هشتمین کنفرانس بین المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۲۴ و ۲۵ آبان ۱۴۰۲

نهان نگاری تصاویر دیجیتال براساس چند جمله ای رخ

زهرا سعیدی[۱]
دانشگاه علم و صنعت ایران، تهران، ایران

سمانه مشهدی
[دانشگاه علم و صنعت ایران، تهران، ایران]

چکیده

با توجه به پیشرفت سریع اینترنت امنیت اطلاعات یکی از مهم ترین موضوعاتی است که مطرح می‌شود. گرچه رمز نگاری می‌تواند امنیت اطلاعات تا حدودی بهبود ببخشد ولی به تنهایی نمی‌تواند مشکل امنیت را برطرف کند. نهان نگاری یکی از روش هایی است که برای افزایش امنیت به کار گرفته می‌شود . در این مقاله قصد داریم از نهان نگاری در حوزه مکانی برای جاسازی داده‌های پنهان استفاده کنیم. در این طرح به دلیل جاسازی در کم‌ترین بیت های با ارزش کیفیت تصویر و ظرفیت جاسازی را افزایش می‌دهد، علاوه بر این در این طرح از چند جمله ای رخ به عنوان کلید برای تعیین مکان های جاسازی استفاده می‌شود و این امر امنیت طرح را در برابر حملات کاربران مخرب افزایش می‌دهد، هم چنین دیگر نیازی به ارسال کلید بین شخص فرستنده و گیرنده نیست.

واژه‌های کلیدی: نهان نگاری ،تصویر راز خاکستری ، چند جمله ای رخ

[2010]: 13D45, 39B42

۱ مقدمه

با توجه به گسترش روز افزون اینترنت نگرانی کاربران در مورد امنیت اطلاعات افزایش یافته است، بنابراین به ارتباط مخفی نیاز است. رمز نگاری و استگانوگرافی دو زمینه برای دسترسی به امنیت داده ها است. رمز نگاری اطلاعات به طور هوشمندانه به اطلاعات بی معنی در هم تبدیل می‌کند به طوریکه که استخراج ان برای کاربر مخرب دشوار است. یکی از معایب رمز نگاری ایجاد سوء ظن بین کاربران مخرب است برای جلو گیری از ایجاد سوء ظن از نهان نگاری استفاده می‌شود در این روش می‌توان داده های مخفی که رمز شده اند در یک تصویر پوششی پنهان کرد[۴، ۳، ۲، ۱]. سه عامل اصلی در نهان نگاری ظرفیت ، امنیت و کیفیت تصویر باید مورد توجه قرار گیرد. مقاومت یک طرح نهان نگاری بدان معنا است که اطلاعات مخفی در مقابل تغییرات ناخواسته و غیر عمدی و عمدی که توسط مهاجم فعال برای از بین بردن اطلاعات اعمال می‌شود مقاوم باشد. منظور از ظرفیت نهان نگاری این است که بتوان داده مخفی بسیاری را در تصویر میزبان جاسازی کرد. منظور از شفافیت مقایسه بین تصویر قبل و بعد نهان نگاری شده است. یکی از ابتدایی ترین روش‌های نهان نگاری روش بیت کم ارزش LSB است. در این از بیت‌های کم ارزش برای درج اطلاعات مخفی استفاده می‌شود در نتیجه تصویر میزبان تغییر زیادی نمی‌کند چون حاوی اطلاعات زیادی نیست این روش تا حدودی کیفیت تصویر استگو را افزایش می‌دهد.

در این طرح نیز برای بهبود کیفیت بصری و افزایش ظرفیت جاسازی از LSB استفاده شده است.

تعریف ۱.۱. فرض کنید r_k تعداد راه‌هایی است که برای قرار دادن k رخ غیر هجومی روی صفحه‌ای B از m ردیف و n ستون است. چند جمله‌ای رخ $R_B(x)$ صفحه شطرنجی B به صورت زیر تعریف می‌شود: [۵]

$$R_B(x) = \sum_{k=0}^{\min(m,n)} r_k x^k. \qquad (۱)$$

[۱] سخنران

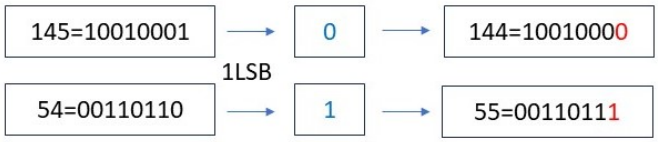
مثال ۲.۱. صفحه شطرنجی شکل ۱ را در نظر بگیرید. در این مثال، چند جمله ای رخ $x^۳ + ۴x^۲ + ۵x + ۱$ است.

شکل ۱: صفحه شطرنجی

تعریف ۳.۱. LSB یکی از معروف‌ترین روش مورد استفاده در نهان نگاری است. فرض کنید $p = x_۸ \dots x_۱$ یک قطعه داده ۸ بیتی است و $u_k \dots u_۱$ بیت هستند که باید در p $(k < ۸)$ جاسازی شوند روش LSB به صورت زیر تعریف می‌شود:

$$p' = x_۸ \dots x_{k+۱} u_k \dots u_۱$$

که در آن بیت‌های کم اهمیت p با $u_k \dots u_۱$ جایگزین می‌شوند. شکل ۲ مثالی از جاسازی به روش LSB نشان می دهد.



شکل ۲: جاسازی با روش LSB

۲ طرح پیشنهادی

طرح پیشنهادی شامل دو بخش جاسازی و استخراج تصویر راز است که هر کدام از بخش‌ها را به طور مفصل توضیح خواهیم داد.

۱.۲ مرحله جاسازی

در این مقاله قصد داریم تصویر راز $S = u_۸u_۷u_۶u_۵u_۴u_۳u_۲u_۱$ به ابعاد $W \times H$ را براساس چند جمله ای رخ در تصویر کاور به ابعاد $۲W \times ۲H$ جاسازی کنیم . تصویر کاور H رابه صورت بلوک‌های ۴ پیکسلی غیر هم پوشانی $h_j = p_۱p_۲p_۳p_۴$ که $k = ۱ : ۴$ $p_k = x_{k۸}x_{k۷}...x_{k۲}x_{k۱}$, تقسیم می‌شود. برای جاسازی کافی است مراحل زیر انجام شود:

(۱) تولید ماتریس ۲×۲ بیت مپ $M_j = \begin{bmatrix} x_{۱۸} & x_{۲۸} \\ x_{۳۸} & x_{۴۸} \end{bmatrix}$

(۲) MSB پیکسل های تصویر کاور را در نظر بگیرید.

(۳) تولید یک صفحه شطرنجی ۲×۲.

(۴) محاسبه چند جمله ای رخ $R_B(x) = ۱ + r_۱x + r_۲x^۲$.

(۵) مقدار $y_i = R_B(i) \bmod ۴$ برای هر $i = ۱, \dots, ۴$ محاسبه می‌شود.

(۶) برای مقدارهای مختلف y_i p'_{y_i+1} با جاسازی دو بیت $u_{2i}u_{2i-1}$ در $2LSB$ p_{y_i+1} جاسازی می‌شود.

(۷) سرانجام اگر $y_i = y_l$ برای $1 \le i < l \le 4$، $u_{2i}u_{2i-1}$ در p_{y_i+1} جاسازی می‌شود و $u_{2l}u_{2l-1}$ در نزدیکترین همسایه p_k، $1 \le k \le 6$ جاسازی می‌شود. ۴ بلوک مربوط h'_j به تصویر استگو H'_i $h'_j = p'_1p'_2p'_3p'_4$، است، که $p'_k = x_{k8}x_{k7}...x_{k3}u_{i+1}u_i$

۲.۲ مرحله استخراج

برای استخراج تصویر راز ابتدا تصویر استگو H'_i را به صورت بلوک ۴ پیکسل غیر هم پوشانی $h'_j = p'_1p'_2p'_3p'_4$ تقسیم می‌شوند. برای استخراج مراحل زیر انجام می‌شود:

(۱) تولید ماتریس 2×2 بیت مپ $M_j = \begin{bmatrix} x_{18} & x_{28} \\ x_{38} & x_{48} \end{bmatrix}$

(۲) MSB پیکسل های تصویر استگو را در نظر بگیرید.

(۳) یک صفحه شطرنجی 2×2 ایجاد می‌شود.

(۴) محاسبه چند جمله ای رخ $R_B(x) = 1 + r_1x + r_2x^2$.

(۵) مقدار $y_i = R_B(i) \bmod 4$ برای هر $i = 1, \ldots, 4$ محاسبه می‌شود.

(۶) برای مقدارهای مختلف y_i p'_{y_i+1} دو بیت $u_{2i}u_{2i-1}$ در دو LSB استخراج می‌شود.

(۷) سرانجام اگر $y_i = y_l$ برای $1 \le i < l \le 4$، $u_{2i}u_{2i-1}$ از p_{y_i+1} استخراج می‌شود و $u_{2l}u_{2l-1}$ در نزدیکترین همسایه p_k، $1 \le k \le 6$ استخراج می‌شود.

شکل های ۳ و ۴ یک نمونه مثال ساده در مورد نحوه جاسازی و استخراج روش پیشنهادی است.

۳ نتایج تجربی

در این جا ما امنیت و استحکام را با معیارهایی مانند $PSNR$ و $SSIM$ اندازه گیری می‌کنیم . آزمایشات با تصاویر کاور با ابعاد 512×512 انجام شده است.

کیفیت بصری بالای تصویر استگو یکی از ویژگی‌های طرح استگونوگرافی مطلوب است. ما از اندازه گیری شاخص تشابه ساختاری $(SSIM)$ استفاده می‌کنیم که به صورت تعریف شده است:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

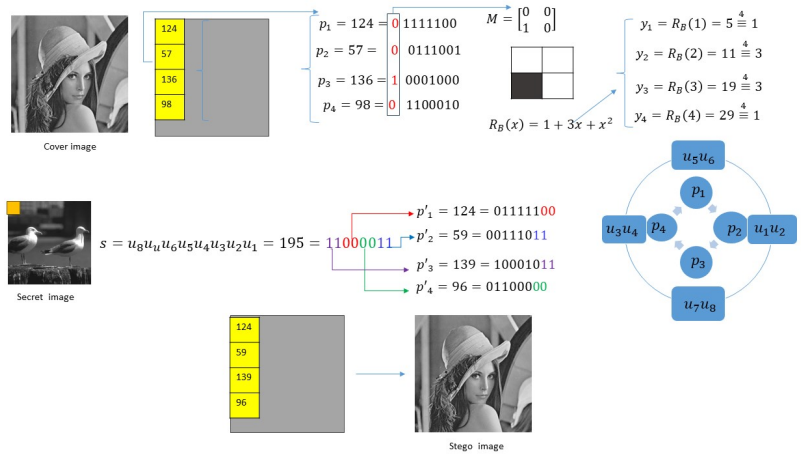
که در آن μ_x و μ_y مقادیر میانگین شدت مقدار پیکسل هستند و σ_x و σ_y به ترتیب شدت واریانس جهات افقی و عمودی هستند. همچنین σ_{xy} کوواریانس را ارائه می‌دهد. ما از نسبت نویز سیگنال پیک $(PSNR)$ استفاده می کنیم که به صورت زیر تعریف می‌شود:

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

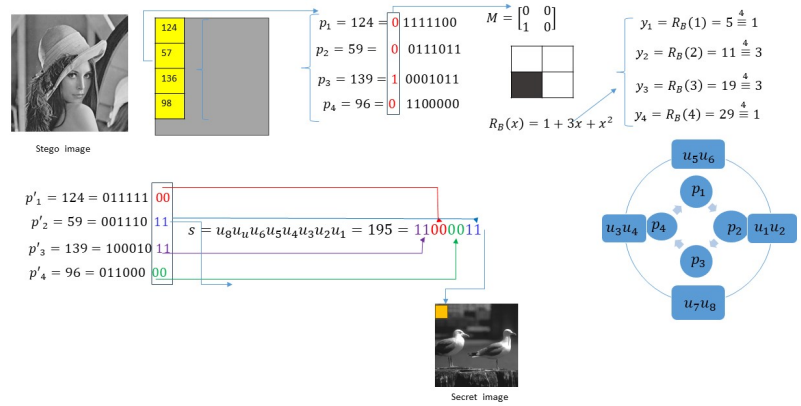
که در آن MSE خطای مقدار میانگین بین تصویر استگو و تصویر میزبان است. اگر تصویر میزبان اندازه $M \times N$ باشد، MSE به صورت زیر تعریف می‌شود:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(H(x,y) - H'(x,y)\right)^2 \qquad (3)$$

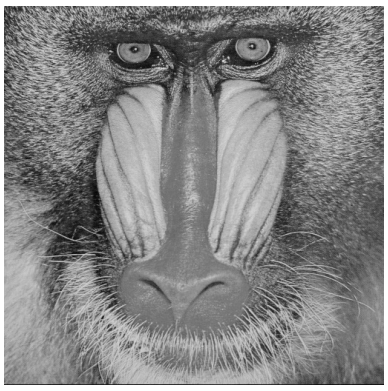
که در آن H تصویر میزبان و H' تصویر استگو است.



شکل ۳: مرحله جاسازی



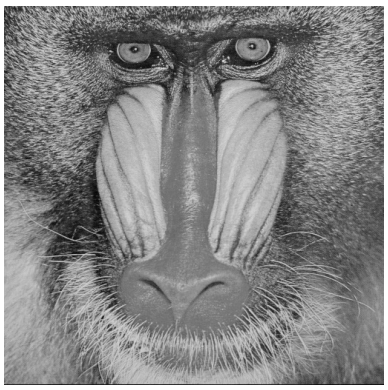
شکل ۴: مرحله استخراج



شکل ۵: تصویر اصلی

شکل ۵ و ۶ به ترتیب تصویر کاور و تصویر نهان نگاری شده را نشان می‌دهند. از هر دو شکل می‌توان نتیجه گرفت هر دو تصویر مشابه یکدیگر هستند و تصویر مخفی پنهان شده قابل مشاهده نیست هم چنین تصویر نهان نگاری شده از کیفیت بصری خوبی برخوردار است.

جدول ۱ مقادیر $SSIM$ و MSE طرح پیشنهادی را نشان می‌دهد از نتایج به دست آمده می‌توان نتیجه گرفت که طرح پیشنهادی از کیفیت بصری بالایی برخودار است و هم‌چنین خطای به دست امده نزدیک به صفر است. در جدول ۲ و شکل ۷ طرح پیشنهادی را با سایر طرح‌های مشابه از لحاظ کیفیت تصویر مقایسه کردیم از مقادیر جدول می‌توان نتیجه گرفت که طرح پیشنهادی نسبت به طرح‌های [۶]و [۷] از کیفیت بصری بالایی



شکل ۶: تصویر نهان نگاری شده

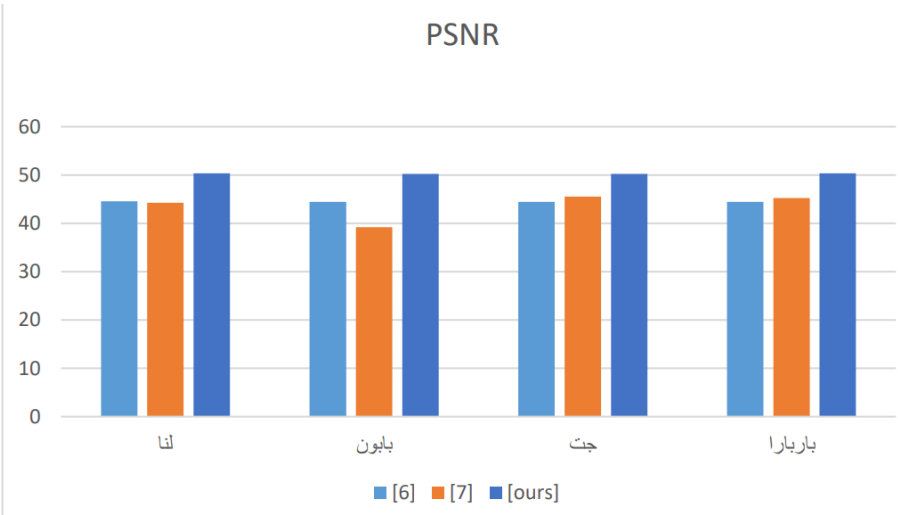
جدول ۱: کیفیت بصری برای تصاویر کاور مختلف

تصویر	MSE	SSIM
لنا	۰٫۰۰۰۲۳	۰٫۹۹۹۱
بابون	۰٫۰۰۰۱۲	۰٫۹۹۸۹
جت	۰٫۰۰۰۱۴	۰٫۹۹۹۷

برخوردار است.

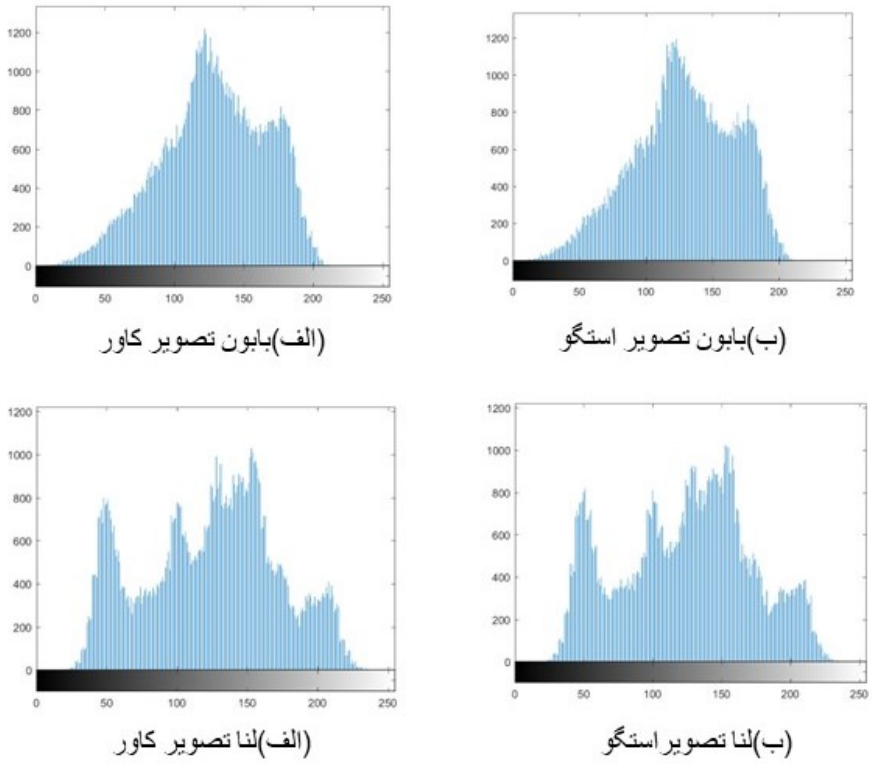
جدول ۲: مقایسه کیفیت تصویر طرح پیشنهادی با طرح های کار های شده

تصویر	[۶]	[۷]	طرح پیشنهادی
لنا	۴۴٫۵۳	۴۴٫۲۳	۵۰٫۳۲
بابون	۴۴٫۴۲	۳۹٫۱۹	۵۰٫۲۳
جت	۴۴٫۴۶	۴۵٫۵۳	۵۰٫۲۵
باربارا	۴۴٫۴۳	۴۵٫۲۳	۵۰٫۳۴



شکل ۷: مقایسه کیفیت تصویر استگو طرح پیشنهادی با طرح های کار شده

هیستوگرام تصویر استگو باید تا حد امکان شبیه به تصویر میزبان باشد تا تحت استگانالیز مبتنی بر هیستوگرام امنیت داشته باشد. در شکل ۸ نشان می‌دهیم که هیستوگرام تصاویر میزبان مشابه تصاویر استگو است. بنابراین هیستوگرام تصاویر سطح قابل قبولی از امنیت را نشان می داد.



شکل ۸: آنالیز هیستوگرام

۴ نتیجه گیری

در این مقاله از نهان نگاری در حوزه مکانی برای جاسازی اطلاعات مخفی استفاده شده است و از یک روش جدید برای تعیین مکان های جاسازی برای افزایش امنیت پیشنهاد شده است. در این طرح از چند جمله ای رخ به عنوان کلید برای تعیین مکان‌های جاسازی به کار گرفته می‌شود و دیگر نیازی به کانال امن برای تبادل کلید بین شخص فرستنده و گیرنده نیست. ما امنیت طرح خود را با تجزیه و تحلیل نظری و هیستوگرام اثبات کردیم. علاوه بر این، استحکام با دو معیار مختلف اندازه‌گیری شد که $PSNR$ و $SSIM$ هستند.

مراجع

[1] S. Mashhadi, and Z. Saeedi, *" A (t, n)-Secret image sharing with steganography based on Rook polynomial and LWE problem."* Multimedia Tools and Application, pp.1-21, 2023.

[2] T. Morkel, J.H. Eloff, and M.S. Olivier, *"An overview of image steganography"*. In ISSA, vol. 1, no. 2, pp. 1-11, 2005 .

[3] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, *"An image steganography approach based on k-least significant bits (k-LSB)"*, IEEE international conference on informatics, IoT, and enabling technologies (ICIoT) , pp. 131-135, 2020.

[4] M.M. Hashim , M.S.M. Rahim , F.A. Johi, *" Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats"*, International Journal of Engineering & Technology, vol. 7, no. 4, pp. 3505-3514, 2018.

[5] J. Riordan, *"Introduction to combinatorial analysis"*, Princeton University Press, 1980.

[6] S. Rajendran, and M. Doraipandian, *" Chaotic map based random image steganography using lsb technique"*. Int. J. Netw. Secur., vol. 19, no. 4, pp. 593-598, 2017.

[7] A. ALabaichi, M.A.A.A.K. Al-Dabbas, and A. Salih, *"Image steganography using least significant bit and secret map techniques."* International journal of electrical & computer engineering , vol. 10, no. 1, pp. 2088-8708, 2020.

پست الکترونیکی: zahra.saeediii74@gmail.com
پست الکترونیکی: smashhadi@iust.ac.ir