رمزنگاری تصویر با استفاده از روش تسهیم راز تصویری آستانه‌ای (k,n) پیشنهادی

سعید آقازیارتی [*,۱]

۱- کارشناسی ارشد دانشگاه شهید باهنر کرمان، ایران

چکیده

در عملیات شناسایی هوایی، ایجاد کانال امن مخابراتی به منظور ارسال تصاویر تهیه شده توسط سامانه‌های الکترواپتیکی هواپایه به ایستگاه‌های زمینی امری ضروری است. در روش‌های تسهیم راز تصویری آستانه‌ای (k,n)، تصویر راز به n تصویر سهم به گونه‌ای تسهیم می‌شود که بازگشایی تصویر راز، تنها با در دسترس بودن حداقل k از n تصویر سهم (1<k<n) امکان‌پذیر است [۱]. مزیت اصلی روش تسهیم راز تصویری آستانه‌ای (k,n) در مقایسه با سایر روش‌های رمزنگاری تصویری، مقاوم بودن آن در برابر سرقت و تهدیدات جنگ الکترونیک است. در روش تسهیم راز تصویری آستانه-ای (k,n) در صورت از بین رفتن حداکثر n-k تصویر سهم، تصویر راز همچنان قابل بازیابی است [۲]. در این مقاله یک روش تسهیم راز تصویری آستانه‌ای (k,n) پیشنهاد شده است. روش پیشنهادی بر پایه جبر خطی بوده و در مقایسه با روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه، از پیچیدگی محاسباتی کمتری در بازیابی تصویر راز برخوردار است.

کلمات کلیدی: تصویر راز، تسهیم راز تصویری آستانه‌ای (k,n)، تصویر سهم، جنگ الکترونیک.

۱. مقدمه

در عملیات شناسایی هوایی، ارسال تصاویر هوایی از طریق یک کانال مخابراتی امن به ایستگاه‌های زمینی از اهمیت ویژه‌ای برخوردار است. از این‌رو بهره‌گیری از روش تسهیم راز تصویری آستانه‌ای (k,n) به عنوان یک راهکار پیشنهاد می-شود[۱]. ایده‌ی اصلی روش تسهیم راز تصویری آستانه‌ای، تسهیم تصویر راز به مجموعه‌ای از سهم‌ها به گونه‌ای است که تصویر راز فقط با در اختیار داشتن تعداد معینی از سهم‌ها، قابل بازیابی است [۲]. در روش تسهیم راز تصویری آستانه‌ای (k,n)، تصویر راز تنها در صورت از بین رفتن بیش از n-k تصویر سهم قابل بازیابی نیست. از این‌رو روش تسهیم راز تصویری آستانه‌ای در مقایسه با سایر روش‌های رمزنگاری تصویری در برابر سرقت و تهدیدات جنگ الکترونیک مقاوم‌تر است [۳].

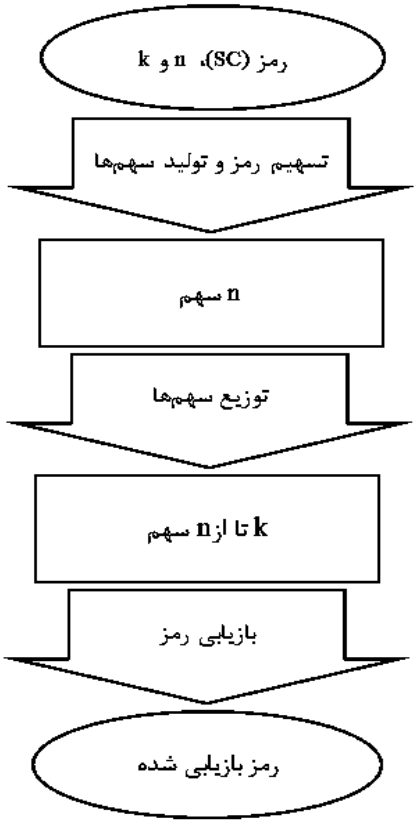
ادامه‌ی این مقاله بدین صورت سازماندهی می‌شود: در بخش بعد به بیان اجمالی از پیشینه‌ی تحقیق پرداخته می-شود. بخش سوم به تشریح مبانی روش تسهیم راز تصویری آستانه‌ای (k,n) پیشنهادی اختصاص یافته است. به منظور بررسی کارایی روش پیشنهادی، نتایج شبیه‌سازی در بخش چهارم ارائه می‌شود و در بخش پنجم مقاله جمع‌بندی می‌شود.

* **Corresponding author:**
Email: saeidziarati22@chmail.ir

۲. پیشینه تحقیق

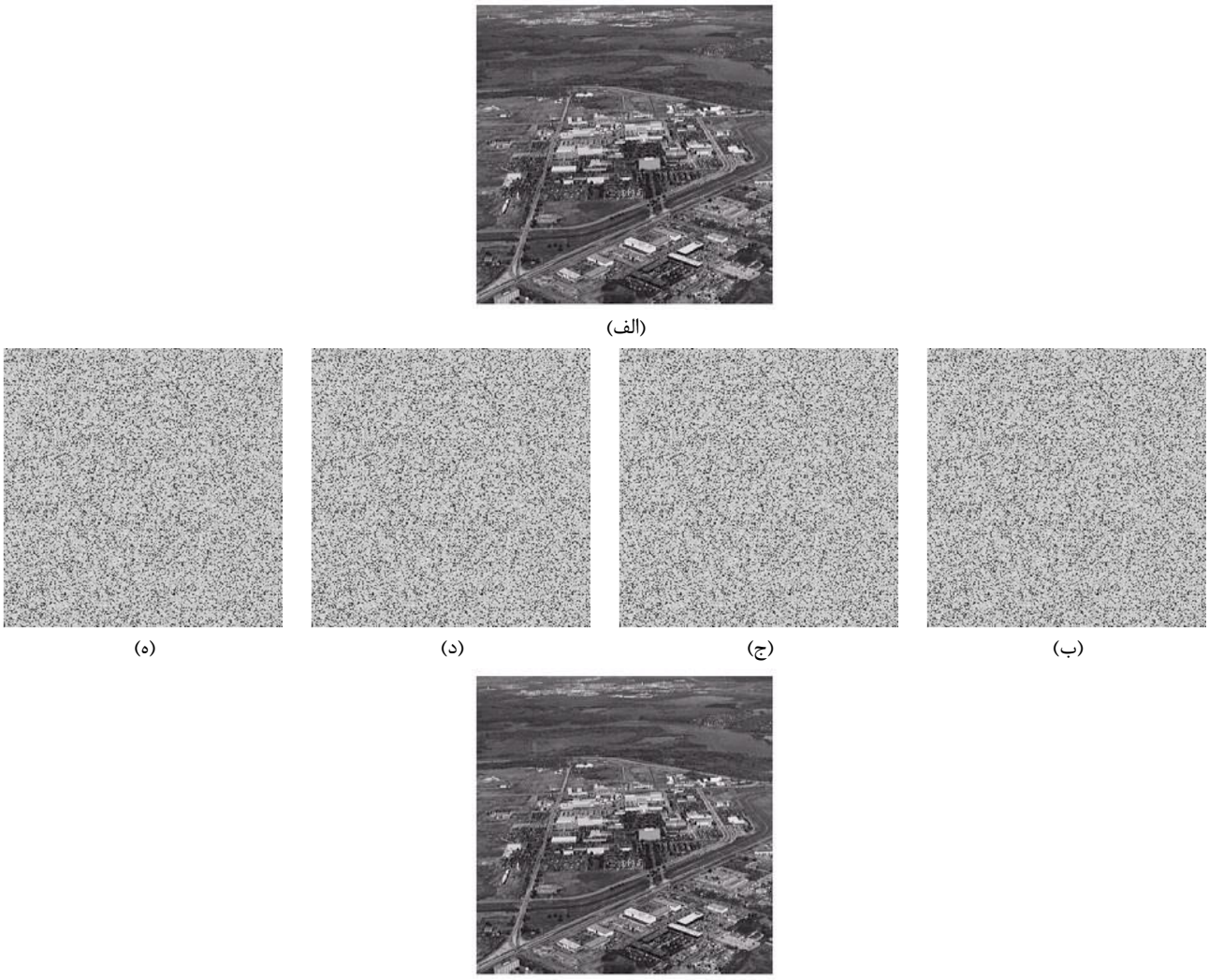
ایده تسهیم راز عددی برای اولین بار توسط بلکلی [۴] و شامیر [۵] به طور مستقل ارائه گردید. روش بلکلی بر اساس اشتراک صفحه‌های هندسی و روش شامیر حالت خاصی از روش بلکلی و بر اساس درون‌یابی لاگرانژ طراحی شده است. ایده اصلی روش تسهیم راز عددی آستانه‌ای (k,n)، شکستن یک راز عددی (SC) به گروهی از سهم‌های عددی (SH) به گونه‌ای است که زیرگروه‌های مجاز از سهم‌ها بتوانند راز را بازیابی کنند و زیرگروه‌های غیرمجاز قادر به بازیابی هیچ گونه اطلاعات در مورد راز نباشند [۶]. شکل ۱ ساختار کلی روش تسهیم راز عددی آستانه‌ای (k,n) را نشان می‌دهد. روش تسهیم راز عددی از سه مرحله تشکیل شده است:

- فرآیند تولید سهم‌ها.
- فرآیند توزیع سهم‌ها.
- فرآیند بازیابی راز [۷].



شکل ۱- ساختار کلی روش تسهیم راز عددی آستانه‌ای (k,n) [۷].

به منظور رمزنگاری تصویر راز با استفاده از روش تسهیم راز عددی، مقدار هر پیکسل از تصویر راز به طور جداگانه به عنوان یک راز عددی در نظر گرفته می‌شود. پس از تسهیم پیکسل‌های تصویر راز، پیکسل‌های سهم تولید شده از تسهیم هر پیکسل تصویر راز، در موقعیت متناظر با موقعیت همان پیکسل در تصویر راز در تصاویر سهم قرار می‌گیرند تا تصاویر سهم تولید شوند. در شکل ۲ نمونه‌ای از تصاویر سهم حاصل از روش تسهیم راز تصویری نوعی به ازای n=4 و k=3 نمایش داده شده است. همانطور که می‌بینید، شکل ۲-الف تصویر راز، شکل‌های ۲-ب، ۲-ج، ۲-د و ۲-ه تصاویر سهم و شکل ۲-و تصویر راز بازیابی شده با استفاده از سه تصویر سهم را نشان می‌دهد.



(الف)

(ب) (ج) (د) (ه)

(و)

شکل ۲- (الف) تصویر راز، (ب، ج، د، ه) تصاویر سهم و (و) تصویر راز بازیابی شده.

روش‌های تسهیم راز تصویری آستانه‌ای (k,n) بر اساس معیارهای حساسیت نسبت به خطا، نرخ اطلاعات، پیچیدگی محاسبات و نیاز به کلید جایگشت ارزیابی می‌شود. در ادامه هر یک از این معیارها تشریح می‌شوند [۸].

- **حساسیت نسبت به خطا**

نسبت تعداد پیکسل خطادار در تصویر راز بازیابی شده به تعداد پیکسل خطادار در تصاویر سهم شرکت‌کننده در بازیابی تصویر راز، حساسیت نسبت به خطا تعریف می‌شود [۹].

- **نرخ اطلاعات**

نسبت اندازه‌ی تصویر راز به اندازه‌ی تصویر سهم را نرخ اطلاعات می‌نامند. نرخ اطلاعات به کمک رابطه‌ی (۱) محاسبه می‌شود [۱۰].

$$\text{نرخ اطلاعات} = \frac{\text{اندازه تصویر راز}}{\text{اندازه تصویر سهم}} \quad (۱)$$

- **پیچیدگی محاسباتی در بازیابی تصویر راز**

این معیار براساس تعداد عملیات محاسباتی صورت گرفته در بازیابی یک پیکسل از تصویر راز بررسی می‌شود. بدیهی است که هر چه میزان پیچیدگی محاسباتی در بازیابی تصویر راز کمتر باشد، آن روش کارایی بهتری دارد [۱۱].

- **نیاز به کلید جایگشت**

در برخی از روش‌های تسهیم راز تصویری به منظور جلوگیری از ظاهر شدن اطلاعات تصویر راز در تصاویر سهم، ابتدا تصویر راز توسط یک کلید جایگشت داده شده، سپس رمزنگاری می‌شود. این امر منجر به ارسال اطلاعات اضافی مربوط به کلید جایگشت از طریق یک کانال مخابراتی امن و مجزا می‌گردد [۱۲].

- **بازیابی بی‌اتلاف تصویر راز**

به منظور اندازه‌گیری میزان اتلاف در بازیابی تصویر راز در روش‌های تسهیم راز تصویری، از معیار PSNR استفاده می‌شود. این معیار برای اندازه‌گیری میزان تشابه بین تصویر راز اصلی و تصویر راز بازیابی شده به کار می‌رود [۱۱]. اگر تصویر راز بازیابی شده را با X و تصویر راز اصلی را با Y نشان دهیم، با شرط اینکه اندازه هر دوی آن‌ها $m\times n$ پیکسل باشد، PSNR به کمک روابط (۳) و (۴) محاسبه می‌شود.

$$MSE = \frac{1}{m\times n}\sum_{i=1}^{m}\ \sum_{j=1}^{n}(X_{ij} - Y_{ij})^2 \quad (۳)$$

$$PSNR = 10\log_{10}\frac{(255)^2}{MSE}\ d\beta \quad (۴)$$

۳. روش تسهیم راز تصویری آستانه‌ای (k,n) پیشنهادی

در این بخش با ارائه‌ی یک روش تسهیم راز تصویری آستانه‌ای (k,n)، بخشی از ضعف‌های موجود در روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه مرتفع می‌شود. در این روش قصد داریم تصویر راز با ابعاد $m_1\times m_2$ پیکسل را به n تصویر سهم با همان ابعاد تسهیم کنیم. تصویر راز را به صورت ماتریس A در نظر بگیرید.

$$A=\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m_2} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m_2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m_1,1} & a_{m_1,2} & \cdots & a_{m_1,m_2} \end{bmatrix} \quad (۵)$$

به ازای هر پیکسل راز $a_{i,j}$، n سهم پیکسلی $S_{1,ij}$ ، $S_{2,ij}$ ، ... ، $S_{n,ij}$ تولید می‌شود که $S_{q,ij}$ زیرپیکسل سهم q-ام از پیکسل راز $a_{i,j}$ است. پس از آن که پیکسل‌های تصویر راز تسهیم شدند، به ازای هر q $(1 \le q \le n)$، زیرپیکسل‌های سهم q-ام از پیکسل‌های مختلف تصویر راز در کنار هم قرار گرفته تا ماتریس متناظر با تصویر سهم q-ام بدست آید. رابطه‌ی (۶) ماتریس متناظر با تصویر سهم q-ام را نشان می‌دهد.

$$S_q = \begin{bmatrix} s_{q,11} & s_{q,12} & \cdots & s_{q,1m_2} \\ s_{q,21} & s_{q,22} & \cdots & s_{q,2m_2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{q,m_1 1} & s_{q,m_1 2} & \cdots & s_{q,m_1 m_2} \end{bmatrix} \quad (۶)$$

۴-۱. فرآیند رمزنگاری تصویر راز

در فرآیند رمزنگاری، با استفاده از a_{ij} (مقدار پیکسل (i,j) در ماتریس تصویر راز)، به چگونگی تولید سهم‌های $s_{1,ij}$, $s_{2,ij}$, … , $s_{n,ij}$ پرداخته می‌شود، به نحوی‌که با در اختیار داشتن هر k از n زیرپیکسل سهم، a_{ij} قابل بازیابی باشد، در حالی‌که اطلاعات هر $k-1$ سهم یا کمتر، حاوی هیچ‌گونه اطلاعاتی از a_{ij} نباشد. از این پس برای سادگی، a_{ij} با a و n زیرپیکسل سهم حاصل از تسهیم پیکسل راز a_{ij} با s_1 , s_2 , … , s_n نشان داده می‌شود. منظور از راز، پیکسلی از تصویر راز در یک جایگاه خاص از تصویر راز و منظور از سهم q-ام، زیرپیکسل سهم q-ام در همان جایگاه است. فرآیند تسهیم هر پیکسل راز و تولید پیکسل‌های سهم طبق مراحل زیر انجام می‌شود:

- به ازای هر i $(1 \le i \le k-1)$، سهم‌های s_i به طور تصادفی از $GF(2^8)$ تولید می‌شود.
- ماتریس $(n-k+1)\times k$ با درایه‌های تصادفی غیرصفر از مجموعه‌ی اعداد حقیقی به صورت رابطه (۷) تولید می‌شود. ماتریس مذکور می‌تواند برای عموم آشکار باشد.

$$C = \begin{bmatrix} b_{k,1} & b_{k,2} & \cdots & b_{k,k-1} & 1 \\ b_{k+1,1} & b_{k+1,2} & \cdots & b_{k+1,k-1} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,k-1} & 1 \end{bmatrix} \quad (۷)$$

به ازای هر i $(k \le i \le n)$، سهم‌های s_i از رابطه‌ی (۸) به دست می‌آید.

$$EQU_i : s_i = (a - (b_{i,1}s_1 + b_{i,2}s_2 + \cdots + b_{i,k-1}s_{k-1})) \bmod 2^8 \quad (۸)$$

۴-۲. فرآیند بازیابی تصویر راز

بازیابی هریک از پیکسل‌های تصویر راز با استفاده از پیکسل‌های متناظر حداقل k از n تصویر سهم، به صورت زیر انجام می‌شود.

فرض کنید $P_{j1}, P_{j2}, \ldots, P_{jm}$ تصویر سهم از مجموعه تصاویر سهم $\{P_k, P_{k+1}, \ldots, P_n\}$ است که در بازیابی تصویر راز استفاده می‌شوند و $P_{jm+1}, P_{jm+2}, \ldots, P_{jk}$ تصویر سهم از مجموعه تصاویر سهم $\{P_1, P_2, \ldots, P_{k-1}\}$ است که در بازیابی تصویر راز استفاده می‌شوند و $m-1$ تصویر سهم از مجموعه تصاویر سهم $\{P_1, P_2, \ldots, P_{k-1}\}$ که در بازیابی تصویر راز استفاده نمی‌شوند، $P_{l1}, P_{l2}, \ldots, P_{lm-1}$ است.

به ازای هر i $(1 \le i \le m)$، دو طرف رابطه EQU_{ji} در ضریب α_{ji} ضرب شده و طرفین m معادله با هم جمع می‌شود. یک ترکیب خطی از معادلات $EQU_{j1}, EQU_{j2}, \ldots, EQU_{jm}$ به صورت رابطه (۹) حاصل می‌شود.

$$\sum_{i=1}^{m} \alpha_{j_i} EQU'_{j_i} : \sum_{i=1}^{m} \beta_{j_i} s_{j_i} + \sum_{i=m+1}^{k} \beta_{j_i} s_{j_i} + \sum_{i=1}^{m-1} \beta_{l_i} s_{l_i} \equiv a'a \pmod{2^8} \quad (۹)$$

به طوری‌که در معادلات (۱۰)، (۱۱)، (۱۲) و (۱۳) داریم.

$$a' = \sum_{i=1}^{m} \alpha_{j_i} \quad (۱۰)$$

$$\beta_{j_t} = \alpha_{j_t} \quad 1 \le t \le m \quad (۱۱)$$

$$\beta_{j_t} = \sum_{i=1}^{m} \alpha_{j_i} b_{j_I, j_t} \quad m+1 \le t \le k \quad (۱۲)$$

$$\beta_{l_t} = \sum_{i=1}^{m} \alpha_{j_i} b_{j_i, l_t} \quad 1 \le t \le m-1 \quad (۱۳)$$

ضرایب α_{j_i} $(1 \le i \le m-1)$ باید به گونه‌ای به دست آید که a' برابر یک و تمام β_{l_t}-ها به ازای $1 \le t \le$ m-1، برابر صفر شوند. دستگاه m-1 معادله، m مجهول رابطه‌ی (۱۴) به دست می‌آید.

$$\begin{cases} b_{j_1,l_1}\alpha_{j_1} + b_{j_2,l_1}\alpha_{j_2} + \cdots + b_{j_m,l_1}\alpha_{j_m} = 0 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ b_{j_1,l_{m-1}}\alpha_{j_1} + b_{j_2,l_{m-1}}\alpha_{j_2} + \cdots + b_{j_m,l_{m-1}}\alpha_{j_m} = 0 \end{cases} \quad (۱۴)$$

معادلات دستگاه فوق مستقل خطی هستند، در غیر این‌صورت ضرایب آن یک ماتریس m-تایی با دترمینان صفر ایجاد می‌کند. اگر معادله‌ی (۱۵) را به دستگاه فوق اضافه کنیم، یک دستگاه m معادله، m مجهول به دست می‌آید که مستقل خطی است و دستگاه توسعه یافته، جواب منحصر به فرد دارد.

$$a' : \quad \alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_m} = 1 \quad (۱۵)$$

از α_{j_i}-ها مقادیر β_{j_t}-ها $(1 \le t \le k)$، بدست می‌آیند و پیکسل راز به کمک رابطه‌ی (۱۶) بازیابی می‌شود.

$$a = \sum_{i=1}^{k} \beta_{j_i} s_{j_i} \pmod{2^8} \quad (۱۶)$$

۵. نتایج شبیه‌سازی

به‌منظور بررسی کارایی روش پیشنهادی، آن به همراه روش‌های تسهیم راز تصویری آستانه‌ای Lin [۱۳]، Yang [۱۴] و Chang [۱۵] در محیط MATLAB پیاده‌سازی شده‌اند. برای ارزیابی کارایی روش تسهیم راز تصویری آستانه‌ای (k,n) پیشنهادی، معیارهای حساسیت نسبت به خطا، نیاز به کلید جایگشت، نرخ اطلاعات و پیچیدگی محاسباتی در روش پیشنهادی با روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه مقایسه می‌شود. شکل ۲ نتایج اعمال روش‌های تسهیم راز تصویری آستانه‌ای Lin ، Yang، Chang و روش پیشنهادی بر روی تصویر راز را نشان می‌دهد. همان‌گونه که در شکل ۲ می‌بینید، روش پیشنهادی در مقایسه با روش Chang دارای حساسیت کمتری نسبت به بروز خطا در تصاویر

سهم بوده و این معیار در روش پیشنهادی با روش‌های Lin و Yang یکسان است.

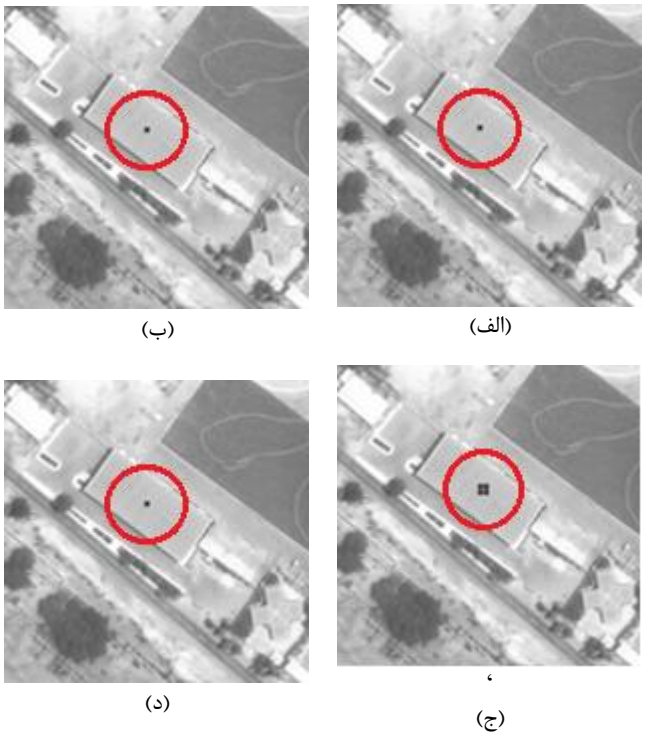
جداول ۱، ۲ ، ۳ و ۴ به ترتیب معیارهای ارزیابی نیاز به کلید جایگشت، نرخ اطلاعات، میزان شباهت تصویر راز اصلی و تصویر راز بازیابی شده و میزان پیچیدگی محاسباتی در روش‌های Lin، Yang، Chang و روش پیشنهادی را نشان می‌دهد. همان‌گونه که در جداول نمایان است، روش پیشنهادی در مقایسه با روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه از کارایی مطلوبی برخوردار است.

جدول ۱- بررسی نیاز به کلید جایگشت

روش‌ها	Lin	Yang	Chang	پیشنهادی
نیاز به کلید جایگشت	دارد	دارد	ندارد	ندارد

جدول ۲- بررسی نرخ اطلاعات

روش‌ها	Lin	Yang	Chang	پیشنهادی
نرخ اطلاعات	>۱	۱	<۱	۱



(الف) (ب) (ج) (د)

شکل ۲- تصاویر راز بازیابی شده در اثر بروز خطا در یک پیکسل از تصاویر سهم مورد استفاده در بازیابی تصویر راز در روش: (الف) Lin. (ب) Yang. (ج) Chang. (د) پیشنهادی.

جدول ۳- میزان شباهت تصویر راز اصلی و تصویر راز بازیابی شده

روش‌ها	Lin	Yang	Chang	پیشنهادی
میزان شباهت بین تصویر راز و بازیابی شده	Inf	Inf	Inf	Inf

جدول ۴- میزان پیچیدگی محاسباتی فرآیند بازیابی تصویر راز

روش‌ها	Lin	Yang	Chang	پیشنهادی
میزان پیچیدگی محاسباتی	$\frac{k^3}{3}$	$\frac{k^3}{3}$	$\frac{k^3}{3}$	$\frac{(m)^3}{3}$

نظر به اینکه $1 \leq m \leq k$ است، میزان پیچیدگی محاسباتی فرآیند بازیابی تصویر راز در روش پیشنهادی در مقایسه با روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه کاهش یافته است.

۶. نتیجه‌گیری

ارسال امن تصاویر هوایی به ایستگاه‌های زمینی در عملیات شناسایی هوایی امری ضروری است. نظر به اینکه روش‌های تسهیم راز تصویری آستانه‌ای (k,n) از مقاومت و امنیت بالایی در انتقال تصویر راز برخوردارند، بیش از سایر روش‌های رمزنگاری مورد توجه قرار گرفته‌اند. در این مقاله مبانی روش‌های تسهیم راز تصویری آستانه‌ای (k,n) تشریح و معیارهای ارزیابی آن‌ها به طور اجمالی معرفی گردید. در ادامه، یک روش تسهیم راز تصویری آستانه‌ای (k,n) به منظور رمزنگاری تصویر پیشنهاد گردید. روش پیشنهادی برخی از ضعف‌های موجود در روش‌های تسهیم راز تصویری تسهیم راز تصویری آستانه‌ای (k,n) پایه ازجمله نیاز به کلید جایگشت و پیچیدگی محاسباتی را با حفظ سایر معیارهای ارزیابی بهبود بخشید. نتایج کمی وکیفی حاصل از شبیه‌سازی نشان‌گر کارایی روش پیشنهادی در مقایسه با روش‌های تسهیم راز تصویری آستانه‌ای (k,n) پایه است.

۷. مراجع

[1] K. Shankar, D. Taniar, E. Yang and O. Yi. "Secure and Optimal Secret Sharing Scheme for Color Images," *Mathematics*, 9, 2360, 2021.
[2] L.Yu, L. Liu, Z. Xia, X. Yan and Y. Lu. "Lossless and Efficient Secret Image Sharing Based on Matrix Theory Modulo 256," *Mathematics*, 8, 1018, 2020.
[3] K. Bisht and M. Deshmukh. "A novel approach for multilevel multi-secret image sharing scheme," *Supercomput*,77, 12157–12191, 2021.
[4] G. R. Blakley, "Safeguarding cryptographic keys," *AFIPS Conference Proceedings*, vol. 48, pp. 313-317, 1979.
[5] A. Shamir, "How to share a secret," *Commun of the ACM*, vol. 22, pp. 612-613, 1979.
[6] T.H. Chen and K.H. Tsao, "Threshold secret image sharing by random grids," *Journal of Systems and Software*, vol. 84, pp. 1197-1208, 2011.
[7] M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Proceedings of the IEEE Global Telecommunications Conference*, pp. 99-102, 2007.
[8] W. Jackson, K. Martin, and C. M. Keefe, "Ideal Secret Sharing Schemes with Multiple Secrets," *Journal of Cryptology*, vol. 9, pp. 233-250, 1996.
[9] H. Koga and E. Ueda, "Basic properties of the threshold secret sharing scheme with perfect reconstruction," *Codes Crypt*, vol. 40, pp. 81–102, 2011.
[10] R. Capocelli, A. Santis, L. Gargano and U. Vaccaro, "On the Size of Shares for Secret Sharing Schemes," *Journal of Cryptology*, vol. 6, pp. 157-167, 1993.
[11] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable image secret sharing schemes," *Information Sciences*, vol. 178, pp. 2262-2274, 2008.
[12] C. Padro and and G. Saez, "Lower bounds on the information rate of secret sharing schemes with homogeneous access structure," *Information Processing Letters*, vol. 83 (6), pp. 345-351, 2006.
[13] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, pp. 405-414, 2004.
[14] C. N. Yang, T. S. Chen, K. H. Yu and C. C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems & Software*, vol. 80, pp. 1070-1076, 2007.
[15] C. C. Chang, Y. P. Hsieh and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41 (1), pp. 3130-3137, 2010.