دانشکده برق و کامپیوتر

پایان‌نامه کارشناسی ارشد برق-گرایش مخابرات

پنهان‌نگاری تصاویر باینری

نگارش:

مرضیه امینی

استاد راهنما:

آقای دکتر خشایار یغمایی

دی ۱۳۸۹


بسم الله الرحمن الرحيم

دانشکده برق و کامپیوتر

پایان‌نامه کارشناسی ارشد برق-گرایش مخابرات

پنهان‌نگاری تصاویر باینری

نگارش:

مرضیه امینی

استاد راهنما:

آقای دکتر خشایار یغمایی

دی ۱۳۸۹

اینجانب **مرضیه امینی** متعهد می شوم که محتوای علمی این نوشتار با عنوان **"پنهان‌نگاری تصاویر باینری"** که به عنوان پایان نامه **کارشناسی ارشد** رشته **برق** گرایش مخابرات به گروه مهندسی –الکترونیک و مخابرات دانشکده مهندسی برق و کامپیوتر دانشگاه سمنان ارائه شده ، دارای اصالت پژوهشی بوده و حاصل فعالیت های علمی اینجانب می باشد .

در صورتی که خلاف ادعای فوق در هر زمانی محرز شود ، کلیه حقوق معنوی متعلق به این پایان نامه از اینجانب سلب شده و موارد قانونی مترتب به آن نیز از طرف مراجع ذیربط قابل پیگیری است .

نام و نام خانوادگی : مرضیه امینی

شماره دانشجویی : ۸۶۲۱۱۰۹۰۰۳

امضاء

تقدیم به

پدر و مادر عزیزم.

سپاس‌گزاری

از استاد عزیزم جناب آقای دکتر خشایار یغمایی که در مدت زمان انجام پایان‌نامه با راهنمایی‌های خود مرا همراهی کردند, کمال تشکر و قدردانی را دارم. از خداوند بزرگ برای ایشان آرزوی توفیق روز افزون در تمام مراحل زندگی را خواستارم.

چکیده

در جوامع امروزی، مقادیر زیادی از تصاویر باینری از قبیل تصاویر اسناد، نقشه‌های مهندسی و راه‌ها، تصاویر چاپ شده رد و بدل می‌شوند. با رشد اینترنت مشکلاتی از قبیل نقض حق نشر، کپی‌برداری، توزیع غیرقانونی و ایجاد هرگونه تغییر بدون اجازه صاحبان آثار در حوزه رسانه‌های دیجیتال و تبادل اطلاعات در اینترنت بوجود آمده است. لذا واترمارکینگ تصاویر باینری اهمیت ویژه‌ای پیدا کرده است. روش‌های واترمارکینگ سطوح خاکستری و تصاویر رنگی مستقیما قابل استفاده برای واترمارکینگ تصاویر باینری نمی‌باشند. در تصاویر باینری نمی‌توان با تغییرات کوچکی در مقادیر پیکسل، واترمارکینگ بر روی آن انجام داد. زیرا تصاویر باینری فقط دارای دو مقدار مشخص "۰" و "۱" می‌باشند. از طرف دیگر به طور مستقیم نمی‌توان از تکنیک‌های حوزه‌ی فرکانس استفاده کرد، زیرا در این روش‌های، واترمارک با تغییر کوچکی در ضرایب فرکانسی منتخب پنهان شده و سپس تصویر به حوزه مکان برگردانده می‌شود. برای باینری باقی ماندن ، از پردازنده‌های باینری‌کننده استفاده کرد که موجب یک سری اعوجاجات مرئی شده و همچنین بازیابی واترمارک را مشکل می‌سازد. هدف اصلی در این پایان‌نامه، مطالعه روش‌های بکار رفته در واترمارکینگ تصاویر باینری و ارائه روش‌های جدید برای واترمارکینگ اینگونه تصاویر می‌باشد.

واترمارکینگ تصاویر باینری را می‌توان به دو دسته تقسیم کرد که در دسته اول، تصویر واترمارک باینری فرض شده و تصویر میزبان با سطوح خاکستری و در دسته دوم تصویر میزبان باینری و تصویر واترمارک نیز باینری در نظر گرفته می‌شود.روش‌های پیشنهاد شده برای دسته اول از تکنیک‌های ترکیبی DWT-SVD و DWT-PCA استفاده شده است. مزایای تبدیل موجک از جمله مزیت سازگاری آن با خواص بینایی انسان مدنظر قرار گرفته شده است. لذا کیفیت تصویر واترمارک شده بالا بوده و تغییرات ایجاد شده در تصویر با چشم انسان قابل تشخیص نمی‌باشد. همچنین از خصوصیت‌های تبدیل SVD و PCA نیز برای افزایش مقاومت روش واترمارکینگ استفاده شده است. در روش ارائه شده برای دسته دوم، با توجه به آنکه تصویر میزبان نیز باینری می‌باشد عملیات باینری سازی باید بعد از مرحله جاسازی واترمارک انجام می‌گیرد. با توجه به اعوجاج ایجاد شده در مرحله باینری‌سازی، در گیرنده ازتکنیک آشکارساز پاسخ همبستگی برای بازیابی واترمارک استفاده شده است. نتایج شبیه‌سازی مقاومت بالای روش را در برابر حملات معمول پردازش تصویر نشان می‌دهد.

کلید واژگان: واترمارکینگ، تصاویر باینری، تبدیل موجک، تبدیل SVD و تبدیل PCA .

فهرست مطالب

فصل اول

مقدمه

۱-۱- مقدمه‌ای بر اصول نهان‌نگاری

مزایای داده‌های دیجیتال نسبت به داده‌های آنالوگ، استفاده روز افزون از متون، تصاویر، اصوات و ویدیوهای دیجیتال را سبب شده است. از جمله این مزایا سهولت ذخیره‌سازی داده‌های دیجیتال، جستجو و بازیابی آسان آن‌ها، کپی کردن ارزان، دوام زیاد، کاربرد آسان و سهولت ایجاد تغییرات بر روی داده‌های دیجیتال بوده که موجب شده است داده‌های آنالوگ به سرعت جایگاه خود را به داده‌های دیجیتال بدهند. همزمان با گسترش استفاده از داده‌های دیجیتال، استفاده از اینترنت نیز به صورت امری ضروری درآمده است و اینترنت به عنوان شبکه‌ای فراگیر محیط مناسبی را برای به اشتراک گذاردن و تبادل اطلاعات فراهم آورده است.

با توسعه فناوری اطلاعات و بوجود آمدن شبکه‌های گسترده دیجیتال مانند شبکه اینترنت، مشکلات جدیدی از قبیل کپی‌برداری غیر مجاز و ادعای مالکیت جعلی سندهای دیجیتالی بوجود آمده است. این مساله بدین دلیل است که متن دیجیتالی با سرعت و بدون افت کیفیت می‌تواند کپی برداری شده و یا تغییر داده شود. بنابراین باید بدنبال راه‌هایی برای مقابله با این مشکلات بود که از جمله این راه‌ها می‌توان به نهان‌نگاری دیجیتال اشاره کرد.

نهان‌نگاری یک حالت خاص از پنهان‌سازی داده است. ایده اصلی نهان‌نگاری، گنجاندن یک قطعه داده در داخل سند دیجیتالی به نام حامل[۱]، کاور[۲] یا میزبان[۳] می‌باشد تا از این داده بتوان در صورت نیاز برای مقاصد خاصی مانند ادعای مالکیت استفاده نمود. به این داده اصطلاحا نهان نگاره[۴] یا پیام[۵] گفته می‌شود. حامل می‌تواند تصویر، فیلم، موسیقی، نوشته و یا حتی یک صفحه وب باشد.

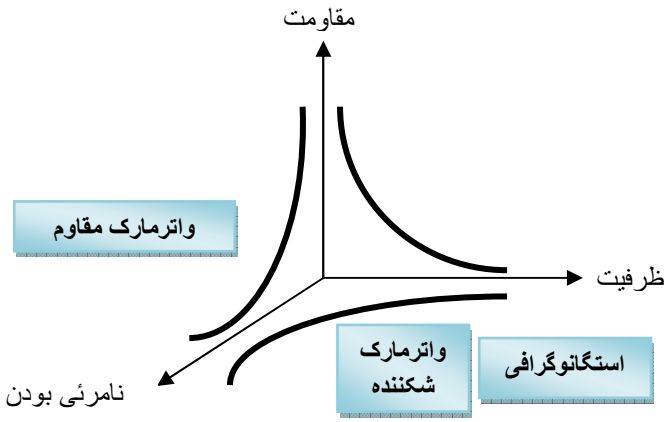
نهان‌نگاری برای اهدافی مانند حفاظت در مقابل کپی غیرمجاز، احراز هویت، کنترل دسترسی و تعیین دست نخوردگی داده‌های دیجیتال بوجود آمد و به سرعت مورد توجه قرار گرفت.

تعبیه‌ی داده در داخل حامل می‌تواند به دو شکل صورت گیرد: مرئی[۶] و نامرئی[۷]. نمونه‌ی خوبی از نوع تعبیه مرئی، قرار دادن لوگوی[۸] کوچکی در یکی از گوشه‌های تصویر است. از آنجا که این نوع تعبیه

---

۱ Carrier
۲ Cover
۳ host
۴ Watermark
۵ Message
۶ Visible
۷ Invisible
۸ logo

کیفیت تصویر را مخدوش می‌کند و از امنیت کافی برخوردار نمی‌باشد، نوع نامرئی تعبیه معرفی گردید. در این نوع، از ظرفیت تغییر در تصویر که از چشم انسان دور می‌ماند برای تعبیه‌ی نهان‌نگاره استفاده می‌شود. در نهان‌نگاری هدف تبادل مخفی اطلاعات می‌باشد. اما واضح است که با گذاشتن قید نامرئی و نامحسوس بودن[۱] نمی‌توان مقاومت[۲] پروسه را از حد معینی بالاتر برد. از طرف دیگر برای اینکه داده‌ی پنهان بتواند در مواجهه با تغییرات عمدی و غیرعمدی‌ای از بین نرود، باید تا حد ممکن مقاومت بالایی داشته و ظرفیت[۳] حمل اطلاعات آن تا حد ممکن بالا باشد. بنابراین به صورت همزمان، نیاز به سه ویژگی مقاومت در برابر حملات، نامرئی بودن و ظرفیت کافی داریم. این سه مولفه همواره با یکدیگر در تضاد هستند، بطوری که افزایش بیش از اندازه هر یک به کاهش دیگری می‌انجامد. بنابراین یک مصالحه بین این کمیت‌ها برقرار است که در شکل (۱-۱) نشان داده است. در مبحث پنهان‌سازی داده، اغلب به دنبال آن هستیم که تصویر نهان‌نگاری شده از تصویر اصلی قابل تفکیک نباشد. این ویژگی در نهان‌نگاری تصویر تحت عنوان نامرئی بودن شناخته می‌شود.



شکل(۱-۱) : ظرفیت، نامرئی بودن و مقاومت در نهان‌نگاری همواره با یکدیگر در مصالحه هستند و با توجه به ناحیه بکارگیری، سه خانواده مهم نهان‌نگاری بدست می‌آید.

ظرفیت، به مقدار اطلاعاتی که می‌توان در تصویر با یک الگوریتم خاص تعبیه نمود گفته می‌شود. مقاومت، عبارت است از مقاومت روش تعبیه نمودن نهان‌نگاره در برابر تغییرات عمدی وغیرعمدی‌ای که ممکن است باعث حذف و یا تضعیف شدید نهان‌نگاره شوند. بنابراین می‌توان نهان‌نگاری نوین را به صورت نوعی

[۱] Invisibility(transparency)
[۲] Robustness
[۳] Capacity

رمزنگاری الکترونیک تعریف کرد که در آن اطلاعات، در حامل به صورتی مخفی می‌شود که تنها توسط گیرنده مجاز ،کاربری که الگوریتم و رمز به کارگرفته شده را می‌داند، قابل بازیابی باشد. البته با این تعریف ممکن است که نهان‌نگاری با رمزنگاری[١] اشتباه گرفته شود و این در صورتی است که این دو تفاوت‌های اساسی دارند. یک تفاوت عمده این است که در نهان‌نگاری موضوع محرمانه بودن پیام و اطلاعات مخفی شده، مطرح نیست. در رمزنگاری اطلاعات ارسالی را با یک الگوریتم خاص و یک کلید رمز به گونه‌ای تغییر می‌دهند که توسط گیرنده غیر مجاز قابل فهم نباشد ولی این به معنای مخفی بودن اطلاعات ارسالی نیست; بلکه هر فردی می‌تواند اصطلاحا کانال را استراق سمع و پیغام را رمزگشایی کند. ولی در نهان‌نگاری، اطلاعات به صورتی مخفی شده است که قابل تشخیص نباشد و فرد غیر مجاز برای بدست آوردن پیام باید محیط انتقال، حامل و الگوریتم نهان‌نگاری را شناسایی کرده و در صورت امکان پیام را بیرون بکشد. بنابراین نهان نگاری به نوعی امنیت بیشتری نسبت به رمزنگاری دارد. البته معمولا از ترکیب هر دو تکنیک استفاده می‌شود; یعنی پیام ابتدا رمز و سپس مخفی می‌شود، بدین ترتیب یک لایه امنیتی دیگر به روش‌های متداول رمزنگاری اضافه می‌شود.

١-٢- اصول پنهان‌نگاری تصاویر باینری[٢]

در جوامع امروزی، روزانه حجم زیادی از اسناد در حوزه‌های مختلف رد و بدل می‌شوند. از آنجائیکه اسناد می‌توانند به راحتی اسکن شده و طی مراحلی کیفیت از دست رفته آن‌ها بدون تلف بازیابی شود; لذا تشخیص مالکیت اسناد از نگرانی‌های اصلی می‌باشد.

روش‌های پنهان‌سازی داده برای تصاویر با سطوح خاکستری[٣] و رنگی پیشرفت‌های زیادی داشته است. در این روش‌ها یک تغییر کوچکی در رنگ یا مقدار شدت روشنایی در مجموعه‌ای از پیکسل‌ها ایجاد می‌شود و از لحاظ بینایی اعوجاج قابل ملاحظه‌ای ایجاد نمی‌کند.

تصاویر باینری نوع خاصی از تصاویر سطوح خاکستری هستند. هر پیکسل از تصویر باینری فقط دو مقدار "٠" یا "١" به معنای سیاه یا سفید را می‌تواند داشته باشد. تصاویر باینری می‌توانند از اسکن دو رنگی اسناد مانند مدارک قانونی، شناسنامه، کتاب‌های دیجیتالی، نقشه‌های مهندسی و ... بدست آیند. اسناد اولین و اصلی‌ترین روش ارتباطات در دنیای امروز بوده و حجم بسیار زیادی از آن‌ها روزانه رد و بدل می-

[١] Cryptography
[٢] Binary
[٣] grayscale Image

شود; لذا نه تنها باید امنیت گیرنده مورد بررسی قرار گیرد، بلکه هویت مالک سند نیز باید نشان داده شود. برای اثبات مالکیت یک سند، می‌توان از واترمارکینگ دیجیتال استفاده کرد.

تکنیک‌های واترمارکینگ تصاویر با سطوح خاکستری و تصاویر رنگی مستقیما برای تصاویر باینری قابل استفاده نمی‌باشند. از آنجائی که تصاویر باینری تنها دو مقدار مشخص "۰" و "۱" دارند، نمی‌توان هیچ مقداری در روشنایی پیکسل آن‌ها پنهان نمود. همچنین نمی‌توان از روش‌های حوزه فرکانس مستقیما استفاده کرد. زیرا در روش‌های حوزه فرکانس، واترمارک بطور نامرئی با تغییر کوچکی در ضرایب فرکانسی منتخب پنهان شده و سپس تصویر به حوزه مکان برگردانده می‌شود. در این مرحله برای آنکه تصویر همچنان باینری باشد، باید از پردازنده‌های باینری‌کننده استفاده کرد و چنین عملیات باینری‌سازی موجب یک سری اعوجاجات مرئی می‌شود و همچنین بازیابی واترمارک را مشکل می‌سازد.

تصاویر باینری به دو دسته نیم‌تن[۱] و اسناد[۲] دسته‌بندی می‌شوند. این دسته‌بندی براساس خصوصیت توزیع پیکسل‌های تصویر که به نحوه ایجاد آن بستگی دارد، انجام شده است. تصاویر نیم‌تن برای ساده-سازی پردازش‌ها و یا در چاپگرها استفاده می‌شود. نمونه‌هایی از تصاویر نیم‌تن، کتاب‌ها، مجلات، روزنامه-ها و خروجی چاپگرها می‌باشند. تصاویر اسناد، نمایش اسکن شده دو رنگی از آن‌ها است مانند اسناد رسمی، شناسنامه، کتاب‌های دیجیتال، نقشه‌های مهندسی و نقشه راه‌ها.

تکنیک‌های واترمارکینگ برای تصاویر باینری، از نوع تصاویر اسناد محدودیت‌های خاص خود را دارند. برای مثال، برای تغییر در تصاویر اسناد باینری نمی‌توان بصورت تصادفی یک سری پیکسل را تغییر داد. زیرا تغییر تنها یک پیکسل سفید به سیاه در یک قسمت تمام سفید، اعوجاج قابل مشاهده‌ای را ایجاد می‌کند.

از آنجایی‌که تکنیک‌های واترمارکینگ مورد استفاده برای سطوح خاکستری و تصاویر رنگی، قابل استفاده برای تصاویر باینری نیستند، تصاویر باینری ، نیازمند تکنیک‌های جاسازی واترمارک متفاوت می‌باشند.

در ادامه، بخش‌های مختلف این پایان نامه بصورت زیر تنظیم شده‌اند :

فصل دوم، مبانی واترمارکینگ تصاویر مطرح شده و در ادامه روش‌هایی از واترمارکینگ تصاویرکه در راستای این پایان‌نامه می‌باشد ، مورد بررسی قرار می‌گیرند.

---

[۱] Half-tone
[۲] Document

فصل سوم، اصول واترمارکینگ تصاویر باینری مطرح شده است. در ابتدای این فصل با تقسیم‌بندی انواع تصاویر باینری، محدویت‌های واترمارکینگ این تصاویر مطرح شده است و سپس روش‌های معمول واترمارکینگ این تصاویر مورد بررسی قرار گرفته است.

فصل چهارم، الگوریتم‌های پنهان‌سازی و آشکارسازی سه روش‌های پیشنهادی در این پایان‌نامه مطرح شده است .

فصل پنجم، شامل نتایج حاصل از شبیه سازی روشهای پیشنهادی می‌باشد. اثرات حملات مختلف بر روی عملیات واترمارکینگ مورد بررسی قرار گرفته و مقاومت روشها ارزیابی شده است.

در فصل ششم، نتیجه گیری و کارهای آینده آورده شده است.

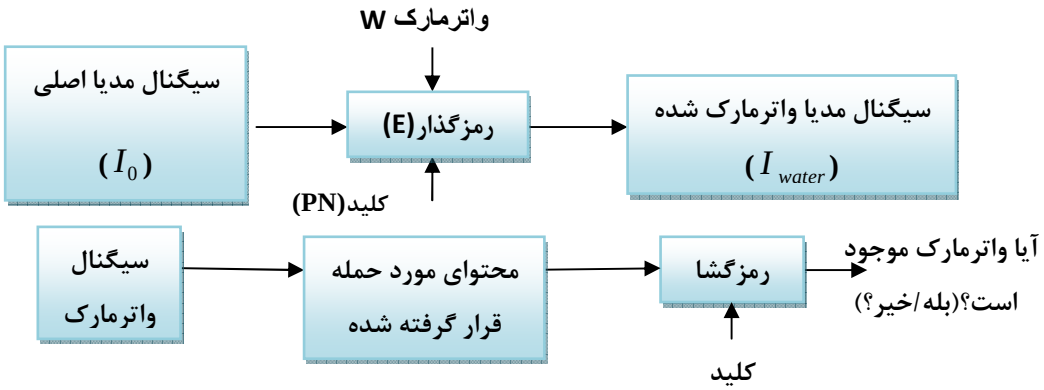
فصل دوم

واترمارکینگ تصویر

۲-۱- اصول روش‌های نهان‌نگاری

روش‌های نهان‌نگاری به دسته‌های اصلی استگانوگرافی[۱] ، نهان‌نگاری شکننده[۲] ، واترمارکینگ[۳] تقسیم می-شوند که مبنای همه آن‌ها یکی است. در شکل (۲-۱) چارچوب کاری یک سیستم نهان‌نگاری نشـان داده شده است. داده پنهان با یک کلید خصوصی تولید و مدوله می‌شود و سپس درون تصویر با یک الگـوریتم خاص تعبیه می‌گردد. در گیرنده، تصویر دریافتی به همراه اطلاعات جانبی که شامل کلید، وضعیت تغییـر و اطلاعات خود تصویر است جهت وجود نهان نگاره بررسی می‌شوند. در صورت وجود، متن داده پنهان نیز آشکارسازی می‌گردد.

در استگانوگرافی هدف تعبیه حجم زیادی از اطلاعات بصورت نامرئی است و در ازای آن مقاومت بـالا مـد نظر نیست. این روش می‌تواند برای انتقال اطلاعات سری از کانال‌های مرسوم مانند وب استفاده شـود. در نهان نگاری شکننده، هدف تعبیه داده‌ای در تصویر است که در گیرنده تغییر و چگونگی انجام تغییـر روی تصویر را آشکار نماید. در این نوع پنهان سازی داده، نامرئی بودن و حـد معقـولی از ظرفیـت فاکتورهـای تعیین‌کننده هستند.



شکل(۲-۱): چارچوب کلی برای نهان‌نگاری الف) مراحل تعبیه نهان‌نگاره ب)مراحل آشکارسازی نهان‌نگاره

[۱] steganography
[۲] یا Tamper proofing
[۳] Watermarking

در نهان‌نگاری شکننده، یک نهان‌نگاره با روش خاصی در تصویر گنجانده می‌شود که در اثر تغییر و یا دستکاری تصویر از بین می‌رود. به عبارت دیگر به محض ایجاد کوچکترین تحریفی در تصویر، نهان‌نگاره از بین می‌رود که نشان‌دهنده عدم اصل بودن اطلاعات می‌باشد.

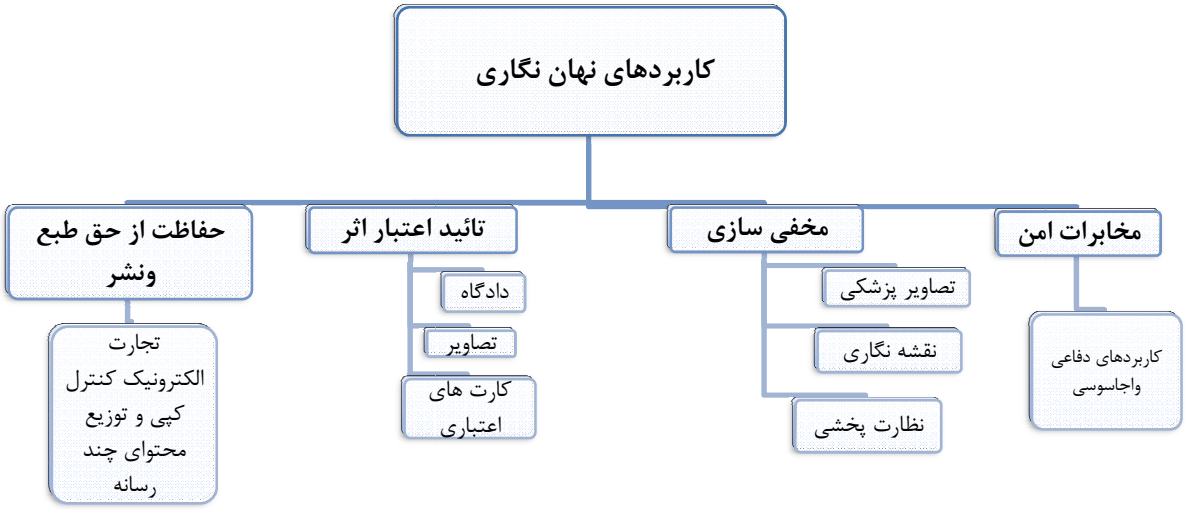
این نوع بررسی دست‌نخوردگی تصویر، در هنگام استناد به یک تصویر مثلا در دادگاه یا پزشک قانونی مورد استفاده قرار می‌گیرد. این نوع نهان‌نگاری نمی‌تواند به منظور حفاظت از حق طبع و نشر مورد استفاده قرار گیرد; زیرا ویژگی مقاومت در آن عمدا ضعیف شده است. یکی از انواع این کاربرد با استفاده از امضای دیجیتال است. همانگونه که می‌دانیم امضای دیجیتال بشکل سیستماتیک می‌تواند برای تعیین دست‌نخوردگی هر داده‌ای مورد استفاده قرار گیرد. در این روش تصویر، بعد از توابع "درهم ریز[۱]" محاسبه و سپس رمز شده و به ضمیمه تصویر ارسال می‌گردد. گیرنده با امتحان امضا و اطمینان از صحت آن می‌تواند آن را تائید کند.

الگوریتم‌های نهان‌نگاری بسته به اینکه در هنگام آشکارسازی نیاز به تصویر اصلی داشته و یا نداشته باشند باشد، به دو دسته غیرکور[۲] و کور[۳] تقسیم می‌شوند. فرض در اختیار داشتن تصویر اصلی در گیرنده، پیچیدگی فرستنده و گیرنده را کاهش می‌دهد و امکان طراحی الگوریتم مقاوم‌تری را بوجود می‌آورد. با این حال بسیاری از الگوریتم‌های نهان‌نگاری بر این اساسند که تصویر اصلی در هنگام آشکار سازی در دسترس نباشد.

۲-۲- حوزه‌های کاربرد نهان‌نگاری

در [۱] به طور خلاصه چند حوزه کاربرد برای استگانوگرافی و واترمارکینگ پیشنهاد شده، که در شکل(۲-۲) به طور خلاصه نشان داده شده است.

[۱] Scrambler
[۲] Non-blind
[۳] blind



شکل(۲-۲) : دسته‌بندی کلی حوزه‌های کاربرد نهان‌نگاری.

در زیر به مهمترین کاربردهای نهان‌نگاری بدون توجه به کاربرد اشاره شده است.

۲-۲-۱-تبادل مخفی داده‌ها در یک کانال عمومی[۱]

در اینجا تبادل مخفی داده‌ها در یک کانال عمومی که مستقیما با تعریف استگانوگرافی در ارتباط است بررسی می‌شود. مخفی کردن اطلاعات مهم در اسناد دیجیتال مانند تصویر، موسیقی و یا ویدیو و ارسال آن‌ها از طریق اینترنت به مراتب ارزان‌تر و راحت‌تر از استفاده از یک کانال اختصاصی امن با رمز نگاری پیچیده است.

۲-۲-۲- حفاظت از حق طبع و نشر[۲]

سادگی فوق‌العاده کپی‌کردن و استفاده غیرمجاز از اسناد دیجیتال، لزوم استفاده از واترمارکینگ را به عنوان برچسب نام دارنده سند آشکار می‌سازد. در واقع با کمک واترمارک می‌توان از کپی غیرقانونی سند

[۱] Covert communication
[۲] Copyright Protection