افقی و قطری جایگشت می‌یابد. جایگشت عمودی و افقی به شرح الگوریتم (۳) می‌باشد.

روند جایگشت قطری یک مقدار پیچیده‌تر است که به‌صورت الگوریتم (۴) تعریف می‌شود.

سپس تصویر جابه‌جا شده با یک کلید دوری xor می‌شود. ماتریس کلید دوری هم‌اندازه تصویر اصلی است که اعضای آرایه‌ای آن با استفاده از نگاشت بیکر تولید می‌شوند. xor کردن با کلید دوری نقش مهمی در توزیع یکنواخت تصویر رمز دارد. الگوریتم تولید ماتریس کلید دوری به شرح الگوریتم (۵) است.

الگوریتم ۲.تولید ماتریس جایگشت آشوبی

```
NoIt =  number of iterations that is number of
plain-image rows
For it = 1 to NoIt do
        [x_n, y_n] = Vector generated according
          to a recursive baker's map
        V(it) = x_n+iy_n
        D(it) = Euclidean distance of V
End For
Pmap = Permutation map that is generated
from D. Pmap elements ∈ {0, 1}.
```

الگوریتم ۳. جایگشت عمودی و افقی مکان پیکسل‌ها

```
P = Plain-image
For it = 1 to NoIt do
        Vertical permutation = Multiplying the
it-th column of plain-image by Pmap     4:
Horizontal permutation = Multiplying
the it-th row of plain-image by Pmap
End For
```

الگوریتم ۴. جایگشت قطری مکان پیکسل‌ها

```
For it = 2 to NoIt do
        Shiftsize = The shift amount for the it-th
row of plain-image, that is (NoIt-it+1).
        C = Circularly right shifted values in
each row of plain-image, by
shiftsize elements.
        VC= Vertical permutation in C.
        Diagonally permuted image = circularly
left shifted values in each row of VC,
by (-shiftsize) elements.
End For
```

الگوریتم ۵. تولید ماتریس کلید دوری

```
NoIt = Number of iterations that is number of
  plain-image pixels
For it = 1 to NoItdo
        [x_n, y_n] = Vector generated according
          to a recursive baker's map
        V(it) = x_n+iy_n
        D(it) = Euclidean distance of V
End For
RK = Matrix containing D with
          floored elements, the same
          size as original image.
```

خلاصه الگوریتم پیشنهادی به شرح زیر است:

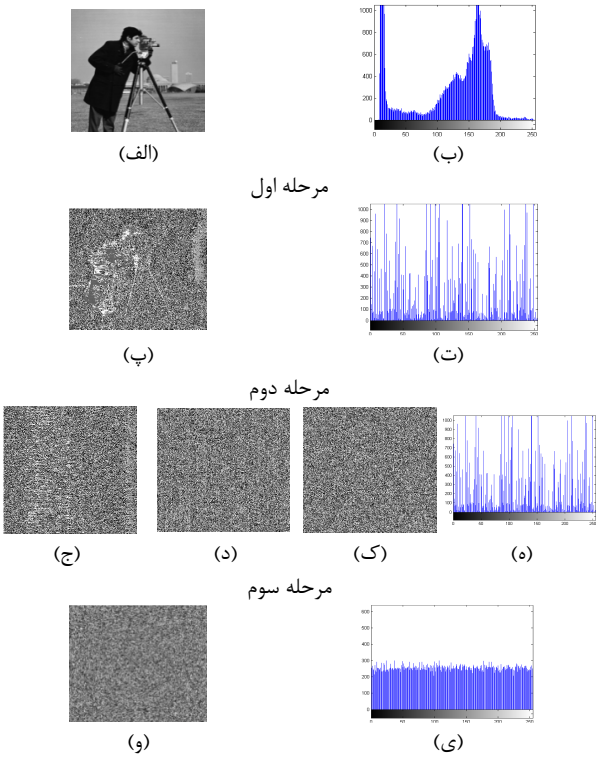
$$SPK^{r}(P) = (Shuffle(Substitute(P)) \oplus RoundKey)^{r} \quad (۶)$$

که P تصویر اصلی و r تعداد دور تکرار الگوریتم می‌باشد. شکل (۴) بلوک دیاگرام الگوریتم پیشنهادی را نشان می‌دهد. آخرین نقطه خروجی

هر نگاشت در هر دور به عنوان بذر اولیه همان نگاشت در دور بعدی استفاده می‌شود. با افزایش r، پیچیدگی طرح افزایش می‌یابد، در حالی‌که از سرعت رمزنگاری کاسته و حجم حافظه بیشتری استفاده می‌شود. این الگوریتم مستقل از ساختار تصویر اصلی می‌باشد و می‌تواند برای رمز کردن هر آرایه بایتی دوبعدی استفاده شود.

شکل(۳)، جانشانی آشوبی با استفاده از ماتریس جانشانی ساخته شده از نگاشت هنون، جابه‌جایی آشوبی در سه جهت با استفاده از ماتریس جایگشت ساخته شده از نگاشت بیکر و xor کردن با کلید دوری را با استفاده از سه جفت بذر[1] اولیه نشان می‌دهد.

همان‌گونه که دیده می‌شود بعد از عمل جانشانی، بافت تصویر قابل تشخیص است. بعد از اعمال جابه‌جا کننده، تغییری در هیستوگرام تصویر ایجاد نشده و فقط همبستگی بین پیکسل‌های تصویر کاهش می‌یابد. در نهایت بعد از xor کردن تصویر با ماتریس کلید دوری، هیستوگرام تصویر رمز یکنواخت می‌شود.



شکل ۳. پیاده‌سازی الگوریتم پیشنهادی با استفاده از تصویر استاندارد مرد عکاس با اندازه ۲۵۶×۲۵۶:
(الف) تصویر اصلی، (ب) هیستوگرام تصویر اصلی، (پ) جانشانی، (ت) هیستوگرام تصویر جانشانی شده، (ج) جایگشت افقی، (د) جایگشت افقی و عمودی، (ک) جایگشت افقی، عمودی و قطری، (ه) هیستوگرام تصویر جابه‌جا شده، (و) تصویر رمز، (ی) هیستوگرام تصویر رمز

[1] Seed Point

۴. تحلیل و ارزیابی الگوریتم پیشنهادی

یک طرح رمزنگاری مناسب بایستی نسبت به کلیه حملات شناخته شده مانند حمله متن اصلی معلوم، حمله متن رمز معلوم[2]، حملات آماری[3]، حملات تفاضلی[4] و انواع حملات جستجوی جامع[5] مصون باشد. جهت ارزیابی و تحلیل امنیتی یک طرح رمزنگاری تصویر، تعدادی آزمون و روش ارزیابی استاندارد وجود دارد که در این بخش به تفضیل به تشریح آنها می‌پردازیم[۲۸و ۲۵].

برای شبیه‌سازی و ارزیابی الگوریتم پیشنهادی، بایستی از یک‌سری تصویر اصلی استاندارد که در دسترس همگان است، استفاده شود. بدین‌علت که ارزیابی‌های صورت گرفته قابل سنجش و تحقیق توسط محققین دیگر نیز باشد. به این منظور، شبیه‌سازی‌ها و ارزیابی‌ها با استفاده از تعدادی تصویر اصلی واقع در پایگاه داده تصویری دانشگاه تگزاس[۲۶] و USC-SIPI [۲۷] انجام شد. برای شبیه‌سازی از تعدادی کلید خصوصی متفاوت استفاده شد که در جدول(۱) لیست شده است.

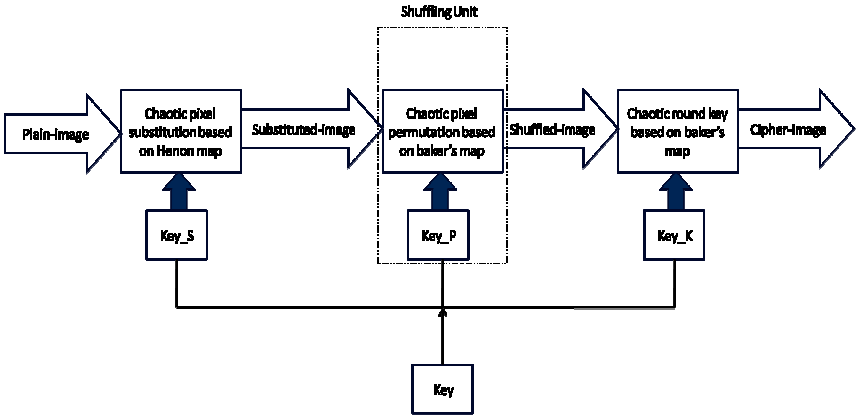
جدول ۱. لیست کلیدهای خصوصی

مجموعه کلیدهای کمی متفاوت						مجموعه کلیدهای اصلی					
Substitution		Shuffling		Round Key		Substitution		Shuffling		Round Key	
x_1	y_1	x_2	y_2	x_3	y_3	x_1	y_1	x_2	y_2	x_3	y_3
0.41	0.1	0.1	0.8	0.5	0.4	0.4	0.1	0.1	0.8	0.5	0.4

۴-۱. تحلیل فضای کلید

بدیهی است که جهت جلوگیری از حمله جستجوی جامع، فضای کلید الگوریتم رمزنگاری بایستی به‌اندازه کافی بزرگ باشد. اندازه فضای کلید، تعداد کل کلیدهای مختلفی است که می‌توان در الگوریتم رمزنگاری استفاده کرد. در واقع قدرت اجرای یک حمله جستجوی جامع وابسته به اندازه فضای کلید می‌باشد. اگر برای مهاجم، آزمون کردن کلیه کلیدهای ممکن با استفاده از کامپیوترهای مدرن بسیار زمان‌بر باشد، به طور مثال چندین دهه، آنگاه می‌گوییم که الگوریتم رمزنگاری نسبت به حمله جستجوی جامع از نظر محاسباتی امن می‌باشد. سازمان NIST[6] حداقل طول کلید ممکن برای برقراری امنیت محاسباتی در برابر حملات جستجوی جامع را تا سال ۲۰۱۵، ۸۰ بیت پیش‌بینی کرده است[۲۹]. الگوریتم پیشنهادی با استفاده از سه زوج بذر اولیه، سه نگاشت آشوبی را تغذیه می‌کند. اگر دقت محاسبات را 10^{-14} در نظر بگیریم، آنگاه فضای کلید سامانه برابر است با $10^{14\times6} \simeq 2^{279}$. بنابراین طرح نسبت به حمله جستجوی جامع مصون می‌باشد.

[2] Known Plaintext Attack
[3] Statistical Attack
[4] Differential Attack
[5] Brute-Force Attack
[6] National Institute of Standards and Technology (NIST)



شکل ۴. بلوک دیاگرام الگوریتم پیشنهادی

۴-۲. آزمون بصری و تحلیل هیستوگرام

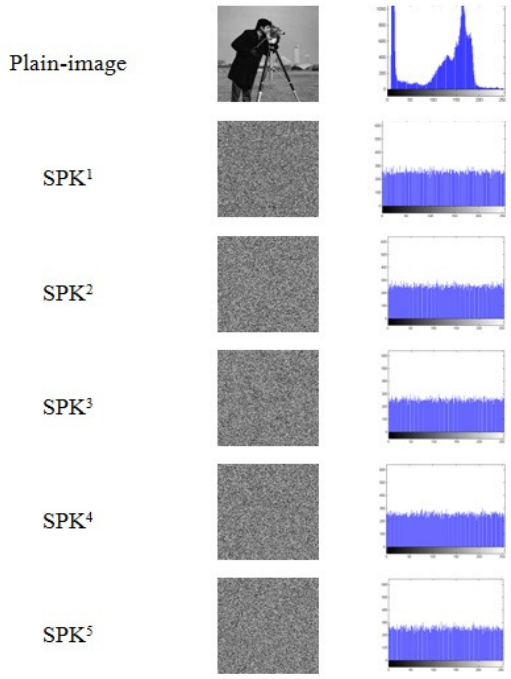
یک روش آزمایش تصویر رمز مشاهده می‌باشد. یک الگوریتم رمزنگاری خوب، بایستی تصویر را به‌گونه‌ای درهم ریزد که ویژگی‌های آن به صورت بصری قابل تشخیص نباشد. همچنین با مقایسه تصویر رمز با تصویر اصلی نبایستی هیچ نوع اطلاعاتی در تصویر رمز مشاهده گردد و حتی با تغییرات شدید در شدت روشنایی پیکسل‌های تصویر اصلی، بایستی تصویر اصلی و تصویر رمز، به صورت بصری متمایز باشند. البته شایان ذکر است، از آنجا که نتیجه آزمون بصری برای بینندگان متفاوت، مختلف می‌باشد، نمی‌توان اعتبار علمی برای آن قائل شد. لذا از تحلیل هیستوگرام استفاده می‌کنیم.

برای جلوگیری از نشت اطلاعات و جلوگیری از حملات مهاجم، مهم است که تضمین شود که تصویر اصلی و تصویر رمز هیچ‌گونه تشابه آماری ندارند. تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از ترسیم تعداد مشاهدات هر میزان شدت روشنایی، بیان می‌کند. الگوریتم رمزنگاری تصویر بایستی به‌گونه‌ای باشد که هیچ نوع سرنخی برای حمله آماری ندهد. توزیع به نسبت یکنواخت هیستوگرام تصویر، می‌تواند نشان‌دهنده کیفیت خوب روش رمزنگاری باشد.

الگوریتم‌های مورد مطالعه را با استفاده از تصویر خاکستری استاندارد مرد عکاس با اندازه ۲۵۶×۲۵۶ آزمایش کردیم. نتیجه شبیه‌سازی در شکل (۵) نشان داده شده است. با مقایسه نتایج شکل (۵)، مشخص است که از نظر بصری، تصاویر رمز نسبت به تصویر اصلی کاملاً متمایز هستند و به نظر دارای توزیع پیکسلی تصادفی یکنواخت هستند.

۴-۳. تحلیل تصادفی بودن

جهت اطمینان از امنیت یک سامانه رمزنگاری تصویر، دنباله کلید اجرایی بایستی برخی خواص احتمالی مناسب ازجمله توزیع خوب، پریود طولانی، پیچیدگی بالا و کارآمدی را داشته باشد.



شکل ۵. نتایج آزمون بصری و تحلیل هیستوگرام

امروزه، روش‌های آزمون آماری بسیاری جهت ارزیابی تصادفی بودن خروجی سامانه رمزنگاری وجود دارد که هر یک حضور یا عدم حضور یک الگوی مشخص را در خروجی سامانه رمزنگاری تعیین می‌کند و اگر یک الگو یافت شود نتیجه می‌گیریم که دنباله خروجی غیرتصادفی است. اخیراً NIST یک مجموعه از آزمون‌های آماری مختلف جهت ارزیابی تصادفی بودن دنباله باینری تولید شده توسط مولدهای اعداد شبه‌تصادفی سخت‌افزاری یا نرم‌افزاری را ارائه کرده است[۳۰]. این آزمون‌ها انواع الگوهای مختلفی که موجب غیرتصادفی شدن دنباله خروجی می‌شود را تشخیص می‌دهند. چارچوب آزمون‌های NIST

همانند آزمون‌های آماری دیگر، مبتنی بر آزمون فرضیه[1] می‌باشد. آزمون فرضیه روندی است جهت تصمیم‌گیری اینکه آیا یک اعلان درباره خصوصیت یک جمعیت منطقی می‌باشد یا خیر. در آزمون فرضیه ابتدا فرضی را در نظر گرفته و سپس با به‌کارگیری یک شیوه خاص، از روی نمونه‌های مشاهده شده، بر پذیرش یا رد فرض تصمیم‌گیری می‌شود.

فرضی که به‌طور معمول در آزمون فرضیه برای قضاوت در مورد سازگاری نتایج نمونه‌ای با یک تابع احتمال مشخص در نظر گرفته می‌شود، بدین صورت است: نمونه‌های آماری در دسترس منطبق بر تابع احتمال مورد نظر هستند و هرگونه اختلاف مشاهده شده صرفاً به دلیل نوسان‌های نمونه است. این فرض را به نام فرضیه صفر[2] خوانده و به صورت H_0 نمایش می‌دهند. آزمون فرضیه با کمک نمونه‌های متغیر تصادفی، تشخیص می‌دهد که تابع احتمال فرضی برای نمونه‌ها قابل قبول یا مردود می‌باشد.

به طور کلی اگر نتایج نمونه‌ها با فرض سازگار به نظر برسند تمایل به پذیرفتن فرض و اگر ناسازگار باشند، تمایل به رد آن فرض پیدا می‌کنیم. در تمام آزمون‌های NIST، اگر P-مقدار محاسبه شده کوچکتر از ۰/۰۱ باشد، آنگاه نتیجه گرفته می‌شود که دنباله غیر-تصادفی است. در غیر این‌صورت، نتیجه گرفته می‌شود دنباله تصادفی است. توصیف ریاضی مجموعه آزمون‌های آماری NIST تحت نام NIST SP800–22، قبلا انجام شده است[۳۰].

به نظر می‌رسد که آزمون‌های فوق جهت ارزیابی یکنواختی داده‌های تصویری کافی نمی‌باشد. هر کانال یک تصویر دیجیتال، یک ماتریس دوبعدی است که کوچکترین عضو آن یک بایت (پیکسل) می‌باشد نه یک بیت. همچنین در ماتریس تصویر هر پیکسل در همسایگی ۸ پیکسل مجاور است.

بنابراین برخلاف داده متنی که هر عضو آن تنها دو همسایگی دارد، همبستگی بین پیکسل‌های تصویر بسیار زیاد است. علاوه بر تصادفی بودن دنباله بیتی تصویر رمز، به‌صورت بصری نبایستی هیچ نوع الگو یا ناحیه‌ی بافتی مشخصی در تصویر رمز یافت شود. وجود نواحی بافتی همگن در تصویر رمز، یک ضعف امنیتی می‌باشد، به‌طوری که مانع از دست‌یابی تصویر به آنتروپی بیشینه می‌شود. با توجه به اینکه آزمون‌های آماری متنوع برای تشخیص تصادفی بودن یک دنباله بیتی وجود دارد، از جمله NISTSP800–22، DIEHARD، FIPS140–2 و غیره، تا کنون آزمون‌های آماری اندکی برای ارزیابی تصادفی بودن دنباله‌های بایتی دوبعدی ارائه شده است[۳۱ و ۱۱].

در نظریه آمار و احتمالات، توزیع گسسته یکنواخت[3]، یک توزیع احتمالی هم‌شانس می‌باشد که در آن هر n مقدار مشاهده شده دارای احتمال برابر 1/n می‌باشد. یکنواختی حاصل از یک تابع رمزنگاری تصویر را می‌توان به‌صورت کمی با استفاده از آزمون مربع کای پیرسون[4] ارزیابی کرد. توزیع مربع خی، جهت مقایسه زیبندگی[5] فراوانی‌های مشاهده شده در یک نمونه اندازه‌گیری شده با فراوانی‌های مورد انتظار در توزیع فرض شده می‌باشد. آماره این آزمون عبارت است از:

$$\chi^2_{test} = \sum_{k=1}^{256} \frac{(v_k - e_k)^2}{e_k} \qquad (۶)$$

که k تعداد سطح خاکستری (۲۵۶)، v_k تعداد رخدادهای مشاهده‌شده هر سطح خاکستری (۲۵۵-۰) و e_k تعداد رخداد مورد انتظار هر سطح خاکستری می‌باشد. به‌طور مثال، اگر تصویر اصلی دارای ابعاد W×H باشد آنگاه $e_k = \frac{H \times W}{256}$. با فرض میزان بحرانی ۰/۰۱، اگر $\chi^2_{test} < \chi^2$ (255, 0.01)، آنگاه نتیجه گرفته می‌شود که فرضیه صفر رد نمی‌شود و توزیع هیستوگرام تصویر رمز یکنواخت می‌باشد.

شکل (۶) نتایج آزمون NIST SP800–22 با استفاده از تصویر خاکستری استاندارد مرد عکاس با اندازه ۲۵۶×۲۵۶ را نشان می‌دهد. نتایج به‌دست آمده نشان می‌دهند که دنباله تصویری رمز شده توسط الگوریتم مورد مطالعه، هیچ‌گونه نقصی ندارد و تمامی آزمون‌های NIST SP800–22 را با مقادیر بالای P-مقدار[6]، با موفقیت می‌گذراند.

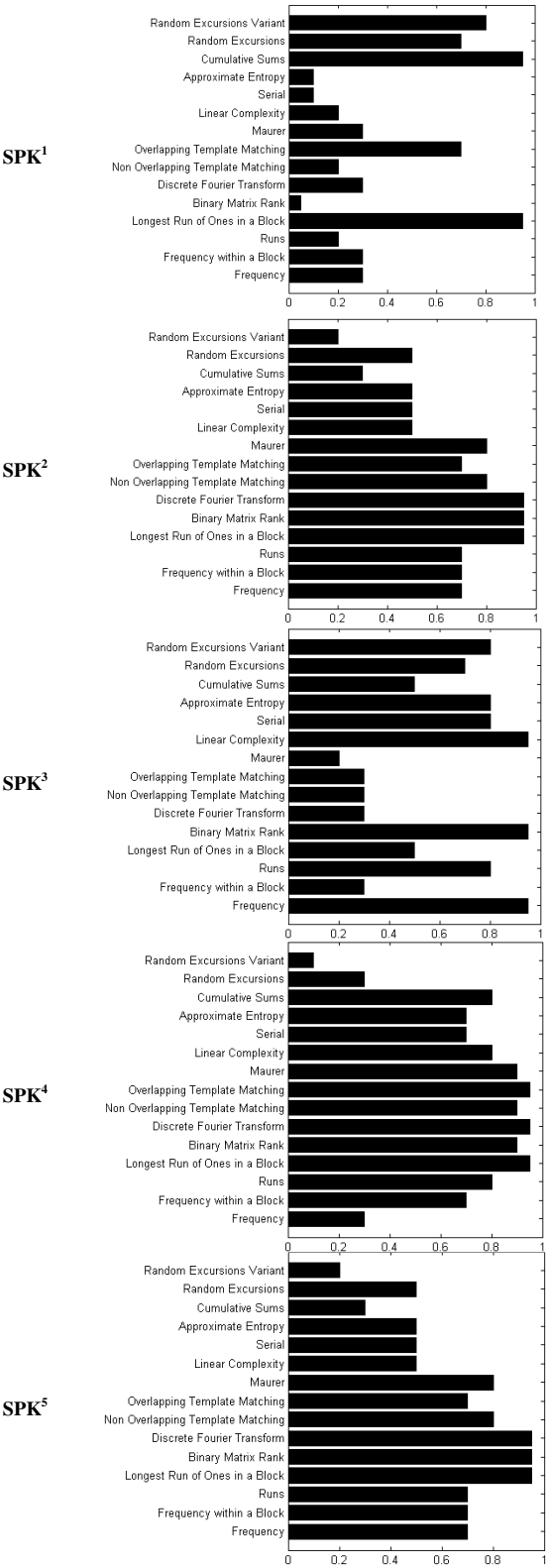
نتایج آزمون مربع خی در جدول (۲) ثبت شده است.

همان‌گونه که مشاهده می‌شود، $\chi^2_{test} < \chi^2$ (255, 0.01)، یعنی فرضیه صفر رد نمی‌شود و توزیع هیستوگرام تصویر رمز یکنواخت می‌باشد.

جدول ۲. نتایج آزمون χ^2

نام تصویر	بابون[7]	ساعت[8]	مرد عکاس	فلفل[9]	تیفانی[10]
اندازه	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶
نوع تصویر	خاکستری	خاکستری	خاکستری	خاکستری	خاکستری
SPK[1]	۲۸۵/۸	۲۸۲/۵	۲۷۰/۵	۲۳۱/۷	۲۴۹/۳
SPK[2]	۲۱۹/۵	۲۳۹/۵	۲۷۲/۱	۲۱۹/۸	۲۴۳/۲
SPK[3]	۲۷۱/۸	۲۵۰/۸	۲۸۳/۸	۲۷۹/۳	۲۶۳/۶
SPK[4]	۲۹۴/۷	۲۵۱/۳	۲۶۵/۱	۲۴۷	۲۶۴
SPK[5]	۲۸۳/۱	۲۴۴/۴	۲۸۶/۲	۲۵۵/۷	۲۲۵/۶

[1] Hypothesis Test
[2] Null Hypothesis
[3] Discrete Uniform Distribution
[4] Pearson's Chi-Square
[5] Goodness of Fit
[6] *P*-Value
[7] Baboon
[8] Clock
[9] Peppers
[10] Tiffany



شکل۶. نتایج آزمون NIST SP800–22 با استفاده از تصویر خاکستری استاندارد مرد عکاس با ابعاد ۲۵۶×۲۵۶

۴-۴. تحلیل آنتروپی

نظریه اطلاعات یک نظریه‌ی ریاضی از مخابرات داده و ذخیره‌سازی می‌باشد که در سال ۱۹۴۹ به‌وسیله شانون معرفی شد[۸]. شانون آنتروپی را به‌عنوان معیاری از میزان اطلاعات در منبع معرفی کرد. مفهوم آنتروپی در ارتباط با میزان بی‌نظمی و عدم قطعیت در یک سامانه فیزیکی می‌باشد. امروزه نظریه اطلاعات مدرن در ارتباط با تصحیح خطا، فشرده‌سازی اطلاعات، رمزنگاری، سامانه‌های مخابراتی و موضوعات مرتبط می‌باشد. آنتروپی یک تصویر، تخمینی از تصادفی بودن آن می‌باشد که به‌طور معمول برای سنجش میزان تیزی قله‌های هیستوگرام می‌باشد که این موضوع مستقیماً در ارتباط با اطلاعات ساختاری با تعریف بهتر می‌باشد. آنتروپی شانون H(s) یک منبع پیام s به صورت زیر تعریف می‌شود:

$$H(s)=\sum_{i=0}^{2^N-1} P(s_i)\log_2\frac{1}{P(s_i)} \qquad (۷)$$

که $P(s_i)$ معرف احتمال سمبل s_i می‌باشد و آنتروپی به صورت بیتی بیان می‌شود. فرض کنید که منبع 2^N سمبل هم‌احتمال تولید کند، یعنی $s=\{s_1,s_2,...,s_{2^N}\}$. بعد از ارزیابی معادله فوق H(s) = N به‌دست می‌آید که متناظر با یک منبع تصادفی حقیقی می‌باشد. به‌طور کلی، یک منبع اطلاعات عملی به‌ندرت پیام‌های تصادفی تولید می‌کند و میزان آنتروپی آن کوچکتر از مقدار ایده‌آل ۸ می‌باشد. با این وجود، هنگامی که پیام‌ها رمز می‌شوند، آنتروپی آنها بایستی نزدیک به مقدار ایده‌آل ۸ باشد.

اگر خروجی یک رمز سمبل‌هایی با آنتروپی کمتر از ۸ ارسال کند، یک میزان معینی از پیش‌بینی‌پذیری پدید می‌آید که امنیت سامانه را تهدید می‌کند.

نتایج تحلیل آنتروپی در جدول (۳) ثبت شده است. نتایج به‌دست آمده بسیار نزدیک به مقدار نظری ۸ هستند. این بدین معنی است که در روند رمزنگاری، نشت اطلاعات بسیار ناچیز است و سامانه‌های تحت مطالعه نسبت به حمله آنتروپی مصون هستند.

جدول ۳. اندازه آنتروپی تصاویر رمز شده تصاویر اصلی متفاوت

نام تصویر	بابون	ساعت	مرد عکاس	فلفل	تیفانی
اندازه	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶
نوع تصویر	خاکستری	خاکستری	خاکستری	خاکستری	خاکستری
SPK^1	۷/۹۹۶۲	۷/۹۹۶۳	۷/۹۹۶۵	۷/۹۹۶۶	۷/۹۹۶۷
SPK^2	۷/۹۹۷۱	۷/۹۹۶۲	۷/۹۹۷۱	۷/۹۹۶۶	۷/۹۹۶۳
SPK^3	۷/۹۹۶۵	۷/۹۹۶۸	۷/۹۹۶۶	۷/۹۹۶۷	۷/۹۹۷۱
SPK^4	۷/۹۹۶۰	۷/۹۹۶۲	۷/۹۹۶۷	۷/۹۹۶۷	۷/۹۹۶۴
SPK^5	۷/۹۹۶۹	۷/۹۹۶۵	۷/۹۹۷۱	۷/۹۹۶۵	۷/۹۹۵۹

۴-۵. سنجش کیفیت رمزنگاری

با اعمال رمزنگاری به تصویر، تغییراتی در مقادیر پیکسل‌ها ایجاد می‌شود که با مقادیر قبل از اعمال رمز متفاوت‌اند. این تغییرات ممکن است نامنظم باشند. تغییرات بیشتر در مقادیر پیکسل‌ها، نشان‌دهنده مؤثرتر بودن رمزنگاری و در نتیجه، بهتر بودن کیفیت رمزنگاری است. بنابراین، کیفیت رمزنگاری به صورت مجموع تغییرات اعمال شده در مقادیر پیکسل‌ها بین تصویر اصلی و تصویر رمز می‌باشد. یک معیار برای سنجش کیفیت رمزنگاری انحراف معیار بین تصویر اصلی و تصویر رمز می‌باشد. کیفیت تصویر رمز به صورت زیر بیان می‌شود[۲۵]:

فرض کنید P و C به ترتیب نشان‌دهنده تصویر اصلی و تصویر رمز باشند که هر کدام H × W پیکسل با L مقدار خاکستری دارند. $P(x,y), C(x,y) \in \{0,...,L-1\}$ مقادیر خاکستری P و C در نقطه (x, y) می‌باشند، به‌طوری که $0 \le x \le H-1$ و $0 \le y \le W-1$. $H_L(P)$ برابر تعداد پیشامدهای هر مقدار خاکستری L در تصویر اصلی و $H_L(C)$ برابر تعداد پیشامدهای هر مقدار خاکستری L در تصویر رمز می‌باشد. کیفیت رمزنگاری متوسط تعداد تغییرات در هر مقدار خاکستری L را نشان می‌دهد و به صورت زیر بیان می‌شود:

$$Encryption\ \ Quality = \sum_{L=0}^{255} (H_L(C) - H_L(P))/256 \quad (۸)$$

ضمناً، نویسنده معیارها و تقسیم‌بندی‌های جدیدی در زمینه سنجش کیفیت رمزنگاری مطرح کرده است(توصیه می‌گردد برای مطالعه کامل و جامع‌تر، به مقاله[۳۲] رجوع گردد). کیفیت رمزنگاری سامانه مورد مطالعه، محاسبه و در جدول (۴) ثبت گردید.

جدول ۴. سنجش کیفیت رمزنگاری الگوریتم رمزنگاری مورد مطالعه برای تعدادی از تصاویر اصلی نمونه

نام تصویر	بابون	ساعت	مرد عکاس	فلفل	تیفانی
اندازه	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶
نوع تصویر	خاکستری	خاکستری	خاکستری	خاکستری	خاکستری
SPK^1	۱۹۳/۴۶	۲۴۲/۴۶	۲۵۲/۳۹	۱۶۰/۱۷	۳۱۴/۹۷
SPK^2	۱۹۳/۹۵	۲۴۳/۵۵	۲۵۲/۳۲	۱۵۹/۴۲	۳۱۴/۰۲
SPK^3	۱۹۴/۲۵	۲۴۳/۳۹	۲۵۳/۴۵	۱۵۹/۷۹	۳۱۳/۶۶
SPK^4	۱۹۳/۷۵	۲۴۳/۲۰	۲۵۲/۱۸	۱۵۹/۹۹	۳۱۵/۹۰
SPK^5	۱۹۳/۰۸	۲۴۲/۹۱	۲۵۱/۷۰	۱۵۸/۹۷	۳۱۳/۳۸

۴-۶. تحلیل ضرایب همبستگی

در داده تصویری هر پیکسل به‌شدت با پیکسل‌های همسایه خود همبسته است[۲۴و ۹]. یک الگوریتم رمزنگاری ایده‌آل بایستی تصاویر رمزی تولید کند که همبستگی بین پیکسل‌های آن کم باشد. از معادلات زیر، برای مطالعه همبستگی بین دو پیکسل همسایه، در راستای افقی، عمودی و قطری استفاده می‌شود.

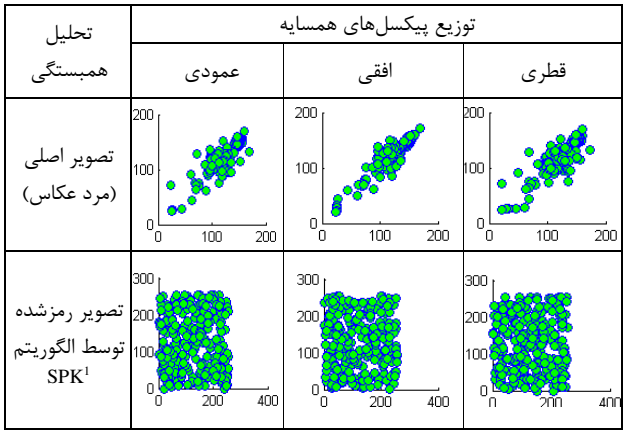
$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (۹)$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)^2 \quad (۱۰)$$

$$Cov(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)(y_j - \frac{1}{N}\sum_{j=1}^{N}y_j) \quad (۱۱)$$

که در آن x و y مقادیر روشنایی دو پیکسل همسایه در تصویر و N تعداد پیکسل‌های همسایه انتخاب شده از تصویر جهت محاسبه همبستگی می‌باشد. به‌طور معمول، جهت انجام آزمون همبستگی در تصویر، ۱۰۰۰ زوج از دو پیکسل همسایه به صورت تصادفی در تصویر انتخاب می‌شوند.

شکل (۷) تحلیل همبستگی بر روی تصویر استاندارد مرد عکاس و تصویر رمز شده توسط الگوریتم SPK^1 را نشان می‌دهد. همان‌گونه که مشاهده می‌شود، پیکسل‌های مجاور در تصویر اصلی همبستگی زیادی دارند، در حالی‌که همبستگی بین پیکسل‌های همسایه در تصاویر رمز بسیار کاهش یافته است.



شکل ۷. تحلیل همبستگی و نمایش نحوه توزیع دو پیکسل همسایه در تصویر اصلی و تصویر رمز

جدول ۵. ضرایب همبستگی بین دو پیکسل همسایه در تصویر اصلی و تصویر رمز

تحلیل ضرایب همبستگی			
تصویر	جهت پیکسل‌های همسایه		
	عمودی	افقی	قطری
تصویر اصلی (مرد عکاس)	۰/۹۱۰۲	۰/۹۴۶۳	۰/۸۸۶۱
SPK^1	۰/۰۰۷۴	۰/۰۱۰۰	۰/۰۱۳۹
SPK^2	۰/۰۰۰۱	۰/۰۱۷۱	۰/۱۰۰۲
SPK^3	۰/۰۵۵۷	۰/۰۳۹۸	۰/۰۰۰۱
SPK^4	۰/۰۵۵۸	۰/۰۰۹۲	۰/۰۳۹۲
SPK^5	۰/۰۲۶۹	۰/۰۳۵۲	۰/۰۱۰۸

جدول (۵) ضرایب همبستگی بین دو پیکسل همسایه در تصویر اصلی و تصاویر رمز را در سامانه رمزنگاری مورد مطالعه نشان می‌دهد. ضرایب همبستگی تصاویر رمز بسیار کوچکتر از ضرایب همبستگی تصویر اصلی هستند.

۴-۷. تمایز بین تصویر اصلی و تصویر رمز

به‌طور کلی یک خاصیت ایده‌آل برای یک تصویر رمز، حساس بودن نسبت به تغییرات جزئی در تصویر اصلی، یعنی فقط تغییر یک پیکسل، می‌باشد. مهاجم تلاش می‌کند که با ایجاد تغییرات جزئی در تصویر ورودی، تغییرات حاصل در تصویر رمز را مشاهده کند. با این روش، رابطه معنی‌دار بین تصویر اصلی و تصویر رمز آشکار می‌شود که این عمل خود منجر به تسهیل در تشخیص و شناسایی کلید می‌شود. اگر یک تغییر کوچک در تصویر اصلی، با توجه به انتشار و اغتشاش، بتواند تغییر قابل ملاحظه‌ای در تصویر رمز ایجاد کند، آنگاه حمله تمایز کارایی خود را از دست می‌دهد و در عمل بی‌استفاده می‌شود.

برای آزمودن اثر تغییر یک پیکسل ورودی بر روی تمام تصویر رمز شده به وسیله الگوریتم پیشنهادی، سه معیار رایج MAE[1]، NPCR[2] و UACI[3] استفاده می‌گردد[۳۳، ۳۰و ۱۳]. MAE متوسط خطای مطلق می‌باشد. NPCR یعنی نرخ تعداد پیکسل‌های تغییر یافته تصویر رمز هنگامی که یک پیکسل تصویر اصلی تغییر یافته است. UACI یعنی متوسط‌گیری روی تغییرات شدت روشنایی به صورت یکپارچه که در آن متوسط اختلاف شدت روشنایی دو تصویر اصلی و تصویر رمز سنجیده می‌شود.

فرض کنید P (i, j) و (i, j) به‌ترتیب نشان‌دهنده سطح خاکستری پیکسل‌های تصویر رمز و تصویر اصلی باشد، طوری‌که $0 \le i \le H-1$ و $0 \le j \le w-1$، H ارتفاع و W عرض تصویر می‌باشد. MAE بین دو تصویر به‌صورت زیر تعریف می‌شود:

$$MAE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} |C(i,j) - P(i,j)| \qquad (۱۲)$$

دو تصویر رمز C و $\overline{C}$ را در نظر بگیرید که تصاویر اصلی متناظر آنها فقط در یک پیکسل متمایزند. NPCR این دو تصویر برای هر کانال رنگی به‌شکل زیر تعریف می‌شود:

$$NPCR = \frac{\sum_{i=0}^{H-1} \sum_{j=0}^{W-1} D(i,j)}{H \times W} \times 100\% \qquad (۱۳)$$

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

معیار دیگر UACI است که با استفاده از فرمول زیر تعریف می‌شود:

$$UACI = \frac{1}{H \times W} \times \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \left[\frac{|C(i,j) - \overline{C}(i,j)|}{255} \right] \times 100\% \qquad (۱۴)$$

نتایج آزمون MAE برای سامانه رمزنگاری مورد مطالعه با استفاده از مجموعه کلیدهای خصوصی اصلی در جدول (۶) ثبت شده است. اطلاعات ثبت شده در جدول (۶) نشان می‌دهد که بین مقادیر MAE محاسبه‌شده سامانه‌های رمزنگاری مورد مطالعه، تفاوت اندکی وجود دارد.

نتایج آزمون NPCR و UACI در جدول (۷) ثبت شده است. نتایج به‌دست آمده برای دور اول سامانه رمزنگاری پیشنهادی، نشان می‌دهد که مقدار NPCR و UACI کمتر از ۱٪ است. این بدین معنی است که حساسیت کمی نسبت به تغییرات در ورودی دارد. در سامانه رمزنگاری پیشنهادی، بعد از دور اول رمزنگاری تغییرات قابل ملاحظه‌ای در مقدار NPCR و UACI دیده می‌شود.

با افزایش تعداد دور رمزنگاری، مقدار NPCR و UACI افزایش می‌یابد و به‌ترتیب، در حدود ۹۹٪ و ۳۳٪ تخمین زده می‌شود که نشان‌دهنده حساسیت طرح نسبت به تغییر در ورودی می‌باشد.

جدول ۶. نتایج آزمون MAE برای سامانه رمزنگاری مورد مطالعه با استفاده از مجموعه کلیدهای خصوصی اصلی

نام تصویر	بابون	ساعت	مرد عکاس	فلفل	تیفانی
اندازه	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶
نوع تصویر	خاکستری	خاکستری	خاکستری	خاکستری	خاکستری
SPK^1	۷۱/۱۷۳	۹۰/۱۰۴	۷۹/۳۷۴	۷۴/۶۶۲	۹۳/۳۵۲
SPK^2	۷۱/۱۳۸	۹۰/۰۶۲	۷۹/۴۸۷	۷۴/۴۴۶	۹۳/۵۸۵
SPK^3	۷۰/۹۵۵	۹۰/۰۶۱	۷۹/۸۶۱	۷۴/۸۳۲	۹۳/۴۶۱
SPK^4	۷۱/۰۱۵	۸۹/۸۵۰	۷۹/۷۶۹	۷۴/۹۵۰	۹۳/۳۶۱
SPK^5	۷۱/۰۹۱	۸۹/۸۴۳	۷۹/۴۴۸	۷۴/۶۳۳	۹۳/۱۰۳

جدول ۷. مقایسه NPCR و UACI در سامانه رمزنگاری مورد مطالعه

سامانه رمزنگاری	NPCR	UACI
SPK^1	٪۰/۰۰۱۵	٪۰/۰۰۰۱
SPK^2	٪۹۹/۴۰۸۰	٪۳۳/۵۰۰۶
SPK^3	٪۹۹/۴۱۴۱	٪۳۳/۳۰۷۹
SPK^4	٪۹۹/۴۰۱۹	٪۳۳/۳۳۴۷
SPK^5	٪۹۹/۴۳۵۴	٪۳۳/۳۵۰۹

[1] Mean Absolute Error
[2] Number of Pixels Change Rate
[3] Unified Average Changing Intensity

۴-۸. تحلیل حساسیت نسبت به کلید

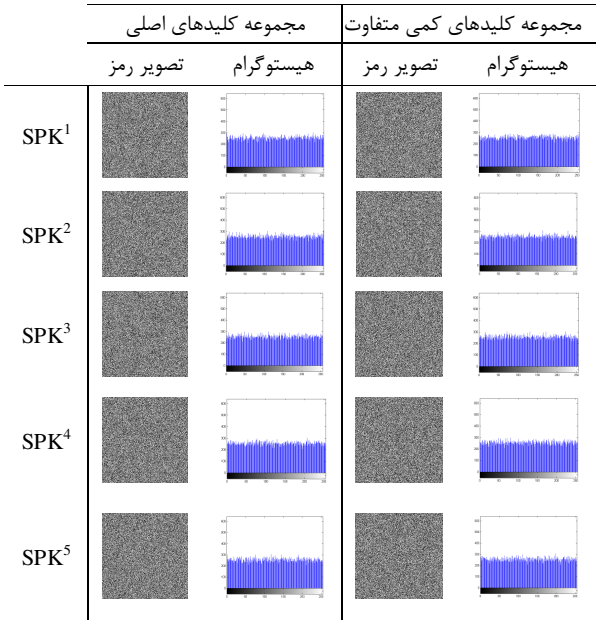
حساسیت نسبت به کلید، یک ویژگی ضروری برای یک سامانه رمزنگاری مطلوب می‌باشد. بدین معنی که تغییر یک بیت در کلید خصوصی، بایستی یک تصویر رمز کاملاً متفاوت تولید کند. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله جستجوی جامع تا حدی تضمین می‌کند.

برای آزمودن میزان حساسیت نسبت به کلید طرح رمزنگاری مورد مطالعه، تصویر مورد آزمایش یکبار با استفاده از کلید محرمانه اصلی و یکبار با استفاده از کلید محرمانه کمی تغییر یافته، رمز می‌شود. اگر مقایسه این دو تصویر رمز به‌صورت بصری امکان‌پذیر نباشد، آنگاه طرح رمزنگاری مورد مطالعه نسبت به کلید حساسیت بالایی دارد.

از آنجا که مقایسه دو تصویر از طریق مشاهده کاری دشوار است، لذا برای مقایسه بهتر می‌توان درصد تعداد پیکسل‌های متمایز دو تصویر رمز با کلیدهای متفاوت را محاسبه کرد.

هر چه مقدار این محاسبه به ۱۰۰٪ نزدیک‌تر باشد، آنگاه حساسیت نسبت به کلید بیشتر است. برای تحلیل حساسیت نسبت به کلید، تصویر استاندارد مرد عکاس به‌وسیله سامانه رمزنگاری مورد مطالعه، با استفاده از مجموعه کلیدهای اصلی و مجموعه کلیدهای کمی متفاوت، رمز شد.

شکل (۸) نتیجه آزمون حساسیت نسبت به کلید را نشان می‌دهد. تشخیص تفاوت بین تصاویر رمز به‌صورت بصری کاری دشوار است. لذا هیستوگرام تصاویر رمز ترسیم شده است تا قیاس آسان‌تر شود.



شکل ۸. تحلیل حساسیت نسبت به کلید

۴-۹. تحلیل اجرایی

مستقل از ملاحظات امنیتی، ملاحظات مهم دیگری نیز وجود دارد که شامل سرعت رمزنگاری برای پردازش‌های بلادرنگ می‌باشد. به‌طور کلی، سرعت رمزنگاری به ساختار پردازنده، اندازه حافظه، ساختار سامانه عامل، زبان برنامه‌نویسی و همچنین نوع کامپایلر وابسته می‌باشد.

بنابراین مقایسه سرعت رمزنگاری دو طرح رمزنگاری، بدون استفاده از محیط برنامه‌نویسی یکسان و روش‌های بهینه، کاری بیهوده است. با توجه به مسایل ذکر شده، برای نشان دادن کارآمدی کاربرد و پیاده‌سازی سامانه‌های رمزنگاری مورد مطالعه، بایستی مقایسه‌ای صریح بین سرعت رمزنگاری سامانه‌های رمزنگاری مورد مطالعه صورت گیرد.

به‌طور معمول برای افزایش دقت در اندازه‌گیری‌های زمانی، یک مجموعه تصویر با اندازه‌های مختلف ۱۰ بار رمز می‌شود و میانگین سرعت رمزنگاری و رمزگشایی ثبت می‌شود. سرعت به‌صورت تعداد بیت خروجی بر مدت زمان تولید آن بیان می‌شود که واحد آن bit/sec است.

کارایی الگوریتم مورد مطالعه با استفاده از یک کد غیر بهینه MATLAB بر روی ماشینی با پردازنده‌ی GHzIntel core 2 Duo 2 و 2 Gbytes of RAM در محیط سامانه‌عامل Windows XP، ارزیابی شد. نتایج این ارزیابی بر حسب ثانیه در جدول (۸) ثبت شده است. مطابق نتایج ثبت شده، الگوریتم پیشنهادی بسیار سریع‌تر از الگوریتم AES-128[1] در مد شمارنده[2] می‌باشد[۱].

لازم به ذکر است که، در رمزنگاری تصویر با الگوریتم AES-128، درایه‌های ماتریس تصویر را به صورت سطری خوانده و آن را به صورت رشته‌ای رمز نمودیم.

جدول ۸. مقایسه NPCR و UACI در سامانه رمزنگاری مورد مطالعه

سامانه رمزنگاری	NPCR	UACI
SPK^1	٪۰/۰۰۱۵	٪۰/۰۰۰۱
SPK^2	٪۹۹/۴۰۸۰	٪۳۳/۵۰۰۶
SPK^3	٪۹۹/۴۱۴۱	٪۳۳/۳۰۷۹
SPK^4	٪۹۹/۴۰۱۹	٪۳۳/۳۳۴۷
SPK^5	٪۹۹/۴۳۵۴	٪۳۳/۳۵۰۹

[1] Advanced Encryption Standard
[2] Counter Mode

۵. نتیجه‌گیری

در این مقاله یک الگوریتم جدید برای رمزنگاری تصویر معرفی شد. به‌منظور ارزیابی کارآمدی، الگوریتم پیشنهادی توسط آزمون‌هایی استاندارد، ارزیابی شد. مطابق تحلیل فضای کلید، الگوریتم پیشنهادی نسبت به حمله جستجوی جامع از نظر محاسباتی مقاوم می‌باشد. نتایج به‌دست آمده از آزمون بصری و تحلیل هیستوگرام، نشان دادند که در تصاویر رمز الگوریتم مورد مطالعه هیچ‌گونه الگو و ناحیه بافت قابل تشخیص و هیچ‌گونه شباهت آماری بین ظاهر تصویر اصلی و تصویر رمز وجود ندارد. نتایج آزمون تصادفی بودن نشان دادند که دنباله بیتی تولید شده توسط الگوریتم مورد مطالعه هیچ‌گونه نقصی ندارد و تمامی آزمون‌های آماری را با مقادیر بالای P-مقدار، با موفقیت می‌گذراند. همچنین نتایج آزمون مربع خی، نشان داد که هیستوگرام تصاویر رمز تقریباً یکنواخت می‌باشد. نتایج به‌دست آمده از تحلیل آنتروپی نشان دادند که در تصاویر رمز الگوریتم مورد مطالعه، نشت اطلاعات بسیار ناچیز است و سامانه تحت مطالعه نسبت به حمله آنتروپی مصون می‌باشد.

مطابق نتایج به‌دست آمده از آزمون سنجش کیفیت رمزنگاری، سامانه رمزنگاری پیشنهادی از کیفیت خوبی برای رمزنگاری تصویر برخوردار است. تحلیل همبستگی نشان داد که ضرایب همبستگی بین پیکسل‌های همسایه در تصویر اصلی بعد از عمل رمزنگاری به‌صورت قابل ملاحظه‌ای کاهش می‌یابد.

جهت سنجش میزان تمایز بین تصویر اصلی و تصویر رمز از سه معیار MAE، NPCR و UACI استفاده شد. تحلیل تمایز نشان داد که در سامانه رمزنگاری مورد مطالعه، به جزء SPK2-5، مقدار NPCR و UACI کمتر از ۱٪ است. در سامانه رمزنگاری پیشنهادی، بعد از دور اول رمزنگاری تغییرات قابل ملاحظه‌ای در مقدار NPCR و UACI دیده می‌شود که نشان‌دهنده حساسیت طرح نسبت به تغییر در ورودی می‌باشد.

مطابق نتایج به‌دست آمده از تحلیل حساسیت نسبت به کلید، می‌توان نتیجه گرفت که سامانه رمزنگاری پیشنهادی نسبت به تغییر در کلید بسیار حساس می‌باشد. نتایج تحلیل اجرایی نشان دادند که سامانه رمزنگاری پیشنهادی بسیار سریع‌تر از الگوریتم AES-128 در مد شمارنده می‌باشد.

۶. مراجع

[۱]. جلفایی، علیرضا "پیاده‌سازی نرم‌افزاری یک الگوریتم بهینه رمز متقارن برای رمز کردن تصاویر"، پایان‌نامه کارشناسی ارشد، دانشگاه جامع امام حسین (ع)، تهران، ایران، ۱۳۸۹.

[2]. Jolfaei, A.; Mirghadri, A. "An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map."; In Proceedings of 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10), 2010, Florida, USA, 279-285.

[3]. Jolfaei, A.; Mirghadri, A. "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1."; In Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI 2010), 2010, Sanya, China.

[4]. Jolfaei, A.; Mirghadri, A. "An Image Encryption Approach Using Chaos and Stream Cipher."; Journal of Theoretical and Applied Information Technology 2010, 19(2), 117-125.

[5]. Sharma, M.; Kowar, M. K. "Image Encryption Techniques Using Chaotic Schemes: a Review."; International Journal of Engineering Science and Technology 2010, 2(6), 2359-2363.

[6]. Li, C.; Li, S.; Asim, M.; Nunez, J.; Alvarez, G.; Guarong, C. "On the Security Defects of an Image Encryption Scheme."; Image and Vision Computing 2009, 27(9), 1371-1381.

[7]. 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.

[8]. Shannon, C. E. "Communication Theory of Secrecy Systems."; Bell Syst. Tech. J. 1949, 28, 656-715.

[9]. Pisarchik, A. N.; Zanin, M. "Image Encryption with Chaotically Coupled Chaotic Maps."; Physica D. 2008, 237(20), 2638-2648.

[10]. Pareek, N. K.; Patidar, V.; Sud, K. K. "Discrete Chaotic Cryptography Using External Key."; Phys. Lett. A. 2003, 309, 75-82.

[11]. Kwok, H. S.; Tang, W. K. S. "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation."; Chaos, Solitons and Fractals, 2007, 32, 1518-1529.

[12]. Fridrich, J. "Symmetric Ciphers Based on Two Dimensional Chaotic Maps."; International Journal of Bifurcate Chaos 1998, 8(6), 1259-1284.

[13]. Chen, G.; Mao, Y.; Chui, C. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps."; Chaos, Solitons & Fractals 2004, 12, 749-761.

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

[15]. Lian, S. G.; Sun, J.; Wang, Z. "A Block Cipher Based on a Suitable Use of Chaotic Standard Map."; Chaos, Solitons and Fractals 2005, 26(1), 117-129.

[16]. Henon, M. "A Two-Dimensional Mapping with a Strange Attractor."; Communication in Mathematical physics 1976, 50, 69-77.

[17]. Forre, R. "The Henon Attractor as Key Stream Generator."; Abstracts of Eurocrypt, 1991, 76-80.

[18]. Machado, R. F.; Baptista, M. S.; Grebogi, C. "Cryptography with Chaos at the Physical Level."; Chaos, Solitons and Fractals 2004, 21(5), 1265-1269.

[19]. Lichtenberg, A. J.; Lieberman, M. A. "Regular and Chaotic Dynamics."; New York : Springer, 1992.

[20]. Ritter, T. "Substitution Cipher with Pseudo-random Shuffling: The Dynamic Substitution Combiner."; Cryptologia 1990, 14(4), 289-303.

[21]. Ritter, T. "Transposition Cipher with Pseudo-random Shuffling: The Dynamic Transposition Combiner."; Cryptologia 1991, 15 (1), 1-17.

[22]. Wong, K. W. "A Fast Chaotic Cryptographic Scheme with Dynamic Lookup Table."; Phys. Lett. A. 2002, 298(4), 238-242.

[23]. Feistel, H.; Notz, W.; Smith, J. L. "Some Cryptographic Techniques for Machine to Machine Data Communications."; Proceedings of IEEE 1975, 63(11), 1545-1554.

[24]. Gonzalez, R. C.; Woods, R. E. "Digital image processing."; 2nd. s. l. : Prentice Hall, 2002.

[25]. Ahmed, H. H.; Kalash, H. M.; Farag Allah, O. S. "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images."; Journal of Optical Engineering 2006, 45.

[26]. Http://www-ee.uta.edu/dip/courses/ee5356/

[27]. Http://sipi.usc.edu/database/

[28]. Lian, S. "Efficient Image or Video Encryption Based on Spatio-temporal Chaos System."; Chaos, Solitons and Fractals, 2009, 40, 2509-2519.

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

[30]. Rukhin, A. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications."; NIST Special Publication, 2010, 800-22

[31]. Etemadi Borujeni, S.; Eshghi, M. "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm."; Mathematical Problems in Engineering, 2009, Doi: 10.1155/2009/762652.

[32]. Jolfaei, A.; Mirghadri, A. "A New Approach to Measure Quality of Image Encryption."; International Journal of Computer and Network Security 2010, 2(8), 38-44.

[33]. Alvarez, G.; Li, S. "Breaking An Encryption Scheme Based on Chaotic Baker Map."; Physics Letters A. 2006, 352(1,2), 78-82.