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

علی نورآذر[1*] ، دکتر زین العابدین نوروزی [2]،مهدی میر[3] و حسن خالقی گرجی[4]

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 نهان‌نگاری در پوشانه تصویر می‌پردازد. هدف اصلی، ارائه‌ی راهکاری نوین و بهینه در برای استفاده از خاصیت کدگذاری برای درج داده‌های محرمانه در الگوریتم جاسازی است. چرا که استفاده از نظریه کدگذاری در نهان‌نگاری ضمن بهره‌مندی از خواص آن و افزایش ظرفیت و مقاومت در حوزه مکان، سبب افزایش امنیت طرح نهان‌نگاری در برابر نهان‌کاوها خواهد شد. برای دست‌یابی به این هدف، ایده‌ی استفاده از ماتریس کنترل مشابهت کدهای خطی در پوشانه تصویر، در روش پیشنهادی مطرح شده است. چرا که با درج داده‌های محرمانه در پیکسل‌های 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 چشم‌گیر شفافیت (۵۸ الی ۷۰) خواهد شد.

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

۱. مقدمه

رشد و توسعه فناوری‌های دیجیتال و به‌دنبال آن تولید انبوهی از داده‌های دیجیتالی چالش‌ها و فرصت‌های زیادی را به همراه داشته است. از زمانی که انسان‌ها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط پنهان و امن یک خواسته

[1] **Email: A_norazar@yahoo.com**

مهم و ضروری افراد بوده است. در این میان روش‌های پنهان‌سازی اطلاعات[1] که تاریخچه‌ای چند هزار ساله دارند، با ظهور داده‌های دیجیتالی شکلی کاملاً جدید به خود گرفته است. علم نهان‌نگاری را می‌توان هنر مخفی کردن پیام در پوششی از اطلاعات بیان نمود. نشان‌گذاری[2] و نهان‌نگاری[3] دو حوزه‌ی اصلی پنهان‌سازی داده‌ها محسوب شده و هر یک اهدافی را دنبال می‌نمایند [۱]. تأمین امنیت با رمزنگاری امکان‌پذیر است؛ در رمزنگاری، رسانه انتقال دارای مفهوم و داده مستقل نبوده و پنهان بودن داده، آشکار می‌باشد و افراد غیرمجاز به پیام محرمانه، دسترسی ندارند. در نشان‌گذاری حفاظت از سیگنال میزبان در برابر تهدیدات گوناگون مورد بحث قرار می‌گیرد و بیش‌ترین کاربرد آن در محصولات نرم‌افزاری است و به جنبه تجاری و اقتصادی قضیه می‌پردازد، حال آن‌که هدف از نهان‌نگاری مخفی ماندن وجود پیام از نظر دشمن است و بیش‌تر به جنبه نظامی و غیرتجاری معطوف می‌گردد. در حقیقت نهان‌نگاری را می‌توان دانش و هنر پنهان‌سازی یک پیام محرمانه در درون یک سیگنال میزبان دانست. سیگنال میزبان می‌تواند صوت، تصویر، متن، ویدئو و غیره را شامل شود که در این‌جا با تأکید بر تصویر کار دنبال خواهد شد.

تاکنون الگوریتم‌های گوناگونی برای نهان‌نگاری اطلاعات ارائه‌شده است. نهان‌نگاری در دو حوزه مکان و تبدیل انجام می‌شود. حوزه مکان شامل آن دسته از الگوریتم‌هایی می‌شود که بیت‌های پیام بین بیت‌های میزبان جاسازی می‌شوند و در انجام عملیات نهان‌نگاری، هیچ تبدیلی روی سیگنال پوشش انجام نمی‌پذیرد به‌عنوان مثال در روش جاگذاری LSB بیت‌های پیام در کم‌ارزش‌ترین بیت هر پیکسل گنجانده می‌شوند. حوزه تبدیل شامل آن دسته از روش‌هایی است که اطلاعات بیت‌های پیام روی تمام یا قسمتی از بیت‌های مقادیر ضرایب تبدیل مدنظر جاسازی می‌گردد (پیام محرمانه، در داخل فضای تبدیل سیگنال پوشش جاسازی می‌شود)؛ بنابراین می‌توان گفت که یکی از بهترین روش‌های ایجاد امنیت اطلاعات، نهان‌نگاری است. امنیت یک سیستم نهان نگار به شفافیت خروجی آن مرتبط است. شفافیت یکی از سه معیار مهم در نهان‌نگاری است. از معیارهای مهم دیگر در نهان‌نگاری، ظرفیت و مقاومت است. طبق آمار ارائه‌شده از تحقیقات و نرم‌افزارهای موجود درزمینهٔ نهان‌نگاری و به دلیل استفاده همه‌گیر، در دسترس بودن و ساده بودن الگوریتم‌ها، سهم تصویر بیشتر از رسانه‌های دیگر در نهان‌نگاری است و با توجه به این مسئله که رسانه تصویر از سایر رسانه‌های این حوزه رایج و متداول می‌باشد، می‌تواند به‌عنوان بهترین ابزار پوششی و فریب استفاده شود. لذا این رسانه به‌عنوان مهم‌ترین و پرکاربردترین رسانه پوششی جهت استفاده در نهان‌نگاری مورداستفاده قرارگرفته است، به‌طوری‌که 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.

روش‌های نهان‌نگاری حوزه مکان باوجود ظرفیت بالا، از مقاومت بسیار پائینی برخوردار است. با توجه به این مطلب، یافتن راه‌هایی برای افزایش مقاومت تصویر حاوی اطلاعات پنهان‌شده ضروری است. بهترین راه‌حل برای این مشکل، این است که به‌جای حوزه مکان، اطلاعات را در داخل حوزه‌های تبدیل تصویر، نظیر فرکانس پنهان نماییم که از مقاومت بالایی نسبت به حوزه مکان برخوردار است. لذا روش‌های نهان‌نگاری در حوزه تبدیل به وجود آمده و گسترش یافتند.

در این مقاله روش جدیدی برای نهان‌نگاری تصویر در حوزه مکان بر اساس نظریه کدگذاری معرفی می‌شود 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 می‌توان بدین منظور از روش کدینگ مشخصه در نهان‌نگاری تصویر استفاده نمود به‌طوری‌که فرستنده پیام پنهانی را با توجه به ماتریس کنترل مشابهت[4] H توافقی، مشخصه‌ای از شیء پوشش‌دهنده

[1] *Information Hiding*
[2] *watermarking*
[3] *steganography*
[4] 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، منحصراً 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 جمع‌آوری‌شده و ارائه می‌گردد.

۲. نهان‌نگاری اطلاعات

برای حفاظت از داده‌های سری در برابر دسترسی غیرمجاز (محرمانگی و تمامیت پیام) از دو تکنیک رمزنگاری[1] و نهان‌نگاری[2] 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[3] می شود 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]

جدول۱- تعداد مقالات منتشرشده درزمینهٔ 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

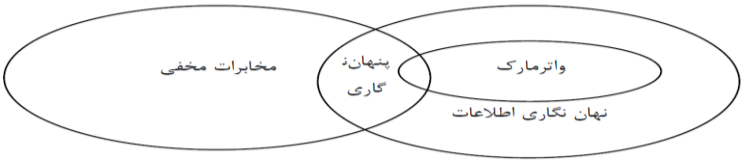
در ادامه ابتدا تاریخچه سیستم‌های مخفی سازی اطلاعات بیان‌شده و سپس مرور کوتاهی بر سیستم‌های رمزنگاری و نحوه برقراری امنیت اطلاعات از طریق این سیستم‌ها می‌پردازیم.

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 پرقدرت 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

[1] encryption
[2] Steganography
[3] embedding

انتشارات الکترونیکی مورداستفاده قرار می‌گیرد که به عدد سریال می‌توان اشاره کرد. امروزه نهان‌نگاری با پیشرفت نرم‌افزارها گسترش یافته و واتر مارکینگ (نقش نگاری) نیز به‌عنوان یک فن در فرایند نهان‌نگاری موردتوجه واقع‌شده 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 شماره۱) [۳،۴].



شکل۱- نسبت بین پنهان نگاری 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 به‌گونه‌ای در پوشانه پنهان گردد که هیچ‌کس به‌جز فرستنده و گیرنده از وجود آن مطلع نشود. به‌عبارت 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[1] با تغییر دادن صورت ظاهری پیام محرمانه، اطلاعات دیگری تحت عنوان متنِ رمزشده که اغلب شکلی نامفهوم و تصادفی دارند، تولید می‌نمایند. به‌عبارت دیگر در رمزنگاری وجود اطلاعات محرمانه و یا ارسال پیام محرمانه کاملاً مشخص است، اما تنها گیرنده‌ی از پیش تعیین‌شده، توانایی بازیابی اطلاعات را دارد، این در حالی است که مشاهده‌ی داده‌های رمزشده بر روی کانال سبب جلب‌توجه مهاجمان خواهد شد. در چنین وضعیتی حتی اگر مهاجم به‌دلیل 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 آن‌که به بیان تفصیلی نهان‌نگاری بپردازیم، ابتدا تعاریف ذیل را ارائه دهیم [۶،۷].

پوشانه یا حامل اطلاعات[2]: 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[3]: 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.

گنجانه اطلاعات[4]: گنجانه فایل حاوی اطلاعات است که پس از جاسازی داده در پوشانه به دست می‌آید. گنجانه پس از جاسازی داده در مسیر انتقال یا در گیرنده می‌تواند تحت تأثیر پاره‌ای از تغییرات عمدی یا غیرعمدی قرار گیرد. این

[1] *Cryptography*
[2] *Host media*
[3] *Embedding*
[4] *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[1]: 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 رمزشده و سپس در پوشانه مخفی شوند. کلید رمزنگاری می‌تواند با کلید نهان‌نگاری متفاوت باشد.

الگوریتم آشکارسازی کور[2]: روش‌هایی که برای بازیابی داده نیاز به پوشانه اطلاعات ندارند و به‌عنوان روش‌های مخفی آشکارسازی نام‌برده می‌شوند.

الگوریتم آشکارسازی غیرکور[3]: روش‌هایی که برای بازیابی داده نیاز به پوشانه اطلاعات دارند و با مقایسه پوشانه و گنجانه اطلاعات داده‌های جاسازی‌شده را بازیابی یا علامت درج‌شده در گنجانه را احراز می‌کنند.

مهاجم غیرفعال[4]: در این‌جا مهاجم در کانال ارتباطی قرار نگرفته و فقط از اطلاعات ارسالی استفاده می‌نماید.

مهاجم فعال[5]: 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[6]: در این‌جا مهاجم می‌تواند خودش را به‌جای فرستنده جا بزند. پیام محرمانه را عوض نماید و پوشانه را تغییر دهد.

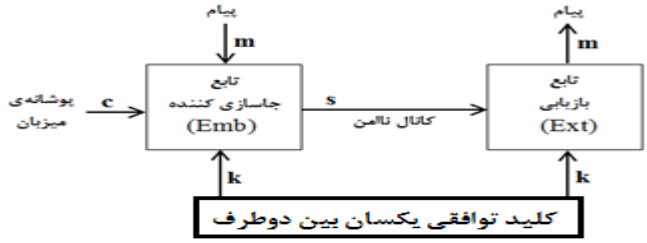
در ادامه قصد داریم تعریفی دقیق از یک فرآیند نهان‌نگاری ارائه دهیم. فرض کنید که k کلید نهان‌نگاری باشد که از مجموعه K (مجموعه‌ای از تمام کلیدهای ممکن نهان‌نگاری) انتخاب شده است؛ M مجموعه‌ی در بردارنده‌ی تمامی پیام‌هایی است که قابلیت مخفی شدن را دارا هستند؛ C نیز مجموعه‌ای از تمامی رسانه‌های پوششی است. یک طرح نهان‌نگاری توسط دو نگاشت تعریف می‌شود: نگاشت جاسازی[7] (Emb) و نگاشت بازگشایی[8] (Ext). این دو نگاشت را می‌توان مطابق معادله‌ی(۱-۲) تعریف نمود [۹ و ۸].

تعریف (۲-۱) : پنج‌تایی (C,M,K,Emb,Ext) را یک دستگاه نهان‌نگاری[9] می‌گویند [۸] هرگاه داشته باشیم:

$$Emb: C \times K \times M \longrightarrow C$$
$$Ext: C \times K \longrightarrow M \qquad (۲-۱)$$

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

[1] *Stego key*
[2] *Blind detection method*
[3] *Non blind detection method*
[4] *Passive*
[5] *Active*
[6] *Malicious*
[7] *Embedding mapping*
[8] *Extraction mapping*
[9] *Steganographic system*



شکل۲: نمودار یک فرآیند نهان‌نگاری [۸]

۲,۳.ملزومات و ویژگی‌های سیستم نهان‌نگاری

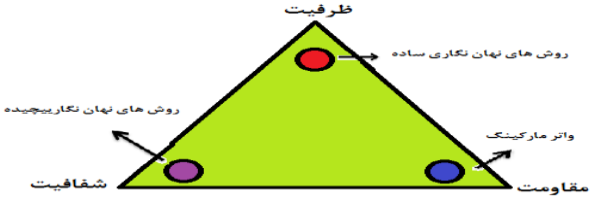
گرچه هر کاربردی از نهان‌نگاری تصویر نیازهای خاص خود را دارد، بااین‌همه تمام روش‌های نهان‌نگاری باید ملزومات مشترکی را رعایت کنند که در این خصوص برای مشخصه‌های مهم هر سیستم نهان‌نگاری اطلاعات می‌توان به پارامتری نظیر شفافیت، استحکام (مقاومت)، ظرفیت سیستم نهان‌نگاری برای پنهان نمودن اطلاعات، امنیت و پیچیدگی آن اشاره نمود که معمولاً رسیدن به برتری در یکی منجر به نتایج ضعیف‌تری در پارامترهای دیگر می‌شود .آنچه مهم است این است که در نهان‌نگاری نباید اطلاعات از لحاظ دیداری و یا شنیداری قابل‌کشف باشد؛ بنابراین می‌توان گفت که این ملزومات به یکدیگر مربوط‌اند.

شفافیت[1]: یکی از معیارهای ارزیابی نهان‌نگاری، میزان شباهت بین تصویر اصلی و تصویر واتر مارک شده می‌باشد . نهان‌نگاری بکار رفته ضمن نامحسوس بودن، نباید از کیفیت تصویر بکاهد و یا اثراتی بر روی تصویر بگذارد که از دید کاربر قابل‌درک باشد.

مقاومت[2]: معیار ارزیابی دیگری که باید از آن یادکرد، میزان مقاومت تصویر نهان‌نگاری در برابر انواع پردازش‌ها می‌باشد. به‌عبارت‌دیگر میزان قابل‌کشف بودن پیام از پوشانه نهان‌نگاری شده در برابر پردازش‌هایی نظیر فشرده‌سازی، فیلترینگ، نویز، چرخش و انواع تبدیلات به چه میزان خواهد بود و همواره این مسئله مطرح خواهد بود که نهان‌نگاری در برابر این پردازش‌ها چه دوامی خواهد داشت.

ظرفیت[3]: در یک سیستم نهان‌نگاری تعداد اطلاعات قابل جاسازی در سیستم را به‌عنوان ظرفیت سیستم تلقی می‌کنیم . مقدار اطلاعاتی را که می‌توان در یک نهان‌نگاری جاسازی کرد باید تا حد امکان بالا باشد. به عبارت کلی ظرفیت برابر ماکزیمم مقدار اطلاعاتی است که می‌توان در یک رسانه‌ی پوششی پنهان کرد بدون اینکه به امنیت سیستم خدشه‌ای وارد شود و اینکه بتوان پیام را با اطمینان بالایی از رسانه جاسازی‌شده بازیابی نمود. ظرفیت نهان‌نگاری عموماً نباید با ظرفیت جاسازی پیام مقایسه گردد. ولی معمولاً ظرفیت نهان‌نگاری خیلی کمتر از ظرفیت جاسازی پیام می‌باشد. عموماً حتی برای طرح‌هایی با جاسازی ساده، تعیین ظرفیت پنهان نگار بسیار سخت می‌باشد.

نکته: سه ویژگی اشاره‌شده تشکیل یک مثلث معروف را می‌دهند که در شکل ذیل نشان داده می‌شود:



شکل۳: سه ویژگی اساسی سیستم نهان‌نگاری

[1] Invisibility
[2] Robustness
[3] Capacity

سه ویژگی فوق به‌طور بسیار تنگاتنگی به یکدیگر وابسته هستند. یک رابطه‌ی بامعنی در مورد ویژگی‌های مذکور وجود دارد: **ثابت = (مقاومت × ظرفیت)**

رابطه‌ی فوق بدین معناست که با افزایش مقاومت حتماً ویژگی ظرفیت کاهش می‌یابد و بالعکس (درصورتی‌که 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 ازلحاظ مقاومت و شفافیت بهتر از حوزه مکان است.

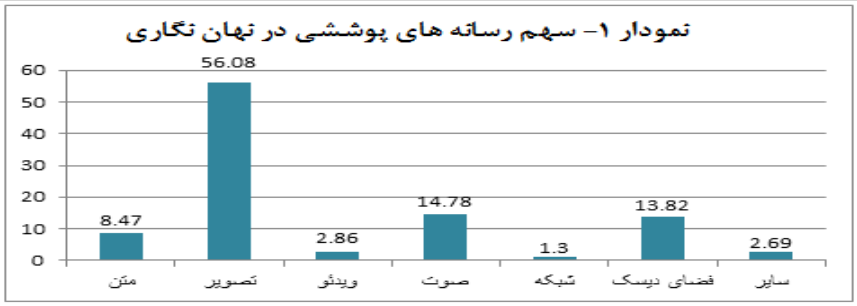
جدول ۲- مقایسه نهان‌نگاری در دو حوزه مکان و تبدیل

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 درزمینهٔ 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 مورداستفاده قرارگرفته است، به‌نحوی‌که 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 بیان‌شده، اهمیت این نوع رسانه درک شده و سعی خواهیم کرد که با مرور کلی بر روش‌های نهان‌نگاری در این نوع رسانه (تصاویر)، روش نوینی در این خصوص معرفی نماییم. نگاهی آماری به تصاویر موجود در دنیای دیجیتال نشان می‌دهد که پرکاربردترین گونه‌های تصاویر، به ترتیبGIF ، JPEG، PNG و درنهایتBMP می‌باشند.

۳,۱. روش‌های نهان‌نگاری تصویر

در این بخش تکنیک‌های مختلف نهان‌نگاری تصاویر دیجیتال موردبررسی و مقایسه قرار می‌گیرند. تکنیک‌های نهان‌نگاری تصاویر دیجیتال به‌طورکلی به دو گروه تکنیک‌های حوزه‌ی مکان و حوزه‌ی فرکانس تقسیم‌بندی می‌شوند. در هر یک از حوزه‌های مکان و فرکانس به شیوه‌های گوناگونی می‌توان داده‌ها را پنهان نمود. هرکدام از این تکنیک‌ها مزایا و معایب خاص خود را داشته و بسته به کاربرد موردنظر می‌توان از آن‌ها استفاده نمود.

۳,۱,۱. حوزه مکان

در روش‌های حوزه‌ی مکان، درج پیام بر اساس تغییر یا دست‌کاری مستقیم مقادیر پیکسل‌های تصویر صورت می‌گیرد و در انجام عملیات نهان‌نگاری، هیچ تبدیل روی پوشانه انجام نمی‌پذیرد و کلیه اقدامات مربوط به نهان‌نگاری در حوزه مکان اعمال می‌گردد. برخی از مهم‌ترین روش‌های این حوزه به شرح ذیل می‌باشند که چند روش اصلی را معرفی می‌نماییم.

- روش نهان‌نگاری افزودنی [۶]
- روش نهان‌نگاری مبتنی بر بیت کم‌ارزش LSB[۱] [۱۰,۱۱]
- روش نهان‌نگاری معکوس در بیت کم‌ارزش LSBF[۲] [۱۲,۱۳]
- روش نهان‌نگاری تطبیقی بر اساس اغتشاش جمع‌شونده LSBM[۳] [۱۴,۱۵]
- روش نهان‌نگاری تصادفی در بیت کم‌ارزش RLSB[۴] [۱۶,۱۷]
- روش مبتنی بر مدولاسیون SSM [۱۸]

نهان‌نگاری افزودنی: ساده‌ترین روش برای درج سیگنال پیام در حوزه‌ی مکان، افزودن یک‌رشته نویز شبه‌تصادفی معرف سیگنال پیام به مقادیر روشنایی پیکسل‌های تصویر مورد نظر است. سیگنال نویز معمولاً به‌صورت اعداد صحیح (۱ و

[1] *least significant bit*
[2] *least significant bit flipping*
[3] *LSB maching*
[4] *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[1] 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 به‌وسیله‌ی ترکیب خطی تصویر با یک سیگنال شبه نویز کوچک که توسط نهان‌نگاری درج‌شده، مدوله شده است جاسازی می‌کند [۱۸].

۳،۱،۲. حوزه فرکانس

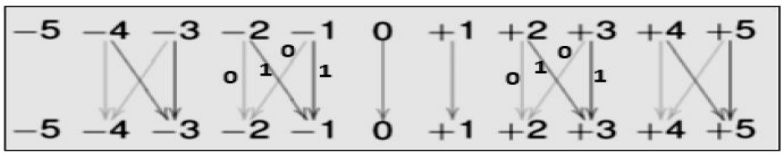
در تکنیک حوزه‌ی فرکانس، ابتدا یک تصویر به مجموعه‌ای از ضرایب این حوزه تبدیل‌شده و سپس پیام در این ضرایب تبدیل‌شده درج می‌شود (پیام محرمانه، در داخل فضای تبدیل سیگنال پو شش جاسازی می‌شود). روش کار به این صورت است که ابتدا توسط یک تابع تبدیل مناسب، تصویر از حوزه‌ی مکان به حوزه‌ی فرکانس انتقال می‌یابد، سپس نهان‌نگاری با تغییر ارزش پیکسل‌ها در حوزه‌ی فرکانس انجام می‌گیرد و درنهایت تصویر به حوزه‌ی مکان برگرداننده می شود. 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 به‌جای 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 مورداستفاده 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 قابل‌درک نبوده، شناسایی‌شده و دور انداخته می‌شود. روش‌های مبتنی بر DCT به دو دسته‌ی DCT منطقه‌ای[2] و

[1] *spread spectrum*
[2] *global*

DCT پایه بلوکی[1] تقسیم‌بندی می‌شوند. COX و همکارانش الگوریتمی را با استفاده از روش DCT منطقه‌ای، مطرح کردند که یک نهان‌نگاری قوی را در مهم‌ترین بخش ادراکی تصویر مبتنی بر HVS درج می‌کرد. درج پیام در این بخش مزیت پایداری نهان‌نگاری در برابر برنامه‌های فشرده‌سازی را فراهم می‌کند، زیرا اکثر برنامه‌های فشرده‌سازی بخش‌هایی از تصویر را حذف می‌کنند که کم‌اهمیت‌ترین بخش از نظر ادراکی باشند. در این روش تصویر را به بلاک‌های ۸*۸ تقسیم می‌کنند، ۶۴ ضریب در تبدیل کسینوسی گسسته به دست می‌آید. توجه کنید که راه مخفی کردن بیت‌های پیام در ضرایب DCT قرار دادن آن‌ها در بیت‌هایی با کم‌ترین ارزش ضرایب است. یکی از محدودیت‌های این روش آن است که تعداد زیادی از ۶۴ ضریب تبدیل کسینوسی DCT در هر قطعه ۸*۸ از پیکسل‌های تصویر مساوی با صفر هستند و تغییر تعداد زیادی صفر به مقادیر غیرصفر می‌تواند بر نرخ فشرده‌سازی تصویر اثر منفی بگذارد، به‌همین دلیل است که ظرفیت پنهان‌سازی در ضرایب DCT خیلی کم‌تر از ظرفیت در حوزه مکان است [۶].

روش نهان‌نگاری Jsteg: این روش توسط درک اوفام[2] طراحی شد. الگوریتم آن، بیت‌های کم‌ترین ارزش ضرایب DCT را به‌صورت متوالی با بیت‌های پیام جایگزین می‌نماید. این الگوریتم دارای کلید محرمانه نیست؛ بنابراین هر کس که به فرآیند نهان‌نگاری واقف باشد، می‌تواند به پیام محرمانه دست یابد. در این روش ضرایب DCT که صفر یا یک باشند، جایگذاری نمی‌شوند. شکل (۴) نحوه جاسازی بیت‌های پیام را نشان می‌دهد[۳۸].



شکل۴: نحوه نهان‌نگاری Jsteg در بیت‌های ضرایب DCT [۲]

این روش اولین روشی که در دسترس عموم قرار گرفته و ساده و بدون پیچیدگی محاسباتی است. هم‌چنین به‌دلیل استفاده از فرمت JPEG نرخ فشرده‌سازی آن بالا است. در این روش به‌دلیل ذخیره کردن در ضرایب غیرصفر و یک، دارای حجم پنهان‌سازی کم است، هیستوگرام تصویر پوشش را تغییر می‌دهد و با تغییر در جفت مقدارهای کنار هم در هیستوگرام تصویر پوشش توسط حمله کای‌اسکوار (مربع خی‌دو) قابل اجراء است.

روش نهان‌نگاری F5: در این روش الگوریتم نهان‌سازی، پیام را در بیت‌های با کم‌ترین ارزش ضرایب DCT از ابتدا و به‌صورت متوالی ولی به شیوه‌ای خاص با بیت‌های پیام جایگزین می‌نماید. در این روش تغییرات ضرایب DCT به کم‌ترین مقدار خود خواهند رسید. در این روش برخلاف روش‌های قبلی، پیام در کل تصویر به‌صورت گسترده پخش و نهان‌نگاری می‌شود. از آنجایی‌که الگوریتم F5 هیستوگرام ضرایب DCT را اصلاح می‌کند، محققین این روش نشان دادند که این روش بسیاری از مشخصه‌های مهم هیستوگرام مثل یکنواختی را حفظ می‌کند و نمی‌تواند توسط حمله مربع خی‌دو آشکارسازی شود [۱۹]. مزایای این روش عبارتند از: به‌دلیل استفاده از فرمت JPEG نرخ فشرده‌سازی بالا می‌باشد و حجم تصویر نهایی کم است، برای ذخیره‌سازی هر دو بیت، احتیاج به تغییر تنها یک بیت می‌باشد. بدین دلیل دارای کارایی ذخیره‌سازی بالاتری نسبت به روش‌های F3، F4 و Jsteg است و در مقابل مربع خی‌دو مقاوم است. معایب آ نیز عبارتند از: در برابر حمله آماری مقاوم نیست و هیستوگرام ضرایب DCT تغییر می‌کند.

۳,۲.حملات بر سیستم نهان‌نگاری تصاویر

[1] *block based*
[2] *Derek Upham*

حملات عمدی و غیرعمدی متعددی وجود دارد که یک تصویر نهان‌نگاری شده می‌تواند در معرض آن قرار گیرد. در دسترس بودن طیف گسترده‌ای از نرم‌افزارهای پردازش تصویر این امکان را فراهم ساخته است که اجرای حملات بر روی تصاویر نهان‌نگاری شده امکان‌پذیر باشد. هدف این حملات جلوگیری از نهان‌نگاری برای اجرای اهداف موردنظر است. در شکل شماره ۵ تقسیم‌بندی کلی حملات و اهداف آن‌ها را مشاهده می‌نمایید که هرکدام آن‌ها شامل چندین حمله در آن کلاس می‌تواند باشد.

شکل۵- دسته‌بندی کلی حملات بر اساس اهداف

فارغ از تقسیم‌بندی فوق، برخی از متداول‌ترین حملات نهان‌نگاری عبارت‌اند از: حملات تخریب تصویر، حملات هندسی، حملات حذف‌کننده و حملات رمزنگاری. [۱،۲]

۴. نهان‌نگاری تصویر با استفاده از خاصیت کدگذاری

بامطالعه روش کدگذاری مشخصه که آن را "روش تعبیه ماتریس" نیز می‌نامند، نتیجه می‌گردد که در این روش از کد خطی به‌عنوان عنصر اصلی استفاده می‌شود که می‌توان از ویژگی‌های آن در سیستم نهان‌نگاری 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 تشکیل‌دهنده، بعد ثابت و درنتیجه نرخ اطلاعات ثابت، کدی بهینه محسوب می‌شود که مفهومی مناسب با شعاع پوشش این کاربرد خاص را جایگزین نماید. کدهای بهینه خطی که در روش کدگذاری سندرم استفاده می‌شود، می‌توانند متشکل از کدهایی یک یا دوبعدی بر روی GF(2) باشند.

یکی از ویژگی‌های اصلی نهان‌نگاری می‌تواند مقاومت آن در مقابل حملات آماری یا به‌عبارت دیگر آشکارسازی آماری باشد که برای تحقق این هدف از جایگذاری شبه‌تصادفی بر مبنای نظریه کدگذاری می‌توان استفاده گردد، به‌طوری‌که فرآیند جاسازی کم‌ترین تغییرات را داشته و از لحاظ آماری مقاومت بالایی داشته باشد و خواص اصلی را حفظ نماید [۲۰]. بر همین اساس می‌توان از روش نظریه کدگذاری در نهان‌نگاری استفاده نمود به‌طوری‌که فرستنده پیام محرمانه را با توجه به ماتریس کنترل مشابهت (H) 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 جاسازی شده توسط فرستنده را از داخل پوشانه بازگشایی نموده و تشخیص و تصحیح خطا را روی آن اعمال نماید [۲۱،۲۲].

حال می‌توان از روش کدینگ مشخصه در نهان‌نگاری استفاده نمود به‌نحوی‌که فرستنده پیام پنهانی را با توجه به H توافقی، به‌عنوان یک سندروم از شیء پوشش‌دهنده دریافت می‌کند.

در این فصل تمام کدهایی که در نظر گرفته شده‌اند در میدان F2 می‌باشند. فرض کنید C⊆F2n 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 F2n تا C می‌باشد و می‌توان آن را به‌صورت مفهوم کلاسیک شعاع پوششی C در نظر گرفت [۲۰].

یک تصویر دیجیتال را به‌عنوان 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 ایجادشده، 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 به‌صورت 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 به‌صورت یک جفت از توابع بازیابی کننده و تعبیه‌کننده (از اطلاعات) به‌صورت S=(emb,rec) با استفاده از کدگذاری، طبق رابطه-۱ قابل‌تعریف می‌باشد.

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

به‌این‌ترتیب برای $(x,m) \in F_2^n \times F_2^n$ خواهیم داشت: rec(emb(x,m))=m.

تمام این حالت تضمین می‌کند ما همیشه پیام صحیح m را از بردار پنهان emb(x,m) به‌درستی بازیابی کنیم که این پیام در حقیقت، پیام پنهان (راز) در این بردار است؛ بنابراین دغدغه اصلی طراحی یک سیستم نهان‌نگار غیر قابل‌تشخیص این است که تعداد تغییرات پیام تعبیه‌شده d(x,emb(x, m)) زمانی که d به‌قدری 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 استخراج‌شده از پیکسل‌های شیء پوششی موردنظر باشد، فرض کنید $M \in F_2^m$ پیام موردنظر برای تعبیه در آن عبارت باشد ($m \leq n$). ارسال‌کننده و دریافت‌کننده از پیش‌بر روی ماتریس $H \in F_2^{m*n_2}$ از درجه (رتبه) m و متناسب با کد C=[n,k,d] ، توافق می‌کنند. برای اجرای تعبیه پیام پنهان، فرستنده عبارت ذیل (emb) را محاسبه نموده و شماره یک بیت از رشته n بیتی رسانه که باید تغییر نماید را به‌عنوان خروجی به دست می‌آورد (همان A). سپس با تغییر یک بیت از رشته بیت رسانه، X' را برای گیرنده ارسال می‌نماید. دریافت‌کننده، پیام پنهان m را با استفاده از رابطه rec از پوشانه اصلی که تنها یک بیت از n بیت آن تغییر نموده است، استخراج می‌نماید.

$$\text{emb: } (X, M) \to (H.X^t) \text{ xor } M^t = A, (X, A) \to X'$$
$$\text{rec: } H.X'^t = M^t \to M \qquad (۲)$$

با این روش ساخت نهان‌نگاری‌های مبتنی بر کد امکان‌پذیر 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 cov(ρ,N,n) استفاده نمود [۵] که در آن جاسازی n بیت در N بیت با حداکثر تغییرات ρ بیت صورت می‌گیرد. بهتر است برای کارایی بالا از کدهایی استفاده نماییم که در آن کران ρ حداقل باشد.

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

$$\text{Emb: } H=\begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix} \rightarrow \begin{bmatrix}1110100\\1101010\\1011001\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix} \text{ xor } \begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\end{bmatrix} \rightarrow X'=1110010$$

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

دقت داشته باشید که این روش تنها برای کدهای خطی یا کد همینگ صادق نیست و فرستنده و گیرنده می‌توانند بر روی کد دیگری به توافق رسیده و فرایند نهان‌نگاری را اجرا نمایند. 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 ۳ بیتی (M=100) در ۶ 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.

$$\text{Emb: } H=\begin{bmatrix}001000\\000110\\010101\end{bmatrix} \rightarrow \begin{bmatrix}001000\\000110\\010101\end{bmatrix}.\begin{bmatrix}1\\1\\1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\end{bmatrix} \oplus \begin{bmatrix}1\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\end{bmatrix} \rightarrow X'=1110001$$

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

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 می‌شود. درنتیجه گرچه مراحل بالا در مرحله تئوری بر روی تمام کدها با شرایطی نظیر داشتن رمزگشایی کارآمد ازلحاظ محاسباتی قابل کاربرد هستند، زیرا تنها اندکی از کدها به‌صورت عملی قابل‌استفاده‌اند. اصلی‌ترین نقش را در بین تمام آن‌ها، کدهای همینگ به دلایلی چون رمزگشایی ساده و نیز کارآمدی بالای آن‌ها، وظیفه تعبیه سازی (جاسازی) طرح نهان‌نگاری بر عهده‌دارند.

در مواردی که ملزم به پیروی از یک الگوی متنی خاص برای مخفی کردن اطلاعات هستیم می‌توان از کدهای تصحیحی خطای خطی به‌منظور بازیابی درست پیام استفاده کرد. با استفاده از این کدها می‌توان بیت‌های خطا را در یک پیام تشخیص و آن را تغییر داد. در مواردی که کدهای تصحیح خطا در مورد داده‌های پوشانه استفاده می‌شوند نیز می‌توان

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 ازجمله کدهایی است که در این رابطه استفاده می‌شود. کد تصحیح خطای گردشی به‌منظور تصحیح خطاهای دسته‌ای که در فایل‌های دیجیتالی معمول‌تر است، مناسب‌تر 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 به‌کارگیری این روش‌ها در مورد پیام‌های طولانی مناسب نیست. روش ساده‌تر استفاده از پریتی در تشخیص خطا می‌باشد. اگرچه پریتی تنها ۱ بیت اضافه به هر بایت پیام اضافه می‌کند ولی درصورتی‌که تنها ۱ بیت خطا رخ داده باشد می‌تواند در تشخیص آن مفید واقع شود.

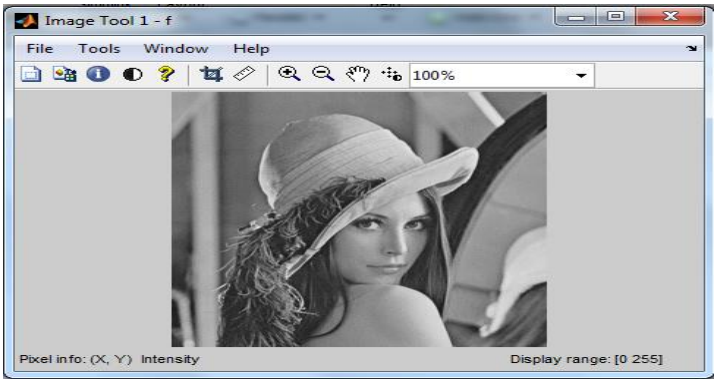
۴,۲. کاربرد کد بهینه

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 درنتیجه اطلاعات زیادی را می‌توان در آن تعبیه کرد.

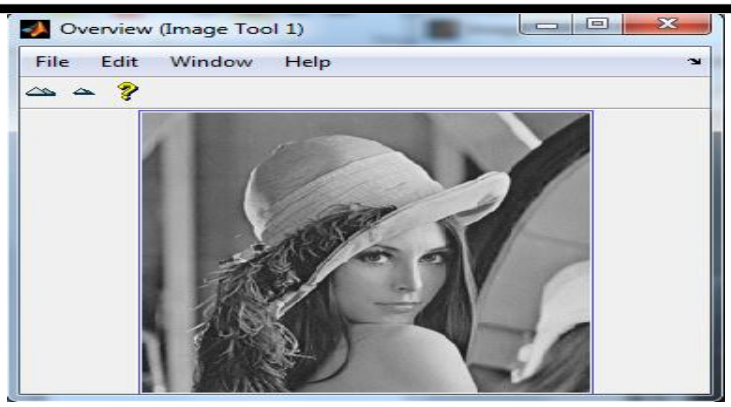
مورد دیگری که کدها می‌توانند در آن استفاده شوند سناریوهای غیر خصمانه. هستند که درآن امنیت مسئله اصلی نیست. در اینجا هدف اصلی ارتباطات غیرقابل ردیابی به هدف ارتباطات غیر ناراحت‌کننده تقلیل داده‌اند و درنتیجه دگرگونی‌های بیشتری را می‌توان در اشیا تحت پوشش ایجاد کرد به‌خصوص اگر شیء تحت پوشش را در شرایط اختلالی به‌صورت نیمه بهینه در دریافت‌کننده بتوان تغییر داد مانند گوش دادن به یک فایل موسیقی در ماشین. برای مثال، فرد ممکن است از موج‌های رادیو به‌عنوان 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 به‌عنوان 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. به‌عبارت‌دیگر می‌توان معادل ۳۷,۵٪ حجم کل رسانه اولیه بدون تغییر سایز آن، اطلاعات داخل رسانه جاسازی نمود. در همین راستا و با اجرا روش نهان‌نگاری پیشنهادی بر روی نقاط لبه‌ای رسانه اصلی، نتیجه‌ای طبق شکل شماره ۷ و جدول ۳ حاصل می‌گردد.



شکل ۶- تصویر اولیه رسانه بدون جاسازی

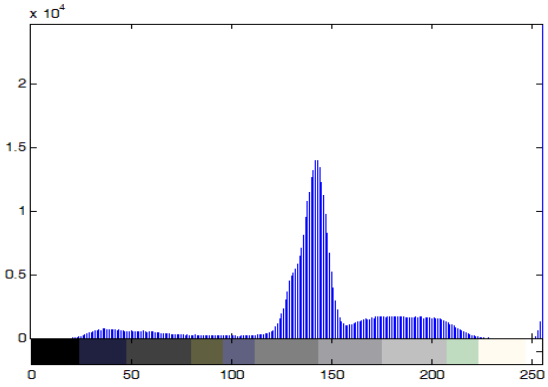


شکل ۷- اجرای روش پیشنهادی بر روی لبه‌های کنی

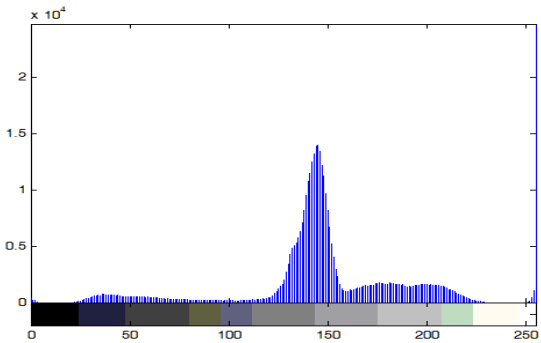
جدول ۳- شبیه‌سازی روش پیشنهادی در نقاط لبه‌ای پوشانه

ظرفیت جاسازی	PSNR	SSIM	مقاومت
3bit*تعداد لبه‌ها(۱۳۰ کیلوبایت)	۶۸,۰۸	۰,۹۶۹	٪۷۵

لازم به ذکر می‌باشد که با این روش، در هر نقطه لبه‌ای با عمق ۸ بیتی تصویر خاکستری می‌توان ۳ بیت اطلاعات جاسازی نمود، به‌طوری‌که تغییرات تصویر رسانه خیلی اندک باشد. این امر را با مقایسه نمودار هیستوگرام تصویر رسانه اصلی (شکل ۶) و تصویر نهان‌نگاری شده با روش پیشنهادی، طبق شکل‌های ذیل می‌توان به‌وضوح مشاهده نمود.



شکل ۸- نمودار هیستوگرام رسانه اصلی



شکل۹- نمودار هیستوگرام رسانه نهان‌نگاری شده

همان‌طوری که مشاهده می‌نمایید، نتیجه این روش نهان‌نگاری 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 نهان‌نگاری تصاویر دیجیتال موردمطالعه، بررسی و مقایسه قرار گرفت. نتیجه‌ی به‌دست‌آمده این است که تکنیک‌های نهان‌نگاری در حوزه‌ی مکان، دارای مزیت سادگی و سرعت هستند. این تکنیک‌ها پیچیدگی محاسباتی کمتری نسبت به تکنیک‌های حوزه‌ی فرکانس داشته و میزان اطلاعاتی که با استفاده از آن‌ها در تصویر درج می‌گردد نسبتاً زیاد و انحرافاتی که درنتیجه‌ی 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 نهان‌نگاری را در اختیار کاربران غیرمجاز قرار می‌دهند. از این‌رو بیشتر در سیستم‌های نهان‌نگاری شکننده به کار می‌روند. ازآنجاکه نهان‌نگاری در حوزه‌ی فرکانس بسیار قدرتمندتر از حوزه‌ی مکان است، درنتیجه تکنیک‌های حوزه‌ی فرکانس به‌طور گسترده‌تر اعمال می شوند. اگرچه این تکنیک‌ها به الگوریتم‌های پیچیده و هزینه‌ی محاسباتی بیشتری نسبت به حوزه‌ی مکان نیاز دارند، اما در مقایسه با تکنیک‌های حوزه‌ی مکان، تکنیک‌های حوزه‌ی فرکانس در دست یافتن به الگوریتم‌های نهان‌نگاری تصاویر دیجیتال ازلحاظ غیرقابل مشاهده بودن و نیازمندی‌های استحکام بهتر می‌باشند و در برابر حملات مقاومت زیادی از خود نشان می دهند.

با توجه به مطالب بیان‌شده 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 به‌سوی حوزه تبدیل‌شده که شاهد گسترش و رونق روزافزون آن هستیم.

حال می‌توان روش نهان‌نگاری 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 پنهان نگاری"* 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 نهان‌نگاری ویدئو با در نظر گرفتن برخی از مؤلفه‌های نهان‌کاوی "*، 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, “Disaapearing 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.