



دانشگاه فنی و حرفه ای

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پنهان نگاری اطلاعات

فرنوش معنوی

شماره دانشجویی

بهار --



دانشگاه فنی و حرفه ای

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پنهان نگاری اطلاعات

فرنوش معنوی

شماره دانشجویی

— بهار —

بسم الله الرحمن الرحيم

ملتی که از علم و دانش بهره‌مند باشند، دیگر طعم گرسنگی را نچشیده و زندگی راحت و آسوده ای خواهند داشت.

"کنفوسیوس"

فهرست مطالب

فصل اول : مقدمه

- ۱-۱ مقدمه ۲
- ۱-۲ هدف ۲
- ۱-۳ تعریف مسئله ۲
- ۱-۴ ساختار مطالب ارائه شده ۳

فصل دوم : آشنایی با پنهان نگاری اطلاعات

- ۲-۱ مقدمه ۵
- ۲-۲ تاریخچه ۵
- ۲-۳ معرفی پنهان نگاری ۶
 - ۲-۳-۱ تفاوت پنهان نگاری و رمزنگاری ۶
 - ۲-۳-۲ الگوریتم‌ها و روش‌های پنهان نگاری ۶
 - ۲-۳-۳ انواع مختلف پنهان نگاری اطلاعات ۸
 - ۲-۳-۴ کاربردهای پنهان نگاری اطلاعات ۹
 - ۲-۴ نتیجه گیری ۱۰

فصل سوم : پنهان نگاری در تصاویر

- ۳-۱ مقدمه ۱۲
- ۳-۲ معرفی پنهان نگاری در تصاویر ۱۲
- ۳-۳ مثال‌ها و ابزارهای لازم ۱۲
- ۳-۴ نتیجه گیری ۱۵

فصل چهارم : پنهان نگاری در فایل های صوتی و تصویری

- ۴-۱ مقدمه ۱۷
- ۴-۲ معرفی پنهان نگاری در صوت ۱۷

۴-۳ معرفی پنهان نگاری در تصاویر صوتی ۱۹

۴-۴ نتیجه گیری ۲۰

فصل پنجم : پنهان نگاری در اسناد و متون

۵-۱ مقدمه ۲۲

۵-۲ معرفی پنهان نگاری در اسناد و متون ۲۲

۵-۳ نتیجه گیری ۲۳

فصل ششم : نتیجه گیری

۶-۱ دستاوردهای ارائه ۲۵

۶-۲ دستاوردهای آینده ۲۵

منابع و مراجع ۲۶

فهرست اشکال

- شکل ۱-۲ تصویر حامل اولیه ۷
- شکل ۲-۲ تصویر حامل ثانویه ۷
- شکل ۳-۲ نمایی از نرم افزار هگز ایدیتور ۸
- شکل ۱-۳ مثال پنهان نگاری در عکس ۱۳
- شکل ۲-۳ مثال پنهان نگاری در عکس ۱۴
- شکل ۱-۴ امواج صوت ۱۸
- شکل ۲-۴ نمایی از محیط ویرایشگر ویوپد ۱۹

چکیده

از زمانی که انسان‌ها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط مخفیانه یک خواسته مهم بین افراد بوده است. گسترش روز افزون اینترنت و رشد سریع استفاده از آن، انسان‌ها را به سوی جهان دیجیتال و ارتباط از طریق داده‌های رقمی¹ سوق داده است. در این میان امنیت ارتباطات² یک نیاز مهم است و هر روز نیاز به آن بیشتر احساس می‌شود. به طور کلی دو شیوه ارتباط پنهانی وجود دارد، در روش اول که رمزنگاری³ نام دارد، اطلاعات به طریقی رمز می‌شوند که برای شخص ثالث قابل فهم نیست اما گیرنده و فرستنده با استفاده از کلید مشترک می‌توانند اطلاعات مورد نظر را رمزگشایی کنند.

پنهان نگاری⁴ شیوع دوم ارتباط محرمانه است، در پنهان نگاری علاوه بر مخفی ماندن اطلاعات، وجود ارتباط محرمانه مخفی می‌ماند. در واقع پنهان نگاری اطلاعات هنر و علم پنهان کردن ارتباطات است و هدف آن مخفی کردن وجود هرگونه ارتباط بین فرستنده و گیرنده است. اغلب اوقات تصور می‌شود که با رمزگذاری پیام مورد مبادله ارتباط امن است اما در عمل، بعضی اوقات تنها رمز کردن کافی نیست و به همین دلیل روش‌هایی برای پنهان کردن داده به جای کد کردن آن ارائه شده است، مانند پنهان کردن داده در تصاویر یا در فایل‌های صوتی و تصویری که در این ارائه به بیان جزئیات آنها خواهیم پرداخت.

واژه های کلیدی: پنهان نگاری، پنهان کردن اطلاعات، رمزنگاری، فایل حامل، تصویر، تصاویر ویدئویی، صوت، اسناد

¹ Digital data

² Communications Security

³ Cryptography

⁴ Steganography

فصل اول

مقدمه

۱-۱ مقدمه

برای حفاظت از محصولات دیجیتال چند رسانه‌ای در برابر کپی‌های غیرمجاز^۱ و حفظ حق انتشار^۲ برای داده‌های صوتی، تصویری و ویدئویی از دوتکنیک رمز نگاری و پنهان نگاری 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 رمز گشایی می‌شوند از این پس دیگر هیچگونه حفاظتی از داده صورت نمی‌گیرد، ولی در تکنیک‌های پنهان نگاری، یک سیگنال پنهانی نام واترمارک^۳، مستقیماً در داخل داده حک می‌شود و همواره در آن باقی می‌ماند. برای استفاده از داده پنهان نگاری شده، نیازی به برداشتن سیگنال واترمارک نیست زیرا این سیگنال طوری در داده میزبان درج می‌شود که هیچ تأثیر نامطلوبی بر داده اصلی نمی‌گذارد. به عنوان مثال در پنهان نگاری داده در تصویر، چشم انسان نباید تفاوت بین تصویر اصلی و تصویر واترمارک شده را حس کند. در صورت هر گونه استفاده غیر مجاز از تصویر واترمارک شده، مانند کپی غیر مجاز از آن و یا هرگونه تحریف و تغییر تصویر توسط افراد غیر مجاز، صاحب اصلی داده می‌تواند با استخراج سیگنال واترمارک، که تنها توسط او امکان پذیر است، مالکیت خود را به اثبات برساند و یا محل تغییرات صورت گرفته بر روی تصویر را مشخص کند.

۱-۲ هدف

پنهان نگاری اطلاعات موضوعی است که به ندرت از طریق هواخواهان امنیتی فن آوری اطلاعات در دهه گذشته مورد توجه قرار گرفته است. اغلب مردم از موضوع پنهان نگاری اطلاعات بی‌خبرند و حتی نمی‌دانند پنهان نگاری اطلاعات چیست و در بیشتر مواقع با رمزنگاری اطلاعات^۴ آن را اشتباه می‌گیرند. هدف از این ارائه معرفی دقیق این علم (پنهان نگاری اطلاعات)^۵ و فواید استفاده از آن و کاربردهایش است.

۱-۳ تعریف مسئله

با توجه به گسترش فناوری در دنیای امروز و امکان انجام اکثر عملیات از راه دور با استفاده از شبکه‌های جهانی و محلی، همچنین عدم لزوم تمرکز همه داده‌ها در یک محل و نیاز به دستیابی به برخی از اطلاعات از راه دور و هم چنین حفظ امنیت اطلاعات در زمان ارسال و دریافت، اهمیت مسئله نگهداری اطلاعات از دسترسی های غیر مجاز را بیش از پیش آشکار می‌سازد، لذا به دنبال روش‌های پنهان کردن اطلاعات و بازیابی آنها خواهیم بود.

¹ Copy protection

² copyright protection

³ watermark

⁴ embedding

⁵ information hiding

⁶ cryptography

⁷ steganography

۱-۴ ساختار مطالب ارائه شده

در این ارائه در فصل دوم به معرفی پنهان نگاری اطلاعات و تاریخچه‌ی این علم خواهیم پرداخت و روش‌ها و الگوریتم‌های عمده‌ی این حوزه را بیان می‌کنیم، در فصل بعد به بررسی پنهان نگاری اطلاعات در تصاویر می‌پردازیم. سپس در فصل چهارم پنهان نگاری در فایل‌های صوتی و تصویری را بیان خواهیم کرد و در نهایت در فصل پنجم پنهان نگاری در اسناد و متون را شرح خواهیم داد.

فصل دوم

آشنایی با پنهان نگاری

اطلاعات

۲-۱ مقدمه

در این فصل به معرفی علم پنهان نگاری اطلاعات و تاریخچه‌ی آن خواهیم پرداخت و مثالهایی از مردمان گذشته را بیان خواهیم کرد که چگونه از این علم استفاده می‌کردند. سپس به تعریف دقیق این علم و انواع پنهان نگاری‌ها و فواید استفاده از آن خواهیم پرداخت و در این میان دو روش عمده که اساس کار پنهان نگاری اطلاعات است را شرح خواهیم داد.

۲-۲ تاریخچه

استفاده از پنهان سازی اطلاعات در گذشته دارای سابقه‌ای طولانی است و تاریخچه پنهان نگاری به ۵ قرن قبل از میلاد مسیح و به کشور یونان برمی‌گردد. در آن زمان مردی به نام هیستایاکاس می‌خواست پیغامی را به صورت محرمانه برای شخص دیگری بفرستد، وی برای فرستادن پیغام مورد استفاده از این روش استفاده کرد. او برده‌ای را برای این کار انتخاب کرد و موهای سر برده را تراشید و پیغام محرمانه را بر روی پوست سر برده خالکوبی کرد و سپس مدتی صبر کرد تا موهای فرد رشد کرده و به حالت اول برگردد و بعد او را به سمت مقصد (گیرنده) روانه کرد در مقصد، گیرنده‌ی پیغام دوباره موهای برده را تراشید و پیغام را بر روی پوست سر او مشاهده کرد [۲].

سربازان یونانی برای انتقال پیام بجای آنکه طبق روال عادی آن زمان، که روی موم کشیده شده بر لوح پیام نوشته می‌شد پیام را بنویسند، روی خود لوح می‌نوشتند و سپس روی آن را با موم می‌پوشاندند و اکنون از این لوح مثل یک لوح عادی استفاده می‌کردند و روی آن یک پیام عادی می‌نوشتند [۲].

اولین کتاب واقعی پنهان نگاری اطلاعات را گسپری اسکاتی^۱ در سال ۱۶۶۵ در ۴۰۰ صفحه با نام استگانوگرافیک^۲ نوشت که بیشتر مطالب این کتاب برگرفته از ایده‌های تریتمیوس^۳ بود. سپس پنهان نگاری در قرن‌های ۱۵ و ۱۶ توسعه یافت و نویسندگان بسیاری در این زمینه کتاب نوشتند اما برای اینکه از تفرقه بین احزاب و به وجود آمدن فرقه‌های مختلف جلوگیری کنند نام خود را در کتابهایشان پنهان می‌کردند [۲].

^۱ Gasperi Sehotti

^۲ Steganographica

^۳ Johannes Trithemius

۲-۳ معرفی پنهان نگاری

۲-۳-۱ تفاوت پنهان نگاری و رمزنگاری

پنهان نگاری ترجمه واژه استگانوگرافی است که از لغت یونانی استگانوس^۱ و گرافتوس^۲ گرفته شده است. در واقع استگانوگرافی دانشی است برای پنهان کردن داده یا فایلی در فایل دیگر، بطوری که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند. استفاده از این تکنیک در مواردی بسیار، عالی و کاربردی است. برخلاف رمزگذاری که فایل حفاظت شده را کاملاً حساس جلوه می‌دهد و جلب توجه می‌کند، این روش از ناآگاهی افراد، برای جلوگیری از دستیابی آن‌ها به اطلاعات خاص بهره می‌برد [۱].

تفاوت اصلی رمزنگاری و پنهان نگاری آن است که در رمز نگاری هدف اختفاء محتویات پیام است و نه به طور کلی وجود پیام، بلکه پیام دیده می‌شود ولی به وسیله الگوریتم‌هایی رمزگذاری شده است. اما در پنهان نگاری هدف مخفی کردن هر گونه نشانه‌ای از وجود پیام است. به عنوان مثال اگر شخصی به متن رمزنگاری شده‌ای دسترسی پیدا کند، به هر حال متوجه می‌شود که این متن حاوی پیام رمزی می‌باشد، اما در پنهان نگاری شخص سوم ابدأً از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند. در موارد حساس ابتدا متن را رمزنگاری کرده، آنگاه آن را در متن دیگری پنهان نگاری می‌کنند [۲].

۲-۳-۲ الگوریتم‌ها و روش‌های پنهان نگاری

در این جا ۲ روش معرفی می‌شود. ۱ - کمترین بیت با ارزش^۳ ۲- تزریق^۴

روش کمترین بیت با ارزش : معمولاً زمانی که فایل‌ها ایجاد می‌شوند، شامل بایت‌هایی هستند که واقعا به آنها نیازی نیست، یا حداقل مهم نیستند. این مناطق می‌توانند با اطلاعاتی که باید در فایل مخفی شود، بدون صدمه و تغییر در فایل، تعویض شوند. این امکان، به فرد اجازه می‌دهد که اطلاعات را در فایل مخفی کند و مطمئن باشد که هیچ کسی نمی‌تواند تغییرات اعمال شده در فایل را تشخیص دهد. این روش معمولاً باعث افزایش حجم فایل نمی‌شود، اما بسته به حجم اطلاعاتی که باید درون فایل مخفی شوند، فایل حامل به صورت قابل ملاحظه‌ای دارای افت و اعوجاج می‌شود، به همین خاطر اگر فایل حامل کیفیت مناسبی نداشته باشد بعد از اعمال این روش به طور قابل مشاهده‌ای در تصویر تغییر ایجاد می‌شود [۳].

به عنوان مثال به شکل ۲-۱ نگاه کنید بعد از تغییر چند بیت در آن به شکل ۲-۲ تبدیل شده که افت کیفیت شدیدی در آن قابل مشاهده است [۷].

^۱ پوشاندن
^۲ نوشتن

^۳ Least Significant Bits (LSB)

^۴ injection



شکل ۱-۲ تصویر حامل اولیه



شکل ۲-۲ تصویر حامل ثانویه

در تصاویری که کیفیت و تعداد رنگ استفاده شده بالایی دارند و در فایل‌های صوتی که صداها متفاوته درون خود دارند روش کمترین بیت ارزش بهترین عملکرد را دارد.

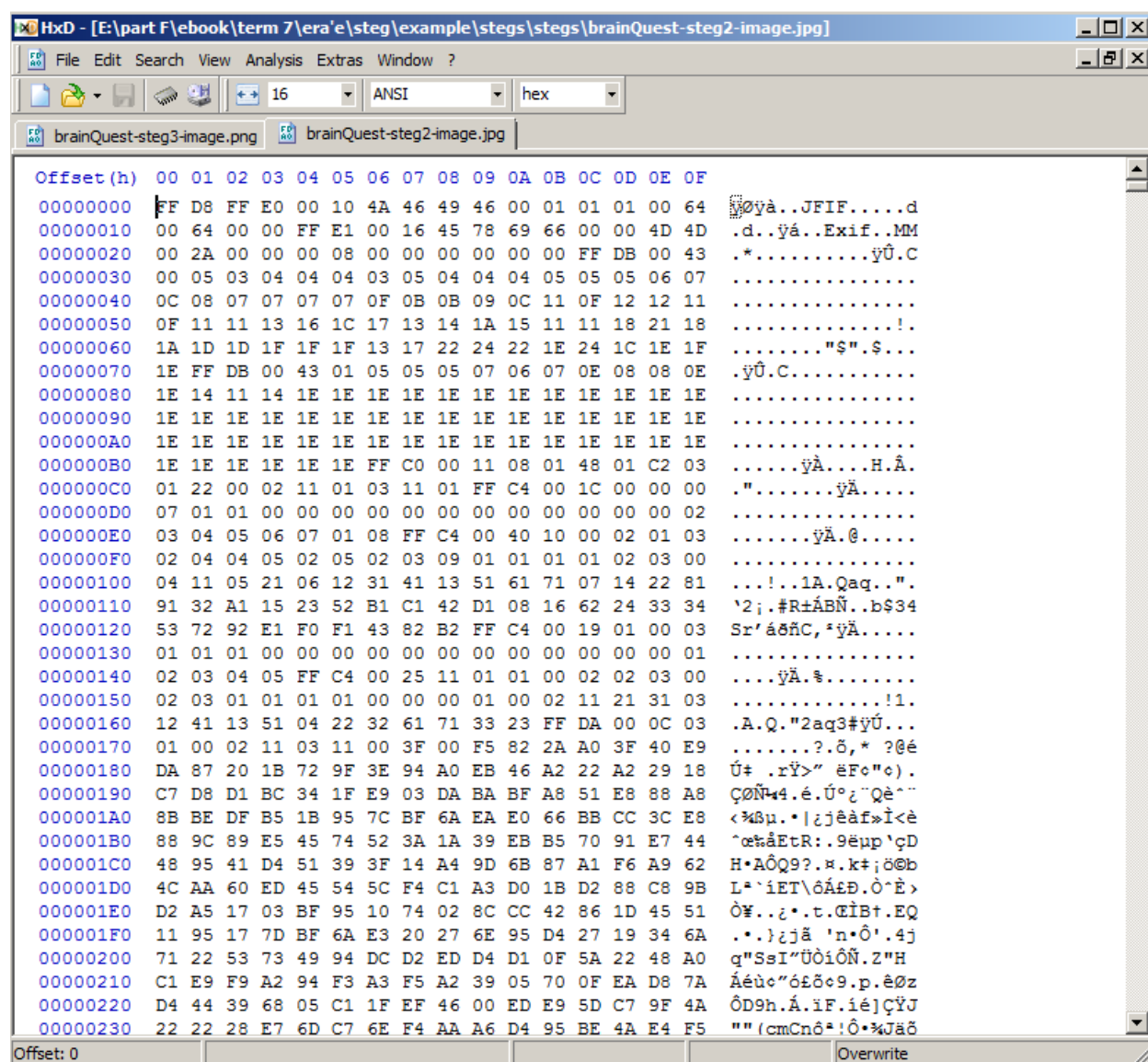
تزریق: تزریق روش ساده‌ای است که به صورت مستقیم، اطلاعات مخفی را در فایل حامل تزریق می‌کند. مشکل اصلی این روش این است که می‌تواند به میزان قابل ملاحظه‌ای باعث افزایش حجم فایل شود که همین مسئله می‌تواند مشکوک به نظر برسد و آشکار کننده‌ی مسئله برای فرد سوم باشد. در این روش ابتدا معادل باینری فایل حامل را به دست می‌آورند بعد به صورت مستقیم دیتای مورد نظر را به این معادل باینری اضافه می‌کنند [۳].

یکی از نرم افزارهایی که در این حوزه کمک می‌کند "هگز ادیتور"^۱ می باشد که این نرم افزار یک ویرایشگر هگزادسیمال برای ویرایش اطلاعات از فایل های باینری است. رابط کاربری این نرم افزار بسیار شبیه به یک نرم افزار ویرایشگر متن است که در آن قابلیت های پیشرفته تری لحاظ شده است. این نرم افزار به شما اجازه می‌دهد که یک فایل را باز کرده و داده های خام (هگزادسیمال) آن را مشاهده کرده و ویرایش نمایید. به راحتی می‌توانید یک رشته ی متنی یا مقدار هگز را تشخیص داده و آن را کپی یا درج نمایید و در کل می‌توانید محتوای فایل را ویرایش کنید. این نرم افزار به شما اجازه خواهد داد قسمت های مهمی از کد برنامه را به رنگ دلخواه دیگری تغییر دهید تا در یک نگاه برای شما قابل تشخیص باشد. کاربران می‌توانند داده های فایل های باینری خود را

¹ hex editor

² hexadecimal

توسط عملیات منطقی، ریاضی و یا اعمال توابع و عبارات شرطی، ویرایش نمایند. شکل ۲-۳ نمایی از این نرم افزار را نشان می‌دهد
[۳] [۸] (با [۳، ۸]).



شکل ۲-۳ نمایی از نرم افزار هگز ایدیتور

۲-۳-۳ انواع مختلف پنهان نگاری اطلاعات

به طور کلی می‌توان پنهان نگاری را در ۴ دسته تقسیم بندی کرد که شامل :

۱- **پنهان نگاری در تصاویر** : در این نوع پنهان نگاری اطلاعات در فایل حاملی که از نوع تصویر می باشد پنهان می شوند و معمولاً از روش کمترین بیت با ارزش استفاده می شود. در فصل سوم به این نوع پنهان نگاری به طور مفصل می پردازیم [۱] [۲].

۲- **پنهان نگاری در صوت** : در این نوع پنهان نگاری اطلاعات درون فایل حاملی که از نوع صوت می باشد، پنهان می شوند. در این نوع پنهان نگاری تکنیک استفاده شده معمولاً رمزگزاری سطح پایین بیتی است که چیزی شبیه به روش کمترین بیت با ارزش استفاده شده در تصاویر است. مشکل رمزگزاری سطح پایین بیتی در این است که معمولاً توسط حس شنوایی انسان به صورت مشخص، قابل تشخیص است. بنابراین برای کسانی است که می خواهند اطلاعات را در فایل صوتی مخفی کنند، یک روش ریسکی است [۳].

۳- **پنهان نگاری در تصاویر ویدئویی** : در این نوع پنهان نگاری اطلاعات درون فایل حاملی که از نوع ویدئو می باشد، پنهان می شوند. در این نوع پنهان نگاری معمولاً از روش فشرده سازی استفاده می کنند [۴] [۵].

۴- **پنهان نگاری در اسناد** : این نوع از پنهان نگاری بی نهایت مؤثر است، زیرا استفاده از فضای سفید همیشه از دید مردم، حداقل در بیشتر ویرایشگرهای متنی، نامرعی باقی می ماند و فضای سفید به طور طبیعی به واسطه تب^۲ یا فاصله^۳ در اسناد ایجاد می شود [۸].

۲-۳-۴ کاربردهای پنهان نگاری اطلاعات

پنهان نگاری در امور تجاری بسیار پرکاربرد است و در کشورهایی که متعهد به اجرای قانون حق تکثیر هستند خدمات خوبی برای صاحبان تولیدات الکترونیکی روی شبکه اینترنت ارائه نموده است. در کشور ما ایران در حال حاضر متاسفانه به دلیل عدم رعایت قانون ذکر شده شاید اهمیت کاربردی این علم زیاد مورد توجه نباشد لیکن با پیشرفت صنعت فناوری اطلاعات در آینده ای نه چندان دور توجه بیشتر به آن گریز ناپذیر خواهد بود. همچنین به لحاظ ارتباط این علم با مسائل امنیتی در برقراری ارتباطات پوشیده توجه ارگان ها و نهادهای ذیربط و ذینفع را می طلبد و غفلت از آن زیانهای جبران ناپذیری را متصور می سازد. متاسفانه در این میان گروه های خرابکار و گروه های تروریستی نیز که معمولاً از امکانات مالی خوبی برخوردار هستند از این فناوری چشم پوشی نمی کنند، لذا توجه به تحلیل پنهان نگاری بسیار ضروری است. [۸]

به طور کلی می توان کاربردهای پنهان نگاری را به صورت زیر خلاصه سازی کرد :

۱- اثبات حق مالکیت و یا حفظ حق نشر

۲- پنهان کردن داده های مختلف با امکان ردگیری

¹ DCT

² Tab

³ Enter

۳- کنترل عمل کپی برداری

۴- نظارت بر پخش تصدیق صحت داده و برچسب زدن به تصاویر

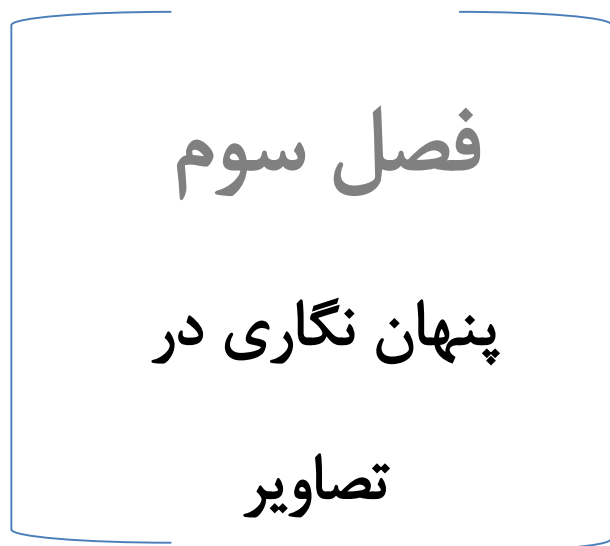
۵- ارتباطات مخفیانه و پنهان سازی داده

۲-۴ نتیجه گیری

پنهان نگاری اطلاعات روشی است که می توان به وسیله آن اطلاعات مورد نظر را در قالب یک عامل پوشاننده با بیشترین میزان دقت و با امنیت، بین نقاط موردنظر جابجا نمود، به گونه ای که حتی اگر در طی مسیر، اطلاعات از طریق افراد غیرمجاز شنود^۱ قرار گرفت امکان دستیابی به داده های پنهان شده وجود نداشته باشند. در واقع پنهان نگاری هنر و علم جاسازی اطلاعات در یک رسانه حامل است که با توجه به پیشرفت قابل توجه ارتباطات دیجیتال استفاده از آن رو به افزایش می باشد. در پنهان نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است.

باتوجه به اینکه امروزه روش های زیادی برای ارسال امن اطلاعات در بستر فضای مجازی وجود دارد استفاده از روش های پنهان نگاری می تواند کمک شایانی جهت ارسال و دریافت داده ها نمایند به طوری که فقط افراد فرستنده و گیرنده قابلیت استخراج اطلاعات را داشته باشند و از طرفی در زمینه کپی برداری های غیرمجاز به شناخت مجرمان کمک کند.

¹ sniff



فصل سوم

پنهان نگاری در

تصاویر

۳-۱ مقدمه

یکی از روش‌های پنهان نگاری که امروزه طرفداران خاص خود را پیدا کرده است پنهان نگاری در تصاویر می‌باشد. در این نوع پنهان نگاری اطلاعات در فایل حاملی که از نوع تصویر می‌باشد پنهان می‌شوند و معمولاً از روش کمترین بیت با ارزش که در فصل گذشته توضیح داده شد استفاده می‌شود و در این فصل با مثال‌ها متنوع این مسئله را بیان خواهیم کرد.

۳-۲ معرفی پنهان نگاری در تصاویر

از آن‌جا که تصاویر مهمترین رسانه مورد استفاده به خصوص در اینترنت هستند و درک تصویری انسان از تغییرات در تصاویر محدود است، تصاویر به عنوان یکی از بهترین رسانه‌های پوششی در پنهان نگاری معرفی شدند و بدین ترتیب الگوریتم‌های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر خام^۱ (۲۴ بیتی رنگی یا ۸ بیتی سیاه و سفید)، تصاویر پالت (۱۶ رنگ، ۲۵۶ رنگ، ...) تصاویر فشرده جی‌پگ^۲ و جی‌پگ ۲۰۰۰ و ... در حوزه مکانی^۳ و حوزه تبدیل^۴ ارائه شده است. استفاده از ساختار جی‌پگ برای انتقال تصویر به خصوص در محیط اینترنت بسیار مرسوم‌تر از بقیه ساختارها است. لذا روش‌های متعددی برای پنهان نگاری در تصاویر جی‌پگ معرفی شده است. در مورد تصاویر جیف^۵ بایست اشاره نمود که علی‌رغم کاربرد وسیع این تصاویر در سطح اینترنت و علاقه کاربران به استفاده از آن، استفاده از آن‌ها برای پنهان نگاری محدودیت‌هایی دارد. در حقیقت محدودیت تعداد رنگ‌های موجود در یک تصویر پالت (مانند جیف) و سایز کوچک این تصویر استفاده امن از الگوریتم‌های پنهان نگاری را دچار اشکال می‌کند.

برای استفاده بهتر از ظرفیت تصویر و بعلاوه دلایل امنیتی، اعمال دو ماژول فشرده سازی^۶ و رمزنگاری^۷ روی داده مورد نظر قبل از انجام تابع جاسازی و متعاقباً استفاده از الگوریتم‌های رمزگشایی^۸ و بازنگری^۹ روی پیام استخراج شده الزامی است [۳] [۷].

۳-۳ مثال‌ها و ابزارهای لازم

ذهن خلاق از مهم‌ترین ابزارهای کار پنهان نگاری در تمام شاخه‌های آن می‌باشد و همچنین در حوزه پنهان نگاری از علم رمز نگاری هم استفاده کثیری می‌شود در زیر مثالهایی بیان شده که بر این مطلب مهر تاییدی خواهد زد.

^۱ BMP

^۲ Joint Photographic Experts Group (JPEG)

^۳ Spatial

^۴ Transform

^۵ Graphics Interchange Format (GIF)

^۶ Compression

^۷ Encryption

^۸ Decryption

^۹ Decompression



شکل ۳-۲ مثال پنهان نگاری در عکس

در این جا از گیمپ که یک برنامه دستکاری (و روتوش) تصاویر گنو است استفاده می‌کنیم. برای این کار با استفاده از این ویرایگشر عکس مورد نظر را باز کرده و با استفاده از اختیارات این ویرایگشر تضاد در تصویر را دستکاری می‌کنیم و با این کار نوشته‌هایی در تصویر نمایان خواهند شد که نشان دهنده اطلاعات پنهان شده در تصویر هستند.

شکل ۳-۱ و شکل ۳-۲ تقریباً مثال‌های ساده از پنهان نگاری در تصاویر بودند اما همیشه به این راحتی و آسانی نیست گاهی اوقات باید ساعت‌ها و حتی روزها صرف تحلیل تصویر شود تا بتوان اطلاعات پنهان شده درون تصویر را به عنوان شخص ثالث از آن بیرون کشید، ولی نرم افزارهایی توسعه پیدا کرده اند که تحلیل را کمی راحت تر می‌کنند و این نرم افزارها به صورت رایگان و یا با پرداخت هزینه در ورژن‌های مختلف برای استفاده‌ی عموم در اینترنت قرار گرفته شده است، مانند هگز ایدیتور^۱ که در فصل قبل هم به معرفی آن پرداختیم [۳].

¹ contrast

² hex editor

۳-۴ نتیجه‌گیری

پنهان نگاری در تصاویر یکی از انواع پنهان نگاری است، که اطلاعات در قالب فایل حاملی که از نوع عکس می‌باشند پنهان می‌کند. این نوع پنهان نگاری از زمانی وارده عرصه میدان شد که کامپیوترهای قدرتمند وارد بازار شدند و نرم افزارای مربوط به این شاخه به صورت کاملاً رایگان در بستر اینترنت در اختیار کاربران گذاشته شد.

اساس پنهان نگاری در تصاویر ویدویی هم که در فصل بعدی به آن می‌پردازیم مانند پنهان نگاری در تصاویر می‌باشد.

فصل چهارم

پنهان نگاری در

فایل‌های صوتی و

تصویری

۴-۱ مقدمه

از آنجا که محدوده سیستم شنوایی انسان محدود است امکان جاسازی اطلاعات در صوت نیز وجود دارد. سیستم شنوایی انسان می‌تواند قدرتی بین یک تا یک میلیون و فرکانسی بیشتر از یک تا یک هزار را درک کند، همچنین نسبت به پارازیت‌هایی که اضافه می‌شود حساس است. هرگونه مزاحمتی در یک فایل صوتی قابل درک است، حتی اگر به کوچکی یک قسمت از ده میلیون باشد. به هر حال با اینکه سیستم شنوایی انسان حساسیت زیادی دارد ولی در برابر بعضی تغییرات حساسیت خود را از دست می‌دهد، مثلاً صداهای بلند و یا صداهای آرام را در خود جای می‌دهد. با تکیه بر همین ضعف علم پنهان نگاری اطلاعات در صوت به وجود آمده است.

۴-۲ معرفی پنهان نگاری در صوت

در هنگام پنهان نگاری در صوت دو نکته مهم را بایستی مورد توجه قرار داد.

- باید از ضعف سیستم شنوایی انسان سو استفاده کرد.
- توجه خاصی به حساسیت فوق العاده سیستم شنوایی انسان داشت.

در این نوع پنهان نگاری اطلاعات درون فایل صوتی پنهان می‌شوند. در زمان مخفی سازی اطلاعات درون یک فایل صوتی، تکنیک استفاده شده معمولاً رمزگذاری سطح پایین بیتی است که چیزی شبیه به روش کمترین بیت با ارزش استفاده شده در تصاویر است. مشکل رمزگذاری سطح پایین بیتی در این است که معمولاً توسط حس شنوایی مردم به صورت مشخص، قابل تشخیص است. بنابراین برای کسانی است که می‌خواهند اطلاعات را در فایل صوتی مخفی کنند، یک روش ریسکی است [۴] [۶].

انتشار طیف روش دیگری برای مخفی سازی اطلاعات در فایل صوتی است، این روش با اضافه کردن صداهای تصادفی به سیگنال، اطلاعات را در فایل حامل مخفی کرده و طیفی را در طول فرکانس منتشر می‌کند. به عنوان مثال به شکل ۴-۱ دقت کنید ۳ فرکانس را مشاهده خواهید کرد که ۲ فرکانس مربوط به صوت اصلی و فرکانس قهوه ای رنگ حامل اطلاعات پنهان شده است که در مجاورت ۲ فرکانس اصلی قرار گرفته بدون اینکه مشکلی برای صوت ایجاد کند.

اگر فایل صوتی به فرمت ام‌پی۳^۱ باشد معمولاً نرم افزار "ام پی ۳ استگو"^۲ می‌تواند به اطلاعات پنهان شده در آن اشاره کند.

یکی دیگر از نرم افزارهایی که در این حوزه کمک می‌کند "ویرایشگر صدای ویوپد"^۳ است. این نرم افزار ویرایشگر صوتی کامل با امکانات حرفه ای می‌باشد که شما با استفاده از این نرم افزار قادر خواهید بود تا هرگونه فایل صوتی را ویرایش کرده و یا بواسطه آن اقدام به ضبط صدا کنید و ویرایش های لازم را بر روی آن اعمال کنید. شما براحتمی می‌توانید هرگونه فایل صوتی را در برنامه بارگذاری کنید و سپس با کمک ابزارهایی که برنامه در اختیار شما قرار می‌دهد اقدام به ویرایش آنها کنید. بطور مثال می‌توانید

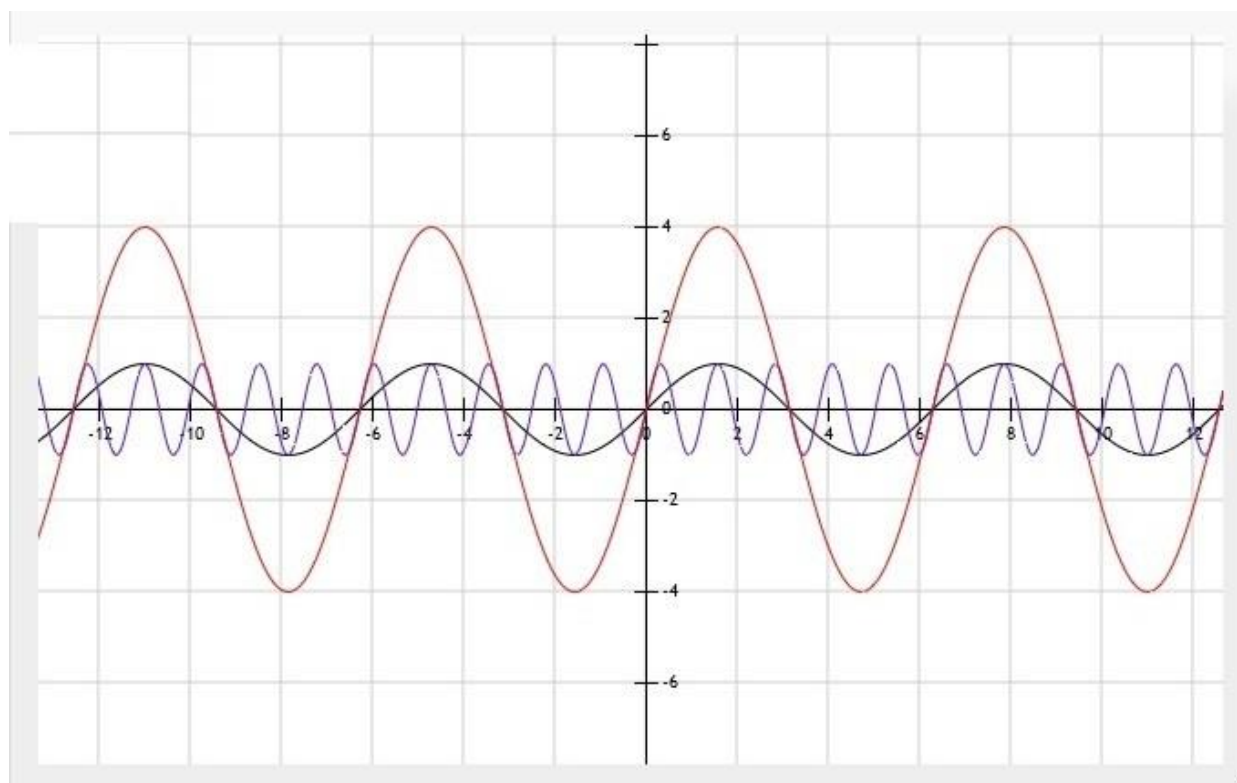
¹ MP3

² MP3Stego

³ WavePad Sound Editor

قسمتی از فایل‌های صوتی را برش داده، چندین فایل صوتی را به یکدیگر متصل کنید و اثرهای مختلفی مانند پژواک^۲، تقویت و کاهش صدا، حذف نویزهای موجود در صدا، حذف صداهای ناخواسته را بر روی آنها اعمال کنید. این نرم افزار قابلیت پشتیبانی و ویرایش اکثر فرمت های صوتی مانند ام پی ۳، ویو^۳، ای ام آر^۴ را دارا می باشد و شما می توانید بصورت دسته ای اقدام به ویرایش فایلها کنید و سپس آنها را با بالا کیفیت ذخیره کنید [۶].

شکل ۴-۲ نمایی از محیط کار این نرم افزار می باشد.



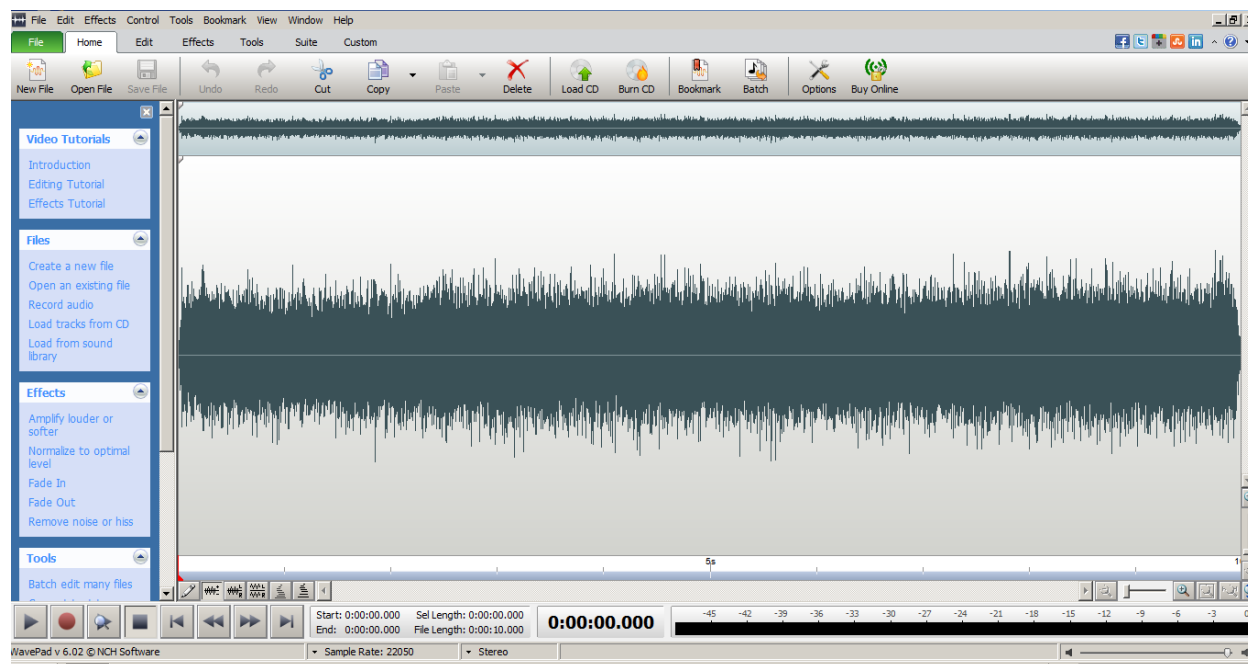
شکل ۴-۱ امواج صوت

¹ effect

² echo

³ WAV

⁴ AMR



شکل ۴-۲ نمایی از محیط ویرایشگر ویوید

۴-۳ معرفی پنهان نگاری در تصاویر صوتی

این نوع پنهان نگاری تقریباً ترکیبی از پنهان نگاری در صوت و تصاویر است که در فصل قبل به آن پرداخته شد. در مخفی سازی اطلاعات درون فایل ویدیویی، فرد یا شخصی که اطلاعات را مخفی میکند، معمولاً از روش از روش فشرده سازی^۱ استفاده میکند.

روش فشرده سازی به صورت اعمال کمی تغییرات در هر تصویر از ویدیو، فقط به اندازه‌ای که از دید مردم محسوس نباشد، عمل می‌کند مثلاً از گرد کردن استفاده می‌کند و ۲,۷۷۷۷ را به ۳ گرد می‌کند. پنهان نگاری در ویدئو همانند پنهان نگاری در تصاویر است، چون فریم‌های ویدئو تشکیل شده از تصاویر هستند و این روش هم، همان تصاویر را تغییر می‌دهد. معمولاً زمانی که تنها اطلاعات کمی در فایل ویدیویی مخفی می‌شوند قابل تشخیص نیستند، به هر حال هر چقدر اطلاعات بیشتری مخفی شوند، قابل تشخیص تر خواهند شد. [۱] [۴].

معمولاً با استفاده از نرم افزار "ام‌اس‌یو استگو ویدئو"^۲ می‌توان به اطلاعات پنهان شده در تصاویر ویدیویی پی برد [۳].

^۱ DCT

^۲ MSU StegoVideo

۴-۴ نتیجه گیری

پنهان نگاری در فایل‌های صوتی از ضعف شنوایی انسان استفاده می‌نماید. سامانه شنوایی قادر به کشف تغییراتی که در بردارهای شدت در فرکانس‌های بالاتر از طیف شنیداری انجام می‌شود، نیست. در این نوع پنهان نگاری با توجه به زوج یا فرد بودن مقدار دامنه اولیه نهان نگاری با معرفی یک پژواک کوتاه به سیگنال صوتی انجام شده و داده در آن پنهان می‌شود. پس از اضافه کردن پژواک، سیگنال پژواک، تمامی ویژگی‌های اصلی را حفظ می‌کند. مهم‌ترین خصوصیت روش پیشنهادی مقاومت در برابر نویز، فشرده‌سازی و امنیت است.

فصل پنجم

پنهان نگاری در

اسناد و متون

۵-۱ مقدمه

یکی از مشکلاتی که برای نویسندگان وجود دارد توزیع غیرقانونی نوشته‌هایشان است. بدین معنی که بدون پرداخت هزینه به نویسنده، نوشته وی را به دیگران می‌دهند. لذا برای مقابله با آن روش‌هایی ابداع شده است. مانند، ساختن کلمه‌ای که از نظر خواننده دیده نمی‌شود ولی مشخصه‌ی متن است یا کد کردن کلمه یا تغییر آن به روشی که قابل کپی برداری با دستگاه‌های فتوکپی نباشد.

۵-۲ معرفی پنهان نگاری در اسناد و متون

یکی دیگر از انواع پنهان نگاری‌ها، پنهان نگاری در اسناد و متون می‌باشد که امروزه با توجه به حق نا دیده گرفتن نویسنده اهمیت بسیاری پیدا کرده است. این نوع از پنهان نگاری بی نهایت مؤثر است، زیرا استفاده از فضای سفید همیشه از دید مردم، حداقل در بیشتر ویرایشگرهای متنی، نامرعی باقی می‌ماند و فضای سفید به طور طبیعی به واسطه تب^۱ یا فاصله^۲ در اسناد ایجاد می‌شود [۲].

در این نوع پنهان نگاری از روشی جدید در زبان فارسی به منظور وارد کردن اطلاعات اضافی معمولاً در متن استفاده می‌کنند که بر مبنای استفاده از دیکشنری کلمات و عبارات کاملاً مترادف است. مثلاً کلمه‌ی "شاد" به جای "خوشحال" می‌تواند استفاده شود. روش عمومی بر اساس قرار دادن اطلاعات اضافی از طریق تغییر ظاهری المان‌های متن نظیر فاصله خطوط یا شکل کلمات و حروف می‌باشد، که با روش جدید تمایز دارد.

در روش جدید، متن اولیه با استفاده از دیکشنری کلمات و عبارات معادل جهت تعیین کلمات یا عبارات دارای مترادف‌های کاملاً هم معنی پردازش می‌شود و سپس نرم افزار نهان نگاری از طریق تعیین کلمه مترادف که باید در متن قرار گیرد، اطلاعات اضافی مورد نظر را در متن جا سازی می‌نماید. در انتخاب کلمات و عبارات مترادف برای جاسازی اطلاعات اضافی از یک مولد اعداد تصادفی بر مبنای کلید رمز استفاده می‌گردد تا به سطح امنیت مطلوب در نهان نگاری اطلاعات دست یابند. ظرفیت جاسازی اطلاعات در روش ارایه شده برای نهان نگاری متن که با استفاده از تکنیک‌های آماری محاسبه شده است، نشان دهنده آن است که این روش از کارایی بالایی در جاگذاری اطلاعات در متن برخوردار می‌باشد [۲].

^۱ Tab

^۲ Enter

۳-۵ نتیجه گیری

امروزه به دلیل رعایت نکردن حق کپی رایت در آثار نوشتاری مانند کتاب‌ها یا اثبات حق مالکیت در اسناد این نوع پنهان نگاری از ارزش بالایی برخوردار شده است. همچنین چون فضای سفید متون در ویرایشگرها هم نادیده گرفته می‌شود ارزش این نوع پنهان نگاری را چند برابر خواهد کرد.

فصل ششم

نتیجه گیری

۶-۱ دستاوردهای ارائه

با توجه به گسترش فناوری در دنیای امروز و امکان انجام اکثر عملیات از راه دور، با استفاده از شبکه‌های جهانی و محلی، همچنین عدم لزوم تمرکز همه داده‌ها در یک محل و نیاز به دستیابی به برخی از اطلاعات راه دور و هم چنین حفظ امنیت اطلاعات در زمان ارسال و دریافت، اهمیت مسئله نگهداری اطلاعات از دسترسی های غیر مجاز را بیش از پیش آشکار می سازد. در این ارائه به تفاوت میان رمزنگاری اطلاعات و پنهان نگاری اطلاعات پرداخته شد و انواع روش‌های پنهان نگاری اطلاعات شرح داده شد و همچنین بیان شد که باید با توجه به داده‌ی مورد نظر جهت پنهان کردن، حجم و اهمیت آن از یکی از روش های پنهان نگاری در تصاویر، صوت، تصاویر ویدیوی، اسناد و متون استفاده کرد.

لذا می‌توان نتیجه گرفت که پنهان نگاری اطلاعات همان راه حلی است که می‌تواند امنیت را در جابه جایی داده‌ها تضمین کند.

۶-۲ دستاوردهای آینده

مسلماً در آینده استفاده بسیار متنوعی را می‌توان از این تکنولوژی انتظار داشت مثلاً ایده کدهای سریع پاسخ^۱ یا شابک^۲ که مدتهاست از آن استفاده می‌شود نشأت گرفته از این علم می‌باشد. در باب کاربردهای متنوع این کدها سخن بسیار است اما بهتر است بر روی جنبه های جدیدتر و عمومی تری تمرکز کرد تا بتوان این تکنولوژی را بهتر و بیشتر گسترش داد، مثلاً الگوریتم‌های جدیدتر جهت پنهان سازی اطلاعات و تکنیک‌های متنوعی جهت فشردن سازی داده و تزریق آنها به فایل حامل.

^۱ QR codes(Quick Response codes)

^۲ ISBN

منابع و مراجع فارسی

- ۱- ف. ادیسی ، ل. احسان ، " نهان نگاری دیجیتال تصویر به روش پایان نامه کارشناسی ارشد مخابرات گرایش سیستم ، طیف گسترده در حوزه DCT " ، دانشکده صداوسیما ، تابستان ۱۳۸۱

منابع و مراجع لاتین

- 2- Bender, W., et al. "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, Nos. 3&4, 1996: 313-336.
- 3- Fridrich, Jessica, et.al. "Detecting LSB Steganography in Color and Grayscale Images", Magazine of IEEE Multimedia Special Issue on Security, Nov. 2001: 22-28.
- 4- G.C.Langelaar , I. Setyawan and R. L. Lagendijk , " Watermarking Digital Image and Video Data " in IEEE Signal Processing Magazine , Sept. 2000 , pp.1053-1058.
- 5- J.K. O Ruanaidh , T.Pun, " Rotation , Scale and Translation Invariant Spread Spectrum Digital Image Watermarking" , IEEE Signal Processing , vol. 66 , No.3 , may 1998 , pp. 303-317.
- 6- M. D. Swanson , M. Kobayashi and A. H. Tewfik , " Multimedia Data -Embedding and Watermarking Technologies " , Proceedings of the IEEE , Vol. 86 , No. 6, June 1998 , pp. 1064-1087 .
- 7- Johnson, Neil F. and Jajodia, Sushil. "Steganalysis of Images Created Using Current Steganography Software", Lecture Notes in Computer Science, Vol .1525, Springer-Verlag, 1998.
- 8- Fabien A. P. Petitcolas, Ross J. Anderson and Markus G.Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, vol. 87, no.7, pp.1062-1078, 1999.