نشریه علمی «علوم و فناوری‌های پدافند نوین»

سال دوازدهم، شماره ۴، زمستان ۱۴۰۰؛ ص ۳۵۶- ۳۴۵

علمی- پژوهشی

یک طرح جدید رمزنگاری بصری بر اساس تریدهای اشتاینری

سعیده رشیدی[۱*]، نسرین سلطان‌خواه[۲]

۱- استادیار، دانشگاه شهید باهنر کرمان، کرمان، ایران ۲- استاد، دانشگاه الزهرا (س)، تهران، ایران

(دریافت: ۱۳۹۹/۱۲/۰۱، پذیرش: ۱۴۰۰/۰۸/۲۵)

چکیده

در سامانه‌های رمزنگاری متقارن نیاز به کانال امن برای تبادل کلید، همواره یکی از مسائل اصلی است. در مقابل سامانه‌های رمزنگاری با کلید عمومی (نامتقارن) ایجاد شده‌اند که این مسأله را برطرف می‌سازند. اما در اکثر سامانه‌های رمزنگاری با کلید عمومی، محاسبات نقش بسیار مهمی ایفا می‌کند. در اینجا می‌توان به طرح‌های رمزنگاری بصری اشاره کرد. در این نوع سامانه برای رمزگشایی تنها از چشم انسان استفاده می‌شود و هیچ‌گونه نیازی به محاسبات نیست. این سامانه دارای امنیت بدون قید و شرط است. در این سامانه، تصویر رمز بین n شرکت‌کننده به اشتراک گذاشته می‌شود و k شرکت‌کننده از روی هم گذاشتن لایه‌های تصویر، رمز را بازیابی می‌کنند. مدل‌های متنوعی از طرح رمزنگاری بصری تا به امروز ساخته شده است. در این نوشته به بررسی طرح‌های رمزنگاری بصری ساخته‌شده بر پایه طرح‌های بلوکی می‌پردازیم و روش جدیدی برای ساخت طرح رمزنگاری بصری بر پایه تریدهای اشتاینری همگن معرفی می‌کنیم. در این روش شرکت‌کنندگان در این طرح افزایش یافته اما از کنتراست تصویر کم نمی‌شود. همچنین الگوریتم مرتبط با روش پیشنهادی جدید با زبان پایتون نوشته شده و سه تصویر از نتایج اجرای آن در مقاله آمده است.

کلیدواژه‌ها: سامانه رمزنگاری بصری، طرح بلوکی، ترید اشتاینری همگن

A Novel Visual Cryptography Scheme Based on Steiner Trades

S. Rashidi[*1], N. Soltankhah[2]

Assistant Professor, Shahid Bahonar University of Kerman, Kerman, Iran.

(Received: 01/03/2021; Accepted: 16/11/2021)

Abstract

The existence of a secure channel for sharing secret key, is the main problem in the symmetric cryptography. This problem is solved by the asymmetric cryptography (Public key cryptography). Computation has the main rule in the public key cryptography. Here, we investigate the visual cryptography schemes. Human vision decodes the secret image in the visual cryptography scheme and no computations required for this aim. The visual cryptography scheme has an unconditional security. In this system, the secret image is shared between n participants and k participants can recover the secret image by stacking image layers. Various constructive models of the visual cryptography schemes have been constructed up to now. We investigate one type of the visual cryptography scheme that is based on BIBDs (Balanced Incomplete Block Design). In this paper, we introduce and construct new visual cryptography schemes based on homogeneous Steiner trades. The concept of homogeneous steiner trades is closely related to BIBDs.

Keywords: Visual Cryptography Scheme, Block Design, Homogeneous Steiner Trade.

[*]Corresponding Author E-mail: saeedeh.rashidi@uk.ac.ir

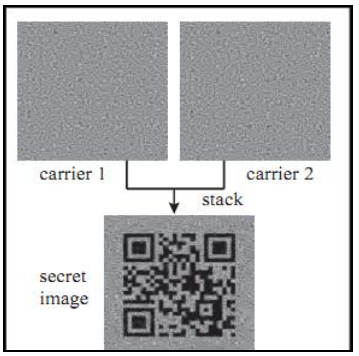
۱. مقدمه

فرآیند تبدیل متن خام به متن رمز را رمزنگاری و تبدیل متن رمزشده به متن‌خام را رمزگشایی گویند. دو هدف اصلی، حفظ حریم خصوصی و اصالت داده‌ها در رمزنگاری مطرح است. منظور از «حفظ حریم خصوصی» به دست نیاوردن اطلاعات در رابطه با پیام ارسالی توسط دشمن است. همچنین «اصالت داده‌ها» به عدم امکان ایجاد تغییر در پیام ارسالی توسط رقیب اشاره دارد.

تاکنون سامانه‌های رمزنگاری مختلفی طراحی و بررسی شده‌اند. یکی از آنان طرح رمزنگاری بصری است. در این مقاله به‌طور خاص در رابطه با طرح رمزنگاری بصری و مفهوم کنتراست در طرح رمزنگاری بصری بحث می‌شود. طرح رمزنگاری بصری در واقع یک طرح تسهیم راز (اشتراک گذاشتن رمز) است. اشتراک‌گذاری رمز از زمان‌های گذشته رایج بوده است. به‌عنوان مثال تقسیم نقشه یک گنج بین چندین نفر در گذشته و حساب‌های بانکی مشترک در زمان حال از نمونه‌های طرح تسهیم راز می‌باشد. طرح تسهیم راز یکی از مباحث مهم و کاربردی در شاخه‌ی رمزنگاری است که در آن اطلاعات یک موضوع رمزی بین افراد تقسیم می‌شود [۱]. رمز می‌تواند یک عدد صحیح، یک تصویر و یا یک رشته بولین باشد. این طرح که نخستین بار در سال ۱۹۷۹ توسط شامیر[1] ارائه شد، اکنون در کارهای بسیار مهمی که برای آن نیاز به حضور افرادی خاص است، مورد استفاده قرار می‌گیرد [۲].

به‌طورکلی «طرح تسهیم راز» شامل دو مرحله است: مرحله‌ی اول توزیع و تولید سهم و مرحله‌ی دوم بازیابی راز. در مرحله‌ی تولید و توزیع سهم، مقسم سهم‌ها را از سهم‌بندی راز به دست آورده و بین سهام‌داران توزیع می‌کند. در مرحله‌ی بازیابی رمز زیرمجموعه‌های مجاز از سهام‌داران با اشتراک گذاشتن سهم‌های خود می‌توانند، رمز را به‌دست آوردند. لازم به ذکر است، منظور از سهم، اطلاعاتی است که از تقسیم کردن راز به دست می‌آید. سهم‌های به‌دست‌آمده توسط فردی به نام مقسّم به سهام‌داران اختصاص می‌یابد. سهام‌داران نیز افراد شرکت‌کننده در طرح می‌باشند. بازیابی رمز توسط فرد قابل اطمینانی به نام ترکیب‌کننده انجام می‌گیرد.

در طرح رمزنگاری بصری، راز یک تصویر است. سهم‌ها هیچ اطلاعاتی از تصویر اصلی ندارند و زمانی که سهم‌ها بر روی طلق‌های شفاف چاپ شوند و بر روی هم قرار بگیرند، رمز قابل بازیابی است. در واقع، در این طرح برای تقسیم تصویر رمز هر پیکسل از آن به m زیر پیکسل تقسیم می‌شود. پارامتر m را گسترش پیکسل می‌گویند [۳] (شکل ۱).



شکل ۱. روی هم گذاردن دو لایه

۱-۱. طرح‌های رمزنگاری بصری

طرح رمزنگاری بصری نخستین بار توسط شامیر و نائور در سال ۱۹۹۴ ارائه شد [۲]. پیام در طرح رمزنگاری بصری (VCS)[2] یک تصویر سیاه و سفید و یا رنگی خواهد بود. سهم‌ها لایه‌هایی از تصویر می‌باشند که بر روی طلق‌هایی شفاف چاپ می‌شوند و از روی هم قرار دادن لایه‌ها، تصویر اصلی بازیابی می‌شود. در این مقاله به انواعی از روش‌های ساخت طرح‌های رمزنگاری بصری با تصاویر سیاه و سفید خواهیم پرداخت که در آن‌ها از مفاهیم ریاضی به‌ویژه اشیای ترکیبیاتی استفاده شده است. منظور از یک شیء ترکیبیاتی، ساختار ریاضیِ مشخص در ترکیبیات مانند مربع‌های لاتین یا طرح‌های بلوکی است.

طرح‌های رمزنگاری از سه نوع امنیتِ محاسباتی، امنیتِ قابل اثبات و امنیتِ بدون قید و شرط برخوردارند. یک طرح رمزنگاری در صورتی دارای امنیت بدون قید و شرط است که رمزِ آن با در اختیار داشتنِ بی‌نهایت منابع محاسباتی شکسته نشود [۴]. در طرح‌های رمزنگاری بصری هدف این است که ارتباطی امن از طریق کانال‌های ناامن برقرار شود و مزیت این طرح‌ها این است که از حس بینایی در رمزگشایی استفاده می‌شود و احتیاجی به دانش پیچیده یا الگوریتم‌های محاسباتی نیست.

قبل از تعریف دقیق *VCS* نیاز به بیان مفهوم «ساختار دسترسی» داریم که به این صورت تعریف می‌شود:

تعریف ۱. ساختار دسترسی: اگر P مجموعه شرکت‌کنندگان در یک طرح باشد و Γ_Q مجموعه‌ای از زیرمجموعه‌های P، به‌طوری‌که زیرمجموعه‌هایِ متعلق به آن، زیرمجموعه‌هایی از سهام‌داران باشند که بتوانند رمز را محاسبه کنند (مجموعه‌های مجاز) و Γ_F مجموعه‌ای از زیرمجموعه‌های P، به‌طوری‌که زیرمجموعه‌های متعلق به آن، زیرمجموعه‌هایی از سهام‌داران باشند که قادر به بازیابی رمز نباشند (مجموعه‌های ممنوع)، آنگاه (Γ_Q, Γ_F) را ساختار دسترسی گویند [۴].

[1] Shamir

[2] Visual cryptography Scheme

تعریف ۲. ساختار دسترسی آستانه: اگر تمام مجموعه‌های مجاز در ساختار دسترسیِ (Γ_Q, Γ_F)، k عضوی باشند و مجموعه‌های ممنوع کمتر از k عضو داشته باشند، آن را یک ساختار دسترسی آستانه (k, n) می‌نامیم [۴].

در تعریف زیر، طرح رمزنگاری بصری بر اساس ماتریس‌های پایه $\mathbf{S^0}$ و $\mathbf{S^1}$ (ماتریس‌های صفر و یک) بیان می‌شود. ماتریس‌های پایه به این صورت ساخته می‌شوند: فرض کنیم که تصاویر مخفی شامل خانواده‌ای از پیکسل‌های سیاه و سفید باشد. هر پیکسل سفید به n سهم تقسیم‌بندی می‌شود، به‌طوری‌که برای هر سهم یک طلق شفاف در نظر گرفته می‌شود. هر سهم خانواده‌ای از m زیرپیکسل سیاه و سفید است. ساختار حاصل به‌صورت یک ماتریس بولین $n\times m$، $\mathbf{S^0}$ است به‌طوری‌که $s^0_{ij=1}$ اگر j امین زیر پیکسل در i امین طلق شفاف سیاه باشد. به همین ترتیب ماتریس $\mathbf{S^1}$ برای پیکسل سیاه تعریف می‌شود. منظور ازw در تعریف زیر وزن همینگ بردار است که در واقع تعداد یک‌های بردار V را به ما می‌دهد. عمل or نیز طبق جدول (۱) انجام می‌شود.

جدول ۱. عمل or

A	B	A or B
۱	۱	۱
۱	۰	۱
۰	۱	۱
۰	۰	۰

تعریف ۳. *VCS*: فرض کنید (Γ_Q, Γ_F)، یک ساختار دسترسی روی مجموعه‌ای با n شرکت‌کننده باشند. یک طرح رمزنگاری بصری (Γ_Q , Γ_F)-*VCS* با تفاوت نسبی $\alpha(m)$ با استفاده از ماتریس‌های پایه $n\times m$، $\mathbf{S^1}$ و $\mathbf{S^0}$ و مجموعه آستانه $\{t_X\}_{X\in\Gamma_Q}$ ایجاد می‌شود، در صورتی که:

۱- اگر $X=\{i_1,...,i_q\}$ و $X\in\Gamma_Q$ آنگاه بردار V^0 از عمل or سطرهای $i_1,...,i_q$ ماتریس $\mathbf{S^0}$ به‌دست می‌آید در شرط $\omega(V^0)\le t_X-\alpha(m)m$ صدق کند و برای سهم‌های متناظر ماتریس $\mathbf{S^1}$ داشته باشیم $\omega(V1)\ge t_X$.

۲- اگر $X\in\Gamma_F$ و $X=\{i_1,...,i_q\}$ آنگاه دو ماتریس $q\times m$، $\mathbf{D^1}$ و $\mathbf{D^0}$ که سطرهای متناظر با $i_1,...,i_q$ از ماتریس $\mathbf{S^1}$ و $\mathbf{S^0}$ می‌باشند با جایگشت دادن ستون‌ها یکسان شوند [۴].

نکته ۱. ویژگی اول تعریف (۳) مرتبط با کنتراست تصویر است و بیانگر این موضوع است که اعضای مجموعه مجاز می‌توانند، تصویر را به‌درستی بازیابی کنند. ویژگی دوم مربوط به مسأله امنیت است و بیان می‌کند که اعضای مجموعه غیرمجاز حتی با روی هم گذاشتن طلق‌هایشان هیچ اطلاعاتی در رابطه با اینکه کدام پیکسل سیاه و یا کدام پیکسل سفید بوده است به‌دست نمی‌آورند.

مثال ۱. فرض کنید $n=4$ به‌طوری‌که $P=\{1,2,3,4\}$، مجموعه مجاز به‌صورت [۱]:

$$\Gamma_Q=\{\{1,2\},\{2,3\},\{3,4\},\{1,2,3\}\}$$

و مجموعه غیرمجاز ساختار به‌صورت:

$$\Gamma_F=\{\{1\},\{3\},\{3\},\{4\},\{1,3\},\{1,4\},\{2,4\}\}$$

باشد. ساختار یک طرح رمزنگاری (Γ_Q, Γ_F)-*VCS* به‌صورت زیر با استفاده از ماتریس‌های پایه $\mathbf{S^1}$ و $\mathbf{S^0}$ ساخته می‌شود.

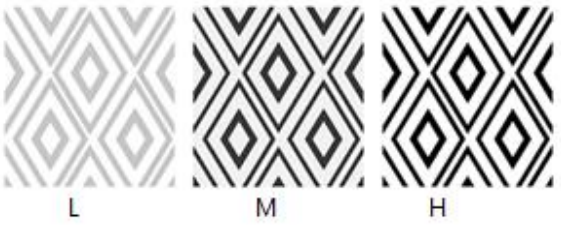
$$S^0=\begin{bmatrix}1&0&1\\1&0&0\\1&0&0\\1&1&0\end{bmatrix}\quad S^1=\begin{bmatrix}0&1&1\\1&0&0\\0&0&1\\1&1&0\end{bmatrix}$$

در این طرح $\alpha(m)=\dfrac{\omega(V1)-\omega(V^0)}{3}=\dfrac{1}{3}$.

با در نظر گرفتن مجموعه آستانه‌ی بالا واضح است که: $t_{\{1,2,3\}}=3, t_{\{1,2\}}=t_{\{2,3\}}=t_{\{3,4\}}=2$.

۱-۲. کنتراست

کنتراست و گسترش پیکسل مهم‌ترین پارامترها در سامانه رمزنگاری تصویری‌اند. اکثر پژوهش‌های سامانه رمزنگاری تصویری در رابطه با بهترین مقدار برای این دو پارامتر است. در این بخش مفهوم کنتراست و انواعی از آن را شرح می‌دهیم. مقیاس سنجش وضوح تصویر (اختلاف بین سفیدی و سیاهی) را کنتراست گویند. به‌عنوان مثال در شکل (۲) یک تصویر یکسان با کنتراست کم، متوسط و بالا دیده می‌شود.



شکل ۲. سه تصویر با کنتراست متفاوت

تصویری که در سامانه رمزنگاری بصری بازیابی می‌شود به واضحی تصویر اولیه نمی‌باشد. وضوح تصویر اولیه در مقایسه با تصویر بازیابی شده توسط مفهوم کنتراست سنجیده می‌شود.

تعریف ۴. منظور از سطح تیرگی، تعداد زیرپیکسل‌های سیاه در یک پیکسل (سیاه یا سفید) بازیابی شده است. کران پایین سطح تیرگی پیکسل‌های سیاه تصویر بازیابی شده با پارامتر h و کران بالای سطح تیرگی در پیکسل‌های سفید تصویر بازیابی شده (زمان رمزگشایی) با پارامتر l نمایش داده می‌شود [۴].

نکته ۲. در پیکسل‌های بازیابی‌شده برای اینکه متمایل به رنگ سیاه باشند، بایستی سطح تیرگی از عدد مشخصی بیشتر باشد که این عدد همان پارامتر h است و برای اینکه متمایل به رنگ سفید باشند، بایستی سطح تیرگی از عدد مشخصی کمتر باشد که این عدد همان پارامتر l است. مشهورترین فرمول کنتراست توسط نائور و شامیر به‌صورت زیر ارائه شده است [۵].

$$\alpha_{NS}=\frac{h-l}{m} \qquad (۱)$$

اگر l و h به ترتیب مقادیر ۰ و m را اختیار کنند، آنگاه مقدار کنتراست برابر یک می‌شود و تصویر با بهترین وضوح بازیابی می‌شود؛ اما مقدار کنتراست به مقادیر m، l و h وابسته است و با تغییر در این مقادیر با وجود ثابت ماندن مقدار کنتراست وضوح تصاویر متفاوت است. ورهولو وان تیلبرگ تعریف دیگری از کنتراست ارائه دادند [۵]:

$$\alpha_{VV}=\frac{h-l}{m(h+l)} \qquad (۲)$$

در اینجا مانند تعریف قبل تفاوت دو پارامتر h و l در مقدار کنتراست تأثیرگذار است. همچنین مقدار دو پارامتر نیز در مقدار کنتراست تأثیر دارد. در تعریف قبل این موضوع در نظر گرفته نشده بود.

اما یکی از معایب این تعریف این است که یرای $l=0$ (در این حالت تمام پیکسل‌های سیاه بازسازی می‌شوند)، پارامتر h از بین می‌رود و هیچ‌گونه تأثیری در مقدار کنتراست ندارد؛ یعنی تمام طرح‌های رمزنگاری بصری که مقدار یکسان m داشته باشند و $l=0$ دارای کنتراست یکسان خواهند بود و در این صورت در تصویرهای بازیابی شده‌ای که پیکسل‌های سیاه به‌طور کامل بازیابی شده‌اند، تعداد پیکسل‌های سفید بازیابی‌شده موضوعیتی نخواهد داشت. اما در واقع چنین نیست و تصویرهایی که مقدار پارامتر h در آن‌ها متفاوت است، وضوح متفاوت دارند. عیب دوم تعریف این است، تنها در صورتی که $m=1$، مقدار کنتراست l می‌شود؛ یعنی برای $m>1$ حتی در صورت بازیابی تمام پیکسل‌های سیاه و پیکسل‌های سفید، وضوح تصویر بازیابی‌شده از وضوح تصویر اصلی وضوح کمتر است.

ایسن و استینسون رابطه دیگری برای محاسبه مقدار کنتراست در [۸] معرفی کردند:

$$\alpha_{T}=\frac{h-l}{m+l} \qquad (۳)$$

علاوه بر ویژگی مثبت تعاریف می‌توان ۴ ویژگی مثبت زیر را نیز برای این تعریف برشمرد.

۱- تغییر مقدار هر یک از سه پارامتر h، l و m مقدار کنتراست را نیز تغییر می‌دهد.

۲- زمانی که مقدار پارامتر l افزایش می‌یابد، مقدار کنتراست نیز زیاد می‌شود (مانند مثال‌های واقعی).

۳- برای l=0 مقدار کنتراست، h/m است که همچنان به مقدار h وابسته است.

۴- برای l=0 و h=m تصویر کاملاً بازیابی می‌شود و مقدار کنتراست برابر یک است.در سال ۲۰۱۰ سه نفر یا نام‌های وو، لیو و لین تعریف دیگری برای مفهوم کنتراست ارائه دادند [۶].

$$\alpha_{(m,h,l)}=\frac{(h-l)m}{h(m-h)+l(m-l)+m^2} \qquad (۴)$$

از نظر آن‌ها تعریفی که ارائه دادند، ضمن اینکه ویژگی‌های بهتری نسبت به تعاریف قبلی داشت، از معایب تعاریف قبلی نیز عاری بود. این تعریف هماهنگی بیشتری با مثال‌های واقعی داشته به‌گونه‌ای که:

۱- برای h و l زمانی که مقدار m افزایش پیدا می‌کند، مقدار کنتراست کم می‌شود.

۲- اگر مقدار h-l افزایش پیدا کند، آنگاه مقدار کنتراست زیاد می‌شود.

۳- $\alpha(m,h,l)=\alpha(m,m-l,m-h)$

۴- برای m و h-l ثابت، اگر مقدار |h+l-m| کم شود، آنگاه مقدار کنتراست کاهش می‌یابد.

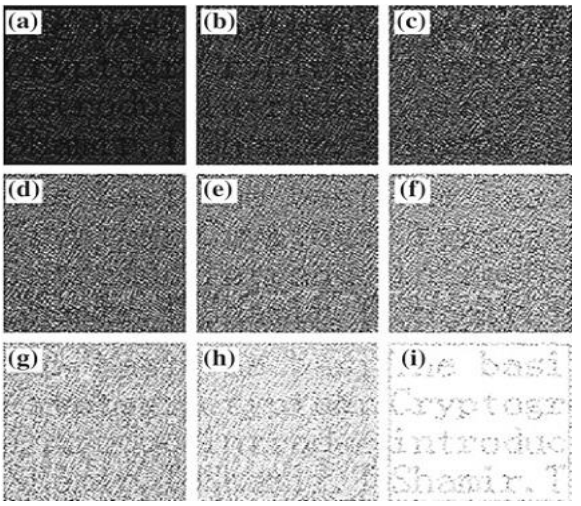
سه تعریف قبل در قسمت سوم و چهارم آخرین تعریف صدق نمی‌کنند. لین و همکارانش در [۷] نشان دادند این چهار نکته در مورد تعریف موردنظرشان برقرار است. در مثال زیر مقدار $\alpha(m,h,l)$ برای یک شکل با پارامترهای متفاوت بررسی شده است.

مثال ۲. در شکل (۳) تصاویر مخفی بهبودیافته به ترتیب با پارامترهای a تا i بیان شده است [۷]. درستی نکته چهارم به‌وضوح در شکل (۳) دیده می‌شود.

$$a=\begin{cases}m=9\\h=9\\l=8\end{cases}\ b=\begin{cases}m=9\\h=8\\l=7\end{cases}\ c=\begin{cases}m=9\\h=7\\l=6\end{cases}$$

$$d=\begin{cases}m=9\\h=6\\l=5\end{cases}\ e=\begin{cases}m=9\\h=5\\l=4\end{cases}\ f=\begin{cases}m=9\\h=4\\l=3\end{cases}$$

$$g=\begin{cases}m=9\\h=3\\l=2\end{cases}\ h=\begin{cases}m=9\\h=2\\l=1\end{cases}\ i=\begin{cases}m=9\\h=1\\l=0\end{cases}$$



شکل ۳. یک تصویر بهبودیافته با پارامترهای متفاوت

مثال ۳. در جدول (۲) چهار مقدار کنتراست برای دو طرح رمزنگاری بصری شناخته‌شده‌ی درسته[1] و بلاندو[2] با یکدیگر مقایسه شده‌اند. پارامترها در طرح VCS-(2,4) درسته، به‌صورت، $h=2$، $m=4$ و $l=1$ می‌باشد. در طرح بلاندو، به‌صورت، $h=4$، $m=4$ و $l=3$ می‌باشد. جدول زیر نشان می‌دهد که وضوح تصویر بازیابی شده در طرح بلاندو نسبت به طرح درسته بیشتر می‌باشد و مقدار $\alpha(m, h, l)$ به یک نزدیک‌تر است. [۸].

جدول ۲. مقایسه کنتراست

	Droste (2,4)-VCS	Blundo (2,4)-VCS
α_{NS}	$\frac{1}{4}$	$\frac{1}{4}$
α_{VV}	$\frac{1}{5}$	$\frac{1}{28}$
α_{ES}	$\frac{1}{12}$	$\frac{1}{7}$
$\alpha_{(m,h,l)}$	$\frac{4}{23}$	$\frac{4}{19}$

۲. طرح‌های بلوکی و طرح‌های رمزنگاری مرتبط

همان‌گونه که در مقدمه اشاره شد در این مقاله به بررسی طرح‌های رمزنگاری بصری ساخته‌شده بر اساس اشیاء ترکیبیاتی پرداخته می‌شود. طرح بلوکی یک شیء ترکیبیاتی است که تعریف آن در زیر آمده است.

تعریف ۵. فرض کنید، v ,k ,λ مقادیر صحیح مثبتی باشند، به‌گونه‌ای که $k \le v$ و $2 \le v$. یک (v,b,r,k,λ)- $BIBD$، یک زوج مرتب (X , B) می‌باشد؛ به‌طوری‌که X یک مجموعه با v عضو می‌باشد و B یک خانواده از زیرمجموعه‌های X می‌باشد که آن‌ها را بلوک نامیده‌اند. به‌طوری‌که هر بلوک دقیقاً شامل k عضو می‌باشد.

[1] Droste
[2] Blundo

هر جفت از اعضای X دقیقاً در λ بلوک ظاهر می‌شوند. ثابت می‌شود، در یک (v,b,r,k,λ)- $BIBD$، رابطه زیر برقرار است [۸]:

$$r(k-1)=\lambda(v-1)$$
$$bk=vr \qquad (۵)$$

معمولاً طرح بلوکی را به اختصار با (v,k,λ)-$BIBD$ نمایش می‌دهند.

نکته ۳. متوازن بودن ویژگی اصلی طرح بلوکی است. منظور از متوازن بودن این است که هر دوتایی از عناصر به تعداد یکسان در طرح ظاهر می‌شوند. این تعداد یکسان همان عدد λ است.

مثال ۴. در اینجا مثالی از یک $BIBD$ - $(7,7,3,3,1)$ را می‌بینیم. در این طرح $\lambda=1$ است، یعنی هر دو عنصری از اعضای مجموعه X به تعداد یکسان در بلوک‌های B ظاهر می‌شود.

$$X=\{1,2,3,4,5,6,7\}$$

$$B=\begin{pmatrix} B_1=\{1,2,3\} & B_3=\{1,6,7\} & B_5=\{2,4,6\} \\ B_2=\{3,4,7\} & B_4=\{3,5,6\} & B_6=\{2,5,7\} \\ & & B_7=\{1,4,5\} \end{pmatrix}$$

تعریف ۶. فرض کنید X مجموعه اعضاء باشد، B مجموعه بلوک‌ها و $B \in \boldsymbol{B}$ بلوکی دلخواه باشد. ماتریس وقوع طرح، یک ماتریس $\mathbf{M}$، $v \times b$ می‌باشد. به‌طوری‌که ورودی سطرهای آن توسط X پر شده و ورودی ستون‌های آن توسط B پر می‌شود. هر درایه از ماتریس به‌صورت زیر می‌باشد [۱۲]:

$$m_{xB}=\begin{cases} 1 & x \in B \\ 0 & O.W. \end{cases} \qquad (۶)$$

مثال ۵. در اینجا ماتریس وقوع مثال قبل دیده می‌شود.

$$\begin{pmatrix} 1&0&1&0&1&0&1 \\ 1&0&0&0&0&1&0 \\ 1&1&0&1&0&0&0 \\ 0&1&0&0&0&0&1 \\ 0&0&0&1&1&1&1 \\ 0&0&1&1&1&0&0 \\ 0&1&1&0&0&1&0 \end{pmatrix}$$

در واقع هر سطر نمایشگر یک عضو و هر ستون نمایشگر یک بلوک است. تعداد یک‌های هر سطر ۳ می‌باشد و تعداد ظاهر شدن هر عنصر در طرح را نمایش می‌دهد، که همان r است. تعداد یک‌های هر ستون نیز ۳ می‌باشد و اندازه بلوک‌ها را نشان می‌دهد، که همان k می‌باشد. هر دو سطر یک عدد ۱ در ستون یکسان دارند

که به‌دلیل متوازن بودن طرح است. در حالت کلی هر دو سطر از ماتریس وقوع به تعداد λ عدد ۱ در ستون یکسان دارند.

قضیه ۱. فرض کنید n یک عدد صحیح زوج باشد. در صورت وجود یک $BIBD(\frac{n}{2},\frac{m(n-2)}{4n-4},n)$-، یک طرح رمزنگاری VCS-$(2,n)$ آستانه با گسترش پیکسل m و تفاوت نسبی $\alpha(m)=\frac{\left\lceil\frac{n}{2}\right\rceil-\left\lfloor\frac{n}{2}\right\rfloor}{n(n-1)}$ وجود دارد [۴].

نکته ۴. در [۵] ثابت شده است که مقدار تفاوت نسبی ذکر شده در قضیه بالا بهینه است.

مثال ۶. فرض کنید $n=11$ و (X, B) یک $BIBD$ با $k=5$ و $\lambda=2$ باشد. در اینجا $X=Z_{11}$ و بلوک‌های این طرح به‌صورت زیر می‌باشند [۵]:

$$\{0,2,3,4,8\},\{1,3,4,5,9\},\{2,4,5,6,10\},$$
$$\{3,5,6,7,0\},\{4,6,7,8,1\},\{10,1,2,3,7\},$$
$$\{6,8,9,10,3\},\{7,9,10,0,4\},\{8,10,0,1,5\},$$
$$\{9,0,1,2,6\},\ \{5,7,8,9,2\}.$$

ماتریس وقوع طرح را به‌صورت زیر است:

$$\begin{bmatrix}1&0&0&1&0&0&0&1&1&1&0\\0&1&0&0&1&0&0&0&1&1&1\\1&0&1&0&0&1&0&0&0&1&1\\1&1&0&1&0&0&1&0&0&0&1\\1&1&1&0&1&0&0&1&0&0&0\\0&1&1&1&0&1&0&0&1&0&0\\0&0&1&1&1&0&1&0&0&1&0\\0&0&0&1&1&1&0&1&0&0&1\\1&0&0&0&1&1&1&0&1&0&0\\0&1&0&0&0&1&1&1&0&1&0\\0&0&1&0&0&0&1&1&1&0&1\end{bmatrix}$$

ماتریس وقوع را به‌عنوان ماتریس پایه $\mathbf{S}^1$ از یک طرح رمزنگاری بصری VCS-$(2,11)$ آستانه با گسترش پیکسل $m=11$ و ماتریس $\mathbf{S}^0$ نیز یک ماتریس 11×11 که همه سطرهای آن یکسان است و هر سطر آن پنج یک دارد.

در این صورت، $\alpha(m)=\frac{\omega(V1)-\omega(V^0)}{11}=\frac{8-5}{11}=\frac{3}{11}$. توجه کنید که بردار V^1 از ترکیب دو سطر از ماتریس $\mathbf{S}^1$ با عمل or به‌دست می‌آید. هر سطر از ماتریس $\mathbf{S}^1$ دارای چهار یک است و در هر دو سطر آن دو عدد یک در ستون یکسان قرار دارد. زیرا $\lambda=2$ (متوازن بودن طرح بلوکی) بنابراین: $w(V^1)=8$.

$$\begin{bmatrix}1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&0&0&0&0&0&0\end{bmatrix}$$

۳. روش پیشنهادی

در مباحث بررسی شده، VCS-$(2,n)$هایی که بر اساس طرح‌های بلوکی ساخته شده است مشاهده شد. اما لزوماً برای ساخت نبایستی همواره از طرح بلوکی استفاده کرد. در واقع ویژگی متوازن بودن طرح بلوکی نقش اصلی در ایجاد VCS-$(2,n)$ دارد. بر اساس برخی اشیاء ترکیبیاتی دیگر نیز می‌توان VCS-$(2,n)$های جدیدی به‌دست آورد. این اشیاء بایستی به‌نوعی دارای ویژگی متوازن بودن باشند. شیء ترکیبیاتی که ما در روش پیشنهادی جدید از آن استفاده می‌کنیم و ویژگی مذکور را دارد، ترید است.

تعریف ۷. یک μ-(v,k,t) ترید از حجم m شامل μ خانواده‌ی مجزا $\{T_1, T_2, \ldots, T_\mu\}$ می‌باشد. هر کدام از این خانواده‌ها از m بلوک تشکیل شده است، هر بلوک یک زیرمجموعه k عضوی از مجموعه v عضوی V است، به‌گونه‌ای که برای هر زیرمجموعه t عضوی از مجموعه v عضوی V، تعداد بلوک‌های شامل این زیرمجموعه t عضوی در هر T_i برای $1\le i\le\mu$ یکسان است [۹].

رشیدی و سلطان‌خواه در [۹] وجود تریدهای سه‌گانه را بررسی کردند و ثابت کردند برای حجم ۶ و حجم‌های بیشتر از ۸ ترید سه‌گانه وجود دارد. منظور از حجم ترید، تعداد بلوک‌های یک خانواده ترید است که در تعریف فوق با نماد m بیان شده است.

تعریف ۸. یک ترید را اشتاینری گوییم هرگاه هر زیرمجموعه t عضوی از مجموعه v عضوی V، حداکثر یک مرتبه در بلوک‌های هر دسته ظاهر شود [۹].

تعریف ۹. اگر هر عضو از مجموعه v عضوی V، در d بلوک از هر دسته ظاهر شود، ترید را d-همگن گویند [۱۰].

گلعلیزاده و سلطان‌خواه در [۱۰] وجود تریدهای چندگانه‌ی d-همگن را بررسی کردند و ثابت کردند برای هر $d \equiv 0$ به پیمانه ۳، ترید چندگانه‌ی d-همگن برای vهای به اندازه کافی بزرگ وجود دارد.

خواننده را جهت مطالعه بیشتر به [۱۱]، [۱۲] و [۱۳] ارجاع می‌دهیم.

نکته ۵. در مفهوم ترید، متوازن بودن خود را به این صورت نشان می‌دهد که هر زیرمجموعه t عضوی از مجموعه v عضوی V در تعداد یکسانی از بلوک‌های هر دسته ظاهر می‌شود.

اکنون در زیر روش ساخت سه $(2,n)$-VCS متفاوت با پارامترهای یکسان را شرح می‌دهیم. ترید اشتاینری و همگن جدول (۳) را در نظر بگیرید. مشابه ماتریس وقوع طرح بلوکی یک ماتریس وقوع برای T_1 می‌نویسم. ابتدای هر سطر یک عنصر از ترید را قرار می‌دهیم. منظور از عنصر در اینجا عددهای ۱ تا ۸ است که بلوک‌های سه‌تایی ترید از آن‌ها تشکیل شده است. ابتدای هر ستون نیز یک بلوک از دسته T_1 را قرار می‌دهیم.

جدول ۳. ترید اشتاینری و ۳- همگن

T_1	T_2	T_3
۱۲۳	۱۲۴	۱۲۷
۱۴۷	۱۳۸	۱۳۵
۱۵۸	۱۵۷	۱۴۸
۲۴۸	۲۳۷	۲۴۶
۲۶۷	۲۶۸	۲۳۸
۳۵۷	۴۶۷	۳۶۷
۳۶۸	۴۵۸	۴۵۷
۴۵۶	۳۵۶	۵۶۸

ماتریس وقوع مربوط به ترید (جدول ۳):

$$\begin{bmatrix} 1&1&1&0&0&0&0&0\\ 1&0&0&1&1&0&0&0\\ 1&0&0&0&0&1&1&0\\ 0&1&0&1&0&0&0&1\\ 0&0&1&0&0&1&0&1\\ 0&0&0&0&1&0&1&1\\ 0&1&0&0&1&1&0&0\\ 0&0&1&1&0&0&1&0 \end{bmatrix}$$

این ماتریس را به‌عنوان ماتریس پایه $\mathbf{S}^1$ از یک طرح رمزنگاری بصری $(2, 8)$-VCS آستانه با گسترش پیکسل $m=8$ و ماتریس $\mathbf{S}^0$ نیز یک ماتریس 8×8 که همه سطرهای آن یکسان است و هر سطر آن سه عدد یک دارد، مثل ماتریس زیر است.

$$\begin{bmatrix} 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0 \end{bmatrix}$$

در این صورت، دو مقدار برای $\omega(V1)$ داریم، زیرا در ترید اشتاینری هر دو عنصر حداکثر یک بار در بلوک‌های هر دسته ظاهر می‌شود یعنی اینکه، یا در یک بلوک ظاهر می‌شوند، یا اینکه در بلوکی ظاهر نمی‌شوند. اگر دو عنصر متناظر با دو سطر در یک بلوک ظاهر شوند، آنگاه $\omega(V1)=5$؛ زیرا در این حالت این دو سطر از ماتریس وقوع دو عدد ۱ در یک ستون مشترک دارند. اگر دو عنصر متناظر با دو سطر در یک بلوک ظاهر نشوند، آنگاه $\omega(V1)=6$؛ زیرا در این حالت این دو سطر از ماتریس وقوع در هیچ ستونی دو عدد ۱ مشترک ندارند. در هر دو حالت $\omega(V^0)=3$ است. اکنون اگر قرار دهید $\alpha(m)=\frac{1}{4}$ و $t_x=5$ برای هر مجموعه دو عضوی X، آنگاه شرایط ۱ و ۲ از تعریف طرح رمزنگاری برقرار است. برقراری شرط اول را در زیر می‌بینیم، توجه کنید که $m=8$.

$$\begin{cases} 3=\omega(V^0)\le t_x-\alpha(m).m=5-\frac{1}{4}\times 8=3 \\ 5=t_x\le\omega(V1) \end{cases} \qquad (۷)$$

برقراری شرط دوم نیز واضح است، زیرا هر سطر از ماتریس $\mathbf{S}^0$ و یا ماتریس $\mathbf{S}^1$ سه یک دارد. توجه کنید که در اینجا $\alpha(m)=\frac{1}{4}=\frac{2}{8}$ بسیار به مقدار کنتراست بهینه نزدیک است. مقدار کنتراست بهینه برای $m=8$ برابر است با:

$$\alpha(m)=\frac{\left\lceil\frac{n}{2}\right\rceil\left\lfloor\frac{n}{2}\right\rfloor}{n(n-1)}=\frac{\left\lceil\frac{8}{2}\right\rceil\left\lfloor\frac{8}{2}\right\rfloor}{8(8-1)}=\frac{4\times 4}{8\times 7}=\frac{2}{7}. \qquad (۸)$$

نکته ۶. اکنون با همین روش با دو دسته دیگر ترید یعنی T_2 و T_3 نیز می‌توان به همین صورت طرح رمزنگاری بصری ساخت. توجه کنید که این طرح‌ها متفاوت هستند اما پارامترهای یکسان دارند. بنابراین، می‌توان تعداد شرکت‌کنندگان در طرح را بدون نیاز به تغییر در پارامترهای طرح، سه برابر نمود.

۵. نتایج تجربی

در این بخش الگوریتمی برای تبدیل دو سهم از تصویر راز با استفاده از بردارهای سطر اول و دوم ماترس $\mathbf{S^0}$ و ماتریس $\mathbf{S^1}$ که در روش پیشنهادی ارائه شده است، آوردیم. این الگوریتم به‌صورت کد زبان پایتون ارائه شده است که برای بردارهای مربوط به سایر طرح‌های رمزنگاری بصری نیز قبلاً از آن استفاده شده است و در اینجا تغییرات کوچکی منطبق با سطرهای موردنظر در آن ایجاد شده است.

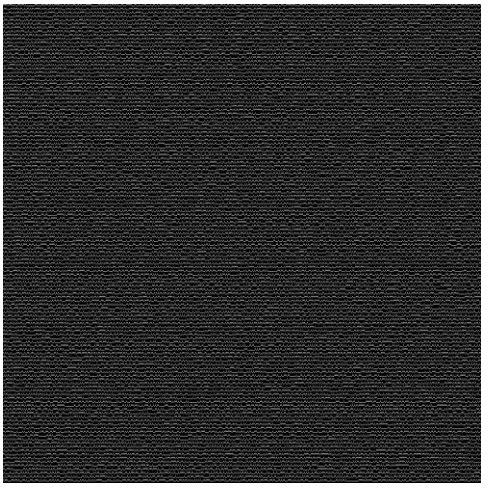
الگوریتم.

```
from PIL import Image

import random
import sys

image = Image.open('pic.png')
image = image.convert('1')

outfile1 = Image.new("1", [dimension * 2 for dimension in
image.size])

outfile2 = Image.new("1", [dimension * 2 for dimension in
image.size])


for x in range(0, image.size[0], 2):
for y in range(0, image.size[1], 2):
sourcepixel = image.getpixel((x, y))
assert sourcepixel in (0, 255)
coinflip = random.random()
if sourcepixel == 0:
if coinflip< .5:
outfile1.putpixel((x * 2, y * 2), 255)
outfile1.putpixel((x * 2 + 1, y * 2), 0)
outfile1.putpixel((x * 2, y * 2 + 1), 0)
outfile1.putpixel((x * 2 + 1, y * 2 + 1), 255)
outfile2.putpixel((x * 2, y * 2), 0)
outfile2.putpixel((x * 2 + 1, y * 2), 255)
outfile2.putpixel((x * 2, y * 2 + 1), 255)
outfile2.putpixel((x * 2 + 1, y * 2 + 1), 0)
else:
outfile1.putpixel((x * 2, y * 2), 0)
outfile1.putpixel((x * 2 + 1, y * 2), 255)
outfile1.putpixel((x * 2, y * 2 + 1), 255)
outfile1.putpixel((x * 2 + 1, y * 2 + 1), 0)


outfile2.putpixel((x * 2, y * 2), 255)
outfile2.putpixel((x * 2 + 1, y * 2), 0)
outfile2.putpixel((x * 2, y * 2 + 1), 0)
outfile2.putpixel((x * 2 + 1, y * 2 + 1), 255)
elifsourcepixel == 255:
if coinflip< .5:
outfile1.putpixel((x * 2, y * 2), 255)
outfile1.putpixel((x * 2 + 1, y * 2), 0)
outfile1.putpixel((x * 2, y * 2 + 1), 0)
outfile1.putpixel((x * 2 + 1, y * 2 + 1), 255)


outfile2.putpixel((x * 2, y * 2), 255)
outfile2.putpixel((x * 2 + 1, y * 2), 0)
outfile2.putpixel((x * 2, y * 2 + 1), 0)
outfile2.putpixel((x * 2 + 1, y * 2 + 1), 255)
else:
outfile1.putpixel((x * 2, y * 2), 0)
outfile1.putpixel((x * 2 + 1, y * 2), 255)
outfile1.putpixel((x * 2, y * 2 + 1), 255)
outfile1.putpixel((x * 2 + 1, y * 2 + 1), 0)


outfile2.putpixel((x * 2, y * 2), 0)
outfile2.putpixel((x * 2 + 1, y * 2), 255)
outfile2.putpixel((x * 2, y * 2 + 1), 255)
outfile2.putpixel((x * 2 + 1, y * 2 + 1), 0)

outfile1.save('out1.jpg')
outfile2.save('out2.jpg')
```

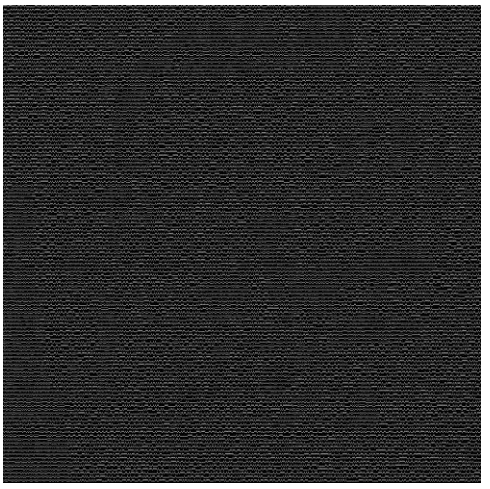
بعد از اجرای الگوریتم روی تصویری که با نام pic.png مشخص شده است دو تصویر غیر قابل تشخیص با نام‌های out1, out 2 ایجاد می‌شود، توجه کنید که قبل از اجرای الگوریتم با یک برنامه ساده به زبان متلب کنتراست تصویر را افزایش می‌دهیم.

از روی هم گذاشتن این تصاویر تصویر اولیه بازیابی می‌شود. این تصویر کیفیت تصویر قبل را ندارد اما کنتراست آن در حد مناسب کنتراست بهینه در رمزنگاری بصری است و تصویر بازیابی شده قابل شناسایی است. در شکل‌های (۴) الی (۲۴) سه تصویر، سهم‌های ساخته شده، هیستوگرام تصاویر، هیستوگرام سهم‌ها و تصویرهای بازیابی شده را مشاهده می‌کنیم.

شکل ۴. تصویر زلدا

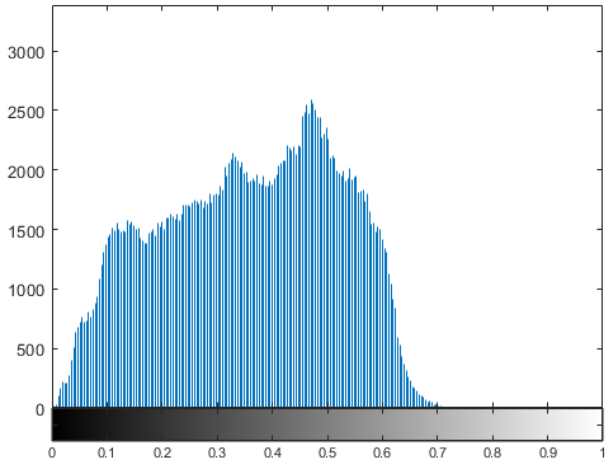


شکل ۵. سهم یک مربوط به تصویر زلدا

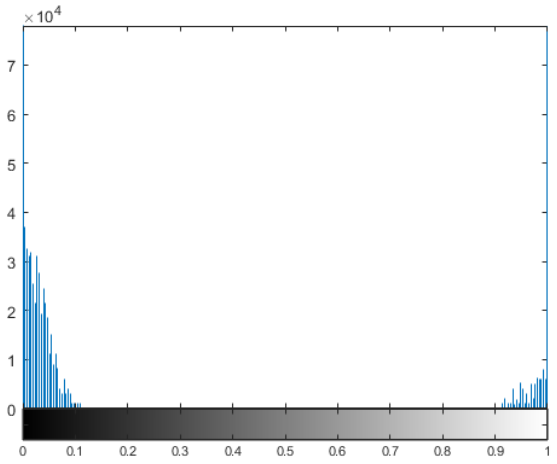


شکل ۶. سهم دو مربوط به تصویر زلدا

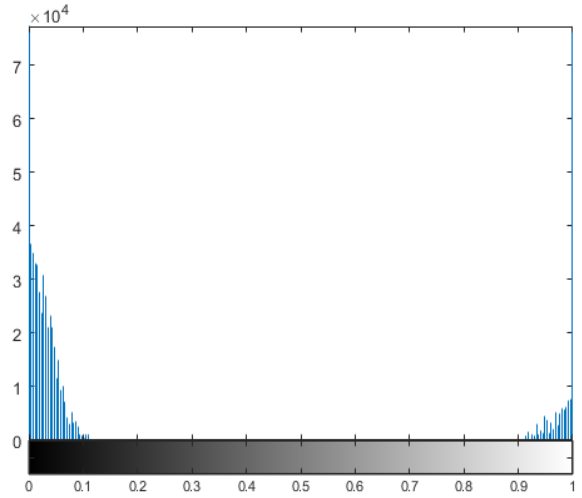
شکل ۷. تصویر بازیابی شده‌ی زلدا



شکل ۸. هیستوگرام تصویر زلدا

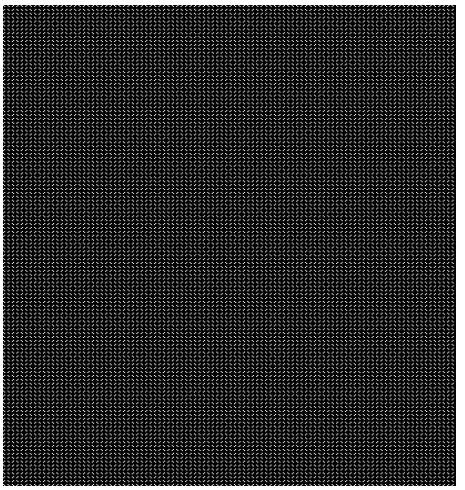


شکل ۹. هیستوگرام سهم یک

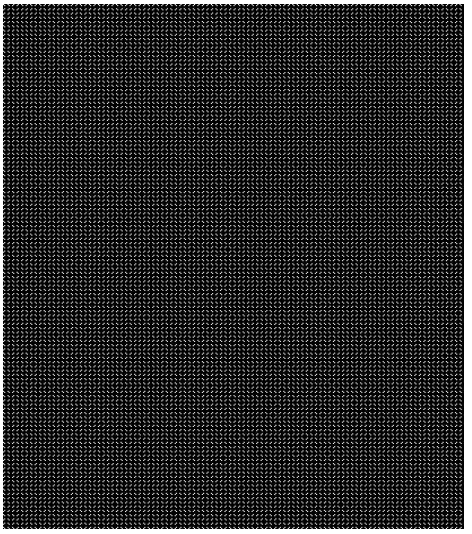


شکل ۱۰. هیستوگرام سهم دو

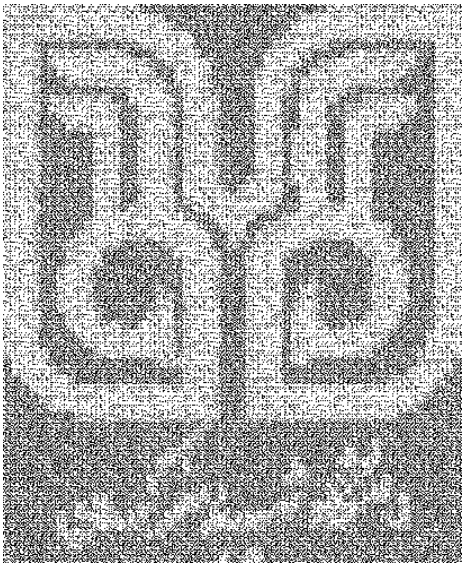
شکل ۱۱. تصویر نماد دانشگاه شهید باهنر کرمان



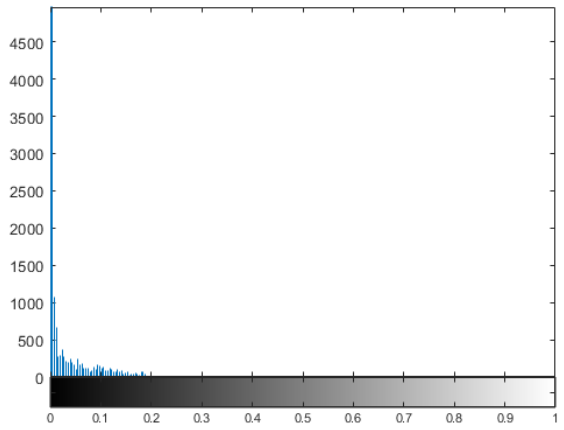
شکل ۱۲. سهم یک مربوط به تصویر نماد دانشگاه شهید باهنر کرمان



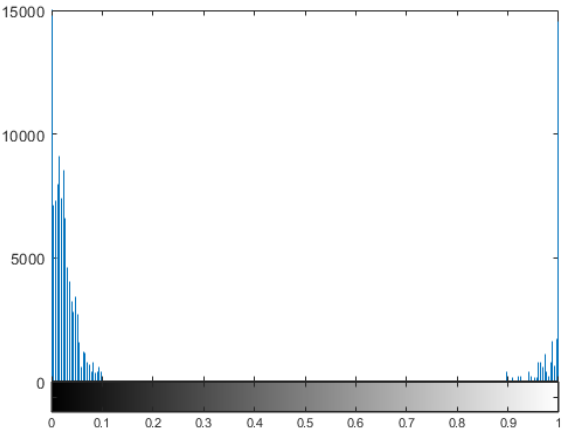
شکل ۱۳. سهم دو مربوط به تصویر نماد دانشگاه شهید باهنر کرمان



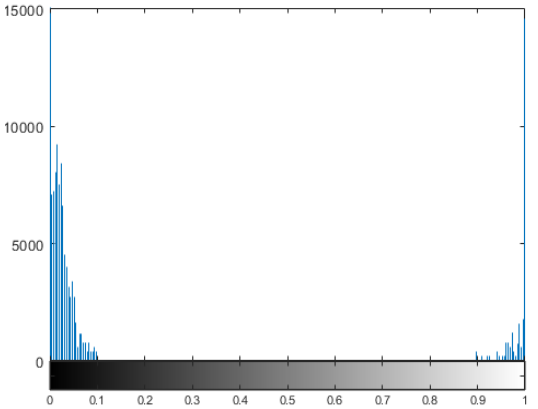
شکل ۱۴. تصویر بازیابی شده مربوط به نماد دانشگاه شهید باهنر کرمان



شکل ۱۵. هیستوگرام تصویر نماد دانشگاه شهید باهنر کرمان



شکل ۱۶. هیستوگرام سهم یک مربوط به تصویر نماد دانشگاه شهید باهنر کرمان



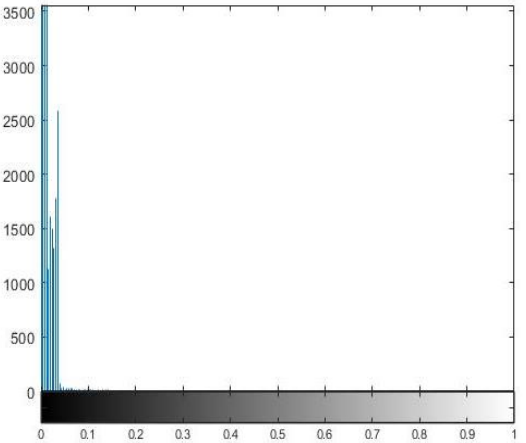
شکل ۱۷. هیستوگرام سهم دو مربوط به تصویر نماد دانشگاه شهید باهنر کرمان

شکل ۱۸. تصویر حرف S

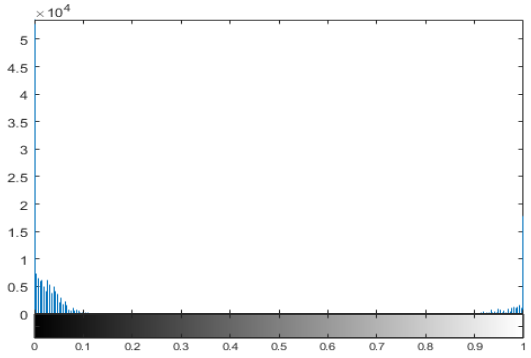
شکل ۱۹. سهم یک تصویر حرف S

شکل ۲۰. سهم دو تصویر حرف S

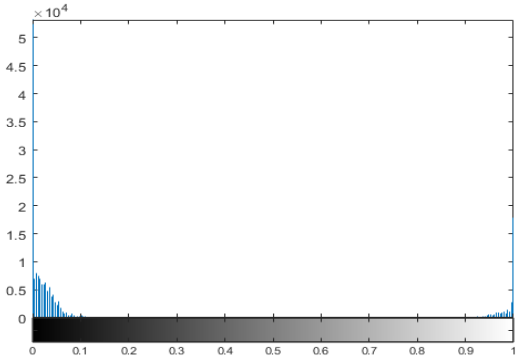
شکل ۲۱. تصویر بازیابی شده حرف S



شکل ۲۲. هیستوگرام تصویر حرف S



شکل ۲۳. هیستوگرام سهم یک تصویر حرف S



شکل ۲۴. هیستوگرام سهم دو تصویر حرف S

۶. نتیجه‌گیری

رمزگشایی در طرح‌های رمزنگاری بصری توسط حس بینایی انسان صورت می‌گیرد و نیاز به محاسبات پیچیده و زیاد ندارد [۱۶-۱۴]. این مزیت در طرح‌های رمزنگاری بصری دلیل پیشرفت این موضوع شده است. در ساختار طرح‌های رمزنگاری بصری به‌صورت گسترده از مفاهیم ریاضی به‌ویژه اشیای ترکیبیاتی استفاده می‌شود. در این مقاله روش جدیدی برای ساخت هم‌زمان چند سامانه رمزنگاری بصری بر پایه مفهوم تریدِ که نزدیک به مفهوم طرح بلوکی است، ارائه شده است. نکته مهم در رابطه با این ساختار این است که مقدار کنتراست در این طرح‌ها بسیار نزدیک به کنتراست بهینه است. علاوه بر طرح‌های بلوکی که اساس ساخت طرح‌های رمزنگاری بصری هستند، بر اساس مربع‌های لاتین نیز طرح‌های رمزنگاری بصری ساخته شده است. اما در این ساختارها توجهی به لاتین تریدها که مفهوم مشابه تریدِ در طرح بلوکی است، نشده است. بنابراین، به‌عنوان یک پیشنهاد جدید می‌توان در این ساختارها لاتین تریدها را جایگزین مربع‌های لاتین کرد و نتایج را بررسی نمود. لازم به ذکر است، در روش پیشنهادی ما قادر به ساخت دو طرح رمزنگاری بصری با پارامترهای یکسان هستیم، در صورتی که تعداد شرکت‌کنندگان در یک طرح سه برابر تعداد شرکت‌کنندگان طرح دیگر است و این موضوعی است که در ساختار سایر طرح‌های رمزنگاری بصری موجود دیده نمی‌شود و از طرفی مقدار کنتراست طرح رمزنگاری بصری جدید بسیار نزدیک به مقدار بهینه است.

۷. مرجع‌ها

[1] Noroozi, Z.; Mohamady, E. "Detection and Correction of Cheat in the Secret Sharing Schemes with Ternary Codes"; Adv. Defence Sci. & Technol. 2011, 1, 5-12.

[2] Naor, M.; Shamir, A. "Visual Cryptography"; Lect. Notes Comput. Sc. 1995, 950, 1–12.

[3] Hajiabolhassan, H.; Cheraghi, A. "Bounds for Visual Cryptography Schemes"; Discrete Appl. Math. 2010, 158, 659-665.

[4] Blundo, C.; De Santis, A.; Stinson, D. R. "On the Contrast in Visual Cryptography Schemes"; J. Cryptol. 1999, 12, 261-289.

[5] Verheul, E.; Tilborg, H. V. "Constructions and Properties of k out of n Visual Secret Sharing Schemes"; Design Code Cryptogr. 1997, 11, 179-196.

[6] Liu, F.; Wu, C. K.; Lin, X. "A New Definition of the Contrast of Visual Cryptography Scheme"; Inform. Process. Lett. 2010, 110, 241–246.

[7] Liu, F.; Yan W. Q. "Visual Cryptography for Image Processing and Security"; New York: Springer, 2014.

[8] Colbourn, C. J. "CRC Handbook of Combinatorial Designs"; Chapman and Hall/CRC, 2010.

[9] Rashidi, S.; Soltankhah, N. "On the Possible Volume of three Way Trades"; Electron. Notes Discret. Math. 2013, 43, 5-13.

[10] Golalizadeh, S.; Soltankhah, N. "On the Existence of d-Homogeneous μ-Way (v, 3, 2) Steiner Trades"; Graphs Combin. 2019, 35, 471-478.

[11] Cavenagh, N.; Donovan, D.; Drápal, A. "3-Homogeneous Latin Trades"; Discrete Math. 2005, 300, 57-70.

[12] Mahmoodian, E. S. "On the Existence of k-Homogeneous Latin Bitrades"; arXiv preprint arXiv:0810.2214. 2008.

[13] Cavenagh, NJ.; Wanless, IM. "Latin Trades in Groups Defined on Planar Triangulations"; J. Algebraic Comb. 2009, 30,323-47.

[14] Mirghaderi, A.; Jolfaei, A. "A Novel Chaotic Image Encryption Scheme Using Chaotic Maps"; Adv. Defence Sci. & Technol. 2011, 2, 111-124.

[15] Jia, X.; Wang, D.; Nie, D.; Zhang, C. "Collaborative Visual Cryptography Schemes"; IEEE Trans. Circuits and Systems for Video Technology, 2018, 28, 1056-1070.

[16] Fatahbeygi, A.; Tab, F. A. "A Highly Robust and Secure Image Water Marking Based on Classification and Visual Cryptography"; J. Inf. Secur. Appl. 2019, 45, 71-78.