مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۲، تابستان ۱۳۹۷، ص ۹۱-۸۳

عدم کارایی ضریب همبستگی پیرسن برای سنجش امنیت رمز نگاری تصویر

مجید فرهادی[1*]، حسین سبزه‌پرور[2]، جواد قاسمیان[3]

۱ و ۳- استادیار، دانشگاه دامغان، ۲- دانشجوی ارشد آماریاضی، دانشگاه علم و صنعت

(دریافت: ۹۶/۰۷/۱۴، پذیرش: ۹۶/۱۱/۰۹)

چکیده

در این مقاله عدم کارایی ضریب همبستگی پیرسن برای تحلیل ارتباط بین یک تصویر و تصویر رمزشده آن نشان داده شد. همچنین ضریب اطلاع به‌عنوان جایگزین مناسب برای ضریب همبستگی پیرسن مورد بررسی قرار گرفته شد. هر چند این ضعف مستقل از سامانه رمز استفاده‌شده در رمزنگاری تصویر می‌باشد، ولی دو الگوریتم رمز AES اصلاح‌شده و رمز جریانی W7 برای محاسبات آزمایشگاهی استفاده و همچنین با بررسی کمی و کیفی استانداردهای دیگر تحلیل رمزنگاری تصویر نشان داده می‌شود که ضریب اطلاع در مقایسه با ضریب همبستگی پیرسن نقاط قوت و ضعف الگوریتم‌های رمزنگاری تصویر را بهتر نشان می‌دهد.

واژه‌های کلیدی: رمزنگاری، رمزنگاری تصویر، ضریب همبستگی پیرسن، آنتروپی، ضریب اطلاع

۱- مقدمه

امروزه در دنیای دیجیتال حفاظت از اطلاعات نقش مهمی در تبادل داده‌ها و مبادلات تجاری ایفا می‌کند. از این رو برای تامین نیازهای امنیتی تراکنش از روش‌های رمزنگاری استفاده می‌شود. رمزنگاری تصویر به‌دلیل برخی ویژگی‌های ذاتی آن همچون همبستگی زیاد میان پیکسل‌ها و حجم بالای داده‌ها متفاوت از رمزنگاری متن است. لذا روش‌های کلاسیک رمزنگاری متن برای این منظور چندان کارآمد نیستند. از رمزهای کلید متقارن برای رمزنگاری تصویر استفاده می‌شود به‌طور مثال از رمزهای جریانی [۱] و همچنین از رمزهای بلوکی [۳-۲] برای رمزگذاری داده‌های تصویری استفاده شده است. از روش‌های مبتنی بر آشوب نیز اخیرا برای رمزگذاری داده‌های تصویری استفاده می‌شود [۸-۴]. از طرف دیگر بررسی اینکه آیا یک سامانه رمزنگاری تصویر امن است، سوالی اساسی می‌باشد. در مقالات کلاسیک رمزنگاری تصویر مولفه هایی برای بررسی امنیت مورد توجه قرار گرفته‌اند. دو مولفه اساسی، یکی آنتروپی و دیگری همبستگی می‌باشد که هر دو مولفه هایی آماری هستند. ضریب همبستگی ابزاری آماری برای تعیین نوع و درجه رابطه یک متغیر کمی با متغیر کمی دیگر است. ضریب همبستگی شدت رابطه و همچنین نوع رابطه (مستقیم یا معکوس) را نشان می‌دهد. این ضریب که کاربرد فراوانی در آمار و رمزنگاری دارد، توسط کارل پیرسن براساس ایده اولیه فرانسیس گالتون تدوین شد [۱۰-۹]. در این مقاله به بررسی ناکارایی ضریب همبستگی پیرسن برای تعیین امنیت رمزنگاری تصویر پرداخته شده است. البته بحث ناکارایی ضریب همبستگی پیرسن مستقل از سامانه رمزگذاری تصویر می‌باشد اما برای مقایسه کارایی ضریب پیرسن از سامانه رمزنگاری AES اصلاح شده و رمز جریانی W7 استفاده شده است [۳-۲].

محک‌های دیگری برای تحلیل امنیت و کارایی رمزنگاری تصویر استفاده می‌شوند محک‌هایی مانند PSNR که برای بررسی کیفیت و پایداری تصویر مورد استفاده قرار می‌گیرند [۶]. همچنین برای بررسی مقاومت رمزنگاری تصویر در برابر حملات تفاضلی از محاسبه NPCR و UACI استفاده می‌شود.

پیشنهاد نویسندگان این مقاله در این مقاله استفاده از ضریب اطلاع به جای ضریب همبستگی پیرسن برای اندازه‌گیری وابستگی میان تصویر اصلی و تصویر رمزشده می‌باشد که این موضوع را هم به‌دلیل محاسبات پنج تصویر نمونه و هم به علت ناکارایی ضریب همبستگی پیرسن برای بعضی از خانواده‌های توزیع‌های آماری نشان داده می‌شود [۱۱].

ساختار این مقاله به‌صورت زیر می‌باشد. ابتدا در بخش اول مقدمه، در بخش دوم معرفی مفهوم رمزنگاری تصویر و سامانه‌های رمز AES و AES اصلاح‌شده و همچنین رمز جریانی

*رایانامه نویسنده مسئول: farhadi@du.ac.ir

W7، بخش سوم همبستگی و ابزار محاسبه آن که شامل ضریب همبستگی پیرسن و ضریب اطلاع می‌باشد، بخش چهارم شاخص‌های کمی مقایسه، بخش پنجم محاسبات شاخص‌های کمی، بخش ششم تحلیل محاسبات و در نهایت بخش هفتم نتیجه‌گیری بیان شده است.

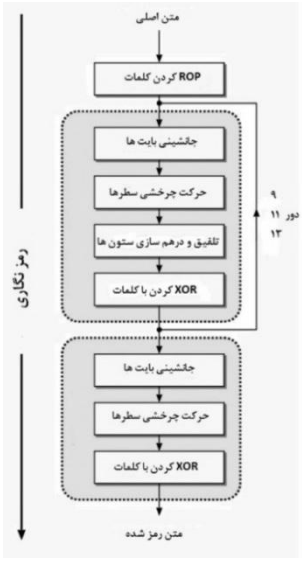
۲- رمز نگاری

۲-۱- رمزگذاری تصویر

در این مقاله رمزگذاری تصویر برای تصاویر خاکستری بیان شده است. بدین صورت که تصاویر با یک ماتریس در ابعاد تصویر نمایش داده می‌شود و درایه‌های این تصویر تنها نشان‌دهنده میزان روشنایی و تیرگی و سایه‌های تصویر هستند. درایه‌های این تصویر با عددی بین صفر تا ۲۵۵ نشان داده می‌شوند و یک نمایش ۸ بیتی دارد که در آن صفر برای سطح شدت سیاه و ۲۵۵ برای سطح شدت سفید می‌باشد. در این روش ابتدا درایه‌های تصویر را به‌صورت یک بردار در نظرگرفته و سپس با جایگزینی ارزش بیتی، هر یک از پیکسل‌ها به‌صورت برداری از صفر و ۱ در می‌آید. در ادمه این بردارها به بلوک‌هایی با طول مشخص با توجه به سامانه رمزنگاری در آورده شده است و سپس بلوک‌ها تک تک رمزگذاری و رمزگشایی شده‌اند [۲].

۲-۲- الگوریتم استاندارد رمز نگاری پیشرفته

الگوریتم استاندارد رمزنگاری پیشرفته[1] که به نام الگوریتم رایندال[2] نیز شناخته شده است، یک الگوریتم رمز متقارن و بلوکی است که دارای کلیدی با طول ۱۲۸، ۱۹۲ یا ۲۵۶ بیت می‌باشد. تعداد مراحل رمزنگاری AES به ترتیب با توجه به طول کلید ۱۰، ۱۲ یا ۱۴ می‌باشند [۳].



شکل (۱): مراحل پیاده سازی رمز AES

1- AES : Advanced Encryption Standard
2- RijnDael

۲-۳- سامانه استاندارد رمزنگاری پیشرفته اصلاح‌شده[3]

این طرح توسط الگوریتم AES و یک مولد جریانی کلید، تشکیل شده است. ابتدا در الگوریتم AES به جای استفاده از مرحله تلفیق و درهم‌سازی ستون‌ها[4] از یک مرحله جایگشت استفاده شده است. مرحله تلفیق و درهم‌سازی ستون‌ها باعث امنیت بهتری در الگوریتم می‌شود اما محاسبات زیادی دارد که الگوریتم را کند می‌کند. در نتیجه با حذف این مرحله و استفاده از یک مرحله جایگشت، الگوریتم سریع‌تر خواهد بود [۶]. الگوریتم رمزنگاری استاندارد رمزنگاری داده[5] جدول جایگشت را برای ما فراهم می‌کند. ورودی جدول جایگشت ۶۴ بیت است ولی خروجی مرحله چرخشی سطرها ۱۲۸ بیت است برای حل این مشکل ابتدا بلوک ۱۲۸ بیتی به دو بلوک ۶۴ بیتی تقسیم خواهد شد و هر بلوک به‌طور جداگانه زیر مرحله جایگشت فرستاده می‌شود. در این جدول جایگاه بیت‌ها به ترتیب مشخص شده‌اند به‌طوری که بیت جایگاه ۱ در ورودی به جایگاه ۵۸ و بیت جایگاه ۹ به جایگاه ۶۰ در خروجی و جایگاه ۶۴ به جایگاه ۷ در خروجی می‌رود سپس خروجی دو بلوک ۶۴ بیتی با هم الحاق شده و یک بلوک ۱۲۸ بیتی تشکیل می‌شود. جدول جایگشت IP در زیر می‌آید . با اعمال این تغییر، زمان رمزگذاری کاهش می‌یابد [۳ و ۱۲].

جدول (۱): جدول جایگشت IP

۵۸	۵۰	۴۲	۳۴	۲۶	۱۸	۱۰	۲
۶۰	۵۲	۴۴	۳۶	۲۸	۲۰	۱۲	۴
۶۲	۵۴	۴۶	۳۸	۳۰	۲۲	۱۴	۶
۶۴	۵۶	۴۸	۴۰	۳۲	۲۴	۱۶	۸
۵۷	۴۹	۴۱	۳۳	۲۵	۱۷	۹	۱
۵۹	۵۱	۴۳	۳۵	۲۷	۱۹	۱۱	۳
۶۱	۵۳	۴۵	۳۷	۲۹	۲۱	۱۳	۵
۶۳	۵۵	۴۷	۳۹	۳۱	۲۳	۱۵	۷

۲-۴- الگوریتم رمز W7

الگوریتم رمز ، W7 یک الگوریتم رمز جریانی با کلید متقارن است که طول کلید آن ۱۲۸بیت است. رمز W7 شامل ۸ حالت مشابه است. هر حالت شامل سه LFSR[6] و یک تابع اکثریت است که ۱۲۸بیت کلید را به عنوان ورودی گرفته و یک بیت خروجی را

3- Modified AES
4- Mixcolumns
5- DES: Data Encryption Standard
6- Linear-Feedback Shift Register

تولید می‌کنند که با کنار هم قرار دادن ۸ بیت، یک بایت از رشته کلید مورد نظر تولید می‌شود [۱۴-۱۳،۵].

۳- همبستگی و ابزار محاسبه آن

برای محاسبه میزان وابستگی بین متغیرهای تصادفی و به تبع آن داده‌های مشاهده شده، روش‌های متعددی وجود دارد که از میان آنها می‌توان به ضریب کندال[۱]، ضریب اسپیرمن[۲]، ضریب پیرسن[۳] و ... اشاره کرد که در این مقاله بر ضعف ضریب پیرسن برای سنجش میزان وابستگی میان تصویر اصلی با تصویر رمزشده اشاره، و جایگزینی برای آن معرفی شده است .

۳-۱- ضریب همبستگی خطی پیرسن

دو متغیر تصادفی X و Y را با میانگین‌های μ_X و μ_Y، واریانس‌های $\sigma_X{}^2$ و $\sigma_Y{}^2$ و کوواریانس σ_{XY} در نظر گرفته می‌شود. مولفه

$$\rho = \frac{\sigma_{XY}}{\sigma_X \sigma_Y} \qquad (۱)$$

ضریب همبستگی ساده نامیده می‌شود.

برآورد گشتاوری ضریب همبستگی ساده، به ضریب همبستگی گشتاوری پیرسن شهرت دارد و به‌صورت زیر تعریف می‌شود.

$$R = \frac{S_{XY}}{S_X S_Y} \qquad (۲)$$

هرگاه به جای نمونه تصادفی یافته‌های (برآورد) آن گذاشته شود یافته متغیر تصادفی R که آن‌را با r نشان می‌دهند و در عمل به کار می‌رود به‌دست می‌آید.

ضریب همبستگی هنگامی که برای یک نمونه محاسبه می‌شود به وسیله r نمایش داده و به‌صورت ضریب همبستگی نمونه یا ضریب همبستگی نمونه‌ای پیرسن خوانده می‌شود و به صورت زیر به‌دست می‌آید:

$$r = \frac{s_{XY}}{s_X s_Y} = \frac{\overline{xy} - \bar{x}\bar{y}}{\sqrt{\overline{x^2} - \bar{x}^2}\sqrt{\overline{y^2} - \bar{y}^2}} = \frac{n\sum xy - \sum x \sum y}{\sqrt{(n\sum x^2) - ((\sum x)^2)(n\sum y^2) - ((\sum y)^2)}} \qquad (۳)$$

ضریب همبستگی همواره بین ۱- و ۱+ است و هنگامی که صفر شود و یا به سمت صفر میل کند بدین معنا است که وابستگی میان داده‌های ما کم است و وقتی که برابر ۱+ یا ۱- شود و یا به سمت آنها میل کند یعنی وابستگی در حال افزایش است [۱۷-۱۵].

در این مقاله x یافته‌های تصویر اصلی و y یافته‌های تصویر رمز شده است.

۳-۲- ایرادات ضریب همبستگی پیرسن

ضریب همبستگی پیرسن دارای مشکلات و محدودیت‌های زیادی است. این ضریب نسب به شکاف تصویر[۴]، بالشتک‌سازی تصویر[۵] و سایه روشن‌ها[۶] در سامانه‌های تصویربرداری حساس است. این موارد به خصوص در اسکن الکترونی[۷] تصاویر میکروسکوپی رایج است آن هم به‌دلیل پیچیدگی‌های غیرخطی اپتیکی- الکترونی که در سامانه تصویربرداری وجود دارد می‌باشد. همچنین شکاف تصویر هنگامی رخ می‌دهد که یک تصویر در یک جهت هنگام تصویربرداری حرکت کند برای مثال هنگام تصویربرداری رفتار سلول‌ها در زیر میکروسکوپ که منجر به گرفتن تصاویر پشت سر هم شده و تغییرات جزیی، تصویربرداری می‌شود و یا بالشتک‌سازی زمانی است که لبه‌های تصویر مقعر باشد همچنین سایه روشن زمانی است که یک کاهش در شدت تصویر در نزدیکی لبه به‌دلیل سنجش جمع‌آوری اپتیکی نور رخ دهد که هر دوی این‌ها در روش نهان نگاری[۸] مشهود است.

مشکل دیگری که اغلب در کاربردهای عملی نادیده گرفته شده است این است که r تعریف نشده باشد. هنگامی که تقسیم بر صفر شود و این زمانی رخ می‌دهد که یکی از تصاویر آزمایش ثابت و دارای شدت رنگ یکنواخت باشد.

یکی دیگر از مشکلات ضریب همبستگی پیرسن میزان اریب بودن آن است بدین صورت که درهنگام محاسبه دو تصویر که دارای خطای بالقوه می‌باشند عملکرد مناسبی نخواهد داشت. پیچیدگی‌های تفسیری، حساسیت زیاد برای نویز پیکسل‌ها و افزایش اختلاف بین آنها، مشکل پرداختن به منابع نوری متحرک، رفتار نامطلوب برای تصاویر حاوی ساختار با انسجام خیلی زیاد یا با انسجام خیلی کم و مشکل برخورد با تصاویر دارای اختلاف شیب سه‌بعدی قوی، از جمله این مشکلات است [۱۸].

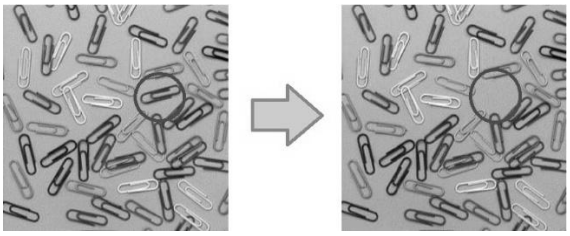
علاوه بر آن در مراجع [۱۱و ۱۹] مشکلات و محدودیت‌های ضریب همبستگی پیرسن به‌صورت زیر فهرست شده است:

۱- گاهی اوقات هنگامی که متغیرها مستقل نباشند ضریب

1- Kendall Coefficient
2- Spearman Coefficient
3- Pearson Coefficient

4- Image Skewing
5- Image Pincushioning
6- Vignetting
7- Electron Scan
8- Watermarking

پیرسن صفر می‌شود.
۲- هنگامی که متغیرها دارای همبستگی کامل باشند ضریب پیرسن ممکن است یک نشود.
۳- برای تبدیل غیرخطی از متغیرها ضریب پیرسن تغییر می‌کند.
۴- وابستگی بین دو متغیر کیفی در یک جدول توافقی را نمی‌توان بر حسب ضریب همبستگی بیان کرد.
۵- در بعضی موارد، شاید ضریب پیرسن وجود نداشته باشد (برای بعضی خانواده توزیع‌ها).
مثال: دو تصویر زیر را در نظر بگیرید.



شکل (۲): مثال برای عدم دقت تشخیص ضریب همبستگی پیرسن [۱۸]

شکل (۲) یک مثال واضح از شکست ضریب همبستگی برای تشخیص تغییرات در یک تصویر را نشان می‌دهد. شناختن قطعه‌های منحصر به فرد از دست رفته، برای برنامه‌های کاربردی مانند برچسب‌های بازتابنده ذرات[1] حیاتی است. آنها از ذرات کوچک و بازتابنده متصل به یک جسم تشکیل شده‌اند. RPT ها اثر انگشت یکپارچه را براساس توزیع فضایی پیچیده خود به‌وجود می‌آورند.

شکل سمت چپ یک تصویر ۸ بیتی تک رنگ با ابعاد ۵۱۲×۵۱۲ پیکسل است. این تصویر با مجموعه‌ای از کلیپس‌های کاغذ پلاستیکی و به‌صورت تصادفی بر روی یک سطح نشان داده شده است. شکل سمت راست همان تصویر سمت چپ را نشان می‌دهد به جز اینکه یکی از کلیپس‌های کاغذ از این تصویر حذف شده است. ضریب همبستگی پیرسن بین شکل اول و شکل دوم برابر ۰/۹۸ است که این خود نشان از ضعف در تشخیص قطعات از دست رفته است.

۳-۳- معیار واگرایی کولبک

در آمار ریاضی از معیار واگرایی کولبک لایر[2] به‌عنوان معیاری برای اندازه‌گیری واگرایی یک توزیع احتمال از یک توزیع احتمال ثانویه، یاد می‌شود از جمله کاربردهای این مفهوم شامل توصیف آنتروپی نسبی شانون در سامانه‌های اطلاعاتی، تصادفی بودن در سری‌های زمانی پیوسته و بهره اطلاعاتی هنگامی که به مقایسه با مدل‌های آماری استنباطی پرداخته می‌شود، می‌باشد. این معیار، یک معیار نامتقارن می‌باشد و در نتیجه نمی‌توان آن را به‌عنوان یک معیار پراکندگی معرفی کرد. به‌عبارت دیگر، مقدار صفر برای معیار واگرایی کولبک-لایر نشان می‌دهد که انتظار می‌رود رفتار مشابهی و نه دقیقا یکسان از دو توزیع داشته باشد در حالی که مقدار ۱ برای این معیار نشان می‌دهد که دو توزیع رفتارهای متضادی دارند. مفهوم واگرایی کولبک-لایر در اصل توسط سالومان کولبک[3] و ریچار لایر[4] در سال ۱۹۵۱ به عنوان واگرایی جهت‌دار بین دو توزیع معرفی گردید. نام‌های دیگر این اندازه آنتروپی نسبی[5]، آنتروپی متقاطع[6] و واگرایی کولبک لایر[7] است [۲۰]. واگرایی کولبک لایر توزیع f_1 نسبت به f_2 اغلب به‌صورت $\mathrm{D}(f_1:f_2)$ نوشته می‌شود. در حوزه ماشین افزار از $\mathrm{D}(f_1:f_2)$ عموما به نام بهره اطلاعاتی حاصله به شرطی که به‌جای توزیع f_1 از توزیع f_2 استفاده شود، یاد می‌شود. از منظر نظریه اطلاع، به این مسئله آنتروپی نسبی از توزیع f_1 با توجه به توزیع f_2 گفته می‌شود. در حوزه نظریه کدگذاری یا رمزنگاری، $\mathrm{D}(f_1:f_2)$ می‌تواند به‌عنوان معیاری برای اندازه‌گیری متوسط تعداد بیت‌های اضافی مورد نیاز به‌منظور کد کردن نمونه‌ای از توزیع f_1 با استفاده از یک کد بهینه‌سازی‌شده برای توزیع f_2 به‌جای استفاده از کد بهینه‌سازی‌شده برای f_1 باشد. از منظر استنتاج بیزین $\mathrm{D}(f_1:f_2)$ ، یک معیار اندازه‌گیری اطلاع کسب‌شده هنگامی که یک اصلاح از توزیع پیشین احتمال f_2 به توزیع پسین احتمال f_1 رخ دهد. به‌عبارت دیگر، مقداری از اطلاع است که به واسطه تقریب زدن f_1 در هنگامی که از f_2 برای آن استفاده می‌شود، می‌باشد. در عمل، f_1 به‌طور معمول نشان‌دهنده توزیع صحیح داده‌ها، مشاهدات یا یک توزیع تئوری می‌باشد که دقیق محاسبه شده است، در حالی که f_2 به‌طور معمول نشان‌دهنده یک نظریه، مدل، توصیف یا تقریبی از f_1 می‌باشد. به‌منظور پیدا کردن یک توزیع f_2 که نزدیک‌ترین توزیع به f_1 باشد، می‌توان به دنبال محاسبه توزیعی گشت که معیار واگرایی کولبک لایر را کمینه کند [۲۳-۲۱].

$f_1(x)$ و $f_2(x)$ دو تابع چگالی احتمال می‌باشند. بنابراین اندازه معیار واگرایی کولبک به‌صورت زیر نوشته می‌شود:

$$\mathrm{D}(f_1:f_2) = \int f_1(x) \ln \frac{f_1(x)}{f_2(x)}\, dx \qquad (۴)$$

1- RPTS
2- Kullback- Leibler divergence

3- Solomon Kullback
4- Richard Leibler
5- Relative Entropy
6- Cross Entropy
7- KL Divergence

۳-۴- اندازه نرمال‌شده اطلاع دوطرفه تعمیم‌یافته

بر اساس الگوی کاپور و دانـد [۱۹ و ۲۴]، کیم [۲۵] شاخص وابستگی[1] یا ضریب اطلاع[2] را به عنوان اندازه نرمال‌شده‌ای از اطلاع دو طرفه تعمیم یافته[3] $D(f_1:f_2)$ ، به‌صورت زیر تعریف کرد [۲۶-۲۷]:

$$DI = 1 - e^{-D(f_1:f_2)} \qquad (۵)$$

که

۱- $0 \le DI \le 1$
۲- مقدار $DI = 0$ اگر و فقط اگر f_1 از f_2 متمایز نباشد. بدین معنی که وابستگی کامل است.
۳- هرگاه $D(f_1:f_2)$ به‌طور نامتناهی افزایش یابد DI به ۱ میل می‌کند. بدین معنی که عدم وابستگی کامل است.

در رمزنگاری تصویر متغیرهای تصادفی که در این مقاله X در نظر گرفته شده است مقادیری بین ۰ تا ۲۵۵ می‌باشند و چه در تصویر اصلی و چه در تصویر رمزشده این مقادیر یکسان و فقط در بازه ۰ تا ۲۵۵ تغییر می‌کنند به همین جهت اطلاع دو طرفه را بر مبنای تک متغیره (فقط X) محاسبه می‌کنیم.

۴- شاخص‌های کمی مقایسه

در این قسمت به چند شاخص کمی برای مقایسه بین تصویر اصلی و تصویر رمزشده به غیر از ضریب همبستگی پیرسن پرداخته شد.

آنتروپی یکی از بهترین مشخصه‌ها برای اندازه‌گیری میزان تصادفی بودن داده‌ها (پیکسل‌ها) و پراکندگی آنها در تصویر اصلی و تصویر رمزشده است. میانگین میزان اطلاعاتی که در هر تصویر دریافت می‌شود به‌صورت زیر است [۲۰-۲۱]:

$$H(x) = \int_0^{255} f(x)\log(\frac{1}{f(x)}) \qquad (۶)$$

و چون برای تصاویر خاکستری محاسبه می‌شود بنابراین $x \in [0,255]$.

شاخص دیگر مورد استفاده میزان خطای بین تصویر اصلی و تصویر رمزشده به‌وسیله میانگین مربع خطای[4] قابل محاسبه است که فرمول آن به‌صورت زیر است:

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}(p(i,j)-q(i,j))^2 \qquad (۷)$$

1- Dependence Index: Di
2- Information Index
3- Normal Size of Generalized Mutual Information
4- Mse: Mean Square Error

که در آن q(i,j) و p(i,j) نشان‌دهنده عددهای رنگ پیکسل و (i,j) موقعیت‌های تصویر اصلی و تصویر رمزشده می‌باشند [۶].

و در نهایت نتیجه حاصل از حداکثر نسبت سیگنال به نویز[5] یک مقایسه بین کیفیت تصویر اصلی و تصویر رمز شده است و یک روش استاندارد برای محاسبه میزان پایداری تصویر می‌باشد و به‌صورت زیر قابل محاسبه است:

$$PSNR = 20*\log[\frac{I_{MAX}}{\sqrt{MSE}}] \qquad (۸)$$

که، I_{MAX} بیشترین مقدار از پیکسل‌ها بوده که در محاسبه، برای تصاویر خاکستری ۸ بیت برابر ۲۵۵ می‌باشد. مقدار زیاد PSNR نشان‌دهنده کیفیت بالا و پایداری تصویر و مقدار کم آن نشان‌دهنده تفاوت عددی زیاد بین تصویر اصلی و تصویر رمز شده است که در رمز نگاری تصویر این مقادیر باید کم باشد که دلیلی بر کیفیت تصویر رمز شده است [۶] .

در رمزنگاری تصویر، مقاومت رمزنگاری نسبت به حملات تفاضلی معمولا از طریق نرخ تغییرات پیکسل‌ها[6] و نرخ میانگین یکپارچه تغییرات[7] محاسبه می‌شود به‌طوری که این دو مقوله جهت آزمایش اثر تغییر یک پیکسل ورودی بر روی تمام تصویر رمزشده به وسیله الگوریتم رمز می‌باشند و به‌صورت زیر قابل محاسبه‌اند [۲۸-۲۹]:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} d(i,j)}{m \times n} \times 100\% \qquad (۹)$$

$$UACI = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\left|p(i,j) - q(i,j)\right|}{255} \times 100\% \qquad (۱۰)$$

که در آن، p و q پیکسل‌های تصویر اصلی و تصویر رمزشده هستند و d به‌صورت زیر تعریف می‌شود:

$$d(i,j) = \begin{cases} 0 & p(i,j) = q(i,j) \\ 1 & p(i,j) \neq q(i,j) \end{cases} \qquad (۱۱)$$

مقدار $NPCR$ برابر $(NPCR \le 99.6)$ بدین معنی که موقعیت‌های پیکسل‌ها بین تصویر اصلی و تصویر رمزشده به‌طور زیادی تصادفی هستند همچنین مقدار مناسب برای $UACI$ برابر $(UACI \ge 33.3)$ می‌باشد بدین معنی که بیشتر سطوح خاکستری پیکسل‌ها در تصویر رمزشده تغییر کرده و مخلوط شده‌اند.

5- Psnr: Peak Signal to Noise Ratio
6- Npcr: The Number of Pixels Change Rate
7- Uaci: The Unified Average Changing Intensity

۵- محاسبات

برای ۵ تصویر با اندازه ۶۴×۶۴ و خاکستری ابتدا به‌وسیله نرم‌افزار متلب تصاویر فراخوانی شدند و سپس تصاویر به‌وسیله دو الگوریتم Modified AES و W7 به‌صورت پیکسل به پیکسل رمزگذاری شدند و در مراحل بعد برای تصویر اصلی و تصاویر رمزشده یک توزیع آماری مناسب پیدا کرده و با استفاده از این توزیع‌ها و فرمول‌های بالا محاسبات انجام شد.

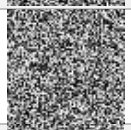
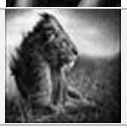
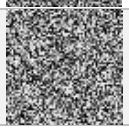
۵-۱- گام اول

تصاویر اصلی به‌وسیله الگوریتم‌های پیشنهادی رمز و در جدول (۲) ارائه شده است.

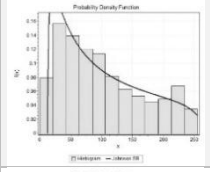
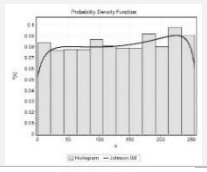
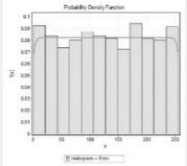
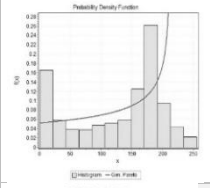
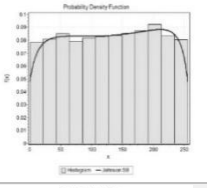
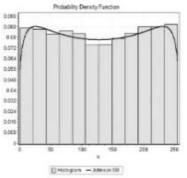
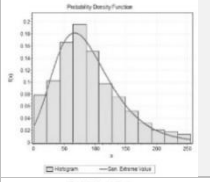
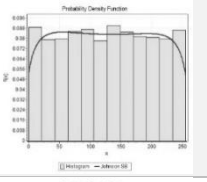
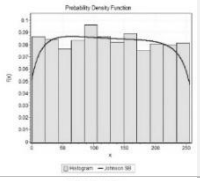
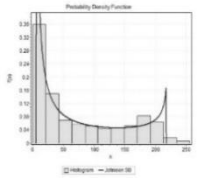
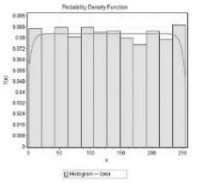
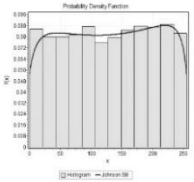
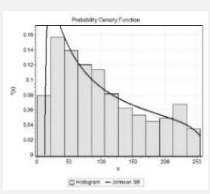
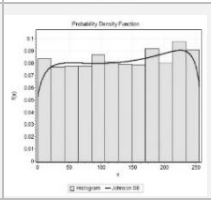
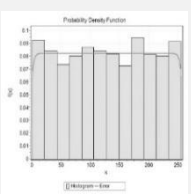
۵-۲- گام دوم

توزیع‌های آماری برای تصاویر اصلی و رمزشده محاسبه شده است که با توجه به [۱۱] می‌توان گفت تمام توزیع‌های به‌دست‌آمده برای تصاویر جزو خانواده‌هایی بودند که برای به‌دست آوردن ضریب همبستگی پیرسن مناسب نبوده و نتایج درستی را نمی‌دهند.

جدول(۲): جدول تصاویر اصلی و تصاویر رمزشده متناظر با الگوریتم‌های پیشنهادی

نام تصاویر	تصویر اصلی	تصویر رمزشده با سامانه رمز AES اصلاح‌شده	تصویر رمزشده با سامانه رمز جریانی W7
Veniz			
Young girl 1			
London			
Young girl 2			
Loin			

جدول(۳): جدول توزیع‌ها

نام تصاویر	نمودار تصویر اصلی	نمودار تصویر رمز شده با سامانه Modified	نمودار تصویر رمز شده با سامانه W7
Veniz	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Error 
Young girl 1	تابع توزیع آماری: Gen pareto 	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Johnson SB 
London	تابع توزیع آماری: Gen extreme value 	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Johnson SB 
Young girl 2	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Error 	تابع توزیع آماری: Johnson SB 
Lion	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Johnson SB 	تابع توزیع آماری: Error 

۵-۳- گام سوم

میزان آنتروپی برای تصاویر اصلی و رمزشده با استفاده از توابع توزیع احتمالی محاسبه (جدول ۴) و همچنین میزان ضریب همبستگی پیرسن و شاخص‌های کمی مقایسه (جدول ۵ و ۶) به‌دست آورده شده است.

جدول(۴): جدول آنتروپی تصاویر

نام تصویر	آنتروپی تصویر اصلی	سامانه رمز	آنتروپی تصویر رمزشده
Veniz	۵/۹۳۷۰	**Modified**	۵/۵۱۱۴
		W7	۵/۵۲۰۰
Young girl 1	۵/۹۳۷۰	**Modified**	۵/۵۳۲۰
		W7	۵/۵۵۲۵
London	۵/۱۴۶۹	**Modified**	۵/۳۹۰۷
		W7	۵/۳۳۳۶
Young girl 2	۴/۷۶۴۳	**Modified**	۵/۴۵۱۱
		W7	۵/۵۱۴۵
Lion	۴/۷۶۴۳	**Modified**	۵/۵۵۶۲
		W7	۵/۴۱۱۳

جدول (۵): جدول ضریب همبستگی پیرسن و شاخص های کمی MSE و PSNR

نام تصویر	تصویر اصلی در مقابل تصویر رمز شده	ضریب همبستگی پیرسن	MSE	PSNR
Veniz	**Main vs modified**	-۰/۰۰۳۸	۹/۹۷۷۹e +۰۳	۸/۱۴۰۴
	Main vs W7	-۰/۰۰۶۲	۱/۰۰۹۰e+۰۴	۸/۰۹۱۷
Young girl 1	**Main vs modified**	-۰/۰۰۲۸	۱/۰۶۸۲e+۰۴	۷/۸۴۴۱
	Main vs W7	-۰/۰۱۲۳	۱/۱۱۰۸e+۰۴	۷/۶۷۴۳
London	**Main vs modified**	-۰/۰۲۳۲	۹/۸۹۰۴e+۰۳	۸/۱۷۸۷
	Main vs W7	-۰/۰۰۸۰	۹/۵۹۲۴e+۰۳	۸/۳۱۱۵
Young girl 2	**Main vs modified**	-۰/۰۲۶۹	۱/۳۵۰۴e+۰۴	۶/۸۲۶۱
	Main vs W7	-۰/۰۱۷۹	۱/۳۲۴۷e+۰۴	۶/۹۰۹۶
Lion	**Main vs modified**	-۰/۰۰۱۴	۱/۱۰۶۳e+۰۴	۷/۶۹۲۱
	Main vs W7	۰/۰۱۱۱	۱/۰۷۶۳e+۰۴	۷/۸۱۱۶

جدول (۶): جدول مقادیر NPCR و UACI

نام عکس	تصویر رمزشده با AES اصلاح‌شده			
	NPCR		UACI	
	Score	P-value	Score	P-value
Veniz	۹۹/۶۸	۰/۷۷۳۸۱	۳۱/۸۶	۱.۵۴۹۱e-۰۵
Young girl 1	۹۹/۵۶	۰/۳۰۸۱	۳۳/۱۳	۰/۳۶۸۶
London	۹۹/۴۳	۰/۰۳۹۷۶	۳۱/۹۷	۵.۵۵۹۰e-۰۵
Young girl 2	۹۹/۴۸	۰/۱۰۵۲	۳۷/۴۸	۰
Lion	۹۹/۵۸	۰/۴۰۱۱	۳۳/۷۳	۰/۴۵۵۶
نام عکس	تصویر رمز شده با W7			
	NPCR		UACI	
	Score	P-value	Score	P-value
Veniz	۹۹/۵۸	۰/۴۰۱۱	۳۲/۳۰	۰/۰۰۱۷
Young girl 1	۹۹/۵۸	۰/۴۰۱۱	۳۳/۷۴	۰/۴۳۹۲
London	۹۹/۷۰	۰/۸۴۱۸	۳۱/۲۷	۳/۰۴۰۴e-۰۹
Young girl 2	۹۹/۶۰	۰/۵۰۰۰	۳۶/۹۶	۰
Lion	۹۹/۷۰	۰/۸۴۱۸	۳۳/۲۴	۰/۵۴۶۱

۵-۴- گام چهارم

میزان آنتروپی متقاطع و ضریب اطلاع (جدول ۷) برای تصاویر اصلی و رمزشده، با استفاده از تابع‌های توزیع احتمالی محاسبه شده است

جدول (۷): جدول آنتروپی متقاطع و ضریب اطلاع

نام عکس	تصویر رمزشده با AES اصلاح‌شده		تصویر رمزشده با W7	
	آنتروپی متقاطع	ضریب اطلاع	آنتروپی متقاطع	ضریب اطلاع
Veniz	۰/۱۷۳۹	۰/۱۵۹۶	۰/۳۹۳۲	۰/۳۲۵۱
Young girl 1	۰/۵۲۱۶	۰/۴۰۶۴	۰/۴۸۶۸	۰/۳۸۵۴
London	۰/۲۸۸۱	۰/۲۵۰۳	۰/۲۹۴۹	۰/۲۵۵۴
Young girl 2	۰/۴۳۳۵	۰/۳۵۱۸	۰/۴۵۶۲	۰/۳۶۶۳
Lion	۰/۳۱۷۵	۰/۲۷۲۰	۰/۳۲۶۱	۰/۲۷۸۳

۶- تحلیل محاسبات

با توجه به جدول آنتروپی مشاهده می‌کنیم که در تصاویر Veniz و Young girl 1 به علت پراکندگی شدید پیکسل‌ها، آنتروپی به ترتیب از ۵/۹۳۷۰ و ۵/۹۳۷۰ برای سامانه رمز AES اصلاح‌شده به ۵/۵۱۱۴ و ۵/۵۳۲۰ و همچنین برای سامانه رمز **W7** به ۵/۵۲۰۰ و ۵/۵۵۲۵ کاهش یافته (جدول ۴) در حالی که در سامانه رمز معمولا ما با افزایش آنتروپی روبرو هستیم و همچنین به این نکته باید توجه کرد که با توجه به کاهش آنتروپی، میزان ضریب همبستگی برای تصاویر اصلی و سامانه رمز AES اصلاح‌شده به ترتیب ۰/۰۰۳۸- و ۰/۰۰۲۸- می‌باشد، همچنین به‌طور مشابه برای تصاویر اصلی و سامانه رمز W7 برابر ۰/۰۰۶۲-

و ۰/۰۱۲۳می‌باشد که نزدیک به صفر است و این بدین معنی است که ضریب همبستگی پیرسن نتیجه قابل قبولی را ارائه نکرده است. همچنین در مورد تصاویر London، Young girl 2 و Lion، الگوریتم رمز، مقدار آنتروپی را به‌ترتیب از ۵/۱۴۶۹، ۴/۷۶۴۳ و ۴/۷۶۴۳ برای سامانه رمز modified به ۵/۳۹۰۷، ۵/۴۵۱۱ و ۵/۵۵۶۲ و همچنین برای سامانه رمز **W7** به ۵/۳۳۳۶، ۵/۵۱۴۵ و ۵/۴۱۱۳، افزایش (جدول ۴) و مقدار ضریب همبستگی را برای تصاویر اصلی و سامانه رمز modified (به‌ترتیب ۰/۰۲۳۲-، ۰/۰۲۶۹- و ۰/۰۰۱۴-) و همچنین به‌طور مشابه برای تصاویر اصلی و سامانه رمز W7 (به ترتیب ۰/۰۰۸۰-، ۰/۰۱۷۹و ۰/۰۱۱۱) کاهش داده است (جدول ۵). بنابراین میزان امنیت این دو سامانه رمز از نظر ضریب پیرسن قابل قبول است. در صورتی که به‌دلیل وجود سایه روشن‌هایی که در تصویر وجود دارد و همچنین کاهش در شدت تصویر در نزدیکی لبه [۱۶، ۱۸] و این نکته که برای هیچ یک از خانواده توزیع‌های آماری به‌دست آورده شده تصاویر [۱۱]، ضریب همبستگی پیرسن معتبر نیست، می‌توان گفت این ضریب کارایی لازم را ندارد و نتایج غیردقیقی را می‌دهد در مقابل ضریب اطلاع از میزان وابستگی بین تصاویر و تصاویر رمزشده خود اطلاع می‌دهد که می‌توان گفت این ضریب از دقت عملکرد بالایی برخوردار است (جدول ۷)[1]. با توجه به جدول خطا و حداکثر نویز (جدول ۵)، از PSNR می‌توان نتیجه گرفت که کیفیت بین تصاویر اصلی و رمزشده به‌دلیل کم بودن مقدار عددی آن، نسبتا کم بوده و ناپایدار است و تصاویر رمزشده به‌صورت بصری تقریبا قابل تشخیص نیستند. با توجه به جدول (۶) مقدار NPCR برای تصاویر رمزشده با AES اصلاح‌شده به غیر از تصویر Veniz (با مقدار ۹۹/۶۸) مابقی مقادیر کمتر از ۹۹/۶ می باشند بدین معنی که موقیت‌های پیکسل‌ها بین تصویر اصلی و تصویر رمزشده به‌طور زیادی تصادفی نیستند و همچنین برای تصاویر رمزشده با W7 تصاویر Veniz و Young girl 1 (با مقادیر ۹۹/۵۸ و ۹۹/۵۸) نیز این مقوله مشاهده می‌شود اما مقدار NPCR برای تصویر Veniz در رمز AES اصلاح‌شده (با مقدار **99.68**) و برای تصاویر London و Young girl 2 و Lion در رمز W7 (با مقادیر ۹۹/۷۰، ۹۹/۶۰، ۹۹/۷۰) برعکس بوده و نشان‌دهنده مقدار نسبتا بالای تصادفی بودن است که می‌توان گفت سامانه‌های رمز ما ثبات کافی برای رمز کردن تصاویر را نداشته‌اند و در برابر حملات تفاضلی مقاوم نیستند. با بررسی مقادیر UACI برای تصاویر رمزشده با AES اصلاح‌شده، تصاویر Veniz و London وYoung girl1 (با نتایج کمی ۳۲/۳۰، ۳۱/۹۷ و ۳۳/۱۳) مقادیر کمتر از ۳۳/۳ هستند بدین معنی که بیشتر سطوح شدت پیکسل‌ها در تصویر رمزشده تغییر نکرده و مخلوط نشده‌اند و برای تصاویر Young girl 2 و Lion (با نتایج کمی ۳۷/۴۸ و ۳۳/۷۳) مقادیر بیشتر از ۳۳/۳ بوده بدین معنی که بیشتر سطوح خاکستری پیکسل‌ها در تصویر رمزشده تغییر کرده و مخلوط شده‌اند همچنین برای تصاویر رمزشده با W7 تصاویر London و Lion (با نتایج کمی ۳۱/۲۷ و ۳۳/۲۴) مقادیرشان کمتر از ۳۳/۳ بوده بدین معنی که بیشتر سطوح شدت پیکسل‌ها در تصویر رمزشده تغییر نکرده و مخلوط نشده‌اند و بیشتر سطوح خاکستری پیکسل‌ها در تصویر رمزشده تغییر کرده و مخلوط شده‌اند. با این تفاسیر می‌توان نتیجه گرفت که سامانه‌های رمز ما در تلفیق سطوح به‌صورت ثابت عملکرد مناسبی نداشته است.

۷- نتیجه‌گیری

با توجه به نتایج آزمایشگاهی به‌دست آمده و نیز دلایل نظری برای عدم کارایی ضریب همبستگی پیرسن برای بعضی خانواده‌های توزیع‌های آماری، پیشنهاد می‌شود به جای ضریب همبستگی پیرسن از معیار ضریب اطلاع برای تعیین میزان همبستگی یک تصویر و تصویر رمز شده آن استفاده شود که این نیز به‌دلیل دقت و عملکرد بالای ضریب اطلاع در مقایسه با ضریب همبستگی پیرسن و نیز طبیعت غیرخطی و ارتباط پیوسته بین پیکسل‌های تصویر به‌عنوان نوع خاصی از داده‌ها می‌باشد.

۸- مراجع

[1] A. Mirghadri and A. Jolfaei, "Survey: Image Encryption Using Salsa20," IJCSI International Journal of Computer Science Issues, vol. 7, Issue .5, pp. 0814-1694, September 2010.

[2] B. K. Singh, N. Sharma, N. Singla, N. Sharma, and N. Choudhary, "Image Encryption Using Block-Based Transformation Algorithm," IJISET International Journal of Innovative Science, Engineering & Technology, vol. 1 Issue 3, May 2014.

[3] M .A. Bani Younes and A. Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption," IJCSNS International Journal of Computer Science and Network Security, vol. 8 no. 4, April 2008.

[4] A. Mirghadri and A. Jolfaei, "A Novel Image Encryption Scheme Using Chaotic Maps," IHU Passive Defence Sci. & Tech., vol. 2, pp. 111-124, 2011. (In Persian)

[5] A. Mirghadri and A. Jolfaei, "An image encryption approach using chaos and stream cipher," Journal of Theoretical and Applied Information Technology, Sep. 2010.

[6] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh and M. R. Mosavi, "A simple sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Multimedia tools and applications, vol. 71, pp. 1469-1497, 2014.

[7] Gh. R. Karamali and E. Kavand, "Designing Fast Algorithm to Encrypt Images Using The Chinese Remainder Theorem and Elliptic Curve," Journal of Electronical & Cyber Defence, vol. 5, no. 3, Serial no. 19, 2017. (In Persian)

[8] B. Fathi Vajargah, R. Asghari, and J. Vahidi, "Design and Analysis of a Novel Synchronous Stream Cipher Using Secure Pseudo Random Number Generator," Journal of

۱- به مقادیر جدول ۷، قسمت ضریب اطلاع توجه شود.

[29] Fawaz.Z, Noura.H, and Mostefaoui.A, "An efficient and secure cipher scheme for images confidentiality preservation", Signal Processing: Image Communication ,42,90–.108-.2016

۹- پیوست

توابع چگالی احتمال توزیع های درون جدول (۳)

الف) تابع چگالی جانسون SB[1]

$$f(x)=\frac{\delta}{\lambda\sqrt{2\pi}z(1-z)}\exp(-\frac{1}{2}(\gamma+\delta\ln(\frac{z}{1-z}))^2)$$

$$z\equiv\frac{x-\xi}{\lambda},\xi\le x\le\xi+\lambda$$

که γ مولفه شکل، $\delta>0$ مولفه شکل ، $\lambda>0$ مولفه مقیاس و ξ مولفه مکان است.

ب) تابع چگالی خطا[2]

$$f\ (x)=c_1\sigma^{-1}\exp(-\left|c_0z\right|^k)$$

$$c_0=(\frac{\Gamma(\frac{3}{k})}{\Gamma(\frac{1}{k})})^{\frac{1}{2}},c_1=\frac{kc_0}{2\Gamma(\frac{1}{k})},z\equiv\frac{x-\mu}{\sigma}$$

که k مولفه شکل ، $\sigma>0$ مولفه مقیاس و μ مولفه مکان هستند.

ج) تابع چگالی پارتو تعمیم‌یافته[3]

$$f\ (x)=\begin{cases}\frac{1}{\sigma}(1+k\ \frac{(x-\mu)}{\sigma})^{-1-1/k},k\neq0\\ \frac{1}{\sigma}(-\frac{(x-\mu)}{\sigma}),\mathrm{k}=0\end{cases},\begin{cases}\mu\le x\ \le+\infty,k\ge0\\ \mu\le x\ \le\mu-\sigma/k,\mathrm{k}<0\end{cases}$$

که k مولفه شکل ، $\sigma>0$ مولفه مقیاس و μ مولفه مکان می‌باشند.

د) تابع چگالی GEV[4]

$$f(x)=\begin{cases}\frac{1}{\sigma}\exp(-(1+kz)^{-1/k})(1+kz)^{-1-1/k},k\neq0\\ \frac{1}{\sigma}\exp(-z-\exp(-z)),k=0\end{cases},\begin{cases}1+k\frac{(x-\mu)}{\sigma}>0,k\neq0\\ -\infty<x<+\infty,k=0\end{cases}$$

$$z\equiv\frac{x-\mu}{\sigma}$$

که k مولفه شکل ، $\sigma>0$ مولفه مقیاس و μ مولفه مکان هستند.

1- Johnson SB
2- Error
3 -Generalized Pareto
4- Generalized Extreme Value

Electronical &Cyber Defence, vol. 4, no. 1, Serial no. 13, 2016. (In Persian)

[9] F. Galton, "Regression towards mediocrity in hereditary stature," Journal of the Anthropological Institute of Great Britain and Ireland, vol. 15, pp. 246-263, 1986.

[10] F. Galton, "The British Association: Section II, Anthropology: Opening address by Francis Galton, F.R.S., etc., President of the Anthropological Institute, President of the Section," Nature, vol. 32 (830), pp. 507-510, Sep. 1985.

[11] N. Ebrahimi, N. Y. Jalali, and E. Soofi, "Comparison, utility, and partition of dependence under absolutely continuous and singular distributions," Journal of Multivariate Analysis, vol. 131, pp. 32-50, Oct. 2014.

[12] J. Daemen and V. Rijmen, "The block cipher Rijindael," Proceedings of the Third Conference on smart card International Research and Applications, CARDIS'98, Lecture Notes in computer Science, vol. 1820, Springer, Berlin, 2000.

[13] A. Canteaut and E. Filiol, "Ciphertext Only Reconstruction of LFSRbased Stream Ciphers," Institute National de Recherche en Informatique et en Automatique (INRIA), Technical report no. 3887, Feb. 2000.

[14] S. Thomas, D. Anthony, T. Berson, and G. Gong, "The W7 Stream Cipher Algorithm Internet Draft," Apr. 2002.

[15] J. Behboudian, "Non Parametric Statistic," Shiraz University, 2004. (In Persian)

[16] J. L. Rodgers and W.A. Nicewander, "Thirteen ways to look at the correlation coefficient," The Amer. Statistician, vol. 42, pp. 59-66, Feb. 1988.

[17] O. J. Dunn and V. A. Clark, "Applied Statistics: Analysis of Variance and Regression," New York: Wiley, 1974.

[18] E. K. Yen and R. G. Johnston, "The Ineffectiveness of the Correlation Coefficient for Image Comparisons," Los Alamos National Laboratory, LA-UR-96-2474.

[19] J. N. Kapur and M. Dhande, "On the entropy measure of stochastic dependence," Indian journal of pure and applied mathematics, vol. 5(17), pp. 581-595, 1986.

[20] T. M. Cover and J. A. Thomas, "Elements of Information Theory, 2nd ed," John Wiley & Sons, Inc. Hoboken, NJ, USA, 2005.

[21] D. J. C MacKay, "Information Theory, Inference, and Learning Algorithms," 4th ed., Cambridge University Press: Cambridge, UK, 2003.

[22] S. Kullback and R. A. Leibler, "On information and sufficiency," Annals of Mathematical Statistics, vol. 22 (1), pp. 79–86, 1951.

[23] S. Kullback, "Information Theory and Statistics," Dover Publications, Inc. , 1968.

[24] J. N. Kapur and M. Dhande, "On a family of normalized measure of inter dependence," acta ciendica vol. XVI, M, 2, pp. 193-198, 1990.

[25] H. J. Kim, "On information theoretic index for measuring the stochastic dependence among sets of variate," Journal of Korean Stat. Society, vol. 26(1), pp. 131-146, 1997.

[26] J. N. Kapur, "New measure of stochastic dependence," IIT/ kapur Res. Rep. No. 243-109-1985.

[27] J. N. Kapur, "Normalized measure of stochastic dependence," IIT/kapur. Res. Rep. No. 279-110-1985.

[28] H. Noura, L. Sleem, M. Noura, M. Mansour1, A. Chehab1, and R. Couturier, "A New Efficient Lightweight and Secure Image Cipher Scheme," Multimedia Tools and Applications, Aug. 2017.

Journal of Electronical & Cyber Defence
Vol. 6, No. 2, 2018, Serial No. 22

Non-Performance of Pearson Correlation Coefficient for Evaluating Image Encryption Security

M. Farhadi*, H. Sabzehparvar, J. Ghasemian

*Department of mathematics of Damghan university

(Received: 06/10/2017, Accepted: 29/01/2018)

ABSTRACT

In this paper, we described Pearson's correlation coefficient inefficiency for analyzing the relationship between an image and encrypted one. Also, the information index was investigated as a suitable substitute for Pearson correlation coefficient. This weakness is independent of the encryption system of the image encryption; however, two encryption algorithms such as modified AES and W7 stream cipher have been used for laboratory calculations. In addition, by quantitative and qualitative examination of other standards for encryption analyzing of the image, the information index, in comparison with the Pearson correlation coefficient, shows the strengths and weaknesses of the image encryption algorithms better.

Keywords: Cryptography, Image Encryption, Pearson Correlation Coefficient, Entropy, Information Index

* Corresponding Author Email: farhadi@du.ac.ir