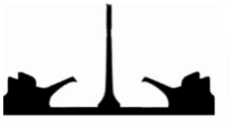
دسترسی در سایتِ http://jnrm.srbiau.ac.ir
سال هشتم، شماره سی و هشتم، مهر و آبان ۱۴۰۱
شماره شاپا: ۲۵۸۸X-۵۸۸



دانشگاه آزاد اسلامی، واحد علوم و تحقیقات

پژوهش‌های نوین در ریاضی

نهان نگاری اطلاعات در تصاویر ، بر اساس اختلاف مقادیر پیکسل‌ها در بلوک‌های ۱۶ پیکسلی

بشیر عمرانی هرزند[۱]، محمدرضا معتدل[۲*]، علی برومندنیا[۳]

[۱و۲] گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
[۲] گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

تاریخ ارسال مقاله: ۱۳۹۹/۱۰/۲۲ تاریخ پذیرش مقاله: ۱۴۰۰/۰۴/۱۳

چکیده

امروزه نهان‌نگاری به عنوان هنر یا تکنیکی برای پنهان کردن داده ها در رسانه های مختلف، کاربردهای بسیار متنوعی در مدیریت اطلاعات دارد. نهان‌نگاری می‌تواند در راستای انتقال یک پیام محرمانه، ارتقاء امنیت، دسته بندی اطلاعات، نگهداری اطلاعات خاص و... مورد استفاده قرارگیرد. تصویر یکی از محبوبترین رسانه‌های مورد استفاده در جریان پنهان‌سازی داده‌ها است و روش‌های مختلفی برای نهان‌نگاری اطلاعات در تصاویر وجود دارد که متداول‌ترین آنها روش جاسازی اطلاعات در بیت‌های کم ارزش تصویر می‌باشد و برای آن الگوریتم‌ها و روش‌های متنوعی ابداع شده است. یکی از این روش‌ها که مبنای ریاضی دارد، بهره‌گیری از محاسبه اختلاف مقادیر دو پیکسل همجوار درجهت شناسایی نقاط مناسب برای جاسازی اطلاعات محرمانه است. در این مقاله دو روش جدید برای نهان نگاری اطلاعات در تصاویر براساس محاسبه میزان تفاوت‌های مقادیر پیکسل‌های همجوار در بلوک‌های ۴×۴ پیشنهاد و بر روی تصاویر مختلف آزمایش و با استفاده از معیارهای ارزیابی میانگین مربعات خطا، نسبت پیک سیگنال به نویز و شاخص شباهت ساختاری مورد بررسی و تجزیه و تحلیل قرار گرفته است و ارزیابی‌ها نشان می‌دهد که یکی از روش‌های پیشنهادی به‌جهت داشتن نتایج بهتر و ظرفیت بیشتر جاسازی اطلاعات مطلوب‌تر می‌باشد.

واژه‌های کلیدی: نهان نگاری در تصویر، جایگزینی در بیتهای کم ارزش، جاسازی اطلاعات، نسبت پیک سیگنال به نویز، واترمارک، شباهت ساختاری.

* عهده‌دار مکاتبات: Email: dr.motadel@gmail.com

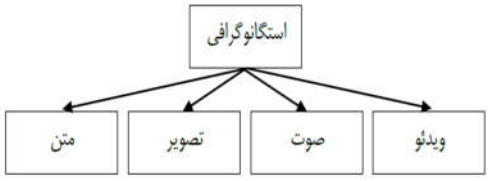
۱- مقدمه

در عصر اطلاعات و گسترش شبکه‌های جهانی، تامین امنیت و تضمین عدم دسترسی غیرمجاز به اطلاعات محرمانه از موضوعاتی است که از اهمیت فوق‌العاده‌ای برخوردار است. آگاهی رو به رشد کاربران از مقوله‌های اطلاعات و چگونگی دسترسی، تغییر و به اشتراک‌گذاری آنها از یک سو و سهولت دستکاری آنها در رسانه‌های مختلف مانند متن، تصویر، صوت و فیلم از سویی دیگر سبب می‌شود بحث امنیت و نگهداری اطلاعات به عنوان یکی از مقوله‌های مهم دنیای امروز اطلاعات باشد. با توجه به روند رو به رشد استفاده از اسناد دیجیتال در سازمان‌ها و موسسات کوچک و بزرگ که برای سهولت پاسخگویی به مخاطبین خود تصاویر اسناد و مدارک را نگهداری می‌نمایند امروزه مدیریت اسناد نقشی جدید و حیاتی در ارائه خدمات الکترونیکی ایفا می‌کند. اجرای موثر این سیستم‌ها یک عنصر مهم در ایجاد یک محیط کار مجازی و تغییر قابلیت‌های یک سازمان مدرن و نیروی کار آن است. بدیهی است اطلاعاتی که از طریق کانال‌های ناامن عبور می‌کنند می‌توانند براحتی رهگیری شوند بنابراین، استفاده از روشهای رمزنگاری و نهان-نگاری[۲] نقش مهمی در امنیت اطلاعات دارد. [۱]

یکی از مناسبترین راهکارهای افزایش امنیت اسناد الکترونیکی در برابر حملات منجر به تحریف یا تغییر اسناد الکترونیکی استفاده از نهان نگاری اطلاعات در اسناد مذکور است. نهان نگاری اطلاعات هزاران سال قدمت دارد. رساندن پیام‌های محرمانه یا دستورات نظامی به‌شکل پنهان در تمدن‌های قدیمی بسیار متداول بوده است و در طول تاریخ حسب فناوری‌های موجود شیوه‌های خاصی برای آن ابداع شده است. کهن‌ترین این روایات در یونان باستان است. زمانیکه پادشاه یونان برای ارسال یک پیام محرمانه موی سرغلامی را تراشید و پیام مورد نظر را برسر او خالکوبی نمود و وقتی موهای غلام به اندازه کافی رشد کرد او را عازم مقصد کرد.

در یک تعریف ساده نهان نگاری، هنر پنهان کردن اطلاعات در رسانه‌های دیجیتال مانند تصویر، صدا و متن است به‌عبارتی دیگر تکنیکی برای انتقال اطلاعات محرمانه بصورت نامحسوس است. [۲]

نهان نگاری برحسب رسانه، بر چهار نوع تقسیم بندی می‌شود که در شکل شماره (۱) انواع آن نمایش داده شده است. [۳]



شکل۱ . انواع نهان نگاری. [۳]

۲- مبانی نظری

اطلاعات به روشهای متفاوتی می‌توانند در تصویر مخفی شوند، ساده‌ترین و محبوب‌ترین روش موجود جایگزینی در بیت‌های کم ارزش[۳] تصویر نام دارد که به اختصار LSB گفته می‌شود. در این روش بیت-های پیام با ترتیبی مشخص، مستقیما در بیت‌های کم ارزش تصویر وارد می‌شود. ایجاد تغییر در بیت های کم ارزش یک تصویر با چشم انسان قابل تشخیص نیست. برای مخفی ساختن یک پیام درون یک فایل تصویر، نیاز به یک فایل تصویر پوشاننده مناسب است.

نهان نگاری شامل چند مرحله مختلف است و برای درک بهتر عملکرد آن باید ابتدا برخی از واژه هایی که در فرایندنهان‌نگاری مورد استفاده قرار می‌گیرد تعریف گردد:

[2] Steganography

[3] Least Significant Bit insertion

تصویر پوشش: تصویری است که جهت پنهان کردن پیام از آن استفاده می‌شود.

تصویر استگو (نهان نگاری شده): تصویر نهایی و خروجی فرایند نهان نگاری است.

پیام: عبارت از متنی است که باید در تصویر جاسازی شود.

کلید: رمزگذاری پیام، قبل از جاسازی در تصویر است. (اختیاری است)

فرایند جاسازی: به فرایند درج پیام درون تصویر به صورتی که قابل رویت نباشد اطلاق می‌گردد.

فرایند استخراج: به فرایند استخراج پیام یا متن پنهان شده از تصویر استگو اطلاق می‌گردد.

فرایند نهان نگاری در قالب رابطه ریاضی ذیل قابل تبیین است:

$$S = Em\ (C, M, K) \qquad (۱)$$

که در آن:

K: کلید M: پیام C: تصویر پوشش

و فرمول ریاضی استخراج پیام پنهان شده را می‌توان به شکل زیر نشان داد:

$$M = Ex\ (S, K) \qquad (۲)$$

که در آن:

k: کلید S: تصویر استگو

و کاملا بدیهی است که متن یا پیام بدست آمده از جریان استخراج (M) باید با پیام پنهان شده در تصویر یکسان باشد. [۴]

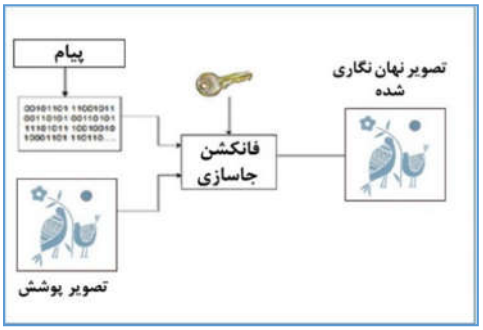
نهان‌نگاری بدلیل ماهیت پنهان‌سازی نامشهود اطلاعات در تصاویر می‌تواند راهکار مناسبی جهت افزایش امنیت تصاویر باشد. در یک نگاه کلی نهان نگاری سه بخش عمده دارد:

۱- متن یا پیام مخفی مورد نظر جهت پنهان سازی در تصویر.

۲- تصویری که مقرر است در آن پیام یا متن موردنظر جاسازی شود.

۳- فانکشن‌های جاسازی اطلاعات.

در شکل شماره (۲) نمایی کلی از فرایند نهان نگاری تصاویر نمایش داده شده است.



شکل۲. چارچوب کلی فرایند نهان نگاری. [۵]

نقطه مقابل نهان نگاری مبحث مهم دیگری تحت عنوان کشف پیامهای پنهان شده در رسانه‌هاست که به این فرایند اصطلاحا **استگانالیز**[4] گفته می‌شود که در واقع فرایند معکوس عمل نهان نگاری تصاویر است.

در یک جمع‌بندی کلی می‌توان گفت نهان نگاری یک تضمین نهایی برای تأیید اعتباری است که هیچ ابزار امنیتی دیگر نمی‌تواند از آن اطمینان حاصل کند و هدف اولیه تکنیک‌ها و روش‌های نهان‌نگاری به حداکثر رساندن نرخ جاسازی اطلاعات و به حداقل رساندن قدرت تشخیص و واکاوی تصاویر بر اساس روشهای رایج استگانالیز می‌باشد. [۶]

مزیت استفاده از نهان نگاری امکان رمزکردن و پنهان ساختن اطلاعات از دید کاربران به گونه ای است که بدون ابزار و برنامه‌های خاص امکان کشف آن وجود ندارد.

۳- پیشینه تحقیق

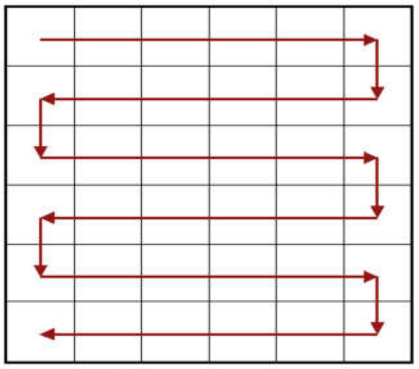
روش‌های متعدد و متنوعی در زمینه نهان نگاری

[4] Steganalysis

اطلاعات مبتنی بر جایگزینی در بیتهای کم ارزش وجود دارد که در این قسمت صرفاً به روش‌هایی که مبنای ریاضی داشته و براساس روش محاسبه اختلاف مقادیر خاکستری پیکسل‌های همجوار می‌باشد اشاره می‌شود.

۳-۱- روش اختلاف مقادیر پیکسل‌ها[5] (PVD)

در این روش که توسط تسایی و وو[6] ابداع شده است اختلاف دو پیکسل افقی همجوار در تصویر پوشش، جهت تعیین طول بیت‌های مخفی محاسبه می‌گردد. اختلاف مقادیر در بلوک‌های غیرهمپوشان دو پیکسلی تمام ردیف‌های تصویر، به صورت زیگزاگی مطابق شکل ۳ پیمایش و محاسبه می‌گردد. [۷]



شکل ۳. چگونگی پیمایش بلوک‌های دو پیکسلی. [۷]

تعداد بیت‌هایی که در دو پیکسل متوالی قابل جاسازی است، براساس میزان تفاوت و یک جدول محدوده تعریف شده توسط کاربر محاسبه می‌شود. اگر تفاوت (d_i) نزدیک به صفر باشد، آن یک بلوک در ناحیه‌ای صاف و اگر نزدیک به ۲۵۵ یا ۲۵۵- باشد در بخش لبه است.

فرض کنیم که P_i و P_{i+1} دو پیکسل متوالی در تصویر پوشش باشند و تفاوت آنها d_i از رابطه ۳ بدست می‌آید.

$$d_i=|p_i \quad p_{i+1}| \qquad (۳)$$

و تعداد بیت قابل جایگذاری n بر اساس فرمول زیر قابل محاسبه است و در آن u,l به عنوان مرزهای پایین و بالای محدوده تعریف شده است.

$$n=log_2(u-l+1) \qquad (۴)$$

از مقدار n برای به روز رسانی d از معادله زیر استفاده می‌کنیم.

$$d' = \begin{cases} l_k + b & \text{for } d \geq 0 \\ (l_k + b) & \text{for } d < 0 \end{cases} \qquad (۵)$$

مقادیر جدید p'_i و p'_{i+1} با استفاده از رابطه زیر ایجاد می‌گردد.

در این رابطه m تفاوت,d' d می‌باشد.

$$(p'_i, p'_{i+1}) = \begin{cases} \left(p_i \quad \frac{m}{2}, p_{i+1} + \frac{m}{2}\right) \\ \left(p_i \quad \frac{m}{2}, p_{i+1} + \frac{m}{2}\right) \end{cases}$$

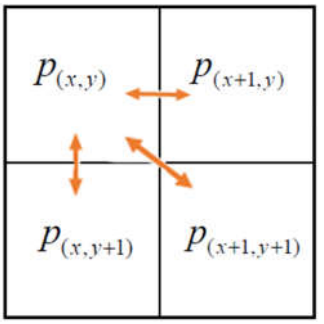
چن سال بعد نسخه اصلاح شده‌ای از این روش توسط این پژوهشگران ارائه شد که در آن از جدولی شامل دو بخش پایینی و بالایی در مراحل محاسبه اختلاف ارزش پیکسل‌ها استفاده شده است. تفاوت‌های کوچک و بزرگ به ترتیب نشان دهنده مناطق صاف و لبه در تصویر هستند.

برای عمل جایگذاری در نواحی صاف از روش جایگزینی در ۳ بیت کم ارزش اول و در نواحی لبه از روش قبلی استفاده شده شده و نتایج حاکی از بهبود مقدار PSNR و در نتیجه افت کمتر کیفیت تصویر نسبت به روش قبل است. نتایج آزمون این روش بر روی سه تصویر استاندارد، در جدول ۳ نمایش داده شده است. [۸]

[5] Pixel Value Differencing
[6] Tsai & Wu

۳-۲- روش مبتنی بر اختلاف پیکسل‌های همجوار افقی، عمودی و قطری در بلوک‌های ۲×۲

این روش توسط چانگ و همکارانش ارائه گردیده است. رویکرد این پژوهشگران استفاده از محاسبه اختلاف مقادیر ۳ زوج پیکسل واقع در یک بلوک ۲×۲ همانند شکل ۴ بوده است. ابتدا میزان تفاوت مقادیر پیکسل‌های همجوار افقی، عمودی و قطری محاسبه شده است و تفاوت‌های بدست آمده با مقادیر محدوده تعریف شده (شکل ۵) مقایسه می‌گردد و حسب اینکه هر یک از تفاوت‌ها متعلق به کدام ناحیه باشد مقدار حداقل آن محدوده انتخاب و با جریان بیتی پیام مورد نظر ترکیب و تفاوت جدید را ایجاد می‌نماید. [۹]



شکل۴. بلوک ۲ × ۲

$$d1=P(x,y) - p(x,y+1)$$
$$d2=P(x,y) - p(x+1,y+1) \qquad (۷)$$
$$d3=P(x,y) - p(x+1,y)$$

بسته به اینکه مقدار dها در کدام ناحیه محدوده تعریف شده (شکل ۵) قرار بگیرد مقدار بیت قابل جاسازی از پیام مشخص می‌گردد. برای تعیین نقاط جدید نیز از فرمول ۸ استفاده می‌گردد:

$$(P'_i ,P'_{i+1}) = (p_{i-} \frac{m}{2} , p_{i+1}+ \frac{m}{2}) \qquad (۸)$$
$$m=d'_i-d_i$$

R1	R2	R3	R4	R5	R6
0 7	8 15	16 31	32 63	64 127	128 255

شکل ۵. بخش‌بندی محدوده‌ها

نتایج آزمون این روش بر روی سه تصویر استاندارد در جدول ۳ نمایش داده شده است.

۳-۳- روش مبتنی بر محاسبه اختلاف مقادیر چهار پیکسل غیر همپوشان متوالی افقی

این روش توسط لیائو و همکارانش[۷] ارائه شده است. در این روش ۴ پیکسل غیرهمپوشان بصورت افقی در یک تصویر پوشش خاکستری ۲۵۶ بیتی در نظر گرفته شده است و مقدار D بر اساس فرمول زیر برای ۴ پیکسل متوالی $(p_i , p_{i+1} , p_{i+2} , p_{i+3})$ چنین محاسبه می‌گردد. [۱۰]

$$D=\frac{1}{3}\sum_{i=0}^{3}(p_i-p_m)^2 \qquad (۹)$$
$$p_m=\min(p_i,p_{i+1},p_{i+2},p_{i+3})$$

تعداد بیت‌های جاسازی n از مقایسه D با مقدار آستانه از قبل تعیین شده T تعیین می‌شود. بسته به اختلاف‌های یک ناحیه صاف یا لبه، بیت‌های جاسازی متفاوت هستند.

سطح پایین و سطح بالا n_l و n_h با چنین مفروضاتی در نظر گرفته شده است.

$$n = \begin{cases} n_l & \text{if } D \le T \\ n_h & \text{if } D > T \end{cases} \qquad (۱۰)$$

آستانه T و سطوح مرزی، شرایط $2^{n_l} \le T \le 2^{n_h}$ و $1 \le 2^{n_l} , 2^{n_h} \le 5$ را برآورده می‌کند.

اگر زیربلوک مد نظر زیربلوک خطا نباشد، جاسازی n بیت برای پیکسل‌های $(p_i^1 , p_{i+1}^1 , p_{i+2}^1 , p_{i+3}^1)$ صورت گرفته و سپس محاسبه LSB اصلاح شده انجام می‌پذیرد.

$(p_i^2 , p_{i+1}^2 , p_{i+2}^2 , p_{i+3}^2)$

[7] Liao et al

و بالاخره پیکسل‌های $(p'_i , p'_{i+1}, p'_{i+2}, p'_{i+3})$ در روند تنظیم مجدد قرار می‌گیرند.
پیکسل‌های جدید نباید از بلوک خطا باشند و تفاوت میانگین جدید D' برای $(p^1_i , p^1_{i+1}, p^1_{i+2}, p^1_{i+3})$ پیکسل‌های در سطح D باشند. در نهایت مقدار M بر اساس روش LSB اصلاح شده مورد استفاده قرار گرفته مطابق فرمول زیر انتخاب می‌شود.

$$M=\frac{1}{3}\sum_{i=0}^{3}(p'_i-p_i)^2 \qquad (۱۱)$$

نتایج آزمون این روش بر روی سه تصویر استاندارد در جدول ۳ نمایش داده شده است.

۳-۴- روش مبتنی بر محاسبه اختلاف مقادیر پیکسل‌های همجوار در بلوک‌های ۳×۳

در این روش که توسط گانداربا سواین[8] ارائه شده است، هدف اصلی ایجاد ظرفیت جاسازی بالاتر اطلاعات، با استفاده از محاسبه تفاوت مقادیر ۹ پیکسل با جایگزینی LSB اصلاح شده می‌باشد. در روش مذکور ابتدا تصویر به بلوک‌های ۳×۳ غیرهمپوشان همانند الگوی نمایش داده شده در شکل (۶) تقسیم می‌شود. [۱۱]

X_0	X_1	X_2
X_3	X_4	X_5
X_6	X_7	X_8

شکل ۶. بلوک ۳×۳. [۱۱]

و در هر بلوک میانگین تفاوت مقادیر پیکسل‌ها بر اساس فرمول زیر محاسبه می‌شود.

$$d=\frac{1}{8}\sum_{i=1}^{8}|x_i \quad x_{min}| \qquad (۱۲)$$

x_{min} حداقل x_i هاست.
براساس این مقدار، بلوک در یکی از سطوح چهار گانه: سطح پایین، نزدیک به متوسط، بالاتر از متوسط و بالا دسته‌بندی می‌شود. اگر d<=7 باشد بلوک متعلق به سطح پایین بوده و از روش جایگزینی در ۲ بیت کم ارزش در آن استفاده می شود. اگر 8≤d≤15 باشد در سطح نزدیک به متوسط بوده و از روش جایگزینی در ۳ بیت کم ارزش در آن استفاده می‌شود.
چنانچه 16≤d≤31 باشد در سطح بالاتر از متوسط قرار گرفته و از روش جایگزینی در ۴ بیت کم ارزش در آن استفاده می‌شود و نهایتاً اگر d≥32 باشد در سطح بالا خواهد بود و روش جایگزینی در ۵ بیت کم ارزش برای آن استفاده می‌شود. پس از جایگذاری‌ها، مقادیر پیکسل برای تعدیل اصلاح می‌شوند تا بیتهای تعبیه شده را مختل نکنند.
نتایج تجربی نشان می‌دهد که نهان نگاری تصاویر غیر قابل تشخیص بوده و ظرفیت پنهان سازی اطلاعات نیز بیشتر شده است.

۳-۵- روش ترکیبی اختلاف پیکسلهای همجوار و بهینه سازی ازدحام ذرات در بلوکهای ۲×۲

این روش توسط ژائوتونگ لی و یینگ هه [9] ارائه شده است که در آن، از یکی از الگوریتم‌های تکاملی و فرا ابتکاری تحت عنوان بهینه‌سازی ازدحام ذرات[10] استفاده شده است.
شیوه عملکرد این الگوریتم که از رفتار ماهی‌ها و پرندگان الهام گرفته شده جستجوی راه حل بهینه از طریق یک فرایند تکراری مبتنی بر راه حل‌های تصادفی و انتخاب مقادیر مناسب است و مهمترین ویژگی این الگوریتم، داشتن حافظه است. به گونه‌ای

[8] Gandharba Swain

[9] Zhaotong Li & He Ying
[10] particle swarm optimization

که این الگوریتم قادر است بهترین موقعیت تاریخی ذره‌ها را حفظ و به ذرات دیگر منتقل نماید. [۱۲]
گام‌های اصلی این روش ترکیبی بدین شرح است:
ابتدا تصویر پوشش به بلوک‌های ۲×۲ غیرهمپوشان تقسیم می‌شود و پیکسل‌ها برحسب مقدار از کمترین تا بیشترین به صورت g3,g2,g1,g0 در نظر گرفته می‌شود.
اختلاف مقادیر پیکسل‌ها به شکل زیر محاسبه می‌شود:

$$d_i = g_i - g_0 \qquad i=1,2,3 \qquad (۱۳)$$

تعداد بیت قابل جاسازی از پیام از رابطه زیرقابل محاسبه است:

$$w_{ki} = u_{ki} \quad l_{ki} + 1 \quad , \quad i=1,2,3 \qquad (۱۴)$$

با حل معادله شماره ۱۵ پارامترهای بهینه‌سازی ازدحام ذرات مقداردهی اولیه می‌گردد.

$$\begin{cases} (g'_1 + g'_0) \mod 2^{t1} = b_1 \\ (g'_2 + g'_0) \mod 2^{t2} = b_2 \\ (g'_3 + g'_0) \mod 2^{t3} = b_3 \end{cases} \qquad (۱۵)$$

که در آن:

$$t_i = log_2(w_{ki}) \qquad i = 1,2,3$$

و b_i مقدار دسیمال t_i است.
پروسه تعیین ذرات بهینه با توجه به فانکشن اول (f1) انجام می‌شود و اگر خروجی این فانکشن صفر باشد پروسه با فانکشن دوم (f2) و در غیر این صورت با فانکشن اول مجدد انجام و ادامه می‌یابد.
ذرات بهینه با توجه به حداکثر مقدار محاسبه شده در فانکشن دوم محاسبه شده و نهایتاً ذرات بهینه جدید برای جایگزینی در پیکسل‌ها بدست می‌آید.

$$f1 = |(g'_1 + g'_0) \mod 2^{t1} \quad b_1| + |(g'_2 + g'_0) \mod 2^{t2} \quad b_2| + |(g'_3 + g'_0) \mod 2^{t3} \quad b_3|$$

و

$$f2 = 10\, log_{10}\left(\frac{255^2}{MSE}\right) \qquad (۱۶)$$

نتایج آزمون این روش بر روی سه تصویر استاندارد در جدول ۳ نمایش داده شده است.

۳-۶. روش مبتنی بر اختلاف پیکسل‌های همجوار در بلوک‌های ۲×۲

بهویان و همکارانش در سال ۲۰۱۸ ویرایش جدیدی از الگوریتم محاسبه اختلاف مقادیر پیکسلها برای نهان نگاری ارائه نمودند. این پژوهشگران قبل از عملیات نهان نگاری، پیام را رمزگذاری و نرمالسازی کرده و سپس تصویر را به بلوک‌های ۲×۲ تقسیم نموده و تفاوت‌های مقادیر افقی، عمودی و قطری پیکسل‌های همجوار واقع در بلوک‌های مذکور را محاسبه کرده‌اند و از مقادیر بدست آمده برای جاسازی اطلاعات بر اساس دو جدول ثابت ۴ یا ۳ بیتی (جداول ۱ و ۲) که تعیین کننده محدوده‌های بالایی یا پایینی است استفاده نموده‌اند. [۱۳]

جدول ۱. تعریف محدوده های بالا و پایین (۴ بیتی). [۱۳]

Lower= [0 16 32 48 64 80 96 112 128 144 160 176 192 208 224 240]
Upper = [15 31 47 63 79 95 111 127 143 159 175 191 207 223 239 255]

جدول ۲. تعریف محدوده‌های بالا و پایین (۳ بیتی). [۱۳]

Lower = [0 8 16 24 32 40 48 56 64 72 80 88 96 104 112 120 128 136 144 152 160 168 176 184 192 200 208 216 224 232 240 248]
Upper = [7 15 23 31 39 47 55 63 71 79 87 95 103 111 119 127 135 143 151 159 167 175 183 191 199 207 215 223 231 239 247 255]

در صورتیکه مقادیر d بین بخش‌های پایین و بالای تعریف شده در جداول فوق باشد ۳ بیت از پیام رمزگذاری شده (bi) جایگذاری می‌شود و مقدار جدید d نیز براساس فرمول ۱۷ تعیین می‌گردد.

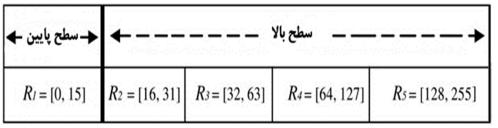
$$nd(i) = lower(j) + dec(bi) \qquad (۱۷)$$

و این عمل تا پایان بلوکهای تصویر ادامه می‌یابد.
نتایج آزمون این روش بر روی سه تصویر استاندارد در جدول ۳ نمایش داده شده است.

۴- روش پیشنهادی

در این مقاله دو روش جدید همراه با الگوریتم‌های اجرایی آن، برای جاسازی پیام در تصویر ارائه می‌گردد. از مهمترین ویژگی‌های روش‌های پیشنهادی می‌توان به محاسبات نسبتاً آسان و امکان جاسازی مقادیر زیادی از داده‌ها بدون افت کیفیت تصاویر اشاره کرد. در هر دو روش ارائه شده، جاسازی اطلاعات براساس محاسبه اختلاف مقادیر پیکسل‌های دوتایی همجوار افقی، عمودی و قطری در بلوک‌های ۴×۴ تصویر می‌باشد.

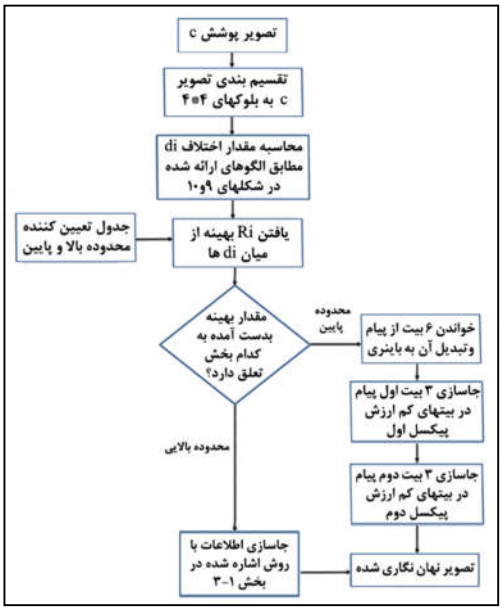
روش کار بدین شرح است که ابتدا تصویر پوشش در قالب بلوک‌های ۴×۴ غیرهمپوشان در نظر گرفته می‌شود و مقدار اختلاف زوج پیکسل‌هایی که بصورت افقی، عمودی یا قطری در کنار یکدیگر می‌توانند قرار بگیرند محاسبه می‌گردد. پیمایش الگوریتم در سطرهای ۴ پیکسلی از سمت چپ به راست انجام می‌شود. همانگونه که در شکل‌های ۹ و ۱۰ نشان داده شده است در هر بلوک ۴×۴ اختلاف مقادیر زوج پیکسل‌های همجوار در جهات افقی و عمودی (روش اول) یا جهات افقی، عمودی و قطری (روش دوم) محاسبه می‌شود. مقدار اختلاف زوج پیکسل‌ها d_i عددی بین ۰ تا ۲۵۵ است اگر این مقدار عددی کوچک باشد منطقه ای صاف و در غیر اینصورت منطقه لبه است. باتوجه به محدودیت‌های بینایی انسان نهان‌نگاری مطلوب اطلاعات معمولاً در منطقه لبه انجام می‌پذیرد. جدولی برای تفکیک این دو بخش تحت عنوان سطح پایین و بالا در نظر می‌گیریم. (شکل ۷)



شکل ۷. تفکیک دو بخش بالا و پایین با D=15

با یافتن مقدار بهینه اختلاف مقادیر برای هر بلوک و در نظر گرفتن اینکه این مقدار به بخش بالا یا پایین جدول تعلق داشته باشد شیوه جاسازی اطلاعات متفاوت خواهد بود. اگر به بخش بالا تعلق داشته باشد به همان شیوه اشاره شده در بخش ۱-۳ انجام می‌پذیرد و اگر به بخش پایین تعلق داشته باشد۶ بیت از جریان داده پیام خوانده شده و سپس در دوپیکسل همجوار جاسازی می‌گردد.

در شکل ۸ دیاگرام چگونگی عملکرد روش پیشنهادی نمایش داده شده است.



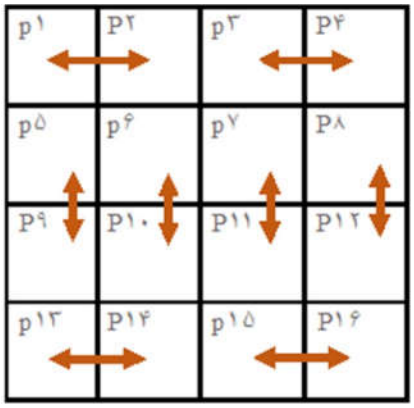
شکل ۸. دیاگرام روش پیشنهادی

۴-۱- الگوریتم جاسازی اطلاعات (روش پیشنهادی اول)

گام ۱. تصویر ورودی با ابعاد M×N را با چیدمان تفکیکی سطرهای ۴ پیکسلی در کنار هم در نظر می‌گیریم، بنابراین تصویر را می‌توانیم به‌صورت L=(M×N)/4 نشان دهیم. درنتیجه تصویر را می‌توان L×۴ فرض نمود.

گام ۲. تصویر با اندازه L×۴ را به بلوک‌های ۴×۴ غیرهمپوشان تقسیم‌بندی می‌نماییم.

گام ۳. لبه‌های افقی و عمودی هر بلوک ۴×۴ جهت جاسازی پیام و براساس محاسبه مقادیر اختلاف دو پیکسل همجوار (افقی یا عمودی) مطابق الگویی که در شکل شماره ۹ نشان داده شده است در نظر می‌گیریم.



شکل ۹. الگوی انتخاب پیکسل‌ها در روش پیشنهادی اول

محاسبات مربوط به شکل ۹:

برای هرزوج پیکسل همجوار افقی مطابق فرمول زیر:

$$d_i=|p_i \quad p_{i+1}| \quad i=1,3,13,15 \qquad (۱۸)$$

و برای زوج پیکسل‌های همجوار عمودی طبق فرمول زیر:

$$d_i=|p_i \quad p_{i+4}| \quad i=5,6,7,8 \qquad (۱۹)$$

گام ۴. یافتن مقدار بهینه Ri از d_iها به گونه‌ای که Ri=min(ui-k) و با شرایط زیر:

ui>k و k=$|d_i|$ و Ri ∈ [li,ui] و بهینه Ri برای تمام مقادیر 1≤i≤n می‌باشد. طول پیام یک واحد بیشتر از تفاضل li و ui است.

گام ۵. اگر Ri متعلق به سطح بالا باشد جاسازی داده‌ها با همان شیوه معمولی اشاره شده در بخش ۱-۳ اتفاق می‌افتد. در غیر اینصورت ابتدا پیام به باینری تبدیل و سپس ۶ بیت از جریان داده آن خوانده می‌شود و به روش 3-LSB در پیکسل‌ها جاسازی می‌گردد. (۳ بیت اول پیام، جایگزین ۳ بیت کم ارزش پیکسل اول و ۳ بیت دوم پیام، جایگزین ۳ بیت کم ارزش پیکسل دوم می‌گردد)

گام ۶. تکرار مراحل ۳ تا ۵ تا پایان بلوک‌ها.

۴-۲- الگوریتم استخراج پیام مخفی (روش پیشنهادی اول)

گام ۱. تقسیم تصویر استگو به بلوک‌های ۴×۴ مشابه روش تقسیم‌بندی در فرایند جاسازی اطلاعات.

گام ۲. محاسبه مقدار d'_i براساس فرمول‌های زیر برای پیکسل‌های همجوار افقی و عمودی مطابق با الگوی نمایش داده شده در شکل ۹.

محاسبات برای هر زوج پیکسل همجوار افقی مطابق فرمول زیر:

$$d'_i=|p'_i \quad p'_{i+1}| \quad i=1,3,13,15 \qquad (۲۰)$$

و برای زوج پیکسلهای همجوار عمودی مطابق فرمول زیر:

$$d'_i=|p'_i \quad p'_{i+4}| \quad i=5,6,7,8 \qquad (۲۱)$$

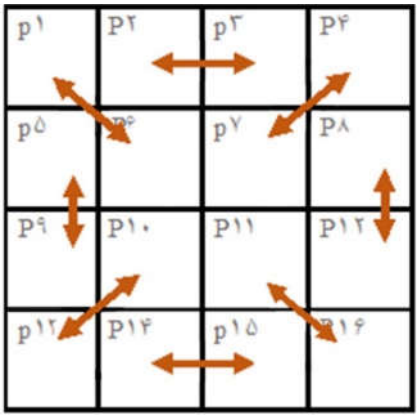
گام ۳. یافتن مقدار بهینه Ri از d'_i با توجه به تقسیم‌بندی تعیین شده در خصوص سطوح بالا و پایین (شکل ۷). اگر Ri متعلق به سطح بالا باشد

استخراج اطلاعات مخفی با استفاده از روش اشاره شده در بخش ۱-۳ انجام می‌شود و در غیر اینصورت گام ۴ اجرا می‌گردد.

گام ۴. بطور مستقیم ۳ بیت اول مربوط به p'_i و p'_{i+1} از تصویر استگو استخراج می‌گردد تا ۳ بیت دوم مربوط به p'_i و p'_{i+1} با اطلاعات پنهان شده نمایش داده شود.

۴-۳- الگوریتم جاسازی و استخراج پیام (روش پیشنهادی دوم)

الگوریتم‌های جاسازی اطلاعات و استخراج پیام در روش دوم مشابه الگوریتم روش پیشنهادی اول است با این تفاوت که در روش پیشنهادی دوم علاوه بر پیکسل‌های همجوار عمودی و افقی، از پیکسل‌های همجوار قطری نیز به گونه ای که در شکل ۱۰ نشان داده شده استفاده شده است.



شکل۱۰. الگوی انتخاب پیکسل‌ها درروش پیشنهادی دوم

و محاسبات مربوط به یافتن مقادیر اختلاف دو پیکسل نیز چنین می‌باشد. برای زوج پیکسل‌های همجوار قطری مطابق فرمول‌های زیر:

$$d_i=|p_i \quad p_{i+5}| \quad i=1,11 \qquad (۲۲)$$
$$d_i=|p_i \quad p_{i+3}| \quad i=4,10$$

و برای هر زوج پیکسل همجوار افقی و عمودی مطابق فرمول‌های زیر:

$$d_i=|p_i \quad p_{i+1}| \quad i=2,14 \qquad (۲۳)$$
$$d_i=|p_i \quad p_{i+4}| \quad i=5,8$$

۵- معیارهای بررسی و نتایج

برای بررسی و تجزیه تحلیل الگوریتمهای ارائه شده از سه معیار نسبت پیک سیگنال به نویز، میانگین مربع خطاها و شباهت ساختاری استفاده شده است.

معیار MSE میانگین مربعات خطای بین تصویر پوشش و تصویر استگو می‌باشد و فرمول آن به شکل زیر است.

$$\mathrm{MSE} = \frac{1}{M\ N} \sum_{i=1}^{M} \sum_{i=1}^{N} (c_{i,j} \quad s_{i,j})^2 \qquad (۲۴)$$

که در آن M وN به ترتیب تعداد پیکسلهای افقی و عمودی تصویر اولیه و $C_{i,j}$ و $S_{i,j}$ به ترتیب مقادیر پیکسل‌های تصویر پوشش و تصویر استگو یا تصویر نهان نگاری شده هستند.

معیار نسبت پیک سیگنال به نویز (PSNR) برای سنجش کیفیت تصویر خروجی (نهان نگاری شده) مورد استفاده قرار می‌گیرد و فرمول آن به صورت زیر تعریف شده است.

$$\mathrm{PSNR} = 10 \quad log_2 \frac{max^2}{MSE} \ db \qquad (۲۵)$$

که درآن متغیر max مقدار حداکثری ارزش بیتی پیکسلها برحسب عمق بیتی است (مثلا برای یک تصویر با عمق بیتی ۸ مقدار آن حداکثر ۲۵۵ است).

معیار SSIM شباهت ساختاری بین دو تصویر پوشش و استگو را با مقایسه روشنایی، کنتراست و ساختار دو تصویر انجام می‌دهد. این مقایسه به صورت محلی در بلوک‌های متناظر دو تصویر انجام می‌شود. اگر xو y بلوک‌های محلی متناظر در دو تصویر پوشش و استگو باشند، توابع مقایسه روشنایی و کنتراست و ساختار به صورت روابط زیر تعریف می‌شوند.

$$\mathrm{L(x,y)} = \frac{2\mu_x \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \qquad (۲۶)$$

$$\mathrm{C(x,y)} = \frac{2\sigma_x \sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \qquad (۲۷)$$

$$S(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x \sigma_y + C_3} \quad (۲۸)$$

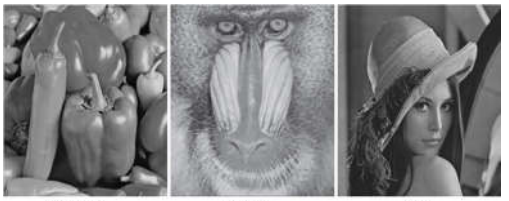
C_1 و C_2 و C_3 مقادیر ثابتی هستند که از ناپایداری معادله‌ها در زمانی که مخرج کسر مقدار کوچکی است، جلوگیری می‌کنند.

μ_x و μ_y میانگین مقادیر پیکسل‌ها، σ_x و σ_y انحراف معیار و σ_{xy} کواریانس x و y می‌باشد و نهایتاً برای محاسبه شباهت ساختاری بین دو تصویر از رابطه ذیل استفاده می‌شود.

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (۲۹)$$

با توجه به انجام آزمون‌های فوق و اجرای آن با نرم افزار متلب ۲۰۱۸ بر روی تصاویر استانداردی که به طور معمول در پژوهش‌های نهان نگاری مورد استفاده قرار می‌گیرد (تصاویر نمایش داده شده در شکل ۱۱)، نتایج حاصله حاکی از میزان قابل قبول PSNR و SSIM و افزایش مطلوب ظرفیت جاسازی اطلاعات است.

از طرفی باتوجه به اینکه در روش‌های پیشنهادی از پیمایش ۴ سطری و بلوک‌های ۴×۴ استفاده شده است می‌تواند از سرعت مناسبتری نیز نسبت به روش‌های قبل برخوردار باشد.



شکل ۱۱. تصاویر پوشش استفاده شده در آزمون

در جداول ۳ و ۴ به ترتیب نتایج پژوهش‌های قبل و نتایج روش‌پیشنهادی جهت مقایسه ارائه شده است.

جدول ۳. مقایسه نتایج روش‌های پیشنهادی با سایر روش‌ها بر روی سه تصویر لنا، بابون و فلفل

تصویر پوشش	روش تسایی– وو [۷]		روش چانگ و همکاران [۹]		روش لیائو و همکاران [۱۰]		روش ژائوتونگ و یینگ [۱۲]		روش بهویان و همکاران [۱۳]	
	ظرفیت	PSNR	ظرفیت	PSNR	ظرفیت	PSNR	ظرفیت	PSNR	ظرفیت	PSNR
Lena	۵۰۹۶۰	۴۱.۷۹	۷۵۸۳۶	۳۸.۸۹	۵۶۱۷۴۰	۴۱.۴۸	۵۶۱۷۴۰	۴۲.۷۴	۷۴۰۴۷	۳۸.۹۱
Baboon	۵۶۲۹۱	۳۷.۹۰	۸۲۴۰۷	۳۳.۹۳	۶۹۱۷۳۵	۳۵.۶۱	۵۹۱۷۳۵	۳۶.۶۳	۷۴۰۴۷	۳۹.۳۰
Peppers	۵۰۶۸۵	۴۱.۷۳	۷۵۵۷۹	۳۸.۵۰	۵۶۲۲۴۹	۴۱.۲۸	۵۶۲۲۴۹	۴۲.۴۵	۷۴۰۴۷	۳۹.۱۵

جدول ۴. نتایج دو روش پیشنهادی

تصویر پوشش	روش پیشنهادی اول			روش پیشنهادی دوم		
	ظرفیت	PSNR	SSIM	ظرفیت	PSNR	SSIM
Lena	۵۲۲۲۸۱	۳۹.۲۱	۰.۹۸۰۳	۵۱۸۶۲۴	۳۸.۹۴	۰.۹۸۰۱
Baboon	۵۳۱۶۶۵	۳۶.۱۳	۰.۹۸۱۹	۵۲۸۰۰۸	۳۵.۹۹	۰.۹۸۱۱
Peppers	۵۲۸۱۹۱	۳۷.۷۴	۰.۹۸۴۹	۵۲۴۵۳۲	۳۷.۵۵	۰.۹۸۴۶

درخصوص تجزیه و تحلیل نتایج بدست آمده در این پژوهش اشاره به این نکات ضرورت دارد. همانگونه که در ابتدای بخش ۵ و در معرفی معیارهای ارزیابی آزمونهای این پژوهش دیده می‌شود، معیار PSNR با معیار MSE رابطه معکوس دارد، یعنی هر چقدر میانگین مربعات خطای بین دو تصویر اولیه و تصویر نهان نگاری شده کمتر باشد طبیعتا مقدار PSNR افزایش می‌یابد و هر چقدر این مقدار بیشتر باشد نشان از کمتر بودن افت کیفیت تصویر، پس از فرایند نهان‌نگاری دارد و پژوهشگران با تلاش‌های مستمر به ایجاد الگوریتم‌های ابتکاری و یا بهبود الگوریتم‌های موجود برای جاسازی اطلاعات، در جهت افزایش مقدار این معیار ارزیابی هستند.

مقدار معیار SSIM که شباهت ساختاری بین تصویر اولیه و تصویر نهان نگاری شده را با توجه به سه ویژگی بسیار مهم روشنایی، کنتراست و ساختار در دو تصویر بررسی می‌کند، عددی بین ۰و۱ است که هر چه این عدد به ۱ نزدیکتر باشد نشان دهنده شباهت بیشتر دو تصویر و به عبارتی افت کمتر کیفیت می باشد و به عنوان مثال برای دو تصویر دقیقاً یکسان مقدار این شاخص عدد ۱ خواهد بود.

مقادیر بدست آمده برای این معیار در هر دو روش ارائه شده در این مقاله، بیش از ۰.۹۸ است و این حاکی از شباهت ساختاری مناسب بین تصاویر قبل و بعد از نهان نگاری است و به این مفهوم که اجرای روش‌های ارائه شده اختلالی در کیفیت تصاویر ایجاد نمی‌نماید.

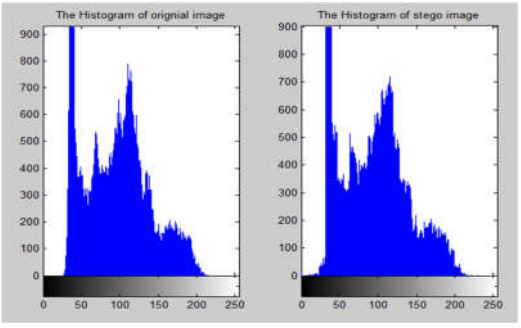
در مجموع با توجه به مقادیر بدست آمده و با ارزیابی از طریق معیارهای فوق، می‌توان اذعان داشت که روش‌های پیشنهادی در قیاس با سایر روش‌ها از مطلوبیت نسبی برخوردار است و در این بین، روش پیشنهادی اول در مقایسه با روش دوم به جهت داشتن نتایج مناسب‌تر، روش بهینه‌تری محسوب می‌گردد.

یکی دیگر از روشهای ارزیابی رایج در مبحث نهان نگاری، بررسی افت کیفیت تصاویر نهان نگاری شده با استفاده از ترسیم نمودار هیستوگرام تصاویر قبل و بعد از جاسازی اطلاعات است.

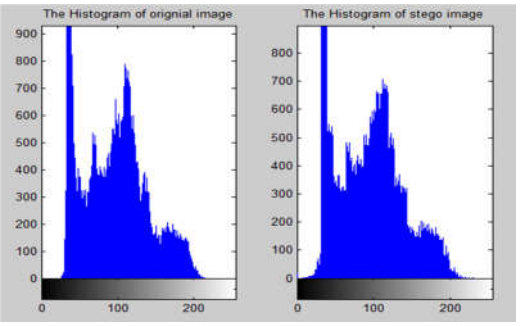
کاملا طبیعی است که پس از قرارگیری اطلاعات در درون نقاط مختلف یک تصویر، در بخش‌هایی از تصویر تفاوتهایی ایجاد می‌گردد که هر چه این تفاوتها بیشتر باشد باعث افت بیشتر کیفیت تصویر می‌گردد. نقطه قوت روش‌ها و الگوریتم‌هایی که توسط محققان ابداع می‌شود، پنهان‌سازی اطلاعات در نقاطی است که کمترین اختلال را در تصویر ایجاد نماید.

با ترسیم و مقایسه هیستوگرامهای هر تصویر ، قبل و بعد از نهان‌نگاری این مساله را می‌توان به سادگی بررسی نمود.

در شکل‌های ۱۲ و ۱۳ مقایسه هیستوگرام تصویر لنا، قبل و بعد از عمل نهان نگاری با روش‌های پیشنهادی اول و دوم نمایش داده شده است. در اینجا نیز مشاهده می‌شود که هیستوگرام تصویر قبل و بعد از جاسازی اطلاعات در روش پیشنهادی اول از شباهت بیشتری نسبت به روش پیشنهادی دوم برخوردار است.



شکل ۱۲. مقایسه هیستوگرام تصویر لنا قبل و بعد از جاسازی اطلاعات به روش پیشنهادی اول



شکل ۱۳. مقایسه هیستوگرام *تصویر* لنا قبل و بعد از جاسازی اطلاعات به روش پیشنهادی دوم

۶- نتیجه‌گیری

در مجموع با توجه به بررسی‌ها و تحلیل‌های انجام شده و در نظر گرفتن نتایج بدست آمده و ارزیابی مقادیر معیارهایی چون: نسبت پیک سیگنال به نویز، ظرفیت و شاخص شباهت ساختاری در دو روش پیشنهادی و همچنین قیاس هیستوگرام‌های تصاویر منتخب، قبل و بعد از عمل نهان‌نگاری، روش پیشنهادی اول، مناسب‌تر و بهینه‌تر از روش پیشنهادی دوم می‌باشد.

فهرست منابع

[1] A. Soria-Lorente, S. Berres, "A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information," *Security and Communication Networks,* (2017), p. 1.

[2] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," *I. J. Computer Network and Information Security,* (2019), p. 11.

[3] Madhuri R. Shende, Amit Welekar, "Advanced Steganography for Hiding Data and Image using Audio-Video," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 4, no. 1, (2016), p. 112.

[4] Hayat Al-Dmour , Ahmed Al-Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding," *Expert Systems with Applications,* (2015), p. 3.

[5] Fouroozesh, zohreh. "Image Steganography based on LSB in Spatial Domain, "Master Thesis, (2014), p. 9.

[6] Sumeet Kaur, Savina Bansal ,R. K. Bansal,"Steganography and Classification of Image Steganography Techniques," *International Conference on Computing for Sustainable Global Development, (*2014), p. 871.

[7] Da-Chun Wu, Wen-Hsiang Tsai, "A Steganographic method for images by pixel-value differencing" *Pattern Recognition Letters,* (2003), pp. 1615-1617.

[8] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *Image Signal Process,* vol. 152, no. 5, (2005), pp. 612-613.

[9] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing" *Journal of Mulyimedia,* vol. 3, no. 2, (2008), pp. 39-40.

[10] Xin Liao, Qiao-yan Wen, Jie Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image R., (*2011), p. 2.

[11] G. Swain, "Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution," *Indian Journal of Science and Technology,* vol. 7, (2014), p. 1445.

[12] Zhaotong Li, Ying He, "Steganography with pixel-value differencing and modulus function based on PSO," *Journal of Information Security and Applications, (*2018), pp. 48-49.

[13] Sharif Shah Newaj Bhuiyan, Norun Abdul Malek, Othman Omran Khalifa, "An Improved Image Steganography Algorithm based on PVD," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 10, no. 2, (2018), pp. 571-573.