
بسم الله الرحمن الرحیم

دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

افزایش بازدهی جاسازی پنهان نگاری در رسانه‌های صوتی

پایان نامه‌ی کارشناسی ارشد مهندسی برق- مخابرات سیستم

حسن شفیعی‌علویجه

استاد راهنما

دکتر مسعود عمومی

۱۳۹۱

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه‌ی کارشناسی ارشد رشته مهندسی برق- مخابرات گرایش سیستم آقای حسن شفیعی‌علویجه

تحت عنوان

افزایش بازدهی جاسازی پنهان نگاری در رسانه‌های صوتی

در تاریخ۱۳۹۱/۱۱/۵ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان نامه	دکتر مسعود عمومی
۲- استاد مشاور پایان نامه	دکتر سیّد محمّدعلی خسروی‌فرد
۳- استاد داور	دکتر شادرخ سماوی
۴- استاد داور	دکتر مهدی برنجکوب
سرپرست تحصیلات تکمیلی	دکتر مسعود عمومی

تشکر و قدردانی

حمد و سپاس فراوان به درگاه خداوندی برم که دگر بار الطاف بیکران خود را شامل این حقیر نمود تا با استعانت از بارگاه احدیتش گامی دیگر در جهت کسب دانش بردارم و دری بر نادانسته‌های خود بگشایم و امید که در آینده نیز مشمول عنایات خاصه‌اش قرار گیرم.

بر دستان پدر و مادری که بذر عشق به آموختن را در وجودم نهادند بوسه می‌زنم و آن دو را که تجلی مهر و لطف خداوندی بر من هستند عاشقانه می‌ستایم. با تمام وجود از مقام شامخ اساتید راهنما و مشاور آقایان دکتر مسعود عمومی و دکتر سیّدمحمّدعلی خسروی‌فرد که در نهایت لطف و بزرگواری تمامی سعی و تلاش خود را در جهت اعتلای واقعی ارزش‌های آموزشی در کالبد هدایت‌ها و رهنمودها نسبت به اینجانب مبذول فرموده‌اند، کمال قدردانی را می‌نمایم. از آقایان دکتر شادرخ سماوی و دکتر مهدی برنجکوب که زحمت داوری این پایان‌نامه را پذیرفتند کمال تشکر و قدردانی را دارم.

از آقایان هوشنگ میره‌کی، سیّدعباس رحیمی، رضا قادرمزی، حامد بیکی، ابوالفضل ابراهیمی‌سرست، سیّدمجتبی رضویان و امین احمدزاده که در سال‌های تحصیل در دانشگاه و همچنین در مراحل مختلف این پژوهش یاری‌گر اینجانب بودند، سپاس‌گزاری نموده و پیروزی ایشان را در تمامی مراحل زندگی آرزومندم. یاد و خاطره تمامی دوستان عزیزم در دوره کارشناسی و کارشناسی ارشد که ذکر نام یکایک ایشان در این مجال نمی‌گنجد را گرامی داشته و برای تمامی آن‌ها سعادت، سلامت و پیروزی را آرزو دارم.

و در پایان شایسته است که بگویم:

رنگین کمان پاداش کسانی است که تا آخرین لحظه زیر باران می‌مانند.

حسن شفیعی‌علویجه

زمستان ۹۱

تقدیم به

پدر و مادرم که صبر و مهرشان پیمودن راه را برایم آسان می‌نماید،

و

برادرانم که امید بخش راهم می‌باشند.

تقدیم به

همه‌ی کسانی که لحظه‌ای بعد انسانی و وجدانی خود را فراموش نمی‌کنند

و بر آستان گران‌سنگ انسانیت سر فرود می‌آورند

و انسان را با همه‌ی تفاوت‌هایش ارج می‌نهند.

فهرست مطالب

عنوان **صفحه**

فصل سوم: ساختار سیستم شنوایی انسان و روش‌های پنهان‌نگاری صوتی

فصل چهارم:روش پیشنهادی پربازده در پنهان‌نگاری صوتی

چکیده

رمزنگاری از دیرباز به عنوان وسیله‌ای برای حفاظت از اطلاعات محرمانه توسط اشخاص مختلف و برای جلوگیری از دسترسی‌های غیرمجاز مورد استفاده قرار گرفته است. امّا در بعضی مواقع علاوه بر مخفی ماندن اطلاعات محرمانه، کشف نشدن وجود ارتباط میان دو گروه توسط سایرین نیز حائز اهمیت می‌باشد. دانشی که به پنهان کردن یک پیام در یک رسانه‌ی پوششی (مانند صوت، تصویر و ویدئو) می‌پردازد، پنهان‌نگاری نام دارد. پنهان‌نگاری همراه با رمزنگاری می‌تواند امنیت بالایی را برای تبادل اطلاعات فراهم نماید. در مقابله با پنهان‌نگاری شیوه‌های پنهان شکنی ارائه گردیده‌اند که مبادرت به کشف وجود پیام پنهان در رسانه‌های پوششی می‌کنند.

یکی از مهمترین شاخص‌ها در پنهان‌نگاری، بازدهی جاسازی سیستم پنهان‌نگار است که به صورت تعداد بیت جاسازی شده در شیء پوشانه به ازای هر واحد تغییرات ایجاد شده در آن تعریف می‌گردد. تا کنون روش‌های متعددی برای افزایش بازدهی جاسازی ارائه گردیده‌اند، با این وجود مساله‌ی افزایش بازدهی سیستم پنهان‌نگار صوتی همچنان مسأله‌ای چالش‌برانگیز است. در این پایان‌نامه ابتدا روش‌های موجود پنهان‌نگاری در رسانه‌های صوتی، بررسی شده است و بازدهی جاسازی برای طرح‌هایی که تا کنون ارائه شده‌اند محاسبه می‌شود. سپس به معرفی یک طرح پیشنهادی پربازده جهت جاسازی اطلاعات در رسانه‌های صوتی معرفی شده است. در طرح پیشنهادی با بهره‌گیری از خواص سیستم شنوایی انسان قسمت‌هایی از صوت که سیستم شنوایی انسان قادر به درک آن‌ها نمی‌باشد دچار تغییرات بیشتری می‌گردند تا از تغییرات سایر قسمت‌های سیگنال صوتی کاسته گردد. به این ترتیب جاسازی به شکلی انجام می‌گردد که کمترین اعوجاج قابل درک بر روی صوت حاصل شده ایجاد گردد و سیگنال صوتی ایجاد شده دارای کیفیت بالایی باشد. در طرح پیشنهادی، بیت‌های داده با ایجاد تغییرات در دو نمونه‌ی متوالی جاسازی می‌گردند. این تغییرات با محاسبه‌ی باقیمانده‌ی تفاضل دونمونه به گونه‌ای انجام می‌شود که میزان تغییراتی که برای جاسازی بیت‌های پیام بر روی نمونه‌ها انجام می‌گیرد کاهش قابل توجهی یابد. کاهش میزان تغییرات انجام شده بر روی نمونه سیگنال صوتی برای جاسازی تعداد بیت مشخص، همان افزایش بازدهی جاسازی می‌باشد. بازدهی طرح پیشنهادی با پیاده سازی آن اندازه‌گیری، و همچنین کیفیت سیگنال صوتی پس از جاسازی داده در آن سنجیده شده است و با پر بازده‌ترین طرح موجود مقایسه گردیده است. نتایج به‌دست آمده نشان دهنده‌ی افزایش چشم‌گیر میزان پیام جاسازی شده برای یک سیگنال صوتی مشخص نسبت به طرح‌های موجود می‌باشد و بازدهی بیشتر طرح پیشنهادی نسبت به سایر طرح‌ها را نشان می‌دهد.

کلمات کلیدی: ۱- پنهان‌نگاری ۲- پنهان‌شکنی ۳- بازدهی جاسازی ۴- سیستم شنوایی

فصل اول

مقدمه

۱-۱ پیشینه‌ی موضوع تحقیق

رمزنگاری[1] از دیرباز به عنوان وسیله‌ای برای حفاظت از اطلاعات محرمانه در برابر افراد مختلف و همچنین جلوگیری از دسترسی‌های غیرمجاز مورد استفاده قرار گرفته‌است. در رمزنگاری با استفاده از الگوریتم‌های طراحی شده و یک کلید[2] امن، متن پیام محرمانه به متنی غیرقابل فهم تبدیل می‌گردد و تنها گیرنده‌ی مجاز با در دست داشتن کلید امن و اطلاع از الگوریتم رمزنگاری قادر به استخراج پیام محرمانه از این متن غیرقابل فهم، خواهد بود. کلید در رمزنگاری رشته‌ای از داده‌های دیجیتال، مانند یک کلمه‌ی عبور، می‌باشد. در یک سیستم رمزگذار بیت‌های پیام محرمانه با توجه به کلید، به گونه‌ای جابه‌جا شده و تغییر می‌یابند که دسترسی به پیام محرمانه از روی متن رمز شده بدون در دست داشتن کلید در زمان معقول غیرممکن باشد. امنیت کامل[3] در رمزنگاری توسط شانون در [۱] مترادف با صفربودن اطلاعات متقابل[4] بین متن رمزشده و متن اصلی تعریف گردید که برای برقراری این شرط باید ابهام[5] کلید، بیشتر یا مساوی با ابهام پیام باشد و این باعث طولانی شدن اندازه‌ی کلید می‌شود.

سیستم‌های رمزنگاری هرقدر هم که امنیت قابل قبولی داشته‌باشند، ولی به هرحال وجود یک ارتباط محرمانه را آشکار می‌سازند. اما در مواردی پنهان بودن وجود یک ارتباط از دید شخص ثالث، حائز اهمیت است. به عنوان مثال در مبادله‌ی پیام، در کاربردهای نظامی، جاسوسی و ارتباطات میان سازمان‌ها، حتی برقرار شدن ارتباط نیز باید

---

[1] Cryptography
[2] Key
[3] Perfect Security
[4] Mutual Information
[5] Entropy

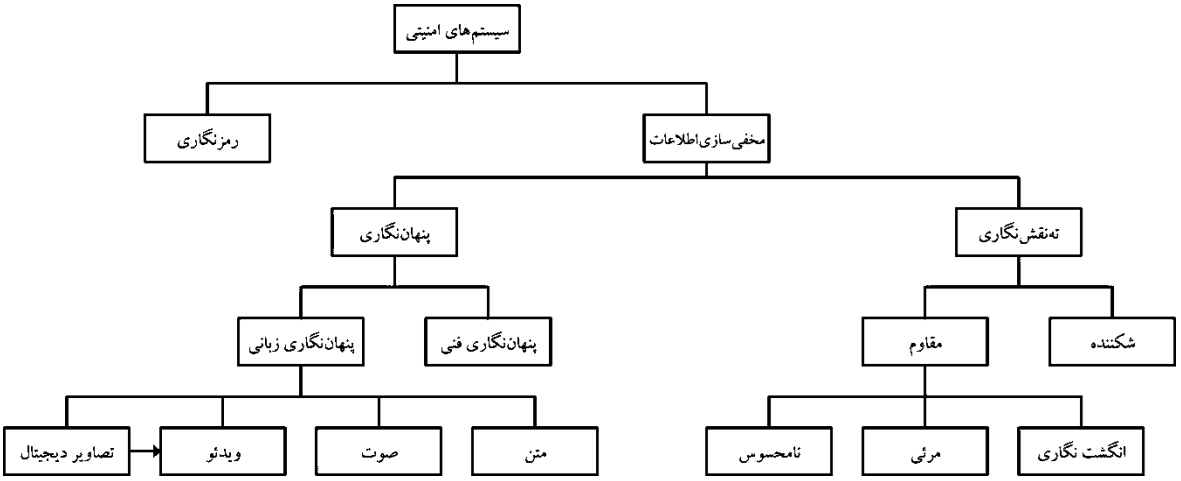
مخفی نگاه داشته شود. در این موارد فرد مهاجم اگرچه نتواند به محتوای پیام دسترسی پیدا کند اما وجود ارتباط بین دو گروه را شناسایی می‌کند و می تواند پیام مبادله شده را مخدوش کند، قسمتی از آن را حذف کند و یا مانع برقراری ارتباط شود. دانشی که به پنهان کردن وجود ارتباط بین دو گروه می‌پردازد پنهان‌نگاری[1] نام دارد. پنهان‌نگاری برگردان فارسی واژه‌ی Steganography می‌باشد که یک واژه‌ی مرکب یونانی است و از دو کلمه‌ی Steganos (στεγανός) به معنای پوشیده و پنهان و *Graphei* (γραφή) به معنای نوشتن تشکیل شده‌است [۲]. در مقابل پنهان‌شکنی[2] دانشی است که به کشف وجود ارتباط مخفی شده مبادرت می‌ورزد. با کشف وجود یک ارتباط پنهان حتی اگر پیام محرمانه قابل استخراج نباشد، سیستم پنهان‌نگار با شکست مواجه شده‌است. روش‌های پنهان‌نگاری و پنهان‌شکنی در تقابل با یکدیگر رشد کرده و توسعه یافته‌اند.

دانش پنهان‌نگاری خود زیر شاخه‌ای از علم مخفی‌سازی‌اطلاعات[3] است. ته‌نقش‌نگاری[4] شاخه‌ی دیگری از علم مخفی‌سازی‌اطلاعات می‌باشد. درشکل ۱-۱ تقسیم‌بندی کلی سیستم‌های امنیتی نشان داده شده‌است. ته‌نقش‌نگاری مانند پنهان‌نگاری به قرار دادن اطلاعات در یک رسانه می‌پردازد. اما تفاوت ته نقش‌نگاری با پنهان‌نگاری در این است که میزان اطلاعات جاسازی شده‌ی آن نسبت به پنهان‌نگاری بسیار کمتر بوده و این اطلاعات توضیحاتی در مورد پوشانه می‌باشند. هدف از ته‌نقش‌نگاری معمولاً کنترل کپی‌برداری و بیان حق کپی‌رایت[5] می‌باشد. وجود یک ته‌نقش می‌تواند علنی باشد اما مسئله‌ی اصلی، مقاومت ته‌نقش در برابر تغییرات، حذف نشدن و تغییر نیافتن آن توسط افراد دیگر است. مخفی کردن اطلاعات در یک رسانه علاوه بر کاربرد ارتباطات پنهانی، کاربردهای گوناگون دیگری نیز دارد. تعیین اصالت یک رسانه، نظارت کردن بر پخش، دنبال کردن و پیگیری مشتری، جاسازی داده برای کاهش پهنای باند مورد نیاز، اثبات حق مالکیت، کنترل کپی برداری و افزودن اثر انگشت برای تعیین هویت فرستنده از جمله کاربرد های دیگر پنهان کردن اطلاعات در یک رسانه می‌باشد. در فصل دوم در مورد این کاربردها توضیحات مفصل‌تری داده‌خواهدشد.

در این فصل به معرفی مختصر مفاهیم مربوط به پنهان‌نگاری پرداخته می‌شود. هدف از این فصل توصیف اجمالی و کلی از سیستم‌های پنهان نگار و بیان کاربردهای مختلف این علم است. پس از بیان مختصر کاربردها به بیان چالش‌های موجود در پنهان‌نگاری پرداخته می‌شود و در نهایت هدف و ساختار کلی پایان‌نامه تشریح می گردد.

---

[1] Steganography
[2] Steganalysis
[3] Data Hiding
[4] Watermarking
[5] Copyright Law



شکل ۱-۱ تقسیم‌بندی سیستم‌های امنیتی [۸]

۱-۲ کلیات پنهان‌نگاری

در روش‌های پنهان‌نگاری، وجود ارتباط با قرار دادن پیام محرمانه در یک پیام عادی دیگر، مخفی نگاه داشته می‌شود. به رسانه‌ای که پیام محرمانه در آن جاسازی می‌شود، قبل از جاسازی پیام محرمانه در آن، "پوشانه"[1] و بعد از جاسازی، "گنجانه"[2] می‌گویند. در پنهان‌نگاری با ایجاد تغییرات اندک و غیرقابل تشخیص، پوشانه به شکلی در می‌آید که گیرنده بتواند با داشتن کلید و دانستن نوع الگوریتم پنهان‌نگاری از روی گنجانه بدست آمده، پیام محرمانه را استخراج کند. کلید در پنهان‌نگاری برای بالا بردن امنیت سیستم استفاده می‌شود. کلید می‌تواند به صورت یک عدد باشد که به عنوان هسته‌ی[3] اولیه برای تولید دنباله‌ای از اعداد تصادفی به کار برده می‌شود. دنباله‌ی اعداد تصادفی ایجاد شده، مکان و ترتیب تغییرات اعمال شده بر روی پوشانه را مشخص می‌کنند. این اطلاعات در هنگام استخراج پیام محرمانه با داشتن کلید و تولید مجدد دنباله‌ی اعداد تصادفی در دسترس گیرنده خواهند بود که از آن‌ها جهت استخراج پیام استفاده می‌کند.

سه شاخص مهم در یک طرح پنهان نگاری، امنیت، ظرفیت[4] و مقاومت[5] می‌باشند [۳]. امنیت یک سیستم پنهان‌نگار مهمترین شاخص آن است [۴]. امنیت در پنهان‌نگاری به معنای محسوس نبودن تغییرات به وجود آمده در پوشانه می‌باشد. علاوه براین‌که تغییرات نباید از نظر دیداری و شنیداری قابل درک باشند، تحلیل‌های آماری بر روی گنجانه نیز نباید وجود پیام محرمانه را تشخیص دهند. بنابراین یکسان بودن آمارگان پوشانه و گنجانه مترادف با ایمن بودن طرح پنهان‌نگاری درنظر گرفته‌می‌شود [۵]. همچنین می‌توان برای بررسی امنیت یک طرح پنهان‌نگاری نتیجه‌ی

[1] Cover
[2] Stego
[3] Seed
[4] Capacity
[5] Robustness

حملات[1] مختلف پنهان‌شکنی را بر روی آن بررسی کرد. اگر چه امنیت مهمترین شاخص برای یک طرح پنهان نگاری محسوب می‌شود، امّا برای این‌که یک طرح قابل قبول باشد باید علاوه بر امنیت، ظرفیت نسبتاً خوبی نیز داشته باشد. به مقدار نسبی پیام جاسازی شده در گنجانه ظرفیت می‌گویند. هرچه حجم پیام پنهان شده در یک گنجانه بیشتر باشد، تغییرات به وجود آمده در پوشانه نیز بیشتر است و میزان امنیت پایین خواهد آمد. بنابراین مقایسه‌ی امنیت و ظرفیت سیستم‌های پنهان نگار به طور جداگانه، سنجش خوبی نخواهد بود. معیاری که امنیت و ظرفیت را به طور همزمان بررسی می‌کند بازده جاسازی[2] نام دارد. به مقدار پیام جاسازی شده به ازای مقدار مشخصی از تغییرات اعمال شده در پوشانه، بازده جاسازی می‌گویند [۶]. پیام محرمانه‌ی موجود در گنجانه باید بعد از تغییراتی که ممکن است بر روی آن اعمال گردد، مانند نویز کانال، دستکاری عمدی و فشرده سازی بااتلاف، نیز قابل استخراج باشد که این عامل تحت عنوان مقاومت تعریف می‌گردد. امنیت، ظرفیت و مقاومت در تقابل با یکدیگر هستند و افزایش یک عامل باعث کاهش عوامل دیگر می‌شود[۳].

برای سیستم‌های پنهان‌نگار دسته‌بندی‌های گوناگونی ارائه شده‌است. یکی از انواع دسته‌بندی‌های پنهان‌نگاری، دسته‌بندی براساس نوع پوشانه است. پوشانه می‌تواند انواع مختلفی از یک متن نوشته شده در یک صفحه تا رسانه‌های دیجیتال را شامل گردد. به علت افزایش استفاده از رسانه‌های دیجیتال، استفاده از این رسانه‌ها به عنوان پوشانه کمتر شک برانگیز خواهد بود. امروزه رسانه‌های دیجیتال گوناگونی نظیر پروتوکل‌های اینترنتی، فایل‌های اجرایی[3]، صفحات وب، متن، صوت، تصویر و ویدئو به عنوان پوشانه انتخاب می‌شوند. هرچه قدر میزان استفاده از یک رسانه بیشتر باشد، انتخاب آن به عنوان پوشانه برای تبادل اطلاعات محرمانه، کمتر جلب توجه خواهد نمود. همچنین هر اندازه افزونگی موجود در پوشانه بیشتر باشد، اطلاعات بیشتری را می‌توان در آن جاسازی کرد. رسانه‌های صوتی به طور گسترده، در مواردی مانند خطوط تلفن، رادیو و فایل‌های موسیقی استفاده می‌شوند. اگر چه تعداد فایل‌های تصویری موجود در اینترنت نیر بسیار زیاد است و این فایل‌ها از افزونگی خوبی برای پنهان‌کردن پیام محرمانه برخوردارند، اما در مقایسه با روش‌های موجود پنهان‌شکنی برای تصاویر، بر روی پنهان‌شکنی صوتی کارهای بسیار کم‌تری انجام شده است[۷]، بنابراین فایل‌های صوتی می‌توانند انتخاب خوبی برای پوشانه باشند.

از جمله چالش‌های مورد بررسی در پنهان‌نگاری، افزایش ظرفیت، امنیت و مقاومت طرح پنهان‌نگاری می‌باشد. مقاومت یک سیستم پنهان‌نگار هنگامی اهمیت پیدا می‌کند که گنجانه بعد از عبور از یک کانال دچار نویز یا اعوجاج گردد و یا توسط افراد دیگری تغییر داده شود و فشرده‌سازی بااتلاف و یا تغییر فرمت بر روی آن انجام شود. معمولاً بعد از بارگذاری یک فایل در اینترنت، فایل بدون نویز و اعوجاج به گیرنده می‌رسد و توسط اشخاص

[1] Attacks
[2] Embedding Efficiency
[3] Executive

دیگر تغییر داده نمی‌شود. اما در ته‌نقش‌نگاری، افراد جهت کپی برداری غیر قانونی با اطلاع از وجود ته‌نقش، مایل به تغییر یا از بین بردن آن می‌باشند و افزایش مقاومت، بیشتر در مورد طرح‌های ته‌نقش‌نگاری اهمیت پیدا می‌کند. از مسائل مهم در ارتباط با پنهان‌نگاری افزایش امنیت است. چرا که با افشا شدن وجود پیام محرمانه، سیستم پنهان‌نگار به طور کلی با شکست مواجه خواهد شد. افزایش امنیت و ظرفیت را می‌توان تحت عنوان افزایش بازدهی به صورت همزمان بررسی کرد. که موضوع مورد بررسی در این پایان‌نامه در این راستا می‌باشد.

۱-۳ ساختار پایان‌نامه

تا کنون اکثر کارهای انجام شده و تحقیقات صورت گرفته بر روی پنهان‌نگاری، در زمینه‌ی تصویر بوده و کارهای انجام شده در زمینه‌ی صوت در مقایسه با تصویر بسیار محدود می‌باشند. لذا در این پایان‌نامه سعی بر آن است تا این موضوع به شکل گسترده‌تری باز شده و اکثر اطلاعات مورد نیاز خواننده هر چند به صورت مختصر ذکر شود.

در فصل دوم، اصول مورد نیاز در پنهان‌نگاری به شکل مختصر بررسی شده و مفاهیم کلی که در این زمینه وجود دارند تا حدودی بیان می‌شوند. در انتهای فصل نیز به کاربرد پنهان‌نگاری و ته‌نقش نگاری پرداخته می‌شود و زمینه‌های کاربرد عملی آن بیان می‌گردد.

فصل سوم به اصول روان‌شنیداری می‌پردازد. در این فصل تقریباً تمامی نیازهای پردازشی صوت که برای پنهان‌نگاری لازم است به صورت مختصر مورد بحث و بررسی قرار می‌گیرد. در این فصل اصول عملکرد HAS[1] در شنوایی صوت بیان شده است. مهم‌ترین کاربرد مدل روان‌شنیداری در سیستم‌های پنهان‌نگاری، قرار دادن پیام محرمانه در سیگنال میزبان به گونه‌ای که زیر آستانه شنوایی قرار گیرد، می‌باشد. در ادامه‌ی این فصل روش‌های پنهان‌نگاری در صوت مورد بررسی قرار می‌گیرند و بازدهی جاسازی برای این روش‌ها محاسبه می‌شود.

در فصل چهارم یک روش پربازده برای جاسازی در فایل‌های صوتی پیشنهاد می‌گردد. این روش از جاسازی داده در باقیمانده‌ی اختلاف مقادیر دو نمونه‌ی متوالی برای کاهش اعوجاج در سیگنال صوتی کمک می‌گیرد. همچنین در این روش برای افزایش کیفیت سیگنال گنجانه، پوشش زمانی مدل سازی شده و مورد استفاده قرار می‌گیرد. در انتهای این فصل نتایج پیاده‌سازی الگوریتم پیشنهادی نشان داده شده‌است.

در فصل پنجم ضمن مرور اجمالی بر کارهای انجام شده در این پایان نامه، نتایج بدست آمده توضیح داده خواهد شد و درنهایت پیشنهادات و توصیه‌هایی برای ادامه‌ی کار مطرح شده‌است.

---

[1] Human Auditory System

فصل دوم
مفاهیم و کاربردها

۲-۱ مقدمه

با توجه به کاربردهای گسترده‌ی مخابرات دیجیتال مانند تبادل اطلاعات محرمانه‌ی مالی و نظامی، حفظ امنیت اطلاعات مبادله شده، ضروری می‌باشد. حفاظت از این اطلاعات با استفاده از روش‌های رمزنگاری باعث جلوگیری از دسترسی افراد غیرمجاز به آن‌ها می‌شود. اما وجود یک ارتباط محرمانه کاملاً آشکار و مشهود می‌باشد و فرد معاند می‌تواند متن رمز شده را تغییر داده، قسمتی از آن را حذف کند و یا مانع برقراری ارتباط شود. پنهان‌نگاری دانشی است که اصل وجود یک ارتباط محرمانه را پنهان می‌سازد. در این فصل ضمن مرور مفاهیم و کاربردهای پنهان نگاری انگیزه‌ی تحقیق در مورد افزایش بازدهی جاسازی پنهان‌نگاری بیان می‌گردد.

۲-۲ مدل‌سازی سیستم پنهان‌نگار

مخفی‌سازی‌اطلاعات عنوانی عام برای علمی است که دارای زیرشاخه‌های گوناگونی می‌باشد. دو زیر شاخه‌ی اصلی مخفی‌سازی‌اطلاعات، ته‌نقش‌نگاری و پنهان‌نگاری می‌باشند. هر یک از این زیرشاخه‌ها خود دارای روش‌ها و تکنیک‌های گوناگون پیاده‌سازی هستند. در [۸] یک تقسیم‌بندی برای زیرشاخه‌های علم مخفی‌سازی‌اطلاعات ارائه شده است. در این تقسیم بندی علم مخفی‌سازی‌اطلاعات نیز خود به عنوان زیر شاخه‌ای از سیستم‌های امنیتی درنظر گرفته‌شده‌است. پنهان‌نگاری به دو زیرشاخه‌ی کلی پنهان‌نگاری زبانی و پنهان‌نگاری فنی تقسیم می‌گردد. در پنهان‌نگاری زبانی با استفاده از شیوه‌های مختلف نگارش و به‌کار بردن علائم نگارشی، پیام محرمانه درون متن جاسازی می‌شود. پنهان‌نگاری فنی، شامل دستکاری غیر محسوس در داده‌هایی مانند تصاویر، ویدئو، صوت و متن؛ به منظور جاسازی داده‌ی محرمانه در آن می‌باشد. ته‌نقش‌نگاری نیز شاخه‌ای از علم مخفی‌سازی اطلاعات است که

مانند پنهان‌نگاری به مخفی کردن اطلاعات درون شیء گنجانه می‌پردازد.

در ته نقش نگاری شیء پوشانه انتخابی نیست. در ته‌نقش‌نگاری برای احراز حق کپی‌رایت اطلاعاتی در یک رسانه دیجیتال جایگذاری می‌شود. این اطلاعات معمولاً در رابطه با آن رسانه است و معمولاً سایرین از وجود پیام پنهان در رسانه مطلع می‌باشند. اطلاعات در رسانه به گونه‌ای جاسازی می‌شوند که با ایجاد تغییراتی مانند تغییر فرمت و فشرده‌سازی بااتلاف حذف نشوند. مقاومت در برابر تغییرات و مقدار اطلاعات جاسازی شده، از مهم‌ترین تفاوت‌های میان پنهان‌نگاری و ته‌نقش‌نگاری می‌باشند. همچنین طرح‌های ته‌نقش‌نگاری معمولاً به صورتی پیاده‌سازی می‌گردند که برای استخراج پیام پنهان شده نیاز به داشتن شیء پوشانه می‌باشد. ته‌نقش نگاری را می‌توان به انواع مختلفی که در زیر بیان شده است، دسته‌بندی کرد.

ته‌نقش‌های مقاوم[1]: این ته نقش‌ها باید در مقابل دستکاری‌های ناهمگون[2] مقاوم باشند. همه کاربردهایی که امنیت پیش‌فرض آن‌ها است به این نوع ته‌نقش احتیاج دارند.

ته‌نقش‌های شکننده[3]: این نوع ته‌نقش‌ها از مقاومت بسیار پایینی برخوردار هستند و ممکن است حتّی در مقابل کمترین میزان تغییرات از بین روند. از این نقطه‌نظر، این نوع از ته‌نقش‌ها قابل قیاس با پیام‌های مخفی در تکنیک‌های پنهان‌نگاری است. در مواردی که هدف بررسی یکپارچگی یک شیء است از چنین ته‌نقش‌هایی استفاده می‌شود. مثلاً برای بررسی اینکه آیا در یک عکس مشخصات یک ناحیه تغییر کرده است یا نه، عکس را به صورت شکننده ته‌نقش می‌کنند. حال زمانی که این عکس مورد بررسی قرار گیرد، چنانچه دوباره تغییراتی در آن داده شده باشد، ته‌نقش باید از بین رفته باشد.

ته‌نقش‌های عمومی و خصوصی[4]: ته‌نقش‌ها متناظر با نیازهای امنیتی که برای کلید مورد استفاده در جاسازی و بازیابی ته‌نقش لازم است با هم تفاوت دارند. بر طبق اصل اساسی ته‌نقش‌نگاری، از کلید مشابهی در فرآیند کدگذاری و کدگشایی استفاده می‌شود. اگر کلید شناخته شده باشد، در این صورت به این نوع ته‌نقش عمومی گفته می‌شود و اگر کلید مخفی باشد به آن، ته‌نقش خصوصی گفته می‌شود. ته‌نقش‌های عمومی می‌توانند در کاربردهایی که نیازی به امنیت نیست، به کار روند.

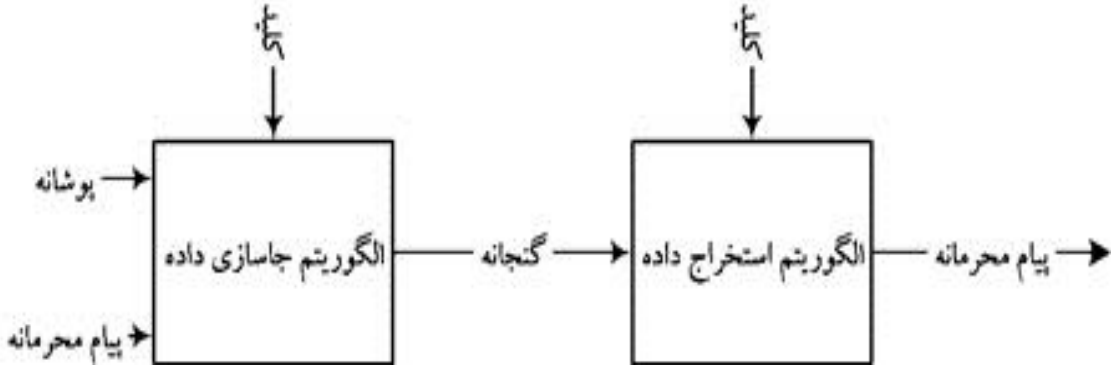
ته‌نقش‌های آشکار یا محلی[5]: مثل لوگوها یا پوشش در تصاویر در زمینه ته‌نقش‌نگاری تصویر یا ویدئو که به خاطر محلی بودن ضمنی اطلاعات، این نوع ته‌نقش‌ها مقاوم نیستند.

یکی از توصیفات معروف ارائه شده برای یک سیستم پنهان‌نگار، مسأله‌ی زندانیان [۹] است. در این توصیف، آلیس و باب دو زندانی هستند که برای طرح‌ریزی نقشه‌ی فرار ناگزیر به مبادله‌ی پیام با یکدیگر هستند. تبادل پیام میان آلیس و باب باید در غالب پیام‌های مجاز صورت بگیرد و نگهبان این پیام‌ها را قبل از رسیدن به دست گیرنده

[1] Robust watermarks
[2] Heterogeneous
[3] Fragile watermarks
[4] Public and private watermarks
[5] Visible or localized watermarks

مورد بررسی قرار می‌دهد. در صورتی که نگهبان پیام را غیرمجاز تشخیص دهد، از برقراری ارتباطات بعدی میان باب و آلیس ممانعت به عمل خواهد آورد. بنابراین ارتباط بین باب و آلیس باید در غالب پیام‌های عادی برقرار شود و پیام محرمانه به گونه‌ای درون پیام عادی گنجانده شود که باعث سوءظن نگهبان نشود و گیرنده بتواند پیام محرمانه را به طور کامل از درون پیام عادی استخراج کند. درصورتی که در طرح پنهان نگاری نگهبان به وجود پیام محرمانه پی ببرد، حتّی اگر قادر به استخراج پیام محرمانه نباشد، طرح پنهان‌نگاری با شکست مواجه خواهد شد. در ساده‌ترین حالت، نگهبان غیر فعّال است و تنها ارتباط میان باب و آلیس را کنترل می‌کند. امّا یک نگهبان فعّال علاوه بر کنترل ارتباط میان گیرنده و فرستنده، می‌تواند پیام را قبل از رسیدن به دست فرستنده تغییر داده، یا قسمتی از آن را حذف کند. در طرح ارائه شده در این پایان‌نامه نگهبان غیرفعال فرض شده‌است.

مدل کلی یک سیستم پنهان‌نگار در شکل ۲-۱ نشان داده شده است. در این مدل تابع جاسازی بر اساس کلید بر روی پوشانه و پیام محرمانه عمل می‌کند و شیء گنجانه را تولید می‌نماید. شیء گنجانه درون کانال مخابراتی ارسال می‌گردد و به‌دست گیرنده می‌رسد. گیرنده نیز با داشتن تابع استخراج داده و کلید، پیام محرمانه را از درون گنجانه استخراج می‌کند.



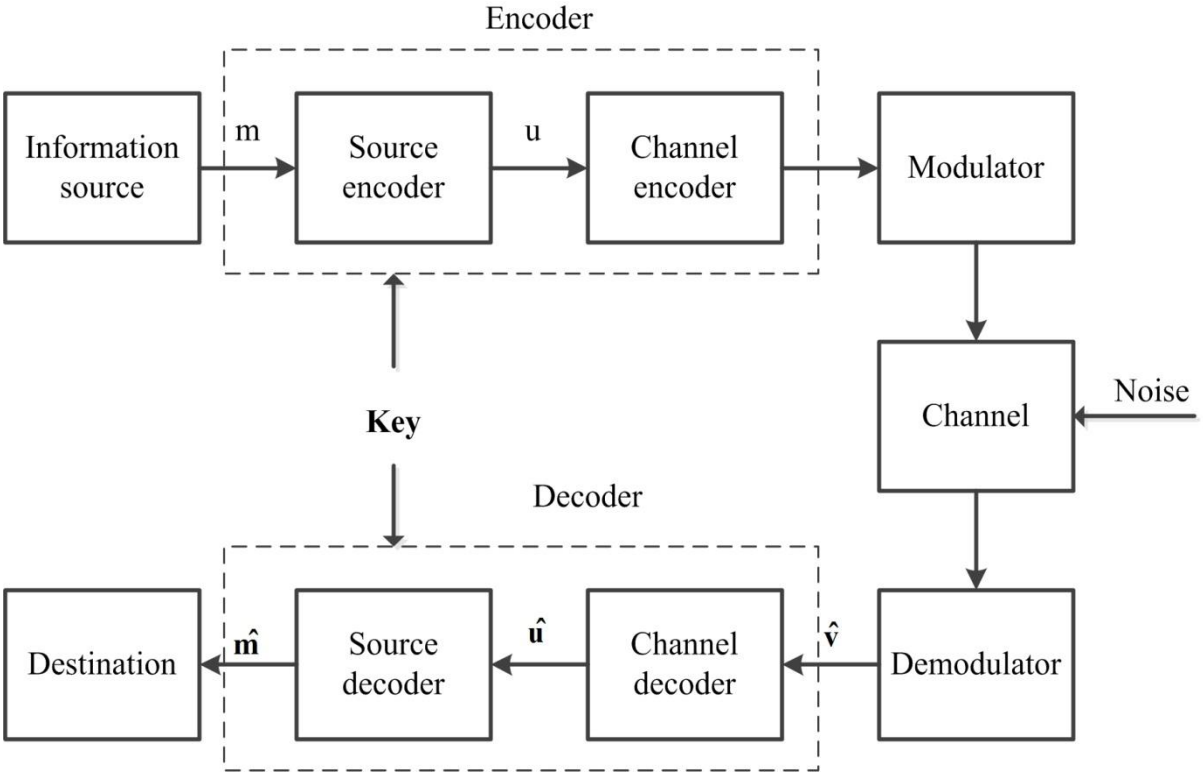
شکل ۲-۱ مدل کلی سیستم پنهان‌نگار

۲-۳ مدل‌سازی مخابراتی سیستم‌های پنهان‌نگاری

پنهان‌نگاری را می‌توان به صورت مخابره‌ی پیام محرمانه در سرتاسر کانالی که شامل سیگنال پوشانه است، در نظر گرفت. در نتیجه یک راه منطقی برای توسعه مدل‌های مفهومی سیستم‌های پنهان‌نگاری ، مطالعه شباهت‌های میان مدل‌های مخابراتی و الگوریتم‌های پنهان‌نگاری نظیر است [۱۰]. هر دو مدل، داده‌ای را از یک منبع به مقصد منتقل می‌نمایند. یکی از مهمترین بخش‌های مدل‌های مخابراتی برای سیستم‌های پنهان‌نگاری، کانال مخابراتی است، زیرا از یک دسته کانال‌های مخابراتی برای مدل کردن اعوجاج‌های وارد شده به سیستم پنهان‌نگاردر اثر حملات، استفاده می‌شود [۱۰و۱۱و۱۲ و۱۳]. از دیگر موضوعات مهم، امنیت بیت‌های جاسازی شده است، زیرا در طرح یک سیستم پنهان‌نگاری، دسترسی دشمن به کانال باید در نظر گرفته شود.

۲-۳-۱ اجزای مدل مخابراتی

عناصر اصلی یک مدل مخابراتی مرسوم در شکل ۲-۲، نشان داده شده است. هدف اصلی، ارسال پیام m در یک کانال مخابراتی است. به طور مرسوم، از آنجایی که با داده و سیگنال‌های دیجیتال سروکار داریم، کدگذار شامل کدگذارمنبع[1] کدگذار کانال[2] و یک مدولاتور است. کدگذار منبع داده‌های اضافه در پیام ورودی را حذف می‌کند و یک پیام را به یک رشته سمبل که از برخی حروف به دست می‌آید، نگاشت می‌دهد. کدگذار کانال معمولاً پیام را به گونه‌ای کد می‌کند که برای ارسال در کانال مناسب باشد. به عبارت دیگر، کدگذار کانال تابعی است که هر پیام ممکن را به یک کلمه‌ی کد نگاشت می‌دهد. این کلمه‌ی کد، v ، از یک مجموعه سیگنال که می‌توانند در کانال ارسال شوند، به دست می‌آید. وظیفه‌ی مدولاتور، تبدیل رشته سمبل‌های کدگذار کانال به سیگنال‌های مناسب برای ارسال در طول کانال مخابراتی فیزیکی است. در این بخش از مدولاسیون‌های مختلفی مثل مدولاسیون دامنه، فاز یا فرکانس استفاده می‌شود. فرم قطعی خروجی کدگذار کانال به نوع کانال مخابراتی که در یک مدل خاص به کار می‌رود، بستگی دارد اما به صورت یک رشته با مقادیر حقیقی که با دقت دلخواه کوانتیزه شده‌اند، توصیف می‌شود. علاوه بر این، فرض می‌کنیم که محدوده‌ی مقادیر کدکننده کانال به گونه‌ای که توسط توان یا محدودیت دامنه تعیین می‌شود، محدود است.



شکل ۲-۲ مدل استاندارد یک سیستم مخابراتی امن [۱۰]

سیگنال خروجی مدولاتور یعنی x در کانال مخابراتی ارسال می‌شود. کانالی که فرض می‌کنیم نویزی باشد.

[1] Source encoder
[2] Channel encoder