نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۲، تابستان ۱۳۹۸، ص ۳۹-۳۳

افزایش ظرفیت درج و مقاومت در مخفی‌نگاری تصاویر با استفاده از نگاشت و کاهش بیت‌ها

یعقوب خراسانی[۱]، جلیل مظلوم[۲*]، محمد شایسته‌فرد[۳]
۱- کارشناس ارشد مهندسی مخابرات، ۲- دانشیار، دانشگاه علوم و فنون هوایی شهید ستاری،
۳- کارشناس ارشد مهندسی مخابرات، دانشگاه آزاد اسلامی شاهرود، ایران
(دریافت: ۹۷/۰۲/۰۲، پذیرش: ۹۷/۰۷/۲۱)

چکیده

در تمام الگوریتم‌های نهان‌نگاری، ظرفیت درج اطلاعات و مقاومت تصویر نهایی در برابر روش‌های نهان‌کاوی مورد توجه می‌باشد. از این رو در این مقاله روشی ارائه خواهد شد که نه تنها ظرفیت بالایی برای درج دارد، بلکه مقاومت بالایی درمقابل روش‌های نهانکاوی از خود نشان می‌دهد. در این روش با استفاده از ابتکار تطبیق پیام محرمانه با ماتریسی به نام k، از انتقال حجم زیادی از اطلاعات در کانال بی‌نیاز خواهیم شد که این موضوع در امنیت، ظرفیت درج، مقاومت و شفافیت تاثیرگذار است. مقدار اطلاعات مورد نیاز برای انتقال، پس از کلاس‌بندی و نگاشت، به اعدادی بین ۷ الی ۷- تبدیل می‌شوند. به این ترتیب با کاهش بیت‌های محرمانه مورد نیاز برای ارسال، تغییرات در تصویر پوشانه نیز کاهش می‌یابد و نتایج بهینه می‌گردد. از دیگر مزایای این روش می‌توان به سهولت در مراحل درج و استخراج و محاسبات اندک اشاره کرد. با مقایسه پارامترهای نسبت سیگنال به نویز (PSNR) و نسبت شباهت (SSIM) این روش با دیگر روش‌های مشابه و مطرح در این حوزه، می‌توان بهبود این پارامترها را به وضوح مشاهده کرد. میانگین عددی پارامترهای PSNR و SSIM به‌ترتیب ۴۴/۳۶ و ۰/۹۷ است که هر دو در محدوده قابل قبولی قرار دارند. مقدار عددی میانگین درج در هر پیکسل در این روش ۵/۹۹ بیت بر پیکسل است که ظرفیت بسیار بالایی را برای درج فراهم می‌آورد.

کلید واژه‌ها: نهان‌نگاری، ظرفیت درج، مقاومت، نهان کاوی، تصویر پوشانه

۱- مقدمه

به هنر مخفی کردن اطلاعات محرمانه در رسانه دیگر را نهان‌نگاری می‌گویند. در رمزنگاری، وجود ارتباط بین گیرنده و فرستنده غیر قابل انکار است [۱] در حالی که در مخفی‌نگاری، همیشه وجود ارتباط بین فرستنده و گیرنده مخفی خواهد ماند.این عمل به همراه رمز کردن اطلاعات، می‌تواند امنیت اطلاعات محرمانه را تا حد زیادی افزایش دهد و از دسترسی افراد غیرمجاز به اطلاعات محرمانه ممانعت کند [۳-۲].

باتوجه بهاین‌که امروزه حجم زیادی از اطلاعات درکانال‌های غیرامن جابه‌جا می‌شود، حفظ امنیت اطلاعات محرمانه در این کانال‌هاهمیشهمورد توجه بوده است. از این‌رو، مبحث نهان‌نگاری، برای بهبود بخشیدن به امنیت اطلاعات مطرح می‌گردد. در نهان‌نگاری، حجم اطلاعات مخفی شده و غیرقابل تشخیص بودن آن توسط ادراک انسانی دارای اهمیت بالایی است [۴]، از این‌رو، روش‌های متعددی برای بهبود این دو پارامتر مطرح شده‌اند. از ابتدایی‌ترین و معروف‌ترین این روش‌ها می‌توان به نهان‌نگاری در بیت‌های کم ارزش کاور اشاره کرد [۵]. این روش توسط آقای Eason [۶]، مطرح شد که به‌علت پلکانی شدن هیستگرام تصویر نهایی به سادگی قابل تشخیص است. روش‌های متعددی بر اساس درج در لبه‌ها برای بهبود روش قبل ارائه شدند. در لبه‌ها به این علت که چشم انسان به تغییرات حساسیت کمتری دارد، می‌توان اطلاعات بیشتری را جاسازی کرد. این در حالی است که تغییرات اندک در نواحی صاف و یکنواخت باعث تحریک ادراک انسانی می‌شود [۸-۷]. با توجه به توضیحات فوق یک سوال مطرح می‌شود که اگرk، مقدار اطلاعات جاسازی‌شده در هر پیکسل (بر حسب بیت) فرض شود، مقدار k چقدر باشد تا اطلاعات درج شده قابل تشخیص نباشد؟

آقای Who و Tsai [۹] مقدار k را براساس مقدار اختلاف پیکسل‌های مجاور در تصویر پوشانه تخمین زدند. Chang و Tseng [۱۰] روش مشابهی را پیشنهاد دادند که در آن برای مشخص کردن تعداد بیت‌های درج، از اختلاف پیکسل‌های بالا و چپ استفاده شد. Wu [۱۱] روشی را پیشنهاد داد که در آن اختلاف بین پیکسل‌ها و جانشینی در بیت‌های کم ارزش با هم ترکیب شدند. Park [۱۲] و همکاران با تنظیم اختلاف دو پیکسل، K مورد نظر را مشخص کردند. آقای Yang و Weng این کار را بر اساس مقدار اختلاف پیکسل‌های یک بلوک ۴ پیکسلی

*رایانامه نویسنده مسئول: jalil.mazloum@ssau.ac.ir

محاسبه کردند [۱۶-۱۳]. پس از آن روش‌های زیادی بر اساس اختلاف پیکسل‌های یک بلوک (PVD) و به‌منظور بهینه کردن روش‌های فوق ارائه شد [۱۸-۱۷].

روش‌های مبتنی به تطبیق در کنار PVD از معروفترین روش‌های درج است که یکی از بهترین نمونه‌های آن در توسط CHENG ارائه شد [۱۹].

علاوه بر روش‌های فوق، روش‌های دیگری نیز در نهان‌نگاری تصاویر در حوزه مکان مطرح شده است. به‌عنوان مثال نهان‌نگاری مبتی بر کدهای خطی که با استفاده از ماتریس مشابهت و کدهای توافقی با گیرنده به جاسازی اطلاعات در پوشانه می‌پردازد.

عمل مخفی‌نگاری به جز در حوزه مکان در حوزه‌های مختلفی همچون DCT، FFT و WAVELET انجام می‌شود [۲۵-۲۰]. اما در حوزه مکان ظرفیت درج بالاتری فراهم است.

در این مقاله روشی ارائه می‌شود که اطلاعات محرمانه پس از مطابقت با ماتریس کلید، به مد ۵ رفته و حاصل آن به گروه‌های با مشخصه‌های خاص، کلاس‌بندی می‌شود و در نهایت بر اساس نگاشتی، در پیکسل‌های تصویر پوشانه درج می‌گردد.

در ادامه در بخش ۲ به ارائه روش پیشنهادی خواهیم پرداخت. در قسمت ۳ به تجزیه و تحلیل نتایج آزمایشگاهی، آزمون ROC و هیستگرام این روش اشاره می‌شود. در قسمت ۴ روش پیشنهادی با چندین روش مطرح مقایسه می‌شود و در نهایت در قسمت ۵ نتیجه‌گیری را مطرح خواهیم کرد.

۲- روش پیشنهادی

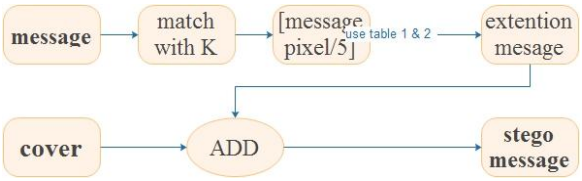
مقاومت در نهان‌نگاری عبارت است از استحکام الگوریتم در قبال روش‌های نهان‌کاوی.

به مقدار اطلاعات جاسازی‌شده در کاور، ظرفیت درج اطلاق می‌گردد.

پارامترهای ظرفیت درج در کنار مقاومت در همه الگوریتم‌های نهان‌نگاری دارای اهمیت هستند. رابطه این دو پارامتر به گونه‌ای است که با افزایش مقدار ظرفیت، مقدار مقاومت کم می‌شود و یا با کاهش ظرفیت درج، می‌توان مقاومت را بهبود بخشید. سوالی که همیشه مطرح می‌شود این است: آیا روشی وجود دارد که با داشتن ظرفیت بالا ، مقاومت مطلوبی نیز داشته باشد؟ به‌طوری که بتوان هر کدام از این پارامترها را جداگانه با روش‌های مشابه، مقایسه کرد؟

۲-۱- درج پیام

در این روش قبل از این‌که پیام در تصویر پوشانه درج شود، تغیراتی در چهار مرحله طبق الگوریتم زیر، روی آن انجام می‌شود. در ادامه این چهار مرحله را تشریح می‌کنیم.



شکل(۱): فلوچارت روش پیشنهادی

مرحله ۱- ابتدا فرستنده و گیرنده، بر یک ماتریس هم‌اندازه با پیام که همه عناصر آن اعدادی بیت ۰ تا ۴ هستند، به‌عنوان کلید توافق می‌کنند. این کلید می‌تواند ثابت و غیرمحرمانه باشد. (اعداد ۰ الی ۴ تمام باقیمانده‌های ممکن به مد ۵ می‌باشند)

مرحله ۲- در این مرحله با اضافه و یا کم کردن ۰ ، ۱ و یا ۲ واحد از مقدار هر پیکسل، مقدار هر پیکسل طوری تعیین می‌شود که حاصل آن به مد ۵، برابر با مقدار عدد متناظر آن در ماتریس کلید شود. (تشکیل میدان بر مبنای عدد اول ۵)

$$Message(i,j) \pm 1 \text{ or } 2 \text{ or } 0 (\text{mod } 5) = key(i,j) \qquad (۱)$$

مرحله ۳- در این مرحله مقدار به‌دست‌آمده از مرحله ۲، بر پنج تقسیم و جزء صحیح آن ذخیره می‌گردد. از این رو اگر تصویر پیام را uint8 در نظر بگیریم، ماتریس به‌دست‌آمده از این مرحله، دارای عضوهایی بین ۰ الی ۵۱ می‌باشد.

$$M = [message/5] \quad ,, \qquad (۲)$$
$$M=\{0,1,2,\ldots..51\}$$

در این رابطه [] تابع جزءصحیح است.

مرحله ۴- مرحله ۴ اصلی‌ترین مرحله در روش پیشنهادی است، در این مرحله هر کدام از مقادیر درایه‌های ماتریس m را ابتدا به کلاس‌هایی با مشخصه‌های خاص و سپس به اعداد کوچک‌تر نگاشت می‌کنیم. در مقابل مجبور به گسترش اندکی در این ماتریس کاور خواهیم بود. بخش‌های این مرحله به شرح زیر می‌باشد.

الف- ابتدا تمام مقادیر ماتریس m که اعدادی بین ۰ تا ۵۱ می‌باشد را به ۵ کلاس که هر کلاس، دارای یک مشخصه است، تقسیم می‌کنیم. این تقسیم‌بندی می‌تواند به شکل زیر باشد.

جدول (۱): کلاسهای پیکسل ها

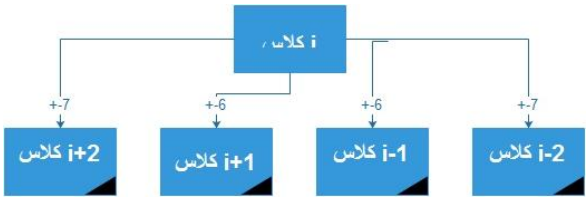
کلاس پنجم(۵)	کلاس چهارم(۴)	کلاس سوم(۳)	کلاس دوم (۲)	کلاس اول(۱)
۴۰	۳۰	۲۰	۱۰	۰
۴۱	۳۱	۲۱	۱۱	۱
۴۲	۳۲	۲۲	۱۲	۲
۴۳	۳۳	۲۳	۱۳	۳
۴۴	۳۴	۲۴	۱۴	۴
۴۵	۳۵	۲۵	۱۵	۵
۴۶	۳۶	۲۶	۱۶	۶
۴۷	۳۷	۲۷	۱۷	۷
۴۸	۳۸	۲۸	۱۸	۸
۴۹	۳۹	۲۹	۱۹	۹
۵۰	۵۱			

ب- حال تک تک اعضای جدول (۱) را که در مرحله الف تشریح شد، به اعدادی بین ۵- تا ۵، همانند جدول (۲) نگاشت می‌کنیم و مشخصه هر کلاس را به ترتیب ۱، ۲، ۳، ۴ و ۵ قرار می دهیم.

جدول (۲): نگاشت اعضای کلاس ها

۵	۴	۳	۲	۱
-۵	-۵	-۵	۵	-۵
-۴	۴	-۴	۴	-۴
-۳	۳	-۳	۳	-۳
-۲	۲	-۲	۲	-۲
-۱	۱	-۱	۱	-۱
۰	۰	۰	۰	۰
۱	-۱	۱	-۱	۱
-۲	۲	-۲	-۲	۲
۳	-۳	۳	-۳	۳
۴	-۴	۴	-۴	۴
۵	-۵			

مرحله پنجم درج: در این مرحله اولین درایه از تصویر پوشانه که روی آن تغییر اعمال می‌شود، نشان‌دهنده کلاس داده‌های بعدی خود است. تغییرات این پیکسل که اعدادی بین ۱، ۲، ۳، ۴ و ۵ است، نشان‌دهنده پنج کلاس فوق‌الذکر می‌باشد. بعد از تغییر اولین پیکسل، داده‌های پیام با پیکسل‌های تصویر پوشانه جمع می‌شود.باید دقت کرد در صورت تغییر کلاس باید طبق الگوریتم زیر مشخصه کلاس را محاسبه و در پیکسل متناظر درج کرد.



شکل (۲): تغییر از کلاس iبه سایر کلاس ها

به‌عنوان مثال فرض کنید تعدادی از پیکسل‌های پیام بعد ازهمسانی با کلید به شرح زیر باشد.

۲۸-۲۸-۲۹-۳۰-۳۰-۳۰

که با توجه مرحله آخر و کلاس‌بندی و نگاشت، به اعداد زیر تبدیل می‌شود:

۳-۳-۳-۶-۴-۳-۳-۵-۵-۵

عدد ۳ که به‌صورت برجسته مشخص شده است، مشخص‌کننده کلاس اعداد بعد از خود است و عدد ۶ که آن نیز به‌صورت برجسته مشخص شده است، طبق الگوریتم بالا نشان دهنده تغییر از کلاس ۳ به کلاس ۴ می‌باشد.

فرض کنید مقدار پیکسل‌های تصویر پوشانه که برای درج انتخاب می‌شود به‌صورت زیر است:

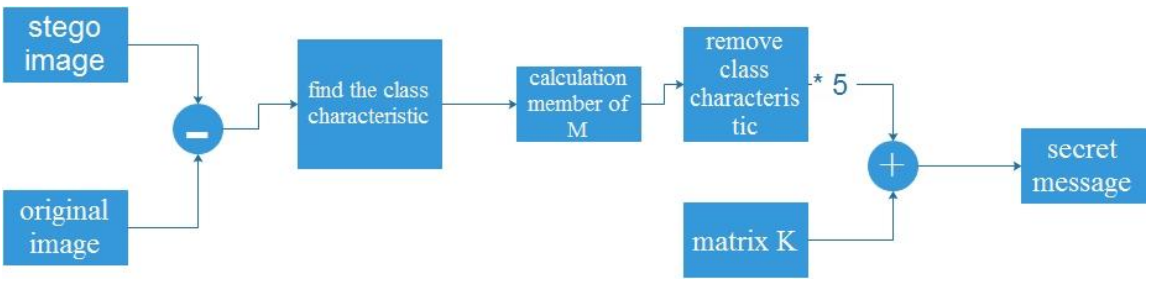
۱۳۰-۱۳۱-۱۳۱-۱۳۱-۱۳۲-۱۳۲-۱۳۳-۱۳۳-۱۳۴

با جمع مقدارهای بالا با مقدار پیکسل‌های تصویر پوشانه، پیکسل‌های ماتریس stego به‌دست می‌آید.

۱۳۳-۱۳۴-۱۳۴-۱۳۴-۱۳۶-۱۳۸-۱۳۸-۱۳۸-۱۳۹

۲-۲- استخراج پیام

برای استخراج پیام با توجه به جدول‌ها و روند الگوریتم تصمیم‌گیری، مراحل را از آخر به اول انجام می‌دهیم. باید توجه کرد که با تغییر اعداد اختصاص داده به هر ردیف و ستون می‌توان امنیت پیام را در صورت شکست پنهان‌نگاری بالا برد.



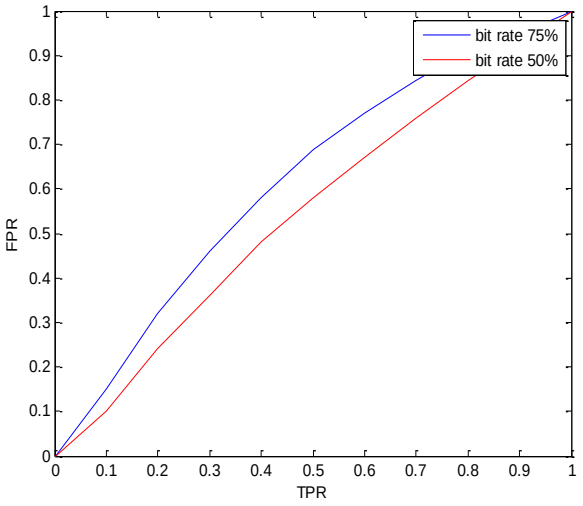
شکل (۳): الگوریتم استخراج پیام

۳- نتایج آزمایشگاهی

در ادامه با ارائه جدول‌ها و نمودارهایی به تشریح نتایج آزمایشی این روش می‌پردازیم. در ابتدا نیازمند معرفی آزمون و نمودار RS، هیستگرام و همچنین دو معیار SSIM و PSNR هستیم.

آزمون RS یکی از آزمون‌های امنیت در نهان‌نگاری است. این آزمون بر اساس تحلیل‌های آماری انجام می‌شود، از این‌رو، در بسیاری از روش‌های نهان‌کاوی از این آزمون استفاده می‌شود. نتایج آزمونRS به‌صورت دو منحنی بر روی نموداری با محورهای TPR و FPR قابل نمایش است. TPR به معنی، احتمال صحیح تشخیص درست و FPR به معنی، احتمال ناصحیح تشخیص غلط است.

در این آزمون ۱۰۰ تصویر مختلف مورد بررسی قرار گرفته است که با توجه به نرخ درج، نمودار آنها در زیر قایل مشاهده می‌باشد.

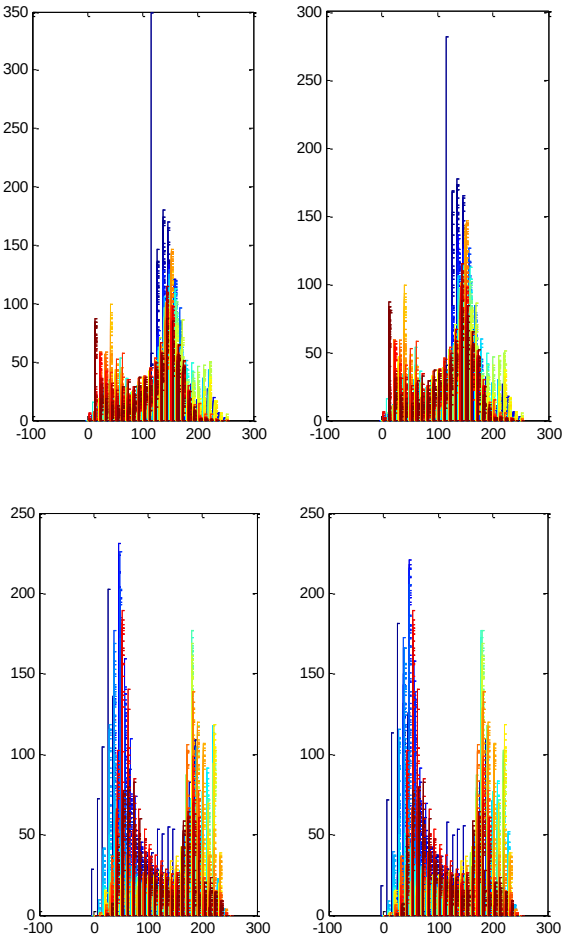


شکل(۴): نمودار ROC با محورهای TPRبه معنی، احتمال صحیح تشخیص درست و FPR به معنی، احتمال ناصحیح تشخیص غلط

با توجه به نمودار بالا به‌سادگی می‌توان دریافت که حتی در نرخ‌های بالای درج، نهان‌کاوی روش پیشنهادی، بسیار مشکل است. زیرا تغییرات منحنی‌های بالا به خط فرضی y=x بسیار نزدیک است.

تصاویر ارائه‌شده در شکل (۵)، دو نمونه از تصاویر stego است که هیستگرام و کاور آنها در شکل (۶) قابل مشاهده است.

شکل (۵): دو تصویر stego در راست به همراه کاور آنها در چپ



شکل (۶): هیستگرام تصاویر شکل (۵)

عدم تغییر فرکانس، در تصویر خروجی بیانگر موثر بودن این روش است. معیارهای SSIM و PSNR دو پارامتری هستند که به ترتیب معرف میزان تشابه بین تصویر اصلی تصویر پوشانه و تصویر stego و میزان توان سیگنال به نویز می‌باشند.

$$(\text{MSE}=f(x)=\frac{1}{m*n}\sum_{n=1}^{\infty}(\text{I}(\text{m},\text{n})-I(m,n))\text{^}2 \quad (۳)$$

$$\text{PSNR}=10\log_{10}(m\text{^}2)/MSE \quad (۴)$$

and

$$SSim(x,y)=[l(x,y)]^{\alpha}.[c.(x,y)]^{\beta}.[s.(x.y)]^{\gamma} \quad (۵)$$

$$l(x,y)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2}$$

$$s(x,y)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3}$$

$Where \mu_x,\mu_y,\sigma_x,\sigma_y and \sigma_{xy} are the local means, standard deviation and cross-covariance for image x,y. if \alpha = \beta = \gamma = 1 (the default ....Exponents)\ and c_3 = \frac{c_2}{2}\ (default selection of c_3) the index simplifies to$

$$SSIM(x.y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}++c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}$$

$$\text{t rate}=(\text{message size})*8/(\text{caver size}) \quad (۶)$$

$$\text{Capacity}=(\text{caver size})*\text{bit rate} \quad (۷)$$

در این آزمایش (۱) تصویر مشخص و ثابت زیر (۲۵۶*۲۵۶) را در پوشش‌های مختلف درج کرده و مقدار معیارهای SSIM و PSNR و همچنین نسبت پیام به تصویر پوشانه و نرخ درج را محاسبه می‌کنیم.

شکل(۷):تصویر پیام در آزمایش (۱)

جدول (۳):نتایج آزمایش (۱)

	نسبت پیام به کاور	PSNR	SSIM	Bit rate	اندازه کاورمورد نیاز
Lena	۹۳%	۴۲/۴۴۰۵	۰/۹۷۹۱	۷/۴۴	۲۸۳×۲۵۶
Baboon	۹۳%	۴۳/۱۶۵۳	۰/۹۸۰۱۹	۷/۴۴	۲۸۳×۲۵۶
Boat	۹۳%	۴۴/۱۹۱۴	۰/۹۸۴۵	۷/۴۴	۲۸۳×۲۵۶
Pepper	۹۳%	۳۷/۸۵۸۴	۰/۹۵۹۰	۷/۴۴	۲۸۳×۲۵۶

در ادامه در آزمایش (۲) با در نظر گرفتن یک تصویر ثابت به عنوان کاور (Lena)، پیام‌های مختلفی با اندازه ۲۲۵*۲۲۵ در آن درج می‌کنیم. جدول (۴) نتایج به‌دست آمده از این آزمایش را نشان می‌دهد (اندازه کاور متغیر است).

شکل (۸):تصویر پوشانه در آزمایش (۲)

جدول(۴): نتایج آزمایش (۲)

	نسبت پیام به کاور	PSNR	SSIM	Bit rate	حداقل اندازه پوشش	*ظرفیت (بیت)
Paper	۸۵%	۴۴/۷۲۵۱	۰/۹۸۱۷	۶/۸	۲۶۶*۲۲۵	۱۷۸۲۵۷۹
Baboon	۷۳%	۴۳/۲۹۰۸	۰/۹۴۸۶	۵/۸۴	۳۱۰*۲۲۵	۱۵۳۰۹۲۱
Boat	۸۷%	۴۴/۳۵۴۳	۰/۹۷۰۴	۶/۹۶	۲۶۰*۲۲۵	۱۸۲۴۵۲۲
Man	۹۴%	۴۵/۱۲۰۵	۰/۹۷۹۵	۷/۵۲	۲۴۰*۲۲۵	۱۹۷۱۳۲۳
Average	۸۵%	۴۴/۳۷۲۶	۰/۹۷۰۰	۶/۷۸	۲۶۹*۲۲۵	۱۷۷۷۳۳۶

* ظرفیت با در نظر گرفتن کاوری با اندازه ۵۱۲*۵۱۲ محاسبه شده است.

۴- مقایسه روش پیشنهادی با چند روش مطرح

در جدول (۵) روش پیشنهادی با چهار روش ذکر شده در منابع [۱۹-۱۷و ۲۵] مقایسه شده است. روش‌های بیان‌شده در [۱۷]، [۱۹] و [۲۵] بر اساسPVD (اختلاف چهار پیکسل در یک بلوک) و [۱۸] با روش جاسازی تطبیقی در لبه‌ها ارائه شدند. نتایج در جدول (۵) قابل مشاهده می‌باشند.

جدول (۵): مقایسه با مراجع [۱۹-۱۷] و [۲۵]

	میانگین بیت بر پیکسل	میانگین ظرفیت	میانگین (PSNR)	میانگین (SSIM)
Xin Liao et al[۱۷]	۴/۱	۱۰۷۲۵۱۸	۳۳/۶۹	----------
Masoumesabokdast[۱۸]	۴/۰۵	۱۰۶۲۳۵۲	۴۳/۸۸	
Chen- hsing yang[۱۹]	۴/۰۸	۱۰۶۹۴۰۰	۳۲/۷۳	----------
Gandhara Swain[۲۵]	۳/۳۱	۳۵۸۱۳۹۵ در سه مولفه R،B،G	۳۷/۲۲	---
روش پیشنهادی	۵/۹۹	۱۷۷۷۳۳۶	۴۴/۳۷۲	۰/۹۷۰۰

۵- نتیجه‌گیری

در این مقاله روشی ارائه شد که علاوه بر ظرفیت بالای درج، دارای امنیت قابل ملاحظه‌ای نسبت به روش‌های دیگر می‌باشد. بهبود در ظرفیت درج و امنیت، در ازای مقدار خطایی به‌دست آمد که در مرحله ۲ با تغییر بیت‌ها اعمال شد. در این روش با استفاده از کلید محرمانه مرحله اول و محرمانه بودن مشخصه کلاس‌ها، پارامتر امنیت در پنهان‌نگاری بهبود یافته و همچنین با میانگین درج ۵/۹۹ بیت در هر پیکسل، حجم درج بالایی در مقایسه با دیگر روش‌های پنهان‌نگاری به‌دست آمده است. نیاز به محاسبات کم در این روش و سهولت در انجام مراحل درج و استخراج، نشان از کارایی بیشتر و چابکی روش پیشنهادی می‌باشد. همچنین نتایج به‌دست‌آمده از دو پارامتر SSIM و PSNR (با مقدار متوسط ۰/۹۷ و۴۴/۳۷) در آزمایش‌های مختلف نشان‌دهنده کیفیت قابل قبول تصویر خروجی است.

۶- منابع

[1] H. J. Highland, "Data encryption: A non-mathematical approach," Comput. Secur., 1997.

[2] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," IEEE J. Sel. Areas Commun., 1998.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hidinga survey," Issue prot. multimedia content, 1998.

[4] D. W. Bender, N. M. Gruhl, and A. Lu, "Techniques for data hiding," IBM syst. J., 1998.

[5] H. Wang and S. Wang, "Cyber warfare Steganography vs. Steganalysis," commun. ACM., 1998.

[6] R. O. Eason and E. Kawaguchi, "Principle and applications of bpcs," Steganography In proceedings of SPIE, 1998.

[7] I.C. Lin, Y. B. Lin, and C. M. Wang, "Hiding data in spatial domain images with distortion tolerance," Comput. Stand. Inter., 2003.

[8] C. K. Chan and L. M. Chen, "Hiding data in images by simple LSB substitution," Pattern recognit., 2004.

[9] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern recognit. Lett., 2004.

[10] C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," Pattern recognit. Lett., 2004.

[11] 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," Proc. Inst. Elect. Eng., Vis. Images signal process, 2005.

[12] Y. R. Park, H. H. Kang, S. U. Shin, and K. R. Kwon, "A steganographic scheme in digital images using information of neighboring pixels," vol. 3612, Springer-verlag,Berlin, Germany, 2005.

[13] C. H. Yang and C. Y. Weng, "A steganographic method for digital images by multi-pixel differencing," Proceedings of international computer symposium, Taipei, 2006.

[14] K. H. Jung, K. J. Ha, and K. Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods," International conference on convergence and hybrid information technology, 2008.

[15] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function," J. Syst. Softw., 2008.

[16] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Secur. 2008.

[17] X. Liaoa, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," ELSEVIER, 2011.

[18] M. Sabokdast and M. Mohammadi, "A steganographic method for images with modulus function and modified LSB replacement based on PVD," 5th Conference on information and knowledge technology, IEEE, 2013.

[19] C.-H. Yang, C.-Y. Weng, and S.-J. Wang, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Ttransations on information forensics and security, 2008.

[20] B. Kaur, A. Kaur, and J. Singh, "Steganography approach for hiding image in DCT domain," International journal of Advances in engineering & technology, 2011.

[21] X. Song, S. Wang, and X. Niu, "An integer DCT and affine transformation based image steganography method," Eighth international conference on intelligent information hiding and multimedia signal processing, 2012.

[22] Tamanna and A. Sethi, "Steganography a juxtaposition between LSB DCT, DWT," International journal of computer applications, 2015.

[23] A. Goswami and S. Khandelwal, "Coloured and gray scale image steganography using block level DWT, DCT transformation," International journal of computer applications, 2016.

[24] A. Nourazar, Z. Noroozi, and M. Mir, "An Optimal Method for Images Steganography Based on Linear Codes Features," Journal of Electronical& Cyber Defence, 2017. (in Persian)

[25] G. Swain, "Very high capacity image steganography technique using quotient value differencing and LSB substitution," Arabian journal for science and engineering, 2018.

Journal of Electronical & Cyber Defence
Vol. 7, No. 2, 2019, Serial No. 26

Increasing Insertion Capacity and Resistance in Image Steganography Based on Mapping and Bits Reduction

Y. Khorasani, J. Mazloum*, M. Shayesteh far

*Shahid Sattari Aeronautical University of Science and Technology

(Received: 22/04/2018, Accepted: 13/10/2018)

ABSTRACT

Abstract: In all of the image steganography algorithms, the embed capacity and resistance are considered. Hence, in this paper a new method is proposed that not only has high capacity for embed, but also has high resistance against steg analysis methods. This method presents an initiative to collate the confidential secret message with a matrix called K, thus large amount of information does not need to be transferred across the channel which effects security, resistance and embed capacity. After classification and mapping, the amount of information that is needed to be sent, changes to numbers between -7 and 7. Hence, by reducing the secret bits needed to send, the changes in the cover are also reduced and the result are optimized. B y comparing PSNR and SSIM for this method with other methods in this area, we clearly see improvements in these parameters. The average of PSNR and SSIM is 44.36 and 0.97, respectively both of which are in the perfect range. The average of numerical value of insertion is 5.99 bits per pixel, which provides a very high capacity for insertion.

Keywords: Steganography, Embed Capacity, Resistance, Steganlysis, Cover

* Corresponding Author Email: jalil.mazloum@ssau.ac.ir