بسم الله الرحمن الرحيم

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر گرایش معماری سیستم

طراحی وپیاده سازی پنهان نگاری داده درVoIP با استفاده از ترکیب الگوریتم‌های LACK وLSB

استاد راهنما:

دکتر احمد رضا نقش نیلچی

پژوهشگر:

حسین مودی

تیر ماه ۱۳۸۹

کلیه حقوق مترتب بر نتایج مطالعات، ابتکارات

و نوآوری‌های ناشی از تحقیق موضوع این پایان نامه

متعلق به دانشگاه اصفهان می باشد.

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه ی کارشناسی ارشد رشته ی مهندسی کامپیوتر گرایش معماری سیستم آقای حسین مودی

تحت عنوان

طراحی وپیاده سازی پنهان نگاری داده درVoIP با استفاده از ترکیب الگوریتم‌های LACK وLSB

در تاریخ ۱۳۸۹/۵/۲۲ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد راهنمای پایان نامه دکتر احمد رضا نقش نیلچی با مرتبه‌ی علمی استادیار امضا

۲- استاد داور داخل گروه دکتر امیرحسین منجمی با مرتبه ی علمی استادیار امضا

۳- استاد داور خارج از گروه دکتر شادرخ سماوی با مرتبه ی علمی استاد امضا

امضای مدیر گروه

با تشکر و قدردانی از

استاد گرانقدر جناب آقای دکتر نقش نیلچی که استاد راهنمای این پروژه بودند و من را در تمام مراحل انجام این کار یاری رساندند.

تقدیم به

پدر ، مادر و همسر عزیزم

چکیده

در این پایان نامه روش جدیدی برای پنهان نگاری داده در محیطهای بلادرنگ تحت شبکه ارائه شده است. این فرآیند ترکیبی از روش‌های LSB و LACK به نام (LASB) می باشد. با ترکیب این روش‌ها احتمال تشخیص داده‌ی پنهان شده به حداقل می رسد. برای فراهم آوردن محیط VoIP از پروتکل RTP استفاده شده و الگوریتم‌های LACK ، LSB و LASB در محیط VoIP با استفاده از زبان برنامه نویسی C# پیاده‌سازی شده‌اند. برای پی بردن به کارایی روش LASB، این روش با روش‌های LACK و LSB مقایسه شده است. بدین منظور سه مرحله آزمایش بر روی روش‌های فوق صورت گرفت. در مرحله‌ی اول، تحمل پذیری خطا در صورت بروز مشکل در شبکه بر روی پیاده‌سازی‌های روش-های LSB و LASB آزمایش شد. در نتیجه‌ی این آزمایش مشخص شد روش LASB در مقابل حملات دارای انعطاف پذیری بیشتری نسبت به روش LSB می باشد. در مرحله‌ی دوم، مدت زمان مکالمه برای ارسال فایل پنهان مورد بررسی قرار گرفت . در نتیجه‌ی آن مشخص شد روش LASB به مدت زمان مکالمه کمتری برای ارسال فایل پنهان نسبت به روش‌های LACK و LSB نیاز دارد. در این حالت می توان نتیجه گرفت که روش LASB توانایی جابجایی حجم داده-ی پنهان بیشتری را نسبت به روش‌های فوق دارا می باشد. در مرحله‌ی سوم حالتی در نظر گرفته شد که ناظر سیستم به وجود داده‌ی پنهان شده در صدای ارسالی پی برد و بخواهد این داده را توسط فرآیندهای LACK یا LSB بازیابی نماید. در نتیجه‌ی این آزمایش مشخص شد در صورتی که فایل پنهان از طریق الگوریتم LASB ارسال گردد، ناظر قادر به بازیابی فایل پنهان جاسازی شده در بسته‌های صدا از طریق الگوریتم‌های LACK یا LSB نخواهد بود. در نهایت، سه مرحله آزمایش نشان می‌دهد که روش جدید LASB سریعتر از روش‌های LACK و LSB بوده و دارای ظرفیت جابجایی داده‌ی پنهان بیشتری نسبت به این روش‌ها می‌باشد. همچنین روش LASB در مقابل حملات معمول مقاوم‌تر از روش‌های فوق می‌باشد.

کلمات کلیدی: پنهان نگاری، VoIP، LASB ، شبکه داده‌ی دیجیتال

فهرست مطالب

عنوان **صفحه**

عنوان **صفحه**

فصل چهارم : پیاده سازی و نتایج آزمایشات

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل دوم :

فصل سوم :

فصل چهارم :

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فصل دوم :

فصل سوم :

فصل چهارم :

فصل اول – مقدمه

۱-۱ مقدمه

امروزه ارتباطات دیجیتال به بخش مهمی از زیر ساخت ها تبدیل شده است. بسیاری از برنامه‌های کاربردی، مبتنی بر اینترنت می‌باشند. با فراگیر شدن اینترنت در سطح دنیا، درخواست‌های مربوط به سرویس VoIP افزایش چشمگیری یافته است. مهمترین امتیاز VoIP را می توان ارزان بودن این سرویس، نسبت به سرویس PSTN که شرکت‌های مخابراتی ارائه می‌دهند دانست. یکی از موضوعات اساسی در این زمینه امنیت اطلاعات می‌باشد. اینترنت محیط بازی است، هکرها و سارقان اطلاعات به راحتی می‌توانند اطلاعات افرادی را که در آن مشغول به فعالیت هستند، بربایند یا فعالیت آنها را مختل کنند. با توجه به اینکه از سرویس VoIP در اینترنت و شبکه‌های محلی استفاده می‌گردد، در برخی موارد مطلوب است که ارتباط به صورت محرمانه باشد برای رسیدن به این هدف دو روش وجود دارد: روش اول رمزنگاری[۱] می‌باشد. در این روش فرستنده کلید رمزنگاری را جهت رمز کردن پیام مورد نظر بکار می‌برد، پیام رمز شده از طریق کانال عمومی ناامن به مقصد ارسال می‌شود. در مقصد بازگشایی پیام رمز شده در صورتی امکان پذیر است که گیرنده دارای کلید مناسب رمزگشایی باشد. روش دوم پنهان نگاری[۲] می‌باشد. در این روش پیام محرمانه در پیام دیگری جاسازی می‌شود. با استفاده از این تکنیک حتی وجود داده‌ی پنهان شده در پیام مخفی می‌ماند. به دلیل بلادرنگ بودن VoIP، روش پنهان نگاری در این محیط‌ها کاربرد بیشتری دارد (در محیط بلادرنگ، زمان در اولویت قرار دارد، روش رمزنگاری به زمان زیادی جهت

---

[۱] Cryptography

[۲] Steganography

کدگذاری و کشف کد اطلاعات نیازمند است) و امروزه بیشتر تحقیقات در این زمینه صورت می‌گیرد[۱] .

در پنهان سازی اطلاعات دو بحث اصلی وجود دارد.

۱. محافظت تنها در مقابل تشخیص وجود داده‌ی پنهان توسط دشمن غیرفعال[۱]

۲. پنهان کردن اطلاعات بطوری که حتی دشمن فعال[۲] نتواند آنرا کشف کند.

راه حل کلاسیک معروف به "Prisoners' problem" به شرح زیر است: آلیس و باب در زندان هستند و سعی می‌کنند در مورد نقشه فرار با هم گفتگو کنند، اما ارتباطات آنها می تواند توسط ناظر کنترل شود. اگر نقشه آنها یا این حقیقت که آنها در مورد نقشه‌ی فرار با هم بحث می‌کنند کشف شود، آنها به زندانی با درجه‌ی امنیت بالاتر منتقل خواهند شد. بنابراین آنها زمانی می توانند موفق شوند که ناظر نتواند حتی وجود پیام مخفی را تشخیص دهد [۲].

پنهان نگاری کابردهای حقیقی فراوانی دارد. بعنوان مثال در طول دهه‌ی ۸۰ میلادی برخی از اسناد محرمانه کابینه-ی انگلیس به مطبوعات این کشور راه یافت. مارگارد تاچر[۳] نخست وزیر وقت انگلیس از نرم افزاری برای ویرایش اسناد محرمانه استفاده می‌کرد که هویت کاربری را که از اسناد استفاده می‌نمود در فضاهای خالی متن پنهان می‌ساخت. از این رو توانست شخصی که اسناد محرمانه را به مطبوعات واگذار نموده بود، پیدا نماید[۳] .

با فراگیر شدن VoIP، پنهان نگاری در این محیط بیشتر مورد توجه قرار گرفته است. پنهان نگاری VoIP ، روشی برای انتقال داده پنهان کاربر به کاربری دیگر در یک ارتباط VoIP می‌باشد. این کار باید به گونه‌ای صورت پذیرد که توسط شخص سومی قابل تشخیص نباشد. یکی از تکنیک‌های مشهور در این زمینه Covert Channel می‌باشد. این تکنیک سبب می شود تغییرات حاصله در محیط ارتباطی، غیر قابل دید و غیر قابل پیش بینی باشد. این تکنیک امروزه در زمینه‌ی پنهان نگاری بلادرنگ تحت شبکه بسیار محبوب است و از آن استفاده می‌شود[۴]. روش‌های زیادی در حوزه این تکنیک ارائه شده و مورد تجزیه و تحلیل قرار گرفته است[۵][۶]. این روش در فصل سوم به طور مفصل مورد بررسی قرار گرفته است.

این پایان نامه در ۵ فصل ارائه شده و شامل موارد زیر می‌باشد.

---

۱ Passive Adversary

۲ Active Adversary

۳ Margaret Thatcher

فصل اول مقدمه می‌باشد که در ابتدای فصل مقدمه‌ای در زمینه‌ی پنهان نگاری و VoIP ذکر شد.

فصل دوم تاریخچه‌ی پنهان نگاری و کارهای صورت گرفته شده در این زمینه را مورد بحث قرار می‌دهد. در قسمت تاریخچه، کارهای صورت گرفته شده در زمینه‌ی پنهان نگاری از زمان باستان تا جنگ جهانی دوم بیان می‌گردد. محیط‌هایی که امروزه پنهان نگاری در آنها کاربرد دارد (از جمله صوت، تصویر، ویدئو، شبکه و ...) و روش‌های پنهان نگاری استفاده شده در این محیط‌ها در قسمت کارهای صورت گرفته شده در زمینه‌ی پنهان نگاری بحث شده است. در ضمن ابزارهایی نیز در این زمینه‌ها معرفی شده است.

فصل سوم به شرح و بیان VoIP و پنهان نگاری‌های صورت گرفته در این محیط می‌پردازد. در قسمت اول این فصل VoIP معرفی می‌گردد و در قسمت بعد الگوریتم‌ها و روش‌های پنهان نگاری که در این زمینه ارائه شده است بیان می‌گردد.

در فصل چهارم الگوریتم ابداعی LASB که ترکیبی از الگوریتم‌های LACK و LSB است شرح داده شده و در ادامه‌ی آن چگونگی پیاده سازی الگوریتم‌های LACK، LSB و LASB بیان می‌گردد. در انتهای این فصل نیز آزمایش‌ها متعددی که بر روی پیاده سازی‌های الگوریتم‌های فوق صورت گرفته بیان می‌شود و کارایی روش LASB با روش‌های LACK و LSB مقایسه می‌گردد.

در فصل پنجم نتایج بدست آمده از آزمایش‌ها و حملات صورت گرفته بر روی روش‌های LACK، LSB و LASB بیان شده و کارایی روش LASB با روش‌های فوق مقایسه می‌شود. در پایان این فصل نیز کارهای آتی که می‌تواند در زمینه‌ی پنهان نگاری در VoIP صورت پذیرد بیان می‌گردد.

فصل دوم – پنهان نگاری

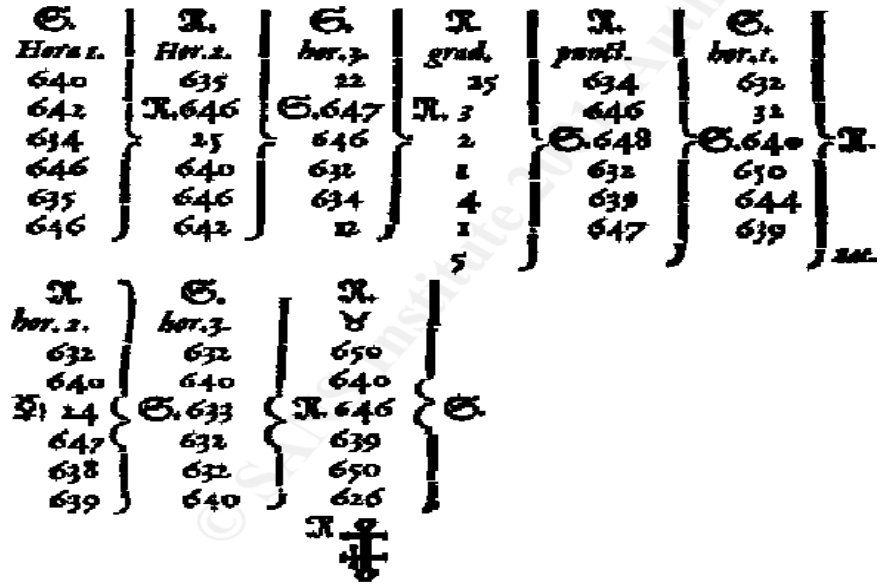
۲-۱- مقدمه

پنهان نگاری به شکل‌های مختلف از حدود ۲۵۰۰ سال پیش مورد استفاده قرار می‌گرفت. این تکنیک به اشکال گوناگون در امور نظامی، دیپلماتیک و شخصی کاربرد دارد. بطور خلاصه، پنهان نگاری اصطلاحی است که برای تمام فرآیندهایی که پیام را درون شیئی پنهان می‌کنند به کار می‌رود. این فرآیند باید بگونه‌ای صورت پذیرد که پیام پنهان شده قابل رویت برای مشاهده کننده نباشد. امروزه، از پنهان نگاری درکاربردهای تجاری نیز استفاده می‌گردد. نرم افزارهایی در زمینه‌ی پنهان نگاری داده در محیط‌های مختلف تولید شده است که در این فصل با تعدادی از آنها آشنا خواهیم شد.

در این فصل ابتدا تاریخچه‌ی پنهان نگاری از دوران باستان تا جنگ جهانی دوم را به صورت مختصر مرور می‌نماییم. در قسمت ۲-۳، پنهان نگاری و کاربردهای امروزی آن و ابزارهایی که به صورت تجاری امروزه از آنها استفاده می‌شود شرح داده خواهد شد. در قسمت ۲-۴ و ۲-۵ درباره‌ی عملیات تشخیص داده‌ی پنهان شده و چگونگی انجام این عملیات به صورت مختصر بحث می‌گردد. در نهایت، از قسمت ۲-۶ تا پایان فصل، محیط‌هایی که امروزه پنهان نگاری در آنها کاربرد دارد از جمله تصویر، ویدئو، فایل‌های متنی، شبکه و ... شرح داده می‌شود.

۲-۲- مروری بر گذشته‌ی پنهان نگاری

در آلمان راهبی بـه نـام Johannes Trithemius (۱۵۱۶-۱۴۶۲) نوشـته‌ای بـا عنـوان " Steganographia: hoc est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" منتشـر نمـود که بظاهر در زمینه‌ی روش‌های برقراری ارتباط با ارواح بود[۷]. یک ترجمه سـطحی از ایـن نوشـته بـا عنـوان "پنهان نگاری : عملی که هر چه بوسیله‌ی آن نوشته می شود پنهان است و نیازمند بازیابی بوسیله‌ی ذهن انسان می باشد." به لاتین منتشر شد. ترجمه‌ی لاتین در سه جلد چاپ شد. دو جلد اول به ظاهر شامل اصول اولیه در رمزنگاری بودکه روش‌های پنهان کردن در نوشته‌ها را توضـیح مـی داد. جلـد سـوم ایـن مجموعـه ظـاهرا در زمینه‌ی اسرار ستاره شناسی می‌باشد. این جلد دارای جدول‌های زیادی است. هر جدول شـامل اعـدادی مـی-باشد. در شکل ۲-۱ این جدول‌ها نمایش داده شده است.



شکل۲-۱ : مثالی از جداول جلد سوم کتاب "Steganographia" [۸]

شکل۲-۲ : Johannes Trithemius [۸]

دو محقق به نام‌های Dr. Thomas Ernst و Dr. Jim Reeds [۹] به وجود کدهای مخفی در جلد سوم این کتاب پی بردند. Dr.Ernst زمانی که از دانشگاه Pittsburgh فارغ التحصیل شد مقاله‌ای ۲۰۰ صفحه‌ای چاپ نمود. این مقاله به زبان آلمانی بود و در سال ۱۹۹۶ در یک ژورنال هلندی به نام Daphnis منتشر شد و مخاطبان محدود خود را مجذوب نمود. Dr.Reeds که یک ریاضیدان بود و در شرکت AT&T کار می‌کرد، بصورت مستقل در حال کاوش در جلد سوم این کتاب بود. وی در حالی که مشغول جمع آوری اطلاعات برای پروژه‌ی Trithemius بود با مقاله‌ی Dr.Ernst آشنا شد.

این دو محقق پس از مدت زمان کمی به این حقیقت پی بردند که جلد سوم کتاب دارای پیام‌های پنهانی می‌باشد. پیام‌ها در جداولی که اهمیت کمتری داشتند قرار گرفته بودند.ترجمه سه پیام از این پیام‌های مخفی این گونه می‌باشد:

- اولین پیام: "روباه قهوه‌ای سریع از روی سگ تنبل پرید."
- دومین پیام: "حمل کننده‌ی این نامه انسان دزد و دغلی است.از خودتان در مقابل او محافظت نمایید. او می خواهد کاری بر علیه شما انجام دهد."
- سومین پیام: قسمت‌های آغازین بیست و سومین سرود مقدس مسیحیان بود.

گرچه "Steganographia" عملی است که واژه پنهان نگاری از آن مشتق شده است، با این حال مطمئنا اولین مثال از نوشته‌های پنهان نخواهد بود. مثال‌هایی در تاریخ وجود دارد که در آن از پیام‌های پنهان استفاده می -