

نهان نگاری در متمم تصویر فشرده شده با استفاده از تجزیه مقدار تکین

رضا اصفهانی^۱، زین العابدین نوروزی^۲

تاریخ دریافت: ۹۲/۰۶/۱۸

تاریخ پذیرش: ۹۲/۱۰/۱۶

چکیده

در سیستم‌های اختفاء اطلاعات، سه عنصر اصلی ظرفیت، امنیت و مقاومت دخیل هستند. امنیت و ظرفیت جاسازی، اهمیت ویژه‌ای در نهان نگاری داشته و روش‌های نهان نگاری بر کاهش تغییرات حاصل از جاسازی تأکید دارند. اما یکی از موارد بسیار مهم در پدافند غیرعامل، استفاده مناسب از فضای حافظه موجود، برای نهان نگاری در زمان‌های بحرانی است. این مقاله به دنبال روشی پویا است که بتواند نهان نگاری در تصویر را با در نظر گرفتن حداقل‌ها در خواص تصویر برای حالت‌های بحرانی انجام دهد. حجم حافظه مصرفی و تشابه تصویر، دو مؤلفه‌ای هستند که در این مقاله به آنها پرداخته شده است. در این مقاله ابتدا با روش تجزیه مقدار تکین، یک تصویر فشرده شده از تصویر اصلی به دست آمده و سپس نهان نگاری انجام می‌شود. در این روش، نهان نگاری در متمم تصویر فشرده شده صورت می‌گیرد و سپس با خود تصویر فشرده شده، جمع می‌شود و تصویر نهایی به دست می‌آید که مشابه تصویر اصلی است و این مقدار تشابه، بستگی به مقدار پارامتری خاص به نام k (مقدار ویژه ماتریس) در محاسبات دارد. هرچه مقدار k کمتر باشد، تشابه کمتری با تصویر اصلی وجود دارد ولی فضای حافظه بیشتری برای نهان نگاری در دسترس خواهد بود.

کلیدواژه‌ها: مقادیر ویژه^۳، بردار ویژه^۴، نهان نگاری^۵، نهان کاوی^۶، هیستوگرام، تجزیه مقدار تکین (SVD)^۷، فشرده سازی تصویر

۱- پژوهشگر دانشگاه جامع امام حسین(ع) resfahani@ihu.ac.ir - نویسنده مسئول

۲- استادیار و عضو هیئت علمی دانشگاه جامع امام حسین(ع)

3- Eigenvalues
4- Eigenvectors
5- Steganography
6- Steganalysis
7- Singular Value Decomposition

۱- مقدمه

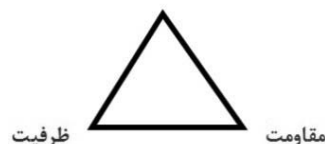
«نهان‌نگاری» دانشی است برای پنهان کردن داده یا فایلی در فایل دیگر؛ به طوری که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند. با توجه به شکل (۱)، پارامترهای مخفی کردن اطلاعات عبارتند از:

۱. ادراک ناپذیری - امنیت: ادراک پذیری یعنی جاگذاری اطلاعات به نحوی باشد که اعوجاج ناشی از آن، روی محیط پوشانه از یک حد معین فراتر رفته و اثر آن از نظر بینایی و ادراکی قابل رؤیت و محسوس گردد. در حالت کلی‌تر، امنیت نشان‌دهنده میزان محسوس بودن بصری و آماری اثر اعوجاج ناشی از جاگذاری است. به عبارت دیگر، امنیت، میزان مقاومت سیستم نهان‌نگاری در برابر حملات نهان‌کاوی (به خصوص حملات آماری) برای کشف وجود نهان‌نگاره است. منظور از حملات آماری، نوعی نهان‌کاوی است که آمارگان تصویر مانند هیستوگرام‌ها را برای وجود نهان‌نگاره بررسی می‌کند.

۲. ظرفیت: عبارت است از مقدار اطلاعاتی که با در نظر گرفتن معیار ادراک‌پذیری می‌توان در یک محیط پوشانه پنهان کرد. به عبارت دیگر، حداکثر تعداد بیت‌هایی که می‌توان در یک محیط پوشانه معین جاگذاری کرد به طوری که احتمال کشف پیغام توسط نهان‌کاو بسیار کم باشد.

۳. مقاومت: میزان پایداری اطلاعات مخفی شده در برابر حملات اعمالی به محیط پوشانه جهت تخریب، حذف و یا تغییر آن، به عبارت دیگر، توانایی پایداری نهان‌نگاره در برابر اعوجاج ناشی از پردازش اطلاعات، غیر عمدی یا خصمانه است.

ادراک ناپذیری - امنیت



شکل ۱- مصالحه بین پارامترهای مخفی کردن اطلاعات

یکی از مسائلی که در زمان بحران ممکن است با آن مواجه شد، عدم دسترسی به فضای حافظه زیاد و کافی است. از آنجا که اشغال کم‌تر فضای حافظه به همراه حفظ تشابه حداقلی تصویر نهایی از مباحث مهم پدافند غیرعامل در زمان‌های بحران است، پرداختن به مؤلفه ظرفیت و حجم حافظه مصرفی به همراه مسئله تشابه تصویر نهایی حاوی اطلاعات نهان‌نگاری شده با تصویر اصلی بسیار با اهمیت خواهد بود.

مطالب مقاله با عناوین بخش‌های زیر مطرح شده است:

- بخش ۲) مقادیر ویژه و تجزیه مقدار تکین (SVD)
- بخش ۳) فشرده‌سازی تصویر با استفاده از SVD
- بخش ۴) نهان‌نگاری در متمم تصویر فشرده‌شده
- بخش ۵) نهان‌کاوی به روش هیستوگرام
- بخش ۶) نتیجه‌گیری

۲- مقادیر ویژه و تجزیه مقدار تکین (SVD)

در این‌جا به نوعی از مبحث مقادیر ویژه و تجزیه مقدار تکین (SVD) استفاده شده است. محاسبه مقادیر ویژه در ماتریس‌ها بحث می‌شود و برای محاسبه معمولاً روی قطر اصلی از ضربی کسر می‌شوند و از طریق دترمینان گرفتن ماتریس، مقدار ضرب محاسبه می‌شود. بردار ویژه و مقدار ویژه ماتریس A طبق رابطه $A \times v = k \times v$ به دست می‌آیند که A ماتریسی $n \times n$ ، بردار ویژه v ماتریسی $n \times 1$ و k مقدار ویژه ماتریس A است. k ریشه معادله $|A - kI| = 0$ یعنی $\det|A - kI| = 0$ می‌باشد که I ماتریس واحد است.

تجزیه مقدار تکین (SVD) به عبارتی همان تعاریف مقادیر ویژه و بردار ویژه را دارا بوده و کاربردهای فراوانی دارد. یکی از کاربردهای آن فشرده‌سازی تصویر است که در این مقاله به آن اشاره شده و با یک روش پیشنهادی، از این مبحث جهت نهان‌نگاری بهره‌برداری شده است. در واقع نهان‌نگاری در متمم تصویر فشرده‌شده صورت می‌گیرد و سپس با خود تصویر فشرده‌شده، جمع می‌شود و تصویر جدیدی به دست می‌آید که مشابه تصویر اصلی است. متمم تصویر فشرده‌شده، همان تفاضل تصویر اصلی از تصویر فشرده‌شده به دست آمده از طریق تجزیه مقدار تکین است.

در روش تجزیه مقدار تکین (SVD) از وابستگی خطی ذاتی موجود بین سطرها و یا ستون‌های یک تصویر استفاده می‌شود و این موضوع توسط این روش توصیف می‌گردد.

اگر A ماتریس یک تصویر با ابعاد $M \times N$ روی میدان حقیقی یا مختلط باشد، آنگاه تجزیه‌ای از A به صورت $A = USV^T$ وجود دارد.

U و V ماتریس‌های متعامد^۱ با ابعاد $M \times M$ می‌باشند. ماتریس متعامد، ماتریسی است که حاصل ضرب داخلی هر سطر یا ستونی از ماتریس در سطر یا ستون دیگری از همان ماتریس برابر صفر باشد.

S ماتریس قطری^۲ مقادیر تکین با ابعاد $N \times N$ است. ماتریس قطری، ماتریسی است که تمام درایه‌های آن به جز قطر اصلی برابر صفر باشد.

V^T نشان‌دهنده ترانهاده مزدوج V است. این روش فاکتورگیری، تجزیه مقدار تکین A نامیده می‌شود. تجزیه مقدار تکین به عبارتی همان تعاریف مقادیر ویژه و بردار ویژه را دارا بوده و کاربردهای فراوانی دارد. یکی از کاربردهای آن فشرده‌سازی تصویر است.

1- Orthogonal Matrix
2- Diagonal Matrix

مثال) فرض شود ماتریس A به صورت زیر داده شده باشد:

$$A = \begin{bmatrix} 0.9501 & 0.8913 & 0.8214 & 0.9218 \\ 0.2311 & 0.7621 & 0.4447 & 0.7382 \\ 0.6068 & 0.4565 & 0.6154 & 0.1763 \\ 0.4860 & 0.0185 & 0.7919 & 0.4057 \end{bmatrix}$$

با توجه به تجزیه مقدار تکین (SVD)، ماتریس A را می توان به صورت $A = \sum_{i=1}^n \sigma_i u_i v_i^T$ نوشت، که در آن ماتریس های U، V و S ماتریس های ۴×۴ بوده و عبارت اند از:

$$U = \begin{bmatrix} 0.7301 & 0.1242 & 0.1899 & -0.6445 \\ 0.4413 & 0.6334 & -0.3788 & 0.5104 \\ 0.3809 & -0.3254 & 0.6577 & 0.5626 \\ 0.3564 & -0.6910 & -0.6229 & 0.0871 \end{bmatrix}$$

$$U = (u_1 \ u_2 \ \dots \ u_n)$$

$$V = \begin{bmatrix} 0.4903 & -0.4004 & 0.5191 & -0.5743 \\ 0.4770 & 0.6433 & 0.4642 & 0.3783 \\ 0.5362 & -0.5417 & -0.2770 & 0.5850 \\ 0.4945 & 0.3638 & -0.6620 & -0.4299 \end{bmatrix}$$

$$V = (v_1 \ v_2 \ \dots \ v_n)$$

$$S = \begin{bmatrix} 2.4479 & 0 & 0 & 0 \\ 0 & 0.6716 & 0 & 0 \\ 0 & 0 & 0.3646 & 0 \\ 0 & 0 & 0 & 0.1927 \end{bmatrix}$$

طبق تعریف، بردارهای مخالف صفر w_1, w_2, w_3, w_4 از فضای برداری R^4 را مستقل خطی گویند هرگاه به ازاء هر ترکیب خطی از این بردارها مانند $\sum_{i=1}^n c_i w_i = 0$ ، آنگاه $c_1 = c_2 = \dots = c_n = 0$ و اگر حداقل یکی از c_i ها مخالف صفر باشد، بردارها وابسته خطی هستند. اگر در مثال قبل، هر سطر ماتریس S را یک مجموعه برداری w_i در نظر بگیریم، w_1, w_2, w_3, w_4 را خواهیم داشت:

$$S = \begin{bmatrix} w_1 | 2.4479 & 0 & 0 & 0 \\ w_2 | 0 & 0.6716 & 0 & 0 \\ w_3 | 0 & 0 & 0.3646 & 0 \\ w_4 | 0 & 0 & 0 & 0.1927 \end{bmatrix}$$

در مرحله اول با صفر کردن مقدار تکین در w_4 ، این سطر وابسته خطی خواهد شد؛ زیرا تمام درایه های آن صفر هستند و با توجه به

با تجزیه مقدار تکین، بردار مقدار تکین به صورت روابط (۱) به دست می آید:

$$(1)$$

$$A = USV^T ; \quad Sv = \text{Diag}(S) = (\sigma_1, \sigma_2, \dots, \sigma_{\min(M,N)})$$

هم چنین Sv بردار مقادیر تکین (جذر مقادیر ویژه یعنی $\sqrt{\sigma_i^2}$ ها) شامل قطر ماتریس S است و $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_{\min(M,N)}$ می باشد.

این مقادیر تکین نشان دهنده انرژی تصویر هستند. به عبارت دیگر، جمع مقادیر ویژه یک ماتریس با کل انرژی آن ماتریس برابر است [۱]. یعنی:

$$\sum_{i=1}^M \sum_{j=1}^N A^2(i,j) = \sum_{i=1}^{\min(M,N)} \sigma_i^2 \quad (2)$$

لازم به ذکر است که تصاویر از تعداد زیادی مربعات کوچک (پیکسل) تشکیل شده اند و هر پیکسل دارای یک شماره رقمی می باشد که بیانگر مقدار روشنایی آن پیکسل است. مقدار پیکسل یا همان مقدار انرژی تصویر که یک تصویر رقمی به هنگام تصویر برداری کسب می کند، رقم های دودویی یا بیت ها را تشکیل می دهند. اگر A یک ماتریس مربعی با p سطر و q ستون وابسته خطی باشد (مفهوم وابسته خطی در ادامه توضیح داده می شود)، چون U و V ماتریس های متعامد با رتبه کامل هستند، تعداد صفرهای بردار مقادیر تکین آن برابر است با [۲]:

$$z = \begin{cases} p-1 & ; p \geq q \\ q-1 & ; q \geq p \end{cases} \quad (3)$$

پس z تعداد صفرهای بردار مقادیر تکین است و p سطر و q ستون ماتریس A است و اما رتبه^۴ یک ماتریس A برابر با بیشینه تعداد ستون های (یا سطرهای) مستقل خطی در آن ماتریس است و رتبه کامل^۵ به صورت روابط (۴) تعریف می شود:

$$A_{n \times n} \text{ غیر تکین} \rightarrow |A| \neq 0 \rightarrow \text{rank}(A) = n \rightarrow \text{رتبه کامل (Full Rank)}$$

$$A_{n \times n} \text{ غیر تکین} \rightarrow \begin{cases} \text{rank}(A) = \min(m, n) \rightarrow \text{رتبه کامل (Full Rank)} \\ \text{rank}(A) < \min(m, n) \rightarrow \text{کاهش رتبه (Rank Deficiency)} \end{cases} \quad (4)$$

- 1- Digital Number
- 2- Digit Binary
- 3- Bits
- 4- Rank
- 5- Full Rank

فشرده‌سازی تصویر با اعمال k مورد نظر در روابط (۷) حاصل می‌شود:

$$A_1 = US_1V^T, S_1 = \text{Diag}(\sigma_1, \sigma_2, \dots, \sigma_{k_1}) \quad (7)$$

که U با ابعاد $M \times K1$ و V با ابعاد $N \times K1$ است. اگر در مثال فوق فرضاً $k=16$ در نظر گرفته شود، در ابتدا یک ماتریس با همان اندازه ماتریس $a_{i,j}$ ، یعنی 512×512 ، با درایه‌های صفر جهت درج مقادیر به‌دست‌آمده در نظر گرفته می‌شود:

Example $k = 16 \rightarrow$

$$\begin{bmatrix} b_{1,1} & \dots & b_{1,512} \\ \vdots & \ddots & \vdots \\ b_{512,1} & \dots & b_{512,512} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$$

با اعمال $k=16$ مقادیر درایه‌های ماتریس به‌صورت ستونی درج خواهد شد (رابطه ۸):

$$\begin{aligned} & \begin{bmatrix} b_{1,1} & \dots & b_{1,512} \\ \vdots & \ddots & \vdots \\ b_{512,1} & \dots & b_{512,512} \end{bmatrix} = \left(\begin{bmatrix} u_{1,1} \\ \vdots \\ u_{512,1} \end{bmatrix} \times [S_{1,1}] \times \begin{bmatrix} v_{1,1} \\ \vdots \\ v_{512,1} \end{bmatrix}^T \right) \\ & + \left(\begin{bmatrix} u_{1,2} & \dots & u_{1,512} \\ \vdots & \ddots & \vdots \\ u_{512,2} & \dots & u_{512,512} \end{bmatrix} \times [S_{2,2}] \times \begin{bmatrix} v_{1,2} & \dots & v_{1,512} \\ \vdots & \ddots & \vdots \\ v_{512,2} & \dots & v_{512,512} \end{bmatrix}^T \right) \\ & + \dots + \left(\begin{bmatrix} u_{1,16} & \dots & u_{1,512} \\ \vdots & \ddots & \vdots \\ u_{512,16} & \dots & u_{512,512} \end{bmatrix} \times [S_{16,16}] \right) \\ & \times \begin{bmatrix} v_{1,16} & \dots & v_{1,512} \\ \vdots & \ddots & \vdots \\ v_{512,16} & \dots & v_{512,512} \end{bmatrix}^T \end{aligned} \quad (8)$$

این مسئله با نرم‌افزار MATLAB پیاده‌سازی شد و نتیجه به صورت شکل (۲) به‌دست آمد (منبع برنامه در پیوست الف).

نتیجه اجرای برنامه‌ای که با نرم‌افزار MATLAB در این قسمت تهیه شده است، در شکل (۲) مشاهده می‌شود. تصویر «یک تانک در بیابان» به‌عنوان تصویر اصلی^۱ با روش SVD به دو تصویر فشرده‌شده^۲ و متمم تصویر با مقدار^۳ k تقسیم شده است. تصویر اصلی با کیفیت و حجم مصرفی حافظه پایین بوده ولی مشخص است که تصویر

- 1- Original Image
- 2- Compressed Image
- 3- Abs Difference k

ترکیب خطی $w_4 = 0$ و $c_1w_1 + c_2w_2 + c_3w_3 + c_4w_4 = 0$ می‌توان $c_4 \neq 0$ را نتیجه گرفت. سپس با توجه به تعریف وابستگی خطی می‌توان گفت که سطر w_4 وابسته خطی است. در مورد سطر سوم هم همین اتفاق می‌افتد و با ادامه این کار مشاهده می‌شود که تعداد سطرها یا ستون‌های وابسته خطی افزایش می‌یابد.

با افزایش وابستگی خطی سطرها و ستون‌ها، مقادیر تکین اندیس‌های بالاتر کاهش و برعکس مقادیر تکین اندیس‌های پایین‌تر افزایش می‌یابند. به عبارت دیگر، انرژی از مقادیر تکین اندیس‌های بالاتر به سمت مقادیر تکین اندیس‌های پایین‌تر جاری می‌گردد به طوری که اگر همه سطرها و یا همه ستون‌های ماتریس وابسته خطی باشند، همه انرژی ماتریس در مقدار تکین اول متمرکز بوده و بقیه مقادیر تکین صفر خواهند شد.

به‌طور کلی می‌توان گفت تعداد سطرها و وابسته خطی یک تصویر با تعیین صفر بودن مقدار تکین یک اندیس خاص برای بلوک‌های مربعی در آن تصویر به دست می‌آیند. یعنی با محاسبه بردار مقادیر تکین برای تمام بلوک‌ها، مقدار تکین اندیس i ام از نظر صفر بودن در تمامی بردارها بررسی و تعداد صفرهای آن شمارش می‌شوند. پس میزان وابستگی‌های خطی با میزان تکین اندیس‌ها رابطه عکس دارد [۴ و ۳].

۳- فشرده‌سازی تصویر با استفاده از SVD

یکی از کاربردهای مفید SVD، فشرده‌سازی تصاویر است. اگر تصویری به‌صورت ماتریس A نمایش داده شود، با توجه به SVD، رابطه‌های (۵) برقرار است [۶ و ۵]:

$$\begin{aligned} A &= USV^T \\ S &= \text{Diag}(\sigma_1, \sigma_2, \dots, \sigma_k, 0, \dots, 0) \end{aligned} \quad (5)$$

که در آن U و V با ابعاد $M \times N$ است. حال به‌عنوان نمونه برای یک تصویر 512×512 یک ماتریس $a_{i,j}$ به شکل رابطه (۶) خواهد بود:

$$\begin{aligned} & \begin{bmatrix} a_{1,1} & \dots & a_{1,512} \\ \vdots & \ddots & \vdots \\ a_{512,1} & \dots & a_{512,512} \end{bmatrix} \\ & = \begin{bmatrix} u_{1,1} & \dots & u_{1,512} \\ \vdots & \ddots & \vdots \\ u_{512,1} & \dots & u_{512,512} \end{bmatrix} \times \begin{bmatrix} s_{1,1} & 0 & \dots & \dots & 0 \\ 0 & s_{2,2} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & s_{512,512} \end{bmatrix} \\ & \times \begin{bmatrix} v_{1,1} & \dots & v_{1,512} \\ \vdots & \ddots & \vdots \\ v_{512,1} & \dots & v_{512,512} \end{bmatrix}^T \end{aligned} \quad (6)$$

در این فصل، نحوه استحصال تصویر فشرده‌شده توضیح داده شد و در فصل بعدی، نحوه استحصال متمم تصویر و نهان‌نگاری در آن و بازسازی تصویر نهایی بیان خواهد شد.

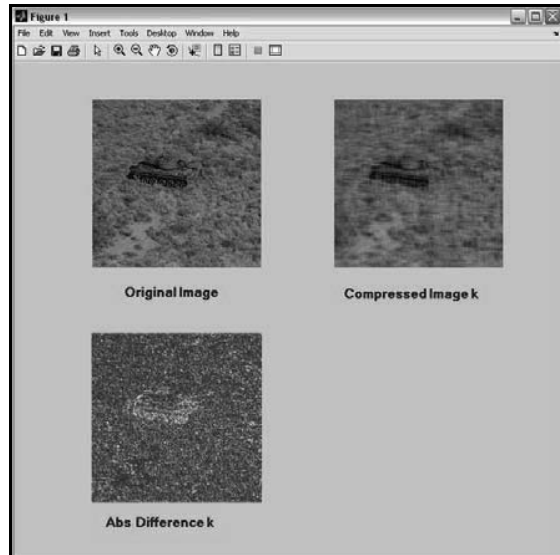
با اجرای برنامه نرم‌افزاری با k های مختلف، تصاویر فشرده‌شده شکل (۳) استحصال می‌گردد:

همان‌طور که مشاهده می‌شود هرچه k کاهش می‌یابد از وضوح تصویر کاسته می‌شود [۷]. بسته به نوع کاربرد می‌توان وضوح تصویر را کاهش داد تا از حجم حافظه کمتری استفاده شود. جدول (۱) میزان حافظه مصرفی در این مثال را نشان می‌دهد:

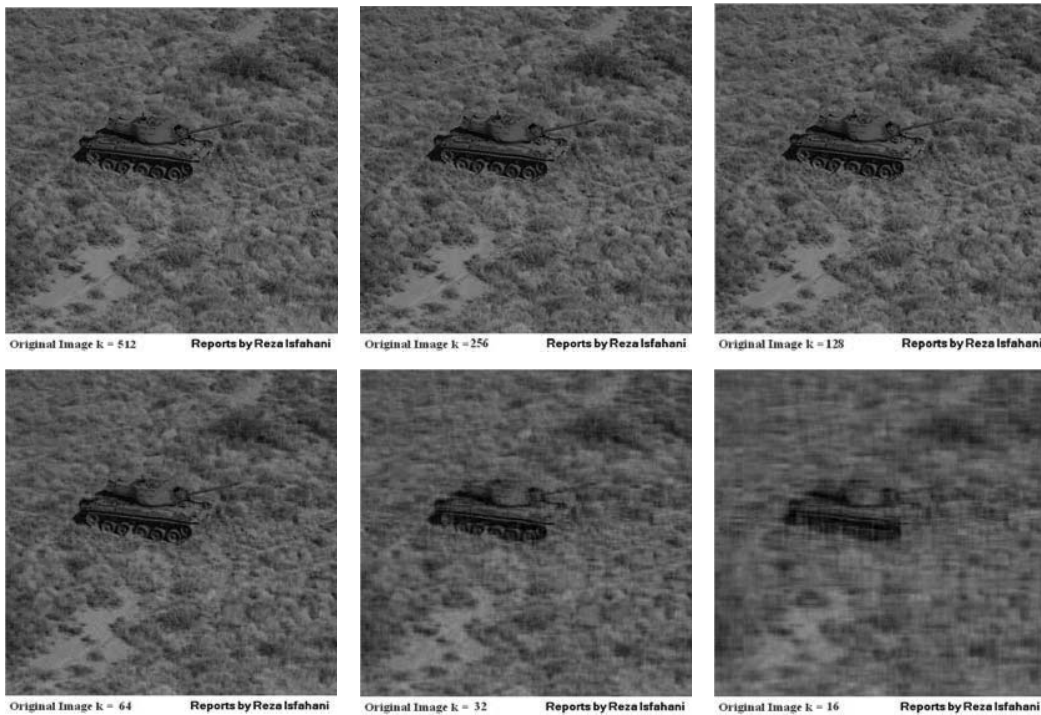
جدول ۱- میزان حافظه مصرفی

No	K	Storage (KB)	Used storage Percent (%)
	512 (Tank original Image)	250	100
	256	249	99.6
	128	243	97.2
	64	230	92
	32	214	85.6
	16	192	76.8

«یک تانک در بیابان» می‌باشد. متمم تصویر با مقدار k هم متمم تصویر حاصل از تفاضل تصویر اصلی و تصویر فشرده شده است که اگر با دقت مشاهده شود، می‌توان تصویر را تا حدودی تشخیص داد.



شکل ۲- فشرده‌سازی تصویر به کمک SVD و به دست آوردن متمم آن



شکل ۳- فشرده‌سازی تصویر به کمک SVD با k های مختلف

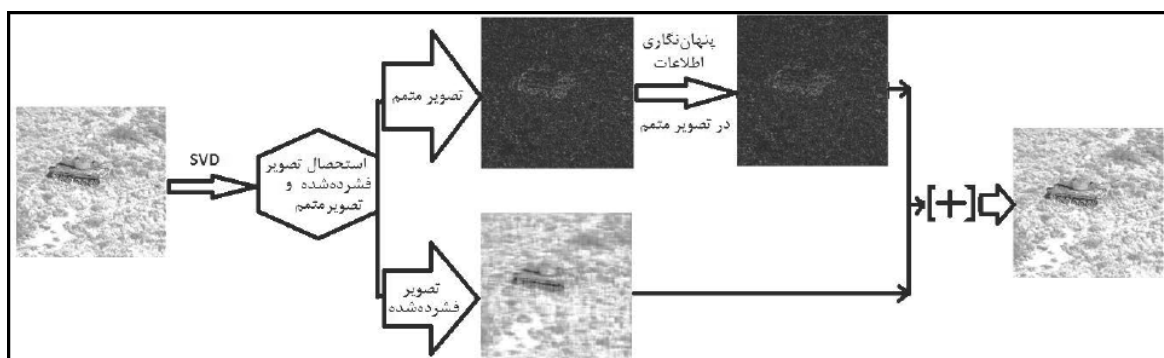
تصویر فشرده شده» نامیده می شود. این تصویر را می توان به صورت ماتریسی به نام $G_{F,F}$ به صورت رابطه (۹) نمایش داد:

$$\begin{bmatrix} G_{1,1} & \dots & G_{1,212} \\ | & & | \\ G_{212,1} & \dots & G_{212,212} \end{bmatrix} = \begin{bmatrix} A_{1,1} & \dots & A_{1,212} \\ | & & | \\ A_{212,1} & \dots & A_{212,212} \end{bmatrix} - \begin{bmatrix} B_{1,1} & \dots & B_{1,212} \\ | & & | \\ B_{212,1} & \dots & B_{212,212} \end{bmatrix} \quad (9)$$

حال اگر داده های مورد نظر که باید پنهان شوند، با روش بیت کم ارزش یا هر الگوریتم پنهان نگاری دیگر، در متمم تصویر قرار گیرند و در نهایت با تصویر فشرده شده به دست آمده با کل مورد نظر جمع گردد، تصویری تولید خواهد شد که به تصویر اصلی شبیه تر خواهد بود.

مثلاً در $k=16$ می توان داشت (رابطه (۱۰)):

$$\begin{bmatrix} B_{1,1} & \dots & B_{1,212} \\ | & & | \\ B_{212,1} & \dots & B_{212,212} \end{bmatrix} = \left(\begin{bmatrix} W_{1,1} & & \\ | & & \\ W_{212,1} & & \end{bmatrix} \times [F_{1,1}] \times \begin{bmatrix} V_{1,1} & & \\ | & & \\ V_{212,1} & & \end{bmatrix}^T \right) + \left(\begin{bmatrix} W_{1,1} & W_{1,2} & \\ | & | & \\ W_{212,1} & W_{212,2} & \end{bmatrix} \times [F_{2,2}] \times \begin{bmatrix} V_{1,1} & V_{1,2} & \\ | & | & \\ V_{212,1} & V_{212,2} & \end{bmatrix}^T \right) + \dots + \left(\begin{bmatrix} W_{1,1} & \dots & W_{1,16} & \\ | & & | & \\ W_{212,1} & \dots & W_{212,16} & \end{bmatrix} \times [F_{16,16}] \times \begin{bmatrix} V_{1,1} & \dots & V_{1,16} & \\ | & & | & \\ V_{212,1} & \dots & V_{212,16} & \end{bmatrix}^T \right) + \begin{bmatrix} t_{1,1} & \dots & t_{1,212} \\ | & & | \\ t_{212,1} & \dots & t_{212,212} \end{bmatrix}$$



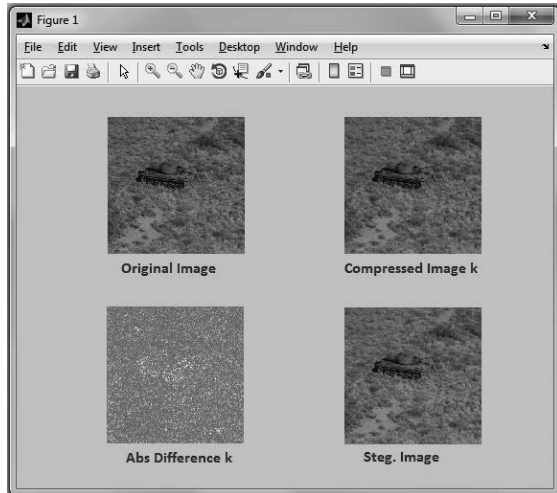
شکل ۴- پنهان نگاری در متمم تصویر فشرده شده [۱۰]

۴- پنهان نگاری در متمم تصویر فشرده شده

در بخش (۳) نحوه به دست آوردن تصویر فشرده شده و متمم تصویر با روش SVD بیان شد. همان طور که در شکل (۴) نشان داده شده است با یک روش پیشنهادی، پنهان نگاری در متمم تصویر فشرده شده صورت گرفته است:

پنهان نگاری در تصویر متمم با یک روش دلخواه صورت خواهد گرفت و تصویر متممی که حاوی اطلاعات پنهان نگاری است با تصویر فشرده شده جمع خواهد شد. در این جا از ساده ترین الگوریتم پنهان نگاری یعنی شیوه بیت کم ارزش^۱ استفاده شده است. در این روش، داده های 0 و 1 در بیت کم ارزش پیکسل ها به ترتیب قرار گرفته است. اگر مقادیر شدت روشنایی پیکسل های تصویر به مقدار دودویی تبدیل شود، اولین بیت از سمت راست، کم ارزش ترین بیت است که تغییر آن، تغییر بسیار کمی در کل تصویر را نتیجه خواهد داد.

اگر قدر مطلق تفاضل تصویر اصلی از تصویر به دست آمده از کل مورد نظر محاسبه شود، تصویری حاصل می شود که در این جا «متمم

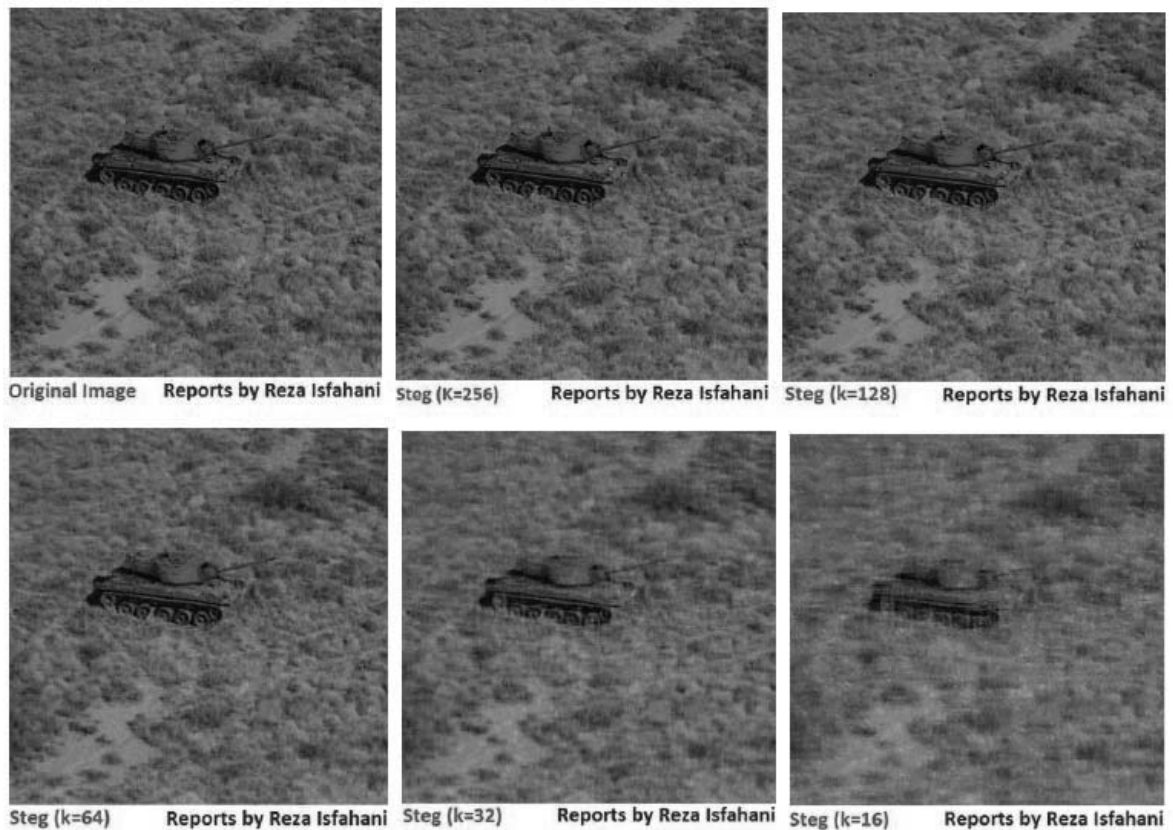


شکل ۵- نهان‌نگاری در تصویر متمم و تجمیع آن با تصویر فشرده‌شده

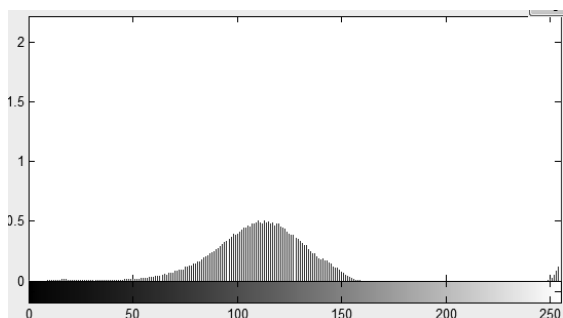
در اینجا ماتریس T_k ماتریسی است که از روی T_k ایجاد شده است. در واقع داده‌های مورد نظر که باید پنهان شوند، در بیت کم ارزش مقادیر ماتریس T_k قرار گرفته‌اند. به‌عنوان مثال، می‌توان دنباله‌ای 1 مانند بردار s در شکل قدر مطلق تفاضل تصویر اصلی تانک از تصویر به‌دست‌آمده از k ی مورد نظر، پنهان کرد:

$$s=[1,0,1,1,1,0,1,1,1,1,1,1,1,1,1,0,0,0,1,0,0,0,0]$$

سپس تصویر حاوی داده‌های پنهان با تصویر فشرده‌شده به‌دست‌آمده از k ی مورد نظر جمع می‌شود. حاصل پیاده‌سازی این مسئله توسط نرم‌افزار MATLAB، به‌صورت شکل (۵) است (منبع برنامه در پیوست ب). تصاویر حاوی داده‌های پنهان (بردار s مطرح‌شده) با k های مختلف به‌صورت شکل (۶) خواهند بود:



شکل ۶- تصاویر حاوی اطلاعات نهان‌نگاری شده (تجمیع تصویر متمم حاوی نهان‌نگاری و تصویر فشرده‌شده) با k های مختلف



شکل ۷- هیستوگرام تمام تصاویر شکل (۶)

۶- نتیجه‌گیری

استفاده از حداقل‌ها در حالت بحرانی و استفاده از شیوه‌های ابتکاری جهت تسریع و راه‌اندازی، دو مسئله مهم در پدافند غیرعامل است؛ نهان‌نگاری هم که از مباحث جدی فناوری اطلاعات و ارتباطات در پدافند غیرعامل است، از این قضیه مستثنی نیست. در این مقاله روشی ابتکاری برای نهان‌نگاری در تصویر مطرح شده است. در این روش به کمک SVD می‌توان تصاویر را فشرده کرد و سپس داده‌های مورد نظر که باید پنهان شوند را در متمم تصویر فشرده شده جاسازی نمود. بعد از فشرده‌سازی و بازسازی مجدد، تصویر جدیدی ایجاد خواهد شد. با توجه به نیاز بایستی k ای را انتخاب نمود که علاوه بر فضای حافظه کم، تصویر بازسازی شده مناسبی را نیز ارائه دهد. هم‌چنین به‌کاربردن الگوریتم مناسب برای نهان‌نگاری نیز مهم است. لذا طراحی الگوریتم و انتخاب k ی مناسب، از موضوعات خوب جهت ادامه تحقیق است. لازم به ذکر است اثبات امنیت، کارایی و مقایسه با روش‌های دیگر، از مسائلی است که در این مقاله به آن پرداخته نشده است و امیدواریم در یک مقاله تحقیقاتی مرتبط علمی- پژوهشی به بررسی آنها بپردازیم.

مراجع

1. IrfanSiap, Education Faculty, Adiyaman University, Turkey, "Motivating the concept of eigenvectors via cryptography", Teaching mathematics and its applications. Volume 27, No. 2, (2008).
2. Gokhan Gul, Ahmet Emir Dirik, and Ismail Avcibas, "Steganalytic Features for JPEG Compressin-Based Perturbed Quantization" IEEE Signal Processing Letters, Vol. 14, No. 3, March (2007).
3. G.Gul, and F.Kurugollu, "SVD-Based Universal Spatial Domain Image Steganalysis", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp. 349-353, June (2010).
4. Kalman, Dan, "A Singularly Valuable Decomposition", The College Mathematics Journal. Vol.27-No. 1-jan (1998), 2-23.
5. Lay, David C.Linear Algebra and Its Applications, Addison Wesley Longman, Inc., (1997).

همان‌طور که در جدول (۲) مشاهده می‌شود، در متمم فشرده‌شده تصاویر، هرچه k کمتر باشد، فضای بیشتری جهت نهان‌نگاری در دسترس قرار می‌گیرد. هرچند تصویر نهایی بازسازی‌شده در k های کمتر، تشابه کمتری به تصویر اصلی دارد:

جدول ۲- فضای حافظه در دسترس، جهت نهان‌نگاری

No	K	Storage (KB)
1	512	9.83
2	256	26
3	128	60.8
4	64	80.8
5	32	92.2
6	16	98.5

۵- نهان‌کاوی^۱ به روش هیستوگرام

نهان‌نگاری به دو روش در حوزه مکان و حوزه تبدیل انجام می‌شود. برای تحلیل در هر دو حوزه، نهان‌کاوی‌های خاصی وجود دارد. روش نهان‌کاوی هیستوگرام، شیوه بسیار ساده و کاربردی در تشخیص داده‌های نهان‌نگاری در حوزه مکان است [۸]. بررسی هیستوگرام با توجه به پیشرفت روش‌های نهان‌نگاری و ارتقاء امنیت آن‌ها برای نهان‌کاوی کافی نبوده و لذا روش‌های نهان‌کاوی دیگری نیز جهت تکمیل تحلیل و ارزیابی باید انجام شوند.

هیستوگرام تصویر، نموداری است که توسط آن، تعداد پیکسل‌های هر سطح روشنایی در تصویر ورودی مشخص می‌شود. فرض کنید تصویر ورودی، یک تصویر مقیاس خاکستری^۲ با ۲۵۶ سطح روشنایی باشد، بنابراین هر یک از پیکسل‌های تصویر، مقداری در بازه [۰...۲۵۵] می‌توانند داشته باشند. برای به‌دست آوردن هیستوگرام تصویر، کافی است با پیمایش کل پیکسل‌های تصویر، تعداد پیکسل‌های هر سطح روشنایی محاسبه شود. اگر نمودار دارای توزیع یکنواخت نباشد، حس کنجکاو می‌شود که جهت نهان‌کاوی بیشتر برمی‌انگیزد. زیرا هرچه هیستوگرام با توزیع یکنواخت اختلاف بیشتر باشد، احتمال وجود اطلاعات نهان‌نگاری شده بیشتر خواهد بود.

در این مقاله که از روش ساده LSB (یکی از روش‌های حوزه مکان) استفاده شده است می‌توان با توجه به تغییرات ناگهانی میله‌های نمودار هیستوگرام تصاویر (شکل ۷)، به‌طور آماری تا حدودی حدس زد که آیا تغییری در تصویر صورت گرفته است یا خیر؟ ولی جالب است بدانید که هیستوگرام تمام تصاویر قبل (تصاویر حاوی اطلاعات نهان‌نگاری شده با k های مختلف) به‌طور یکسان و بدون تغییرات ناگهانی و به‌صورت نمودار زیر است. هرچند بیان این مسئله نیاز به تحقیق و بررسی بیشتری دارد که می‌تواند موضوع مقاله‌ای جداگانه باشد:

1- Steganalysis
2- Grayscale

6. S.Leon, Linear Algebra with Applications, Pearson, Prentice-Hall, (2010).
7. Alexander Svedlov, Scott Dexter,Ahmet M. Eskiciogu, "ROBUST DCT-SVD DOMAIN IMAGE WATERMARKING FOR COPYRIGHT PROTECTION EMBEDDING DATA IN ALL FREQUENCIES".
8. Book: Dr. Rainer Bohme, "Advanced Statistical Steganalysis", Springer, (2009).

پیوست

(پیوست الف)

```

%%%%%%%%%%
%By: Reza Isfahani
% PHD Student
%%%%%%%%%%
close all
clc
clear
fid = fopen('SVD_Result1.txt', 'wt');
[A,map] = imread('033.GIF');
B=im2double(A,'indexed');
[m, n] = size(B);
subplot(2,2,1)
imshow(B,map)

[u,s,v] = svd(B);

C=zeros(size(B));

%Compressed k=KK
KK = 64;
for j = 1:KK
    C = C + s(j, j) * u(:, j) * v(:, j).';
end

C=floor(C);

imwrite(C,['tst.GIF'])

subplot(2,2,2)
imshow(C,map)

%Difference between the original and the re-constructed images
subplot(2,2,3)
D = abs(B-C);
imshow(D,map)

k = find(C<1);
set(gcf, 'Unit', 'inches', 'Paperposition', [0, 0, 2, 1])
print -djpeg '033_tst.jpg'

```

پیوست ب)

```

%By: Reza Isfahani
% PHD Student
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
close all
clc
clear
fid = fopen('SVD_Result1.txt', 'wt');
[A,map] = imread('033.GIF');
B=im2double(A,'indexed');
[m, n] = size(B);
subplot(2,2,1)
imshow(B,map)

[u,s,v] = svd(B);

C=zeros(size(B));

%Compressed k=KK
KK = 64;
for j = 1:KK
    C = C + s(j, j) * u(:, j) * v(:, j).';
end

C=floor(C);

imwrite(C,['tst.GIF'])

subplot(2,2,2)
imshow(C,map)

%Difference between the original and the re-constructed images
subplot(2,2,3)
D = abs(B-C);
imshow(D,map)

%Steg
s=[1,0,1,1,1,0,1,1,1,1,1,1,1,1,0,0,0,1,0,0,0,0];
ss=size(s);
Db=de2bi(D);
Df=fliplr(Db);
[m2, n2] = size(Df)
if(n2 >= ss(2))
    for z=1:ss(2)
        Df(z,n2)=s(z);
    end
end
e=fliplr(Df);
f=bi2de(e);
g=reshape(f,512,512);
t = g + C;
subplot(2,2,4)
imshow(t,map)

k = find(C<1);
set(gcf, 'Unit', 'inches', 'Paperposition', [0, 0, 2, 1])

```

Steganography in the Compressed Image Supplement Using Takin Value Analysis

R. Esfahani¹

Z. A. Norouzi²

Abstract

In the information hiding systems, three main elements of capacity, security and resistance are involved. Security and emplacement capacity have a special position in steganography and the steganography methods emphasize the reduction of changes caused by emplacement. But one of the very important issues in passive defense is the appropriate application of the existing memory space for steganography during crisis. This paper attempts to present a dynamic method to implement image steganography by considering minimum factors in the image properties for critical conditions. The consumed memory space and the similarity of image are two parameters that are dealt with in this paper. In this paper, at first, a compressed image of the main image is obtained using the Takin Value Analysis Method and then the steganography is performed. In this method, steganography in the compressed image supplement is done and later, will be accumulated with the compressed image itself and the ultimate image will be obtained which resembles the main image and this similarity value depends on the value of the special parameter in the computational process called K (special value of matrix). The lower the value of K , the lower the similarity to the main image but a higher memory space will be available for steganography.

Key Words: *Special Values, Special Vector, Steganography, Steganalysis, Histogram, Takin Value Analysis, Image Compressor*