Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 11, Number 3, Autumn, pp. 18-30
Received:01/24/2022, Revised: 08/14/2022, Accepted: 11/07/2022

Meaningful Visual Secret Sharing by Genetic Algorithm

Zeinab Mehrnahad[1], AliMohammad Latif [2*], Jamal Zarepour-Ahmadabadi [3]
[1]PhD Candidate, Computer Engineering Department, Yazd University, Yazd, Iran
[2*] Associated professor, Computer Engineering Department, Yazd University, Yazd, Iran
[3] Assistant professor, Department of Computer Science, Yazd University, Yazd, Iran
[1]z-mehrnahad@stu.yazd.ac.ir , [2*]alatif@yazd.ac.ir ,[3] zarepourjamal@yazd.ac.ir

Corresponding author's address: AliMohammad Latif, Computer Engineering Department, Yazd University, Yazd, Iran.

Abstract In visual secret sharing, the secret image is transformed into several share images and distributed among different people. The share images do not contain any information about the original image, and these images are similar to the noisy image. The original image can be retrieved in the presence of all stakeholders and by stacking the share images. In this regard, the appearance of noisy images may attract the attention of the attackers. To solve this problem, meaningful visual secret sharing was presented. In this article, a method for sharing the image with meaningful shares is introduced. There are a number of hyperparameters in the proposed algorithm. To improve performance, an attempt has been made to determine these hyperparameters using a genetic algorithm. The cost function of the genetic algorithm is the difference between the correct number of bits of the recovered image and the original image and the correct number of integer bits between the cover image and the shares. The proposed method was evaluated using PSNR, MSE, BCR and SSIM criteria and presented good results on different images with different numbers of shares.

Keywords- secret sharing, visual secret sharing, meaningful secret sharing, genetic algorithm.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۱، شماره ۳، پاییز ۱۴۰۱ ، صفحه ۱۸-۳۰
دریافت: ۱۴۰۰/۱۱/۰۴، بازنگری: ۱۴۰۱/۰۵/۲۳، پذیرش: ۱۴۰۱/۰۸/۱۶

تسهیم راز بصری معنادار با استفاده از الگوریتم ژنتیک

زینب مهرنهاد[۱]، علی‌محمد لطیف*[۲]، جمال زارع‌پور احمدآبادی
۱- دانشجوی دکتری دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.
*۲- دانشیار دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.
۳- استادیار دانشکده علوم کامپیوتر، دانشگاه یزد، یزد، ایران.
[1]z-mehrnahad@stu.yazd.ac.ir , [2*]alatif@yazd.ac.ir, [3]zarepourjamal@yazd.ac.ir

* نشانی نویسنده مسئول: علی‌محمد لطیف، یزد، دانشگاه یزد، دانشکده مهندسی کامپیوتر.

چکیده- در تسهیم راز بصری، تصویر راز به چندین تصویر سهم تبدیل می‌شود و بین افراد مختلف توزیع می‌گردد. تصاویر سهم هیچ‌گونه اطلاعاتی از تصویر اصلی را در بر ندارند و این تصاویر مشابه تصویر نویزگونه هستند. در هنگام نیاز با حضور همه افراد سهام‌دار و با قرار دادن تصاویر سهم بر روی هم تصویر اصلی بازیابی می‌شود. در این راستا ظاهر تصاویر نویزگونه ممکن است مورد توجه و سوء استفاده قرار بگیرد. برای حل این مشکل تسهیم راز معنادار ارائه شد. در این مقاله روشی برای تسهیم راز با سهام معنادار معرفی شده است. در الگوریتم ارائه شده تعدادی هایپرپارامتر وجود دارد. برای بهبود عملکرد سعی شده است با استفاده از الگوریتم ژنتیک این هایپرپارامترها تنظیم شوند. تابع هزینه الگوریتم ژنتیک تفاضل میان تعداد بیت صحیح تصویر بازیابی شده و تصویر اصلی و تعداد بیت صحیح بین تصویر پوششی و سهم تعریف شده است. روش پیشنهادی با استفاده از معیارهای PSNR، MSE، SSIM و BCR ارزیابی شد و نتایج مطلوبی بر روی تصاویر مختلف با تعداد سهام مختلف به دست آمد.

واژه‌های کلیدی: تسهیم راز، تسهیم راز بصری، تسهیم راز معنادار، الگوریتم ژنتیک

۱- مقدمه

انسان‌ها از زمانی که قادر به ارتباط با یکدیگر شدند امکان ارتباط پنهان و ایمن خواسته بشر بوده است. توزیع داده‌های مهم مانند داده‌های نظامی و تجاری در معرض خطر قرار دارند. از این رو امنیت رسانه‌های دیجیتال نیاز مهم و در حال افزایش است [۱].

گسترش روز افزون اینترنت و رشد سریع فناوری، انسان‌ها را به‌سوی جهان دیجیتال سوق داد. داده‌های دیجیتالی با توسعه فناوری ارتباطی از طریق شبکه اینترنت توزیع و به اشتراک گذاشته می‌شوند. رمزنگاری یکی از راه‌های امنیت رسانه‌های دیجیتالی است [۲].

در رمزنگاری اطلاعات به کمک یک یا چند کلید که بین طرفین به اشتراک گذاشته شده است رمزگذاری می‌شود و پیام رمز شده از طریق کانال‌های عمومی انتشار می‌یابد. در این میان ممکن است کلید رمزنگاری یا پیام رمزشده مخدوش شود و اطلاعات رمز به‌طور کلی از بین برود [۳].

تسهیم راز یکی دیگر از روش‌های برقراری امنیت در رسانه است. در این روش راز به چندین بخش تقسیم می‌شود، به‌طوری‌که هیچ‌یک از بخش‌ها به‌تنهایی اطلاعاتی را در مورد راز فاش نکند؛ اما زیرمجموعه‌ی خاصی از این بخش‌ها قادر به بازیابی آن باشد. تسهیم راز بصری گونه‌ای از روش تسهیم راز است که اجازه می‌دهد اطلاعات بصری مانند متن چاپ‌شده، یادداشت‌های دست‌نویس و تصویر به‌گونه‌ای رمز شود که بازیابی توسط سیستم بینایی انسان، بدون کامپیوتر و عملیات پیچیده انجام شود. بدیهی است این خاصیت منحصر به فرد تسهیم راز بصری، فرآیند بازیابی را حتی با کمک حمله سیل‌آسا غیرقابل دستیابی می‌کند [۴]. در

جدول ۱ اصطلاح‌های پرکاربرد در تسهیم راز بصری معرفی شده است.

جدول۱: اصطلاح‌های پرکاربردتسهیم راز بصری

$\otimes$	عملگر XOR
$\oplus$	عملگر OR
تصویر اصلی	تصویری است که توسط کاربر به الگوریتم داده می‌شود و علاقه‌مند است آن را به چندین سهم متفاوت تبدیل کند.
تصاویر سهم	تصاویر نویزگونه‌ای هستند که از روی تصویر اصلی با اجرای الگوریتم ساخته می‌شود و هیچ کدام به تنهایی بار اطلاعاتی خاصی ندارند و در صورت برهم نهی بر روی هم تصویر اصلی را خواهند ساخت.
تصویر بازیابی	تصویری است که با برهم نهی تصاویر سهم به دست می‌آید و تصویر اصلی را تولید می‌کند.
تصویر پوششی	تصویری است که برای معنادار کردن تصاویر سهم استفاده می‌شود.

برای توضیح مفهوم اولیه و اصول کار تسهیم راز یک نمونه از تسهیم راز (۲،۲) در مورد تصویر دودویی بیان می‌شود. برای تسهیم هر پیکسل و تولید دو سهم جداگانه از جدول ۲ استفاده می‌شود. اثر برهم نهی پیکسل‌ها در ردیف آخر جدول مشاهده می‌شود. این فرآیند با کاهش کیفیت و توسعه تصویر همراه است.

جدول ۲ : تسهیم راز (۲،۲) [۵]

Pixel	White		Black	
Prob.	50%	50%	50%	50%
Share 1	◧	◨	◧	◨
Share 2	◧	◨	◨	◧
Stack share 1 & 2	◧	◨	■	■

با توجه به این که هر سهم با احتمال برابر به یک جفت زیر پیکسل سیاه - سفید یا سفید - سیاه رمزگذاری می‌شود، یک سهم هیچ اطلاعاتی از تصویر اصلی در بر نخواهد داشت. علاوه بر این، چون رمزگذاری هر پیکسل مستقل از مابقی پیکسل‌ها انجام می‌شود، با مشاهده پیکسل‌های موجود در هر سهم، هیچ اطلاعاتی از تصویر مخفی به دست نخواهد آمد [۶-۵].

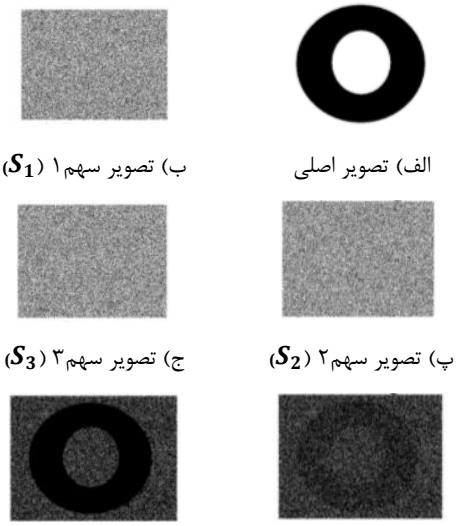
مجموعه الگوهای مختلف برای زیر پیکسل‌ها در شکل ۱ مشاهده می‌شود. در روش‌های موجود برای تسهیم راز از هر یک از سه الگوی افقی، عمودی و قطری می‌توان استفاده کرد.

شکل۱ : الگوهای زیر پیکسل‌های استفاده‌شده در تولید سهم [۷]

در تسهیم راز بصری (k, n) یک تصویر به صورت n سهم با n شرکت‌کننده به اشتراک گذاشته می‌شود. تصویر را می‌توان با روی هم قرار دادن k ($2 \le k \le n$) سهم بازیابی کرد؛ اما اگرکم‌تر از k سهم باشد هیچ اطلاعاتی به دست نخواهد آمد.

برای مثال در تسهیم راز (۲،۳) زیرمجموعه‌های مجاز شامل $\{(1،2)، (1،3)، (2،3)، (1،2،3)\}$ و زیرمجموعه‌های غیرمجاز شامل، $\{\{3\}،\{2\}،\{1\}،\{\phi\}\}$ هستند [۸-۹].

نمونه‌ای از تسهیم راز (۲،۳) در شکل ۲ نشان داده شده است. در قسمت (الف) تصویر اصلی مشاهده می‌شود. در قسمت‌های (ب) تا (ج) تصاویر سهم که هیچ اطلاعاتی از تصویر اصلی را نمی‌دهد به صورت نویزگونه ایجاد شدند و در قسمت (د) و (ه) با روی هم قرار دادن دو سهم و سه سهم تصویر اصلی بازیابی شده است.



الف) تصویر اصلی — ب) تصویر سهم۱ (S_1)

پ) تصویر سهم۲ (S_2) — ج) تصویر سهم۳ (S_3)

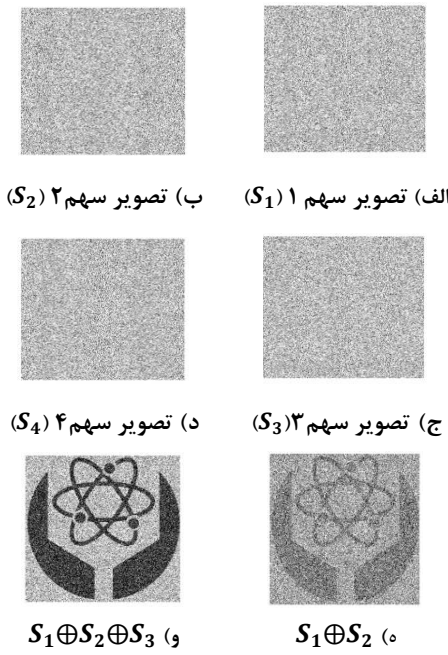
د) $S_1 \oplus S_2$ — ه) $S_1 \oplus S_2 \oplus S_3$

شکل ۲ : تسهیم راز (۲،۳) [۵]

درتسهیم راز بصری تدریجی[1] با روی هم قرار دادن سهم‌های بیش‌تر، می‌توان تصویر اصلی را با کیفیت بالاتری بازیابی کرد. در این روش اگر تعداد کمی سهم وجود داشته باشد، می‌توان یک طرح کلی از تصویر مخفی را به دست آورد. به عبارتی با افزایش سهم‌ها می‌توان وضوح تصویر بازیابی شده و اطلاعات پنهانی را افزایش داد [۱۱-۱۰].

نمونه‌ای از تسهیم راز تدریجی در شکل ۳ نشان داده شده است.

قسمت (الف) تا (د) تصاویر سهم هستند و در قسمت (ه) با قراردادن دو سهم تصویر بازیابی شده قابل مشاهده است و در قسمت (و) و (ی) با قرار دادن تعداد سهم‌های بیش‌تر بر روی هم می‌توان تصویر بازیابی شده با کیفییت بهتری مشاهده کرد.



الف) تصویر سهم ۱ (S_1)　ب) تصویر سهم۲ (S_2)

ج) تصویر سهم۳(S_3)　د) تصویر سهم۴ (S_4)

ه) $S_1 \oplus S_2$　و) $S_1 \oplus S_2 \oplus S_3$

ی) $S_1 \oplus S_2 \oplus S_3 \oplus S_4$

شکل ۳ : تسهیم راز بصری تدریجی [۶]

در تسهیم راز تصاویر مخفی مختلف با ظاهری نویزگونه تولید می‌شود. مدیریت و تمایز چندین تصویر مخفی با ظاهر نویزی دشوار است. یکی از راه‌کارهای حل این مشکل تسهیم راز بصری با سهام معنادار است. تسهیم راز بصری با سهام معنادار نوع گسترش‌یافته طرح‌های تسهیم راز بصری سنتی است [۱۳-۱۲].

در روش تسهیم راز بصری معنادار سهم‌ها دیگر بی‌نظم و بی‌معنا و نویزگونه نیستند و معنای خاصی دارند. یکی از مزایا این است که سهام معنادار هنگام ارسال از طریق شبکه عمومی موجب جلب‌توجه و حساسیت موجودیت‌های مزاحم[۲] برای حمله نمی‌شود و امنیت بهتری می‌تواند داشته باشد [۱۴-۱۲].

در شکل ۴ نمونه‌ای از روش تسهیم راز بصری معنادار دیده می‌شود. در قسمت (الف) تصویر اصلی و در قسمت (ب) تصویر پوششی نشان داده شده است. در قسمت (ج) و (د) تصاویر سهم به صورت معنادار هستند و تصویر پوششی را نشان می‌دهند. در قسمت (ه) با روی هم قرار دادن دو تصویر سهم تصویر اصلی بازیابی می‌شود.

در مطالعه‌های اخیر کیفیت سهم‌های تولیدی و کیفیت تصویر بازیابی شده اهمیت بالایی داشته است. در این پژوهش هدف ارائه

الف) تصویر اصلی　ب) تصویر پوششی

ج) تصویر سهم ۱ (S_1)　د) تصویر سهم ۲ (S_2)

ه) $S_1 \oplus S_2$

شکل ۴ : تسهیم راز بصری با سهام معنادار [۱۴]

راه‌کار جدید برای تسهیم راز بصری با سهام معنادار با استفاده از الگوریتم ژنتیک است.

ساختار مقاله به شکل زیر است. در بخش دوم پژوهش‌های پیشین در زمینه رمزنگاری بصری بیان می‌شود. در بخش سوم روش پیشنهادی بیان شده است. در بخش چهارم و پنجم نتایج و ارزیابی روش پیشنهادی ارائه شده و در بخش آخر نتیجه‌گیری بیان شده است.

۲- پیشینه تحقیق

تسهیم راز برای اولین بار در سال ۱۹۷۹میلادی توسط جرج بلکلی مطرح گردید [۱۵]. پس از آن آدی شمیر در سال ۱۹۹۴ میلادی طرح تسهیم راز بصری را ارائه نمود [۷، ۱۶]. دو عیب روش‌های فوق گستردگی پیکسل و کیفیت پایین تصاویر سهم بود [۱۷].
در سال ۱۹۸۷ میلادی کافری سه الگوریتم برای تسهیم راز بر مبنای شبکه‌های تصادفی ارائه کرد [۱۷]. در این روش‌ها از روی تصویر ورودی دو سهم به صورت تصویر نویزگونه با استفاده از شبکه تصادفی تولید شد.

در سال ۲۰۰۷ میلادی شیو بر اساس الگوریتم‌های معرفی‌شده توسط کافری روشی را برای تسهیم راز تصاویر خاکستری و رنگی ارائه نمود [۱۸] . در این روش برای تسهیم راز تصاویر خاکستری ابتدا تصویر با الگوریتم halftone به تصویر دودویی معادل تبدیل شد و سپس از سه الگوریتم کافری به‌منظور تسهیم راز تصویر باینری به‌دست‌آمده استفاده گردید.

در سال ۲۰۱۵ میلادی وحیدی روشی برای تسهیم راز تصاویر خاکستری مبتنی بر شبکه‌های تصادفی ارائه نمود [۱۹]. در این روش از سطح بیت برای تسهیم راز تصویر خاکستری بهره گرفته‌شد. ابتدا تصویر خاکستری به هشت تصویر سطح بیت معادل تبدیل می‌شود. سپس سطوح بیت با ارزش تصویر توسط الگوریتم زیر رمزنگاری شد.

فرآیند رمزگذاری

مرحله ۱: گرفتن تصویر خاکستری به عنوان ورودی

مرحله ۲: تجزیه سطوح بیتی تصویر ورودی

مرحله ۳: انتخاب سطوح بیت با ارزش (سطوح ۶، ۷ و ۸)

مرحله ۴: رمزگذاری سه سطح بیت با ارزش و تولید ۶ شبکه تصادفی $R_{16}, R_{26}, R_{17}, R_{27}, R_{18}, R_{28}$

مرحله ۵: تولید سهم اول S_1=combine (R_{16}, R_{17}, R_{18})

مرحله ۶: تولید سهم دوم S_2=combine (R_{26}, R_{27}, R_{28})

مرحله ۷: تولید خروجی (S_1, S_2)

فرآیند رمزگشایی

مرحله ۱ : $S_1 \otimes S_2$

در مرحله رمزگشایی با اجرای XOR بر روی تصاویر سهم، تصویر اصلی بازسازی می‌شود. برای اجرای فرایند برهم نهی تصاویر توسط کامپیوتر از دو عملگر OR و XOR می‌توان استفاده کرد. وحیدی نشان داد XOR با سیستم بینایی انسان سازگاری بهتری دارد. بدیهی است XOR حجم محاسباتی بیش‌تری دارد. روش-های فوق مشکل گسترش پیکسل را رفع کرد؛ اما هم‌چنان تصاویر سهم نویزگونه هستند.

در سال ۲۰۱۹ میلادی کوکراجا روشی برای رمزنگاری بصری با کمک اتوماتای سلولی ارائه کرد. در این روش از اتوماتای سلولی برای تولید سهم‌های نویزگونه استفاده شد که باعث حذف گسترش پیکسل شد.

در مرحله اول تصاویر سهم نویزگونه با استفاده از ویولت و اتوماتای سلولی ساخته می‌شوند [۲۰]. در مرحله بعد با استفاده از پارامتری به عنوان پارامتر مصالحه برای کیفیت تصویر سهم و تصویر بازیابی، تصاویر بامعنا تولید می‌شوند. هرچه این پارامتر کم‌تر باشد، کیفیت تصاویر سهم بالاتر و کیفیت تصویر بازیابی پایین‌تر است. در این روش معمولا مقدار این پارامتر ۰/۵ در نظر گرفته می‌شود.

در سال ۲۰۲۰ میلادی موهان روشی بر اساس مرجع [۲۱] ارائه کرد. در این مقاله با استفاده از الگوریتم تسهیم راز بصری می‌توان سهم‌های معنادار ایجاد کرد [۲۲].

الگوریتم در سه مرحله اجرا می‌شود. در مرحله اول با توجه به تعداد تصاویر سهم (n) دو ماتریس با اعداد صفر تا $2^n - 1$ به صورت دودویی ایجاد می‌شود و این ماتریس بر اساس فاصله همینگ به دو ماتریس M_n^{odd} و M_n^{even} تقسیم می‌شود.

برای مثال به ازای n = 2 ماتریس از صفر تا $2^2 - 1$ به دو ماتریس M_n^{odd} و M_n^{even} به صورت زیر تقسیم می‌شود.

$$n = 2 \Rightarrow \begin{bmatrix} 0\ 0 \\ 0\ 1 \\ 1\ 0 \\ 1\ 0 \end{bmatrix} \Rightarrow M_n^{odd} = \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix}, M_n^{even} = \begin{bmatrix} 0\ 0 \\ 1\ 1 \end{bmatrix}$$

در مرحله دوم از روی تصویر دودویی ورودی تعداد n ماتریس سهم به اندازه تصویر ورودی تولید می‌شود. سپس به ازاء همه پیکسل‌های تصویر از یکی از دو ماتریس M_n^{odd} یا M_n^{even} سطری را انتخاب کرده و سپس هر بیت از آن سطر در ماتریس مربوط به هر سهم $S_1, S_2, S_3, \ldots, S_n$ جایگذاری می‌شود. به عنوان مثال برای n = 2 مقادیر سهم‌ها به ازای یک بیت طبق تابع زیر مقداردهی می‌شوند. مقدار r در تابع یک عدد تصادفی صحیح است که معادل شماره سطر ماتریس M است.

$$S_1(i.j) = \begin{cases} M_n^{even}(r.1) & if\ S(i.j) = 0 \\ M_n^{odd}(r.1) & if\ S(i.j) = 1 \end{cases} \quad (۱)$$

$$S_2(i.j) = \begin{cases} M_n^{even}(r.2) & if\ S(i.j) = 0 \\ M_n^{odd}(r.2) & if\ S(i.j) = 1 \end{cases} \quad (۲)$$

در مرحله سوم تصویر پوششی هم اندازه با تصویر اصلی به عنوان ورودی داده می‌شود. در این مرحله به صورت تصادفی بیت‌های معادل از تصویر پوششی انتخاب می‌شود و در ماتریس نهایی مربوط به تصاویر سهم قرار داده می‌شود.

بدیهی است با توجه به این که در این مرحله از تصاویر پوششی استفاده می‌شود سهم‌ها معنادار خواهند بود. برای بازیابی تصویر اصلی از عملگر XOR استفاده می‌شود.

در سال ۲۰۱۹ میلادی چیو و همکاران روشی برای تسهیم راز بصری ارائه کردند[۲۳]. روش معرفی شده از دسته‌ی روش‌های مبتنی بر ORاست. روش معرفی شده با سهام معنادار و (n،۲) است. او از ماتریس‌های کد استفاده کرد تا بتواند تصویر باینری را طبق کدها رمز کند و تصویر بازیابی تا حد ممکن اطلاعات تصویر اصلی را در برداشته باشد.

در سال ۲۰۲۱ میلادی لیو و همکاران روشی ترکیبی برای تسهیم راز معرفی کردند [۲۴]. او در تحقیقش دو روش تسهیم راز معرفی شده است که بازیابی تصویر یکی به صورت بصری است و دیگری با استفاده از برونیابی لاگرانژ است که نیاز به محاسبات دارد و بصری نیست. در روش تسهیم راز بصری معرفی شده از روش‌های مبتنی بر شبکه تصادفی استفاده شده است. سهم‌های تولید شده نویزگونه هستند و روش معرفی شده توسط ایشان برای تصاویر دودویی قابل اجراست.

در سال۲۰۲۲ میلادی ژائو روشی بر مبنای عملگرهای دودویی ارائه کرد [۲۵]. در این روش اعداد تصادفی تولید شده و با بیت-های تصویر اصلی XOR می‌شوند تا تصویر سهم اول به دست آید. مابقی تصاویر سهم با چرخش‌های ۹۰ و۱۸۰ و۲۷۰ درجه تولید می‌شوند. در این روش تصاویر سهم نویزگونه هستند؛ اما بیان شده است که مشکل‌های اصلی از جمله گستردگی پیکسل را ندارد و عملیات تولید سهم برخلاف روش‌های دیگر کم هزینه‌تر است و در زمان کم‌تری صورت می‌گیرد.

مطالعه‌های انجام شده در زمینه تسهیم راز با هدف ارتقا کیفیت تصاویر بازیابی [۲۷-۲۶]، انعطاف‌پذیری ساختار دسترسی[۳] [۲۸-۲۹]، توسعه برای تصاویر رنگی [۳۰-۳۱]، بهبود روش‌های اشتراک‌گذاری [۳۳-۳۲] و امنیت بالای تسهیم راز می‌باشد[۳۴-۳۵].

۳- روش پیشنهادی

در روش پیشنهادی از الگوریتم ژنتیک جهت تنظیم هایپرپارامترهای الگوریتم برای تولید و دستیابی به تصاویر سهم معنادار و تصویر بازیابی شده با کیفیت بالا استفاده شده است. الگوریتم پیشنهادی دارای یک مرحله مقدماتی است که قبل از الگوریتم تسهیم راز باید اجرا شود. در ادامه دو مرحله‌ی الگوریتم پیشنهادی بیان می‌شود.

مرحله مقدماتی

۱- ارائه جواب‌های نامزد

یکی از چالش‌های الگوریتم ژنتیک ارائه جواب به صورت کروموزوم می‌باشد. در این پژوهش برای ارائه جواب‌های کاندید از الگوریتم ۱ استفاده شده است.

الگوریتم ۱

ورودی: تعداد تصاویر سهم (n)

خروجی: کروموزوم به طول 2^n+1

مرحله ۱- با توجه به تعداد سهم‌ها اعداد ۰ تا 2^n-1 به صورت باینری تولید شده و به هم ریزی می‌شود و در کروموزوم قرار می‌گیرد.

مرحله ۲- مقداری بین ۰ تا ۱ به صورت تصادفی تولید شده و در کروموزوم قرار داده می‌شود. این مقدار β نامگذاری می‌شود.

نمونه کروموزوم‌های تصادفی برای n = ۳ در شکل ۶ دیده می‌شود. اعداد ۰ تا ۷ باینری در کروموزوم‌ها به صورت تصادفی در مکان‌های مختلف قرار می‌گیرند و β با مقدار تصادفی بین صفر و یک مقداردهی می‌شود.

Ch1	0.2	010	001	000	111	100	110	101	011
Ch2	0.5	001	000	011	111	101	100	110	010

شکل ۶ : نمونه کروموزوم ایجادشده در الگوریتم پیشنهادی

۲-تولید مقدار r

پارامتر r با هایپرپارامتر β که با الگوریتم ژنتیک در بازه [۰-۱] تنظیم می‌شود، مرتبط است. متغیر r طبق الگوریتم ۲ با صفر یا یک مقداردهی می‌شود.

الگوریتم ۲:

ورودی: مقدار بتا در کروموزوم تولید شده توسط الگوریتم ۱

خروجی: مقدار r

مرحله ۱- عدد تصادفی ***(rand)*** تولید می‌شود.

مرحله ۲- متغیر r به صورت رابطه (۳) مقداردهی می‌شود.

$$r = \begin{cases} 0 & rand < \beta \\ 1 & rand > \beta \end{cases} \qquad (۳)$$

مرحله اصلی

۱- الگوریتم ژنتیک

پارامترهای الگوریتم ژنتیک پژوهش پیشنهادی در جدول ۳ آورده شده است. npop تعداد جمعیت اولیه، Pc نرخ تقاطع، Pm نرخ جهش و maxiter حداکثر تعداد تکرار الگوریتم ژنتیک را نشان می‌دهد. با استفاده از Pc تعداد تقاطع ncross و با استفاده از Pm تعداد جهش nmut مشخص می‌شود.

جدول ۳ : پارامترهای الگوریتم ژنتیک در روش پیشنتهادی

Crossover	One-point crossover
Mutation	Random Uniform
npop	20
Pc	0.6
Pm	0.1
maxiter	100

الگوریتم ۳:

ورودی: پارامترهای الگوریتم ژنتیک
خروجی: تصاویر سهم و تصویر بازیابی شده همراه با کروموزوم و β انتخاب شده

مرحله ۱- ابتدا الگوریتم ۴ به تعداد جمعیت اولیه npop اجرا می‌شود.
مرحله ۲- بر اساس تصاویر سهم تولید شده، تصویر بازیابی برای هر یک از جمعیت با xorکردن ایجاد می‌شود.
مرحله ۳- تابع هدف با استفاده از تابع ۶ اعمال شده و با توجه به خروجی تابع هدف، مقادیر تابع هزینه به صورت صعودی مرتب می‌شوند.
مرحله ۴- به تعداد ncross تقاطع روی کروموزوم‌ها اعمال شده تا کروموزوم‌های جدید ایجاد شوند.
مرحله ۵- به تعداد nmut جهش روی کروموزوم‌ها اعمال شده تا کروموزوم‌های جدید ایجاد شوند.
مرحله ۶- تعداد (npop-ncross-nmut) از بهترین کروموزوم‌ها که در مرحله ۳ مرتب شده‌اند انتخاب می‌شوند.
مرحله ۷- جمعیت جدید به صورت مجموع جمعیت مراحل ۴، ۵ و۶ ساخته می‌شود.
مرحله ۸- به تعداد پارامتر maxiter مراحل ۱ تا ۷ تکرار می شوند.
مرحله ۹: بهترین جواب با استفاده از تابع هدف مشخص شده و تصاویر سهم وتصویر بازیابی به دست آمده به عنوان خروجی برنامه چاپ می‌شوند.

۲- الگوریتم تولید تصاویر سهم

در این الگوریتم نحوه تولید تصاویر سهم با استفاده از کروموزوم تولید شده توسط الگوریتم ۱ توضیح داده شده است.

الگوریتم ۴:

ورودی: تصویر اصلی S
خروجی: سهم های S_1 تا S_n

مرحله ۱- الگوریتم ۱ را اجرا کرده و کروموزوم ch تولید می شود.

مرحله ۲-کروموزوم را به دو قسمت مساوی تقسیم کرده و در ماتریس M_1 و M_2 قرار می‌دهد.
به ترتیب هر پیکسل از تصویر اصلی خوانده می‌شود و مرحله ۳ برای هر پیکسل اجرا می‌شود.
مرحله ۳- عدد r را با استفاده از الگوریتم ۲ تولید کرده:

- اگر $r = 0$ باشد سهم ها به صورت نویزگونه با الگوریتم ۵ مقداردهی شوند.
- اگر $r = 1$ باشد سهم ها با تصویر پوششی با الگوریتم ۶ مقداردهی شوند.

در این قسمت نمونه‌ای از نحوه تولید ماتریس از روی کروموزوم Ch1 نشان داده شده است. نصف ابتدای کروموزوم در ماتریس M_1 و نصف دوم در ماتریس M_2 قرار می‌گیرد. کروموزم Ch1 شکل ۷ به ماتریس‌های M_1 و M_2 تبدیل می‌شود.

Ch1	0.2	010	001	000	111	100	110	101	011

$$M_1=\begin{bmatrix}0&1&0\\0&0&1\\0&0&0\\1&1&1\end{bmatrix} \quad M_2=\begin{bmatrix}1&0&0\\1&1&0\\1&0&1\\0&1&1\end{bmatrix}$$

شکل ۷ : نحوه تقسیم کروموزوم به ماتریس M_1 و M_2

در الگوریتم ۴ از روش پیشنهادی به دنبال یافتن بهترین مقادیر ماتریس‌های M_1 و M_2 است تا تصاویر سهم بیش‌ترین به هم-ریختگی را داشته باشند.

۳- الگوریتم تولید تصاویر نویزگونه

با توجه به مرحله ۳ از الگوریتم ۴ اگر مقدار r صفر باشد، با استفاده از الگوریتم ۵ سهم‌ها به صورت نویزگونه مقداردهی می‌شوند.

الگوریتم ۵:

ورودی : پیکسل تصویر اصلی S(i,j)
خروجی: سهم $S_1,S_2 \ldots S_n$

مرحله ۱- اگر مقدار پیکسل مورد بررسی صفر باشد، عددی مانند p با احتمال $\frac{1}{2^n-1}$ تولید شده و سطر p از ماتریس M_1 انتخاب می‌شود و هر بیت آن در تصاویر سهم $S_1,S_2 \ldots S_n$ قرار داده می‌شود.

مرحله ۲- اگر مقدار پیکسل یک باشد سطر p از ماتریس M_2 در سهم‌ها جای‌گذاری می‌شود.
نحوه تولید عدد p در رابطه ۴ نشان داده شده است.

$$p=\begin{cases} randi\left(\left(2^{n-1}\right).1\right) & \text{if } S(i.j)=0 \\ randi\left(\left(2^{n-1}\right).1\right) & \text{if } S(i.j)=1 \end{cases} \qquad (۴)$$

برای مثال اگر $S(1,1) = 0$ و $p = 1$ باشد، سطر اول از ماتریس M_1 در شکل ۷ انتخاب شده و به صورت زیر در ماتریس‌های تصاویر سهم برای تعداد سهم $n = ۳$ جای‌گذاری می‌شود.

$$S_1=\begin{bmatrix}0&-&-\\-&-&-\\-&-&-\end{bmatrix} \quad S_2=\begin{bmatrix}1&-&-\\-&-&-\\-&-&-\\-&-&-\end{bmatrix} \quad S_3=\begin{bmatrix}0&-&-\\-&-&-\\-&-&-\end{bmatrix}$$

۴- الگوریتم تولید تصاویر معنادار

در مرحله ۳ از الگوریتم ۴ اگر r برابر یک باشد با استفاده از الگوریتم ۶، پیکسل معادل از تصویر پوششی در سهم‌ها جاگذاری می‌شود تا تصویر سهم معنادار شود.

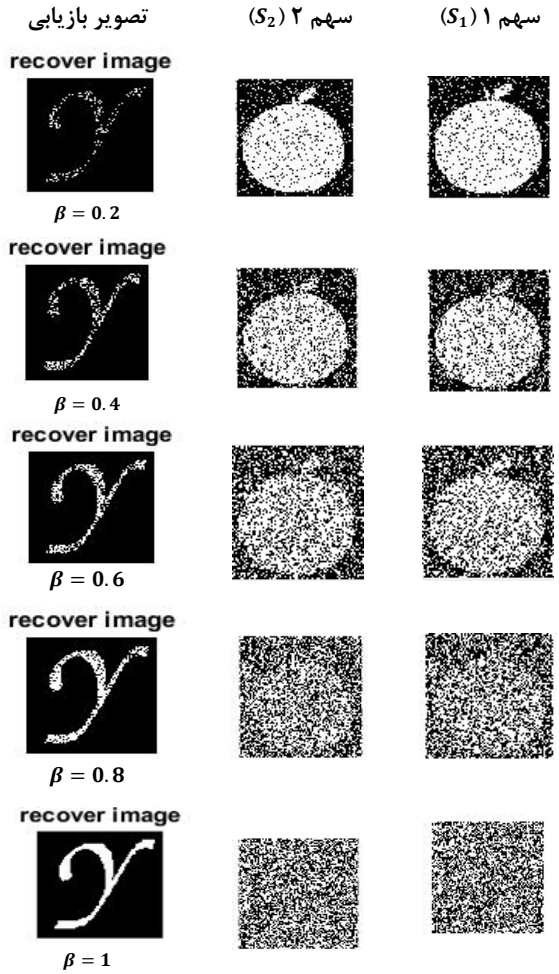
الگوریتم ۶:

ورودی: پیکسل تصویر اصلی S(i,j) و تصویر پوششی C

خروجی: سهم $S_1,S_2\ldots S_n$

مرحله ۱- بیت معادل پیکسل خوانده شده از تصویر پوششی $C(i,j)$ خوانده شده و در بیت معادل تصاویر سهم $S_1S_2\ldots S_n$,قرار داده می‌شود.

با توجه به رابطه ۳ در الگوریتم ۲ هرچه $\boldsymbol{\beta}$ بزرگ‌تر باشد، احتمال $\mathbf{r = 0}$ بیش‌تر است و الگوریتم ۴ به تعداد دفعات بیش‌تری اجرا می‌شود. بنابراین تصاویر سهم بیش‌تر نویزگونه هستند؛ اما تصویر بازیابی شده کیفیت بالاتری دارد. در مقابل هرچه $\boldsymbol{\beta}$ کوچک‌تر باشد احتمال اجرای الگوریتم ۵ بیش‌تر شده و در نتیجه تصاویر سهم مشابه تصویر پوششی و بامعناتر هستند؛ اما تصویر بازیابی شده کیفیت کم‌تری دارد.



شکل ۸: تصاویر سهم و تصویر بازیابی با β های مختلف

در روش پیشنهادی با استفاده از الگوریتم ژنتیک برای هر تصویر ورودی و تعداد تصاویر سهم مشخص شده مقدار β مناسب پیدا می‌شود تا همزمان مصالحه‌ای بین کیفیت تصویر سهم و تصویر بازیابی شده برقرار شود. برای مشاهده اثر β تصاویر سهم و تصویر بازیابی شده با β های مختلف در شکل ۸ نشان داده شده است. در ستون اول و دوم سهم‌های تولید شده و در ستون سوم تصویر بازیابی شده با قرار دادن دو سهم بر روی هم نشان داده شده است. در هر ردیف β مورد استفاده برای تولید سهم‌ها نوشته شده است.

۵- تابع هزینه الگوریتم ژنتیک

در روش پیشنهادی هدف این است که تصاویر سهم تا حد ممکن مشابه تصویر پوششی باشند و تصویر بازیابی شده بیش‌ترین اطلاعات از تصویر اصلی را نشان دهد. برای تابع هزینه از معیار اندازه‌گیری میزان شباهت[۴] دو تصویر استفاده شده است. برای اندازه گیری BCR بین دو تصویر f و g با سایز $M \times N$ از رابطه ۵ استفاده می‌شود.

$$\boldsymbol{BCR = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} 1 - [f(x.y) \oplus g(x.y)]} \qquad (۵)$$

تابع هدف:

ورودی: تصویر اصلی- تصویر بازیابی شده- تصاویر سهم- تصویر پوششی

خروجی: مقدار تابع هزینه برای تصاویر ورودی

طبق رابطه تعریف شده ۵ مقدار BCR برای هرکدام از تصاویر ورودی محاسبه می‌شود.

$$\boldsymbol{Cost = |f1 - f2|} \qquad (۶)$$

$\boldsymbol{f1}$= مقدار BCR تصویر اصلی و تصویر بازیابی شده

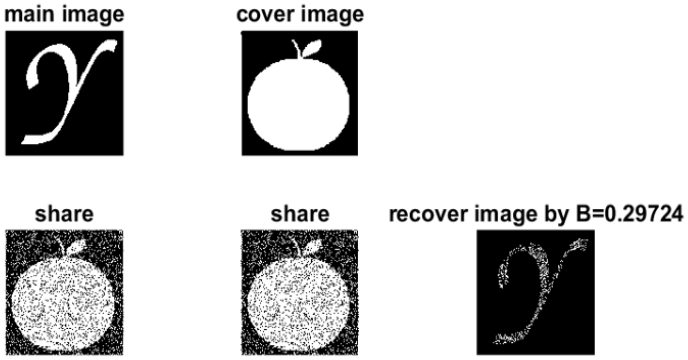
$\boldsymbol{f2}$= میانگین BCR تصاویر سهم و تصویر پوششی

مقدار تابع هزینه قدرمطلق تفاضل BCR بین تصویر بازیابی‌شده و تصویر اصلی با BCR تصویر سهم و تصویر پوششی در نظر گرفته شده است. هر چه تابع هزینه کم‌تر باشد به این معنا است که اختلاف f_1 و f_2 کم است. توجه به تنظیم β که در قسمت قبل توضیح داده شد اگر مقدار f_1 کم باشد، f_2 زیاد است و بالعکس؛ بنابراین با این تابع هزینه پیشنهادی سعی می‌شود تا مصالحه‌ای بین این دو مقدار برقرار شود تا هم‌زمان تصویر پوششی و تصاویر سهم تا حد ممکن شبیه هم باشند و تصویر بازیابی‌شده و تصویر اصلی نیز مشابه شوند. به بیان دیگر در تابع هدف سعی شده تا هم کیفیت تصاویر سهم حفظ شود و با معنا باشند و هم کیفیت تصویر بازیابی شده مطلوب باشد.

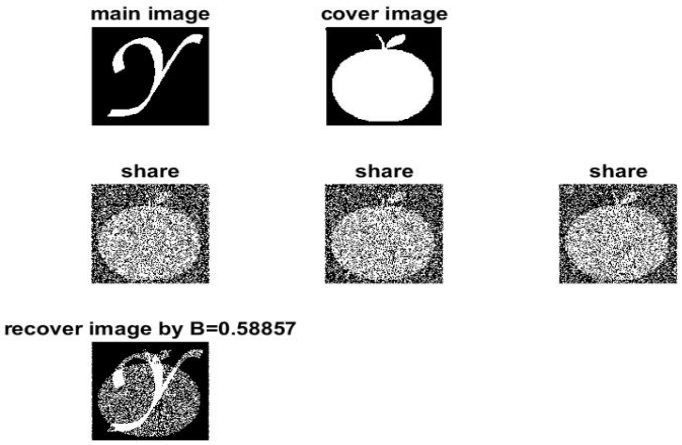
۴- نتایج آزمایش‌ها

نتایج اجرای الگوریتم در شکل ۹ نشان داده شده است. این شکل به ازای nهای متفاوت و تصاویر مختلف ورودی تهیه شده است. سطر اول شکل تصویر اصلی و تصویر پوششی می‌باشد. در سطر دوم سهم‌های تولید شده مشاهده می‌شوند. تصویر بازیابی که با XOR کردن تصاویر سهم به‌دست آمده پس از آن نشان داده شده است. در شکل مقدار β به‌دست آمده برای تصاویر بازیابی‌شده در بالای تصویر بازیابی درج شده است.

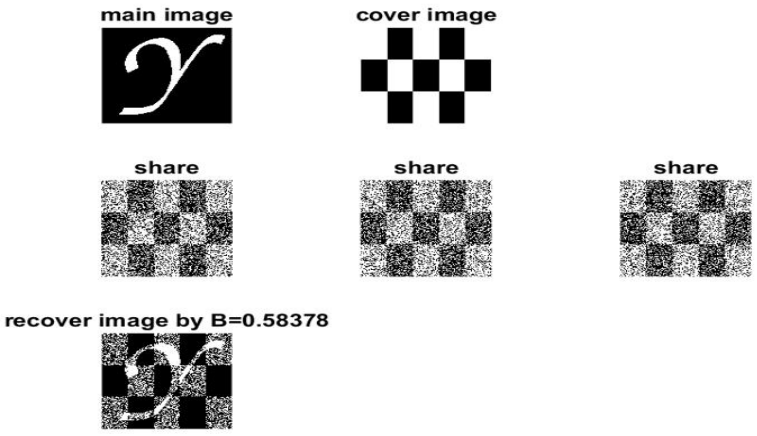
همان گونه که مشاهده می‌شود مقادیر β به دست آمده در هر تصویر متفاوت است. به عبارتی برای هر تصویر ورودی الگوریتم همزمان شرط بامعنا بودن تصاویر سهم و با کیفیت بودن تصویر بازیابی را برآورده کرده است.



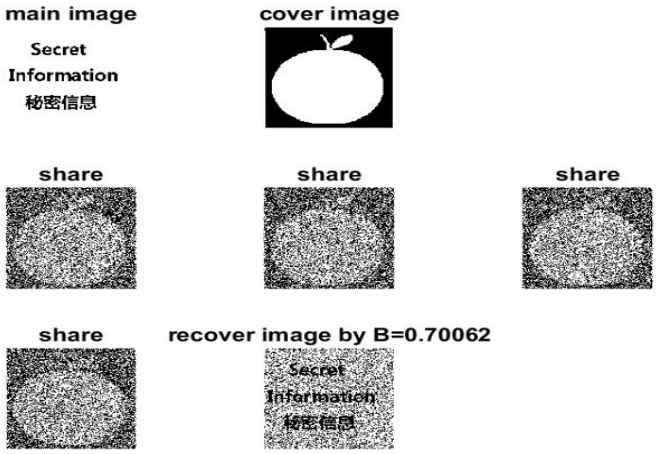
الف) تعداد سهم ۲ = n



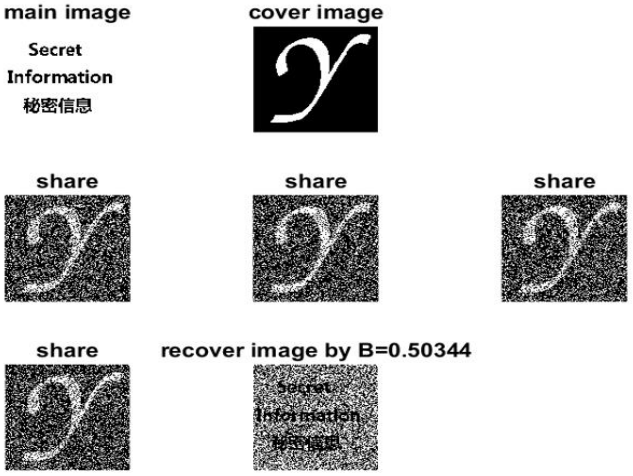
ب) تعداد سهم ۳ = n



ج) تعداد سهم ۳ = n



د) تعداد سهم n =۴



ه) تعداد سهم n =۴

شکل ۹ : نتایج اجرای الگوریتم بر روی تصاویر مختلف

۵- ارزیابی روش پیشنهادی

در تحقیق‌های انجام شده، برای ارزیابی چندین آزمون پیشنهاد شده است [۲۱-۲۰] . در این مقاله سعی شده است تا آزمون‌های معرفی شده بر روی روش پیشنهادی و مراجع [۲۰+، ۲۱، ۲۲، ۲۳، ۲۴، ۲۵] با هم مقایسه شوند.

- ***Mean Square Error (MSE)***

این معیار مجموع مربعات تفاضل بین دو تصویر $\boldsymbol{f}$ و $\boldsymbol{g}$ را محاسبه می‌کند.

$$\boldsymbol{MSE} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[\boldsymbol{f}(x.y) - \boldsymbol{g}(x.y)]^2 \qquad (۷)$$

- ***Peak Signal to Noise Ratio (PSNR)***

یکی از معیارها برای اندازه گیری میزان شباهت بین دو تصویر $\boldsymbol{PSNR}$ است.

$$\boldsymbol{PSNR} = 10\ log_{10}(\frac{255^2}{\boldsymbol{MSE}}) \qquad (۸)$$

- ***(BER) Bit Error Rate***

$\boldsymbol{BER}$ به عنوان معیاری برای تعداد بیت‌های متفاوت بین دو تصویر $\boldsymbol{f}$ و $\boldsymbol{g}$ استفاده می‌شود.

$$\boldsymbol{BER} = \frac{1}{\boldsymbol{M} \times \boldsymbol{N}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[\boldsymbol{f}(x.y) \oplus \boldsymbol{g}(x.y)] \qquad (۹)$$

$\oplus$ به عنوان عملگر $\boldsymbol{XOR}$ معرفی شده است. در این مقاله از معیار مشابه $\boldsymbol{BER}$ به نام $\boldsymbol{BCR}$ استفاده شده است. این معیار میزان شباهت دو تصویر را اندازه گیری می‌کند.

$$\boldsymbol{BCR} = \boldsymbol{1} - \boldsymbol{BER} \qquad (۱۰)$$

- ***(SSIM) Structural Similarity Index***

این معیار برای اندازه گیری شباهت ساختاری بین تصویر خروجی g و تصویر ورودی f است که این دو تصویر را بر اساس درخشندگی، کنتراست و ساختار مقایسه می‌کند. $SSIM$ یک معیار مبتنی بر سیستم بینایی انسان است که به صورت زیر تعریف می شود.

$$SSIM(x.y) = \frac{(2 \times \mu_x \times \mu_y + c_1)(2 \times \sigma_{xy} + c_2)}{(\mu_x^2+\mu_y^2 + c_1)(\sigma_x^2+\sigma_y^2 + c_2)} \quad (11)$$

که در آن μ_x، μ_y، σ_x^2، σ_y^2 و σ_{xy} به ترتیب به مقدار متوسط x، مقدار متوسط y، واریانس x، واریانس y، کوواریانس x و y اشاره دارد. مقدار SSIM از ۱- تا ۱+ متغیر است و برای دو تصویر یکسان ۱ است.

۵-۱- ارزیابی تصویر بازیابی شده

نتایج حاصل از ارزیابی با معیارهای معرفی شده در بالا بر روی الگوریتم‌های مختلف با تعداد سهم‌های مختلف (n) به ترتیب در جداول ۴ تا ۷ نشان داده شده است. این مقادیر متوسط ۲۰ بار تکرار الگوریتم می‌باشد و برای تصاویر بازیابی شده و اصلی محاسبه شده است.

جدول ۴ : مقادیر MSE بین تصویر اصلی و رمزگشایی شده

الگوریتم	MSE n = ۴	MSE n = ۳	MSE n = ۲
روش [۲۰]	۰/۲۷۴۰	۰/۲۹۶۳	۰/۲۹۲۱
روش [۲۱]	۰/۴۴۸۶	۰/۴۴۶۷	۰/۴۶۶۰
روش [۲۲]	۰/۲۷۷۵	۰/۲۷۷۸	۰/۶۱۱۶
روش [۲۳]	۰/۷۰۵۱	۰/۵۷۹۸	۰/۵۸۱۸
روش [۲۴]	۰/۶۵۹۱	۰/۶۵۳۶	۰/۶۶۰۲
روش [۲۵]	۰/۳۰۹۱	۰/۳۱۴۲	۰/۳۱۳۶
روش پیشنهادی	۰/۲۷۰۱	۰/۲۶۵۳	۰/۲۸۵۰

برای تعیین تشابه بین دو تصویر، معیار MSE باید کم باشد. در جدول ۴ میزان این معیار برای روش پیشنهادی در هر حالت به ازای تعداد سهم مختلف کم‌ترین مقدار را نسبت به دیگر روش‌ها دارد. این موضوع نشان‌دهنده اختلاف کم در بین تصویر اصلی و تصویر بازیابی شده است.

جدول۵ : مقادیر PSNR بین تصویر اصلی و رمزگشایی شده

الگوریتم	PSNR n = ۴	PSNR n = ۳	PSNR n = ۲
روش [۲۰]	۵۲,۷۵۳۳	۵۲,۸۷۷۱	۵۳,۴۷۵۵
روش [۲۱]	۵۱,۶۲۹۲	۵۱,۶۳۰۵	۵۱,۶۳۷۹
روش [۲۲]	۵۳,۶۹۸۱	۵۳,۶۹۳۱	۵۰,۲۱۳۶
روش [۲۳]	۴۹/۶۴۸۳	۵۰/۴۹۸۰	۵۰/۴۸۳۱
روش [۲۴]	۴۹/۹۴۱۳	۴۹/۹۷۷۷	۴۹/۹۳۴۰
روش [۲۵]	۵۳/۲۲۹۰	۵۳,۱۵۹۱	۵۳,۱۶۷۰
روش پیشنهادی	۵۳,۸۱۸۵	۵۳,۷۸۹۴	۵۳,۵۸۲۴

معیار PSNR هرچه بیش‌تر باشد، شباهت دو تصویر بیش‌تر است. همان طور که در سطر آخر جدول ۵ مقادیر این معیار برای روش پیشنهادی نشان داده شده است، می‌توان دریافت که این روش تصاویر بازیابی‌شده با کیفیت مطلوبی تولید می‌کند.

جدول ۶ : مقادیر BCR بین تصویر اصلی و رمزگشایی شده

الگوریتم	BCR n = ۴	BCR n = ۳	BCR n = ۲
روش [۲۰]	۰/۷۲۱۲	۰/۷۲۸۹	۰/۷۰۲۵
روش [۲۱]	۰/۵۵۶۹	۰/۵۵۳۳	۰/۵۵۸۶
روش [۲۲]	۰/۷۱۳۰	۰/۷۰۳۷	۰/۷۱۲۲
روش [۲۳]	۰/۶۰۲۹	۰/۵۸۰۲	۰/۵۹۱۲
روش [۲۴]	۰/۳۴۹	/۳۴۶۴	۰/۳۳۹۸
روش [۲۵]	۰/۶۹۰۹	۰/۶۸۵۸	۰/۶۸۶۴
روش پیشنهادی	۰/۷۲۲۲	۰/۷۳۳۸	۰/۷۱۵۲

معیار BCR متوسط تعداد بیت مشابه بین دو تصویر اصلی و بازیابی‌شده را محاسبه می‌کند. این مقدار هرچه بیش‌تر باشد نشان دهنده شباهت بیش‌تر تصویر بازیابی با اصلی است که در روش پیشنهادی نتایج قابل قبولی را نشان می‌دهد.

جدول ۷: مقادیر SSIM بین تصویر اصلی و رمزگشایی شده

الگوریتم	SSIM n = ۴	SSIM n = ۳	SSIM n = ۲
روش [۲۰]	۰/۶۲۴۵	۰/۵۵۲۱	۰/۵۰۴۱
روش [۲۱]	۰/۸۴۵۰	۰/۸۰۲۳	۰/۸۴۷۵
روش [۲۲]	۰/۸۰۴۳	۰/۷۸۵۹	۰/۷۰۲۳
روش [۲۳]	۰/۰۳۸۲	۰/۰۶۴۸	۰/۰۶۶۲
روش [۲۴]	۰/۰۵۹۰	۰/۰۶۱۷	۰/۰۶۳۰
روش [۲۵]	۰/۸۵۶۸	۰/۸۱۱۴	۰/۸۰۶۸
روش پیشنهادی	۰/۸۶۶۱	۰/۸۲۱۲	۰/۷۸۵۸

با توجه به مقادیر جداول ۷ می‌توان دریافت که در روش پیشنهادی تصویر بازیابی شده با کیفیت بالایی تولید می‌شود. بنابراین الگوریتم ژنتیک با تابع هزینه مناسب توانسته جواب رضایت‌بخشی نسبت به روش‌های موجود به‌دست آورد.

۵-۲- ارزیابی تصاویر سهم

نتایج حاصل برای تعیین تشابه تصاویر سهم و پوششی در جداول ۸ تا ۱۰ نشان داده شده است. مقادیر این جداول نشان دهنده تولید تصاویر سهم با کیفیت بالا است. در تابع ارزیابی الگوریتم ژنتیک علاوه بر ماکزیمم کردن تشابه تصویر اصلی و بازیابی شده، میزان تشابه بالا بین تصاویر سهم و پوششی نیز در نظر گرفته شده است. بنابراین الگوریتم ژنتیک سعی می‌کند تصاویر سهم با معنا و با کیفیت بالاتری تولید کند.

جدول ۸ : مقادیر MSE بین تصاویر سهم و پوششی

الگوریتم	MSE n = ۴	MSE n = ۳	MSE n = ۲
روش [۲۰]	۰/۵۰۰۲	۰/۴۹۶۶	/.۴۹۹۰
روش [۲۱]	۰/۲۴۵۸	۰/۲۵۰۸	۰/۲۴۷۷
روش [۲۲]	۰/۲۴۸۵	۰/۲۴۱۸	۰/۲۵۶۵
روش [۲۳]	۰/۳۲۳۷	۰/۳۲۵۳	۰/۳۳۲۶
روش [۲۴]	۰/۵۰۱۳	۰/۵۱۰۹	۰/۴۹۱۴
روش [۲۵]	۰/۲۶۲۴	۰/۲۵۵۶	۰/۲۵۴۴
روش پیشنهادی	۰/۲۲۵۳	۰/۲۴۰۶	۰/۱۰۳۱

در ستون اول در جدول ۸ میزان MSE برای تعداد سهم n = ۲، ستون دوم برای n = ۳ و ستون چهارم برای n = ۴ نشان داده شده است. مقدار این معیار برای روش پیشنهادی کم‌تر است که نشان دهنده تفاوت کم بین تصویر سهم و پوششی می‌باشد.

جدول۹: مقادیر PSNR بین تصاویر سهم و پوششی

الگوریتم	PSNR n = ۴	PSNR n = ۳	PSNR n = ۲
روش [۲۰]	۵۱,۱۳۹۴	۵۱,۱۷۰۷	۵۱,۱۴۹۸
روش [۲۱]	۵۴,۱۷۷۵	۵۴,۱۳۷۵	۵۴,۱۹۱۵
روش [۲۲]	۵۴,۱۷۷۵	۵۴,۲۹۲	۵۴,۰۳۹۹
روش [۲۳]	۵۳/۰۲۹۴	۵۳/۰۰۸۰	۵۲/۹۱۱۶
روش [۲۴]	۵۱/۱۲۹۸	۵۱/۰۴۷۴	۵۱/۲۱۶۵
روش [۲۵]	۵۳,۹۴۱۲	۵۴,۰۵۴۹	۵۴,۰۷۵۶
روش پیشنهادی	۵۴,۶۰۳۲	۵۴,۳۱۷۸	۵۷,۹۹۸۲

مقدار PSNR در جدول ۹ تشابه بین تصاویر سهم و پوششی است. با توجه به اینکه تعداد تصاویر سهم بیش از یک تصویر است، این مقدار به صورت میانگین محاسبه می‌شود. با توجه به جدول و مقایسه نتایج سطر آخر با دیگر روش‌ها می‌توان دریافت که در روش پیشنهادی تصویر سهم شباهت زیادی به تصویر پوششی دارند.

جدول ۱۰ : مقادیر BCR بین تصاویر سهم و پوششی

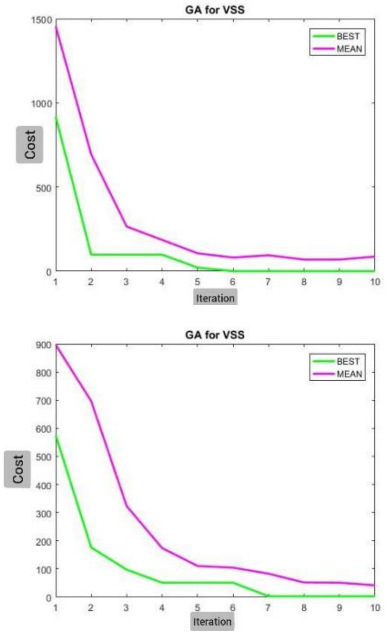
الگوریتم	BCR n = ۴	BCR n = ۳	BCR n = ۲
روش [۲۰]	۰/۴۹۹۸	۰/۵۰۳۴	۰/۵۰۱۰
روش [۲۱]	/۷۴۹۴	/۷۴۹۲	/۷۵۲۳
روش [۲۲]	۰/۷۵۱۵	۰/۷۵۸۲	۰/۷۴۳۵
روش [۲۳]	۰/۶۷۶۳	۰/۶۸۴۷	۰/۶۶۴۹
روش [۲۴]	۰/۴۹۸۷	۰/۴۸۹۱	۰/۵۰۸۶
روش [۲۵]	۰/۷۷۴۷	۰/۷۴۴۴	۰/۷۴۵۶
روش پیشنهادی	۰/۷۷۴۷	۰/۷۵۹۴	۰/۸۹۶۹

تعداد بیت‌های صحیح بیت تصاویر سهم و تصویر پوششی به صورت میانگین در جدول ۱۰ نشان داده شده است. این مقدار برای روش پیشنهادی نسبت به دیگر روش‌ها بیش‌تر است.

بنابراین روش پیشنهادی تاحد ممکن تصاویر سهم با معنا تولید می‌کند.

۵-۳- نمودار همگرایی

نمودار همگرایی الگوریتم ژنتیک در روش پیشنهادی در شکل ۱۰ نشان داده شده است. نمودار در دو حالت متوسط و بهترین پاسخ هرتکرار نمایش داده شده است. محور افقی تعداد تکرار الگوریتم و محور عمودی تابع هزینه است. همانطور که مشاهده می‌شود الگوریتم در زمان کم و با سرعت بالا به همگرایی رسیده است.



شکل ۱۰: نمودار همگرایی روش پیشنهادی

۵-۴- مقایسه ویژگی‌های تسهیم راز بصری روش‌های مختلف

در آخر برخی ویژگی‌های تسهیم راز بصری با مقالات پیشین به صورت خلاصه در جدول ۱۱ نشان داده شده است. اولین ویژگی معنادار بودن تصاویر سهم است. در ستون دوم نوع تصاویری که الگوریتم می‌تواند بر روی آن اجرا شود مشخص شده است. ستون سوم گسترش پیکسل را بررسی می‌کند. در ستون چهارم کیفیت تصویر بازیابی شده مقایسه شده است. در ستون آخر نحوه بازیابی تصویر با عملیات OR یا XOR مشخص شده است.

۶- نتیجه‌گیری

در این مقاله یک روش پیشنهادی برای تسهیم راز بصری معنادار با استفاده از الگوریتم ژنتیک ارائه شده است. طرح پیشنهادی قادر به تولید سهم‌های با معنا به منظور رفع مشکل جلب توجه و مدیریت سهام متعدد در تسهیم راز بصری است. از الگوریتم ژنتیک برای جست و جو و یافتن مقادیر مناسب هایپرپارامترهای

جدول ۱۱: مقایسه ویژگی‌های تسهیم راز بصری روش‌های پیشین با روش پیشنهادی

مقاله ها	سهام معنادار	نوع تصویر راز	گسترش پیکسل	کیفیت تصویر بازیابی	نوع بازیابی
مرجع [۱۸]	خیر	دودویی/هافتون	خیر	کم (n, n)	XOR
مرجع [۱۹]	خیر	خاکستری	خیر	زیاد(n, n)	XOR
مرجع [۲۰]	خیر	دودویی/هافتون	خیر	زیاد(n, n)	XOR + (watermark)
مرجع [۲۱]	بله	دودویی/هافتون	خیر	زیاد	XOR
مرجع [۲۲]	بله	دودویی/هافتون	خیر	زیاد(n, n)	XOR
مرجع [۲۳]	بله	دودویی/هافتون	خیر	زیاد(k, n)	OR
مرجع [۲۴]	خیر	دودویی/هافتون	خیر	زیاد(k, n)	XOR
مرجع [۲۵]	خیر	دودویی/هافتون	خیر	زیاد(k, n)	XOR
روش پیشنهادی	بله	دودویی/هافتون	خیر	خیلی زیاد (n, n)	XOR

موجود در طرح پیشنهادی استفاده شده است. روش پیشنهادی قادر به تولید مناسب هایپرپارامترها برای تصاویر مختلف و تعداد سهم‌های مختلف است تا تصاویر سهم معنادار باشند و تصویر بازیابی شده اطلاعات تصویر اصلی را نمایان کند. روش پیشنهای در مقایسه با روش‌های دیگر در تسهیم راز بصری نتایج بهتری از نظر میزان ***PSNR*** ،***BCR*** و ***SSIM*** دارد.

۷- مراجع

[1]. Y. Luo, J. Yu, W. Lai and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," Multimedia Tools and Applications, vol. 78, no. 15, pp. 22023-22043, 2019.

[2]. Z. Mehrnahad and A. Latif, "A novel image encryption scheme based on reversible cellular automata, "Journal of Electronic & Information Systems. vol. 1, pp.16-23, 2019

[3]. Z. Zhang, Y. Wang, L. Zhang and H. Zhu, "A novel chaotic map constructed by geometric operations and its application," Nonlinear Dynamics, vol. 102, no. 4, pp. 2843-2858, 2020.

[4]. Fu, Y. Cheng, S. Liu and B. Yu, "A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions," Measurement, vol. 141, pp. 267-276, 2019.

[5]. Y. Chen, B. Huang and J. Juan, "A (k, n)-Threshold Progressive Visual Secret Sharing without Expansion," Cryptography, vol. 2, no. 4, pp. 28, 2018.

[6]. S. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, vol. 39, no. 5, pp. 866-880, 2006.

[7]. M. Naorand and A. Shamir, "Visual cryptography," In Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1994, pp. 1-12.

[8]. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, vol. 12, no. 6, pp. 377, 1987.

[9]. S. F. Tua, and Y. C. Houb. "Design of visual cryptographic methods with smoothlooking decoded images of invariant size for grey-level images," The Imaging Science Journal, vol. 55, no. 2, pp. 90–101, 2007.

[10]. K. Gurunathan and S. P. Rajagopalan, "A stegano-visual cryptography technique for multimedia security," Multimedia Tools and Applications, vol.79, no. 5, pp. 3893-3911, 2020.

[11]. X. Wu and W. Sun, "Generalized Random Grid and Its Applications in Visual Cryptography," IEEE Transactions on Information Forensics and Security, vol. 8, no. 9, pp. 1541-1553, 2013.

[12]. D. Ou and W. Sun, "Reversible AMBTC-based secret sharing scheme with abilities of two

decryptions," Journal of Visual Communication and Image Representation, vol. 25, no. 5, pp. 1222-1239, 2014.

[13]. P. Singh, B. Raman and M. Misra, "A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares," Signal Processing, vol. 142, pp. 301-319, 2018.

[14]. W. Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol. 41, no. 4, pp. 1410-1414, 2008.

[15]. G. R. Blakley, "Safeguarding cryptographic Keys," International Workshop on Managing Requirements Knowledge, 1979, pp. 313–318.

[16]. A. Shamir,"How to Share a Secret," Communications of The ACM, vol. 22, no. 11, pp. 612–613, 1979.

[17]. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, vol. 12, no. 6, pp. 377, 1987.

[18]. S. Shyu, "Image Encryption by Random Grids," Pattern Recognition, vol. 40, no. 3, pp. 1014–1031, 2007.

[19]. J. Vahidi, M. Riyahi, and R. Motevalli. "A new approach for gray scale image encryption by random grids," International journal of mechatronics, Electrical and Computer Technology, vol. 5, no. 16, pp. 2169-2174, 2015.

[20]. S. Kukreja, G. Kasana, and S. S. Kasana, "Cellular Automata Based Image Authentication Scheme Using Extended Visual Cryptography," Computing and Informatics, vol. 38, no. 6, pp. 1272–1300, 2019.

[21]. D. Ou, W. Sun and X. Wu, "Non-expansible XOR-based visual cryptography scheme with meaningful shares," Signal Processing, vol. 108, pp. 604-621, 2015.

[22]. J. Mohan and R. R, "Secure Visual Cryptography Scheme with Meaningful Shares," Indian Journal of Computer Science and Engineering, vol. 11, no. 2, pp. 146-160, 2020.

[23]. P.-L. Chiu and K.-H. Lee, "Efficient constructions for progressive visual cryptography with meaningful shares," Signal Processing, vol. 165, pp. 233–249, 2019.

[24]. L. Liu, Y. Lu, and X. Yan, "A novel (k1, k2, n)-threshold two-in-one secret image sharing scheme for multiple secrets," Journal of Visual Communication and Image Representation, vol. 74, no. 102971, pp. 102971, 2021.

[25]. Y. Zhao and F. Fu, "A cheating immune (k, n) visual cryptography scheme by using the rotation of shares", Multimedia Tools and Applications, vol. 81, no. 5, pp. 6235-6257, 2022.

[26]. H. Li, Y. Wang, and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," Optics and Lasers in Engineering, vol. 115, pp. 197–207, 2019.

[27]. G. Shen, F. Liu, Z. Fu and B. Yu, "Perfect contrast XOR-based visual cryptography schemes via linear algebra," Designs, Codes and Cryptography, vol. 85, no. 1, pp. 15-37, 2016.

[28]. C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 2, pp. 189–197, 2014.

[29]. B. Yu, G. Shen, and Z. Fu, "A lossless multi-secret sharing visual cryptography scheme," Journal of Electronics & Information Technology, vol. 34, no. 12, pp. 2885–2890, 2013.

[30]. C.-N. Yang, L.-Z. Sun, and S.-R. Cai, "Extended color visual cryptography for black and white secret image," Theoretical Computer Science, vol. 609, pp. 143–161, 2016.

[31]. H. Hu, G. Shen, Z. Fu, B. Yu, and J. Wang, "General construction for XOR-based visual cryptography and its extended capability," Multimedia Tools and Applications, vol. 75, no. 21, pp. 13883–13911, 2016.

[32]. Y.-C. Chen, "Fully Incrementing Visual Cryptography from a Succinct Non-Monotonic Structure," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1082–1091, 2017.

[33]. H. Li, Y. Wang, and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," Optics and Lasers in Engineering, vol. 115, pp. 197–207, 2019.

[34]. N. C. Mhala and A. R. Pais, "A secure visual secret sharing scheme with CNN-based image enhancement for underwater images," The Visual Computer, vol. 13, pp. 1-5, 2020.

[35]. S. Kukreja, G. Kasana, and S. S. Kasana, "Cellular Automata Based Image Authentication Scheme Using Extended Visual Cryptography," Computing and Informatics, vol. 38, no. 6, pp. 1272–1300, 2019.

پاورقی:

[1] Gradual secret sharing
[2] Intruder
[3] Access structure
4 Bit Correct Ratio (BCR)