# رمزنگاری تصاویر رنگی با استفاده از الگوریتم هیل و درهم سازی کیوب

علی مرادمرد[1]، سید ابوالقاسم میر روشندل[2]، محمد تحقیقی[3]

۱کارشناسی ارشد کامپیوتر نرم‌افزار، دانشگاه آزاد اسلامی واحد زنجان، A.moradmard@gmail.com

۲استادیار دانشکده فنی دانشگاه گیلان

۳ مربی دانشگاه آزاد اسلامی واحد زنجان

تاریخ دریافت: ۹۲/۱۰/۲۲ تاریخ پذیرش: ۹۳/۸/۲۸

## چکیده

*امروزه با پیشرفت شبکه‌های کامپیوتری، سرعت انتقال اطلاعات و انواع داده‌های قابل‌انتقال افزایش‌یافته است، در نتیجه تکنیک‌هایی برای حفظ امنیت داده‌ها موردنیاز است که از آن جمله می‌توان به رمزنگاری داده‌ها اشاره نمود. در این مقاله، برای بهبود رمزنگاری هیل از یک روش رمزنگاری جدید بر مبنای درهم‌ریزی و تغییر پیکسل‌های تصویر استفاده‌شده است. در روش بیان‌شده، در ابتدا برای کم کردن وابستگی پیکسل‌ها، نیمی از تصویر توسط الگوریتم هیل رمزنگاری شده و با نیمه دیگر تصویر ترکیب می‌شود. در مرحله بعد، پیکسل‌های تمام تصویر با کمک الگوریتم کیوب توسعه‌یافته درهم‌سازی می‌شود و در نهایت، تصویر حاصل از درهم سازی شده با استفاده از الگوریتم هیل رمزنگاری می‌شود. برای بررسی کارآیی این الگوریتم از آزمون‌های بصری، تحلیل هیستوگرام، تحلیل کیفی و آزمون‌های تحلیل کلید اصلی و همبستگی استفاده شده است. نتایج حاصله، بهبود کارآیی الگوریتم پیشنهادی را در درهم ریزی پیکسل‌ها و همبستگی بین پیکسل‌ها در مقایسه با الگوریتم هیل استاندارد (به ویژه در تصاویر با پیکسل‌های مشابه) نشان می‌دهد.*

## کلید واژه

*الگوریتم هیل، الگوریتم درهم سازی کیوب ، امنیت، رمزنگاری تصاویر رنگی.*

## مقدمه

با رشد شبکه‌های اینترنتی، داده‌های بزرگی مانند فایل‌های صوتی، ویدئویی و تصاویر به راحتی می‌توانند در محیط اینترنت انتقال یابند بنابراین حفظ امنیت این داده‌ها در طول مسیر نیز همواره مورد توجه است. یکی از راه‌های حفظ امنیت داده‌ها، رمزنگاری است [۱]. رمزنگاری دانش تغییر دادن متن، پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است به طوری که تنها شخصی که از کلید و الگوریتم مطلع است، قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نتواند به اطلاعات دسترسی پیدا کند[۲]. استفاده از روش‌های رمزنگاری متن مانند AES[5], DES[4], RSA[3] به جهت تفاوت‌های بین عکس و متن و حجم زیاد داده‌ها در آن‌ها به طور مستقیم برای رمزنگاری تصاویر کاربردی نیست و باید تغییراتی را در ساختار آن‌ها به وجود آورد[۱].

در این مقاله، در ابتدا به بررسی کارهای انجام شده در زمینه الگوریتم رمزنگاری هیل، الگوریتم در هم سازی کیوب و سایر الگوریتم‌های رمز نگاری مشابه پرداخته می‌شود. در بخش بعدی الگوریتم‌های به‌کاررفته در این مقاله به صورت خلاصه توضیح داده می‌شود.

در ادامه روش ارائه‌شده بیان گردیده است. سپس به بررسی کارآیی الگوریتم پیشنهادی و مقایسه با الگوریتم هیل استاندارد در رمزنگاری تصاویر پرداخته می‌شود، در نهایت با استفاده از الگوریتم پیشنهادی بهبود در رمز نگاری با پیکسل‌های مشابه در مقایسه با الگوریتم هیل استاندارد و افزایش وابستگی بین پیکسل ها در مرحله درهم سازی نسبت به الگوریتم کیوب استاندارد نشان داده می‌شود.

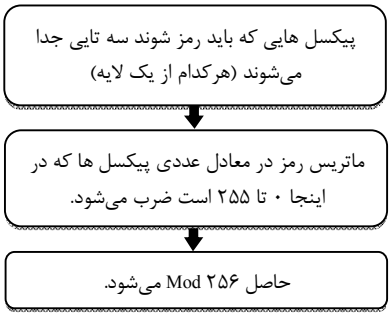
### الگوریتم‌های استفاده شده

در روش ارایه شده برای رمز نگاری تصویر از الگوریتم هیل توسعه یافته و الگوریتم کیوب استفاده شده است که در ادامه به شرح مختصری از هر یک از این دو الگوریتم پرداخته می‌شود.

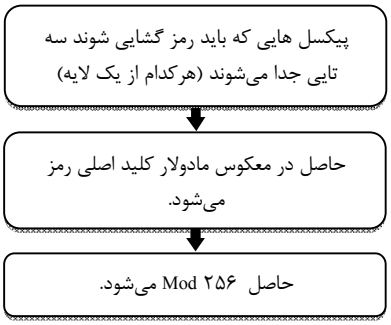
### الگوریتم هیل

رمزنگاری هیل در سال ۱۹۲۹ توسط لستر هیل برای رمزنگاری متن به وجود آمد[۹] هسته رمزنگاری استفاده از یک ماتریس (به عنوان کلید)، برای ضرب در معادل عددی متن برای تبدیل به رمز و استفاده از معکوس ماتریس (به عنوان کلید معکوس شده)، برای رمزگشایی معادل عددی متن مورد نظر است. در شکل زیر با فرض ۳*۳ بودن ماتریس رمز، عملیات ریاضی رمزنگاری و رمزگشایی در

الگوریتم هیل استفاده‌شده نشان داده می‌شود (از ماتریس ۳*۳ در روش ارائه‌شده استفاده می‌شود).




شکل ۱. الگوریتم عملیات رمز نگاری




شکل ۲. الگوریتم عملیات رمز گشایی

### الگوریتم کیوب

کیوب در سال ۱۹۷۲ توسط روبیک به ثبت رسید و بعدها نیز به کیوب جادویی روبیک معروف شد که در اصل یک بازی فکری است که در حالت ساده دارای ۶ سطح و ۵۴ قسمت است. الگوریتم روبیک به دلیل پیچیدگی محاسباتی، طرز کار خاص و همچنین فضای کلید متفاوت آن با سایر الگوریتم‌ها همواره در زمینه‌های مختلف از جمله روش‌های مختلف درهم سازی مورد توجه است[۸]. در این مقاله نیز برای رمزنگاری تصویر از ترکیب پیاده‌سازی خاصی از الگوریتم کیوب با الگوریتم هیل برای بهبود در رمزنگاری استفاده شده است.

## بررسی کارهای انجام‌شده

الگوریتم رمزنگاری هیل استاندارد به جهت استفاده از ماتریس یکسان رمز برای همه بلوک‌های داده، در تصاویر با پیکسل‌های مشابه و مجاور رمزنگاری به درستی عمل نمی‌کند و در آزمون‌های امنیتی نیز در مقابل حملات با داده اولیه مشخص[1] (نفوذ گر علاوه بر دانستن الگوریتم رمزنگاری از داده ورودی نیز اطلاع دارد و سعی در یافتن کلید رمزنگاری دارد) مقاومت خوبی از خود نشان نمی‌دهد[۶]. برای رفع معایب این الگوریتم، سعی در ترکیب این الگوریتم با روش های درهم‌سازی مختلف و تغییر کلید رمز نگاری در ماتریس‌های مختلف انتخاب پیکسل‌ها شده است. در مقاله[۶] برای اصلاح این الگوریتم از کلیدهای متفاوت برای رمزنگاری هر بلوک داده استفاده شده است. برای این منظور در ابتدا یک ماتریس یک بعدی با مقدار یکتا برای ضرب در ماتریس اولیه رمزنگاری ساخته شده و در هر مرحله با ضرب در ماتریس کلید ماتریس دیگری ساخته می‌شود که باعث تغییر در نتیجه رمزنگاری بلوک‌های داده یکسان شده و رمزنگاری هیل استاندارد را بهبود می‌بخشد.

به طور کلی استفاده از الگوریتم در هم ریزی کیوب در مقالات مختلف در حالت ترکیبی با روش‌های دیگر ارائه‌شده است که این ترکیب‌ها شامل ترکیب آن با الگوریتم‌ها آشوبی، الگوریتم‌های کلاسیک (XOR) و دیگر الگوریتم‌های تغییر بیت‌ها است، که این ترکیب به علت خاصیت درهم سازی با پیچیدگی بالای الگوریتم کیوب است. در ادامه به بررسی برخی از این روش‌ها می‌پردازیم.

در یک تحقیق برای رمزنگاری، تصویر را یک بار حول محور عمودی و یک بار حول محور افقی توسط رابطه گسسته فوریه انتقال داده و به این وسیله در دو بعد انتقال فوریه انجام‌شده است [۲] و در مرحله بعدی، تصویر به ۶ قسمت مساوی تقسیم و هر قسمت در یک سطح کیوب قرار می‌گیرد و در نهایت کیوب طبق الگوریتم آشوبی لجستیک درهم‌ریخته و تصاویر رمز شده نهایی را از ترکیب این دو مرحله به دست آمده است. در مقاله [۷] برای رمزنگاری و امنیت داده‌ها در تشخیص داده‌های بیومتریک تصاویر چشم از الگوریتم کیوب استفاده شده است. در مرحله اول، تصویر اصلی به بلوک‌هایی تقسیم و روی هر کدام از این بلوک‌ها با استفاده از الگوریتم کیوب و شیفت پیکسل‌ها تصویری در هم به وجود آمده است. در مرحله بعدی با حاصل الگوریتمی که از ترکیب مجموع سطرها برای هر پیکسل به دست آمده، XOR به صورت بیتی شده است. در مقاله[۸] از ترکیب روش در هم سازی کیوب و الگوریتم آشوبی لجستیک برای رمزنگاری تصویر استفاده شده است. در این مقاله تصویر به بلوک‌هایی تقسیم شده که هر بلوک با استفاده از الگوریتم کیوب درهم شده است. در این الگوریتم تعداد چرخش کیوب در هر مرحله از اعدادی تصادفی به دست آمده از تابع آشوبی لجستیک محاسبه می‌شود، در نتیجه تصویر در هم شده تنها با دانستن الگوریتم کیوب و تابع لجستیک با فاکتورهای مقداردهی اولیه آن قابل بازیابی خواهد بود.

## الگوریتم پیشنهادی

در مقاله ارایه شده، از ترکیب الگوریتم‌های تقسیم نمودن تصویر اصلی، ساخت اعداد تصادفی، کیوب پیشنهادی و هیل پیشنهادی

1. Known plaintext

استفاده شده است. در ادامه الگوریتم‌های ارائه شده به تفکیک بیان شده است.

## تقسیم کردن تصویر اصلی

در الگوریتم ارائه‌شده، در مرحله تقسیم تصویر اصلی مراحل زیر به ترتیب انجام می‌شود.

۱- در ابتدا تصویر اصلی به دو قسمت مساوی تقسیم شده، که یک نیمه آن توسط الگوریتم هیل رمزنگاری می‌شود و نیمه دیگر تصویر رمزنگاری روی آن انجام نمی‌شود.

۲- در گام بعد، پیکسل‌های دو نیمه تصویر باهم ترکیب می‌شوند. عملیات تقسیم، رمزنگاری و ترکیب شرح داده شده، به دلیل در هم سازی پیکسل‌هایی که توسط الگوریتم هیل رمز نگاری شده اند با پیکسل های تصویر اولیه مشکل رمز نگاری در تصویر هایی که پیکسل های مجاور مشابه دارند را بهبود می‌بخشد.

## الگوریتم تولید اعداد تصادفی

برای چرخش کیوب حول سطرها و ستون های خود، از الگوریتم تولید اعداد تصادفی استفاده شده است. این الگوریتم مجموعه اعداد را در بازه و تعداد مورد نیاز تولید می کند. برای ساختن این الگوریتم از مراحل زیر استفاده شده است.

۱- در ابتدا پارامتر شروع الگوریتم مقداردهی اولیه می‌شود.

۲- در مرحله اول ایجاد ماتریس تصادفی، حلقه ای که تعداد اجرای آن به اندازه ۸ برابر تعداد مورد نیاز می باشد، آرایه‌ای متشکل از عدد های صفر یا یک را می‌سازد. برای ساخت این آرایه، از الگوریتم بیان شده در شکل (۳) استفاده می‌شود.

۳- در مرحله بعدی ایجاد ماتریس تصادفی، با علم به اینکه که عدد ۲۵۵ (عددی که در هر خانه از ماتریس قرار می‌گیرد) از ترکیب اعداد ( $a_0*2^0 + a_1*2^1 + a_2*2^2 + a_3*2^3 + a_4*2^4$ $a_5*2^5 + a_6*2^6 + a_7*2^7$) ساخته می‌شود. در هر مرحله، هشت بیت از ماتریسی که با مقدار ۰ و ۱ پر شده انتخاب می‌شود. با جایگذاری مقادیر ۸ بیت انتخاب شده با متغیر های $a_0$ الی $a_7$ در هر خانه از ماتریس تصادفی، عددی بین (۰ تا ۲۵۵) ساخته می شود..

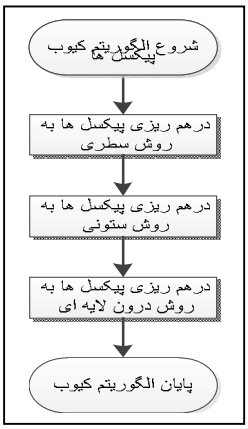
## الگوریتم کیوب سطری، ستونی و ترکیبی در سه لایه تصویر رنگی

در مرحله درهم ریزی پیکسل‌ها از الگوریتم سه مرحله‌ای استفاده شده است که به ترتیب باعث در هم ریزی در سطرها، ستون ها و بین لایه های تصویر(قرمز، سبز و آبی) می‌شود. در شکل (۴) مراحل الگوریتم ترکیبی کیوب نشان داده شده است.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $0^0$ | $0^1$ | $0^2$ | $0^3$ | $0^4$ | $0^5$ | $0^6$ | $0^7$ | =0 |
| $2^0$ | $2^1$ | $2^2$ | $2^3$ | $2^4$ | $2^5$ | $2^6$ | $2^7$ | =255 |

```
org = zeros(n*8,1,'uint8');
x1 =  0.399999;
x2 = 0;
for i= 2 : n
    x2 = 1 - 2* x1 * x1;
  if (x2 > 0.0)
    org(i-1) = 1;
  end
    x1 =  x2;
end
```

شکل ۳. الگوریتم تولید اعداد تصادفی




شکل ۴. الگوریتم کیوب

## الگوریتم کیوب افقی با حفظ وابستگی پیکسل ها

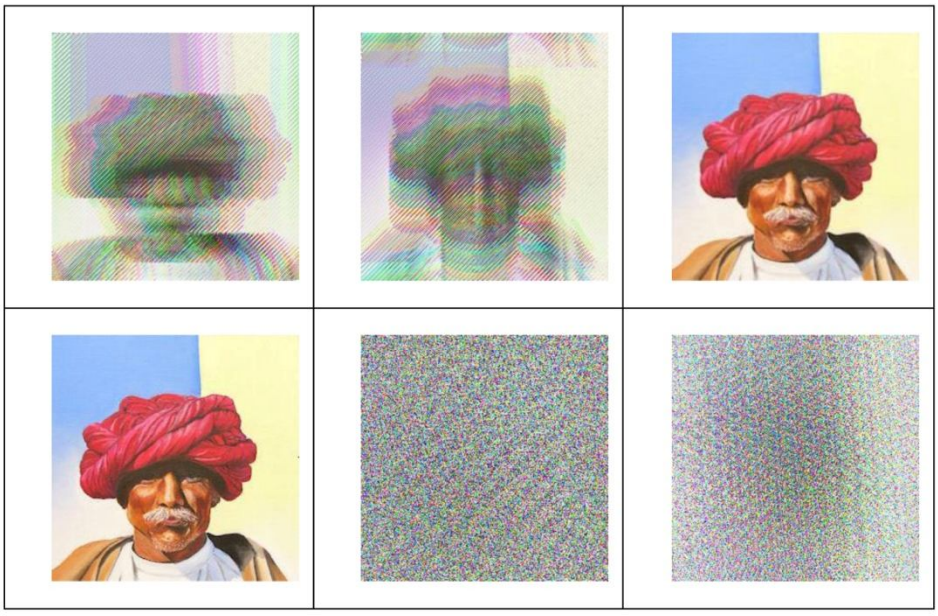
در این الگوریتم، برای در هم ریزی پیکسل ها سطوح کیوب در هر مرحله با پیکسل هایی که به صورت سطری انتخاب می‌شوند پر می شود. با توجه به اینکه هر کیوب ۳*۳*۳ دارای ۵۴ سطح می-باشد، در هر مرحله ۵۴ پیکسل به صورت افقی انتخاب می شود و بعد از درهم ریزی بوسیله کیوب پیکسل های تصویر در جای جدید قرار می‌گیرند برای وابستگی درهم ریزی در این کیوب، در پرکردن کیوب های متوالی از تعدادی از پیکسل های مرحله قبل استفاده می شود. این امر باعث می‌شود که انتشار و درهم سازی پیکسل ها این بار در جهت افقی صورت پذیرد. در شکل (۵) انتشار پیکسل ها در جهت افقی نشان داده شده است.

### الگوریتم کیوب عمودی با حفظ وابستگی پیکسل ها

در این الگوریتم، برای در هم ریزی پیکسل ها سطوح کیوب در هر مرحله با پیکسل هایی که به صورت ستونی انتخاب می‌شوند پر می‌شود. مانند حالت قبل، برای وابستگی درهم ریزی در این کیوب، پر شدن کیوب های متوالی با پیکسل های کاملا جدید انجام نخواهد گرفت. بلکه در هر مرحله، تعدادی از پیکسل های مرحله قبل نیز در کیوب مرحله بعد جایگذاری خواهد شد در شکل (۵) وابستگی پیکسل ها به صورت عمودی نشان داده شده است.

### الگوریتم کیوب بین لایه ای با حفظ وابستگی پیکسل ها

در الگوریتم درهم ریزی پیکسل ها به صورت بین لایه ای، برای پر کردن کیوب های هر مرحله از پیکسل های موجود در هر سه لایه تصویر استفاده می شود. که این امر باعث درهم ریزی بیشتر پیکسل ها در هر سه لایه تصویر است . برای حفظ وابستگی پیکسل ها در این مرحله نیز مانند کیوب های مراحل قبل، در پر کردن کیوب های متوالی از کیوب های مراحل پیشین نیز استفاده شده است. در شکل (۵) وابستگی پیکسل‌های بین لایه ای نشان داده شده است.



| | | |
|---|---|---|
| ۱ | ۲ | ۳ |
| ۴ | ۵ | ۶ |

شکل ۵. نمایش وابستگی‌های ستونی و سطری (تصویر اول تصویر قبل از رمز نگاری، تصویر دوم از تأثیر وابستگی ستونی، تصویر سوم تأثیر وابستگی سطری، تصویر چهارم تصویر رمزنگاری شده تنها با در همسازی پیکسل‌ها، تصویر پنجم تصویر رمزنگاری شده با الگوریتم ارائه‌شده و تصویر ششم تصویر رمز گشایی شده است).

### الگوریتم هیل توسعه‌یافته

در مرحله آخر رمزنگاری، عناصر درهم شده با استفاده از الگوریتم هیل رمزنگاری می‌شوند. در این مرحله نیز با توجه به بلوکی بودن رمزنگاری هیل، بلوک‌ها از پیکسل‌هایی از هر سه لایه تصویر (قرمز، سبز و آبی) انتخاب می‌شوند. این عمل با توجه به وابسته بودن هر سه لایه تصویر برای شکل‌گیری تصویر اصلی، باعث بهبود قابل‌توجهی در رمزنگاری تصویر در مقایسه با اعمال این الگوریتم تنها بر روی یک لایه می‌شود.

با توجه به بازه هر پیکسل ۸ بیتی Mod ۲۵۶ برای نگاشت مناسب به جای Mod ۲۶ به‌کاررفته در هیل متنی استفاده می‌شود. با توجه به وابسته بودن پیکسل های سه لایه تصویر (قرمز، سبز و آبی)، برای پر کردن ماتریس استفاده شده در هر مرحله؛ از ترکیب پیکسل‌های هر سه لایه به جای رمز نگاری هر لایه به صورت مجزا استفاده شده است. این ترکیب، با توجه به وابستگی پیکسل های لایه های مختلف به یکدیگر، به رمزنگاری بهتر تصویر کمک می-کند.

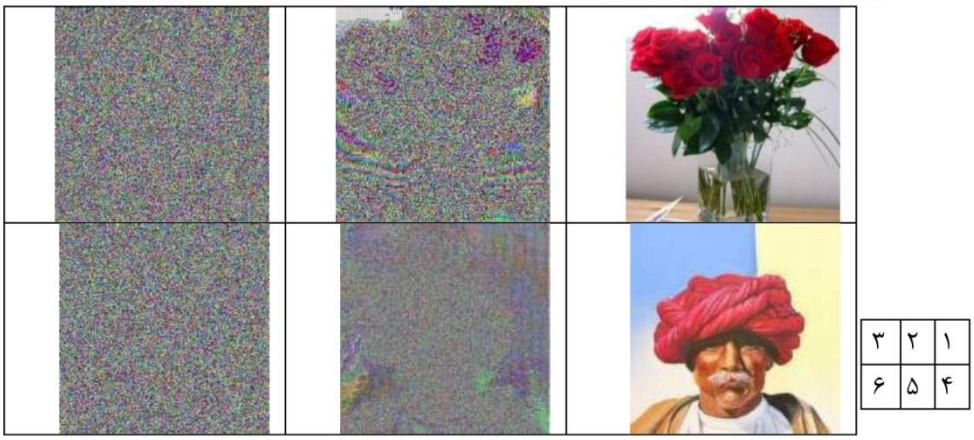
بازه ای که برای رمزنگاری در الگوریتم هیل استاندارد انتخاب شده، با توجه به اعداد نسبت داده شده به حروف انگلیسی (۰-۲۵) است. برای عملکرد مناسب الگوریتم ارایه شده و عملیات رمز نگاری و رمز گشایی مناسب، عملیات تقسیم باید در بازه پیکسل-

های تصویر (۰-۲۵۵) انجام شود. تغییر بازه الگوریتم هیل، باعث نگاشت مناسب پیکسل های تصویر می‌شود. در شکل (۶) نتیجه رمزنگاری قابل مشاهده است.

## رمزگشایی الگوریتم پیشنهادی

در رمزگشایی الگوریتم ارائه شده معکوس عملیات رمزنگاری عمل می شود. یعنی مراحل رمزگشایی از مرحله آخر رمز نگاری شروع شده و الگوریتم رمزگشایی برای هر مرحله انجام می شود.

در الگوریتم پیشنهادی در مرحله اول تصویر به دو نیمه تقسیم شده، یک نیمه توسط الگوریتم هیل رمزنگاری شد و در نهایت دو نیمه تصویر با یکدیگر ترکیب شدند. در مرحله بعدی از الگوریتم کیوب برای درهمسازی بیشتر تصویر با استفاده از دنباله تصادفی انجام گرفت. و در مرحله آخر نیز از الگوریتم رمزنگاری هیل بر روی کل تصویر استفاده شد. برای رمزگشایی کل تصویر در مرحله اول کل تصویر با استفاده از الگوریتم هیل با استفاده از کلید معکوس مرحله آخر رمزنگاری، رمزگشایی می شود. در مرحله بعد برای بازگرداندن مراحل انجام شده در مرحله رمزنگاری و در قسمت کیوب تمامی چرخش کیوب ها باید به صورت معکوس انجام شود یعنی به طور مثال اگر دنباله چرخش کیوب در مرحله رمزنگاری به صورت (۲-۱-۳-۰-۰-۰)، (۰-۰-۰-۱-۰-۱) و (۲-۰-۳-۱-۰-۱) باشد در مرحله رمزگشایی باید از دنباله (۲-۰-۱-۳-۰-۳)،( ۰-۰-۰-۳-۰-۳)و(۲-۳-۱-۰-۰-۰) استفاده شود. همانطور که مشاهده می‌شود برای معکوس کردن در هم ریزی پیکسل ها با استفاده از الگوریتم کیوب دنباله اعداد تصادفی استفاده شده برای رمزگشایی از آخر پیمایش شده و چون هر وجه کیوب ۳*۳*۳ استفاده شده با ۴ چرخش به جای خود بر می‌گردد، حاصل جمع عدد استفاده شده در رمزنگاری با عددی که باید در رمزگشایی استفاده شود باید ۴ شود. در مرحله آخر رمزگشایی نیز تصویری که تا این مرحله از رمزگشایی به دست آمده، به دو قسمت تقسیم شده و یک نیمه از آن با استفاده از الگوریتم هیل و با کلید معکوس مرحله اول رمزنگاری، رمزگشایی می‌شود شکل (۵) ، مراحل رمزنگاری و رمزگشایی به ترتیب نشان داده شده - است.




شکل ۶. تحلیل بصری (تصویر اول گل برای رمزنگاری، شکل دوم تصویر رمز شده با الگوریتم هیل استاندارد، شکل سوم تصویر رمز شده با الگوریتم هیل ارائه‌شده. شکل چهارم تصویر موجود شخص در متلب برای رمزنگاری، شکل پنجم تصویر رمز شده با استفاده از الگوریتم هیل استاندارد، شکل ششم تصویر رمز شده با الگوریتم هیل ارائه‌شده).

## تحلیل کار آیی الگوریتم ارائه‌شده

برای تحلیل الگوریتم ارایه الگوریتم ارایه شده در نرم افزار متلب پیاده سازی شده است و برای مقایسه کارایی الگوریتم ارایه شده معیار های بیان شده با سایر الگوریتم ها نیز مقایسه شده است.

### تحلیل بصری

در این قسمت برای مقایسه بهتر بین دو روش بیان‌شده در این تحقیق، از تصاویری استفاده‌شده که در آن‌ها پیکسل‌های مجاور شبیه به هم باشند. زیرا در این تصاویر الگوریتم هیل افت عملکرد بالایی دارد و قیاس بهتری را به وجود می‌آورد[۶]. با به کمک روش ترکیبی ارائه‌شده در این مقاله نشان داده می‌شود، در تصاویری که روش هیل به تنهایی برای رمزنگاری استفاده شده است تصویر رمز شده تاحد بسیار زیادی قابل‌تشخیص است. ولی همان طور که در شکل(۶) مشخص شده است بعد از استفاده از الگوریتم ترکیبی ارائه‌شده بهبود در رمزنگاری کاملاً قابل مشاهده و مقایسه است.

## تحلیل هیستوگرام

برای جلوگیری از نشت اطلاعات و جلوگیری از حمله مهاجمین، یکی از مهم‌ترین اصول رمزنگاری تصاویر، نداشتن شباهت آماری بین تصویر رمز شده و تصویر اصلی است[۱۰]. تحلیل هیستوگرام چگونگی توزیع پیکسل‌ها در تصویر را با استفاده از میزان تکرار هر پیکسل نشان می‌دهد. هر چه سطح نمودار دو تصویر تمایز بیشتری داشته باشد پراکندگی پیکسل‌ها بهتر صورت گرفته است. برای این آزمون از هیستوگرام پراکندگی پیکسل‌ها شکل(۷) استفاده می‌شود. مقایسه هیستوگرام تصویر رمز شده با تصویر اصلی تمایز دو تصویر را نشان می‌دهد. نکته قابل توجه در این الگوریتم درهم سازی مناسب در این الگوریتم است که باعث شده هر سه لایه تصویر دارای هیستوگرام تقریباً یکسانی باشند. در الگوریتم ارایه شده با توجه به درهمسازی استفاده شده در الگوریتم کیوب بیان شده پیکسل ها در هر سه لایه تصویر با یکدیگر ترکیب شده اند و با توجه به این مطلب هیستوگرام هر سه لایه تصویر دارای یک شکل بوده و نشانگر درهم سازی مناسب پیکسل ها در کل تصویر می باشد.

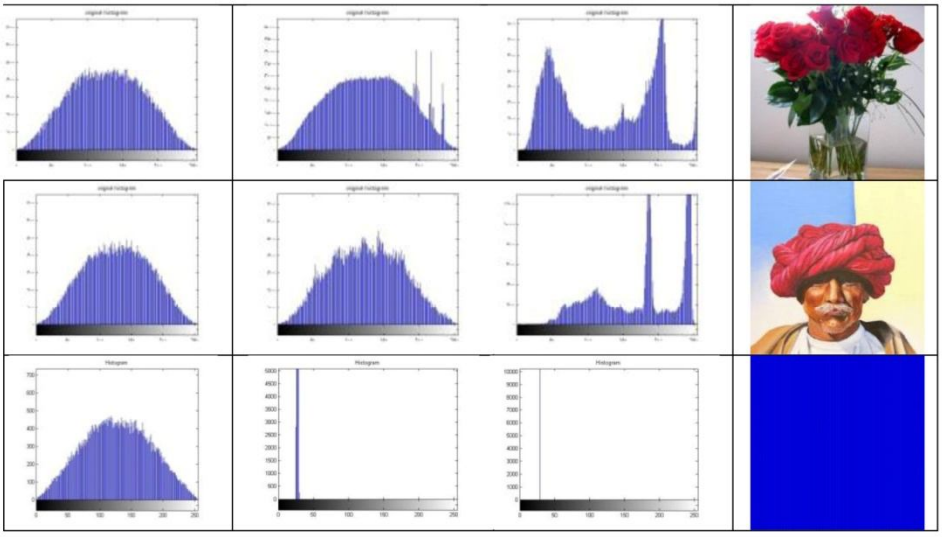
## تحلیل کیفی

یکی از مهمترین عوامل سنجش رمزنگاری، کیفیت رمزنگاری است. در این روش معیار کارآیی رمز نگاری تصاویر بر پایه مطالعات بصری تکنیک های رمزنگاری می باشد. یک سیستم رمزنگاری مطلوب، قادر به پنهان سازی ویژگی های کلی تصویر است. برای سنجش بصری الگوریتم های رمزنگاری از PSNR و SSIM که در ادامه آمده، استفاده می‌شود.

## نرخ سیگنال به نرخ خطا

امروزه از PSNR، هنوز به صورت گسترده ای استفاده می‌شود[۱۷] که دلیل این امر را می توان سرعت و راحتی محاسبه این پارامتر دانست. این پارامتر در واقع نشان دهنده حداکثر توان سیگنال به توان مخرب آن می‌باشد. معمولا از PSNR برای اندازه گیری کیفیت بازسازی تصاویر پس از رمز گشایی یا فشرده سازی استفاده می شود. هر چه میزان این نرخ، بیشتر باشد کیفیت تصویر رمز گشایی شده بیشتر است. یکی دیگر از کاربردهای PSNR در تحلیل امنیت رمزنگاری است.

در این مقایسه هرچه نرخ PSNR کمتر باشد، تفاوت بیشتر بین تصویر رمز شده و تصویر اصلی بیشتراست. این پارامتر، می‌تواند معیاری برای مقایسه تفاوت بین دو تصویر باشد. برای به دست اوردن PSNR در ابتدا باید میانگین نرخ خطای مربعی را به دست آورد. میانگین خطای مربعی، یک روش آماری برای به دست آوردن میانگین تفاوت کمی بین دو تصویر با استفاده از میانگین آماری است. در رابطه(۱)، میانگین خطای مربعی نشان داده شده است که در این رابطه، I تصویری با ابعاد m*n و k نیز تصویر رمزگشایی شده است.



| | | | |
|---|---|---|---|
| ۱ | ۲ | ۳ | ۴ |
| ۵ | ۶ | ۷ | ۸ |
| ۹ | ۱۰ | ۱۱ | ۱۲ |

شکل ۷. تحلیل هیستوگرام (شکل اول تصویر گل، شکل دوم هیستوگرام تصویر گل، شکل سوم هیستوگرام تصویر رمزنگاری شده با الگوریتم هیل استاندارد، شکل چهارم هیستوگرام تصویر رمزنگاری شده با الگوریتم هیل ارائه‌شده (سه لایه تصویر در حالت رمزنگاری هیستوگرام یکسانی را دارند)، شکل پنجم تصویر مرد هندی، شکل ششم هیستوگرام تصویر مرد هندی، شکل هفتم هیستوگرام تصویر رمزنگاری شده با الگوریتم هیل استاندارد، شکل هشتم هیستوگرام تصویر رمزنگاری شده با الگوریتم هیل ارائه‌شده (سه لایه تصویر در حالت رمزنگاری هیستوگرام یکسانی را دارند)، شکل نهم تصویر با مساحت بزرگی از یک رنگ، شکل دهم هیستوگرام تصویر آبی، شکل یازدهم هیستوگرام تصویر تصویر رمزنگاری شده با الگوریتم هیل استاندارد، شکل دوازدهم هیستوگرام تصویر رمزنگاری شده با الگوریتم هیل ارائه‌شده (سه لایه تصویر در حالت رمزنگاری هیستوگرام یکسانی را دارند)).

بعد از محاسبه میانگین خطای مربعی، برای محاسبه PSNR از رابطه (۲) استفاده می‌کنیم که در آن MAX بیشترین مقدار ممکن برای یک پیکسل از تصویر می‌باشد که با فرض ۸ بیتی بودن، این مقدار در هر پیکسل این مقدار ۲۵۵ است. اگر دو تصویر باهم تفاوتی نداشته باشند، مقدار به دست آمده برای MSE برابر صفر خواهد بود در نتیجه مقدار PSNR نیز بی نهایت خواهد شد[۱۷].

$$MSE = \frac{1}{m\,n}\sum_{i=}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \quad (۱)$$

$$PSNR = 1\log_{10}(\frac{I_{Max}^2}{MSE}) \quad (۲)$$

## شباهت ساختاری

شباهت ساختاری، مقیاس اندازه گیری شباهت بین دو تصویر می باشد که توسط وانگ معرفی شد[۱۱]. این پارامتر سه مقدار مختلف از تصویر را در نظر گرفته و در نهایت برای به دست آوردن مقیاس واحد با یکدیگر ترکیب می کند. اولین مقیاس تاثیرات بصری می‌باشد که بوسیله محاسبه شدت روشنایی به صورت محلی قابل مقایسه است، کنتراست و ساختار نیز دو مقدار بعدی هستند. در نهایت شباهت ساختاری طبق رابطه (۵) محاسبه می‌گردد. در این رابطه μx میانگین مقدار x، μ y میانگین مقدار y، $\sigma_x^2$ واریانس متغیر x، $\sigma_y^2$ واریانس متغیر y، $\sigma_{xy}$ کواریانس بین این دو متغیر، C1 و C2 دو متغیر برای ثابت کردن مقدارکه در برخی از موارد برابر صفر می‌باشند، L که از ضریب تغییرات پیکسل به دست میآید و معمولا مقدار آن $(2^{bit\ per\ pixel}-1)$ می‌باشد. ضریب ثابت $K_1$=0.001 و $K_2$=0.003 است.

$$c1 = k1L \quad (۳)$$

$$c2 = k2L \quad (۴)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \quad (۵)$$

## ضریب همبستگی پیرسن

ضریب همبستگی پیرسن، معیاری برای اندازه گیری همبستگی بین دو نقطه x و y است. مقدار این معیار بین ۱+ و ۱- یک متغیر می باشد. اگر مقدار این متغیر برابر ۰ باشد هیچ همبستگی بین دو تصویر وجود ندارد. اگر این مقدار برابر ۱ باشد دو تصویر دارای ضریب همبستگی مثبت کامل بوده و در صورتی که این مقدار برابر ۱- باشد دو تصویر دارای ضریب همبستگی کامل منفی می باشند. این فاکتور نخستین بار توسط کارل پیرسن ارایه شد[۲۰].

## امنیت کلید رمز نگاری

یکی از اصول رمزنگاری امنیت کلید اصلی در مقابل انواع حمله ها است. به طور کلی می توان گفت که امنیت رمز نگاری به طراحی کلید اصلی وابسته است. از مهم ترین ویژگی‌ها برای امنیت کلید اصلی مورد نظر، حساس بودن کلید اصلی به تغییرات جزیی است[۱۲].

جدول ۱. مقایسه فاکتورهای کیفی تصاویر رمزنگاری و رمزگشایی شده.

| ر | تصویر | PSNR | SSIM | P_C_C |
|---|---|---|---|---|
| ۱ | تصویر رمزنگاری شده با تصویر اصلی (تصویر گل) | ۸,۷۱۷۱ | ۰,۰۱۷۶۳۵ | ۰,۰۵۰۲۷۲ |
| ۲ | تصویر رمزگشایی شده با تصویر اصلی (تصویر گل) | ۴۶,۸۰۸۷ | ۰,۹۹۹۴۳ | ۰,۹۹۹۹۲ |
| ۳ | تصویر رمزنگاری شده با تصویر اصلی (تصویر مرد) | ۹,۱۳۷ | ۰,۰۲۰۳۹۶ | ۰,۰۱۶۰۹۷ |
| ۴ | تصویر رمزگشایی شده با تصویر اصلی (تصویر مرد) | ۴۴,۶۰۰۴ | ۰,۹۹۴۱۵ | ۰,۹۹۹۶۱ |
| ۵ | تصویر رمزنگاری شده (شکل لاستیک موجود در متلب) | ۶,۹۶۵۷ | ۰,۰۱۰۹۸ | ۰,۰۱۱۷۴۸ |
| ۶ | تصویر رمزگشایی شده (شکل لاستیک موجود در متلب) | ۳۹,۳۳۷۶ | ۰,۹۷۸۱۲ | ۰,۹۹۸۹۳ |

## تحلیل حساسیت کلید اصلی

در عملیات رمزنگاری حساسیت به کلید اصلی باید به نحوی باشد که با تغییر یک بیت در کلید رمزنگاری تصویر متفاوتی با تصویر اصلی تولید شود در شکل (۸)، تصویر گل رز با دو کلیدی که تنها در یک بیت با هم اختلاف دارند رمزنگاری شده است. همان طور

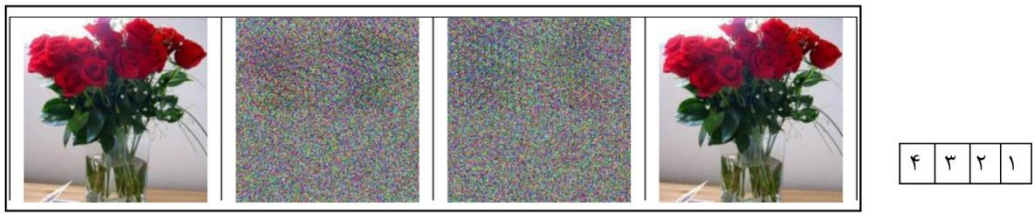
که مشاهده می‌شود تغییر یک بیت باعث شده است که تصویر در هنگام رمزگشایی به درستی به تصویر اولیه تبدیل نشود.

## تفاوت بین تصاویر رمز شده

برای تحلیل حساسیت بین تصاویر رمز شده، تصویر مجددا با استفاده از کلیدی که تنها در یک بیت با هم اختلاف دارند رمزنگاری شده است. در جدول ۲، نتایج مقایسه بین دو تصویر با استفاده از معیارهای (NPCR ، UACI) [۱۳]. و مقایسه آن با کارهای انجام شده آمده است.همانطوریکه مشاهده می شود هر چه مقدار NPCR به عدد یک نزدیک تر باشد الگوریتم ارایه شده از حساسیت بالاتر نسبت تغییر کلید اصلی برخوردار می باشد و هرچه مقدار معیار UACI بیشتر باشد مقدار حساسیت به کلید اصلی بیشتر می باشد.برای مقایسه نتایج الگوریتم ارایه شده با سایر الگوریتم ها از چند مقاله که از این پارامتر برای تحلیل نتایج امنیت خود استفاده کرده اند استفاده شده است. که نتایج این مقایسه در جدول ۲ قابل مشاهده می باشد.

جدول ۲. مقایسه بین الگوریتم ها(فاکتورهای **NPCR** و **UACI** در تحلیل کلید اصلی برای تصویر لنا).

| ر | الگوریتم | NPCR (میانگین) | UACI (میانگین) |
|---|---|---|---|
| ۱ | الگوریتم ارایه شده | ۰,۹۹۶۰۹۴ | ۰,۳۳۴۶۳۵ |
| ۲ | مرجع [۱۵] | ۰,۹۹۶۰۲۴ | ---- |
| ۳ | مرجع [۱۶] | ۰,۹۹۶۰۹۸ | ۰,۳۳۴۶۲۹ |
| ۴ | مرجع [۱۴] | ۰,۹۹۶۶۸۹ | ۰,۳۳۵۵۶۱ |
| ۵ | مرجع [۱۷] | ۰,۹۹۵۷۶۵ | ۰,۳۳۳۲۴۵ |




شکل ۸. تحلیل حساسیت کلید اصلی (تصویر اول عکس اولیه برای رمزنگاری، تصویر دوم رمزنگاری با کلیدی با یک بیت اشتباه، تصویر سوم با دو بیت اشتباه و

## آزمون همبستگی

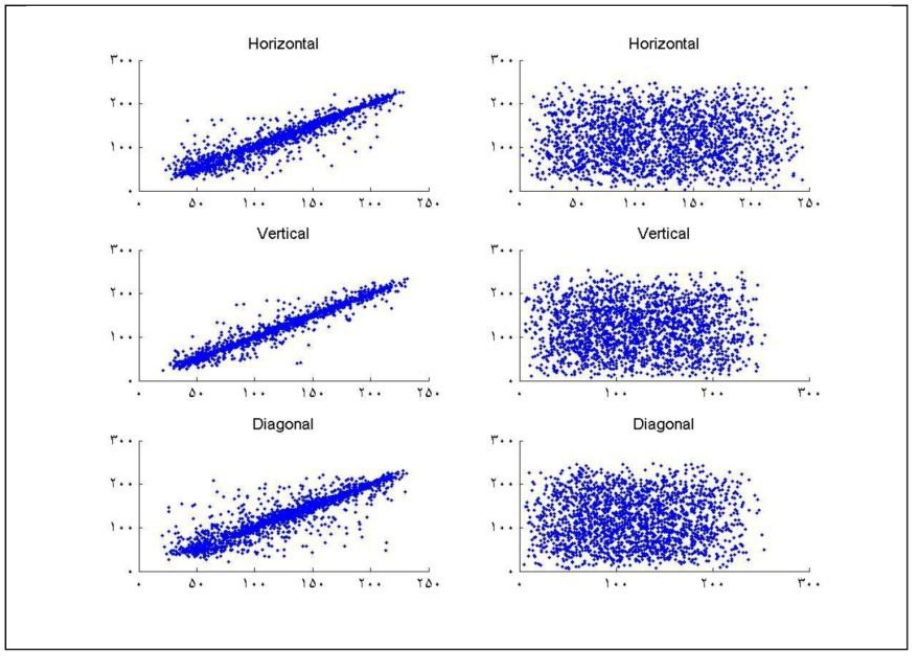
همبستگی بین پیکسل‌های مجاور در تصویر اصلی همواره بالا است به طوریکه هر پیکسل به پیکسل های مجاورش وابسته می باشد یک الگوریتم رمز نگاری مناسب باید ضریب همبستگی را کم کند (نزدیک به صفر)[۱۴]. برای آزمون همبستگی ۲۵۰۰ پیکسل از تصویر به صورت تصادفی انتخاب شده است که برای مقایسه، همبستگی بین تصویر اصلی و تصویر رمز شده، تصویر اصلی و تصویر رمزگشایی شده در شکل (۹) قابل مشاهده است. در جدول ۳، مقایسه ای در این زمینه بین الگوریتم های مختلف انجام شده است. همانطوریکه که در جدول(۳) قابل مشاهده است ضریب همبستگی بیان شده در سطح قابل قبولی قرار دارد.

در سیستم های رمزنگاری رشته ای، کلید رمزنگاری به اندازه ابعاد کل تصویر رمزنگاری شده باید تولید شود که همین امر در خیلی از موارد تولید، نگهداری و انتقال کلید اصلی را با مشکل مواجه می سازد؛ به طور کلی در این الگوریتم ها رمزنگاری به صورت مطلوب تری انجام میگیرد که دلیل این امر طول کلید رمزنگاری به اندازه تصویر رمزشده می‌باشد. در الگوریتم های بلاکی، کلید رمزنگاری به سادگی ساخته شده و فاکتور زمانی رمزنگاری و سادگی در

انتقال کلید از ویژگی های معرض ان می باشد. در الگوریتم بیان شده نیز کلید اصلی از نوع بلاکی می باشد و با توجه با ساختار الگوریتم ارایه شده عملیات انتقال کلید نیز به سادگی انجام می-پذیرد و با توجه به جدول(۳) معیار همبستگی پیکسل های تصویر نیز در حد مطلوب و قابل قبولی نسبت به الگوریتم های ارایه شده مانند الگوریتم [۱۴] قرار دارد.

جدول ۳. ضریب همبستگی (مقایسه فاکتور ضریب همبستگی برای تصویر لنا).

| ر | الگوریتم | افقی | عمودی | قطری |
|---|---|---|---|---|
| ۱ | الگوریتم ارایه شده | -۰,۰۰۲۵۶۴۶ | -۰,۰۰۳۶۳۶۷ | ۰,۰۱۸۶۸۵ |
| ۲ | مرجع [۱۷] | ۰,۰۰۷۶۳۵۲ | ۰,۰۰۸۳۷۳۴ | ۰,۰۰۷۳۶۴۴ |
| ۳ | مرجع [۱۸] | ۰,۰۰۲۴ | ۰,۰۰۱۲ | ۰,۰۰۱۶ |
| ۴ | مرجع [۱۹] | ۰,۰۰۱۰۰۵ | -۰,۰۰۰۸۵ | ۰,۰۰۰۸۹۷ |
| ۵ | مرجع [۱۴] | ۰,۰۰۰۸۲۱۳ | ۰,۰۰۰۸۴۲۳ | ۰,۰۰۰۵۰۸۳ |




| | |
|---|---|
| ۱ | ۴ |
| ۲ | ۵ |
| ۳ | ۶ |

شکل ۷. نمایش همبستگی (شکل اول، دوم ، سوم همبستگی تصویر ۴ قسمت چهارم با خود تصویر و شکل چهارم، پنجم ، ششم همبستگی تصویر اصلی با تصویر رمزگشایی شده).

## زمان اجرای الگوریتم ارایه شده

با توجه به ساختار الگوریتم ارایه شده، سه مرحله کلی وجود دارد که به صورت ترتیبی باید اجرا شوند. در مرحله کیوب که بیشترین زمان اجرا به آن اختصاص دارد از دو ساختار برای کم کردن زمان اجرا استفاده شده است. ساختار اول پیاده سازی چرخش کیوب ها با استفاده از شیفت دورانی ساده می‌باشد که تا حدود زیادی زمان اجرای کیوب را بهبود می بخشد ساختار دوم قابلیت استفاده از شرایط موازی سازی می باشد. با توجه به ترکیب کیوب در چند مرحله(چند کیوب سطری، چند کیوب ستونی و چند کیوب بین لایه ای) ساختار الگوریتم کیوب طوری پیاده سازی شده است که چند کیوب یک نوع به راحتی قابل موازی شده بوده و در بستر هایی مانند **Cuda** قابل پیاده سازی می باشند.

## نتیجه‌گیری

در این مقاله، یک راه حل ساده و کارا برای رمزنگاری تصویر با استفاده از الگوریتم رمزنگاری هیل ارائه شد. در روش ارایه شده ترکیبی از الگوریتم هیل و کیوب همراه با مراحل درهمسازی ارایه شد. برای ارزیابی روش ارائه‌شده از تحلیل بصری، تحلیل کیفی، تحلیل هیستوگرام، تحلیل حساسیت کلید و تحلیل همبستگی استفاده شد که در تحلیل بصری بهبود الگوریتم نسبت به روش رمزنگاری هیل استاندارد و کارآیی الگوریتم پیشنهادی نشان داده شد. در تحلیل هیستوگرام شباهت آماری بین تصویر رمزنگاری شده، تصویر اصلی و تصویر رمزگشایی شده بررسی شد. در این تحلیل نشان داده شد که به دلیل درهم سازی مناسب پیکسل ها هیستوگرام هر سه لایه تصویر شبیه به هم بوده و پیکسل ها بین هر سه لایه تصویر به صورت مساوی تقسیم شده اند. در تحلیل کیفی کیفیت تصویر رمزنگاری شده و تصویر رمزگشایی شده با تصویر اصلی بررسی شد. در تحلیل کلید رمزگشایی، کلیدی با یک بیت اختلاف با کلید اصلی استفاده و امنیت رمزنگاری مورد بررسی قرار گرفت. در تحلیل همبستگی نیز همبستگی بین پیکسل‌ها در تصویر رمزنگاری شده با تصویر اصلی بررسی شد که در تمامی آزمون ها الگوریتم پیشنهادی عملکرد موفقی داشت.

## مرجع‌ها


[1] Xiao Feng, Xiaolin Tian, Shaowei Xia, “A Novel Image Encryption Algorithm Based On Fractional Fourier Transform and Magic Cube”, 4th International Congress on Image and Signal Processing, 2011, Volume 2, pp.1008-1011.

[2] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, 1978, pp.120-126.

[3] Eli Biham, Adi Shamir, “Differential cryptanalysis of DES-like cryptosystems”, Springer, 1991, Volume 4, Issue 1, pp.3-72.

[4] Joan Daemen, Vincent Rijmen, “The Design of Rijndael: AES – The Advanced Encryption Standard”, Springer, February 2002, 14th, p.238.

[5] ISMAIL I.A, AMIN Mohammed, DIAB Hossam, “How to repair the Hill cipher”, Journal of Zhejiang University SCIENCE A, 2006, Volume 7(12), pp. 2022-2030.

[6] Khaled Loukhaoukha, Makram Nabti and Khalil Zebbiche, “An efficient image encryption algorithm based on blocks permutation and Rubik’s cube principle for IRIS images”, 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA),2013 , At Algiers, pp.267-272.

[7] Li ZHANG, Xiaolin TIAN, ShaoweiXIA, “A Scrambling Algorithm of Image Encryption Based on Rubik’s Cube Rotation and Logistic Sequence”, IEEE Computer Society, 2011, Volume 1, pp. 312-315, .

[8] Lester S. Hill, “Cryptography in an Algebraic Alphabet”, The American Mathematical Monthly, 1929, Volume 36, no 6, pp.306-312.

[9] Ahmed A. Abd El-Latif, Li Li, Ning Wang, Qi Han, Xiamu Niu, “A new app roach to chaotic image encryption based on quantum chaotic system, exploiting color spaces Signal Processing”, 2013, Volume 93, pp.387-397.

[10] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity", IEEE Transactions on Image Processing, 2004, Volume 13, no. 4, pp. 600-612,.

[11] Yicong Zhou, Long Bao, C.L. Philip Chen, “Image encryption using a new parametric switching chaotic system", Signal Processing, 2013, Volume 93, p.3039-3052.

[12] Yue Wu, Joseph P. Noonan, “NPCR and UACI Randomness Tests for Image Encryption”, Journal of Selected Areas in Telecommunications (JSAT), April Edition.

[13] Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, Mohammad Reza Mosavi, “A novel image encryption based hash function with only two-round diffusion process”, 2013, springer.

[14] Kwok, H.S., Tang, W.K.S.: “A fast image encryption system based on chaotic maps with finite precision representation”, 2007, Chaos Solitons Fractals ELSEVIER, Volume 32, pp.1518-1529.

[15] S. M. Seyedzadeh, S. Mirzakuchaki, “A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing ELSEVIER, Volume 92, Issue 5, p. 1202-1215.

[16] Yang Liu, Xiaojun Tong, Shicheng Hu, ”A family of new complex number chaotic maps based image encryption algorithm”, Signal Processing: Image Communication, 2013, Volume 28, pp.1548-1559.

[17] Qiang Zhang, Xiaopeng Wei, “A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system”, Optic, 2013, Volume 124, pp.6276-6281.

[18] Zhu, C., “A novel image encryption scheme based on improved hyperchaotic sequences”. J. Opt. Commun 285, 2012, Volume 28(10), pp.29-37.

[19] Karl Pearson, “Notes on regression and inheritance in the case of two parents”, Proceedings of the Royal Society of London, June 20, 1895 240–242.