مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۴، زمستان ۱۳۹۶، ص ۵۳-۴۳

ارائه روشی بهبودیافته برای نهان‌نگاری تصویر مبتنی بر ویژگی‌های کدهای خطی

علی نورآذر[۱]، زین‌العابدین نوروزی[۲*]، مهدی میر[۳]

۱- کارشناسی ارشد، ۲- استادیار، دانشگاه جامع امام حسین(ع) ۳-کارشناس ارشد دانشگاه فردوسی مشهد

(دریافت: ۹۵/۱۱/۱۹، پذیرش: ۹۶/۰۵/۰۱)

چکیده

نهان‌نگاری یکی از حوزه‌های پرکاربرد مخفی‌سازی اطلاعات است که به جاسازی غیرمحسوس پیام محرمانه داخل یک پوشانه می‌پردازد. در این مقاله یک روش بهبودیافته برای جاسازی پیام محرمانه داخل پوشانه تصویر در حوزه مکان، براساس نظریه کدگذاری معرفی می‌کنیم، به‌طوری‌که فرستنده پیام محرمانه را با توجه به ماتریس کنترل مشابهت (H) کد توافقی با گیرنده، در پوشانه با کم‌ترین تغییر جاسازی نموده و آن را برای گیرنده ارسال می‌کند. حال گیرنده تنها با همان ماتریس توافقی به‌راحتی می‌تواند پیام را از پوشانه استخراج کند. در این روش جدید، ضمن برخورداری از مزایای حوزه مکان و تشخیص و تصحیح خطای رشته بیت دریافتی توسط گیرنده، می‌توان مقاومت را بین ۹۴ ٪ الی ۱۰۰ ٪، شفافیت (PSNR) را تا ۷۱/۸۴ ٪ و مشابهت (SSIM) را تا ۹۹/۹۹۹۹ ٪ افزایش داد.

واژه‌های کلیدی: نهان‌نگاری، پوشانه تصویری، کد خطی، ماتریس کنترل مشابهت.

۱- مقدمه

حوزه نهان‌نگاری یکی از جدیدترین حوزه‌ها برای بالابردن حفاظت و امنیت اطلاعات است. نهان‌نگاری[۱] چگونگی جاسازی اطلاعات داخل یک پوشانه[۲] می‌باشد. هدف نهان‌نگاری پنهان‌کردن خود رابطه است و در این خصوص از پوشانه‌هایی مانند تصویر، صوت، ویدئو و غیره جهت درج اطلاعات استفاده می‌گردد. تاکنون الگوریتم‌های گوناگونی برای نهان‌نگاری اطلاعات ارائه شده است. عموماً نهان‌نگاری در دو حوزه مکان و تبدیل انجام می‌شود [۱-۲].

حوزه مکان شامل آن دسته از الگوریتم‌هایی می‌شود که بیت‌های پیام بین بیت‌های میزبان جاسازی می‌شوند [۳]. به‌عنوان مثال، در روش جاگذاری LSB[۳] بیت‌های پیام در کم‌ارزش‌ترین بیت هر پیکسل گنجانده می‌شوند [۴-۵]. برای نهان‌نگاری در این حوزه می‌توان به روش‌های معکوس در بیت کم‌ارزش LSBF۴ [۶]، تطبیقی براساس اغتشاش جمع‌شونده LSBM[۵] [۷] و روش‌های PVD[۶] مبتنی بر اختلاف مقدار شدت پیکسل [۸] و غیره اشاره نمود. این‌گونه روش‌ها اگرچه نسبت به سیستم بینایی انسان (HVS[۷]) کارایی خوبی را از خود به نمایش گذاشته‌اند، اما عملکرد ضعیف آن‌ها در مواجهه با نهان‌کاوها سبب ابداع حوزه تبدیل گردید. در نهان‌نگاری حوزه فرکانس، ابتدا از پوشانه، تبدیلی مانند (DCT[۸]) گرفته می‌شود، سپس پیام در این ضرایب تبدیل‌شده گنجانده می‌شود (پیام محرمانه، در داخل فضای تبدیل سیگنال پوشش جاسازی می‌شود) [۱۰-۹ و ۲۵]. ازجمله الگوریتم‌هایی که برای درج داده‌های محرمانه از ضرایب حاصل از تبدیل DCT استفاده می‌نمایند، می‌توان به روش‌های JSteg [۱۱]، F5 [۱۲] و OutGuess [۱۳] اشاره نمود.

در این مقاله روش جدیدی برای نهان‌نگاری تصویر در حوزه مکان براساس نظریه کدگذاری جهت جاسازی پیام معرفی می‌شود تا ضمن برخورداری از مزایای حوزه مکان، می‌توان مقاومت را تا حد چشم‌گیری افزایش داد. در ضمن، برای ارزیابی روش پیشنهادی از دو معیار PSNR[۹] و SSIM[۱۰] و برای سنجش امنیت از نهان‌کاوی (spam, srmg, srm) استفاده شده است که نتایج حاصل نشان‌دهنده بهبودیافتن مقاومت و امنیت نهان‌نگاری در حوزه مکان می‌باشد. مقاله مشتمل بر چهار بخش می‌باشد، در

* رایانامه نویسنده مسئول: znorozi@ihu.ac.ir

1- Steganography
2- Cover
3- least significant bit
4 -least significant bit flipping
5 -LSB maching
6 -pixel value differencing
7- Hhuman Visual System
8- Discrete Cosine Transform
9- Peak Signal Noise Ratio
10- Structural Similarity Index Measure

بخش دوم به معرفی روش نهان‌نگاری تصویر با استفاده از ساختار کدگذاری و براساس ماتریس کنترل مشابهت پرداخته می‌شود و به‌منظور جبران محدودیت‌های این روش و بهینه‌نمودن آن، روش پیشنهادی را در بخش سوم بیان نموده و در بخش چهارم به شبیه‌سازی روش پیشنهادی براساس بانک تصاویر مختلف پرداخته و نتایج حاصل از آن را براساس معیارهای ذکرشده ارزیابی می‌نماییم. در ادامه، نتیجه‌گیری روش پیشنهادی در بخش پنجم آمده است.

۲- نهان‌نگاری تصویر با استفاده از کدهای خطی (روش جاسازی ماتریس)

فرض کنیم k و n دو عدد طبیعی باشند که $k\leq n$ و V,W دو فضای برداری به‌ترتیب با ابعاد n , k روی میدان GF(q) باشند که در آن q قوایی از اعداد اول است، در این صورت، هر تبدیل یک به‌یک $T: V\rightarrow W$ را یک کد C:=[n,k,d] با طول n، بعد k و کمترین فاصله d روی میدان GF(q) می‌نامیم. اگر T خطی باشد آن‌گاه کد را کد خطی می‌نامند [۱۴]. حال با توجه به مطالب بیان‌شده، مهم‌ترین نقطه ضعف روش‌های حوزه مکان با وجود ظرفیت بالا، مقاومت و امنیت پایین در برابر حملات و نهان‌کاوها می‌باشند. یافتن راه‌هایی برای افزایش مقاومت و امنیت تصویر حاوی اطلاعات پنهان در حوزه مکان، ضروری است. یکی از این راه‌حل‌ها استفاده از نظریه کدگذاری می‌باشد.

در استفاده از نظریه کدگذاری جهت جاسازی اطلاعات، کدهای خطی به‌عنوان پایه اصلی قلمداد شده و می‌توان از ویژگی‌های آن‌ها در نهان‌نگاری، تحت روش جاسازی ماتریس، نام برد [۱۷].

برای کارایی مطلوب این روش بایستی از کدهای مناسب استفاده نمود. توجه داشته باشید که در میان همه کدهای با اندازه و بعد ثابت، کدی مناسب محسوب می‌شود که کم‌ترین تغییرات را نسبت به بیش‌ترین ظرفیت جاسازی، داشته باشند. کدهای بهینه خطی متشکل از کدهای دو و سه‌بعدی بر روی GF(2) و GF(3) که در روش کدگذاری مشخصه استفاده می‌شود، می‌توانند کد مناسب برای نهان‌نگاری ماتریس تلقی شوند.

۲-۱- استفاده از کدهای خطی در نهان‌نگاری

یکی از ویژگی‌های اصلی نهان‌نگاری می‌تواند مقاومت آن درمقابل حمله آماری یا به‌عبارت دیگر آشکارسازی آماری باشد، ما برای تحقق این هدف از جایگذاری شبه‌تصادفی برمبنای نظریه کدگذاری استفاده نموده، به‌طوری‌که روند جاسازی[1] کم‌ترین تغییرات را داشته و از لحاظ آماری مقاومت بالایی داشته و خواص اصلی را حفظ نماید [۱۷]. بر همین اساس، می‌توان از روش نظریه کدگذاری در نهان‌نگاری استفاده نمود. به‌طوری‌که فرستنده پیام محرمانه را با توجه به ماتریس کنترل مشابهت (H^T) توافقی، به‌عنوان یک مشخصه از پوشانه دریافت نموده و پیام را با استفاده از ماتریس کنترل مشابهت، داخل پوشانه‌ای (مانند تصویر) ذخیره نموده، سپس دریافت‌کننده با استفاده از همان ماتریس، پیام جاسازی‌شده توسط فرستنده را از نهانه بازگشایی نموده و تشخیص و تصحیح خطا را روی آن اعمال می‌دارد [۱۶-۱۵].

در چند سال اخیر، روش‌های مختلفی بر این اساس در مقالات متعددی ارائه شده است، ولی اکثر این روش‌ها دارای معایب متنوعی می‌باشند. مواردی از این معایب عبارت‌اند از:

- برخی از روش‌ها تنها مربوط به کدهای خطی و کاربرد آن‌ها در نشانه‌گذاری[3] می‌باشند [۱۸].
- در موارد متعددی از یک فرمول جاسازی واحد و مشخص برای داده‌های مختلف استفاده نمی‌کنند و به‌صورت شرطی بیان شده‌اند (گزاره به شرطی درست است که پارامتر x با خواص مورد نظر را بیابیم) [۱۶-۱۵].
- $\text{Finde } (\delta\in F^{m}_{2}) \text{ For } (H^{t}(E+\delta)=M) \rightarrow \text{Emb and Exc is OK}$
- در موارد خاصی در حد تئوری بوده و هم‌چنین، در یک بانک داده با فرمت‌های مختلف فاقد پیاده‌سازی بوده و یا شبیه‌سازی آن‌ها پیچیده می‌باشد [۱۹].
- بعضی از روش‌های ارائه‌شده، بهینه نبوده و بعضاً نتایج غیرمطلوبی تحت عنوان یک روش نهان‌نگاری دارند [۲۱-۲۰].
- در برخی موارد، ارزیابی مناسبی نسبت به روش بیان‌شده با سایر روش‌های این حوزه، با یک بانک مشترک، صورت نگرفته است [۱۶-۱۵ و ۲۱-۱۸].

فرمول جاسازی و بازیابی اطلاعات را که ارائه و در روش پیشنهادی استفاده می‌نماییم (رابطه-۲)، شکل بهبودیافته [۱۷] است که دارای گزاره جاسازی و بازیابی مشخص برای داده‌های مختلف بوده و به‌صورت کاربردی برای انواع کدها (خطی و غیرخطی) قابل پیاده‌سازی می‌باشد. با توجه به ایده مورد نظر و شبیه‌سازی انجام‌شده، به این نتیجه رسیدیم که روش ارائه‌شده دارای عملکرد مناسبی از نظر پارامترهای ارزیابی و نهان‌کاوها، نسبت به سایر روش‌های موجود در این حوزه می‌باشد.

1- Embedding
2- Parity Check
3- Watermarking

در این مقاله تمام کدهایی که درنظر گرفته شده‌اند در میدان F_2 می‌باشند. فرض کنید $C\subseteq F_2^n$ کدی باشد که با ماتریس کنترل مشابهت H تعریف شود، آن‌گاه میانگین وزن کلمه کد همه مجموعه‌های کد C را با $R_a(C)$ نشان داده و برابر با مقدار میانگین فاصله از محور F_2^n تا C می‌باشد و می‌توان آن را به‌صورت مفهوم کلاسیک شعاع پوششی C در نظر گرفت [۱۷].

فرض کنیم پوشانه، یک فایل دیجیتالی باشد آن‌گاه اطلاعات محرمانه در بیت‌های پوشانه دیجیتال درج می‌شود. برای ارائه توضیحات ملموس‌تر در این مورد، یک تصویر دیجیتال را به‌عنوان پوشانه درنظر می‌گیریم. فرستنده ابتدا یک رشته از بیت‌های داده، (مانند رشته کم‌ارزش‌ترین بیت‌های پیکسل‌ها) از روی تصویر استخراج می‌کند. اصلاح و تغییر برخی از این بیت‌ها متناظر با پیامی هستند که قصد جاسازی آن را در پوشانه داریم. سپس با توجه به تغییرات ایجادشده، چون پیام محرمانه و پوشانه دیجیتال بوده، پیام‌های محرمانه با روش‌های مختلفی مثل روش جاسازی ماتریس، در گیرنده قابل بازیابی هستند و می‌توان آن‌را به‌صورت بردارهای دودویی درنظر گرفت.

اگر $M\in F_2^r$ مجموعه متناهی از پیام‌ها و $x\in F_2^n$ رشته بیت استخراج‌شده از پیکسل‌های تصویر پوشانه که $n\geq r$ باشد، معمولاً یک (n,r) طرح نهان‌نگاری S را به‌صورت یک جفت از توابع بازیابی و جاسازی اطلاعات به‌صورت S= (Emb,Exc) با استفاده از نظریه کدگذاری، طبق رابطه (۱) قابل تعریف می‌باشد.

$$\text{Emb}: F_2^n \times F_2^r \to F_2^n \ , \ \text{Exc} : F_2^n \to F_2^r \qquad (۱)$$

به‌طوری‌که، برای هر $x\in F_2^n$ و $m\in F_2^r$، آن‌گاه:

$$\text{Exc}\ (\text{Emb}(x,m))= m$$

حال فرض کنیم $X\in F_2^n$ یک دنباله از n بیت استخراج‌شده از پیکسل‌های شی پوششی موردنظر باشد و $m\in M= F_2^r$ پیام مورد نظر برای جاسازی در آن باشد. ارسال‌کننده و دریافت‌کننده از پیش بر روی ماتریس H_{r*n} متناسب با کد C= [n,k,d]، توافق می‌کنند. برای جاسازی پیام محرمانه، فرستنده مقدار (Emb) رابطه (۲) را محاسبه نموده و شماره یک بیت از رشته n بیتی پوشانه که باید تغییر نماید را به‌عنوان خروجی به‌دست می‌آورد (همان n^*). سپس با تغییر یک بیت از رشته بیت پوشانه، X' را برای گیرنده ارسال می‌نماید. دریافت‌کننده، پیام محرمانه m را با استفاده از رابطه Exc از پوشانه اصلی که تنها یک بیت از nبیت آن تغییر نموده است، استخراج می‌نماید.

$$\begin{aligned}&\text{Emb: } (X,\ \text{Exc: } H.\ X'^t = M^t \to M \\ &M) \to (H.\ X^t)\ \text{xor}\ M^t = n^*,\ f(X,\ n^*)\ \to X'\end{aligned} \qquad (۲)$$

با این روش، طرح نهان‌نگاری مبتنی بر نظریه کدگذاری امکان‌پذیر شد. لازم به ذکر است با این روش mبیت پیام داخل n بیت پوشانه جاسازی می‌گردد، ولی نکته‌ای که اهمیت دارد، استفاده از کدهایی می‌باشد که کم‌ترین تغییر را نسبت به بیش‌ترین ظرفیت داشته باشند که اصطلاحاً کدهای بهینه نامیده می‌شوند. ازجمله کدهای تصادفی که ظرفیت جاسازی بالا و کم‌ترین خرابی را دارند. بدین منظور، بسته به نوع کدی که استفاده می‌نماییم، برای طرح خود می‌توان از سه مؤلفه cov (ρ,N,n) استفاده نمود که در آن جاسازی n بیت در رشته N بیتی پوشانه با حداکثر تغییرات ρ بیت صورت می‌گیرد. بهتر است برای کارایی بالا از کدهایی استفاده نماییم که در آن کران ρ حداقل باشد [۱۷].

به‌عنوان‌مثال، فرض کنید فرستنده برای نهان‌نگاری پیام M=110 از پوشانه تصویری استفاده می‌کند که رشته بیت استخراجی X=1110000 از پیکسل‌های تصویر پوشانه استخراج‌شده و ماتریس H کد خطی همینگ C=[7,4,3] را به‌صورت ذیل با طرف گیرنده توافق می‌کند. کد مورد استفاده ما در این مثال یک طرح cov (1,7,3) می‌باشد.

$$\text{Emb: } H=\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix} \to \begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}$$

$$=\begin{bmatrix}0\\1\\0\end{bmatrix} \to X' = 1110010$$

$$\text{Exc: } H=\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}\to\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}1\\1\\0\end{bmatrix}\to M=110$$

روش فوق علاوه‌بر کدهای خطی شامل کدهای غیرخطی نیز می‌شود. به‌عنوان‌مثال، ماتریس کنترل مشابهت ذیل مربوط به کد کانولوشن نوع B2 بهینه می‌باشد که می‌توانند بین فرستنده و گیرنده توافق شده باشد. در این مثال، فرستنده از این ماتریس برای جاسازی هر پیام سه بیتی (M=100) در شش بیت پوشانه استخراج‌شده از تصویر (X=111000) استفاده می‌نماید (cov(1,6,3)) و گیرنده بر همین اساس به‌راحتی می‌تواند به پیام درج‌شده در پوشانه برسد.

$$\text{Emb: } H=\begin{bmatrix}001000\\000110\\010101\end{bmatrix} \rightarrow \begin{bmatrix}001000\\000110\\010101\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\end{bmatrix}\oplus\begin{bmatrix}1\\0\\0\end{bmatrix}=$$

$$\begin{bmatrix}0\\0\\1\end{bmatrix} \rightarrow X' = 1110001$$

$$\text{Exc: } H=\begin{bmatrix}001000\\000110\\010101\end{bmatrix} \rightarrow \begin{bmatrix}001000\\000110\\010101\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix} \rightarrow M= 100$$

در این روش، بسته به کدی که مورد استفاده قرار می‌گیرد، می‌توان از سه پارامتر ذیل در بهبود عملکرد روش پیشنهادی بهره جست [۲۱]:

- ظرفیت نسبی $\propto = \frac{n}{N}$
- نرخ تغییرات $R= \frac{\rho}{N}$
- کارایی $e = \frac{\propto}{(\frac{\rho}{N})} = \frac{n}{\rho}$

در همین خصوص ما در طرح خود به‌منظور کسب نتایج مطلوب و بهینه‌نمودن روش، به دنبال کارایی و در نتیجه به دنبال کاهش شعاع پوششی نسبی یا $\frac{\rho}{N}$ می‌باشیم [۱۷].

برای مثال‌های بالا، به‌ترتیب ظرفیت نسبی برابر با $\frac{3}{7}$ و $\frac{3}{6}$، نرخ تغییرات $\frac{1}{7}$ و $\frac{1}{6}$ با کارایی مؤثر در هردو مثال برابر ۳ خواهد بود.

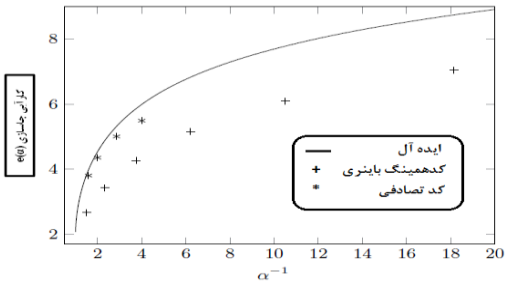
یکی خانواده از کدهای بسیار پرکاربرد، کدهای همینگ هستند. ولی به‌علت بهینه‌نبودن این نوع کدها طبق جدول (۱)، جاسازی مناسبی را در اختیار نمی‌گذارند و از ظرفیت نسبی ایده آلی برخوردار نمی‌باشند. این موضوع را به‌صورت عملی و شبیه‌سازی شده در بخش بعدی نشان خواهیم داد.

جدول (۱): کارایی و ظرفیت نسبی کد همینگ $[2p-1, 2p-1-p]$

بعد همینگ (P)	۱	۲	۳	۴	۵	۶	۷
ظرفیت نسبی ($\propto_p$)	۱/۰۰۰	۰/۶۶۷	۰/۴۲۹	۰/۲۶۷	۰/۱۶۱	۰/۰۹۳	۰/۰۵۵
کارایی (e_p)	۲/۰۰	۲/۶۶۷	۳/۴۲۹	۴/۲۶۷	۵/۱۶۱	۶/۰۹۳	۷/۰۵۵

بنابراین، باید به‌دنبال کدهای بهینه یا تصادفی بود. در نمودار (۱) کارایی کد تصادفی و کد همینگ دودویی را برحسب آنتروپی آن‌ها طبق روابط (۴-۳) نشان داده شده است.

نمودار (۱): مقایسه کارایی کد همینگ و کد تصادفی



$$H(x) = -x\ log_2\ x - (1-x)\ log_2(1-x) \qquad (۳)$$

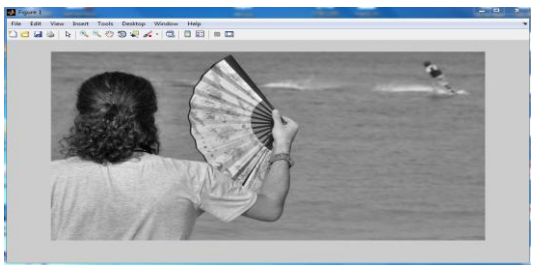
$$e = \frac{\alpha n}{R} \leq \frac{\alpha}{H-1(\alpha)} \qquad (۴)$$

توجه داریم که $\frac{R\alpha}{n}$ میانگین فاصله نسبی کد بوده و به‌نوعی هم تعیین‌کننده کارایی جاسازی و شعاع پوششی نسبی نیز می‌باشد. حال اگر کد توافقی در این روش بهینه یا ایده‌آل باشد ($n\rightarrow\infty$) [۲۴] نمی‌توان از این روش به‌صورت کاربردی استفاده نمود، چراکه $\frac{R}{n} \rightarrow 0$ و خواهیم داشت، $\frac{(n-k)}{n} = 1-\frac{k}{n} = 1$ که در این صورت نمی‌توان مشخصه‌ها و یا سردسته‌ها را در حالت کلی به دست آورد.

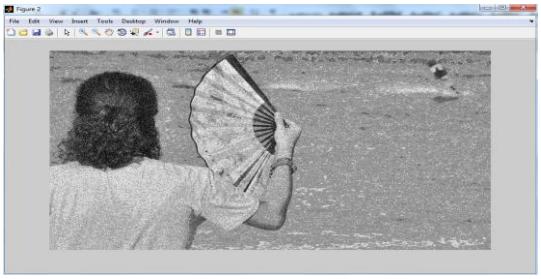
کلیه شبیه‌سازی‌ها و نهان‌نگاری‌ها در این مقاله، برحسب کد همینگ می‌باشد، چرا که این کد در روش جاسازی ماتریس از عملکرد ضعیفی برخوردار است و ما با درنظرگرفتن این کد ضعیف توانسته‌ایم مقاومت و امنیت این روش را تا حد چشم‌گیری بهبود دهیم. در این صورت، می‌توان ادعا نمود که روش‌های پیشنهادی برای سایر کدهای مناسب، عملکرد بهتری از خود نشان خواهد داد.

۲-۲- شبیه‌سازی نهان‌نگاری با استفاده از نظریه کدگذاری (جاسازی ماتریس)

شکل (۱) را با فرمت bmp، به‌عنوان یک پوشانه پوششی با اندازه ۳۵۸ KB درنظر می‌گیریم. حال روش جاسازی ماتریس معرفی‌شده را برحسب رابطه (۲) برروی آن به ازای تمام پیکسل‌های پوشانه با استفاده از نرم‌افزار Matlab براساس ماتریس کنترل مشابهت کد همینگ ذکرشده در مثال اول، شبیه‌سازی می‌نماییم. نتیجه حاصل در شکل (۲) و جدول (۲) آورده شده است.



شکل (۱): تصویر اولیه پوشانه بدون جاسازی



شکل (۲): تصویر پوشانه بعد از جاسازی

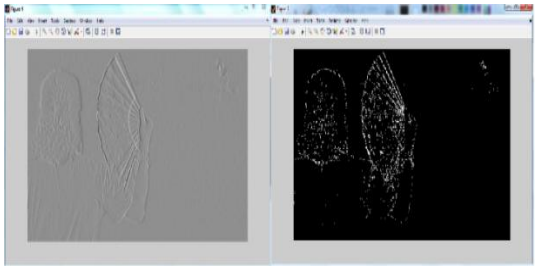
جدول (۲): شبیه‌سازی روش جاسازی ماتریس به ازای تمام پیکسل‌های پوشانه

ظرفیت جاسازی	PSNR	SSIM	امنیت
۱ MB	۱۹/۹۰	۰/۴۳	پایین

در شکل فوق، مقدار ظرفیت جاسازی خوب می‌باشد اما میزان تغییرات بالا رفته است. به‌منظور جلوگیری از این تغییرات بالا می‌توان این روش را در نقاط لبه[1] پیاده نمود.

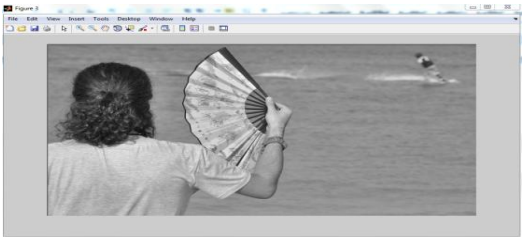
تحقیقات گوناگونی به‌منظور ارائه راه‌حل‌هایی برای یافتن لبه در تصاویر دیجیتال صورت گرفته است. پیکسل‌های لبه را می‌توان پیکسل‌هایی اختیار نمود که در آن‌ها شدت روشنایی تابع تصویر، تغییرات ناگهانی دارد و لبه‌ها را می‌توان مجموعه‌ای از پیکسل‌های لبه متصل به‌هم درنظر گرفت. آشکارسازهای لبه[2] روش‌هایی هستند که تغییرات محلی در شدت روشنایی پیکسل‌ها را تشخیص می‌دهند [۲۲]. هدف از آشکارسازی لبه، مکان‌یابی محدوده اشیا در تصویر است و می‌تواند به‌عنوان بینایی برای استفاده در آنالیزهای تصاویر و ماشین بینایی[3] موردتوجه قرار گیرد [۲۳]. کنی یکی از الگوریتم‌های لبه‌یابی است که یک سطح آستانه دارد. این آستانه تفاضل سطح شدت‌ها است. هرجا سطح شدت روشنایی کم باشد، لبه‌یابی ضعیف می‌شود و هرجا سطح روشنایی زیاد باشد لبه‌یابی مناسب‌تر است. زمانی‌که نیاز به لبه‌یابی قوی باشد، با درنظرگرفتن شیب‌ها از الگوریتم کنی استفاده می‌کنیم. کنی برای اختلاف سطح روشنایی‌ها، سه سطح آستانه دارد. اگر اختلاف سطح شدت از آستانه اول بیش‌تر باشد آن سطح به‌عنوان لبه شناخته می‌شود، اگر از آستانه دوم کوچک‌تر باشد لبه‌ای وجود ندارد و اگر بین این دو مقدار باشد یک لبه ضعیف وجود دارد، یعنی پیوستگی لبه‌ها را حفظ می‌کند.

حال اگر الگوریتم لبه‌یابی کنی را بر روی تصویر پوشانه اصلی (شکل۱) اجرا نماییم، خروجی آن شکل (۳) خواهد بود که نقاط لبه را برای ما مشخص خواهد نمود.



شکل (۳): اجرای الگوریتم کنی بر روی تصویر پوشانه اصلی

با اجرا روش نهان‌نگاری پیشنهادی بر روی نقاط لبه‌ای پوشانه اصلی، نتیجه‌ای طبق شکل (۴) و جدول (۳) حاصل می‌گردد.

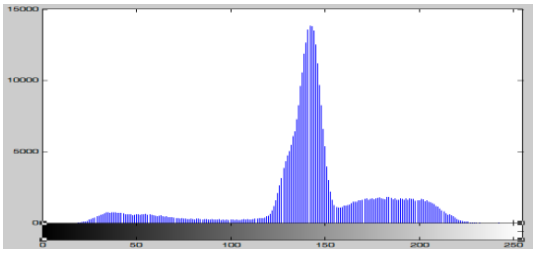


شکل (۴): اجرای روش جاسازی ماتریس بر روی لبه‌های کنی

جدول (۳): شبیه‌سازی روش جاسازی ماتریس در نقاط لبه‌ای پوشانه

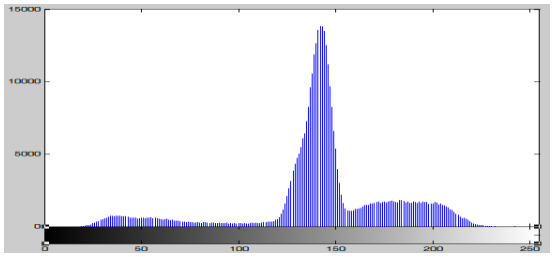
ظرفیت جاسازی	PSNR	SSIM	امنیت
۳ bit *تعداد لبه‌ها= ۱۳۰ KB	۲۹/۹۴	۰/۹۹۶	متوسط

لازم به ذکر می‌باشد که با این روش، در هر نقطه لبه‌ای با عمق ۸ بیتی تصویر خاکستری توانستیم ۳ بیت اطلاعات جاسازی نماییم، اما همان‌طوری‌که از جدول (۳) ملاحظه می‌نمایید امنیت و PSNR این روش به‌عنوان یک روش نهان‌نگاری، مطلوب نمی‌باشد. این امر را با مقایسه نمودار هیستوگرام تصویر پوشانه اصلی (شکل ۱) و تصویر نهان‌نگاری‌شده با روش فوق را طبق شکل‌های ذیل می‌توان به‌وضوح مشاهده نمود به‌طوری که دارای تغییرات محسوسی می‌باشند.



شکل (۵): نمودار هیستوگرام پوشانه اصلی

1- Edge
2- Edge detectors
3- Machine vision



شکل (۶): نمودار هیستوگرام پوشانه نهان‌نگاری شده

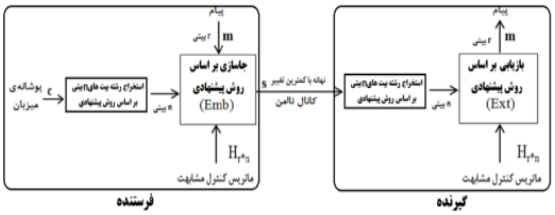
همان‌طوری‌که مشاهده می‌کنیم، نتیجه این روش نهان‌نگاری شفافیت بالای آن است که تنها با یک ماتریس کنترل مشابهت مشترک بین فرستنده و گیرنده می‌باشد.

۳- روش پیشنهادی

این مقاله روش ترکیبی را برای بهبود روش جاسازی ماتریس ارائه می‌دهد که از نظر امنیت و سایر پارامترهای ارزیابی نسبت به بقیه روش‌های این حوزه مناسب‌تر بوده و از کارایی بالایی برخوردار می‌باشد. این روش نهان‌نگاری ترکیبی پیشنهادی، به‌منظور افزایش امنیت، با حفظ مشابهت و شفافیت بالا، روش LSBM را در روش جاسازی ماتریس مورد استفاده قرار داده و آن‌را به‌عنوان یک روش نهان‌نگاری بهبودیافته موردتوجه قرار می‌دهد. مراحل اجرای روش پیشنهادی طبق ترتیب ذیل می‌باشد:

- ابتدا ماتریس کنترل مشابهت H_{k*n} به‌صورت محرمانه، بین فرستنده و گیرنده توافق می‌گردد.
- یک پوشانه با ابعاد C*R را درنظر گرفته که محتویات آن به‌صورت پیکسلی بوده و نشان‌دهنده روشنایی است.
- پوشانه انتخاب‌شده را به‌صورت n پیکسل، n پیکسل مرتب می‌کنیم و با توجه به این‌که کم‌ترین تغییرات پیکسل در LSB آن‌ها است، ما LSB آن n پیکسل را درنظر گرفته و رشته‌های nبیتی x_t $\|x_2\|\ldots.\|x_1$ را $X=x_1\|x_2\|\ldots.\|x_t$ تشکیل می‌دهیم که از پوشانه استخراج شده است.
- پیام را با عمل لایه گذاری[1] مضربی از k نموده و خواهیم داشت: $M=m_1\|m_2\|\ldots.\|m_t$.
- حالا H را در ترانهاده رشته‌های nبیتی x_i پوشانه ضرب نموده و یک رشته kبیتی به دست می‌آوریم. هرکدام از این حاصل‌ضرب‌ها را با پیام m_i =k جمع (xor) نموده و رشته kبیتی به دست می‌آید.
- این رشته‌های kبیتی حاصل‌جمع، نشان‌دهنده ستون i ماتریس H می‌باشد و نشان‌دهنده تغییر بیت iام (0→1) رشته‌های nبیتی پوشانه می‌باشد که نتیجه آن، نهانه خواهد بود ($x_i \rightarrow x'_i$).
- رشته nبیتی حاصل (x'_i) را به‌عنوان LSB متناظر n پیکسل پوشانه درنظر گرفته و آن نهانه را به گیرنده ارسال می‌کنیم.
- چون روند خطی بوده ($A\oplus B=D\leftrightarrow D\oplus A=B$)، لذا بازیابی پیام برگشت‌پذیر خواهد بود و گیرنده به‌راحتی با ضرب ماتریس H در ترانهاده هر رشته nبیتی متشکل از LSB، n پیکسل نهانه دریافتی یا همان $X'=x'_1\|x'_2\|\ldots.\|x'_t$، می‌تواند پیام $M=m_1\|m_2\|\ldots.\|m_t$ را استخراج کند.

بلوک دیاگرام روش پیشنهادی طبق شکل (۷) می‌باشد.



شکل (۷): بلوک دیاگرام روش پیشنهادی

روش فوق را با یک مثال ساده شرح می‌دهیم. فرض کنید C کد همینگ C=[7,4,3] با طرح cov(1,7,3) که Xهای nبیتی را از بیت‌های کم‌ارزش ۷ پیکسل متوالی همانند شکل (۸) تهیه شده، استخراج می‌کنیم.

شکل (۸): جاسازی رشته بیت استخراجی از بیت‌های کم‌ارزش ۷ پیکسل پوشانه

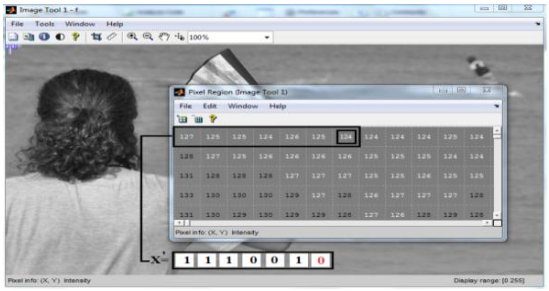
در نتیجه، با روش پیشنهادی خواهیم داشت:

$$\text{Emb: } M=110,\ X=1110011 \rightarrow \begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\1\\1\end{bmatrix}=\begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$\begin{bmatrix}1\\1\\1\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\end{bmatrix}\rightarrow X'=1110010$$

1- Padding

بنابراین، پوشانه حامل(نهانه)، بعد از جاسازی به‌صورت شکل (۹) خواهد شد:

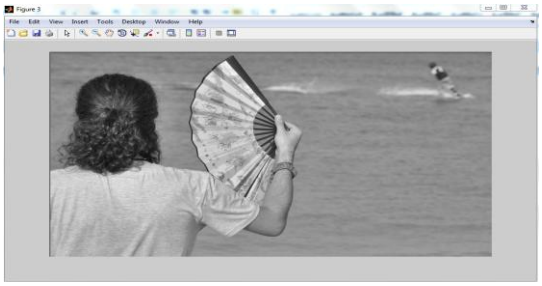


شکل (۹): نهانه حاصل بعد از فرایند جاسازی اطلاعات

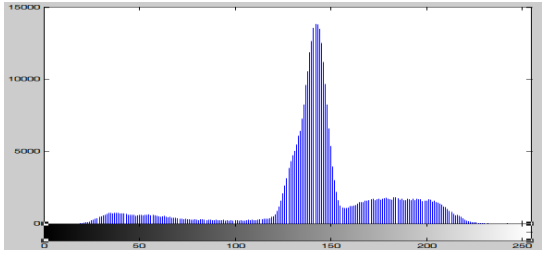
حال گیرنده با دریافت نهانه و همچنین با دانستن ماتریس H، به سادگی می تواند پیام محرمانه را استخراج کند.

$$\text{Exc: } H=\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}\rightarrow\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}1\\1\\0\end{bmatrix}\rightarrow M=110$$

مشاهده می‌کنیم که با کاهش نسبی ظرفیت، مقاومت نهان‌نگاری افزایش می‌یابد. شکل (۱۰)، تصویر نهان‌نگاری‌شده پوشانه اولیه (شکل ۱) می‌باشد به‌طوری‌که در هر ۷ بیت کم‌ارزش پوشانه، ۳ بیت اطلاعات جاسازی‌شده به‌نحوی‌که حداکثر یک بیت از پوشانه اولیه تغییر می‌نماید.



شکل (۱۰): تصویر نهان‌نگاری‌شده با استفاده از روش پیشنهادی



شکل (۱۱): نمودار هیستوگرام شکل نهان‌نگاری‌شده با استفاده از روش پیشنهادی

نتیجه روش نهان‌نگاری به‌صورت جدول (۴) می‌باشد:

جدول (۴): نتیجه نهان‌نگاری شکل (۹) با استفاده از روش پیشنهادی

ظرفیت جاسازی	PSNR	SSIM	امنیت
۱۵۶ KB	۵۹/۱۵	۰/۹۹۹۶	٪۷۵

نکته اساسی: به‌منظور بهبود عملکرد روش پیشنهادی، می‌توان آن‌را در نقاط لبه‌ای اجرا نمود. به‌عبارت دیگر، استفاده ترکیبی از LSB چندپیکسل لبه‌ای که نتایج عملی آن در بخش ۳-۱-۳ ارائه گردیده است.

جدول (۵): شبیه‌سازی نهان‌نگاری روش پیشنهادی و LSB

تصاویر	روش پیشنهادی		LSB	
	PSNR	SSIM	PSNR	SSIM
۱	۵۶/۹۹۳	۰/۹۹۹۳	۵۵/۱۲	۰/۹۹۹۴
۲	۵۷/۱۵۶	۰/۹۹۹۳	۵۵/۱۲	۰/۹۹۸۹
۳	۵۷/۱۲۱	۰/۹۹۹۷	۵۵/۱۳	۰/۹۹۹۶
۴	۵۷/۱۵۸	۰/۹۹۹۸	۵۵/۱۲	۰/۹۹۹۶
۵	۵۷/۱۶۹	۰/۹۹۹۷	۵۵/۱۱	۰/۹۹۹۵
۶	۵۷/۱۶۸	۰/۹۹۹۸	۵۵/۱۱	۰/۹۹۹۶
۷	۵۷/۱۷۰	۰/۹۹۹۷	۵۵/۱۱	۰/۹۹۹۵
۸	۵۷/۱۷۰	۰/۹۹۹۸	۵۵/۱۲	۰/۹۹۹۷
۹	۵۷/۱۶۸	۰/۹۹۹۹	۵۵/۱۱	۰/۹۹۹۸
۱۰	۵۷/۱۷۳	۰/۹۹۹۸	۵۵/۱۱	۰/۹۹۹۶
۱۱	۵۷/۱۵۸	۰/۹۹۹۸	۵۵/۱۱	۰/۹۹۹۶
۱۲	۵۷/۱۶۵	۰/۹۹۹۷	۵۵/۱۱	۰/۹۹۹۵
۱۳	۵۷/۱۷۰	۰/۹۹۹۸	۵۵/۰۸	۰/۹۹۹۷
۱۴	۵۷/۱۶۵	۰/۹۹۹۶	۵۵/۱۱	۰/۹۹۹۳
۱۵	۵۷/۱۷۵	۰/۹۹۹۷	۵۵/۱۴	۰/۹۹۹۵
۱۶	۵۷/۱۷۱	۰/۹۹۹۵	۵۵/۱۰	۰/۹۹۹۲
۱۷	۵۷/۰۸۵	۰/۹۹۹۵	۵۵/۱۴	۰/۹۹۹۵
۱۸	۵۷/۱۷۰	۰/۹۹۹۶	۵۵/۱۱	۰/۹۹۹۴
۱۹	۵۷/۱۶۷	۰/۹۹۹۸	۵۵/۱۲	۰/۹۹۹۷
۲۰	۵۷/۱۶۰	۰/۹۹۹۸	۵۵/۱۳	۰/۹۹۹۷
۲۱	۵۷/۱۶۹	۰/۹۹۹۶	۵۵/۱۳	۰/۹۹۹۴
۲۲	۵۷/۱۵۶	۰/۹۹۹۸	۵۵/۱۰	۰/۹۹۹۶
۲۳	۵۷/۱۷۵	۰/۹۹۹۵	۵۵/۱۳	۰/۹۹۹۲
۲۴	۵۷/۱۷۵	۰/۹۹۹۵	۵۵/۱۱	۰/۹۹۹۳
۲۵	۵۷/۱۶۸	۰/۹۹۹۶	۵۵/۱۲	۰/۹۹۹۴
۲۶	۵۷/۱۶۳	۰/۹۹۹۹	۵۵/۱۱	۰/۹۹۹۹
۲۷	۵۷/۱۷۵	۰/۹۹۹۸	۵۵/۱۲	۰/۹۹۹۷
۲۸	۵۷/۱۵۰	۰/۹۹۹۶	۵۵/۱۴	۰/۹۹۹۴
۲۹	۵۷/۱۸۲	۰/۹۹۹۹	۵۵/۱۱	۰/۹۹۹۸
۳۰	۵۷/۱۵۸	۰/۹۹۹۸	۵۵/۱۳	۰/۹۹۹۶

۳-۱- شبیه‌سازی روش پیشنهادی و ارزیابی آن با سایر روش‌ها

در این‌جا شبیه‌سازی با استفاده از نرم‌افزار MATLAB (2013.b) انجام می‌گیرد؛ بنابراین‌T در اجرای شبیه‌سازی به‌راحتی می‌توان فرمت‌های مختلفی از تصاویر را با اندازه‌های مختلف در نظر گرفت.

۳-۱-۱- شبیه‌سازی و مقایسه روش ترکیبی پیشنهادی و روش LSB با ظرفیت یکسان

در همین راستا، ابتدا به بررسی و اجرای روش نهان‌نگاری بهبودیافته پیشنهادی بر روی ۳۰ تصویر پوشانه با فرمت bmp با ابعاد (۵۱۲×۵۱۲) با اندازه‌های مختلف و براساس همان ماتریس کنترل مشابهت مثال‌های فوق (H3*7) و ظرفیت نهان‌نگاری ۰/۴۳ می‌پردازیم. نتایج حاصل را با خروجی شبیه‌سازی روش LSB با ظرفیت ۰/۴۰ را برای همان تصاویر پوشانه، مورد ارزیابی قرار می‌دهیم.

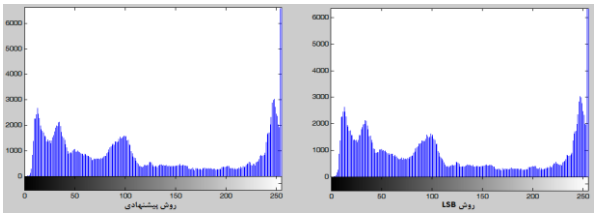
دقت داشته باشید که منظور از روش پیشنهادی استفاده از ۷ بیت LSB، ۷ پیکسل متوالی می‌باشد و به‌عبارت دیگر، اجرای روش در کل تصاویر و به ازای تمام پیکسل‌ها می‌باشد.

در ادامه اگر میانگین را برای هر دو روش شبیه‌سازی‌شده (روش پیشنهادی و روش LSB) محاسبه نماییم، نتایج جدول (۶) به دست خواهد آمد.

جدول (۶):میانگین اجرای روش پیشنهادی و LSB بر روی ۳۰ تصویر

معیار	ظرفیت	PSNR	SSIM	امنیت
روش پیشنهادی	۰/۴۳	۵۷/۱۵۷	۰/۹۹۹۷	خوب
روش LSB	۰/۴۰	۵۵/۱۱	۰/۹۹۹۵	خوب

اگر برای یک تصویر مشخص از بانک تصاویر، در هر دو روش نمودار هیستوگرام را ترسیم نماییم، شکل (۱۲) به دست می‌آید که به کمک جعبه‌ابزار پردازش تصویر نرم‌افزار MATLAB، خواهیم دانست که هیستوگرام روش پیشنهادی بیش‌ترین تشابه را به نمودار تصویر اولیه دارد.



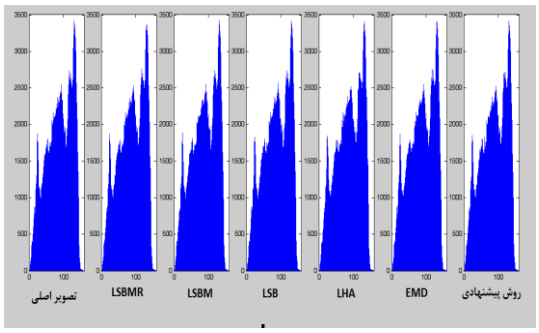
شکل (۱۲): هیستوگرام روش پیشنهادی و LSB برای یک تصویر

با بررسی نتایج به‌دست‌آمده از شبیه‌سازی روش بالا، می‌توان نتیجه گرفت که روش پیشنهادی از عملکرد مناسب و بهتری برخوردار است.

می‌توان خاطرنشان نمود که در روش پیشنهادی اگر ما برای نهان‌نگاری از ماتریس کنترل مشابهتی یا تصویر پوشانه‌ای استفاده نماییم که تعداد ستون‌های ماتریس و ستون‌های تصویر پوشانه مضربی از یکدیگر باشند. یا به‌عبارت دیگر، اگر ابعاد تصویر پوشانه را طوری تغییر دهیم که ستون‌های تصویر مضربی از تعداد ستون‌های ماتریس کنترل مشابهت توافقی باشد؛ در این حالت، حداکثر مقدار شفافیت برای تصویر نهانه قابل تصور می‌باشد.

۳-۱-۲- شبیه‌سازی و ارزیابی روش پیشنهادی و سایر روش‌های حوزه مکان

حال همان بانک تصاویر را با فرمت bmp و اندازه و ابعاد (۵۱۲×۵۱۲) یکسان، برای روش پیشنهادی و سایر روش‌های حوزه مکان با ظرفیت یکسان شبیه‌سازی نموده و نتایج آن را تحت جدول (۷) ارائه می‌نماییم. شکل (۱۳)، مقایسه بین نمودار هیستوگرام‌های روش‌های مختلف برای یک تصویر تصادفی می‌باشد که با مقایسه آن‌ها متوجه می‌شویم که هیستوگرام روش پیشنهادی بیش‌ترین شباهت را به هیستوگرام تصویر اصلی دارد. در همین خصوص و با توجه به جدول مذکور و مقایسه نتایج حاصل از آن، به‌راحتی می‌توان نتیجه گرفت که مبتنی بر ظرفیت برابر، روش پیشنهادی از لحاظ دو معیار SSIM و PSNR عملکرد بهتری دارد.



شکل (۱۳): مقایسه هیستوگرام روش‌های مختلف

از نظر امنیت، روش پیشنهادی و سایر روش‌های موجود نسبت به نرم‌افزار نهان‌کاو، تقریباً عملکرد یکسانی داشته با این تفاوت که فرایند جاسازی در روش پیشنهادی به ازای تمام پیکسل‌های پوشانه بوده است. بر همین اساس و به‌منظور افزایش امنیت و بهبود روش ترکیبی پیشنهادی، سراغ اجرا بر روی نقاط لبه‌ای کنی می‌رویم.

جدول (۷): نتیجه نهان‌نگاری بر روی ۳۰ تصویر bmp در روش‌های مختلف حوزه مکان

تصاویر	روش پیشنهادی		EMD		LHA		LSB		LSBM		LSBMR	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
۱	۵۶/۹۹۳	۰/۹۹۹۳	۵۶/۲۹	۰/۹۹۹۸	۵٤/۱۵	۰/۹۹۹۳	۵٤/۱۵	۰/۹۹۹۲	۵٤/۱۵	۰/۹۹۹۲	۵۲/۷۲	۰/۹۹۸۱
۲	۵۷/۱۵٦	۰/۹۹۹۳	۵٦/۳۰	۰/۹۹۹۲	۵٤/۱۷	۰/۹۹۸۷	۵٤/۱۳	۰/۹۹۸٦	۵٤/۱٤	۰/۹۹۸۷	۵۵/٤۰	۰/۹۹۹
۳	۵۷/۱۲۱	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹۷	۵٤/۱۵	۰/۹۹۹٦	۵٤/۱٤	۰/۹۹۹۵	۵٤/۱۵	۰/۹۹۹۵	۵٤/٦۲	۰/۹۹۹٤
۴	۵۷/۱۵۸	۰/۹۹۹۸	۵٦/۲۸	۰/۹۹۹۷	۵٤/۱۳	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹۵	۵٤/۱۵	۰/۹۹۹۵	۵٤/۹۹	۰/۹۹۹٦
۵	۵۷/۱٦۹	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹۷	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱٤	۰/۹۹۹٤	۵۵/٤۰	۰/۹۹۹٦
۶	۵۷/۱٦۸	۰/۹۹۹۸	۵٦/۲۸	۰/۹۹۹۷	۵٤/۱٤	۰/۹۹۹٦	۵٤/۱۳	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹۵	۵۵/۳۹	۰/۹۹۹۷
۷	۵۷/۱۷۰	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹٦	۵٤/۱۳	۰/۹۹۹٤	۵٤/۱۵	۰/۹۹۹۳	۵٤/۱٤	۰/۹۹۹۳	۵۵/۳۱	۰/۹۹۹۵
۸	۵۷/۱۷۰	۰/۹۹۹۸	۵٦/۲۷	۰/۹۹۹۸	۵٤/۱۵	۰/۹۹۹۷	۵٤/۱٤	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹٦	۵۵/۳۹	۰/۹۹۹۷
۹	۵۷/۱٦۸	۰/۹۹۹۹	۵٦/۲۹	۰/۹۹۹۸	۵٤/۱٤	۰/۹۹۹۸	۵٤/۱٤	۰/۹۹۹۷	۵٤/۱۵	۰/۹۹۹۸	۵۵/۳۹	۰/۹۹۹۸
۱۰	۵۷/۱۷۳	۰/۹۹۹۸	۵٦/۲۹	۰/۹۹۹۷	۵٤/۱۵	۰/۹۹۹٦	۵٤/۱٦	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹٦	۵۵/۳۹	۰/۹۹۹۷
۱۱	۵۷/۱۵۸	۰/۹۹۹۸	۵٦/۲۸	۰/۹۹۹۷	۵٤/۱٤	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹۵	۵٤/۱۵	۰/۹۹۹٦	۵۵/۳۱	۰/۹۹۹۷
۱۲	۵۷/۱٦۵	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹۷	۵٤/۱۲	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹٤	۵٤/۱٦	۰/۹۹۹٤	۵۵/۳۹	۰/۹۹۹٦
۱۳	۵۷/۱۷۰	۰/۹۹۹۸	۵٦/۲۷	۰/۹۹۹۸	۵٤/۱٦	۰/۹۹۹۷	۵٤/۱۳	۰/۹۹۹۷	۵٤/۱۵	۰/۹۹۹۷	۵۵/۲٦	۰/۹۹۹۷
۱۴	۵۷/۱٦۵	۰/۹۹۹٦	۵٦/۳۰	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹۱	۵٤/۱٦	۰/۹۹۹۱	۵٤/۱۵	۰/۹۹۹۱	۵۵/۳۹	۰/۹۹۹۳
۱۵	۵۷/۱۷۵	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹٦	۵٤/۱۳	۰/۹۹۹٤	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱٤	۰/۹۹۹٤	۵۵/٤۰	۰/۹۹۹۵
۱۶	۵۷/۱۷۱	۰/۹۹۹۵	۵٦/۲۹	۰/۹۹۹٤	۵٤/۱٤	۰/۹۹۹۰	۵٤/۱۳	۰/۹۹۹۹	۵٤/۱۵	۹۹۹/۰	۵۵/٤۰	۰/۹۹۹۲
۱۷	۵۷/۰۸۵	۰/۹۹۹۵	۵٦/۲۸	۰/۹۹۹۷	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱٤	۰/۹۹۹۳	۵٤/۱۵	۰/۹۹۹۳	۵۵/۸۲	۰/۹۹۸۹
۱۸	۵۷/۱۷۰	۰/۹۹۹٦	۵٦/۲۸	۰/۹۹۹٦	۵٤/۱٦	۰/۹۹۹۳	۵٤/۱۵	۰/۹۹۹۳	۵٤/۱۲	۰/۹۹۹۳	۵۵/۳۹	۰/۹۹۹۵
۱۹	۵۷/۱٦۷	۰/۹۹۹۸	۵٦/۲۹	۰/۹۹۹۸	۵٤/۱٦	۰/۹۹۹٦	۵٤/۱٤	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹٦	۵۵/٤۰	۰/۹۹۹۷
۲۰	۵۷/۱٦۰	۰/۹۹۹۸	۵٦/۲۹	۰/۹۹۹۸	۵٤/۱٦	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹٦	۵٤/۱٦	۰/۹۹۹٦	۵۵/۳۸	۰/۹۹۹۷
۲۱	۵۷/۱٦۹	۰/۹۹۹٦	۵٦/۲۹	۰/۹۹۹۵	۵٤/۱۵	۰/۹۹۹۳	۵٤/۱٦	۰/۹۹۹۲	۵٤/۱٦	۰/۹۹۹۳	۵۵/۳۹	۰/۹۹۹٤
۲۲	۵۷/۱۵٦	۰/۹۹۹۸	۵٦/۲۹	۰/۹۹۹۷	۵٤/۱۲	۰/۹۹۹٦	۵٤/۱۳	۰/۹۹۹۵	۵٤/۱۸	۰/۹۹۹٦	۵۵/٤۱	۰/۹۹۹۷
۲۳	۵۷/۱۷۵	۰/۹۹۹۵	۵٦/۲۸	۰/۹۹۹٤	۵٤/۱۵	۹۹۹/۰	۵٤/۱۵	۰/۹۹۸۹	۵٤/۱۷	۰/۹۹۹۰	۵۵/۳۸	۰/۹۹۹۲
۲۴	۵۷/۱۷۵	۰/۹۹۹۵	۵٦/۲۹	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹۲	۵٤/۱۵	۰/۹۹۹۱	۵٤/۱٤	۰/۹۹۹۱	۵۵/٤۰	۰/۹۹۹۳
۲۵	۵۷/۱٦۸	۰/۹۹۹٦	۵٦/۲۹	۰/۹۹۹٦	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱٤	۰/۹۹۹۳	۵٤/۱۵	۰/۹۹۹۳	۵۵/۲٤	۰/۹۹۹۵
۲۶	۵۷/۱٦۳	۰/۹۹۹۹	۵٦/۲۸	۰/۹۹۹۹	۵٤/۱۷	۰/۹۹۹۹	۵٤/۱۲	۰/۹۹۹۹	۵٤/۱٤	۰/۹۹۹۹	۵۵/۳٦	۰/۹۹۹۹
۲۷	۵۷/۱۷۵	۰/۹۹۹۸	۵٦/۲۸	۰/۹۹۹۸	۵٤/۱٦	۰/۹۹۹۷	۵٤/۱٤	۰/۹۹۹۷	۵٤/۱۵	۰/۹۹۹۷	۵۵/٤۱	۰/۹۹۹۸
۲۸	۵۷/۱۵۰	۰/۹۹۹٦	۵٦/۲۹	۰/۹۹۹٦	۵٤/۱٦	۰/۹۹۹٤	۵٤/۱۳	۰/۹۹۹۳	۵٤/۱٤	۰/۹۹۹۳	۵٤/۸٦	۰/۹۹۹۳
۲۹	۵۷/۱۸۲	۰/۹۹۹۹	۵٦/۲۹	۰/۹۹۹۹	۵٤/۱۵	۰/۹۹۹۸	۵٤/۱۵	۰/۹۹۹۸	۵٤/۱٤	۰/۹۹۹۸	۵۵/۳٤	۰/۹۹۹۸
۳۰	۵۷/۱۵۸	۰/۹۹۹۸	۵٦/۲۷	۰/۹۹۹۷	۵٤/۱٤	۰/۹۹۹٦	۵٤/۱٤	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹٦	۵۵/٤۰	۰/۹۹۹۷
میانگین	۵۷/۱۵۷	۰/۹۹۹۷	۵٦/۲۹	۰/۹۹۹٦	۵٤/۱۵	۰/۹۹۹۵	۵٤/۱٤	۰/۹۹۹٤	۵٤/۱۵	۰/۹۹۹٤	۵۵/۲٤	۰/۹۹۹۵

۳-۱-۳- شبیه‌سازی روش پیشنهادی بر روی نقاط لبه‌ای و ارزیابی آن با سایر روش‌ها

حال با توجه به مطالب گفته‌شده و با اجرای روش پیشنهادی بر روی نقاط لبه‌ای در همان بانک تصاویر موجود، نتایج جدول (۸) به‌دست خواهد آمد. خاطرنشان می‌کنیم که موفقیت نرم‌افزارهای نهان‌کاوی در این روش بین ۰ ٪ الی ۶ ٪ می‌باشد. در ادامه، اگر روش LSB هم را برای نقاط لبه‌ای بانک تصاویر با همان ظرفیت روش بهبودیافته پیشنهادی اجرا نماییم، نتیجه جدول (۹) خواهد بود. نتیجه ارزیابی و مقایسه دو روش در نقاط لبه‌ای، در جدول (۱۰) آمده است.

جدول (۸): اجرای روش پیشنهادی بر روی نقاط لبه‌ای

تصاویر	PSNR	SSIM	تصاویر	PSNR	SSIM
۱	۷۱/۰۳	۱/۰۰۰	۱۶	۷۷/۴۶	۱/۰۰۰
۲	۸۱/۲۱	۱/۰۰۰	۱۷	۷۰/۱۸	۱/۰۰۰
۳	۷۱/۱۷	۱/۰۰۰	۱۸	۷۳/۷۸	۱/۰۰۰
۴	۷۱/۴۵	۱/۰۰۰	۱۹	۶۹/۲۲	۱/۰۰۰
۵	۷۴/۲۲	۱/۰۰۰	۲۰	۷۸/۹۹	۱/۰۰۰
۶	۶۸/۲۱	۱/۰۰۰	۲۱	۶۸/۵۸	۱/۰۰۰
۷	۷۱/۱۳	۱/۰۰۰	۲۲	۶۹/۱۱	۱/۰۰۰
۸	۷۰/۷۵	۱/۰۰۰	۲۳	۶۸/۴۵	۱/۰۰۰
۹	۶۹/۶۹	۱/۰۰۰	۲۴	۷۳/۰۶	۱/۰۰۰
۱۰	۶۹/۳۴	۱/۰۰۰	۲۵	۷۰/۳۸	۱/۰۰۰
۱۱	۷۰/۵۴	۱/۰۰۰	۲۶	۷۰/۷۳	۱/۰۰۰
۱۲	۷۳/۵۷	۱/۰۰۰	۲۷	۶۹/۴۱	۱/۰۰۰
۱۳	۶۹/۴۰	۱/۰۰۰	۲۸	۷۳/۰۶	۱/۰۰۰
۱۴	۷۴/۷۸	۱/۰۰۰	۲۹	۶۷/۷۲	۱/۰۰۰
۱۵	۷۶/۹۷	۱/۰۰۰	۳۰	۷۳/۳۴	۱/۰۰۰

جدول (۹): اجرای روش LSB بر روی نقاط لبه‌ای

تصاویر	PSNR	SSIM	تصاویر	PSNR	SSIM
۱	۶۵/۰۰	۱/۰۰۰	۱۶	۷۱/۴۸	۱/۰۰۰
۲	۷۵/۲۸	۱/۰۰۰	۱۷	۶۴/۱۰	۱/۰۰۰
۳	۶۶/۱۰	۱/۰۰۰	۱۸	۶۷/۶۷	۱/۰۰۰
۴	۶۵/۴۰	۱/۰۰۰	۱۹	۶۳/۱۲	۱/۰۰۰
۵	۶۸/۲۵	۱/۰۰۰	۲۰	۷۱/۹۲	۱/۰۰۰
۶	۶۲/۲۳	۱/۰۰۰	۲۱	۶۲/۵۳	۱/۰۰۰
۷	۶۵/۰۱	۱/۰۰۰	۲۲	۶۳/۱۱	۱/۰۰۰
۸	۶۴/۶۷	۱/۰۰۰	۲۳	۶۲/۴۵	۱/۰۰۰
۹	۶۳/۶۲	۱/۰۰۰	۲۴	۶۷/۱۴	۱/۰۰۰
۱۰	۶۳/۳۸	۱/۰۰۰	۲۵	۶۴/۴۲	۱/۰۰۰
۱۱	۶۴/۵۸	۱/۰۰۰	۲۶	۶۴/۸۱	۱/۰۰۰
۱۲	۶۷/۴۳	۱/۰۰۰	۲۷	۶۳/۴۰	۱/۰۰۰
۱۳	۶۳/۴۵	۱/۰۰۰	۲۸	۶۷/۱۷	۱/۰۰۰
۱۴	۶۸/۴۰	۱/۰۰۰	۲۹	۶۶/۶۸	۱/۰۰۰
۱۵	۷۱/۱۵	۱/۰۰۰	۳۰	۶۶/۳۰	۱/۰۰۰

جدول (۱۰): ارزیابی روش پیشنهادی و روش LSB بر روی نقاط لبه‌ای

معیار	امنیت	PSNR	SSIM	تشابه هیستوگرام
روش بهبودیافته	٪۹۴ - ٪۱۰۰	۷۱/۸۶	۱/۰۰۰	٪ ۴۸
روش LSB	٪۸۵ - ٪۹۵	۶۵/۸۷	۱/۰۰۰	٪۳۲

با ارزیابی نتایج موجود در می‌یابیم که روش ترکیبی پیشنهادشده از کارایی و امنیت بالایی برخوردار می‌باشد.

۳-۲- مزایای روش پیشنهادی

لازم است در روش ترکیبی پیشنهادی به موارد ذیل تحت عنوان مزایای روش ترکیبی پیشنهادی توجه داشته باشیم:

- همان‌طوری‌که در مثال‌های بخش دوم و سوم مشاهده نمودیم، این روش مختص کدهای خطی نمی‌باشد و می‌تواند براساس سایر کدها نیز پیاده گردد.
- میزان پیام قابل جاسازی در رشته بیت پوشانه با تعداد سطرهای ماتریس کنترل مشابهت توافقی، متناسب می‌باشد.
- طول رشته بیت استخراجی از پوشانه، برای اجرای هر نهان‌نگاری متناسب با تعداد ستون‌های ماتریس کنترل مشابهت توافقی می‌باشد.
- دقت داشته باشید که ظرفیت و مقاومت سیستم نهان‌نگاری می‌تواند به‌صورت دو کفه ترازو عمل نماید. به‌طوری‌که در روش بهبودیافته پیشنهادی، می‌توان به‌جای ۷ بیت کم‌ارزش، ۷ پیکسل متوالی؛ از تعداد کم‌تری استفاده نموده و مقاومت را بالا برد. به‌عنوان مثال، برای جاسازی رشته بیت استخراجی ۷ بیتی، می‌توان از ۳ بیت کم‌ارزش یک پیکسل و ۴ بیت کم‌ارزش پیکسل بعدی استفاده نمود و اطلاعات را جاسازی نمود به‌نحوی‌که فقط یک بیت از ۷بیت رشته استخراجی تغییر می‌کند.
- با وجود کاهش نسبی ظرفیت نسبت به روش جاسازی ماتریس، روش پیشنهادی از ظرفیت مطلوبی نسبت به برخی از روش‌های نهان‌نگاری برخوردار است.
- این روند جاسازی پیام از مقاومت بالایی مقابل نهان‌کاوها برخوردار است.
- طبق نتایج ارائه‌شده، روش پیشنهادی بیش‌ترین PSNR و SSIM ممکن را برای یک سیستم نهان‌نگاری را دارد.
- برای عملکرد حداکثری سیستم، می‌توان از طرح کدهایی با ظرفیت بالا و کم‌ترین خرابی استفاده نماییم.
- از همان کد مشترک می‌توان به‌عنوان افزونگی و تشخیص و تصحیح خطا استفاده نمود.

۳-۳- معایب روش پیشنهادی

- نوع کد و ماتریس کنترل مشابهت آن، باید بین فرستنده و گیرنده به اشتراک گذاشته شود.[۲۶]
- در صورت استفاده از کدهای تصادفی، به‌دست‌آوردن مشخصه‌ها و یا سردسته‌ها در حالت کلی است [۲۶].

۴- نتیجه‌گیری

یکی از معیارهای جذابیت روش‌های نهان‌نگاری بستگی به میزان تحمل‌پذیری آن‌ها در برابر اغتشاش‌هایی دارد که در هریک از

گام‌های فرآیند نهان‌نگاری امکان رخداد داشته و می‌توانند تأثیرات مخربی را بر داده نهان‌نگاری‌شده اعمال نمایند. پیشنهاد این مقاله استفاده از ویژگی‌های کدها، به‌منظور نهان‌نگاری امن موردنیاز برای جاسازی نهان‌نگاری است. در راستای دست‌یابی به این هدف و ظرفیت حداکثری می‌توان از ماتریس کنترل مشابهتی با ابعاد متناسب استفاده نمود و یا ابعاد تصویر را با ابعاد ماتریس متناسب نمود.

براساس نتایج حاصل از آزمون‌های انجام‌شده در مرحله پیاده‌سازی، روش پیشنهادی بهبودیافته، علاوه‌بر ظرفیت و مقاومت بالا از دقت قابل قبولی در مواجه با حملات هندسی به ویژه عملیات فشرده‌سازی برخوردار است و از آن مهم‌تر می‌توان از تشخیص خطای احتمالی در رشته بیت دریافتی توسط گیرنده مجاز، در فرایند خود بهره برد.

۵- مراجع

[1] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevný, "Moving Steganography and Steganalysis from laboratory to Real World," In Proceedings of the ACM IH&MMSec'13, ACM, pp.ACM 978-1-4503-2081-8/13/06, Montpellier, France, June 2013.

[2] A. Bhatacharya, I. Banerjee, and G. Sanyal, "A survey of steganography and steganalysis techniques in image, text, audio and video cover carrier," Journal of Global Research in Computer Science, vol. 2, no. 4, pp. 1-16, 2011.

[3] I. J. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," Morgan Kaufmann Publishers, San Francisco, Calif, USA, 2nd revised dition, 2007.

[4] A. Cheddad, J. Condell, K. Curran, and P. Mckevitt, "Digital image steganography: Survey and analy sis of current methods," Signal Processing, vol. 90, no. 3, pp. 727-752, March 2010.

[5] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Lecture Notes in Computer Science, 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[6] L. J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm," Information Sciences, vol. 177, no. 15, pp. 3099-3109l, 2007.

[7] A. Westfeld, "Detecting low embedding rates," in 5th International Workshop on Information Hiding, Noordwijk erhout, The Netherlands, 2002.

[8] K. Chin Chang, C. Ping Huang, S. Ping, and T. Te-Ming, "A novel image steganographic method using triway pixel-value differencing, "Journal of Multimedia, vol. 3, no. 2, pp. 37-44, June 2008.

[9] H. Malekmohammadi and S. Ghaemmaghami, "Steganalysis of LSB Based Image Steganography Using Spatial And Frequency Domain Feature," IEEE Trans., 2009.

[10] H. Sajedi and M. Jamzad, "Selecting Steganography Method," IEEE, 2010.

[11] G. Cancelli and M. Barni, "MPSteg-color: data hiding through redundant basis decomposition," Inf Forensics Secur, IEEE Trans, vol. 4, no. 3, pp. 346–358, 2009.

[12] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," Secur Privacy, IEEE Trans, vol. 1, no. 3, pp. 32–44, 2003.

[13] A. Westfeld, "F5 a steganographic algorithm," in Information hiding, pp. 289–302, 2001.

[14] M. John Cioffi, "Digital Communication II: Coding," Spring Quarter, 2005-2006.

[15] M. khatirinejad, "Linear codes for high payload steganography, "IEEE Trans., Elsevier, 2009.

[16] M. Carlos, "Hamming codes for wet paper steganography," Springer Science Business, Media New York, 2015.

[17] J. Fridrich, "Steganography in Digital Media," IEEE Trans, Binghamton University, State University of New York, 2008.

[18] M. Morad, "Polar codes for secret sharing," Department of Mathematics Amirkabir University of Technolog, IEEE Trans, arXiv: 1705.03042 v1 [cs.CR], May 2017.

[19] J. Fridrich, "Efficient Wet Paper Codes," IEEE Trans, Binghamton University, State University of New York (SUNY), 2014.

[20] W. Zhang, "Maximizing Steganographic Embedding Efficiency by Combining Hamming Codes and Wet Paper Codes," IEEE Trans, Zhengzhou 450002, China, 2009.

[21] J. urgen Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in Steganography," IEEE Trans, Binghamton University, State University of New York, (NY) 13902-6000, 2015.

[22] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognit, vol. 34, no. 3, pp. 671–683, 2001.

[23] A. D. Ker, "Improved detection of LSB steganography in grayscale images," in Information Hiding, pp. 97–115, 2004.

[24] J. Fridrich, P. Lisoněk, and D. Soukal, "On steganographic embedding efficiency," in Computer Science, Alexandria, VA, pp. 282–296, July 2006.

[25] M. Zolanvar, H. Ghanei Yakhdan, and A. M. Latif, "A New Method in Color Images Watermarking based on YPbPr Color Space in FWHT Domain," Journal Of Electronical & Cyber Defence , vol. 4, no. 4, Serial No. 16, 2017. (in Persian)

[26] A.Nourazar, "Images Steganography Based On Linear Codes and Provide an Method Optimal, " thesis Master of Science in Telecommunication Engineering Cipher and Security, Imam Hussein Comprehensive University, 2016 . (in Persian)

Journal of Electronical & Cyber Defence
Vol. 5, No. 4, 2017, Serial No. 20

An Optimal Method for Images Steganography Based on Linear Codes Features

A. Nourazar, Z. Noroozi*, M. Mir

*Imam Hossein University

(Received: 07/02/2017, Accepted: 23/07/2017)

ABSTRACT

Steganography is an information hiding application which aims to hide secret messages imperceptibly into commonly used media. In this paper, we describe an Optimal embedding method based on linear codes that conforms to least significant bit, that is, the secret data is embedded into a cover message by parity check matrix. The new method not only benefits from the field of location and detection and error correction bit stream received by the receiver, but also can increase the Resistance between 94% to 100%, the transparency (PSNR) up to 84/71, and the similarity (SSIM) up to % 9999/99.

Keywords: Steganography, Image Cover, Linear Code, Parity Check Matrix.

* Corresponding Author Email: znorozi@ihu.ac.ir