ششمین کنفرانس بین المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۲۶ و ۲۷ آبان ۱۴۰۰

الگوریتم رمزنگاری تصاویر مبتنی بر نگاشت های آشوبناک و تبدیل موجک

وحید محمدنژاد، آرتا امیر جمشیدی[1]، غلامرضا رکنی لموکی
آزمایشگاه علوم داده و مدل سازی، دانشکده ریاضی، آمار و علوم کامپیوتر، دانشکدگان علوم، دانشگاه تهران

چکیده

امروزه ذخیره سازی و ارسال تصاویر دیجیتال امری بسیار متداول است. یکی از مشکلات اساسی در این حوزه دسترسی های غیرمجاز به تصاویر می باشد، چرا که بعضا همانند تصاویر پزشکی شخصی بوده و یا حتی کاربرد امنیتی دارند. لذا نیاز به طراحی الگوریتم‌های رمزنگاری جدید و مناسب روزافزون می‌باشد. در این مقاله الگوریتمی مناسب جهت رمزنگاری تصاویر سیاه–سفید، مبتنی بر نگاشت های آشوبناک و تبدیل موجک ارائه شده که با استفاده از الگوریتم و معیارهای دیگر مقالات مورد مقایسه قرار گرفته است. براساس نتایج حاصل، علاوه بر آشکار شدن نقاط ضعف الگوریتم های شبیه سازی شده، الگوریتم پیشنهادی نیز مورد تایید قرار می گیرد که از خصوصیات آن در مقایسه با دیگر الگوریتم ها می توان به سادگی، سرعت، برآورده کردن اکثر معیارها و فضای کلید گسترده و منعطف اشاره کرد.

واژه‌های کلیدی: رمزنگاری تصویر، سیستم های آشوبناک، تبدیل موجک.

[2010]: 68P25, 62H35.

۱ مقدمه

کارایی الگوریتم‌های رمزنگاری امروزی به این وابسته است که تا چه حد اعداد تولیدشده در فرایند رمزنگاری، از دید افراد غیرمجاز تصادفی هستند. در این میان ایده استفاده از سیستم های آشوبناک[2] در علم رمزنگاري به سال ۱۹۴۹ و مقاله شانون [۷] برمی‌گردد. دو ویژگي قطعیت و شبه تصادفي بودن آنها باعث گردیده تا اولین مقاله در خصوص رمزنگاري با استفاده از سیستم های آشوبناک در سال ۱۹۸۹ منتشر گردد [۸]. با وجود ارائه الگوریتم‌های رمزنگاری متنوع، به دلایلی همچون مشکلات پیاده‌سازی، امنیت، مقاومت در برابر نویز، حجم تصاویر و محدودیت پهنای باند شبکه‌های ارتباطی تنها تعداد محدودی به مرحله عملیاتی می‌رسند. این مقاله با انتخاب و بررسی الگوریتم های رمزنگاری تصاویر (مراجع [۳] تا [۶]) و ترکیب ایده های ساده و موثر از یکدیگر، الگوریتمی ساده و کارا جهت رمزنگاری تصاویر سیاه–سفید معرفی کرده است. از ویژگی های الگوریتم می توان به سرعت، فضای کلید گسترده و منعطف و در عین حال برآورده کردن اکثر معیارهای اعتبارسنجی نام برد. این مقاله در بخش بعدی خلاصه ای از سیستم های آشوبناک و تبدیل موجک را گفته و سپس الگوریتم پیشنهادی را معرفی می کند. در ادامه الگوریتم پیشنهادی را همراه با دو الگوریتم مراجع [۱] و [۲] مورد ارزیابی قرار داده و در بخش انتهایی به جمع بندی و نتیجه گیری می پردازد.

۲ پیشینه ریاضی

یک دستگاه دینامیکی آشوبناک است هرگاه اختلاط توپولوژیک و ترایاتوپولوژیک بوده و نسبت به شرایط اولیه حساس باشد [۱۲]. سه نگاشت آشوبناک Logistic (لجستیک)، Sine و Tent از جمله نگاشت های معروف بوده که به ترتیب با روابط ۱ تا ۳ معرفی می شوند.

$$x(n+1) = a\,x(n)\,(1-x(n)) \qquad a \in (0, 4] \tag{1}$$

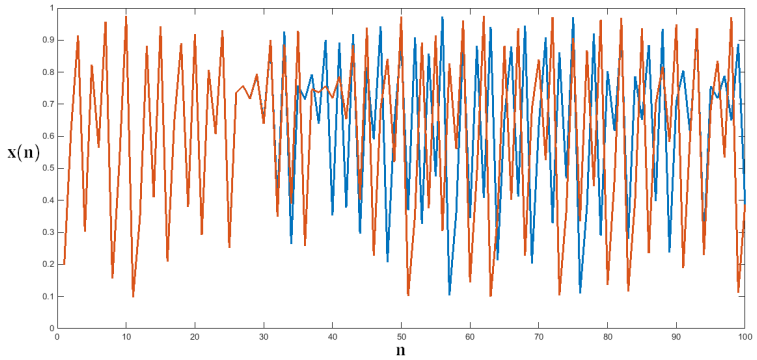
[1] سخنران

[2] Chaotic Systems

$$x(n+۱) = a\,\frac{sin(\pi x(n))}{۴} \qquad a \in (۰, ۴] \tag{۲}$$

$$x(n+۱) = \begin{cases} u\,x(n), & x(n) < ۰/۵ \\ u\,(۱ - x(n)), & x(n) \geq ۰/۵ \end{cases} \tag{۳}$$

یکی از ویژگی های مهم نگاشت های آشوبناک، حساسیت به شرایط اولیه است. آنچنان که در شکل ۱ ملاحظه می‌شود، رفتار سیستم به ازای دو شرط اولیه متفاوت ولی نزدیک به هم، بعد از گذشت مدت زمانی به کلی متفاوت از یکدیگر شده اند. لذا پیش بینی بلند مدت رفتار آنها دشوار است. علی رغم رفتار به ظاهر تصادفی، این توابع کاملا معین و قطعی هستند. یعنی در صورت استفاده مجدد از پارامترهای دقیق و یکسان، دنباله آشوبناک جدیدی تولید نخواهد شد.



شکل ۱: حساسیت به شرایط اولیه در دنباله آشوبناک لجستیک، آبی $x(۰) = ۰/۲$ و قهوه ای $x(۰) = ۰/۲ + ۱۰^{-۹}$

تبدیل موجک شباهت بین یک سیگنال دلخواه را با یک موجک به اصطلاح مادر[۳] بررسی می کند. موجک مادر در طول سیگنال اصلی جابه جا شده و براي هر موقعیت آن، شباهت سیگنال با موجک مادر محاسبه مي شود. سپس این کار برای توابع موجک دختر[۴] (رابطه ۴) که با تغییر مقیاس موجک مادر بدست می آیند تکرار خواهد شد و در نهایت مجموعه‌اي از ضرایب تبدیل موجک بر حسب میزان انتقال تابع موجک و مقیاس آن بدست می آید.

$$h_{a,b}(t) = \frac{۱}{\sqrt{a}} h(\frac{t-b}{a}) \tag{۴}$$

در رابطه فوق h موجك مادر، a پارامتر مقیاس[۵] و b تعیین کننده ی میزان انتقال است. ضریب $\frac{۱}{\sqrt{a}}$ به‌منظور نرمالیزه کردن مقیاس‌هاي مختلف اضافه شده است. تصاویر و محاسبات کامپیوتر حالت گسسته دارند و لذا نیاز به نسخه تبدیل موجك گسسته[۶] است. جهت گسسته سازی، یک مقدار اولیه برای پارامترهای انتقال و مقیاس در نظر گرفته می شود. سپس مقدار آنها براساس رابطه ۵ و با کمک پارامترهای k و j تغییر داده می شوند.

$$a = a_{۰}^{j}, \quad b = k a_{۰}^{j} T \quad j, k \in \mathbb{Z} \tag{۵}$$

در رابطه فوق T یک زمان ثابت می باشد. با تعاریف فوق، ضرایب تبدیل موجك گسسته $c_{j,k}$ به‌صورت رابطه ۶ بدست می آیند.

$$c_{j,k} = \int_{-\infty}^{\infty} f(t) h_{j,k}^{*}(t) dt \tag{۶}$$

در رابطه فوق $*$ عملگر مزدوج مختلط بوده و داریم:

$$h_{j,k}(t) = a_{۰}^{-j/۲} h(a_{۰}^{-j} t - kT) \tag{۷}$$

[3] Mother Wavelet
[4] Daughter Wavelet
[5] Scale Factor
[6] Discrete Wavelet Transform (DWT)

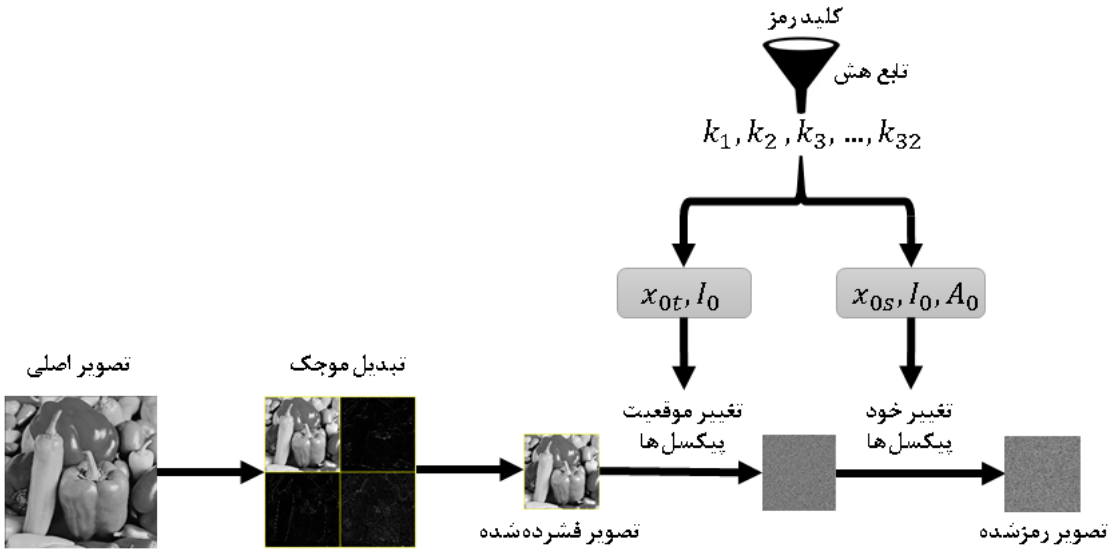
بازسازي سیگنال اصلی نیز براساس ضرایب تبدیل موجک گسسته با رابطه زیر صورت می گیرد.

$$f(t) \approx c \sum_{j} \sum_{k} c_{j,k} h_{j,k}(t) \quad (۸)$$

در رابطه فوق مقدار ثابت c وابسته به موجک مادر انتخابی است. با تعمیم روابط ریاضی فوق، می توان از تبدیل موجک در پردازش و رمزنگاری تصاویر استفاده نمود. لازم به ذکر است که در عمل تبدیل موجک با استفاده از یک بانک فیلتری پیاده‌سازی می‌شود[۹، ۱۰].

۳ الگوریتم پیشنهادی

روند الگوریتم پیشنهادی به صورت فلوچارت در شکل ۲ ترسیم شده است که شامل مراحل زیر می باشد:



شکل ۲: الگوریتم پیشنهادی

۱. فشرده سازی تصویر انتخابی با تبدیل موجک تا یک لایه.

۲. دریافت کلید رمز توسط تابع هش $SHA۲۵۶$ و تولید یک رشته ۳۲ تایی از اعداد صحیح بین ۰ تا ۲۵۵. به عنوان مثال در صورت انتخاب کلید رمز [۰،۲۵۵] خروجی تابع هش به صورت زیر خواهد بود.

$$SHA۲۵۶([۰, ۲۵۵]) = [۴۷\ ۱۳۴\ ۱۵۲\ ۱۵\ ۲۵۳\ ۴۱\ ۲۴۷\ ۱۶۶\ ۱۹\ ۹۳\ ۱۹۷\ ۱۹۹\ ۲۲۶\ ۰\ ۲۱۲\ ۷۵\ ۵۰$$
$$۶۴\ ۲۴۱\ ۴۶\ ۱\ ۱۹۱\ ۱۲۷\ ۱۵۳\ ۲۴۹\ ۱۲\ ۲۲۷\ ۲۴۰\ ۱۹۸]$$

۳. استفاده از خروجی تابع هش جهت تعیین پارامترها و شرایط اولیه مورد نیاز. اگر خروجی تابع هش را به صورت اعداد $k_۳۲, ..., k_۲, k_۱$ در نظر بگیریم، پارامترهای مورد نیاز به صورت روابط زیر تعیین می شوند.

$$\begin{cases} P_۱ = k_۱ \oplus k_۵ \oplus k_۹ \oplus k_{۱۳} + k_{۱۷} \oplus k_{۲۱} \oplus k_{۲۵} \oplus k_{۲۹} \\ P_۲ = k_۲ \oplus k_۶ \oplus k_{۱۰} \oplus k_{۱۴} + k_{۱۸} \oplus k_{۲۲} \oplus k_{۲۶} \oplus k_{۳۰} \\ P_۳ = k_۳ \oplus k_۷ \oplus k_{۱۱} \oplus k_{۱۵} + k_{۱۹} \oplus k_{۲۳} \oplus k_{۲۷} \oplus k_{۳۱} \\ P_۴ = k_۴ \oplus k_۸ \oplus k_{۱۲} \oplus k_{۱۶} + k_{۲۰} \oplus k_{۲۴} \oplus k_{۲۸} \oplus k_{۳۲} \end{cases} \quad (۹)$$

$$\begin{cases} x_{۰s} = mod(P_۱, ۲۵۶)/۲۵۶ \\ x_{۰s} = mod(P_۲, ۲۵۶)/۲۵۶ \\ A_۰ = mod(P_۳, ۲۵۶) \\ I_۰ = P_۴ + ۵۰ \end{cases} \quad (۱۰)$$

در روابط فوق $\oplus$ عملگر XOR بوده و $mod(P, ۲۵۶)$ مقدار باقیمانده حاصل از تقسیم عدد P بر ۲۵۶ می باشد. طبق روابط فوق $P_۱$ تا $P_۴$ اعدادی صحیحی بین ۰ تا ۵۱۲ خواهند بود. در مراحل بعدی پارامتر های $x_{۰s}$، $x_{۰t}$، $A_۰$ و $I_۰$ استفاده خواهند شد.

۴. اگر سایز تصویر $M \times N$ باشد، با استفاده از نگاشت آشوبناک Tent (رابطه ۳) و شرط اولیه $x_{۰t}$ یک دنباله $M \times N + I_۰$ تایی از اعداد شبه تصادفی تولید می کنیم و متناظر با سایز تصویر تنها $M \times N$ عدد انتهایی را نگه می داریم. دلیل صرفه نظر از $I_۰$ عدد نخست، بالا بردن حساسیت الگوریتم به پارامتر $x_{۰t}$ می باشد.

۵. دنباله آشوبناک مرحله قبل را به ترتیب صعودی مرتب کرده و به طور متناظر موقعیت پیکسل های تصویر فشرده شده را نیز تغییر می دهیم. ماتریس حاصل را A می نامیم.

۶. با استفاده از نگاشت آشوبناک Sine (رابطه ۲) و شرط اولیه $x_{۰s}$ یک دنباله $N + I_۰$ تولید کرده و برای مرحله بعد تنها N عدد آخر آن را در نظر می گیریم.

۷. هر کدام از N عدد تولید شده مرحله قبل را به عنوان شرط اولیه نگاشت آشوبناک لجستیک (رابطه ۱) در نظر گرفته و برای هر کدام، یک دنباله M تایی از اعداد را تولید می کنیم. لذا با دو نگاشت Sine و لجستیک یک ماتریس $M \times N$ از اعداد شبه تصادفی تولید می شود که آنرا x می نامیم.

۸. با رابطه زیر درایه های ماتریس x را که بین صفر تا ۱ می باشند، به اعدادی صحیح در بازه $[۰, ۲۵۵]$ تبدیل و در X ذخیره می کنیم.

$$X = (mod(abs(fix((x \times ۱۰^{۲} - round(x \times ۱۰^{۲})) \times ۱۰^{۱۴})), ۲۵۶)) \qquad (۱۱)$$

۹. طبق روابط زیر ماتریس A بدست آمده در مرحله ۵ را با اعداد ماتریس X ترکیب تا تصویر رمزشده E بدست آید.

$$\begin{cases} E(i,j) = A(i,j) \oplus (mod(A_۰ + X(i,j), ۲۵۶) \oplus X(i,j)) & i = j = ۱ \\ E(i,j) = A(i,j) \oplus (mod(E(i-۱,j) + X(i,j), ۲۵۶) \oplus X(i-۱,j)) & i > ۱ \; j = ۱ \\ E(i,j) = A(i,j) \oplus (mod(E(i,j-۱) + X(i,j), ۲۵۶) \oplus X(i,j-۱)) & i > ۱ \; j > ۱ \end{cases}$$

دقت نمایید مراحل فوق با داشتن تصویر رمز شده و کلید رمز معکوس پذیر می باشد.

۴ اعتبارسنجی الگوریتم های رمزنگاری

جهت اعتبارسنجی بهتر الگوریتم پیشنهادی، دو الگوریتم [۱] و [۲] که دارای عملکرد مناسبی در رمزنگاری بوده اند انتخاب و شبیه سازی شده اند و از خروجی کدهای شبیه سازی شده این دو مرجع جهت تکمیل جداول استفاده شده است. در ادامه جهت کاهش نتایج تصویری تنها از تصویر Peppers استفاده شده است اما در جداول نتایج دیگر تصاویر استاندارد سیاه-سفید (Lena، Baboon و Airplane) آورده شده است.

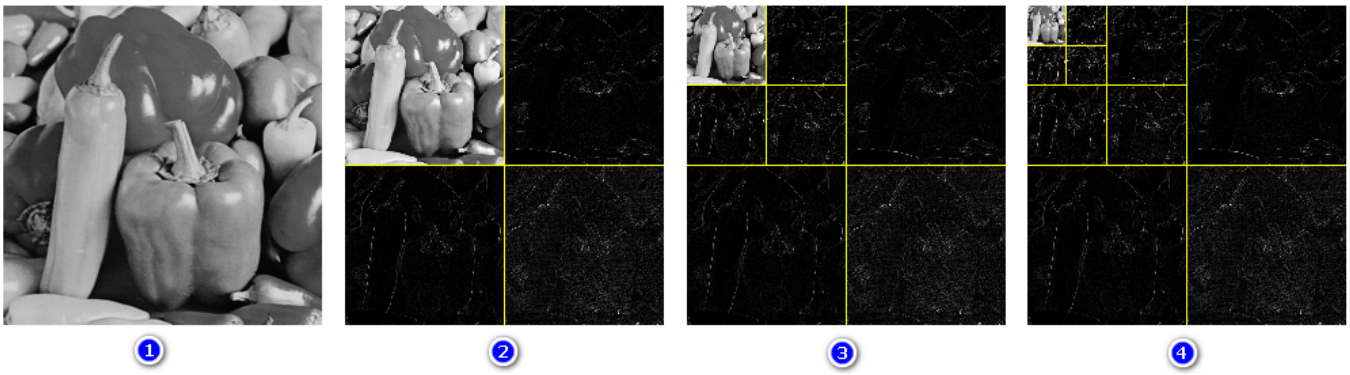
۱.۴ معیار انرژی در تبدیل موجک

شکل ۳ تاثیر استفاده از تبدیل موجک تا ۳ لایه بر روی یک تصویر انتخابی را نشان می دهد. همانطورکه از شکل مشخص است، با هر بار استفاده از تبدیل موجک، حجم داده ها جهت انتقال در کانال ارتباطی ٪۷۵ کاهش می یابد. مطابق مرجع [۲] می توان از معیار نسبت انرژی ER[۷] جهت اندازه گیری نسبت حجم اطلاعات موجود در بخش ماتریس ضرایب فرکانس پایین تبدیل موجک (تصویر تقریب) به کل ضرایب تبدیل موجک استفاده کرد. این معیار به صورت زیر تعریف می شود.

$$ER = \frac{E_{ca}}{E_{total}} \qquad (۱۲)$$

در رابطه فوق E_{ca} انرژی ضرایب بخش فرکانس پایین لایه انتخابی در تبدیل موجک و E_{total} انرژی کل ضرایب می باشد. در رابطه ۱۲ انرژی هر بخش از ماتریس ضرایب تبدیل موجک $A(u,v)$ به صورت رابطه ۱۳ بدست می آید.

[7] Energy Ratio



شکل ۳: تبدیل موجک: ۱-تصویر اصلی، ۲-فشرده سازی تا یک لایه ۳-فشرده سازی تا دو لایه ۳-فشرده سازی تا سه لایه

جدول ۱: معیار انرژی

	Lena	Baboon	Peppers	Airplane
لایه اول	۰/۹۹۸۹	۰/۹۸۳۸	۰/۹۹۶۱	۰/۹۹۷۵
لایه دوم	۰/۹۹۶۰	۰/۹۷۱۲	۰/۹۹۰۶	۰/۹۹۳۶
لایه سوم	۰/۹۸۸۹	۰/۹۶۲۵	۰/۹۸۰۶	۰/۹۸۷۳
لایه چهارم	۰/۹۷۳۲	۰/۹۵۵۱	۰/۹۶۲۳	۰/۹۷۹۳

$$E = \sum_{u} \sum_{v} A(u,v)^{۲} \tag{۱۳}$$

نتایج حاصل از تبدیل موجک بر تصاویر انتخابی تا ۴ لایه و با استفاده از موجک مادر هار[8] مطابق جدول ۱ می باشد. همانطور که از اعداد جدول مشخص است، هر چند معیار انرژی با افزایش لایه انتخابی در تبدیل موجک کاهش یافته است؛ ولی همچنان بخش عمده انرژی و یا به عبارت دیگر اطلاعات، مربوط به تصویر تقریب می باشد. لذا با استفاده از تبدیل موجک و معیار انرژی می توان با کاهش حجم اطلاعات، از کانال های ارتباطی با ظرفیت محدود جهت انتقال تصاویر رمزنگاری شده استفاده نمود.

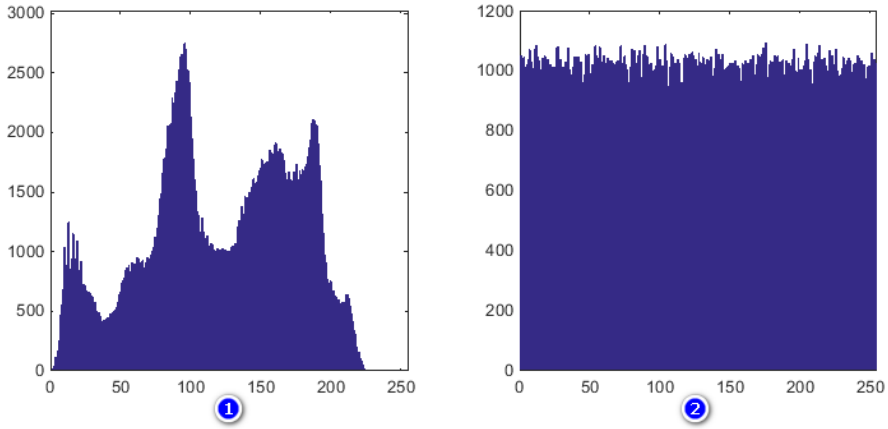
۲.۴ هیستوگرام یک تصویر

هیستوگرام[9] یک تصویر رمزشده که میزان استفاده از هر رنگ در کل تصویر را نشان می دهد بایستی یکنواخت بوده و شباهتی به هیستوگرام تصویر اصلی نداشته باشد. شکل ۴ نشان می دهد الگوریتم پیشنهادی توانسته است به خوبی هیستوگرام تصویر رمز شده را یکنواخت بکند. می توان جهت سنجش یکنواختی نمودار هیستوگرام از آزمون مربع کای [10] مطابق رابطه ۱۴ استفاده نمود [۱]، که نتایج آن در جدول ۲ نشان داده شده است.

$$\chi^{۲} - value = \sum_{i=۱}^{k} \frac{(x_i - m_i)^{۲}}{m_i} \tag{۱۴}$$

در رابطه ۱۴ مقدار k برابر ۲۵۶ و x_i و m_i به ترتیب رخداد پیکسل ها با رنگ $i = ۰, ..., ۲۵۵$ در تصویر و تعداد رخداد ایده آل آن می باشد. جهت داشتن دیدی از یکنواختی اگر میزان تفاوت تنها ۲۰ عدد پیکسل باشد شاخص آزمون مربع کای برابر با ۴۰۰ خواهد بود که طبق جدول ۲ هر سه الگوریتم عملکردی مناسبی دارند و الگوریتم پیشنهادی در سه مورد توانسته است بهتر از دو مرجع دیگر عمل کند.

[8] Haar Wavelet
[9] Histogram
[10] Chi-squared test



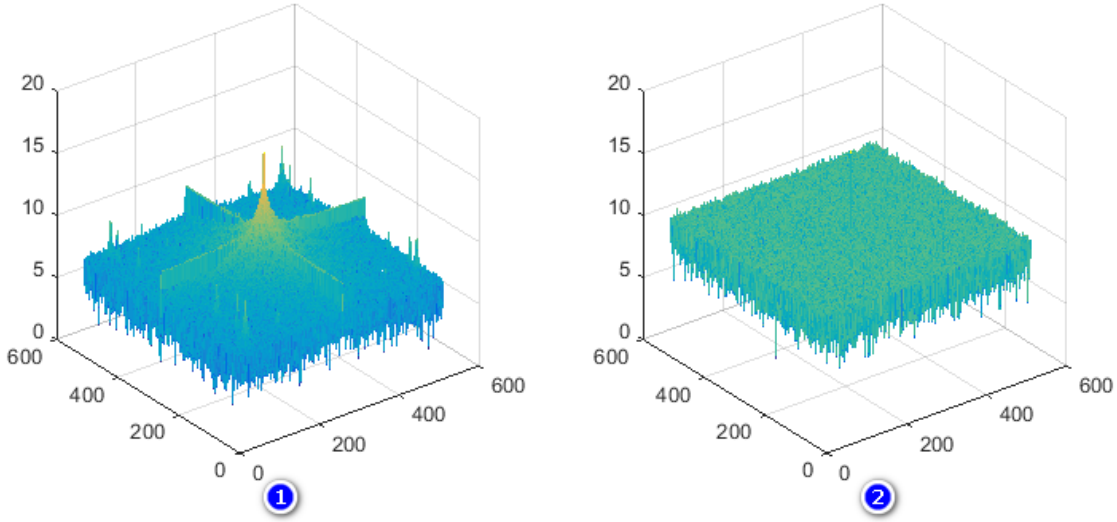
شکل ۴: الگوی رنگ های استفاده شده در ۱- تصویر Peppers و ۲- رمز شده آن

جدول ۲: آزمون مربع کای

	Lena	Baboon	Peppers	Airplane
تصویر انتخابی	۱۵۸۰۶۴	۱۸۷۳۵۶	۱۲۰۱۶۵	۷۱۷۷۷۹
الگوریتم پیشنهادی	۲۸۷٫۵	۲۴۷٫۳	۲۱۹٫۰	۲۲۹٫۱
مرجع [۱]	۳۰۰٫۵	۲۵۷٫۰	۲۸۹٫۴	۲۷۳۰۵
مرجع [۲]	۲۵۸٫۵	۲۵۶٫۷	۲۳۷٫۹	۲۷۱٫۵

۳.۴ حوزه فرکانس تصویر

مشابه معیار قبل تا حد امکان بایستی ضرایب تبدیل فوریه تصویر رمز شده یکنواخت باشد. مطابق شکل ۵ ضرایب تبدیل فوریه تصویر انتخابی در رنج فرکانس پایین بوده، ولی ضرایب تبدیل فوریه تصویر رمز شده به طور یکنواخت در حوزه فرکانس پخش شده اند که نشان دهنده ی عملکرد مناسب الگوریتم پیشنهادی می باشد [۳].



شکل ۵: ۱- تبدیل فوریه تصویر Peppers و ۲- رمز شده آن

جدول ۳: معیار آنتروپی

	Lena	Baboon	Peppers	Airplane
تصویر انتخابی	۷٫۴۴۵۵	۷٫۳۵۸۳	۷٫۵۹۳۷	۶٫۷۰۲۵
الگوریتم پیشنهادی	۷٫۹۹۹۲	۷٫۹۹۹۳	۷٫۹۹۹۴	۷٫۹۹۹۴
مرجع [۱]	۷٫۹۹۹۲	۷٫۹۹۹۳	۷٫۹۹۹۲	۷٫۹۹۹۲
مرجع [۲]	۷٫۹۹۹۳	۷٫۹۹۹۳	۷٫۹۹۹۳	۷٫۹۹۹۳

۴.۴ آنتروپی

آنتروپی[11] یک معیار در اندازه گیری نامعینی و یا میزان رندم بودن یک سری داده می باشد. به نوعی با آنتروپي می توان میزان تیز بودن قله های نمودار هیستوگرام را سنجید. آنتروپی یک تصویر به صورت زیر بدست می آید [۷، ۳].

$$H(m) = \sum_{i=۰}^{۲^N-۱} p(m_i) log_۲ \frac{۱}{p(m_i)} \quad (۱۵)$$

که $p(m_i)$ میزان احتمال رخداد پیکسل m_i در تصویر بوده و N تعداد بیت استفاده شده برای هر پیکسل جهت ذخیره سازی داده ها می باشد. برای تصاویر سیاه-سفید که شدت روشنایی پیکسل‌ها را عموماً با اعدادی بین ۰ تا ۲۵۵ نشان می‌دهند، مقدار ایده آل آنتروپی برابر با ۸ می‌باشد. با توجه به جدول ۳، مقدار آنتروپی تصاویر رمز شده برای الگوریتم های رمزنگاری انتخابی مناسب و نزدیک به مقدار ایده آل می باشند.

۵.۴ ضریب همبستگی

ضریب همبستگی[12] نمایانگر میزان شباهت بین پیکسل‌های مجاور یک تصویر است. این مجاورت می تواند در سه راستای افقی، عمودی و یا قطری باشد. نیاز است که در تصویر رمزنگاری‌شده این همبستگی بسیار کاهش یابد و نزدیک به صفر باشد. ضریب همبستگی γ_{xy} با روابط زیر محاسبه می شود [۳] .

$$cov(x,y) = E[(x - E(x))(y - E(y))] = \frac{۱}{N} \sum_{i=۱}^{N} (x_i - E(x))(y_i - E(y)) \quad (۱۶)$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x).D(y)}} \quad (۱۷)$$

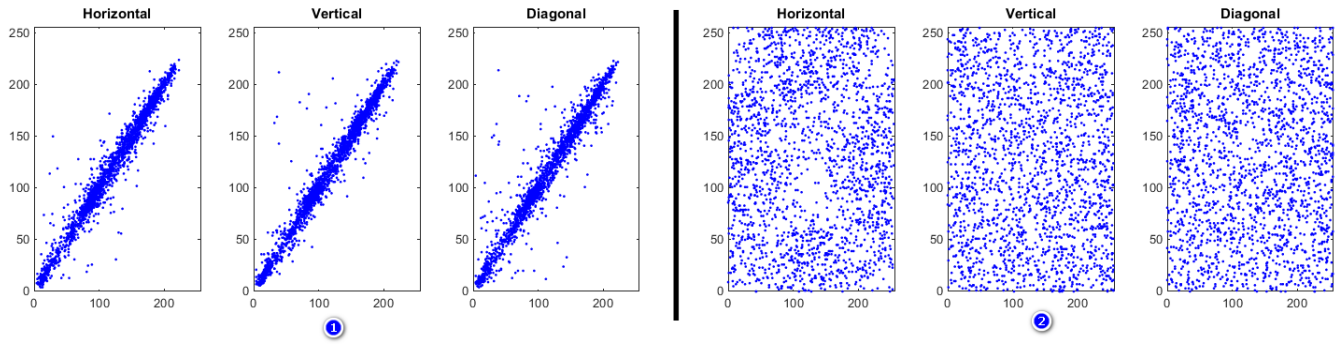
در روابط فوق x و y مقادیر عددی دو پیکسل مجاور بوده و $E(x) = \frac{۱}{N} \sum_{i=۱}^{N} x_i$ و $D(x) = \frac{۱}{N} \sum_{i=۱}^{N} (x_i - E(x))^۲$ می باشد. در این مطالعه از تصاویر اصلی و رمز شده به طور تصادفی ۲۰۰۰ جفت پیکسل مجاور در راستای افقی، عمودی و قطری انتخاب گردید و نتایج حاصل در جدول ۴ آورده شده است. مطابق جدول و شکل ۶ الگوریتم پیشنهادی توانسته است به خوبی دو مرجع دیگر، این معیار را نیز برآورده نماید.

۶.۴ میانگین مربع خطا و پیک نسبت سیگنال به نویز

دو معیار میانگین مربع خطا[13] MSE و پیک نسبت سیگنال به نویز[14] PSNR از معیارهای متداول جهت اندازه گیری کیفیت یک الگوریتم رمزنگاری می باشد که مطابق روابط زیر بدست می آیند [۳، ۱۱].

$$MSE = \frac{۱}{M \times N} \sum_{i=۱}^{M} \sum_{j=۱}^{N} (x(i,j) - y(i,j))^۲ \quad (۱۸)$$

[11] Entropy
[12] Correlation Coefficient
[13] Mean Squared Error
[14] Peak Signal-to-Noise Ratio



شکل ۶: رابطه ۲۰۰۰ پیکسل مجاور از ۱- تصویر Peppers و ۲- رمز شده آن در سه راستای افقی، عمودی و قطری

جدول ۴: معیار ضریب همبستگی

	جهت	Lena	Baboon	Peppers	Airplane
تصویر انتخابی	افقی	۰٫۹۸۴۰	۰٫۷۴۶۶	۰٫۹۷۹۹	۰٫۹۶۰۳
	عمودی	۰٫۹۷۱۷	۰٫۸۶۹۷	۰٫۹۷۷۳	۰٫۹۶۷۸
	قطری	۰٫۹۵۸۷	۰٫۷۳۳۶	۰٫۹۶۵۵	۰٫۹۴۲۰
الگوریتم پیشنهادی	افقی	۰٫۰۰۰۷	۰٫۰۲۰۴	۰٫۰۱۱۹	۰٫۰۲۳۰
	عمودی	۰٫۰۴۴۸	۰٫۰۲۷۰	۰٫۰۴۱۲	۰٫۰۳۷۶
	قطری	۰٫۰۰۸۴	۰٫۰۱۲۳	۰٫۰۱۴۲	۰٫۰۰۸۵
مرجع [۱]	افقی	۰٫۰۱۱۴	۰٫۰۰۱۲	۰٫۰۱۵۷	۰٫۰۰۰۳
	عمودی	۰٫۰۱۹۹	۰٫۰۴۷۷	۰٫۰۲۹۳	۰٫۰۱۲۲
	قطری	۰٫۰۱۸۴	۰٫۰۱۱۰	۰٫۰۱۰۳	۰٫۰۱۵۱
مرجع [۲]	افقی	۰٫۲۶۵۵	۰٫۳۳۲۶	۰٫۲۰۸۱	۰٫۰۰۴۰
	عمودی	۰٫۰۱۰۴	۰٫۰۰۶۵	۰٫۰۱۴۷	۰٫۰۵۶۷
	قطری	۰٫۰۴۰۹	۰٫۰۱۲۱	۰٫۰۱۳۷	۰٫۰۱۶۹

$$PSNR = ۱۰log_{۱۰}\frac{L^۲}{MSE} \qquad (۱۹)$$

در روابط فوق x و y مقادیر عددی پیکسل های دو تصویر بوده و L میزان تغییرات رنگ پیکسل می باشد. برای یک تصویر سیاه-سفید که با ۸ بیت، رنگ هر پیکسل مشخص می شود، این عدد برابر با $L = ۲^۸ - ۱ = ۲۵۵$ می باشد. براساس این دو معیار هر چقدر MSE بین دو تصویر اصلی و رمز شده بزرگتر باشد، به عبارت دیگر مقدار PSNR کوچکتر باشد، بدین معنا خواهد بود که اختلاف بین دو تصویر اصلی و رمز شده زیاد است، که این حالت نشان دهنده ی یک الگوریتم رمزنگاری مناسب می باشد. با توجه به اعداد MSE و PSNR مربوط به سه الگوریتم رمزنگاری در جدول ۵ الگوریتم پیشنهادی به خوبی دو مرجع دیگر، این معیار را برآورده کرده است.

جدول ۵: معیار MSE و PSNR بین تصاویر انتخابی و رمز شده

	Lena		Baboon		Peppers		Airplane	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
الگوریتم پیشنهادی	۷۸۰۴	۹٫۲۰۷	۷۲۳۲	۹٫۵۳۸	۸۴۱۱	۸٫۸۸۲	۱۰۲۸۵	۸٫۰۰۸
مرجع [۱]	۷۷۷۵	۹٫۲۲۳	۷۲۴۹	۹٫۵۲۸	۸۴۲۱	۸٫۸۷۷	۱۰۲۸۵	۸٫۰۰۸
مرجع [۲]	۷۷۶۷	۹٫۲۲۷	۷۲۵۱	۹٫۵۲۶	۸۴۱۹	۸٫۸۷۷	۱۰۲۹۴	۸٫۰۰۴

جدول ۶: فضای کلید رمز الگوریتم پیشنهادی و دیگر مراجع

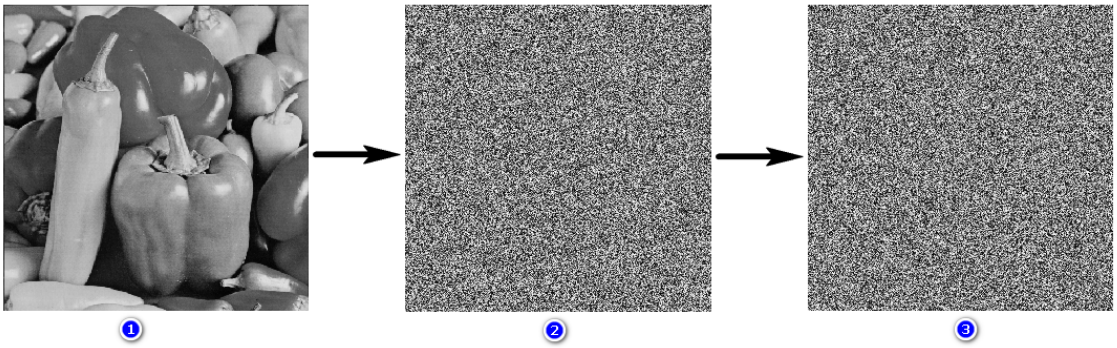
	الگوریتم پیشنهادی	[۵]	[۱۳]	[۱۴]	[۱۵]	[۱۶]	[۱۷]
فضای کلید رمز	∞ (ورودی تابع هش) $۲^{۲۵۶}$ (خروجی تابع هش)	$۲^{۳۶۰} + ۲^{۱۴۴}$	$۱۰^{۳۴}$	$۲^{۲۷۶}$	$۱۰^{۵۶}$	$۲^{۱۴۹}$	$۱۰^{۶۰}$

۷.۴ فضای کلید رمز

در یک الگوریتم رمزنگاری بایستی سعی شود فضای کلید یا پارامترهای قابل حدس برای شکستن رمز بزرگ باشد. برای الگوریتم معرفی شده که در آن یک تابع هش کلید رمز را دریافت می کند، تعداد حالات ممکن برای کلید رمز ∞ می باشد و در صورت مد نظر قرار دادن خروجی آن به عنوان فضای کلید رمز الگوریتم، تعداد حالات ممکن برابر با $۲^{۲۵۶}$ می باشد و لذا در مقایسه با دیگر مراجع (جدول ۶) از فضای کلید رمز قابل قبولی برخوردار می باشد.

۸.۴ حساسیت به کلید رمز

یک الگوریتم رمزنگاری بایستی حساسیت بالایی به هر تغییر اندک در کلید رمز داشته باشد. حساسیت بالای یک الگوریتم به کلید رمز[15] باعث می شود که در صورت تغییر اندک کلید رمز، تصویر رمز شده جدید شباهتی به تصویر رمز شده قبلی نداشته باشد. این امر به هنگام بازیابی تصویر اصلی از تصویر رمزشده نیز صادق است. در شکل ۷ جهت بازیابی تصویر رمزنگاری شده با الگوریتم پیشنهادی، تنها یک پیکسل از کلید رمز الگوریتم را به اندازه یک واحد تغییر داده ایم. همانطور که مشاهده می شود تصویر بازیابی شده هیچ شباهتی به تصویر اصلی ندارد.



شکل ۷: ۱- تصویر اصلی ، ۲- تصویر رمزنگاری شده و ۳- تصویر بازیابی شده با کلید رمز نادرست ولی نزدیک به کلید رمز صحیح

عموما حساسیت یک الگوریتم رمزنگاری به کلید را می توان با توابع NPCR[16] و UACI[17] سنجید [۲].

$$NPCR = \frac{۱}{M \times N} \sum_{i=۱}^{M} \sum_{j=۱}^{N} D(i,j) \times ۱۰۰\% \qquad (۲۰)$$

$$UACI = \frac{۱}{M \times N} \sum_{i=۱}^{M} \sum_{j=۱}^{N} \frac{|C_۱(i,j) - C_۲(i,j)|}{۲^Q - ۱} \times ۱۰۰\% \qquad (۲۱)$$

در روابط فوق M و N نشان دهنده تعداد سطر و ستون های تصویر، Q تعداد بیت استفاده شده برای هر پیکسل، $C_۱$ و $C_۲$ دو تصویر رمز نگاری شده با کلید رمز درست و تغییر یافته آن است. مقدار $D(i,j)$ برابر صفر است اگر دو پیکسل در دو تصویر برابر باشند و مقدار آن یک است اگر با هم برابر نباشند. مقدار ایده آل برای NPCR و UACI به ترتیب برابر ۱۰۰ و ۳۳.۳۳ درصد می باشد. لذا با توجه به جدول ۷ عملکرد هر سه الگوریتم مناسب می باشد.

[15] Key Sensitivity
[16] Number of Pixel Change Rate
[17] Unified Average Changing Intensity

جدول ۷: حساسیت الگوریتم رمزنگاری به تغییر یک درصد کلید رمز

		Lena		Baboon		Peppers		Airplane	
		NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
الگوریتم پیشنهادی	کلید اول	۰٫۹۹۶۰	۰٫۳۳۴۹	۰٫۹۹۶۳	۰٫۳۳۴۲	۰٫۹۹۶۰	۰٫۳۳۳۹	۰٫۹۹۵۹	۰٫۳۳۳۹
	کلید دوم	۰٫۹۹۶۱	۰٫۳۳۵۳	۰٫۹۹۵۹	۰٫۳۳۴۳	۰٫۹۹۵۹	۰٫۳۳۴۶	۰٫۹۹۶۱	۰٫۳۳۳۹
مرجع [۱]	کلید اول	۰٫۹۹۶۰	۰٫۳۳۴۷	۰٫۹۹۶۰	۰٫۳۳۵۲	۰٫۹۹۵۹	۰٫۳۳۴۶	۰٫۹۹۶۰	۰٫۳۳۴۴
	کلید دوم	۰٫۹۹۶۰	۰٫۳۳۴۲	۰٫۹۹۶۳	۰٫۳۳۴۴	۰٫۹۹۶۲	۰٫۳۳۴۵	۰٫۹۹۶۱	۰٫۳۳۴۴
مرجع [۲]	کلید اول	۰٫۹۹۶۲	۰٫۳۳۵۰	۰٫۹۹۶۱	۰٫۳۳۴۵	۰٫۹۹۶۱	۰٫۳۳۵۲	۰٫۹۹۶۲	۰٫۳۳۴۳
	کلید دوم	۰٫۹۹۶۱	۰٫۳۳۴۶	۰٫۹۹۶۱	۰٫۳۳۴۵	۰٫۹۹۶۰	۰٫۳۳۴۰	۰٫۹۹۶۱	۰٫۳۳۴۳

جدول ۸: حساسیت الگوریتم رمزنگاری به تغییر یک واحد در یک پیکسل از تصویر اصلی

	Lena		Baboon		Peppers		Airplane	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
الگوریتم پیشنهادی	۰٫۰۰۱	۴×۱۰^{-۶}	۰٫۰۰۱	۸×۱۰^{-۶}	۰٫۰۰۱۰	۸×۱۰^{-۶}	۰٫۰۰۱۷	۷×۱۰^{-۴}
مرجع [۱]	۰٫۹۹۶۲	۰٫۳۳۴۵	۰٫۹۹۶	۰٫۳۳۴۴	۰٫۹۹۶۲	۰٫۳۳۴۶	۰٫۹۹۵۹	۰٫۳۳۳۵
مرجع [۲]	۰٫۰۹۶۸	۷×۱۰^{-۴}	۰٫۰۹۶۸	۷×۱۰^{-۴}	۰٫۰۹۶۸	۷×۱۰^{-۴}	۰٫۰۹۶۸	۷×۱۰^{-۴}

۹.۴ حساسیت به تغییر تصویر

حساسیت به تغییر در تصویر اصلی [۱۸] یکی دیگر از معیارهای بررسی عملکرد یک الگوریتم رمزنگاری تصویر می باشد. در صورت تغییر کوچک در تصویر اصلی، تصویر رمزنگاری شده بایستی تا حد امکان تغییرات شدیدی نسبت به تصویر رمز شده قبلی داشته باشد. در این صورت الگوریتم در مقابل حملات به اصطلاح تفاضلی مقاوم خواهد بود [۳]. در این مطالعه یک پیکسل از تصویر اصلی را به اندازه ۱ واحد تغییر داده و و مجدد آن را رمزنگاری کردیم. سپس معیارهای NPCR و UACI را بین دو تصویر رمز شده جدید و رمز شده قبلی را مطابق جدول ؟؟ بدست آورده ایم. براساس این جدول تنها الگوریتم مرجع [۱] توانسته است حساسیت مناسبی به تغییرات تصویر داشته باشد. این الگوریتم وابستگی زیادی به اطلاعات تصویر دارد و انتظار می رود که نتواند دو معیار مقاومت در برابر نویز و از دست دادن قسمتی از تصویر را برآورده سازد. معیارهایی که الگوریتم های پیشنهادی و مرجع [۲] عملکرد مناسبی از خود نشان داده اند.

۱۰.۴ مقاومت الگوریتم در برابر نویز

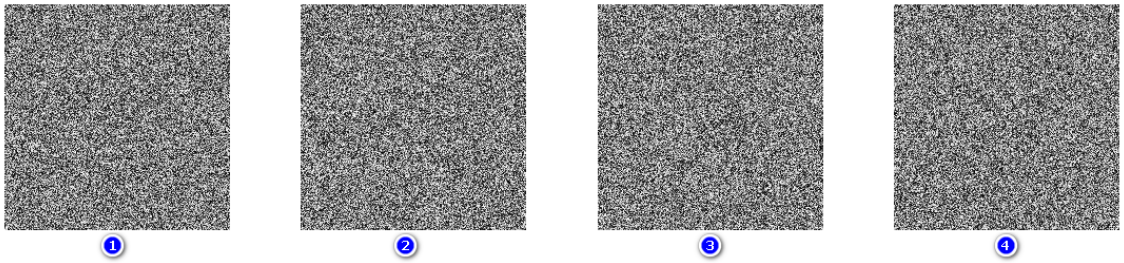
برخی کانال های ارتباطی تحت تاثیر نویز هستند و یک الگوریتم رمزنگاری مناسب بایستی در برابر آن مقاوم بوده و بتواند اطلاعات خود را تا حد امکان حفظ نماید. جهت تست الگوریتم های رمزنگاری، می توان تصویر رمزشده را تحت تاثیر نویزهای گاوسی[۱۹]، پواسون[۲۰]، فلفل-نمکی[۲۱] و نقطه ای[۲۲] قرار داد و سپس تصویر دریافتی را با کلید رمز صحیح بازیابی نمود. شکل های ۸، ۹ و ۱۰ عملکرد سه الگوریتم رمزنگاری را در مقابل چهار نویز نام برده شده را نشان می دهند. مطابق تصاویر و جدول ۹ و برعکس معیار قبلی، بهترین عملکرد را مرجع [۲] و سپس الگوریتم پیشنهادی دارد و الگوریتم مرجع [۱] در مقابل نویز مقاوم نیست.

۱۱.۴ مقاومت الگوریتم در برابر از دست دادن قسمتی از تصویر

مشابه قسمت قبل ممکن است حین ارسال یک تصویر رمز شده، بخشی از داده های آن به کلی از بین برود. مطابق شکل ۱۱ و براساس جدول ۱۰ بهترین عملکرد را الگوریتم پیشنهادی و مرجع [۲] دارند و الگوریتم مرجع [۱] در مقابل از دست رفتن داده در کانال ارتباطی مقاوم نیست.

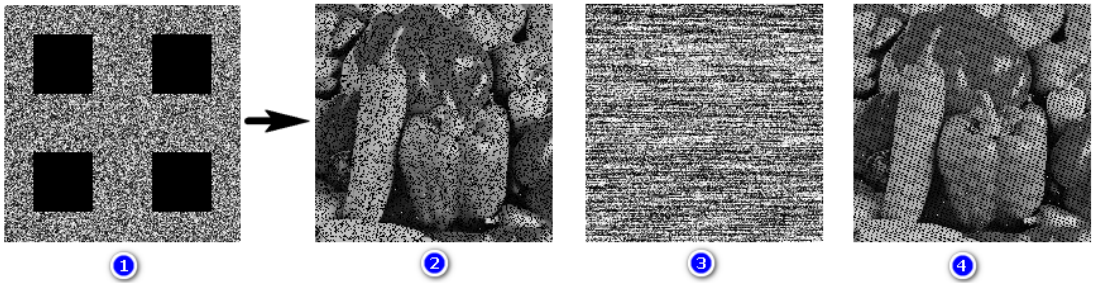
[18] Original Image Sensitivity
[19] Gaussian noise
[20] Poisson noise
[21] Salt and Pepper noise
[22] Speckle noise

شکل ۸: مقاومت الگوریتم پیشنهادی به نویزهای ۱- گاوسی، ۲- پواسون، ۳- فلفل-نمکی و ۴- نقطه ای



شکل ۹: مقاومت الگوریتم مرجع [۱] به نویزهای ۱- گاوسی، ۲- پواسون، ۳- فلفل-نمکی و ۴- نقطه ای

شکل ۱۰: مقاومت الگوریتم مرجع [۲] به نویزهای ۱- گاوسی، ۲- پواسون، ۳- فلفل-نمکی و ۴- نقطه ای



شکل ۱۱: ۱- از دست رفتن داده در کانال ارتباطی و بازیابی با ۲- الگوریتم پیشنهادی، ۳- مرجع [۱] و ۴- مرجع [۲]

۱۲.۴ سرعت اجرای الگوریتم رمزنگاری

طبیعتا یک الگوریتم رمزنگاری تصویر بایستی به گونه ای طراحی بشود که بتواند با سخت افزار موجود، تصویر مورد نظر را در یک زمان مناسب رمزنگاری نماید. هر چند سرعت یک الگوریتم به پارامترهای مختلفی همچون سرعت پردازنده و نحوه نوشتن کد وابسته است؛ با این حال جدول ۱۱ سرعت رمزنگاری سه الگوریتم مورد بحث را بر روی یک سیستم با مشخصات $Intel\,Core\,i۳$: $Processor$ ، $۲٫۲GHz$: CPU و $۲٫۸۵GB$: RAM را نشان می دهد. انتظار می رود مطابق جدول ۱۱ و به دلیل سادگی الگوریتم پیشنهادی، سرعت اجرای آن از الگوریتم های مراجع [۱] و [۲] بیشتر باشد.

جدول ۹: معیار MSE و PSNR بین تصویر اصلی (ترکیب ۴ تصویر انتخابی) و تحت تاثیر نویز

	گاوسی		پواسون		فلفل-نمکی		نقطه ای	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
الگوریتم پیشنهادی	۴۰۱۱	۱۲٫۰۹	۲۰۱۶	۱۵٫۰۸	۱۶۷٫۰	۲۵٫۹۰	۲۴۶۴	۱۴٫۲۱
مرجع [۱]	۸۳۹۹	۸٫۸۸۸	۸۳۹۵	۸٫۸۹۰	۸۳۸۸	۸٫۸۹۴	۸٫۸۸۲	۸۴۱۰
مرجع [۲]	۲۲۳۹	۱۴٫۶۲	۴۲۵٫۵	۲۱٫۸۴	۱۶۸٫۰	۲۵٫۸۷	۷۱۸٫۵	۱۹٫۵۶

جدول ۱۰: معیار MSE و PSNR بین تصاویر اصلی و بازیابی شده تحت تاثیر از دست رفتن ۲۵ درصد داده در کانال ارتباطی

	Lena		Baboon		Peppers		Airplane	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
الگوریتم پیشنهادی	۴۴۵۸	۱۱٫۶۳	۴۶۷۱	۱۱٫۴۳	۴۳۶۹	۱۱٫۷۲	۸۶۳۷	۸٫۷۸۴
مرجع [۱]	۹۰۱۹	۸٫۵۷۹	۸۶۴۲	۸٫۷۶۴	۹۶۲۳	۸٫۲۹۷	۱۱۴۷۱	۷٫۵۳۴
مرجع [۲]	۴۴۵۰	۱۱٫۶۴	۴۶۷۲	۱۱٫۴۳	۴۳۷۶	۱۱٫۷۱	۸۶۰۳	۸٫۷۸۴

۵ جمع بندی و نتیجه گیری

- الگوریتم پیشنهادی می تواند با فشرده سازی مناسب تصاویر با استفاده از تبدیل موجک و معیار انرژی به طور موثر از کانال های ارتباطی با ظرفیت محدود استفاده نماید.
- انتظار می رود به دلیل سادگی و عدم استفاده از برخی تکنیک ها مانند چرخش پیکسل ها، نگاشت گربه آرنولد، جابه جا کردن بلوک ها سرعت الگوریتم پیشنهادی از دو الگوریتم شبیه سازی شده به مراتب بیشتر باشد.
- به دلیل استفاده از یک تابع هش در دریاقت کلید رمز، فضای کلید رمز الگوریتم منعطف و از بیشتر مراجع ذکر شده گسترده تر بود.
- عملکرد الگوریتم پیشنهادی در آزمون مربع کای، تا حدی بهتر از دو الگوریتم دیگر بود.
- الگوریتم پیشنهادی به همراه الگوریتم [۲] مقاومت خوبی دربرابر از دست رفتن اطلاعات در کانال ارتباطی داشت.
- ابتدا الگوریتم [۲] و سپس الگوریتم پیشنهادی عملکرد مناسبی دربرابر انواع نویز داشتند.
- از سه الگوریتم مطرح شده، تنها الگوریتم مرجع [۱] حساسیت مناسبی به تغییر در تصاویر انتخابی را داشت.

در نتایج حاصل یک رابطه معکوس بین معیار حساسیت به تغییر تصویر با معیارهای مقاومت در برابر نویز یا از دست رفتن اطلاعات در کانال ارتباطی مشاهده شده است. در ادامه سعی خواهد شد که الگوریتمی طراحی گردد تا هر سه معیار قبل را برآورده سازد و یا حداقل کابر بتواند توانایی الگوریتم را بین این معیارها تنظیم کند.

جدول ۱۱: سرعت اجرای الگوریتم های رمزنگاری برحسب ثانیه

	Lena	Baboon	Peppers	Airplane
الگوریتم پیشنهادی	۰٫۳۳۶۵	۰٫۳۴۱۶	۰٫۳۱۷۷	۰٫۳۲۵۶
مرجع [۱]	۴٫۶۸۳۴	۴٫۷۱۳۸	۴٫۶۸۱۲	۴٫۶۹۱۲
مرجع [۲]	۸٫۷۳۵۴	۸٫۶۳۰۷	۸٫۶۴۸۱	۸٫۶۹۳۸

مراجع

[1] Cao, C., Sun, K., & Liu, W. (2018). A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Processing*, 143, 122-133.

[2] Li, C. L., Li, H. M., Li, F. D., Wei, D. Q., Yang, X. B., & Zhang, J. (2018). Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik*, 171, 277-286.

[3] Luo, Y., Du, M., & Liu, J. (2015). A symmetrical image encryption scheme in wavelet and time domain. *Communications in Nonlinear Science and Numerical Simulation*, 20(2), 447-460.

[4] Bouhous, A., & Kemih, K. (2018). Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission. *Optics & Laser Technology*, 108, 162-169.

[5] Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R., & Ding, X. (2019). A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Processing*, 161, 227-247.

[6] Harini, M., Dhivya, R., & Rengarajan, A. (2020, January). Implementation of Image Encryption based on Chaos-IWT–An Image security. *IEEE, International Conference on Computer Communication and Informatics (ICCCI)*, 1-4.

[7] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, 28(4), 656-715.

[8] Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1), 29-42.

[9] Rioul, O., & Vetterli, M. (1991). Wavelets and signal processing. *IEEE signal processing magazine*, 8(4), 14-38.

[10] Merry, R. J. E. (2005). Wavelet theory and applications: a literature study. *DCT rapporten*, 2005.

[11] Wang, Z., & Bovik, A. C. (2006). Modern image quality assessment. *Synthesis Lectures on Image, Video, and Multimedia Processing*, 2(1), 1-156.

[12] Colonius, F., & Kliemann, W. (2012). *The dynamics of control*. Springer Science & Business Media.

[13] Zhou, N., Zhang, A., Zheng, F., & Gong, L. (2014). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology*, 62, 152-160.

[14] Zhou, N., Pan, S., Cheng, S., & Zhou, Z. (2016). Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Optics & Laser Technology*, 82, 121-133.

[15] Ponnaian, D., & Chandranbabu, K. (2017). Crypt analysis of an image compression–encryption algorithm and a modified scheme using compressive sensing. *Optik*, 147, 263-276.

[16] Chen, J., Zhang, Y., Qi, L., Fu, C., & Xu, L. (2018). Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. *Optics & Laser Technology*, 99, 238-248.

[17] Hu, G., Xiao, D., Wang, Y., & Xiang, T. (2017). An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *Journal of Visual Communication and Image Representation*, 44, 116-127.

پست الکترونیکی: mohammadnezhad.v@ut.ac.ir
پست الکترونیکی: arta.jamshidi@ut.ac.ir
پست الکترونیکی: rokni@ut.ac.ir