بهینه‌سازی رمزنگاری تصویر مبتنی بر آشوب با استفاده از الگوریتم آموزش و یادگیری

سعید نوشادیان[۱]، عطا ا.. ابراهیم زاده[۲]، سید جواد کاظمی تبار[۳]

[۱]کارشناسی ارشد برق الکترونیک ، دانشگاه صنعتی نوشیروانی

[۲و۳]استاد دانشکده برق و کامپیوتر، دانشگاه صنعتی نوشیروانی

چکیده

به دلیل همبستگی بین پیکسل‌های همجوار، حجم زیاد اطلاعات و نیاز به پردازش بلادرنگ، برای رمزنگاری تصویر نمی‌توان از روش‌های مرسوم در رمزنگاری داده استفاده کرد. در میان روش‌های موجود برای رمز تصویر استفاده از توابع آشوب به دلیل خواص ذاتی همچون تصادفی بودن، حساسیت به مقادیر اولیه و سادگی در پیاده‌سازی بیشتر مورد توجه قرار گرفته است. در این مقاله با استفاده از روشی جدید، تصویر توسط نگاشت لجستیک (تابع آشوب) رمز می‌شود و به کمک الگوریتم نوث پیکسل‌های تصویر جایگشت می‌یابند. در نهایت با استفاده از الگوریتم بهینه‌سازی آموزش و یادگیری(TLBO[۱]) تصویر رمز شده از نظر همبستگی میان پیکسل‌های همجوار ویا آنتروپی بهینه می‌شود. نتایج به دست آمده از آزمون‌های مختلف نشان‌دهنده‌ی دقت و کیفیت روش ارائه شده است به گونه ای که مقدار همبستگی تصویر رمز به میزان 10^{-6} می‌رسد که در مقایسه با روش های دیگر کمترین مقدار را داراست.

کلیدواژه

رمزنگاری تصویر،تابع آشوب، نگاشت لجستیک، الگوریتم TLBO، جایگشت نوث

مقدمه

امروزه به دلیل پیشرفت اینترنت در دنیای دیجیتال، امنیت اطلاعات از اهمیت بیشتری برخوردار شده است. در این زمینه نیز روش‌های زیادی مانند استاندارد رمزنگاری اطلاعات (DES) و استاندارد رمزنگاری پیشرفته (AES) مطرح شده‌اند. اما در بخش رمزنگاری تصویر به دلیل خواص ذاتی آن همچون حجم زیاد اطلاعات، افزونگی بالا و همبستگی قوی بین پیکسل‌های همجوار نمی‌توان از روش‌های مرسوم در رمزنگاری داده استفاده کرد[۱و۲و۳].

برای کاهش همبستگی و افزایش آنتروپی در تصویر از روش‌های جایگشت و جانشانی استفاده می‌شود به صورتی که در عمل جانشانی مقادیر پیکسل‌های تصویر تغییر می‌کند و سبب افزایش آنتروپی می‌گردد. در عمل جایگشت نیز مکان پیکسل‌ها جابه‌جا و موجب کاهش همبستگی پیکسل‌های همجوار می‌شود. ترکیب این دو روش کیفیت رمزنگاری تصویر را افزایش می‌دهد.

برای رمز تصویر روش‌های موجود در مقالات را می‌توان به دو گروه روش‌های غیرآشوبی و روش‌های مبتنی بر توابع آشوب تقسیم‌بندی کرد. در گروه روش‌های غیر آشوبی، روش‌هایی همچون ماشین سلولار[۴و۵]، روش جایگشت بیت ها، پیکسل‌ها و یا بلوک ها[۶و۷]، روش‌های مبتنی بر SCAN [۸]، AES [۹]و امضای دیجیتال[۱۰] وجود دارند.

استفاده از توابع آشوب در رمزنگاری تصویر به دلیل خواصی مانند ارگادیک[۲]بودن، حساسیت به شرایط اولیه، رفتار شبه تصادفی، کاهش زمان محاسبات و پیاده‌سازی ساده، بسیار مورد مطالعه قرار گرفته‌اند[۱۱و۱۲]. بنیامین نوروزی و همکاران[۱۳] روشی بر اساس نگاشت آشوب و محاسبات DNA مطرح کرده‌اند که در آن پس از اعمال یک سری عملیات ریاضی بر روی کلید رمز، مقادیر پارامتر و شرایط اولیه مربوط به تابع آشوب استخراج می‌شود. هر پیکسل از تصویر به دنباله‌ای تبدیل می‌گردد. همچنین عملیات XOR و XNOR نیز برای این دنباله‌ها پیشنهاد شده و از آنها به همراه دنباله‌های آشوب از پیش تشکیل شده، برای رمز کردن دنباله‌های DNA، تصویر طی دو تکرار استفاده می‌گردد. بهره‌گیری از اطلاعات خود تصویر امنیت الگوریتم را در برابر حملات تفضلی افزایش می‌دهد.

[۱] Teaching learning based optimization algorithm
[۲] Ergodic

تاریخ دریافت: ۱۳۹۶/۱۰/۱۲ تاریخ پذیرش: ۱۳۹۷/۰۶/۲۷

در مرجع [۱۴] مقدار پیکسل‌ها نخست با استفاده از یک ماتریس جانشینی مبتنی بر نگاشت هنون[۳] تعویض می‌شوند، سپس مکان پیکسل‌ها با استفاده از واحد جابه‌جا کننده مبتنی بر نگاشت بیکر جابه جا می‌شوند. در نهایت تصویر نهائی با یک کلید دوری مبتنی بر نگاشت بیکر XOR می‌گردد.

روش پیشنهاد شده در مرجع [۱۵]، پیکسل‌های تصویر را با استفاده از تابع لجستیک تغییر می‌دهد سپس تصویر را به چهار بخش تقسیم کرده و آنها را جایگشت می‌دهد. در نهایت به کمک الگوریتم بهینه‌سازی ژنتیک، تصویر رمز شده با کمترین میزان همبستگی میان پیکسل‌های همجوار و بیشترین آنتروپی به دست می‌آید. این روش، ابداعی در بخش بهینه‌سازی رمزنگاری تصویر بوده است اما درطی فرآیند رمزنگاری دچار ضعف امنیتی است.

در این مقاله سعی شد با استفاده از تابع آشوب و الگوریتم بهینه‌سازی آموزش و یادگیری روشی جدید در حوزه بهینه‌سازی رمزنگاری ارائه شود. در بخش دوم توابع آشوب و الگوریتم آموزش و یادگیری تشریح می‌شود. در بخش سوم روش پیشنهادی شامل تشکیل جمعیت اولیه، رمزنگاری و تولید کلید نشان داده می‌شود و در آخر نتایج به دست آمده از این روش ارائه می‌گردد.

مفاهیم مورد نیاز

توابع آشوب

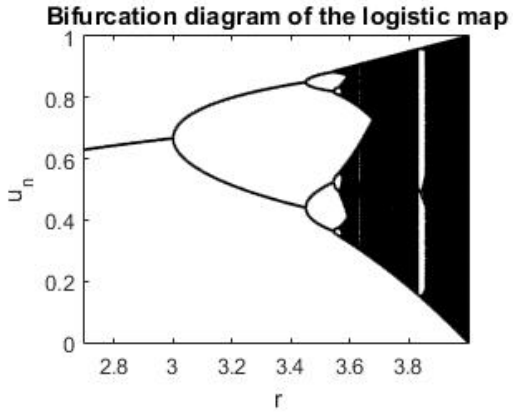
توابع آشوب به دلیل خواصی که دارند در رمزنگاری تصویر بسیار استفاده می‌شوند. یکی‌از مهمترین خواص آنها حساسیت به شرایط اولیه است. ساختار توابع آشوب به‌گونه‌ای است که کوچکترین تغییرات در شرایط اولیه‌ی ورودی موجب تغییرات قابل توجهی در خروجی می‌شود. بنابراین اگر سیگنال ورودی تغییرات کوچکی داشته باشد سیگنال خروجی کاملا متفاوت است[۱۲و۱۳]. خاصیت دیگر آنها ظاهر تصادفی است. یعنی خروجی توابع آشوب در شرایط آشوبی کاملا تصادفی است و می‌توان دنباله‌ای از اعداد تصادفی را از آن به دست آورد. ولی با داشتن مقدار اولیه و پارامترهای تابع می‌توان عدد را بازتولید کرد. به همین دلیل خاصیت قطعیت توابع آشوب مشهود است[۱۵و۱۶].

یکی‌از متداولترین و ساده‌ترین سیستم‌های آشوبی، نگاشت لجستیک است که در برگیرنده‌ی معادله‌ی تفاضلی از نوع مرتبه دوم غیر خطی است. رابطه ی دینامیکی این سیستم اولین بار توسط روبرت می معرفی شد. نگاشت لجستیک به صورت زیر تعریف می‌شود:

$$u_{n+1} = r \times u_n (1-u_n) \qquad (۱)$$

که در آن r ضریب لجستیک است. ناحیه تغییرات r بین صفر تا چهار است اما با تغییر r در این ناحیه خواص متفاوتی به تابع می‌دهد. جدول ۱ تغییرات r و خواص تابع را نشان می‌دهد. همچنین تغییرات تابع لجستیک نسبت به تغییرات r در شکل ۱ نمایش داده شده است[۱۷].

همانطور که در جدول۱ پیداست رفتار تابع لجستیک هنگامی که r در بازه‌ی (3.57,4) قرار دارد رفتاری آشوبناک است و همچنین مقدار اولیه u_0 نیز در بازه‌ی (۰،۱) قرار دارد.



شکل۱. نمودار تغییرات نگاشت لجستیک نسبت به r

جدول۱. رفتار تابع لجستیک در بازه های مختلف تغییرات r

مقادیر r	رفتار سیستم
0<r<1	سیستم به سمت صفر همگرا می‌شود.
1<r<3	سیستم به سمت مقدار r-1/r همگرا می‌شود.
3<r<3.45	سیستم بین دو مقدار ثابت نوسان می‌کند.
3.45<r<3.54	سیستم بین چهار مقدار ثابت نوسان می‌کند.
3.54<r<3.57	سیستم بین ۸ مقدار سپس ۱۶و۲۴و.... نوسان می‌کند.
3.57<r<4	سیستم دارای رفتار آشوبناک خواهد شد.
r>4	سیستم به منفی بینهایت همگرا می‌شود

الگوریتم TLBO

این الگوریتم بر اساس تاثیر یک معلم بر روی خروجی دانش‌آموزان در یک کلاس تعریف شده است. در یک کلاس معلم فردی است که دارای بهترین مقدار باشد و سطح بالاتری نسبت به دیگر دانش‌آموزان داشته باشد و بتواند دانش‌آموزان را با دانش خود سهیم کند. به طور کلی در این الگوریتم از فرایند آموزش و یادگیری که در کلاس درس اتفاق می‌افتد الهام می‌گیرد.

[۳] Henon map

الگوریتم TLBO به دو فاز معلم و دانش‌آموز تقسیم می‌گردد[۱۸و۱۹].

فاز معلم:

در فاز اول معلم از بین دانش‌آموزان انتخاب می‌شود و کسی است که اطلاعاتش از بقیه بیشتر و بهتر باشد. معلم سعی می‌کند تا میانگین کلاس را به سمت خود بکشاند. اما در واقعیت این امکان‌پذیر نمی‌باشد و همه‌ی دانش‌آموزان نمی‌توانند به سطح معلم برسند بلکه در نهایت سطح میانگین را جابه‌جا می‌کنند و به میانگین M_2 خواهند رسید. در این حالت جامعه‌ی آماری جدیدی پدید می‌آید که میانگین آن M_2 و معلم آن T_2 است. این روند در فاز اول آنقدر تکرار می‌شود تا به جمعیت بهتر یا بهینه برسند. در نمودار شکل ۲الف، T_1 به عنوان معلم کلاس انتخاب شده و سعی می‌کند میانگین سطح کلاس یعنی M_1 را به سطح خودش برساند.

رابطه‌ی ریاضی برای فاز معلم به صورت زیر خواهد بود:

$$X_{new} = X_{old} + r(X_{teacher} - T_f \times Mean) \quad (۲)$$

که در آن r یک بردار تصادفی بین صفر و یک بوده که میزان موفقیت یک دانش آموز در درک مطلب یاد شده توسط استاد را نشان می‌دهد. همچنین T_f نشان دهنده‌ی ضریب موفقیت معلم با مقادیر $\{۱،۲\}$ می‌باشد.

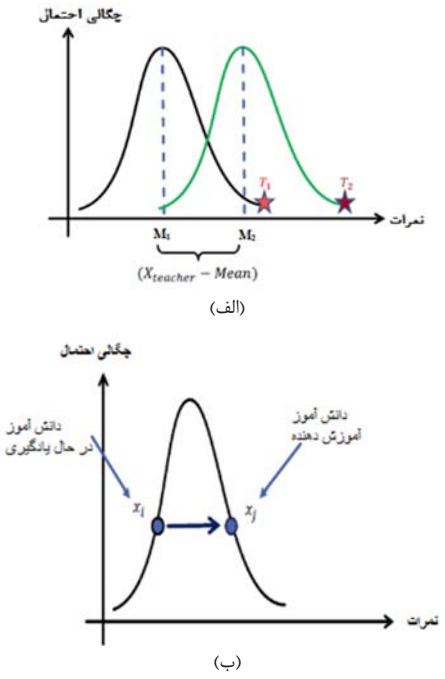
فاز دانش‌آموز:

بعد از فاز معلم فاز دانش‌آموز اجرا می‌شود. دانش‌آموزان می‌توانند از یکدیگر نیز آموزش ببینند و بر روی یکدیگر تاثیر بگذارند. این تعامل باعث می‌شود که سطوح دانش‌آموزان ارتقا پیدا کند. با توجه به شکل ۲ب دو دانش‌آموز به صورت تصادفی از میان جمعیت انتخاب خواهند شد. که در آن دانش‌آموز اول (x_i) می‌خواهد از دانش‌آموز دوم (x_j) آموزش ببیند، بسته به میزان نمره‌ی این دو دانش‌آموز دو حالت به وجود می‌آید:

حالت اول: اگر نمره‌ی x_i از x_j بدتر باشد. در حالی که یک دانش‌آموز ضعیف (x_i) می‌خواهد از دانش‌آموز با نمرات بهتر (x_j) آموزش ببیند. رابطه‌ی ریاضی به صورت زیر خواهد بود:

$$X_{i\ new} = X_i + r(X_j - X_i) \quad (۳)$$

که r در این رابطه یک بردار تصادفی بین صفر و یک است و میزان موفقیت دانش‌آموز x_i در درک مطلب یاد شده را نشان می‌دهد.

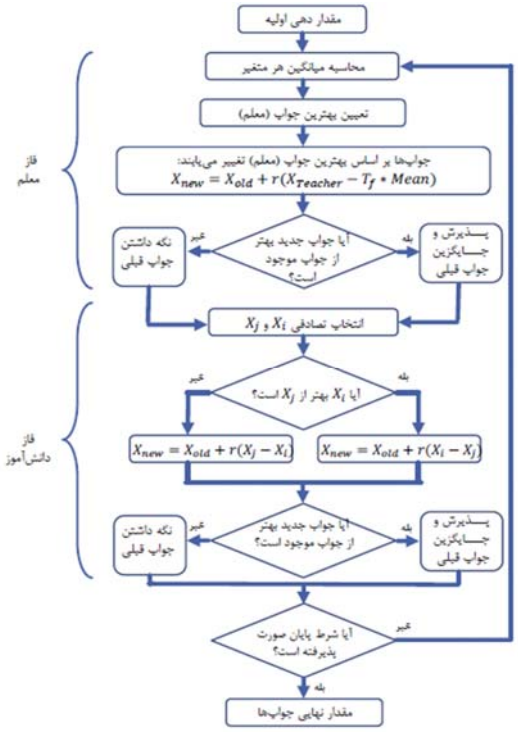


شکل۲. (الف) فاز معلم. (ب) فاز دانش آموز

حالت دوم: اگر نمرات x_i از x_j بهتر باشد. همانند حالت قبل است با این تفاوت که x_j از x_i می‌آموزد و رابطه‌ی ریاضی آن به صورت زیر است.

$$X_{i\ new} = X_i + r(X_i - X_j) \quad (۴)$$

دانستن این نکته ضروری است که در هر دو فاز معلم و دانش‌آموز با به دست آمدن x جدید مقدار تابع هدف آن محاسبه می‌شود و اگر این مقدار از مقدار تابع هدف قدیمی بهتر باشد، اطلاعات دانش‌آموز به‌روز می‌شود در غیر این صورت همان اطلاعات قدیمی بدون تغییر می‌ماند. در شکل۳ فلوچارت الگوریتم TLBO نمایش داده شده است.



شکل۳. فلوچارت الگوریتم TLBO

روش پیشنهادی

روش پیشنهادی به طور خلاصه به صورت زیر می‌باشد. ابتدا جمعیت اولیه‌ای شامل پارامترهای r و u_0 تصادفی را می‌سازیم. سپس با استفاده از الگوریتم TLBO مقدار بهینه هر کدام از پارامترها را می‌یابیم. بعد از آن مقادیر بهینه را تبدیل به کلید می‌کنیم و در آخر با استفاده از کلید منتخب تصویر رمز شده و آماده‌ی ارسال می‌گردد.

ساخت جمعیت اولیه

برخلاف مقالات دیگر که جمعیت اولیه‌ی آنها تصویر رمز شده است[۱۶] در این مقاله جمعیت اولیه متشکل از پارامترهای r و u_0 هستند به طور مثال در مقاله [۱۶] ابتدا به تعداد جمعیت اولیه کلید از تصویر انتخاب می‌شود سپس با هر کدام از کلیدها تصویر به طور جداگانه رمز می‌گردد در نهایت به تعداد جمعیت اولیه تصویر رمز شده داریم. اما در این روش به تعداد جمعیت اولیه (تعداد دانش‌آموزان کلاس) مقادیر u_0 (مقدار اولیه تابع لجستیک) و r (پارامتر متغیر تابع لجستیک) را به صورت تصادفی تولید می‌کنیم. البته این مقادیر باید در محدوده‌ی تعیین شده باشند. در تحقیقات گذشته، مقدار r ثابت و نزدیک به ۴ در نظر گرفته شده است ولی در این مقاله مقدار r به صورت وقفی است تا تصویر رمز شده بیشترین آنتروپی و یا کمترین میزان همبستگی بین پیکسلی داشته باشد.

بهینه‌سازی تصویر

همانطور که در بخش قبل گفته شد می خواهیم مقدار بهینه r و u_0 را در تابع لجستیک به دست آوریم. پس با توجه به الگوریتم آموزش و یادگیری هر دانش‌آموز به صورت زیر تعریف می‌شود.

$$X = [r, u_0] \qquad (۵)$$

در حالی که x همان دانش‌آموز کلاس است و یک جفت مشخصه‌ی r و u_0 دارد. r پارامتر متغیر تابع لجستیک و u_0 مقدار اولیه تابع لجستیک است. برای محاسبه‌ی نمره هر دانش آموز یا تابع هزینه الگوریتم می‌بایست ابتدا تصویر با استفاده از نگاشت لجستیک که پارامترهای آن را دانش‌آموزان تشکیل می‌دهند رمز می‌شود (نحوی رمزنگاری در بخش مربوطه توضیح داده خواهد شد). سپس تابع هزینه را برای هر دانش‌آموز به دست می‌آوریم (در این جا تابع هزینه را آنتروپی تصویر در نظر می‌گیریم) پس از به‌دست آوردن تابع هزینه همه‌ی تصویرها و یا همان نمره‌ی دانش‌آموزان، بهترین مقدار آن (که در اینجا بزرگترین آنهاست) به عنوان معلم انتخاب می‌شود. در طی اجرای الگوریتم TLBO، معلم انتخاب می‌شود. در طی اجرای الگوریتم TLBO، معلم سعی در آموزش دانش‌آموزان و همچنین دانش‌آموزان سعی در یادگیری از یکدیگر دارند تا نمره‌ی بهتری به‌دست آورند. در نتیجه میانگین نمرات کلاس بهبود می‌یابد. در هر تکرار بهترین دانش آموز از نظر اطلاعات انتخاب می‌شود و سعی‌می‌کند سطح میانگین دانش‌آموزان را به سمت خود بکشاند. در ادامه‌ی این روند بهترین دانش آموزان کلاس انتخاب می‌شود. بهترین جواب در اینجا همان (u_0, r)ای است که بیشترین آنتروپی را در تصویر رمز ایجاد می‌کند.

ساخت کلید

پس از یافتن مقدار بهینه r و u_0 به عنوان کلید باید آن به کد باینری تبدیل شود. به دلیل آنکه اعداد انتخابی اعشاری هستند می‌بایست از الگوریتم تبدیل عدد اعشاری به باینری استفاده شود. در این تبدیل قسمت صحیح اعداد r و u_0 کنار گذشته می‌شود زیرا قسمت صحیح r و u_0 به ترتیب همیشه ۳ و ۰ است. بنابراین تنها قسمت اعشاری آنها تبدیل می‌شود. در تبدیل، اندازه‌ی قسمت باینری ثابت نیست و همواره تغییر می‌کند به همین دلیل عدد را به گونه‌ای انتخاب می‌کنیم که برای هر کدام از پارامترها حداکثر ۶۴ بیت باشد. در نتیجه طول کلید ۱۲۸ می‌گردد. در صورتی‌که پس از تبدیل عدد باینری کمتر از ۶۴ بیت بود باقی اعداد را صفر قرار می‌دهیم. در صورتی که در

سیستم‌های رمزنگاری نیاز به کلید بزرگ‌تر باشد می‌توانیم از ۲ جفت پارامتر (u_0,r)، یکی در هسته‌ی تابع لجستیک در قسمت تغییر مقدار پیکسل‌ها و دیگری برای همین تابع در قسمت جایگشت استفاده کنیم. از این طریق می‌توانیم کلید ۲۵۶ بیتی داشته باشیم. در قسمت رمزگشایی عکس این تبدیل انجام می‌شود تا عدد باینری به اعشاری برگردد.

رمزنگاری تصویر

در مرحله ی آخر می‌بایست تصویر را با استفاده از تابع لجستیک که با پارامترهای بهینه تشکیل شده رمز کرد. عملیات رمزنگاری طی دو مرحله انجام می‌شود: جانشانی پیکسل‌ها و جایگشت آنها.

جانشانی پیکسل ها:

برای تغییر مقدار پیکسل‌های تصویر با استفاده از تابع لجستیک بدین صورت عمل می‌کنیم که ابتدا توسط رابطه‌ی ۱ و مقادیر بهینه به دست آمده از بهینه‌ساز TLBO به تعداد پیکسل‌های تصویر مقدار u_n تولید می‌کنیم در نتیجه طول ماتریس U برابر با $M \times N$ است که M و N به ترتیب طول و عرض تصویر است. پس از آن هر درایه ماتریس را در عدد ۲۵۵ (ناحیه تغییرات رنگ پیکسل) ضرب می‌کنیم و سپس با پیکسل متناظر از تصویر XOR می‌نماییم تا مقدار آن تغییر یابد با تکرار این روند تمام پیکسل‌های تصویر تغییر می‌کنند.

$$Newvalue = round(Ui * 255) \oplus Oldvalue \qquad (۶)$$

در رابطه‌ی بالا Ui هر درایه‌ی بردار U است و علامت exclusive or(XOR) است.

جایگشت پیکسل ها:

برای امن‌تر شدن و کیفیت رمزنگاری و همچنین پایین آمدن همبستگی بین پیکسل‌های همجوار مکان پیکسل‌ها تغییر داده می‌شود. برای این کار از الگوریتمی به نام جایگشت نوث[۴] استفاده می‌کنیم که برای جایگشت ماتریس کاربرد دارد. در هسته‌ی اصلی این الگوریتم از تابع rand برای تولید عدد تصادفی استفاده می‌شود[۲۰] اما در این جا برای رمزنگاری و رمزگشایی به هسته‌ای نیاز است که علاوه بر تولید عدد تصادفی با شرایطی بتوان آن عدد را بازتولید کرد زیرا در بخش رمزگشایی برای یافتن تصویر ابتدا بایست مکان پیکسل‌ها را به حالت اولیه تغییر داد به همین دلیل از توابعی که خاصیت شبه تصادفی دارند می‌توان استفاده کرد. برای سهولت کار از تابع لجستیک به جای تابع rand در قسمت هسته‌ی الگوریتم نوث استفاده می‌شود.

برای درک بهتر این موضوع روند رمزنگاری تصویر در شکل ۴ و۵ نشان داده شده است. اگر فرض کنیم تصویر ما شامل ۴ پیکسل به صورت زیر و خروجی بهینه‌ساز $x=(r,u_0)=(3.79,0.58)$ باشد. داریم:

$$u_{1,1} = 3.79 \times 0.58(1-0.58) = 0.9232,$$
$$u_{1,2} = 3.79 \times 0.9232(1-0.9232) = 0.2687,$$
$$u_{2,1} = 3.79 \times 0.2687(1-0.2687) = 0.7447,$$
$$u_{2,2} = 3.79 \times 0.7447(1-0.7447) = 0.7206$$

$$im_{1_{new}} = round(0.9232 \times 255) \oplus 160 = 75,$$
$$im_{2_{new}} = round(0.0.2687 \times 255) \oplus 190 = 250,$$
$$im_{3_{new}} = round(0.7447 \times 255) \oplus 150 = 40,$$
$$im_{4_{new}} = round(0.7206 \times 255) \oplus 200 = 112,$$

(الف)

Plain-image	
160	190
150	200

Cypher-image	
75	250
40	112

(ب)

شکل۴. انجام مراحل جانشانی با ماتریس نمونه ی ۴ پیکسلی. (الف) تشکیل ماتریس U و تغییر پیکسل های تصویر. (ب) سمت چپ تصویر اصلی، سمت راست تصویر رمز شده.

حال اگر بخواهیم با استفاده از پارامترهای $x=(r,u_0)$، عمل جایگشت را انجام دهیم به صورت شکل ۵ عمل می‌کنیم البته بردار U تولید شده همان بردار U در شکل ۴ است. هر چه تصویر بزرگ‌تر باشد کیفیت عمل جایگشت بهتر نشان داده می‌شود.

$$M_1 = ceil(0.9232 \times 4) = 4,$$
$$M_2 = ceil(0.2687 \times 4) = 2,$$
$$M_3 = ceil(0.7447 \times 4) = 3,$$
$$M_4 = ceil(0.7206 \times 4) = 3,$$

```
for i=numel(x):-1:1
im([M(i),i])=im([i,M(i)]);
end
```

Permuted Cypher-image		
	250	75
	40	112

شکل۵. فرایند جایگشت تصویر با تشکیل بردار تصادفی M

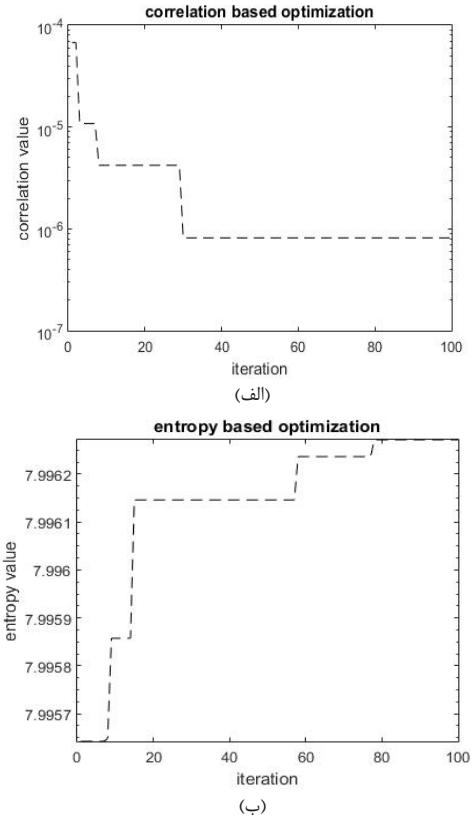
نتایج شبیه سازی

برای اجرای روش مطرح شده در این مقاله از تصاویر استاندارد با اندازه ۲۵۶*۲۵۶ استفاده شده است همچنین عملیات

[۴] Knuth shuffle

بهینه‌سازی در ۱۰۰ تکرار و با نرم‌افزار متلب در لب تاپی با پردازنده‌ی 1.6GH core i7 انجام شد. در شکل ۶الف فرایند رمزنگاری بر روی تصویر lena بر اساس همبستگی بین پیکسل‌های همجوار انجام شده است و در شکل ۶ب بهینه‌سازی بر پایه آنتروپی را نشان می‌دهد. البته باید این نکته را ذکر کرد که نمودارهای نشان داده شده میانگین شبیه‌سازی در طی تکرارهای مختلف است.

رمزنگاری تصویر مبتنی بر آشوب نسبت به تغییرات پارامترهای تعیین شده بسیار حساس است بنابراین در بهینه کردن این مسأله جواب یکتایی وجود ندارد تا دسته جواب‌ها به آن همگرا شوند اما می‌توان با تعیین حداقل مقدار برای همبستگی و حداکثر مقدار مورد نیاز برای آنتروپی یا تعیین حداکثر تکرار به عملیات بهینه‌سازی پایان داد.



شکل۶. (الف) بهینه سازی تصویر بر اساس همبستگی بین پیکسل ها در ۱۰۰ تکرار. (ب) بهینه سازی تصویر بر اساس آنتروپی در ۱۰۰ تکرار.

تحلیل هیستوگرام

تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از ترسیم تعداد مشاهدات هر میزان شدت روشنایی، بیان می‌کند. الگوریتم رمزنگاری باید به‌گونه‌ای باشد که هیچ اطلاعاتی در مورد تصویر اصلی به حمله کننده ندهد. این امر در صورتی ممکن است که نمودار هیستوگرام که شبیه نمودار چگالی احتمال است کاملا یکنواخت باشد[۲۱]. برای آن که نمودار هیستوگرام به یکنواختی نزدیک باشد الگوریتم رمزنگاری خود را بر اساس حداکثر شدن آنتروپی بهینه می‌کنیم. شکل ۷ب به وضوح یکنواختی نمودار هیستوگرام تصویر رمز شده را نشان می‌دهد.

تحلیل ضرایب همبستگی

در تصویر ساده پیکسل‌های همجوار همبستگی بالایی با هم دارند. یک الگوریتم رمزنگاری تصویر امن باید بر این همبستگی غلبه کند. برای محاسبه‌ی ضریب همبستگی بین پیکسل‌های همجوار از روابط زیر استفاده می‌کنیم. البته همسایگی به سه روش مختلف عمودی، افقی و قطری تعریف می‌شود.

$$\mathrm{cov}(x,y)=E[(x-E(x))(y-E(y))], \quad (۷)$$

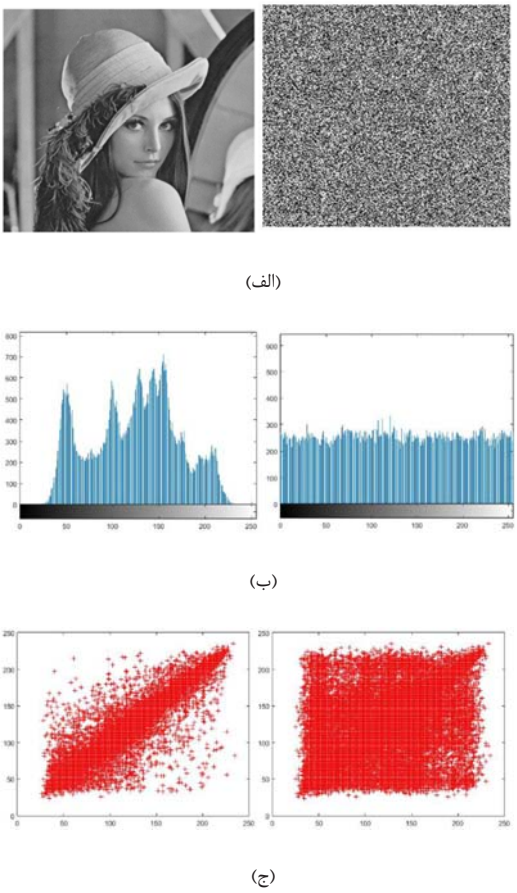
$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (۸)$$

$$E(x)=\frac{1}{N}\sum_{i=0}^{N}x_i, \quad (۹)$$

در روابط بالا x و y مقدار سطح خاکستری دو پیکسل همسایه را نشان می‌دهند و N تعداد جفت‌های همسایگی است. در مقالات مختلف برای سادگی و سرعت محاسبات ۱۰۰۰ جفت پیکسل همسایه به صورت تصادفی انتخاب می‌کنند اما ما در این مقاله مقدار N را برابر با تمام پیکسل‌های تصویردر نظر می‌گیریم تا در هر بار محاسبه، ضریب همبستگی ثابت باشد و کل تصویر را پوشش دهد. حداکثر ضریب همبستگی برابر عدد یک و بیانگر وجود همبستگی بالا بین پیکسلهای مجاور است. یک الگوریتم رمزنگاری خوب باید تصویر را به گونه‌ای رمز نماید که ضرایب همبستگی بین پیکسلهای مجاور در تصویر رمزشده بسیار کوچک و نزدیک به صفر باشد تا حمله‌کننده با تحلیل فوق به هیچگونه اطلاعات درخوری دسترسی نیابد. توزیع همبستگی پیکسلهای مجاور برای راستای افقی در تصویر اصلی و تصویر رمزشده در شکل (۷) نشان داده شده است.

در مرحله ی دوم تصویر لِنا را بر اساس سه نوع ضریب همبستگی (عمودی، افقی و قطری) به صورت جداگانه بهینه سازی کردیم یعنی در قسمت تابع هزینه الگوریتم تکاملی هر کدام از این توابع را قرار دادیم و ضرایب همبستگی تصویر رمز شده ی حاصل را محاسبه کردیم. نتایج حاصل نشان می دهد وقتی که تصویر رمز شده بر اساس ضریب همبستگی قطری بهینه‌سازی می شود مقدار همبستگی قطری آن به طور میانگین تا 10^{-6} می‌رسد و این مقدار در مقایسه با بهترین و به‌روزترین الگوریتم‌های رمزنگاری کمترین مقدار را دارد. همچنین در حالتی که بر اساس همبستگی عمودی و یا افقی بهینه شود همین نتیجه حاصل

می‌گردد. جدول ۲ نتایج بدست آمده و مقایسه‌ی آن با روش‌های دیگر را نشان می‌دهد.



(الف)

(ب)

(ج)

شکل۷. مقایسه‌ی تصویر اصلی و تصویر رمز شده. (ب) سمت چپ نمودار هیستوگرام تصویر اصلی و سمت راست هیستوگرام تصویر رمز شده. (ج) همبستگی پیکسل های همجوار تصویر اصلی در مقابل تصویر رمز شده.

تحلیل آنتروپی

نظریه‌ی اطلاعات یک نظریه ریاضی از مخابرات داده و ذخیره سازی می‌باشد که در سال ۱۳۴۹ به وسیله شانون معرفی شد. شانون آنتروپی را به عنوان معیاری از میزان اطلاعات در منبع معرفی کرد. مفهوم آنتروپی در ارتباط با میزان بی‌نظمی و عدم قطعیت در یک سامانه فیزیکی می‌باشد آنتروپی شانون H(s) یک منبع پیام s به صورت زیر تعریف می شود:

$$H(s)=\sum_{i=0}^{2^N-1} p(s_i)\log_2\frac{1}{p(s_i)} \qquad (10)$$

که p(si) احتمال سمبل si است و آنتروپی به صورت بیتی بیان می‌شود. فرض کنید که منبع، ۲N سمبل هم احتمال تولید کند، یعنی $s=\{s_1,s_2,\ldots,s_{2^N}\}$. بعد از ارزیابی معادله فوق H(s)=N به دست می‌آید که متناظر با یک منبع اطلاعات علمی به ندرت پیام‌های تصادفی تولید می‌کند و میزان آنتروپی آن کمتر از مقدار ایده‌آل ۸ می‌باشد. با این وجود هنگامی که پیام‌ها رمز می‌شوند، آنتروپی آنها بایستی نزدیک به مقدار ایده‌آل ۸ باشد. در جدول ۴ تصاویر رمز شده بر اساس آنتروپی و ضریب همبستگی بهینه شده اند. در مقایسه با مرجع [۱۶] هنگامی که تصاویر بر اساس آنتروپی بهینه شده‌اند مقدار بهتری را به‌دست می‌دهد.

سنجش کیفیت رمزنگاری

بعد از عمل رمزنگاری بر روی تصویر مقادیر پیکسل‌ها تغییر کرده و در نهایت متفاوت از تصویر اصلی می‌شود. هر چه میزان تغییرات در مقادیر پیکسل‌ها بیشتر باشد روش رمزنگاری مؤثرتر و در نتیجه کیفیت تصویر بهتر است. یک معیار برای سنجش کیفیت رمزنگاری، انحراف معیار بین تصویر اصلی و تصویر رمز شده می‌باشد. کیفیت رمزنگاری تصویر به صورت زیر تعریف می‌شود[۲۱]:

$$EQ=\sum_{L=0}^{255}|H_L(C)-H_L(P)|/256 \qquad (11)$$

در حالی که p و c به ترتیب نشان دهنده‌ی تصویر اصلی و تصویر رمز هستند که هر کدام H*W پیکسل با L سطح خاکستری دارند. $H_L(p)$ تعداد پیشامدهای هر مقدار خاکستری L در تصویر ساده و $H_L(c)$ تعداد پیشامدهای مقدار خاکستری L در تصویر رمز است. جدول ۵ مقدارکیفیت رمزنگاری تصاویر مختلف را بعد از عملیات رمز و بهینه‌سازی نشان می‌دهد. همچنین در مقایسه با مرجع [۲۹] مقدار قابل قبولی دارد (جدول ۶).

اختلاف بین تصویر اصلی و تصویر رمز

یکی از خواص مهم الگوریتم‌های رمزنگاری، حساسیت تصویر رمز به تغییرات جزئی در تصویر ساده است. هر چه تصویر رمز به تغییرات حساس‌تر باشد الگوریتم نسبت به حملات مختلف مقاوم‌تر است. در حالت کلی ممکن است که حمله‌کننده تغییراتی ایجاد کند، به طور مثال یک پیکسل تصویر رمز شده را تغییر می‌دهد و تغییرات خروجی را مشاهده می‌کند. در این صورت ممکن است بتواند روابط معنی‌داری بین تصویر رمز شده و تصویر ساده پیدا کند و رمز را بشکند. بنابراین برای اندازه‌گیری تاثیر تغییر یک پیکسل از تصویر ساده بر روی پیکسل‌های تصویر رمز از سه روش معمول استفاده می‌کنیم. میانگین قدر مطلق خطا (MAE)، نرخ تغییرات تعداد پیکسل‌ها (NPCR)، شدت تغییرات میانگین متحد (UACI) سه معیار برای اندازه‌گیری این تغییرات است[۱۵و۲۱].

اگر P(i,j) و C(i,j) پیکسل‌های تصویر ساده و تصویر رمز را نشان می دهند و H و W به ترتیب طول و عرض تصویر باشند داریم:

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

دو تصویر رمز C_1 و C_2 را در نظر بگیرید که تصاویر اصلی آنها تنها در یک پیکسل با هم تفاوت دارند. NPCR به صورت زیر تعریف می شود.

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

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (۱۴)$$

مقدار سطح خاکستری پیکسل‌ها در نقطه ی (i, j) از تصاویر C_1 و C_2 به صورت $C_1(i,j)$ و $C_2(i,j)$ تعریف می شود. معیار NPCR درصد اختلاف پیکسل‌ها بین دو تصویر را نشان می دهد.

همچنین معیار UACI به صورت زیر بیان می‌شود که میانگین تغییرات شدت روشنایی بین دو تصویر را اندازه‌گیری می‌کند.

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \qquad (۱۵)$$

درجدول ۵ سه معیار MAE، NPCR، UACI برای روش پیشنهادی با تصاویر مختلف نشان داده شده است. جدول ۶ نیز مقایسه‌ی این سه معیار روش پیشنهادی را با روش‌های دیگر بر روی تصویر لنا را بیان می‌کند.

جدول۲. مقایسه‌ی همبستگی تصویر رمز شده بین روش پیشنهادی و روش‌های دیگر در سه جهت عمودی، افقی و قطری. روش پیشنهادی در سه جهت به صورت جداگانه بهینه شده است.

Lena	Diagonal correlation	Horizontal correlation	Vertical correlation
Diagonal-based	**۱,۳۲×۱۰$^{-۶}$**	-۱×۱۰$^{-۶}$	-۵,۴×۱۰$^{-۶}$
Horizental-based	۳×۱۰$^{-۳}$	**-۹,۳۱×۱۰$^{-۶}$**	۲,۶×۱۰$^{-۳}$
Vertical-based	۱,۹×۱۰$^{-۳}$	-۱,۲×۱۰$^{-۳}$	**-۲,۴×۱۰$^{-۶}$**
Zhu's algorithm[23]	۱,۶۵×۱۰$^{-۳}$	۲,۰۱×۱۰$^{-۳}$	-۹,۱×۱۰$^{-۴}$
Yicong's algorithm[27]	-۷,۲۴×۱۰$^{-۴}$	- ۹,۷۷×۱۰$^{-۶}$	- ۵,۷×۱۰$^{-۶}$
Enhanced TDCEA[22]	-۱,۷×۱۰$^{-۴}$	۱,۸۲×۱۰$^{-۳}$	۲,۳۷×۱۰$^{-۳}$
Lian's algorithm[24]	۴,۴۳×۱۰$^{-۳}$	۱,۹۷×۱۰$^{-۲}$	۲۴,۶×۱۰$^{-۳}$
Chen's algorithm[26]	۳,۶×۱۰$^{-۳}$	۵,۳×۱۰$^{-۳}$	-۰,۲۰۸۸
Abdullah's algorithm[16]	-۹×۱۰$^{-۴}$	۹,۳×۱۰$^{-۳}$	-۵,۴×۱۰$^{-۳}$
Liao's algorithm[25]	۱,۸×۱۰$^{-۳}$	-۹,۷۵×۱۰$^{-۵}$	-۸,۰۵×۱۰$^{-۴}$

جدول۳. همبستگی تعدادی از تصاویر رمز شده با الگوریتم پیشنهادی

Vertical correlation	Lena	Baboon	Barbara	Peppers	Aerial
Vertical-based	-۲,۴۶۷۰×۱۰$^{-۶}$	۱,۴۹۹۵×۱۰$^{-۶}$	۳,۱۳۶۵×۱۰$^{-۶}$	-۱,۹۰۳۸×۱۰$^{-۶}$	۷,۴۸۸۴×۱۰$^{-۶}$

جدول۴. مقایسه آنتروپی هنگامی که تصویر رمز شده بر اساس همبستگی و آنتروپی بهینه شده باشد.

Entropy	Lena	Baboon	Barbara	Peppers	Aerial
Correlation based	۷,۹۸۸۰	۷,۹۹۱۹	۷,۹۹۰۱	۷,۹۹۰۵	۷,۹۷۷۶
Entropy based	۷,۹۹۶۵	۷,۹۹۶۲	۷,۹۹۶۲	۷,۹۹۵۰	۷,۹۹۳۵
Abdullah's algorithm[21]	۷,۹۹۲۳	۷,۹۹۲۶	-	۷,۹۹۲۹	-

جدول۵. نتیجه آزمون‌های مختلف امنیت در تصویرهای متفاوت.

	Lena	Baboon	Barbara	Peppers	Arial
EQ	۱۸۰,۵۷۰۳	۲۲۰,۵۴۴۷	۲۱۷,۶۳۲۸	۱۶۵,۶۵۶۳	۱۸۷,۷۵۸۸
MAE	۷۴,۴۱۷۰	۶۶,۳۱۳۶	۷۳,۲۶۵۶	۷۴,۱۵۹۸	۷۲,۲۸۹۰
NPCR	۹۹,۶۴۴۶%	۹۹,۶۲۰۱%	۹۹,۶۱۰۴%	۹۹,۶۱۰۹%	۹۹,۶۰۴۸%
UACI	۳۴,۱۴۷۴%	۳۳,۵۶۳۲%	۳۳,۲۴۰۵%	۳۳,۱۷۱۷%	۳۳,۰۳۵۹%

جدول۶. مقایسه‌ی روش پیشنهادی با روش‌های دیگر در آزمون‌های مختلف.

	NPCR	UACI	EQ	MAE
Proposed method	۹۹,۶۴%	۳۴,۱۴%	۱۸۰,۲۵	۷۴,۴۱
Besharati's algorithm[29]2013	۹۹,۶۳%	۳۳,۵۱%	۱۶۸,۲۹	۷۲,۳۲
Norouzi's algorithm[21]2014	۹۹,۶۱%	۳۳,۵۷%	-	-
Y.Zhang's algorithm[31]2014	۹۹,۶۶%	۳۳,۵۷%	-	-
Enayatfar's algorithm[30]2014	۹۹,۷۱%	۳۳,۶۲%	-	-
Khan's algorithm[28]2015	۹۹,۰۶%	۳۳,۵۶%	-	-

نتیجه گیری

در این پژوهش با ارائه‌ی روشی جدید و ترکیب مباحث بهینه‌سازی و رمزنگاری تصویر مبتنی بر توابع آشوب توانستیم به کمک الگوریتم آموزش و یادگیری (TLBO) تصویر را به گونه‌ای رمز کنیم که بیشترین آنتروپی و کمترین همبستگی ممکن را داشته باشد. نتایج به دست آمده در جدول ۲و ۳ نشان می‌دهد که تصویر رمز شده توسط روش پیشنهادی دارای کمترین همبستگی در بین روش‌های موجود و آنتروپی مناسب است. همچنین آزمون‌های مختلف انجام شده بر روی تصویر حاصل نشان دهنده‌ی امنیت قابل قبول الگوریتم پیشنهادی است.

مراجع

[1] Belkhouche, F. and Qidwai, U., "Binary image encoding using 1D chaotic maps," IEEE Region 5, 2003 Annual Technical Conference (pp. 39-43). IEEE, 2003, April.

[2] Chen, G., Mao, Y. and Chui, C.K., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons \& Fractals, 21(3), pp.749-761.

[3] Zhang, G. and Liu, Q., 2011. A novel image encryption method based on total shuffling scheme. Optics Communications, 284(12), pp.2775-2780.

[4] Zefreh, E.Z., Rajaee, S. and Farivary, M., 2011, June. Image security system using recursive Cellular automata substitution and its parallelization. In Computer Science and Software Engineering (CSSE), 2011 CSI International Symposium on (pp. 77-86). IEEE.

[5] Lafe, O., 1996, November. Data compression and encryption using cellular automata transforms. In Intelligence and Systems, 1996., IEEE International Joint Symposia on (pp. 234-241). IEEE.

[6] Mitra, A., Rao, Y.S. and Prasanna, S.R.M., 2006. A new image encryption approach using combinational permutation techniques. International Journal of Computer Science, 1(2), pp.127-131.

[7]

[8] Guan, Z.H., Huang, F. and Guan, W., 2005. Chaos-based image encryption algorithm. Physics Letters A, 346(1), pp.153-157.

[9] Kamali, S.H., Shakerian, R., Hedayati, M. and Rahmani, M., 2010, August. A new modified version of advanced encryption standard based algorithm for image encryption. In Electronics and Information Engineering (ICEIE), 2010 International Conference On (Vol. 1, pp. V1-141). IEEE.

[10] Maniccam, S.S. and Bourbakis, N.G., 2004. Image and video encryption using SCAN patterns. Pattern Recognition, 37(4), pp.725-737.

[11] Sinha, A. and Singh, K., 2003. A technique for image encryption using digital signature. Optics communications, 218(4), pp.229-234.

[12] Wang, Y., Wong, K.W., Liao, X. and Chen, G., 2011. A new chaos-based fast image encryption algorithm. Applied soft computing, 11(1), pp.514-522.

[13] Zhang, Q., Guo, L. and Wei, X., 2010. Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11), pp.2028-2035.

[14] Lian, S., Sun, J. and Wang, Z., 2005. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons \& Fractals, 26(1), pp.117-129.

[15] Jolfaei, A. and Mirghadri, A., 2010. A new approach to measure quality of image encryption. International Journal of Computer and Network Security, 2(8), pp.38-44.

[16] Abdullah, A.H., Enayatifar, R. and Lee, M., 2012. A hybrid genetic algorithm and chaotic function model for image encryption. AEU-International Journal of Electronics and Communications, 66(10), pp.806-816.

[17] Alligood, K.T., Sauer, T.D. and Yorke, J.A., 1997. Chaos. In Chaos (pp. 105-147). Springer Berlin Heidelberg.

[18] Rao, R.V., Savsani, V.J. and Vakharia, D.P., 2011. Teaching–learning-based optimization: a novel method for constrained mechanical design optimization problems. Computer-Aided Design, 43(3), pp.303-315.

[19] Rao, R.V., Savsani, V.J. and Vakharia, D.P., 2012. Teaching–learning-based optimization: an optimization method for continuous non-

linear large scale problems. Information Sciences, 183(1), pp.1-15.
[20] Knuth, D.E., 1998. The art of computer programming: sorting and searching (Vol. 3). Pearson Education.
[21] Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S.M. and Mosavi, M.R., 2014. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimedia tools and applications, 71(3), pp.1469-1497.
[22] Li, C., Li, S., Chen, G., Chen, G. and Hu, L., 2005. Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP Journal on Advances in Signal Processing, 2005(8), pp.1-12.
[23] Zhu, Z.L., Zhang, W., Wong, K.W. and Yu, H., 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6), pp.1171-1186.
[24] Lian, S., Sun, J. and Wang, Z., 2005. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons \& Fractals, 26(1), pp.117-129.
[25] Liao, X., Lai, S. and Zhou, Q., 2010. A novel image encryption algorithm based on self-adaptive wave transmission. Signal Processing, 90(9), pp.2714-2722.
[26] Chen, G., Mao, Y. and Chui, C.K., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons \& Fractals, 21(3), pp.749-761.
[27] Zhou, Y., Bao, L. and Chen, C.P., 2014. A new 1D chaotic system for image encryption. Signal processing, 97, pp.172-182.
[28] Khan, J., Ahmad, J. and Hwang, S.O., 2015, May. An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. In Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on (pp. 1-6). IEEE.
[29] Fard, E.B. and Atani, R.E., 2013, October. A novel image encryption method based on chaotic maps. In Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on (pp. 190-195). IEEE.
[30] Enayatifar, R., Abdullah, A.H. and Isnin, I.F., 2014. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56, pp.83-93.
[31] Zhang, Y. and Xiao, D., 2014. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-International Journal of Electronics and Communications, 68(4), pp.361-368.