

رمز شکنی و بهبود یک طرح جدید رمز تصویر آشوبی

بهروز خادم^{۱*}، مهدی پازوکی^۲، بهزاد علیزاده^۲

۱- مربی ۲- کارشناس ارشد، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۳/۰۱/۰۷، پذیرش: ۹۴/۰۱/۰۴)

چکیده

در این مقاله یک طرح رمز تصویر آشوبی مورد حمله خطی و تفاضلی قرار گرفته و نشان داده شده است که مهاجم می تواند برخی از تقریب های خطی و شاخص های تفاضلی با احتمال بزرگ که باعث کشف تصویر اصلی می شوند را پیدا کند. همچنین تعداد دیگری از نقاط ضعف طرح، مانند ضعف ذاتی یکی از نگاشت های آشوبی، به کارگیری نادرست آن و استفاده از کلیدهای ضعیف رمزنگاری مورد اشاره قرار گرفته اند. به علاوه در این مقاله یک طرح جایگزین کامل پیشنهاد و شبیه سازی شده است. نتایج حاصل از آزمایشات طرح بهبود یافته با طرح قبلی و چند طرح رمز تصویر آشوبی جدید دیگر مورد مقایسه قرار گرفته و برتری امنیتی و کارایی آن نشان داده شده است.

کلید واژه ها: رمز تصویر، نگاشت آشوبی، تقریب خطی و شاخص تفاضلی.

Cryptanalysis and Improvement of a New Chaotic Image Encryption Scheme

B. Khadem^{*}, M. Pazooki, B. Alizade

Department Of Computer Engineering, Engineering Faculty, Bu-Ali Sina University

(Received: 27/03/2014; Accepted: 23/03/2015)

Abstract

In this paper, a linear and differential attack to a chaotic image encryption scheme have been introduced and it has been shown that the intruder can obtain the plain image using these approximations with high probability. Also other weaknesses as inherent weakness of a chaotic map, improper use of map and weak keys have been presented. A complete alternative scheme has been suggested and simulated. The experimental results has shown the security and performance improvement of suggested scheme compared to the original and some other new schemes.

Keywords: Image encryption, Chaotic Map, Linear and Differential Approximation.

^{*}Corresponding Author E-mail: Bkhadem@ihu.ac.ir

۱. مقدمه

پیکسل‌ها با استفاده از یک ماتریس جابه‌جا کننده، مبتنی بر نگاشت بیکر جابه‌جا می‌شود (انتشار). در انتها نیز تصویر به‌دست آمده با یک دنباله کلید دوری مبتنی بر نگاشت بیکر یای انحصاری^۲ می‌شود.

۲. خلاصه‌ای از طرح SPK

در طرح SPK با استفاده از نگاشت‌های آشوبی هنون و بیکر، تصویر اصلی که یک تصویر خاکستری به اندازه 256×256 پیکسل است، با الگوریتم‌های ۱ تا ۵ و در چند دور تکراری مورد رمزنگاری قرار می‌گیرد. ابتدا با انتخاب مقادیر اولیه نگاشت هنون و تولید یک دنباله آشوبی، یک ماتریس جانسانی (SUB) تولید می‌شود و با استفاده از آن، مقادیر پیکسل‌های تصویر اصلی^۳ تعویض می‌شوند (الگوریتم ۱). در مرحله بعدی با انتخاب مقادیر اولیه و استفاده از ماتریس جایگشت تولید شده از نگاشت بیکر (الگوریتم ۲)، پیکسل‌های تصویر حاصل از مرحله جانسانی، به صورت عمودی و افقی جابه‌جا می‌شوند (الگوریتم ۳). سپس پیکسل‌های تصویر حاصل، به صورت قطری جابه‌جا می‌شوند (الگوریتم ۴). در انتها با انتخاب مقادیر اولیه نگاشت بیکر، یک دنباله آشوبی از نگاشت بیکر و سپس یک دنباله پیکسل هم اندازه با تصویر اصلی تولید شده و اعضای آن پیکسل به پیکسل با تصویر به‌دست آمده یای انحصاری می‌شوند (الگوریتم ۵). به علاوه پیشنهاد شده است که برای ایجاد پیچیدگی بیشتر در تصویر رمزی، بهتر است که کلیه الگوریتم‌ها در چند دور متوالی روی تصویر اصلی به ترتیب زیر تکرار شوند [۱۷].

$$SPK^r(p) = (\text{shuffle}(\text{substitute}(p)) \oplus \text{Roundkey})^r \quad (1)$$

همچنین دوره‌های تکرار عملیات رمزنگاری به ازای $r = 1, \dots, 5$ تحت عنوان SPK^1 تا SPK^5 معرفی شده‌اند.

۳. ارزیابی طرح SPK

به منظور تحلیل طرح، یک نسخه نرم‌افزاری بر اساس [۱۷] پیاده‌سازی و با آن آزمایش‌های مختلفی بر روی طرح انجام شده است. در ادامه طرح را از دو جنبه اصلی یعنی نگاشت‌های آشوبی و الگوریتم‌ها مورد ارزیابی قرار داده می‌شود.

۳-۱. ارزیابی نگاشت‌های آشوبی

در این قسمت ابتدا دنباله‌های آشوبی هنون و بیکر را از نظر خواص شبه تصادفی آزمایش می‌شود و سپس تضعیف تدریجی خواص آشوبی دنباله‌های رقمی تولید شده توسط این دو نگاشت را نشان داده می‌شود. برای بررسی (مطابق استاندارد [۱۸]) به ازای ۱۰۰ کلید مختلف (از جمله کلیدهای اصلی طرح) ۱۰۰ دنباله گسسته شده با طول ۱,۰۰۰,۰۰۰ بیت تولید کرده و آن‌ها را مورد ارزیابی قرار دادیم که نتایج آن در جدول‌های (۱ و ۲) نشان داده شده است.

یکی از اهداف مهم و اصلی پدافند غیرعامل در حوزه فناوری اطلاعات تأمین امنیت و حصول اطمینان از عدم دسترسی‌های غیر مجاز به اسرار و اطلاعات کشور است. در سالیان اخیر با توجه به رشد سریع رایانه‌های مدرن و پیشرفت‌های روزافزون در حوزه‌های مختلف فناوری اطلاعات و ارتباطات، امنیت داده‌های چندرسانه‌ای از اهمیت ویژه‌ای در شبکه‌های الکترونیکی اقتصادی، تجاری و نظامی در کشور برخوردار شده است. با پیشرفت‌های سریع در انتقال داده‌های چندرسانه‌ای در اینترنت، امنیت و محرمانگی تصاویر رقمی در برابر نسخه‌برداری، دسترسی‌های غیر مجاز و توزیع غیر قانونی از اهمیت زیادی برخوردار شده است. با توجه به برخی از ویژگی‌های خاص در رمزگذاری تصویر، مانند حجم بزرگ داده‌ها، افزونگی زیاد و همبستگی میان پیکسل‌ها، روش‌های سنتی رمزگذاری برای تصاویر مناسب نیستند. برای برطرف کردن نیازهای امنیتی، طرح‌های جدید رمز تصویر بسیاری معرفی شده‌اند که در میان آن‌ها، روش‌های رمز تصویر مبتنی بر آشوب با الگوریتم‌های سریع و کارآمد و بسیار امن پیشنهاد شده‌اند. همه روش‌های مبتنی بر آشوب شامل دو مرحله اصلی، انتشار و اغتشاش هستند. در مرحله انتشار مکان پیکسل‌ها در تصویر اصلی توسط یک نگاشت آشوبی تغییر می‌کند و در مرحله اغتشاش مقادیر پیکسل‌های تصویر اصلی با یک نگاشت آشوبی دیگر تغییر می‌کنند. این مراحل باید به گونه‌ای انجام شوند که در نتیجه آن‌ها، یک تغییر جزئی در هر پیکسل تصویر اصلی، باعث ایجاد تغییر بزرگی در تصویر رمزی بشود و تصویری کاملاً متفاوت را ایجاد کند. همچنین یک روش مبتنی بر جایگشت آشوبی باید یک فضای بزرگ کلید داشته باشد و در آن از دوره‌های تناوب کوتاه اجتناب شده باشد.

به نظر می‌رسد فردریک در مقاله‌اش برای اولین بار پیشنهاد داد تا از یک نگاشت آشوبی برای رمزنگاری تصویر استفاده شود [۱]. از آن زمان به بعد، الگوریتم‌های رمز تصویر آشوبی متنوعی طراحی شده‌اند [۱۱-۲] که بسیاری از آن‌ها مورد حمله قرار گرفته و شکسته شده‌اند. گالاتولو و همکاران [۱۲] مروری بر پیشرفت‌های اخیر نظری و عملی رمز تصویر آشوبی را ارائه کرده‌اند. آن‌ها همچنین فهرستی از معیارهای امنیتی و کارایی لازم را برای این رمزها معرفی کرده‌اند. نیز به ضرورت تدوین یک یا چند شرط کافی برای امنیت رمزهای آشوبی اشاره شده است و پیشنهادهایی به این منظور ارائه شده است [۱۳]. مقالات مروری دیگری نیز در این زمینه به چاپ رسیده است [۱۴-۱۶].

به تازگی، برخی از الگوریتم‌های رمزنگاری تصویر بر اساس در هم ریزی کلی^۱ ارائه شده‌اند. میرقدری و جلفایی، یک طرح رمزنگاری تصویر با استفاده از نگاشت‌های آشوبی پیشنهاد کرده‌اند [۱۷]. در طرح پیشنهادی (که برای رعایت اختصار در این مقاله طرح SPK نامیده می‌شود) ابتدا مقدار پیکسل‌های تصویر با استفاده از یک ماتریس جانسانی مبتنی بر نگاشت هنون تغییر می‌کنند (اغتشاش). سپس، مکان

^۲ Xor

^۳ Plain-Image

^۱ Total Shuffling

جدول ۱. نتایج آزمون دنباله خروجی نگاشت بیکر

نام آزمون	میانگین (درصد)	مقدار خي دو	نتیجه آزمون
فراوانی	۰	۹۹	رد
فراوانی در یک بلوک	۰	۹۹	رد
رن	۰	۹۹	رد
طولانی ترین رن	۰	۹۹	رد
رتبه ماتریس دودویی	۰	۹۹	رد
تبدیل فوری گسسته	۰	۹۹	رد
تطابق غیر همپوشان	۱۰۰	۰/۰۱۰۱	قبول
تطابق همپوشان	۰	۹۹	رد
ماورر	۰	۹۹	رد
فشرده‌گی لمپل-زیو	۰	۹۹	رد
سریال	۰	۹۹	رد
آنترپوی تقریبی	۰	۹۹	رد
جمع‌های تجمعی جلورونده	۱۰۰	۰/۰۱۰۱	قبول
جمع‌های تجمعی عقب رونده	۱۰۰	۰/۰۱۰۱	قبول
گشت‌های تصادفی	۱۰۰	۰/۰۱۰۱	قبول
گشت‌های تصادفی متغیر	۱۰۰	۰/۰۱۰۱	قبول

اعداد حقیقی در روش ممیز شناور و حساسیت شدید نگاشت‌های آشوبی به مقدار ورودی، دنباله‌های تولیدشده توسط این نگاشت‌ها، پس از یک دوره زمانی معین به تدریج خواص آشوبی خود را از دست می‌دهند [۱۹]. به همین دلیل برای جلوگیری از این مشکل یا کاهش تأثیر آن، لازم است در زمان به‌کارگیری این نگاشت‌ها ترفندهای خاصی به‌کار برود. یکی از این ترفندها استفاده از روش‌های گسسته‌سازی مفید و مناسب است [۱۹]. بر اساس پیاده‌سازی طرح SPK و آزمایش‌های انجام شده روی خروجی الگوریتم‌های آن مشاهده شد که به علت تضعیف تدریجی خواص آشوبی دنباله نگاشت بیکر، بعد از یک بار اجرای همه الگوریتم‌ها (بعد از SPK¹) در الگوریتم ۲ ماتریس Pmap تبدیل به یک ماتریس یکه شده و در نتیجه الگوریتم‌های ۳ و ۴ هیچ تأثیری روی فرآیند درهم‌ریزی^۱ نگذاشته‌اند (شکل ۱- قسمت د و قسمت ز).

اغلب نگاشت‌های آشوبی در دامنه تعریف خود نقاط ثابتی دارند که استفاده از آن‌ها در رمزنگاری ممکن است منجر به پیدا شدن کلیدهای ضعیف شود [۲۱]. یک کلید ضعیف باعث می‌شود که طرح رمزنگاری، دو تصویر اصلی متفاوت را به یک تصویر رمزی مشابه تصویر کند. در طرح SPK، مقادیر اولیه $x_0 = 0$ و $x_0 = 0.5$ نقاط ثابت نگاشت بیکر هستند [۲۰]. بنابراین این مقادیر باید از دامنه تعریف آن خارج شوند تا به عنوان کلید مخفی به‌کار نروند.

۳-۲. ارزیابی الگوریتم‌ها

یکی از مهم‌ترین معیارهای امنیت در یک طرح رمز تصویر حساسیت تصویر رمزی نسبت به تغییرات جزئی تصویر اصلی است [۷].

معمولاً برای تعیین میزان تأثیر تغییرات جزئی پیکسل‌های تصویر ورودی بر روی پیکسل‌های تصویر خروجی از معیارهای NPCR^۲ و UACI^۳ استفاده می‌شود. برای بررسی این معیارها در طرح SPK، دو تصویر اصلی از مرد عکاس که تنها در یک پیکسل اختلاف دارند به نام‌های PI₁, PI₂ را در نظر می‌گیریم. تصویرهای رمزی به-دست آمده و متناظر با این دو را به ترتیب CI₁, CI₂ می‌نامیم. همان-طور که از جدول (۳)، مشاهده می‌شود، در طرح SPK مقدار حساسیت دو تصویر رمزی CI₁, CI₂ (حتی در تکرارهای دوم به بعد هم) بسیار کم است [۲۱].

به نظر می‌رسد یکی از دلایل اصلی عدم حساسیت تصویر رمزی به تصویر اصلی در SPK آن است که مراحل اغتشاش و انتشار در الگوریتم‌های ۱ تا ۴ به طور ناقص و نامتوازن انجام می‌شوند. به عبارت دقیق‌تر داده‌هایی که در مرحله اغتشاش قرار می‌گیرند بیت‌های هر پیکسل هستند ولی در مرحله انتشار (به جای اینکه بیت‌های هر پیکسل مورد پردازش قرار بگیرند)، بایت‌ها یا خود پیکسل‌ها مورد پردازش قرار می‌گیرند.

جدول ۲. نتایج آزمون دنباله خروجی نگاشت هنون

نام آزمون	میانگین (درصد)	مقدار خي دو	نتیجه آزمون
فراوانی	۰	۹۹	رد
فراوانی در یک بلوک	۰	۹۹	رد
رن	۰	۹۹	رد
طولانی ترین رن	۰	۹۹	رد
رتبه ماتریس دودویی	۰	۹۹	رد
تبدیل فوری گسسته	۰	۹۹	رد
تطابق غیر همپوشان	۰	۹۹	رد
تطابق همپوشان	۰	۹۹	رد
ماورر	۰	۹۹	رد
فشرده‌گی لمپل-زیو	۰	۹۹	رد
پچیدگی خطی	۱۰۰	۰/۰۱۰۱	قبول
سریال	۰	۹۹	رد
آنترپوی تقریبی	۰	۹۹	رد
جمع‌های تجمعی جلورونده	۱۰۰	۰/۰۱۰۱	قبول
جمع‌های تجمعی عقب رونده	۱۰۰	۰/۰۱۰۱	قبول
گشت‌های تصادفی	۱۰۰	۰/۰۱۰۱	قبول
گشت‌های تصادفی متغیر	۱۰۰	۰/۰۱۰۱	قبول

این نتایج نشان می‌دهند که هیچ یک از آن‌ها از نظر خواص شبه تصادفی برای کاربردهای رمزنگاری که از دنباله‌های آشوبی طولانی استفاده می‌کنند، مناسب نیستند. به ویژه استفاده از نگاشت بیکر فقط در شرایط خاصی مفید است [۱]. همچنین با توجه به اینکه دنباله حاصل از این نگاشت به سرعت همگرا به صفر می‌شود، استفاده از آن برای تولید دنباله‌های شبه تصادفی در الگوریتم ۵، باعث ساده شدن الگوریتم شده است،

$$SPK^r(p) \cong (\text{shuffle}(\text{substitute}(p)))^r \quad (۲)$$

این ساده شدن الگوریتم تأثیرات نامطلوبی بر خواص رمزی خروجی به وجود آورده است. به علاوه با توجه به محدودیت ارقام قابل نمایش

¹ Shuffling

² Number Absolute Error

³ United Average Changing Intensity

جدول ۳. مقایسه حساسیت در دوره های مختلف طرح SPK

UACI	NPCR	
۰/۰۰۰۱	۰/۰۰۱۵	SPK ^۱
۰/۰۰۰۹	۰/۰۰۱۵	SPK ^۲
۰/۰۰۰۱	۰/۰۰۱۵	SPK ^۳
۰/۰۰۰۱	۰/۰۰۱۵	SPK ^۴
۰/۰۰۰۸	۰/۰۰۱۵	SPK ^۵

۴. حمله خطی به ماتریس جانشرانی

حمله خطی مبتنی بر وجود تقریب های خطی در الگوریتم رمزنگاری است. در طرح SPK به ازای هر مقدار کلید مخفی، ماتریس جانشرانی یک نگاشت $SUB: \{0,1\}^8 \rightarrow \{0,1\}^8$ است. در اینجا یک تقریب خطی عبارتی شامل تعدادی از بیت های یک پیکسل ورودی به یک ماتریس جانشرانی آشوبی به نام $x = (x_1, x_2, \dots, x_8)$ به همراه تعدادی از بیت های پیکسل خروجی از آن به نام $y = (y_1, y_2, \dots, y_8)$ است. به عنوان مثال و با استفاده از کلید اصلی در SPK، ماتریس SUB را تشکیل می دهیم. برای انجام حمله خطی در یک مدل تصویر رمزی انتخابی ابتدا جدول (۵) را تشکیل می دهیم. سپس ترکیب های مختلف از بیت های ورودی و خروجی را مطابق رابطه زیر محاسبه کرده و با شمارش $N_L(a, b)$ مقدار حاصل را در یک جدول مشابه جدول (۶) قرار می دهیم:

$$\left\{ \begin{array}{l} a = (a_1, a_2, \dots, a_8), b = (b_1, b_2, \dots, b_8) \\ N_L(a, b) = |\{(x, y) | y = SUB(x) \wedge \left(\bigoplus_{i=1}^8 a_i x_i \right) \oplus \left(\bigoplus_{i=1}^8 b_i y_i \right) = 0\}| \end{array} \right.$$

هر یک از سطرهای جدول حاصل نشان دهنده یک پیکسل ورودی ماتریس جانشرانی (با ضرایب a_i) و هر یک از ستون های آن نشان گر یک پیکسل خروجی ماتریس جانشرانی (با ضرایب b_j) است.

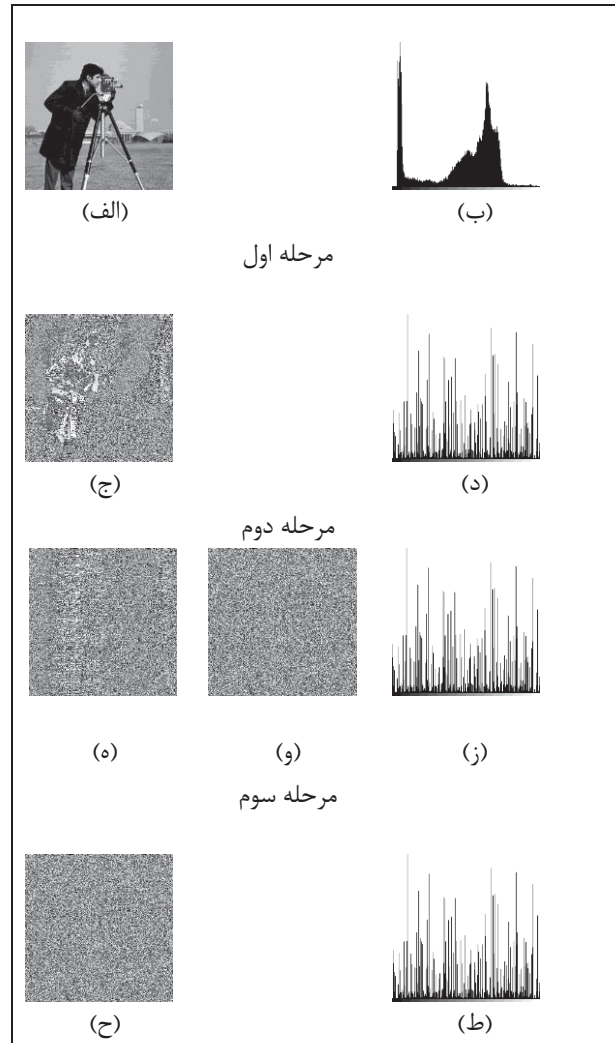
جدول ۴. نتایج آزمون MAE برای سامانه رمزنگاری طرح SPK

بایون	ساعت	مرد عکاس	فلفل	
۶۶/۷۴۳	۹۲/۱۶۸	۷۸/۱۱۵	۷۱/۴۹۸	SPK ^۱
۸۲/۰۷۰	۸۴/۲۶۳	۸۲/۹۵۴	۸۲/۹۳۳	SPK ^۲
۸۴/۳۳۲	۸۵/۶۲۶	۸۶/۴۷۰	۸۵/۴۸۱	SPK ^۳
۸۳/۹۳۶	۸۷/۶۶۰	۸۸/۸۴۷	۸۴/۷۵۱	SPK ^۴
۸۵/۷۷۵	۹۱/۳۳۵	۸۸/۵۰۰	۸۵/۸۲۱	SPK ^۵

برای ارزیابی ماتریس جانشرانی SUB با استفاده از الگوریتم ۱ و کلیدهای اصلی طرح SPK، ماتریس را تولید کرده و با ماتریس جانشرانی AES و ماتریس جانشرانی Lorenz مورد مقایسه و ارزیابی قرار داده شد. می توان نشان داد مقدار متوسط قابل انتظار برای $N_L(a, b)$ مقدار $\delta = 128$ است [۱۴]. در مثال بالا به ازای هر $1 \leq i \leq 8$ و هر $1 \leq j \leq 8$ مقدار $\delta_{SUB} = N_L(a, b)$ طرح SPK نامعادله زیر صدق می کند،

$$۹۳ < \delta_{SUB} < ۱۶۳$$

از طرف دیگر با استفاده از ماتریس های جانشرانی AES و Lorenz و



شکل ۱. نتایج پیاده سازی یک تکرار SPK با استفاده از تصویر مرد عکاس (الف) تصویر اصلی، (ب) هیستوگرام تصویر اصلی، (ج) جانشرانی، (د) هیستوگرام تصویر جانشرانی شده، (ه) جایگشت افقی و عمودی، (و) جایگشت افقی، عمودی و قطری، (ز) هیستوگرام تصویر جایگشت شده، (ح) تصویر رمزی، (ط) هیستوگرام تصویر رمزی

متأسفانه طرح SPK شامل ابهامات و اشکالات دیگری نیز هست که در زیر مورد اشاره قرار می گیرند. در شکل (۳) قسمت (ج) از [۱۷]، تصویر رمزی پس از اجرای جایگشت افقی دیده می شود در حالی که طبق ادعای مؤلفین در الگوریتم ۳، جایگشت عمودی و افقی مکان پیکسل ها، به صورت توأم و هم زمان در یک الگوریتم اجرا می شوند.

در قسمت ۴-۹ از مرجع [۱۷] اظهار شده است که نتایج کارایی طرح در جدول (۸) از مرجع [۱۷] ارائه شده است، در صورتی که این جدول مربوط به موضوع دیگری بوده و در ضمن با جدول (۷) [۲۰] مشابه است. محاسبات جدول (۷) [۱۷] با ورودی های مشابه، مجدداً انجام شد که به جز دور اول، مقادیر NPCR و UACI برای دوره های دوم به بعد با نتایج طرح SPK متفاوت بود (جدول ۳).

به علاوه محاسبات مربوط به جدول (۶) [۱۷] دوباره انجام شد و نتایج متفاوتی حاصل گردید (جدول ۴). همچنین برخی اشکالات نگارشی در متن الگوریتم های ۱ تا ۵ مشاهده شده است [۱۷]. برای مشاهده سایر ابهامات به مرجع [۲۰] مراجعه شود.

حمله خطی ضعیف تر است. امنیت ماتریس های AES و Lorenz در برابر حمله خطی تقریباً مشابه یکدیگر هستند [۲۲]. برای جزئیات بیشتر به مرجع [۲۰] مراجعه شود.

جدول ۷. مقایسه فراوانی مقدار تقریب های خطی

	AES	SUB	Lorenz
92-101	۰	۳۱	۰
102-110	۰	۱۰۴۰	۰
111-121	۱۴۶۶۶	۲۲۶۴۶	۱۵۸۸۶
122-131	۲۶۵۱۸	۳۰۱۸۴	۲۶۴۸۴
132-141	۲۱۶۷۲	۱۹۵۷۱	۲۱۰۵۱
142-151	۲۶۷۵	۶۵۱۲	۲۱۱۴
152-162	۰	۱۳۰	۰

۵. حمله تفاضلی^۱ به ماتریس جانشانی

دسترسی مهاجم به تفاضل دو تصویر اصلی از روی تفاضل دو تصویر رمزی انتخابی نتیجه انجام یک حمله تفاضلی در مدل تصویر رمزی انتخابی است و بر پایه جدول تقریب های تفاضلی انجام می شود. در جدول (۸) هر یک از سطرها نشان دهنده تفاضل دو ورودی ماتریس جانشانی SUB از مثال قبل و ستون های آن نشانگر تفاضل دو خروجی آن است. فرض x' تفاضل دو تصویر ورودی به صورت زیر باشد:

$$x'_i = x_i \oplus x^*_i \quad 0 \leq i \leq 255 \quad (۵)$$

و y' هم تفاضل دو تصویر خروجی به صورت زیر باشد:

$$y'_i = y_i \oplus y^*_i \quad 0 \leq i \leq 255 \quad (۶)$$

که به صورت زیر محاسبه شده اند:

$$\begin{cases} y_i = SUB(x_i) \\ y^*_i = SUB(x^*_i) \end{cases} \quad (۷)$$

برای هر (x', y') مقدار فراوانی $N_D(x', y')$ را مطابق با رابطه زیر محاسبه کرده و در جدول (۸) قرار می دهیم.

$$N_D(a, b) = |\{(x_i, x^*_i) \in \Delta x_i | SUB(x_i) \oplus SUB(x^*_i) = y'_i\}|$$

در جدول (۸) مقدار متوسط قابل انتظار برای $N_D(a, b)$ برابر مقدار $\bar{\delta} = 2$ است [۱۴].

مهاجم برای انجام حمله تفاضلی به ماتریس جانشانی ابتدا جدول (۸) را تشکیل داده و با انتخاب دو تصویر رمزی خروجی که حاصل تفاضل آن ها دارای فراوانی بیشینه در جدول تقریب های تفاضلی است (y') ، به تفاضل دو تصویر اصلی ورودی (x') متناسر با آن ها

پایه سازی جدول تقریب های خطی مربوطه، مقدار $N_L(a, b)$ برابر است با،

$$\begin{aligned} 111 < \delta_{AES} < 145 \\ 112 < \delta_{Lorenz} < 148 \end{aligned}$$

همچنین فراوانی طبقه بندی شده $N_L(a, b)$ در SUB و AES و Lorenz در جدول (۷) مقایسه شده اند.

جدول ۵. ورودی ها و خروجی های یک ماتریس جانشانی SUB

بیت های خروجی					بیت های ورودی				
y_8	y_7	...	y_2	y_1	x_8	x_7	...	x_2	x_1
۱	۰	...	۰	۱	۰	۰	...	۰	۰
۱	۱	...	۰	۰	۱	۰	...	۰	۰
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
۰	۰	...	۰	۱	۱	۱	...	۱	۱

در جدول (۶)، اربیی بیشینه مطابق رابطه (۳) محاسبه می شود و برای $N_L = 94$ و $N_L = 162$ مشابه بوده و برابر ۳۴ هست. مهاجم برای انجام حمله خطی کافی است یک تصویر رمزی را که تمام پیکسل های آن مقادیر 8A یا 0C است را انتخاب کند و با احتمال بزرگ، از خروجی ماتریس جانشانی به ورودی آن دسترسی پیدا کند.

با محاسبه این احتمال دیده می شود مهاجم از هر ۸ تصویر خروجی منتخب از SUB به یک تصویر ورودی متناسر آن دسترسی پیدا می کند.

$$\varepsilon_0 = |128 - 94| = 34 = |128 - 162| \quad (۳)$$

$$per_1 = \frac{\varepsilon_0}{2^8} \approx \frac{1}{8} \approx 0.125 \approx \%12 \quad (۴)$$

جدول ۶. تقریب های خطی ماتریس SUB

		b							
		00	...	8A	...	0C	...	FF	
a	00	۱۲۸	...	۱۲۸	...	۱۲۸	...	۱۲۸	
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	
	A4	۱۲۸	...	۹۴	...	۹۹	...	۱۲۲	
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	
	F4	۱۲۸	...	۱۱۰	...	۱۶۲	...	۱۱۱	
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	
	FF	۱۲۸	...	۱۰۲	...	۱۳۵	...	۱۰۸	

همان طور که از جدول (۷) مشاهده می شود به دلیل وجود تقریب های خطی با اربیی زیاد، ماتریس جانشانی SUB ضعیف و در نتیجه در برابر حمله خطی آسیب پذیر است. به علاوه بازه فراوانی در ماتریس جانشانی SUB نسبت به AES بزرگ تر است که شاهدی برای احتمال وقوع بیشتر برای انجام حمله خطی به SUB توسط یک مهاجم باشد [۲۱].

به علاوه از جدول (۷) دیده می شود که فراوانی تقریب های خطی ماتریس SUB هم از AES و هم از Lorenz بیشتر و در نتیجه در برابر

¹ Differential Attack

جدول (۱۰) نشان می‌دهد که ماتریس جاننشانی SUB از ماتریس‌های جاننشانی AES و Lorenz ضعیف‌تر است و بنابراین در برابر حمله تفاضلی به مراتب آسیب‌پذیرتر است. برای جزئیات بیشتر به مرجع [۲۱] مراجعه شود.

جدول ۱۰. مقایسه ماتریس‌های جاننشانی AES، SUB و Lorenz

	AES	SUB	Lorenz
per_3	% ۰/۳۹	% ۸/۹۷	% ۰/۵۸

۶. بهبود SPK

در این قسمت به منظور برطرف کردن برخی از نقاط ضعف SPK یک طرح بهبودیافته به نام SPK^+ را پیشنهاد می‌شود. در SPK^+ در الگوریتم ۱ از نگاشت آشوبی Lorenz و با روشی متفاوت یک ماتریس جاننشانی تولید می‌شود. همچنین در الگوریتم‌های ۲، ۴ و ۵ یک نگاشت آشوبی مرکب شامل نگاشت‌های آشوبی لجستیک و رینی به کار می‌رود. در ادامه این قسمت SPK^+ را در یک مدل حمله تصویر رمزی انتخابی از نظر حمله‌های خطی و تفاضلی، آزمون‌های آماری نگاشت‌های آشوبی، آزمون تمایز بصری، تحلیل هیستوگرام و تحلیل تصادفی مورد ارزیابی قرار داده و نشان داده می‌شود و در همه این آزمون‌ها، نتایج بهتری نسبت به SPK دارد.

۶-۱. جایگزینی نگاشت لورنتز با نگاشت هنون

به منظور بهبود الگوریتم ۱، به جای نگاشت هنون از نگاشت لورنتز^۱ برای تولید ماتریس جاننشانی استفاده می‌شود. در قسمت قبل این نگاشت را در برابر تحلیل‌های خطی و تفاضلی مورد ارزیابی قرار داده و از جدول‌های (۷) و (۹) دیده می‌شود که ماتریس Lorenz در برابر حمله‌های خطی و تفاضلی رفتاری بهتر از SUB و مشابه AES و حتی بهتر از آن دارد. بنا به ادعای مؤلفین، خواص جبری، غیرخطی و همبستگی ماتریس Lorenz هم از AES بهتر است [۳]. جدول‌ها تقریب‌های خطی و تفاضلی ماتریس Lorenz، به ازای کلیدهای پیشنهادی در جدول (۱۱) را پیاده‌سازی کرده و مشاهده می‌شود که بازه فراوانی $N_L(a, b)$ مربوط به Lorenz و AES به شرح زیر است:

$$111 < \delta_{Lorenz} < 145 \quad (11)$$

$$112 < \delta_{AES} < 144 \quad (12)$$

برای سنجش میزان مقاومت در برابر حمله خطی و تفاضلی مشاهده می‌شود که فراوانی $N_D(a, b)$ مربوط به Lorenz با AES مشابه است (جدول (۹)).

همچنین از جدول (۱۰) مشاهده می‌شود که هر دو ماتریس جاننشانی Lorenz و AES از این جهت، از مقاومت زیادی در برابر حمله‌های خطی و تفاضلی برخوردار هستند. بنابراین می‌توان نتیجه گرفت که به طور کلی در الگوریتم ۱ ماتریس Lorenz از مقاومت بیشتری نسبت به SUB برخوردار است.

دسترسی پیدا می‌کند. (به عنوان مثال در این طرح، بیشینه فراوانی ۱۰ است که در تقاطع سطر $x' = A9$ و ستون $y' = A6$ قرار دارد).

جدول ۸. تقریب‌های تفاضلی ماتریس SUB

		y'				
		00	...	A6	...	FF
x'	00	۲	...	۴	...	۲
	⋮	⋮	⋮	⋮	⋮	⋮
	A9	۲	...	۱۰	...	۸
	⋮	⋮	⋮	⋮	⋮	⋮
	FF	۰	...	۶	...	۸

جدول ۹. مقایسه فراوانی مقدار تقریب‌های تفاضلی

	AES	SUB	Lorenz
0	۳۳۱۵۰	۳۹۸۸۲	۳۳۲۷۶
2	۳۲۱۳۰	۱۹۷۶۹	۳۱۸۷۸
4	۲۵۵	۴۹۲۳	۳۸۱
6	۰	۸۳۴	۰
8	۰	۱۱۲	۰
10	۰	۱۵	۰
256	۱	۱	۱

در جدول (۸) آریبی بیشینه را با رابطه (۸) و میزان ضعف تفاضلی ماتریس جاننشانی در طرح SPK را با رابطه (۹) محاسبه می‌شود و با نماد per_2 ، نشان داده می‌شود.

$$\varepsilon_0 = |10 - 2| = 8 \quad (8)$$

$$per_2 = \frac{\varepsilon_0}{2^8} = \frac{8}{256} = \frac{1}{32} \approx 0.032 \quad (9)$$

به عنوان مثال در این طرح مهاجم از هر ۳۲ تفاضل تصویر خروجی به یک تفاضل تصویر ورودی متناظر دسترسی پیدا می‌کند.

در جدول (۹) فراوانی $N_D(a, b)$ برای سه ماتریس جاننشانی AES و SUB و Lorenz انجام شده است. همان‌گونه که مشاهده می‌شود، ماتریس SUB، به دلیل بزرگ‌تر بودن بازه فراوانی نسبت به دو ماتریس جاننشانی AES و Lorenz در برابر حمله تفاضلی ضعیف‌تر است. در جدول (۹) هر چه تکرار تفاضل‌ها بیشتر باشد، مهاجم با امکان انتخاب بیشتری از تصویر رمزی به تفاضل دو تصویر اصلی دسترسی پیدا می‌کند. به علاوه در جدول (۹) مشاهده می‌شود فراوانی تفاضل‌ها به ازای مقدار $N_D = 6$ برابر ۸۳۴ است. این مقدار نشان می‌دهد، مهاجم با احتمال زیاد می‌تواند به این تعداد از تفاضل‌های تصویر اصلی دسترسی پیدا کند، اما در ماتریس جاننشانی AES به ازای $N_D = 6$ مهاجم نمی‌تواند به هیچ تفاضلی از تصویر اصلی دست پیدا کند. همچنین درصد سلول‌هایی از جدول (۸) که آریبی زیادی دارند و مهاجم می‌تواند با انتخاب یک کلید مجاز و دو تصویر رمزی معین به دو تصویر اصلی متناظر برسد را با مقدار per_3 نمایش داده می‌شود و در جدول (۱۰) ارائه می‌شود.

$$per_3 = |\{N_D(a, b), |N_D(a, b) - 2| \geq 6\}| \quad (10)$$

¹ Lorenz

$$C_k = \begin{cases} 0, & (x_k - \frac{1}{2}) \cdot (y_k - \frac{1}{2}) \geq 0 \\ 1, & (x_k - \frac{1}{2}) \cdot (y_k - \frac{1}{2}) < 0 \end{cases} \quad (15)$$

به دلیل تغییرات انجام شده در الگوریتم‌های ۱، ۲ و ۵ دیده می‌شود که هیستوگرام تصویر رمزی در طرح SPK⁺ مطابق شکل‌های (۲ و ۳) در مقایسه با تصویر رمزی SPK در شکل (۱) از توزیع یکنواخت قابل توجهی برخوردار است. همچنین جهت مقایسه دقیق‌تر، آزمون تحلیل حساسیت را بین تصویر ورودی و خروجی در الگوریتم‌های ۱ و ۵ (جدول‌های ۱۳ و ۱۴) نشان داده شد که میزان حساسیت را بر اساس معیارهای NPCR، UACI و MAE نشان می‌دهد.

جدول ۱۲. نتایج آزمون دنباله تکرارهای نگاشت مرکب

نام آزمون	میانگین (درصد)	مقدار خي دو	نتیجه آزمون
فراوانی	۹۹	۰	قبول
فراوانی در یک بلوک	۹۹	۰	قبول
رن	۱۰۰	۰/۰۱۰۱	قبول
طولانی‌ترین رن	۹۹	۰	قبول
رتبه ماتریس دودویی	۹۹	۰	قبول
تبدیل فوریه گسسته	۹۹	۰	قبول
تطابق غیر همپوشان	۹۷	۴/۴۰۴۰	قبول
تطابق همپوشان	۱۰۰	۰/۰۱۰۱	قبول
ماورر	۱۰۰	۰/۰۱۰۱	قبول
فشرده‌گی لمپل-زیو	۱۰۰	۰/۰۱۰۱	قبول
پیچیدگی خطی	۱۰۰	۰/۰۱۰۱	قبول
سریال	۱۰۰	۰/۰۱۰۱	قبول
آنتروپی تقریبی	۱۰۰	۰/۰۱۰۱	قبول
جمع‌های تجمعی جلورونده	۹۹	۰	قبول
جمع‌های تجمعی عقب رونده	۹۸	۰/۰۱۰۱	قبول
گشت‌های تصادفی	۱۰۰	۰/۰۱۰۱	قبول
گشت‌های تصادفی متغیر	۹۹	۰	قبول

جهت اطمینان از امنیت یک سامانه رمز تصویر، دنباله کلید اجرایی می‌بایست برخی خواص احتمالی مناسب از جمله توزیع یکنواخت، دوره تناوب طولانی، پیچیدگی بالا و کارآمدی را داشته باشد. امروزه روش‌های آماری متنوعی برای ارزیابی میزان تصادفی بودن تصویر رمزی در سامانه رمزنگاری وجود دارد. برای بررسی این معیار آزمون آماری را بر روی تصویر رمزی، در هر دو طرح (SPK⁺ و SPK)، مطابق جدول‌های (۱۵ و ۱۶) انجام داده شد. نتایج این آزمون نشان می‌دهد که طرح SPK تنها ۷ آزمون از ۱۶ آزمون NIST را می‌گذراند در حالی که طرح SPK⁺ همه آزمون‌ها را با موفقیت می‌گذراند.

به طور کلی حساسیت تصویر رمزی نسبت به کلید یک ویژگی ضروری برای یک سامانه رمزنگاری مطلوب است. بدین معنی که تغییر یک بیت در کلید خصوصی باید یک تصویر رمزی کاملاً متفاوت تولید کند. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزنگاری را در برابر حمله جستجوی

۲-۶. جایگزینی یک نگاشت آشوبی مرکب با نگاشت بیکر

در این قسمت، با توجه به خواص آماری نامناسب و همچنین تضعیف تدریجی خواص آشوبی دنباله تکرارهای نگاشت بیکر، به جای آن از یک نگاشت آشوبی مرکب در الگوریتم‌های ۲ و ۵ استفاده می‌شود. نگاشت پیشنهادی از ترکیب دو نگاشت آشوبی لجستیک و رینی، مطابق رابطه (۱۳) به دست می‌آید. رابطه بازگشتی این نگاشت به ازای مقادیر $0 \leq k$ به صورت رابطه (۱۴) زیر است:

$$\begin{cases} x_{k+1} = 4x_k(1 - x_k), & x_k \in (0,1) \\ y_{k+1} = 3y_k - [3y_k], & y_k \in (0,1) \end{cases} \quad (13)$$

$$z_k = (x_k) \cdot (y_k) \quad (14)$$

در این نگاشت مقادیر اولیه در هر دو نگاشت لجستیک و رینی، مساوی در نظر گرفته می‌شوند ($x_0 = y_0$) اما در تکرارهای بعدی، هر نگاشت تحول درونی و مستقلی از دیگری خواهد داشت. ضمناً در هر تکرار دنباله‌های تولیدشده با رابطه (۱۴) با هم ترکیب می‌شوند. به منظور ارزیابی خواص شبه تصادفی دنباله آشوبی مرکب، ضمن تولیدی ۱۰۰ دنباله یک میلیون بیتی، آن‌ها را مورد آزمون‌های آماری NIST قرار داده شد. برای شبیه‌سازی از تعدادی کلید خصوصی برای نگاشت مرکب، مطابق با جدول (۱۱) استفاده شده است.

جدول ۱۱. کلیدهای خصوصی در SPK⁺

مجموعه کلیدهای اصلی					
الگوریتم ۱		الگوریتم ۲		الگوریتم ۵	
x_0	y_0	x_0	y_0	x_0	y_0
۰/۴	۰/۴	۰/۱	۰/۱	۰/۳	۰/۳

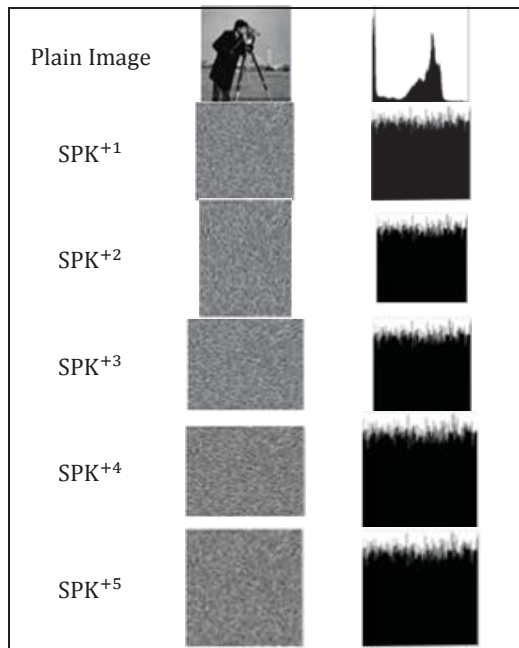
نتایج نهایی این آزمایش نشان می‌دهد که دنباله تولید شده همه آزمون‌های مربوطه را با موفقیت می‌گذراند. (جدول ۱۲). در الگوریتم ۲، دنباله حقیقی $\{z_k\}_{k=1}^{256}$ را برای تولید ماتریس جایگشت Pmap استفاده کرده و جایگشت‌های سطری و ستونی و قطری را مطابق با الگوریتم‌های ۳ و ۴ انجام می‌شود.

در الگوریتم ۵ نیز برای تولید ماتریس کلید دوری، ابتدا دنباله حقیقی $\{z_k\}_{k=1}^{8 \times 256 \times 256}$ را تولید کرده، سپس با توجه به روش گسسته‌سازی مطابق رابطه (۱۵) یک دنباله بیتی تولید کرده و با تصویر خروجی از الگوریتم ۴، XOR می‌شود.

۳-۶. بهبود جامع در SPK و تحلیل امنیت و کارایی

در این قسمت نشان داده می‌شود کاربرد بهبودهای جزئی در کنار هم و به طور یکپارچه، چگونه امنیت کلی طرح پیشنهادی را افزایش می‌دهند. برای بهبود جامع، به صورت هم‌زمان از ماتریس جانشرانی Lorenz در الگوریتم ۱ و از نگاشت مرکب (۱۳) و (۱۴) و تبدیل (۱۵) در الگوریتم‌های ۲ و ۵ استفاده شد. طرح بهبود جامع رمز تصویری را بر اساس آزمون‌های آماری نگاشت‌های آشوبی، آزمون تمایز بصری و تحلیل هیستوگرام و تحلیل تصادفی بودن دنباله‌های تصویر رمزی مورد ارزیابی قرار داده می‌شود.

شده است که نتایج آن در جدول (۱۷) و شکل (۴) دیده می شود. این نتایج نشان می دهند تصویر رمزی در SPK^+ نسبت به SPK از حساسیت بیشتری نسبت به کلید برخوردار است.



شکل ۳. نتایج آزمون بصری و تحلیل هیستوگرام در ۵ دور طرح SPK^+

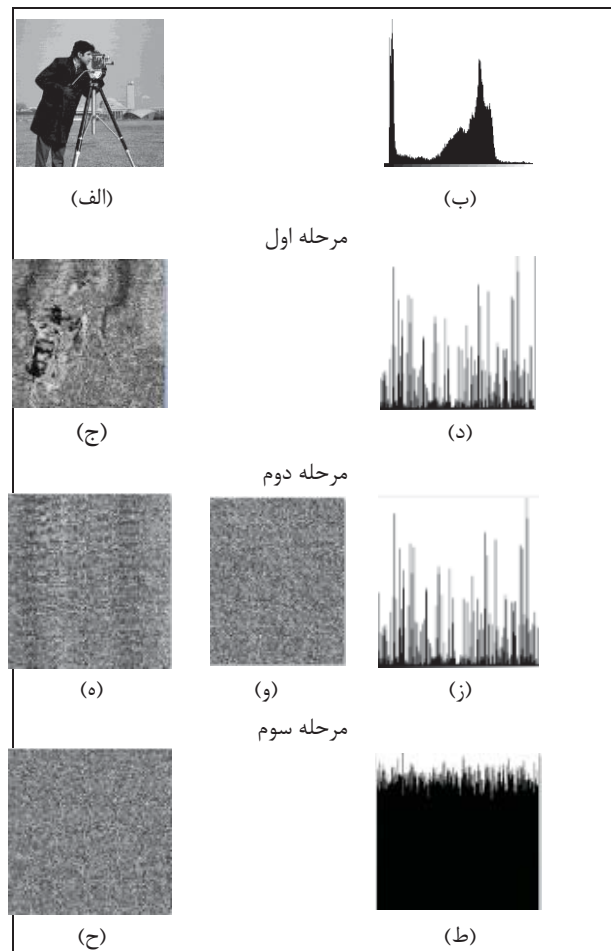
جدول ۱۵. نتایج تحلیل تصادفی بیت های تصویر رمزی در طرح SPK

نتیجه آزمون	مقدار خی دو	میانگین (درصد)	نام آزمون
رد	۹۹	۰	فراوانی
رد	۹۹	۰	فراوانی در یک بلوک
رد	۹۹	۰	رن
رد	۹۹	۰	طولانی ترین رن
قبول	۰/۰۱۰۱	۱۰۰	رتبه ماتریس دودویی
رد	۹۹	۰	تبدیل فوریه گسسته
رد	۹۹	۰	تطابق غیر همپوشان
قبول	۰/۰۱۰۱	۱۰۰	تطابق همپوشان
رد	۹۹	۰	ماورر
قبول	۰/۰۱۰۱	۱۰۰	پیچیدگی خطی
رد	۹۹	۰	سریال
رد	۹۹	۰	آنتروپی تقریبی
قبول	۰/۰۱۰۱	۱۰۰	جمع های تجمعی جلو رونده
قبول	۱/۰۱۰۱	۱۰۰	جمع های تجمعی عقب رونده
قبول	۱/۰۱۰۱	۱۰۰	گشت های تصادفی
قبول	۰/۰۱۰۱	۱۰۰	گشت های تصادفی متغیر

همچنین در جدول (۱۸) مقایسه نتایج تحلیل حساسیت تصویر رمزی به کلید، بین طرح بهبود یافته با تعدادی از طرح های مشابه رمز تصویر آشوبی [۸-۱۱] از جمله طرح قبلی [۲۰] دیده می شود. این جدول به طور کلی نشان می دهد که طرح SPK^+ از نظر میزان حساسیت تصویر رمزی نسبت به کلید از سایر طرح ها (به جز طرح Giesl) برتر است.

از جهت دیگر چون از یک طرف پیشنهاد شده که برای ایجاد پیچیدگی بیشتر در تصویر رمزی بهتر است که کلیه الگوریتم های

جامع تا حدی تضمین می کند. برای آزمون میزان حساسیت تصویر رمزی نسبت به کلید، تصویر مورد آزمایش یک بار با استفاده از کلید مخفی اصلی و یک بار با استفاده از همان کلید (که به اندازه کمی تغییر کرده) رمز می شود.



شکل ۲. نتایج پیاده سازی الگوریتم SPK^+ با استفاده از تصویر مرد عکاس (الف) تصویر اصلی، (ب) هیستوگرام تصویر اصلی، (ج) تصویر باجانشانی، (د) هیستوگرام تصویر باجانشانی شده، (ه) تصویر با جایگشت افقی و عمودی، (و) تصویر با جایگشت افقی، عمودی و قطری، (ز) هیستوگرام تصویر جابه جا شده، (ح) تصویر رمزی، (ط) هیستوگرام تصویر رمزی

جدول ۱۳. مقایسه نتایج تحلیل حساسیت در الگوریتم ۱

	NPCR	UACI	MAE
SUB	۹۹/۸۷	۳۰/۶۷	۷۸/۲۱
AES	۹۹/۹۷	۲۷/۴۸	۷۰/۰۸
Lorenz	۱۰۰	۳۳/۲۲	۸۴/۷۱

جدول ۱۴. مقایسه نتایج تحلیل حساسیت در الگوریتم ۵

	NPCR	UACI	MAE
Compound	۹۸/۸۳	۳۲/۹۵	۸۴/۰۲

برای مقایسه دقیق تر اثر این تغییر از معیارهای NPCR و UACI استفاده می شود. برای تحلیل حساسیت نسبت به کلید، تصویر استاندارد مرد عکاس به وسیله سامانه رمزنگاری SPK^+ یک بار با استفاده از کلیدهای اصلی و بار دیگر با کلیدهای کمی متفاوت، رمز

جدول ۱۸. مقایسه تحلیل حساسیت بین SPK^{1+} و چند طرح اخیر

UACI	NPCR	
۰/۰۰۰۱	۰/۰۰۱۵	SPK^1
۳۳/۴۱	۹۹/۶۱	Amin[۲۰]
۳۳/۵	۹۹/۶۱	Zhou[۱۶]
۲۹/۶	۹۱/۸۵	Giesl[۱۷]
۳۳/۲۵	۹۹/۶۲	Chattopadhyay[۱۸]
۳۲/۷۶	۹۹/۶۷	SPK^{1+}

۷. نتیجه گیری

در این مقاله یک طرح رمز تصویر آشوبی به نام SPK ، مورد حمله خطی و تفاضلی قرار گرفت و نشان داده شد که مهاجم می‌تواند در یک مدل حمله تصویر رمزی انتخابی تصویر اصلی را با استفاده از تقریب‌های تفاضلی کشف کند. به علاوه تعدادی از کلیدهای ضعیف آن پیدا شد و با استفاده از معیارهای $UACI$ و $NPCR$ نشان داده شد که تصویر رمزی حساسیت لازم نسبت به تغییرات جزئی تصویر اصلی را ندارد. همچنین با بررسی خواص شبه تصادفی و آشوبی دنباله‌های نگاشت‌های آشوبی به کار رفته در SPK ، نشان داده شد که الگوریتم قابلیت ساده شدن را دارد. بنابراین می‌توان نتیجه گرفت که این طرح ناامن است. در ادامه، طرح بهبود یافته SPK^+ پیشنهاد شد که در ساختار آن از یک نگاشت آشوبی لورنتز در الگوریتم ۱ و از یک نگاشت آشوبی مرکب شامل نگاشت‌های لجستیک و رینی در الگوریتم‌های ۲ و ۵ برای تولید ماتریس جایگشت و ماتریس کلید استفاده شده است. نتایج آزمایش‌های حاصل از پیاده‌سازی نرم‌افزاری نشان داد که از جهت امنیتی در SPK^+ خواص خطی و تفاضلی، حساسیت نسبت به کلید، خواص آماری، عدم تباهدگی نگاشت‌های آشوبی، آزمون بصری، تحلیل هیستوگرام و تحلیل تصادفی بودن تصویر رمزی نسبت به SPK ارتقاء یافته و از نظر کارایی نیز سرعت رمزنگاری آن ۵ برابر افزایش یافته است. به علاوه مقایسه تحلیل حساسیت طرح SPK^+ با چند طرح رمز تصویر آشوبی اخیر نشان داد که از این جهت نیز این طرح برتری قابل ملاحظه‌ای نسبت به سایر طرح‌های مشابه دارد.

۸. مراجع

- [1] Fridrich, J. "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps"; Int. J. of Bifurcation and Chaos 1998, 8, 1259-1284.
- [2] Yang, D.; Liao, X.; Wang, Y.; Yang, H.; Wei, P. "A Novel Chaotic Block Cryptosystem Based on Iterating Map with Output-Feedback"; Chaos, Solitons & Fractals 2009, 41, 505-510, 2009.
- [3] Patidar, V.; Sud, K. "A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing"; Electronic J. of Theoretical Physics 2009, 6, 327-344.
- [4] Mao, Y.; Chen, G.; Lian, S. "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps"; Int. J. of Bifurcation and Chaos 2004, 14, 3613-3624.

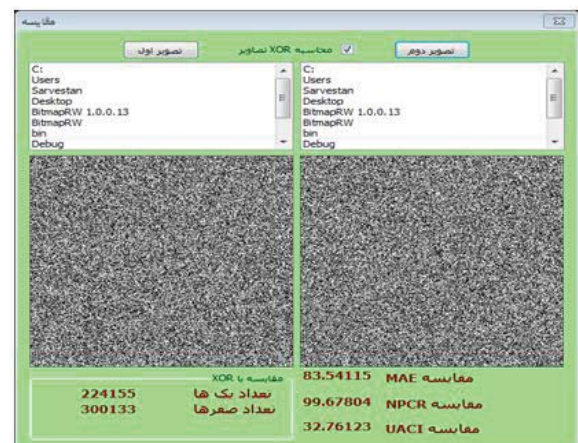
طرح SPK حداقل در پنج دور متوالی روی تصویر اصلی تکرار شوند [۱۷]. و از طرف دیگر از جدول (۱۸) دیده می‌شود که در SPK^+ حساسیت لازم در همان دور اول (یعنی SPK^{1+}) به وجود آمده است و نیازی به تکرار دوره‌های بیشتر نیست، بنابراین می‌توان از جدول (۱۸) به طور ضمنی نتیجه گرفت که سرعت رمزنگاری در SPK^+ نسبت به SPK ۵ برابر بیشتر شده است.

جدول ۱۶. نتایج تحلیل تصادفی بیت‌های تصویر رمزی در SPK^+

نام آزمون	میانگین (درصد)	مقدار خي دو	نتیجه آزمون
فراوانی	۱۰۰	۱/۰۱۰۱	قبول
فراوانی در یک بلوک	۱۰۰	۱/۰۱۰۱	قبول
رن	۱۰۰	۱/۰۱۰۱	قبول
طولانی‌ترین رن	۱۰۰	۱/۰۱۰۱	قبول
رتبه ماتریس دودویی	۱۰۰	۱/۰۱۰۱	قبول
تبدیل فوریه گسسته	۱۰۰	۱/۰۱۰۱	قبول
تطابق غیر همپوشان	۱۰۰	۱/۰۱۰۱	قبول
تطابق همپوشان	۱۰۰	۱/۰۱۰۱	قبول
ماورر	۱۰۰	۱/۰۱۰۱	قبول
فشرده‌گی لمپل-زیبو	۱۰۰	۱/۰۱۰۱	قبول
پیچیدگی خطی	۱۰۰	۱/۰۱۰۱	قبول
سربال	۱۰۰	۱/۰۱۰۱	قبول
آنتروپی تقریبی	۱۰۰	۱/۰۱۰۱	قبول
جمع‌های تجمعی جلورونده	۱۰۰	۱/۰۱۰۱	قبول
جمع‌های تجمعی عقب رونده	۱۰۰	۱/۰۱۰۱	قبول
گشت‌های تصادفی	۱۰۰	۱/۰۱۰۱	قبول
گشت‌های تصادفی متغیر	۱۰۰	۱/۰۱۰۱	قبول

جدول ۱۷. مقایسه تحلیل حساسیت تصویر رمزی نسبت به کلید در SPK^+

MAE	UACI	NPCR	SPK^+
۸۳/۵۴	۳۲/۷۶	۹۹/۶۷	



شکل ۴. حساسیت تصویر رمزی نسبت به کلید در SPK^+

- [14] Wang, X.; He, G. "Cryptanalysis on a Novel Image Encryption Method Based on Total Shuffling Scheme"; *Optics Communications* 2011, 284, 5804-5807.
- [15] Philip, M.; Das, A. "Survey of Image Encryption using Chaotic Cryptography Schemes"; *IICA Special Issue on Computational Science, New Dimensions and Perspectives, NCCSE*, 2011, 1, 1-4.
- [16] Sharma, M.; Kowar, M. K. "Image Encryption Techniques using Chaotic Schemes"; *International Journal of Engineering Science and Technology* 2010, 2, 2359-2363.
- [17] Mirghadri, A.; Jolfai, M. "A New Image Encryption Scheme with Chaotic Maps"; *Advanced Defence Sci. & Tech.* 1390, 2, 11-124 (In Persian).
- [18] Rukhin, A.; Soto, J.; Nechvatal, J.; Barker, E.; Leigh, S.; Levenson, M.; et al. "Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication"; 2010.
- [19] Addabbo, T.; Fort, A.; Kocarev, L.; Rocchi, S.; Vignoli, V. "Pseudo-Chaotic Lossy Compression of TRBGs"; *IEEE Int. Symposium on Circuits and Systems (ISCAS)*, 2011, 1980-1983.
- [20] Pazooki, M. "Evaluation of A New Image Encryption Scheme with Chaotic Maps"; MSc. Thesis, Imam Hossein Univ., 1392 (In Persian).
- [21] Stinson, D. R. "Cryptography, Theory and Practice"; 3rd Ed. Chapman & Hall/CRC Press, 2006.
- [22] Amani, P.; KhalooZade, H.; Aref, M. "Design of Alternative S-Box for AES with Application of Chaotic Maps", 6th Conference of Iranian society of Cryptology, 1386 (In Persian).
- [5] Liu, H.; Wang, X. "Color Image Encryption using Spatial Bit-Level Permutation and High-Dimension Chaotic System"; *Optics Communications* 2011, 284, 3895-3903.
- [6] Huang, C.; Nien, H. "Multi Chaotic Systems Based Pixel Shuffle for Image Encryption"; *Optics Communications* 2009, 282, 2123-2127.
- [7] Gao, T.; Chen, Z. "A New Image Encryption Algorithm Based on Hyper-Chaos"; *Physics Letters A* 2008, 372, 394-400.
- [8] Amin, M.; Faragallah, O.; Abd El-Latif, A. "A Chaotic Block Cipher Algorithm for Image Cryptosystems"; *Communications in Nonlinear Science and Numerical Simulation* 2010, 11, 3484-3497.
- [9] Zhou, Q.; Wong, KW.; Liao, X.; Xiang, T., Hu, Y. "Parallel Image Encryption Algorithm Based on Discretized Chaotic Maps"; *Chaos, Soliton & Fractals* 2008, 38, 1081-1091.
- [10] Giesl, J.; Vlcek, K. "Image Encryption Based on Strange Attractors"; *Int. J. Graph. Vis. Image Process* 2009, 2, 19-26.
- [11] Chattopadhyay, D.; Mandal, MK.; Nandi, D. "Robust Chaotic Image Encryption Based on Perturbation Technique"; *Int. J. Graph. Vis. Image Process* 2011, 2, 41-50.
- [12] Galatolo, S.; Hoyrup, M.; Rojas, C. "Statistical Properties of Dynamical Systems – Simulation and Abstract Computation", *Chaos, Solitons and Fractals* 2012, 45, 1-14.
- [13] Khadem, B. "Security and Performance Criterias for Chaotic Encryption"; *J. of Iranian Society of Cryptology (Monadi)*; winter and spring issue, 1393, 23-28 (In Persian).