



## ارزیابی نهان نگاری تصویر و ارائه یک روش بهینه در حوزه مکان

علی نورآذر<sup>۱\*</sup>، دکتر زین العابدین نوروزی<sup>۲</sup>، مهدی میر<sup>۳</sup> و حسن خالقی گرجی<sup>۴</sup>

۱- کارشناس ارشد مهندسی مخابرات رمز دانشگاه جامع امام حسین (ع)

۲- استادیار گروه رمز و امنیت دانشگاه جامع امام حسین (ع)

۳- کارشناس ارشد مهندسی مخابرات سیستم دانشگاه فردوسی

۴- کارشناس ارشد ریاضی کاربردی دانشگاه جامع امام حسین (ع)

### چکیده

در شبکه های مخابراتی و ارتباطی تأمین امنیت اطلاعات یکی از مسائل اساسی می باشد و یکی از روش های تأمین امنیت اطلاعات، نهان نگاری است؛ زیرا در نهان نگاری ارتباط مخفی می ماند و پیام محرمانه در پوشش اطلاعات متداول و رایج ارسال می گردد. از سوی دیگر نیاز برای تأمین امنیت ارتباطات از مسائل اجتناب ناپذیر محسوب شده و با توجه به گستردگی روزافزون شبکه های مخابراتی بر اهمیت آن افزوده می شود. از جمله راه کار هایی که برای حل این مسئله وجود دارد، استفاده از روش های بهینه نهان نگاری است.

در همین راستا مقاله حاضر به موضوع نهان نگاری در پوشانه تصویر می پردازد. هدف اصلی، ارائه راهکاری نوین و بهینه در برای استفاده از خاصیت کدگذاری برای درج داده های محرمانه در الگوریتم جاسازی است. چرا که استفاده از نظریه کدگذاری در نهان نگاری ضمن بهره مندی از خواص آن و افزایش ظرفیت و مقاومت در حوزه مکان، سبب افزایش امنیت طرح نهان نگاری در برابر نهان کاوها خواهد شد. برای دستیابی به این هدف، ایده ی استفاده از ماتریس کنترل مشابهت کدهای خطی در پوشانه تصویر، در روش پیشنهادی مطرح شده است. چرا که با درج داده های محرمانه در پیکسل های پوشانه بر اساس این روش، ضمن دستیابی به سادگی و ظرفیت مناسب حوزه مکان، تصویر نهانه بیشترین شباهت ممکن را به تصویر پوشانه داشته (۹۷٪) و سبب افزایش چشم گیر شفافیت (۵۸ الی ۷۰) خواهد شد.

**کلمات کلیدی:** نهان نگاری، پوشانه تصویری، کد گذاری، ماتریس کنترل مشابهت.

### ۱. مقدمه

رشد و توسعه فناوری های دیجیتال و به دنبال آن تولید انبوهی از داده های دیجیتالی چالش ها و فرصت های زیادی را به همراه داشته است. از زمانی که انسان ها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط پنهان و امن یک خواسته

<sup>1</sup> Email: [A\\_norazar@yahoo.com](mailto:A_norazar@yahoo.com)



مهم و ضروری افراد بوده است. در این میان روش های پنهان سازی اطلاعات<sup>۱</sup> که تاریخچه ای چند هزار ساله دارند، با ظهور داده های دیجیتالی شکلی کاملاً جدید به خود گرفته است. علم پنهان نگاری را می توان هنر مخفی کردن پیام در پوششی از اطلاعات بیان نمود. نشان گذاری<sup>۲</sup> و پنهان نگاری<sup>۳</sup> دو حوزه اصلی پنهان سازی داده ها محسوب شده و هر یک اهدافی را دنبال می نمایند [۱]. تأمین امنیت با رمزنگاری امکان پذیر است؛ در رمزنگاری، رسانه انتقال دارای مفهوم و داده مستقل نبوده و پنهان بودن داده، آشکار می باشد و افراد غیرمجاز به پیام محرمانه، دسترسی ندارند. در نشان گذاری حفاظت از سیگنال میزبان در برابر تهدیدات گوناگون مورد بحث قرار می گیرد و بیشترین کاربرد آن در محصولات نرم افزاری است و به جنبه تجاری و اقتصادی قضیه می پردازد، حال آن که هدف از پنهان نگاری مخفی ماندن وجود پیام از نظر دشمن است و بیش تر به جنبه نظامی و غیرتجاری معطوف می گردد. در حقیقت پنهان نگاری را می توان دانش و هنر پنهان سازی یک پیام محرمانه در درون یک سیگنال میزبان دانست. سیگنال میزبان می تواند صوت، تصویر، متن، ویدئو و غیره را شامل شود که در این جا با تأکید بر تصویر کار دنبال خواهد شد.

تاکنون الگوریتم های گوناگونی برای پنهان نگاری اطلاعات ارائه شده است. پنهان نگاری در دو حوزه مکان و تبدیل انجام می شود. حوزه مکان شامل آن دسته از الگوریتم هایی می شود که بیت های پیام بین بیت های میزبان جاسازی می شوند و در انجام عملیات پنهان نگاری، هیچ تبدیلی روی سیگنال پوشش انجام نمی پذیرد به عنوان مثال در روش جاگذاری LSB بیت های پیام در کم ارزش ترین بیت هر پیکسل گنجانده می شوند. حوزه تبدیل شامل آن دسته از روش هایی است که اطلاعات بیت های پیام روی تمام یا قسمتی از بیت های مقادیر ضرایب تبدیل مدنظر جاسازی می گردد (پیام محرمانه، در داخل فضای تبدیل سیگنال پوشش جاسازی می شود)؛ بنابراین می توان گفت که یکی از بهترین روش های ایجاد امنیت اطلاعات، پنهان نگاری است. امنیت یک سیستم پنهان نگار به شفافیت خروجی آن مرتبط است. شفافیت یکی از سه معیار مهم در پنهان نگاری است. از معیارهای مهم دیگر در پنهان نگاری، ظرفیت و مقاومت است. طبق آمار ارائه شده از تحقیقات و نرم افزارهای موجود در زمینه پنهان نگاری و به دلیل استفاده همه گیر، در دسترس بودن و ساده بودن الگوریتم ها، سهم تصویر بیشتر از رسانه های دیگر در پنهان نگاری است و با توجه به این مسئله که رسانه تصویر از سایر رسانه های این حوزه رایج و متداول می باشد، می تواند به عنوان بهترین ابزار پوششی و فریب استفاده شود. لذا این رسانه به عنوان مهم ترین و پرکاربردترین رسانه پوششی جهت استفاده در پنهان نگاری مورد استفاده قرار گرفته است، به طوری که در دهه اخیر و حتی در سال های اخیر سعی شده تا با معرفی قالب های جدید تصویر، روش های پنهان نگاری نوینی بر روی تصاویر، چه در حوزه مکان و چه در حوزه فرکانس طراحی و پیاده سازی شود.

روش های پنهان نگاری حوزه مکان باوجود ظرفیت بالا، از مقاومت بسیار پائینی برخوردار است. با توجه به این مطلب، یافتن راه هایی برای افزایش مقاومت تصویر حاوی اطلاعات پنهان شده ضروری است. بهترین راه حل برای این مشکل، این است که به جای حوزه مکان، اطلاعات را در داخل حوزه های تبدیل تصویر، نظیر فرکانس پنهان نماییم که از مقاومت بالایی نسبت به حوزه مکان برخوردار است. لذا روش های پنهان نگاری در حوزه تبدیل به وجود آمده و گسترش یافتند.

در این مقاله روش جدیدی برای پنهان نگاری تصویر در حوزه مکان بر اساس نظریه کدگذاری معرفی می شود تا ضمن برخورداری از مزایای این حوزه (سادگی و ظرفیت بالا)، مقاومت را افزایش و بحث تشخیص و تصحیح خطا را در فرایند جاسازی برای ما فراهم سازد. حال می توان بدین منظور از روش کدینگ مشخصه در پنهان نگاری تصویر استفاده نمود به طوری که فرستنده پیام پنهانی را با توجه به ماتریس کنترل مشابهت<sup>۴</sup> H توافقی، مشخصه ای از شیء پوشش دهنده

<sup>1</sup> Information Hiding<sup>2</sup> watermarking<sup>3</sup> steganography<sup>4</sup> Parity Check Matrix



جاسازی نموده و آن را به گیرنده ارسال کند. گیرنده نیز با استفاده از همان H توافقی به سادگی می‌تواند به پیام محرمانه دست پیدا کند. در همین خصوص نوشته حاضر مشتمل بر چهار بخش می‌باشد که ابتدا بعد از مقدمه و در بخش دوم به معرفی دانش مخفی سازی اطلاعات (نهان‌نگاری)، به همراه واژه‌های کلیدی، مفاهیم و تعاریف اولیه در آن پرداخته‌ایم. در بخش سوم، منحصرأ نهان‌نگاری تصویر را به همراه انواع روش‌های آن را در دو حوزه ارائه می‌دهیم. در بخش چهارم نیز به معرفی و پیشنهاد یک روش نوین در خصوص نهان‌نگاری تصویر و شبیه سازی آن می‌پردازیم. این روش، نهان‌نگاری تصویر با استفاده از ساختار کدهای خطی می‌باشد. در پایان مراجع بکار رفته و مقالاتی که به فهم بیشتر خواننده کمک می‌کند جمع‌آوری شده و ارائه می‌گردد.

## ۲. نهان‌نگاری اطلاعات

برای حفاظت از داده‌های سری در برابر دسترسی غیرمجاز (محرمانگی و تمامیت پیام) از دو تکنیک رمزنگاری<sup>۱</sup> و نهان‌نگاری<sup>۲</sup> استفاده می‌شود. تکنیک‌های رمزنگاری برای حفاظت داده دیجیتال به هنگام انتقال از فرستنده به گیرنده به کار می‌روند. داده‌ها در فرستنده رمز می‌شوند و پس از دریافت در گیرنده رمزگشایی می‌شوند. از این پس دیگر هیچ‌گونه حفاظتی از داده صورت نمی‌گیرد. ولی در تکنیک‌های نهان‌نگاری، یک داده پنهانی مستقیماً در داخل یک رسانه پوششی حک<sup>۳</sup> می‌شود و همواره در آن باقی می‌ماند. برای انتقال داده نهان‌نگاری شده، نیازی به برداشتن سیگنال پوششی نیست زیرا این سیگنال طوری در داده میزبان درج می‌شود که هیچ تأثیر نامطلوبی بر داده اصلی نمی‌گذارد. به‌عنوان مثال در نهان‌نگاری داده در تصویر، چشم انسان نباید تفاوت بین تصویر اصلی و تصویر نهان‌نگاری شده را حس کند. در جدول شماره- ۱ زیر روند رو به گسترش علوم مربوط به مخفی سازی اطلاعات دیده می‌شود. [۱]

جدول ۱- تعداد مقالات منتشر شده در زمینه مخفی سازی اطلاعات

سال انتشار	۱۹۹۲	۱۹۹۳	۱۹۹۴	۱۹۹۵	۱۹۹۶	۱۹۹۷	۱۹۹۸	۱۹۹۹	۲۰۰۰ به بعد
تعداد مقالات	۲	۲	۴	۱۳	۲۹	۶۴	۱۰۳	۵۶۴	هزاران مقاله

در ادامه ابتدا تاریخچه سیستم‌های مخفی سازی اطلاعات بیان شده و سپس مرور کوتاهی بر سیستم‌های رمزنگاری و نحوه برقراری امنیت اطلاعات از طریق این سیستم‌ها می‌پردازیم.

### ۲.۱. تاریخچه نهان‌نگاری

تاریخچه نهان‌نگاری به سال‌های بسیار دور برمی‌گردد، شاید زمانی که ایرانیان برای نشانه‌گذاری بر روی احشام و سفالگران بر روی سفال‌های خود به‌منظور حق مالکیت در ۲۸۰۰ تا ۳۰۰۰ سال قبل از میلاد از آن استفاده می‌کردند و همچنان از این نشانه‌گذاری‌های در حال حاضر نیز استفاده می‌شود. [۲] اما در قرن بیستم بود که حقیقتاً پنهان‌نگاری شکوفا شد. روش‌های قدیمی مخفی کردن با ورود کامپیوترهای پر قدرت نیرو گرفتند. در طول دهه ۱۹۸۰ مارگات تاچر که از لو رفتن اطلاعات و اسناد کابینه‌اش بسیار ناراحت بود توانست با استفاده از یک پردازشگر کلمات هر وزیر را در فاصله بین کلمات به نحوی ثبت کند و بنابراین وزرای خائن را از این طریق ردیابی نماید. در حال حاضر نیز فنی مشابه در ردیابی

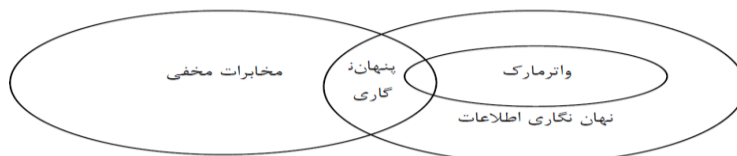
<sup>1</sup> encryption

<sup>2</sup> Steganography

<sup>3</sup> embedding



انتشارات الکترونیکی مورد استفاده قرار می‌گیرد که به عدد سریال می‌توان اشاره کرد. امروزه نهان‌نگاری با پیشرفت نرم‌افزارها گسترش یافته و واتر مارکینگ (نقش نگاری) نیز به عنوان یک فن در فرایند نهان‌نگاری مورد توجه واقع شده است. در نقش نگاری، اطلاعات ثانویه داخل سیگنال میزبان قرار می‌گیرند تا رسانه دیجیتال در مقابل جعل و یا دست‌کاری محصول، مصون نگه‌داشته شود، بدون آنکه خدشه‌ای در کیفیت سیگنال میزبان وارد شود. در اینجا برعکس نهان‌نگاری میزبان از اهمیت بیشتری برخوردار بوده و این وظیفه پیام است که از میزبان محافظت کند. (شکل شماره ۱) [۳،۴].



شکل ۱- نسبت بین پنهان‌نگاری و فیلدهای مختلف آن

## ۲.۲. تعاریف و مفاهیم کلی

نهان‌نگاری را می‌توان هنر و علم پنهان ساختن داده‌های محرمانه درون سایر پوشانه‌ها نامید. در این فرآیند، پیام محرمانه بایستی به گونه‌ای در پوشانه پنهان گردد که هیچ‌کس به‌جز فرستنده و گیرنده از وجود آن مطلع نشود. به عبارت دیگر در صورت آشکار شدن وجود پیام محرمانه در یک پوشانه، طرح نهان‌نگاری با شکست مواجه شده است [۵]. باید به این نکته توجه نمود که روش‌های رمزنگاری<sup>۱</sup> با تغییر دادن صورت ظاهری پیام محرمانه، اطلاعات دیگری تحت عنوان متن رمز شده که اغلب شکلی نامفهوم و تصادفی دارند، تولید می‌نمایند. به عبارت دیگر در رمزنگاری وجود اطلاعات محرمانه و یا ارسال پیام محرمانه کاملاً مشخص است، اما تنها گیرنده‌ی از پیش تعیین شده، توانایی بازیابی اطلاعات را دارد، این در حالی است که مشاهده‌ی داده‌های رمز شده بر روی کانال سبب جلب توجه مهاجمان خواهد شد. در چنین وضعیتی حتی اگر مهاجم به دلیل وجود الگوریتم‌های رمزنگاری قوی نتواند به پیام محرمانه دست پیدا کند، با ایجاد اختلال در کانال ارتباطی، ارسال اطلاعات به گیرنده را دچار مشکل خواهد نمود. در این حالت با پیاده‌سازی موفق یک روش نهان‌نگاری و مخفی نمودن ارتباط از دید مهاجم، علاوه بر تأمین امنیت اطلاعات، امنیت ارتباط نیز فراهم خواهد شد. بهتر است قبل از آن که به بیان تفصیلی نهان‌نگاری بپردازیم، ابتدا تعاریف ذیل را ارائه دهیم [۶،۷].

پوشانه یا حامل اطلاعات<sup>۲</sup>: پوشانه فایل صوتی، تصویری، متنی و غیره می‌باشد که برای جاسازی اطلاعات در آن استفاده می‌شود. منظور از اطلاعات هرگونه داده دودویی یا علامت و نشانه خاصی است که برای جاسازی در پوشانه استفاده می‌شود.

جاسازی اطلاعات<sup>۳</sup>: به روندی که در آن داده‌های دودویی داخل پوشانه مخفی با بیت‌های آن ترکیب می‌شوند، تحت عنوان جاسازی اطلاعات نام‌برده می‌شود. جاسازی اطلاعات باید به نحوی انجام شود که کم‌ترین تغییرات را در پوشانه، هم از نظر ظاهری و هم از نظر مشخصات آماری ایجاد کند.

گنجانده اطلاعات<sup>۴</sup>: گنجانده فایل حاوی اطلاعات است که پس از جاسازی داده در پوشانه به دست می‌آید. گنجانده پس از جاسازی داده در مسیر انتقال یا در گیرنده می‌تواند تحت تأثیر پاره‌ای از تغییرات عمدی یا غیرعمدی قرار گیرد. این

<sup>1</sup> Cryptography

<sup>2</sup> Host media

<sup>3</sup> Embedding

<sup>4</sup> Marked media



تغییرات می‌تواند حملات عمدی مانند جاسازی عمدی داده در آن بوده و یا تغییرات معمول بر روی تصویر مانند فشرده‌سازی و یا تغییرات ناشی از نویز در مسیر انتقال باشد.

کلید مخفی‌سازی<sup>۱</sup>: کلید محرمانه توافق شده بین فرستنده و گیرنده که برای ارتقای سطح امنیت الگوریتم جاسازی و بازیابی اطلاعات استفاده می‌شود، کلید مخفی‌سازی نامیده می‌شود. ممکن است اطلاعات قبل از جاسازی با استفاده از یک کلید رمزنگاری و بر اساس یکی از الگوریتم‌های رمز کلید متقارن یا نامتقارن رمز شده و سپس در پوشانه مخفی شوند. کلید رمزنگاری می‌تواند با کلید نهان‌نگاری متفاوت باشد.

الگوریتم آشکارسازی کور<sup>۲</sup>: روش‌هایی که برای بازیابی داده نیاز به پوشانه اطلاعات ندارند و به‌عنوان روش‌های مخفی آشکارسازی نام‌برده می‌شوند.

الگوریتم آشکارسازی غیرکور<sup>۳</sup>: روش‌هایی که برای بازیابی داده نیاز به پوشانه اطلاعات دارند و با مقایسه پوشانه و گنجانده اطلاعات داده‌های جاسازی‌شده را بازیابی یا علامت درج‌شده در گنجانده را احراز می‌کنند.

مهاجم غیرفعال<sup>۴</sup>: در این‌جا مهاجم در کانال ارتباطی قرار نگرفته و فقط از اطلاعات ارسالی استفاده می‌نماید. مهاجم فعال<sup>۵</sup>: مهاجم در هر قسمت از الگوریتم نهان‌نگاری و هم‌چنین در هرکجای کانال حضور داشته و امکان تغییر نهان‌نگاری برایش فراهم می‌باشد؛ مثلاً ممکن است پوشانه را فشرده نموده و در یک انتقال از یک پهنای باند خاصی استفاده نماید.

مهاجم مخرب<sup>۶</sup>: در این‌جا مهاجم می‌تواند خودش را به‌جای فرستنده جا بزند. پیام محرمانه را عوض نماید و پوشانه را تغییر دهد.

در ادامه قصد داریم تعریفی دقیق از یک فرآیند نهان‌نگاری ارائه دهیم. فرض کنید که  $k$  کلید نهان‌نگاری باشد که از مجموعه  $K$  (مجموعه‌ای از تمام کلیدهای ممکن نهان‌نگاری) انتخاب شده است؛  $M$  مجموعه‌ای در بردارنده‌ی تمامی پیام‌هایی است که قابلیت مخفی شدن را دارا هستند؛  $C$  نیز مجموعه‌ای از تمامی رسانه‌های پوششی است. یک طرح نهان‌نگاری توسط دو نگاشت تعریف می‌شود: نگاشت جاسازی<sup>۷</sup> ( $Emb$ ) و نگاشت بازگشایی<sup>۸</sup> ( $Ext$ ). این دو نگاشت را می‌توان مطابق معادله‌ی (۱-۲) تعریف نمود [۹ و ۸].

تعریف (۱-۲): پنج‌تایی  $(C, M, K, Emb, Ext)$  را یک دستگاه نهان‌نگاری<sup>۹</sup> می‌گویند [۸] هرگاه داشته باشیم:

$$Emb: C \times K \times M \longrightarrow C \quad (2-1)$$

$$Ext: C \times K \longrightarrow M$$

به‌طوری‌که برای هر  $k \in K$ ، هر  $c \in C$  و  $m \in M$  داشته باشیم  $Ext(Emb(c, k, m), k) = m$  هم‌چنین پوشانه‌ای که در آن پیام محرمانه درج‌شده است،  $s = Emb(c, k, m)$  را گنجانده می‌نامند. برای فهم بهتر این مطلب می‌توان به (شکل ۲) مراجعه نمود.

<sup>1</sup> Stego key

<sup>2</sup> Blind detection method

<sup>3</sup> Non blind detection method

<sup>4</sup> Passive

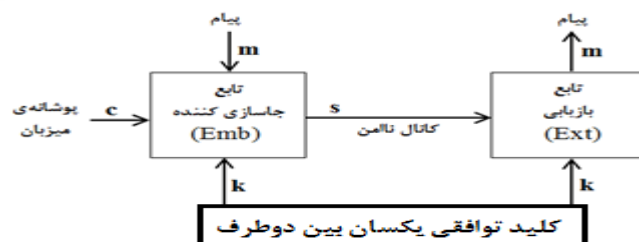
<sup>5</sup> Active

<sup>6</sup> Malicious

<sup>7</sup> Embedding mapping

<sup>8</sup> Extraction mapping

<sup>9</sup> Steganographic system



شکل ۲: نمودار یک فرآیند نهان نگاری [۸]

## ۲.۲. ملزومات و ویژگی های سیستم نهان نگاری

گرچه هر کاربردی از نهان نگاری تصویر نیازهای خاص خود را دارد، با این همه تمام روش های نهان نگاری باید ملزومات مشترکی را رعایت کنند که در این خصوص برای مشخصه های مهم هر سیستم نهان نگاری اطلاعات می توان به پارامتری نظیر شفافیت، استحکام (مقاومت)، ظرفیت سیستم نهان نگاری برای پنهان نمودن اطلاعات، امنیت و پیچیدگی آن اشاره نمود که معمولاً رسیدن به برتری در یکی منجر به نتایج ضعیف تری در پارامترهای دیگر می شود. آنچه مهم است این است که در نهان نگاری نباید اطلاعات از لحاظ دیداری و یا شنیداری قابل کشف باشد؛ بنابراین می توان گفت که این ملزومات به یکدیگر مربوط اند.

شفافیت<sup>۱</sup>: یکی از معیارهای ارزیابی نهان نگاری، میزان شباهت بین تصویر اصلی و تصویر واتر مارک شده می باشد. نهان نگاری بکار رفته ضمن نامحسوس بودن، نباید از کیفیت تصویر بکاهد و یا اثراتی بر روی تصویر بگذارد که از دید کاربر قابل درک باشد.

مقاومت<sup>۲</sup>: معیار ارزیابی دیگری که باید از آن یاد کرد، میزان مقاومت تصویر نهان نگاری در برابر انواع پردازش ها می باشد. به عبارت دیگر میزان قابل کشف بودن پیام از پوشانه نهان نگاری شده در برابر پردازش هایی نظیر فشرده سازی، فیلترینگ، نویز، چرخش و انواع تبدیلات به چه میزان خواهد بود و همواره این مسئله مطرح خواهد بود که نهان نگاری در برابر این پردازش ها چه دوامی خواهد داشت.

ظرفیت<sup>۳</sup>: در یک سیستم نهان نگاری تعداد اطلاعات قابل جاسازی در سیستم را به عنوان ظرفیت سیستم تلقی می کنیم. مقدار اطلاعاتی را که می توان در یک نهان نگاری جاسازی کرد باید تا حد امکان بالا باشد. به عبارت کلی ظرفیت برابر ماکزیمم مقدار اطلاعاتی است که می توان در یک رسانه ی پوششی پنهان کرد بدون اینکه به امنیت سیستم خدشه ای وارد شود و اینکه بتوان پیام را با اطمینان بالایی از رسانه جاسازی شده بازیابی نمود. ظرفیت نهان نگاری عموماً نباید با ظرفیت جاسازی پیام مقایسه گردد. ولی معمولاً ظرفیت نهان نگاری خیلی کمتر از ظرفیت جاسازی پیام می باشد. عموماً حتی برای طرح هایی با جاسازی ساده، تعیین ظرفیت پنهان نگار بسیار سخت می باشد.

نکته: سه ویژگی اشاره شده تشکیل یک مثلث معروف را می دهند که در شکل ذیل نشان داده می شود:



شکل ۳: سه ویژگی اساسی سیستم نهان نگاری

<sup>1</sup> Invisibility<sup>2</sup> Robustness<sup>3</sup> Capacity





سه ویژگی فوق به‌طور بسیار تنگاتنگی به یکدیگر وابسته هستند. یک رابطه‌ی بامعنی در مورد ویژگی‌های مذکور وجود دارد:

$$\text{ثابت} = (\text{مقاومت} \times \text{ظرفیت})$$

رابطه‌ی فوق بدین معناست که با افزایش مقاومت حتماً ویژگی ظرفیت کاهش می‌یابد و بالعکس (در صورتی که ویژگی اول یعنی شفافیت ثابت بوده و تفاوتی نکند)

## ۲.۴. انواع نهان‌نگاری

روش‌های نهان‌نگاری از منظر حوزه عملیات را می‌توان به دو دسته نهان‌نگاری در حوزه مکان و حوزه تبدیل به شرح ذیل تقسیم نمود.

روش‌های نهان‌نگاری در حوزه مکان: در این دسته از روش‌ها، به‌منظور انجام عملیات نهان‌نگاری هیچ تبدیلی روی سیگنال پوششی انجام نمی‌گیرد و کلیه اقدامات مربوط به نهان‌نگاری در حوزه مکان اعمال می‌گردد.

روش‌های نهان‌نگاری در حوزه تبدیل: در این روش‌ها، پیام محرمانه در داخل فضای تبدیل سیگنال پوشش (ازجمله حوزه فرکانس) جاسازی می‌شود. نهان‌نگاری در حوزه تبدیل از لحاظ مقاومت و شفافیت بهتر از حوزه مکان است.

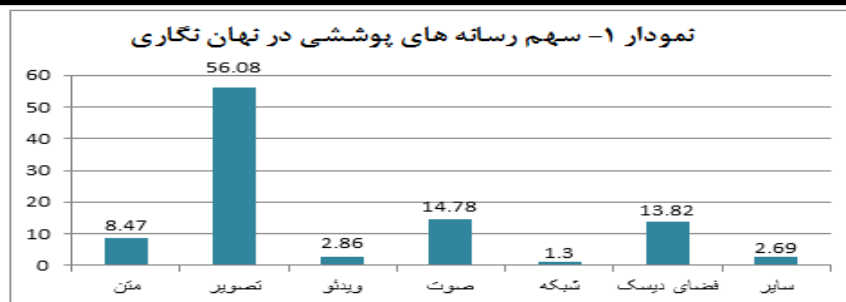
### جدول ۲- مقایسه نهان‌نگاری در دو حوزه مکان و تبدیل

حوزه نهان‌نگاری / پارامتر	ظرفیت	مقاومت	آشکارناپذیری	پیچیدگی
نهان‌نگاری در حوزه مکان	بیشتر	کمتر	کمتر	کمتر
نهان‌نگاری در حوزه تبدیل	کمتر	بیشتر	بیشتر	بیشتر

بر اساس رسانه‌های پوششی مختلف: با توجه به اینکه بیشتر روش‌های قدیمی نهان‌نگاری با دست انجام می‌گرفت، دارای معایبی مانند دقت کم، حجم بالا، سرعت کم و غیره بودند، با توجه به رشد فناوری، روش‌های جدیدی نیز برای نهان‌نگاری ارائه گردید که می‌تواند در رسانه‌های مختلفی ازجمله متن، تصویر، صوت، ویدئو، پروتکل‌های شبکه و غیره انجام شود.

## ۳. نهان‌نگاری در رسانه تصویر

در این بخش به معرفی انواع روش‌های نهان‌نگاری داده در تصاویر می‌پردازیم. چنانچه در نمودار شماره ۱ - ملاحظه می‌کنید، طبق آمار ارائه‌شده از تحقیقات و نرم‌افزارهای موجود در زمینه نهان‌نگاری، سهم تصویر بیشتر از رسانه‌های دیگر است. پس بدون تردید می‌توان نتیجه گرفت که رسانه تصویر پرکاربردترین و فراگیرترین رسانه‌های موردتوجه کاربران، هم در امور روزمره و شخصی مثل تلفن همراه و دوربین عکاسی و هم در محیط اینترنت جهت تبادل با اشخاص دیگر محسوب می‌شود. لذا این رسانه به‌عنوان مهم‌ترین و پرکاربردترین رسانه پوششی جهت استفاده در نهان‌نگاری مورد استفاده قرار گرفته است، به‌نحوی که در دهه اخیر و حتی در سال‌های اخیر سعی شده تا با معرفی قالب‌های جدید تصویر، روش‌های نهان‌نگاری نوینی بر روی تصاویر، چه در حوزه مکان و چه در حوزه فرکانس طراحی و پیاده‌سازی شود.



با توجه به مطالب بیان شده، اهمیت این نوع رسانه درک شده و سعی خواهیم کرد که با مرور کلی بر روش های نهان نگاری در این نوع رسانه (تصاویر)، روش نوینی در این خصوص معرفی نماییم. نگاهی آماری به تصاویر موجود در دنیای دیجیتال نشان می دهد که پرکاربردترین گونه های تصاویر، به ترتیب GIF، JPEG، PNG و در نهایت BMP می باشند.

### ۳.۱. روش های نهان نگاری تصویر

در این بخش تکنیک های مختلف نهان نگاری تصاویر دیجیتال مورد بررسی و مقایسه قرار می گیرند. تکنیک های نهان نگاری تصاویر دیجیتال به طور کلی به دو گروه تکنیک های حوزه ی مکان و حوزه ی فرکانس تقسیم بندی می شوند. در هر یک از حوزه های مکان و فرکانس به شیوه های گوناگونی می توان داده ها را پنهان نمود. هر کدام از این تکنیک ها مزایا و معایب خاص خود را داشته و بسته به کاربرد مورد نظر می توان از آن ها استفاده نمود.

#### ۳.۱.۱. حوزه مکان

در روش های حوزه ی مکان، درج پیام بر اساس تغییر یا دست کاری مستقیم مقادیر پیکسل های تصویر صورت می گیرد و در انجام عملیات نهان نگاری، هیچ تبدیل روی پوشانه انجام نمی پذیرد و کلیه اقدامات مربوط به نهان نگاری در حوزه مکان اعمال می گردد. برخی از مهم ترین روش های این حوزه به شرح ذیل می باشند که چند روش اصلی را معرفی می نماییم.

- روش نهان نگاری افزودنی [۶]
- روش نهان نگاری مبتنی بر بیت کم ارزش<sup>۱</sup> LSB [۱۰، ۱۱]
- روش نهان نگاری معکوس در بیت کم ارزش<sup>۲</sup> LSBF [۱۲، ۱۳]
- روش نهان نگاری تطبیقی بر اساس اغتشاش جمع شونده<sup>۳</sup> LSBM [۱۴، ۱۵]
- روش نهان نگاری تصادفی در بیت کم ارزش<sup>۴</sup> RLSB [۱۶، ۱۷]
- روش مبتنی بر مدولاسیون SSM [۱۸]

**نهان نگاری افزودنی:** ساده ترین روش برای درج سیگنال پیام در حوزه ی مکان، افزودن یک رشته نویز شبه تصادفی معرف سیگنال پیام به مقادیر روشنایی پیکسل های تصویر مورد نظر است. سیگنال نویز معمولاً به صورت اعداد صحیح (۱ و

<sup>۱</sup> least significant bit

<sup>۲</sup> least significant bit flipping

<sup>۳</sup> LSB maching

<sup>۴</sup> Random LSB





۰ و ۱-) یا اعداد ممیز شناور است. برای اطمینان از قابل تشخیص بودن پیام، نویز توسط یک کلید تولید می‌شود. امنیت این روش به کلید بکار رفته در تولید نویز بستگی دارد. در این روش استخراج پیام با استفاده از مقدار همبستگی بین تصویر نهان‌نگاری شده و سیگنال اصلی پیام صورت می‌گیرد. برای درج تعداد زیادی بیت در تصویر میزبان، می‌توان آن را به تعدادی زیرتصویر تقسیم کرد و هر بیت را به یکی از این زیرتصویرها اضافه نمود. مهم‌ترین مزیت این روش شفافیت آن است، اما مقاومت آن در برابر عملیات پردازش تصویر ضعیف است [۶].

**بیت کم‌ارزش LSB:** یکی از رایج‌ترین روش‌های نهان‌نگاری در حوزه‌ی مکان، روش کم‌ارزش‌ترین بیت است. این روش پیام را در کم‌ارزش‌ترین بیت پیکسل‌های تصویر درج می‌کند. درج پیام در تصویر با انتخاب زیرمجموعه‌ای از پیکسل‌ها و جایگزین کردن بیت‌های پیام با کم‌ارزش‌ترین بیت هر پیکسل انتخاب شده انجام می‌گیرد. پیام ممکن است در طول تصویر یا در مکان‌های انتخاب شده از تصویر گسترش یابد. پیاده‌سازی و درک این روش بسیار سریع و آسان است و انحراف جدی در تصویر ایجاد نمی‌کند. مهم‌ترین خصوصیت LSB شفافیت آن است. این روش به عملیات پردازش تصویر حساس بوده و در برابر نویز و حملات هندسی نیز آسیب‌پذیر می‌باشد و پیام می‌تواند به آسانی از بین برود [۱۳].

**روش مبتنی بر مدولاسیون SSM:** در روش‌های طیف گسترده<sup>۱</sup> انرژی تولید شده، در یک یا چند فرکانس گسسته در زمان، پخش و توزیع می‌شود. علت استفاده از این روش، دلایل مختلف از جمله ایجاد ارتباطات امن، افزایش مقاومت در برابر تداخل طبیعی و پارازیت‌ها و جلوگیری از تشخیص نهان‌نگاری می‌باشد. الگوریتم نهان‌نگاری بر اساس SSM، اطلاعات را به وسیله‌ی ترکیب خطی تصویر با یک سیگنال شبه نویز کوچک که توسط نهان‌نگاری درج‌شده، مدوله شده است جاسازی می‌کند [۱۸].

### ۳.۱.۲. حوزه فرکانس

در تکنیک حوزه‌ی فرکانس، ابتدا یک تصویر به مجموعه‌ای از ضرایب این حوزه تبدیل‌شده و سپس پیام در این ضرایب تبدیل‌شده درج می‌شود (پیام محرمانه، در داخل فضای تبدیل سیگنال پوشش جاسازی می‌شود). روش کار به این صورت است که ابتدا توسط یک تابع تبدیل مناسب، تصویر از حوزه‌ی مکان به حوزه‌ی فرکانس انتقال می‌یابد، سپس نهان‌نگاری با تغییر ارزش پیکسل‌ها در حوزه‌ی فرکانس انجام می‌گیرد و در نهایت تصویر به حوزه‌ی مکان برگردانده می‌شود. به این تکنیک حوزه‌ی تبدیل نیز گفته می‌شود. نهان‌نگاری در حوزه تبدیل می‌تواند بسیار مقاوم‌تر از نهان‌نگاری در حوزه مکان باشد. مهم‌ترین نقطه‌ضعف روش‌های حوزه مکان، مقاومت بسیار پایین آن‌ها در مقابل پردازش‌های تصویری مانند برش، افزودن نویز، تغییر فرمت تصویر و یا چرخاندن تصویر می‌باشد. با توجه به این نکات یافتن راه‌هایی برای افزایش مقاومت تصویر حاوی اطلاعات پنهان‌شده ضروری است. بهترین راه‌حل برای این مشکل، این است که به جای حوزه مکان، اطلاعات را در داخل لایه‌های بالاتر تصویر نظیر فرکانس پنهان نماییم. لذا روش‌های نهان‌نگاری در حوزه تبدیل به وجود آمده و گسترش یافتند. تبدیلات حوزه‌ی فرکانس که عموماً در الگوریتم‌های نهان‌نگاری تصاویر دیجیتال مورد استفاده قرار می‌گیرد. [۴]

**تبدیل کسینوسی گسسته (DCT):** تبدیل کسینوسی گسسته، روشی برای تبدیل یک سیگنال به اجزای فرکانسی آن می‌باشد. این روش نسبت به روش‌های حوزه‌ی مکان بیشتر با سیستم بینایی انسان (HVS) منطبق است، زیرا بخشی که قابل درک نبوده، شناسایی شده و دور انداخته می‌شود. روش‌های مبتنی بر DCT به دو دسته‌ی DCT منطقه‌ای<sup>۲</sup> و

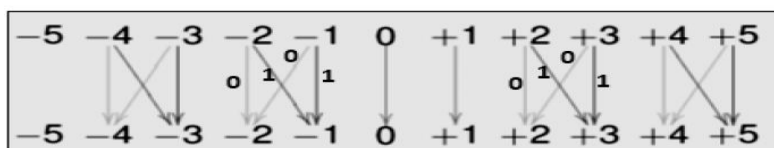
<sup>۱</sup> spread spectrum

<sup>۲</sup> global



DCT پایه بلوکی<sup>۱</sup> تقسیم بندی می شوند. COX و همکارانش الگوریتمی را با استفاده از روش DCT منطقه ای، مطرح کردند که یک نهان نگاری قوی را در مهم ترین بخش ادراکی تصویر مبتنی بر HVS درج می کرد. درج پیام در این بخش مزیت پایداری نهان نگاری در برابر برنامه های فشرده سازی را فراهم می کند، زیرا اکثر برنامه های فشرده سازی بخش هایی از تصویر را حذف می کنند که کم اهمیت ترین بخش از نظر ادراکی باشند. در این روش تصویر را به بلاک های  $8 \times 8$  تقسیم می کنند،  $64$  ضریب در تبدیل کسینوسی گسسته به دست می آید. توجه کنید که راه مخفی کردن بیت های پیام در ضرایب DCT قرار دادن آن ها در بیت هایی با کم ترین ارزش ضرایب است. یکی از محدودیت های این روش آن است که تعداد زیادی از  $64$  ضریب تبدیل کسینوسی DCT در هر قطعه  $8 \times 8$  از پیکسل های تصویر مساوی با صفر هستند و تغییر تعداد زیادی صفر به مقادیر غیر صفر می تواند بر نرخ فشرده سازی تصویر اثر منفی بگذارد، به همین دلیل است که ظرفیت پنهان سازی در ضرایب DCT خیلی کم تر از ظرفیت در حوزه مکان است [۶].

**روش نهان نگاری Jsteg:** این روش توسط درک اوفام<sup>۲</sup> طراحی شد. الگوریتم آن، بیت های کم ترین ارزش ضرایب DCT را به صورت متوالی با بیت های پیام جایگزین می نماید. این الگوریتم دارای کلید محرمانه نیست؛ بنابراین هر کس که به فرآیند نهان نگاری واقف باشد، می تواند به پیام محرمانه دست یابد. در این روش ضرایب DCT که صفر یا یک باشند، جایگذاری نمی شوند. شکل (۴) نحوه جاسازی بیت های پیام را نشان می دهد [۳۸].



شکل ۴: نحوه نهان نگاری Jsteg در بیت های ضرایب DCT [۲]

این روش اولین روشی که در دسترس عموم قرار گرفته و ساده و بدون پیچیدگی محاسباتی است. همچنین به دلیل استفاده از فرمت JPEG، نرخ فشرده سازی آن بالا است. در این روش به دلیل ذخیره کردن در ضرایب غیر صفر و یک، دارای حجم پنهان سازی کم است، هیستوگرام تصویر پوشش را تغییر می دهد و با تغییر در جفت مقدارهای کنار هم در هیستوگرام تصویر پوشش توسط حمله کای اسکوار (مربع خی دو) قابل اجراء است.

**روش نهان نگاری F5:** در این روش الگوریتم نهان سازی، پیام را در بیت های با کم ترین ارزش ضرایب DCT از ابتدا و به صورت متوالی ولی به شیوه ای خاص با بیت های پیام جایگزین می نماید. در این روش تغییرات ضرایب DCT به کم ترین مقدار خود خواهند رسید. در این روش برخلاف روش های قبلی، پیام در کل تصویر به صورت گسترده پخش و نهان نگاری می شود. از آنجایی که الگوریتم F5 هیستوگرام ضرایب DCT را اصلاح می کند، محققین این روش نشان دادند که این روش بسیاری از مشخصه های مهم هیستوگرام مثل یکنواختی را حفظ می کند و نمی تواند توسط حمله مربع خی دو آشکار سازی شود [۱۹]. مزایای این روش عبارتند از: به دلیل استفاده از فرمت JPEG، نرخ فشرده سازی بالا می باشد و حجم تصویر نهایی کم است، برای ذخیره سازی هر دو بیت، احتیاج به تغییر تنها یک بیت می باشد. بدین دلیل دارای کارایی ذخیره سازی بالاتری نسبت به روش های F3، F4 و Jsteg است و در مقابل مربع خی دو مقاوم است. معایب آن نیز عبارتند از: در برابر حمله آماری مقاوم نیست و هیستوگرام ضرایب DCT تغییر می کند.

### ۳.۲. حملات بر سیستم نهان نگاری تصاویر

<sup>1</sup> block based

<sup>2</sup> Derek Upham



حملات عمدی و غیر عمدی متعددی وجود دارد که یک تصویر نهان نگاری شده می تواند در معرض آن قرار گیرد. در دسترس بودن طیف گسترده ای از نرم افزارهای پردازش تصویر این امکان را فراهم ساخته است که اجرای حملات بر روی تصاویر نهان نگاری شده امکان پذیر باشد. هدف این حملات جلوگیری از نهان نگاری برای اجرای اهداف مورد نظر است. در شکل شماره ۵ تقسیم بندی کلی حملات و اهداف آن ها را مشاهده می نمایید که هر کدام آن ها شامل چندین حمله در آن کلاس می تواند باشد.



شکل ۵- دسته بندی کلی حملات بر اساس اهداف

فارغ از تقسیم بندی فوق، برخی از متداول ترین حملات نهان نگاری عبارت اند از: حملات تخریب تصویر، حملات هندسی، حملات حذف کننده و حملات رمزنگاری. [۱،۲]

#### ۴. نهان نگاری تصویر با استفاده از خاصیت کدگذاری

بامطالعه روش کدگذاری مشخصه که آن را "روش تعبیه ماتریس" نیز می نامند، نتیجه می گردد که در این روش از کد خطی به عنوان عنصر اصلی استفاده می شود که می توان از ویژگی های آن در سیستم نهان نگاری استفاده نمود. برای دستیابی به کارایی مطلوب این روش بایستی از کدهای بهینه استفاده نمود. توجه داشته باشید که در میان همه کدهایی با یک اندازه تشکیل دهنده، بعد ثابت و در نتیجه نرخ اطلاعات ثابت، کدی بهینه محسوب می شود که مفهومی مناسب با شعاع پوشش این کاربرد خاص را جایگزین نماید. کدهای بهینه خطی که در روش کدگذاری سندرم استفاده می شود، می تواند متشکل از کدهایی یک یا دوبعدی بر روی  $GF(2)$  باشند.

یکی از ویژگی های اصلی نهان نگاری می تواند مقاومت آن در مقابل حملات آماری یا به عبارت دیگر آشکارسازی آماری باشد که برای تحقق این هدف از جایگذاری شبه تصادفی بر مبنای نظریه کدگذاری می توان استفاده گردد، به طوری که فرآیند جاسازی کم ترین تغییرات را داشته و از لحاظ آماری مقاومت بالایی داشته باشد و خواص اصلی را حفظ نماید [۲۰]. بر همین اساس می توان از روش نظریه کدگذاری در نهان نگاری استفاده نمود به طوری که فرستنده پیام محرمانه را با توجه به ماتریس کنترل مشابَهت (H) توافقی، به عنوان یک مشخصه از پوشانه دریافت نموده و پیام را با استفاده از ماتریس کنترل مشابَهت، داخل پوشانه ای (مانند تصویر) ذخیره نموده سپس دریافت کننده با استفاده از همان ماتریس، پیام جاسازی شده توسط فرستنده را از داخل پوشانه بازگشایی نموده و تشخیص و تصحیح خطا را روی آن اعمال نماید [۲۱،۲۲].

حال می توان از روش کدینگ مشخصه در نهان نگاری استفاده نمود به نحوی که فرستنده پیام پنهانی را با توجه به H توافقی، به عنوان یک سندرم از شیء پوشش دهنده دریافت می کند.



در این فصل تمام کدهایی که در نظر 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  $Ra(C)$  نشان داده و برابر با مقدار میانگین فاصله از محور  $F_2^n$  تا  $C$  می‌باشد و می‌توان آن را به صورت مفهوم کلاسیک شعاع پوششی  $C$  در نظر گرفت [۲۰].

یک تصویر دیجیتال را به عنوان پوشانه در نظر می‌گیریم. فرستنده ابتدا یک رشته از بیت‌های داده، (مانند رشته 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 ایجاد شده، چون پیام محرمانه و پوشانه دیجیتال بوده، پیام‌های محرمانه با روش‌های مختلفی مثل روش جاسازی ماتریس، در گیرنده قابل بازیابی هستند و می‌توان آن را به صورت بردار-های دودویی در نظر گرفت.

#### ۴.۱. روش پیشنهادی

توجه داشته باشید که اگر  $M \in F_2^r$  پیام ما و  $x \in F_2^n$  رشته بیت استخراجی از پیکسل‌های تصویر رسانه و وقتی  $n \geq r$  باشد، معمولاً یک  $(n, r)$  طرح نهان نگاشته  $S$  را به صورت یک جفت از توابع بازیابی کننده و تعبیه کننده (از اطلاعات) به صورت  $S = (\text{emb}, \text{rec})$  با استفاده از کدگذاری، طبق رابطه ۱ قابل تعریف می‌باشد.

$$\text{Emb}: F_2^n \times F_2^r \rightarrow F_2^n \text{ and } \text{rec}: F_2^n \rightarrow F_2^r \quad (1)$$

به این ترتیب برای  $(x, m) \in F_2^n \times F_2^r$  خواهیم داشت:  $\text{rec}(\text{emb}(x, m)) = m$ . تمام این حالت تضمین می‌کند ما همیشه پیام صحیح  $m$  را از بردار پنهان  $\text{emb}(x, m)$  به درستی بازیابی کنیم که این پیام در حقیقت، پیام پنهان (راز) در این بردار است؛ بنابراین دغدغه اصلی طراحی یک سیستم نهان نگار غیر قابل تشخیص این است که تعداد تغییرات پیام تعبیه شده  $d(x, \text{emb}(x, m))$  زمانی که  $d$  به قدری کوچک باشد تا شخص سوم نتواند آن را شناسایی کند و یا تشخیص دهد.

حال فرض کنید  $x \in F_2^n$  ممکن است یک توالی از  $n$  بیت استخراج شده از پیکسل‌های شیء پوششی مورد نظر باشد، فرض کنید  $M \in F_2^m$  پیام مورد نظر برای تعبیه در آن عبارت باشد  $(m \leq n)$ . ارسال کننده و دریافت کننده از پیش بر روی ماتریس  $H \in F_2^{m \times n_2}$  از درجه (رتبه)  $m$  و متناسب با کد  $C = [n, k, d]$ ، توافق می‌کنند. برای اجرای تعبیه پیام پنهان، فرستنده عبارت ذیل  $(\text{emb})$  را محاسبه نموده و شماره یک بیت از رشته  $n$  بیتی رسانه که باید تغییر نماید را به عنوان خروجی به دست می‌آورد (همان  $A$ ). سپس با تغییر یک بیت از رشته بیت رسانه،  $X'$  را برای گیرنده ارسال می‌نماید. دریافت کننده، پیام پنهان  $m$  را با استفاده از رابطه  $\text{rec}$  از پوشانه اصلی که تنها یک بیت از  $n$  بیت آن تغییر نموده است، استخراج می‌نماید.

$$\begin{aligned} \text{emb}: (X, M) &\rightarrow (H \cdot X^t) \text{ xor } M^t = A, (X, A) \rightarrow X' \\ \text{rec}: H \cdot X'^t &= M^t \rightarrow M \end{aligned} \quad (2)$$

با این روش ساخت نهان نگاری‌های مبتنی بر کد امکان پذیر است. توجه داشته باشید که ما با این روش  $m$  بیت پیام را داخل  $n$  بیت رسانه جاسازی نماییم، ولی نکته که اهمیت دارد، استفاده از کدهایی می‌باشد که کمترین تغییر را داشته باشد. بدین منظور، بسته به نوع کدی که استفاده می‌نماییم، برای طرح خود می‌توان از سه مؤلفه  $\text{cov}(\rho, N, n)$  استفاده نمود [۵] که در آن جاسازی  $n$  بیت در  $N$  بیت با حداکثر تغییرات  $\rho$  بیت صورت می‌گیرد. بهتر است برای کارایی بالا از کدهایی استفاده نماییم که در آن کران  $\rho$  حداقل باشد.



به عنوان مثال فرض کنید فرستنده برای نهان نگاری پیام  $M=110$  از رسانه تصویری استفاده می کند که رشته بیت استخراجی  $X=1110000$  از پیکسل های تصویر رسانه استخراج شده و ماتریس  $H$  کد خطی همینگ  $C=[7,4,3]$  را به صورت ذیل با طرف گیرنده توافق می کند. (دقت داشته که کد مورد استفاده ما در این مثال یک طرح  $\text{cov}(1,7,3)$  می باشد).

$$\text{Emb: } H = \begin{bmatrix} 1110100 \\ 1101010 \\ 1011001 \end{bmatrix} \rightarrow \begin{bmatrix} 1110100 \\ 1101010 \\ 1011001 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \text{ xor } \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \rightarrow X' = 11100\mathbf{1}0$$

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

دقت داشته باشید که این روش تنها برای کدهای خطی یا کد همینگ صادق نیست و فرستنده و گیرنده می توانند بر روی کد دیگری به توافق رسیده و فرایند نهان نگاری را اجرا نمایند. به عنوان مثال ماتریس کنترل مشابهت ذیل مربوط به کد کانولوشن نوع B2 بهینه می باشد که می توانند بین فرستنده و گیرنده توافق شده باشد. در این مثال فرستنده از این ماتریس برای جاسازی هر پیام ۳ بیتی ( $M=100$ ) در ۶ بیت پوشانه استخراج شده از تصویر ( $X=111000$ ) استفاده می نماید ( $\text{cov}(1,6,3)$ ) و گیرنده بر همین اساس به راحتی می تواند به پیام درج شده در پوشانه برسد.

$$\text{Emb: } H = \begin{bmatrix} 001000 \\ 000110 \\ 010101 \end{bmatrix} \rightarrow \begin{bmatrix} 001000 \\ 000110 \\ 010101 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \rightarrow X' = 111000\mathbf{1}$$

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

نکته) در این اینجا به این مسئله دقت کنید کلمه "رمزگشایی" به معنای "رمزگشایی کامل" است. به خاطر بیاورید رمزگشایی کامل نوعی مسئله NP کامل محسوب می شود. در نتیجه گرچه مراحل بالا در مرحله تئوری بر روی تمام کدها با شرایطی نظیر داشتن رمزگشایی کارآمد از لحاظ محاسباتی قابل کاربرد هستند، زیرا تنها اندکی از کدها به صورت عملی قابل استفاده اند. اصلی ترین نقش را در بین تمام آن ها، کدهای همینگ به دلایلی چون رمزگشایی ساده و نیز کارآمدی بالای آن ها، وظیفه تعبیه سازی (جاسازی) طرح نهان نگاری بر عهده دارند.

در مواردی که ملزم به پیروی از یک الگوی متنی خاص برای مخفی کردن اطلاعات هستیم می توان از کدهای تصحیحی خطای خطی به منظور بازیابی درست پیام استفاده کرد. با استفاده از این کدها می توان بیت های خطا را در یک پیام تشخیص و آن را تغییر داد. در مواردی که کدهای تصحیح خطا در مورد داده های پوشانه استفاده می شوند نیز می توان





پیام‌های خود را به شکل بیت‌های اشتباه پوشانه در آن مخفی کرد و گیرنده پیام نیز بدون اعمال کدهای تصحیح خطا پیام را بازیابی کند. کد تصحیح خطای همینگ و کد گردشی از جمله کدهایی است که در این رابطه استفاده می‌شود. کد تصحیح خطای گردشی به منظور تصحیح خطاهای دسته‌ای که در فایل‌های دیجیتالی معمول تر است، مناسب تر می‌باشد. مهم‌ترین عیب این روش‌ها بیت‌های اضافی است که به داده‌های واقعی تحمیل می‌شود و عملاً با توجه به اینکه افزایش ظرفیت باعث پائین آمدن فاکتورهای امنیتی دیگر در مخفی سازی می‌شود به کارگیری این روش‌ها در مورد پیام‌های طولانی مناسب نیست. روش ساده‌تر استفاده از پیریتی در تشخیص خطا می‌باشد. اگرچه پیریتی تنها ۱ بیت اضافه به هر بایت پیام اضافه می‌کند ولی در صورتی که تنها ۱ بیت خطا رخ داده باشد می‌تواند در تشخیص آن مفید واقع شود.

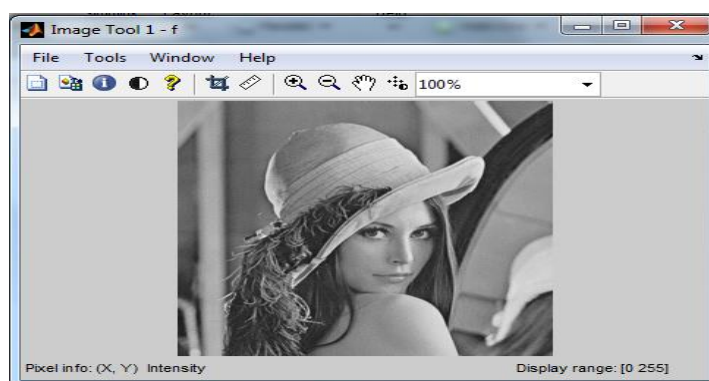
#### ۴.۲. کاربرد کد بهینه

یافتن کدهای بهینه  $[n, k]$  علاوه بر اینکه نوعی مسائل ترکیبی هستند، یافتن کوچک‌ترین مقدار  $k$  دارای کاربردهای زیر است. همان‌گونه که قبلاً بیان شد، شیء پوششی مانند یک تصویر اسکن شده را نوعی دگرگونی بالاتر معرفی می‌کند و در نتیجه اطلاعات زیادی را می‌توان در آن تعبیه کرد.

مورد دیگری که کدها می‌توانند در آن استفاده شوند سناریوهای غیر خصمانه هستند که در آن امنیت مسئله اصلی نیست. در اینجا هدف اصلی ارتباطات غیرقابل ردیابی به هدف ارتباطات غیر ناراحت‌کننده تقلیل داده‌اند و در نتیجه دگرگونی‌های بیشتری را می‌توان در اشیا تحت پوشش ایجاد کرد به خصوص اگر شیء تحت پوشش را در شرایط احتمالی به صورت نیمه بهینه در دریافت‌کننده بتوان تغییر داد مانند گوش دادن به یک فایل موسیقی در ماشین. برای مثال، فرد ممکن است از موج‌های رادیو به عنوان شیء پوشش استفاده کند و تگ‌ها یا اطلاعات اضافی زیادی را در ابتدای آن ایجاد کند مانند شرایط آب و هوایی فعلی یا شرایط ترافیک حال حاضر و غیره.

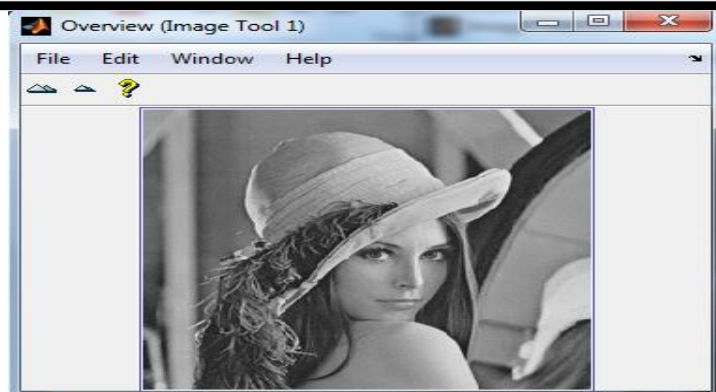
#### ۴.۳. شبیه‌سازی روش پیشنهادی

شکل شماره ۶ را به عنوان یک رسانه پوششی با سایز ۳۵۸ کیلوبایت در نظر بگیرید. حال اگر روش پیشنهادی را روی آن به ازای تمام پیکسل‌های رسانه با استفاده از نرم‌افزار Matlab شبیه سازی نمائیم، اطلاعاتی معادل ۱۳۴,۳ کیلوبایت داخل رسانه ذخیره نموده‌ایم. به عبارت دیگر می‌توان معادل ۳۷,۵٪ حجم کل رسانه اولیه بدون تغییر سایز آن، اطلاعات داخل رسانه جاسازی نمود. در همین راستا و با اجرا روش نهان نگاری پیشنهادی بر روی نقاط لبه‌ای رسانه اصلی، نتیجه‌ای طبق شکل شماره ۷ و جدول ۳ حاصل می‌گردد.



شکل ۶- تصویر اولیه رسانه بدون جاسازی



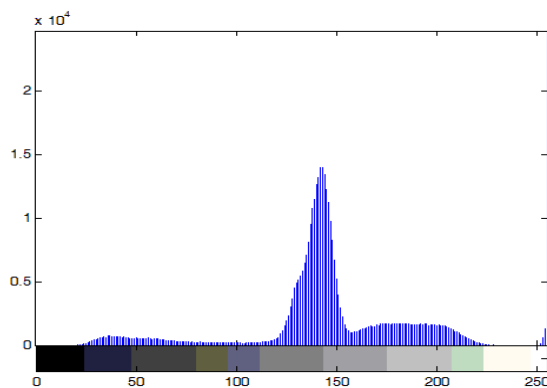


شکل ۷- اجرای روش پیشنهادی بر روی لبه های کنی

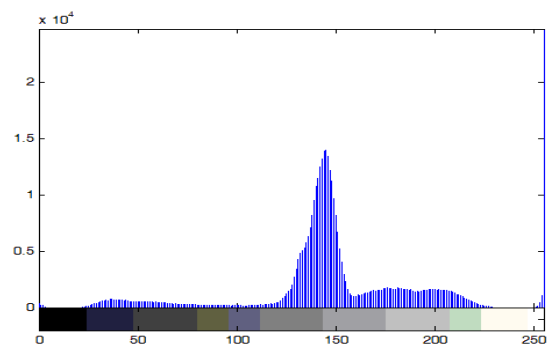
جدول ۳- شبیه سازی روش پیشنهادی در نقاط لبه ای پوشانه

مقاومت	SSIM	PSNR	ظرفیت جاسازی
۰.۷۵٪	۰.۹۶۹	۶۸.۰۸	3bit*تعداد لبه ها (۱۳۰ کیلوبایت)

لازم به ذکر می باشد که با این روش، در هر نقطه لبه ای با عمق ۸ بیتی تصویر خاکستری می توان ۳ بیت اطلاعات جاسازی نمود، به طوری که تغییرات تصویر رسانه خیلی اندک باشد. این امر را با مقایسه نمودار هیستوگرام تصویر رسانه اصلی (شکل ۶) و تصویر نهان نگاری شده با روش پیشنهادی، طبق شکل های ذیل می توان به وضوح مشاهده نمود.



شکل ۸- نمودار هیستوگرام رسانه اصلی



شکل ۹- نمودار هیستوگرام رسانه نهان نگاری شده



همان طوری که مشاهده می‌نمایید، نتیجه این روش پنهان‌نگاری ظرفیت، شفافیت و مقاومت بالای آن، تنها با یک ماتریس کنترل مشابهت مشترک بین فرستنده و گیرنده می‌باشد.

## ۵. نتیجه‌گیری

در این مقاله تکنیک‌های مختلف پنهان‌نگاری تصاویر دیجیتال مورد مطالعه، بررسی و مقایسه قرار گرفت. نتیجه به دست آمده این است که تکنیک‌های پنهان‌نگاری در حوزه مکان، دارای مزیت سادگی و سرعت هستند. این تکنیک‌ها پیچیدگی محاسباتی کمتری نسبت به تکنیک‌های حوزه فرکانس داشته و میزان اطلاعاتی که با استفاده از آن‌ها در تصویر درج می‌گردد نسبتاً زیاد و انحرافات که در نتیجه‌ی درج این اطلاعات به وجود می‌آید بسیار کم است، اما تکنیک‌های موجود در این حوزه در برابر عملیات پردازش تصویر و حملات هندسی بسیار ضعیف و شکننده بوده و اطلاعات پنهان‌نگاری را در کاربران غیرمجاز قرار می‌دهند. از این رو بیشتر در سیستم‌های پنهان‌نگاری شکننده به کار می‌روند. از آنجاکه پنهان‌نگاری در حوزه فرکانس بسیار قدرتمندتر از حوزه مکان است، در نتیجه تکنیک‌های حوزه فرکانس به طور گسترده‌تر اعمال می‌شوند. اگرچه این تکنیک‌ها به الگوریتم‌های پیچیده و هزینه‌ی محاسباتی بیشتری نسبت به حوزه مکان نیاز دارند، اما در مقایسه با تکنیک‌های حوزه مکان، تکنیک‌های حوزه فرکانس در دست یافتن به الگوریتم‌های پنهان‌نگاری تصاویر دیجیتال از لحاظ غیرقابل مشاهده بودن و نیازمندی‌های استحکام بهتر می‌باشند و در برابر حملات مقاومت زیادی از خود نشان می‌دهند.

با توجه به مطالب بیان شده می‌توان نتیجه گرفت که روش‌های حوزه مکان مزیت‌هایی همچون جاسازی و بازیابی سریع و ظرفیت بالا را دارا می‌باشند اما مهم‌ترین اشکال استفاده آن، مقاومت پایین و سوءاستفاده راحت مهاجمان باعث گرایش به سوی حوزه تبدیل شده که شاهد گسترش و رونق روزافزون آن هستیم. حال می‌توان روش پنهان‌نگاری با استفاده از نظریه کدگذاری را برای حوزه مکان ارائه نمود که علاوه بر برخورداری از مزایای این حوزه مثل ظرفیت و سادگی بالا، همچون حوزه تبدیل از مقاومت مناسب بهره برد و دیگر نیازی به الگوریتم‌های پیچیده و هزینه‌ی محاسباتی بیشتری نباشد.

## ۶. مراجع

۱. امیر اسماعیلی. (۱۳۹۳)، "بررسی و مقایسه روش‌های پنهان‌نگاری"، پایان‌نامه کارشناسی ارشد، دانشگاه جامع امام حسین(ع)، تهران.
۲. مولا نژاد حسین، "مخفی‌سازی و نشانه‌گذاری اطلاعات"، پایان‌نامه کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، ۱۳۸۵.
۳. امانی شهرک محمد عرفان، "ارائه یک الگوریتم پنهان‌نگاری ویدئو با در نظر گرفتن برخی از مؤلفه‌های پنهان‌کاو"، پایان‌نامه کارشناسی ارشد، دانشگاه امام حسین(ع)، ۱۳۹۵.
- 4.L. Zhang, H. Wang, and R. Wu, "A high-capacity steganography scheme for JPEG2000 baseline system," IEEE Trans. Image Process., vol. 18, no. 8, pp. 1797–1803, 2009.



- 5.R. Böhme, "Advanced statistical steganalysis". Springer Science & Business Media, 2010.
- 6.I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography", Morgan Kaufmann, 2007.
- 7.G. J. Simmons, "The prisoner's problem and the subliminal channel," Advances in Cryptology Proceedings of Crypto, vol. 83. pp. 51–67, 1984.
- 8.R. J. Anderson, "Proceedings Information Hiding: First International Workshop", Cambridge, UK, May 30-June 1, 1996. Proceedings. Vol. 1. Springer Science & Business Media, 1996.
- 9.Li. Xiaoxia, and Jianjun Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm", Information Sciences 177.15: 3099-3109, 2007.
10. C. Gonzalez, "Digital Image Processing 2nd Edition," 2008 by Pearson Education, Inc.
11. A. D. Ker, "Improved detection of LSB steganography in grayscale images," in Information Hiding, 2004, pp. 97–115.
12. Ko. Chin. Chang, Chien-Ping, Huang, Ping S, and Tu, Te-Ming, A novel image steganographic method using tri-way pixel-value differencing, Journal Of Multimedia, Vol. 3, NO. 2, p 37-44 June 2008.
13. L. Xiaoxia and W. Jianjun, "A steganographic method based upon JPEG and particle swarm optimization algorithm", Department of Electronics Engineering, Fudan University, Shanghai, China, accepted 11 February 2007.
14. A. Westfeld, "Detecting low embedding rates," International Workshop on Information Hiding, Springer Berlin Heidelberg, 2002.
15. T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in Information hiding, 2010, pp. 161–177.
16. P. Wayner, "Disappearing Cryptography," 2nd Ed, Elsevier Science: US, 2002.
17. P. Salle, "model-based methods for steganography and steganalysis," International journal of image Graphics, vol.5,no. 1,pp. 167-190,2005.
18. M. N Agarwal, , & M. N.Singh,. "Survey of Transform Domain Digital Image Watermarking". Vol.02, No. 06, pp. 240-244, 2013.
19. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," Secur. Privacy, IEEE, vol. 1, no. 3, pp. 32–44, 2003.
20. J. Bierbrauer urgen, J. Fridrich, "Constructing good covering codes for applications in Steganography," BINGHAMTON (NY) 13902-6000, 2015.
21. M. Khatirinejad, "Linear codes for high payload steganography," Elseier, 2009.
22. C. Munuera, "Hamming codes for wet paper steganography," Springer Science Business Media New York, 2015.