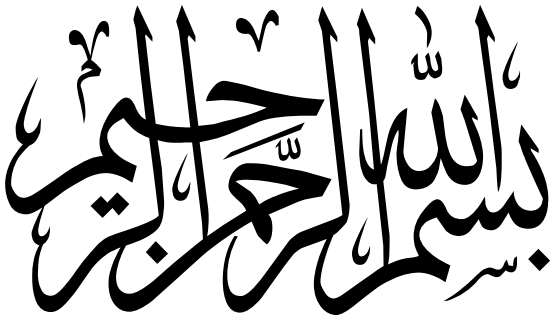
بسم الله الرحمن الرحيم

دانشگاه شهید باهنر کرمان

دانشکده فنی و مهندسی

نهان نگاری اصوات دیجیتال

دانشجو:

سمیه مهدوی جعفری

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی برق گرایش مخابرات

استاد راهنما:

دکترسعید سریزدی

استاد مشاور:

دکتر سعید صید نژاد

شهریور ۱۳۸۸

پیش کش به:

چشمها و تبسمهای زیبای مادر مهربانم،

قامت استوار پدر بزرگوارم،

گرمای وجود همسر فداکارم،

و

مقام شامخ استاد گرانقدرجناب آقای
مهندس علی محمدیان نژاد

سپاس و قدر دانی:
سپاس خدا را که مرا یاری بخشید تا به مرحله ای از دیگر مراحل تحصیل راه پیدا کنم، این راه پر مشقت را طی کنم و امروز نیز در پرتو الطاف گیتی گستر او این مرحله را به پایان برسانم.
سپاس من همچنین نثار دو عزیزی که وجودم همچون ساقه نیلوفری بر گرد شاخه مستحکم وجود آنها پیچید تا امروز بتواند قد علم کند. کلام را از بیان سپاسی که برتعالیم ارزشمندشان متصوراست قاصر و دست را در برآوردن دینی که بر مقامشان رواست ناتوان می بینم.
از همسر عزیزم که وجودش گرمابخش زندگی ام است وفداکارانه در تدوین این پایان نامه مرا یاری نمودند، کمال تشکر را دارم.
همچنین ازدو برادر عزیزم که در تمامی لحظات تحصیل یار و یاورم بودند وبا از خود گذشتگی هایشان زمینه موفقیتهای مرا فراهم آوردند، متشکرم.
از جناب آقای دکتر سریزدی که با وجود مشغله کاری فراوان زحمت راهنمایی این پایان نامه را پذیرفتند، کمال تشکر را دارم.
همچنین از جناب آقای دکتر صید نژاد که نه تنها استاد علم که استاد درس زندگی بودند و با وجود شرایط خاص من برای حضور در دانشگاه با سعه صدر انجام این پروژه را مدیریت نمودند، تشکر می نمایم.
بر خود می دانم که از کلیه اساتید بزرگوار در بخش برق دانشگاه شهید باهنر کرمان که برای به ثمر نشستن درخت علم من کوشیدند و به ویژه جناب آقای دکتر طالبی و جناب آقای دکتر نظام آبادی که زحمت داوری این پایان نامه را نیز بر عهده داشتند، تشکر کنم.
لازم می دانم از جناب آقای مهندس دوست محمدی عضو محترم هیأت مدیره شرکت مخابرات استان کرمان که با بلند نظری زمینه حضور فعال اینجانب در دانشگاه را فراهم آوردند، تشکر نمایم.
همچنین از جناب آقای مهندس مطهری معاونت محترم نگهداری شرکت مخابرات استان کرمان که با ادامه تحصیل اینجانب موافقت فرمودند، تشکر می نمایم.
در انتها به صورت ویژه ازجناب آقای مهندس محمدیان مدیریت مخابرات شهرستان رفسنجان که در راه ادامه تحصیل من از هیچ کمکی دریغ نورزیدند و ادامه تحصیل من جز در پرتو بلند نظری ها، همدلی ها و حمایتهای ایشان امکانپذیر نبود، تشکر می نمایم.
جبران زحمات این بزرگواران و همچنین کسانی که به نوعی در راه موفقیتهای من مؤثر بوده اند و در این مجال از قلم افتاده اند را ماورای توان خود می دانم و لذا آن را به خدا واگذار می نمایم که بهترین یار و یاور است.

چکیده:

نهان نگاری دیجیتال یک روش جدید برای حفاظت از حقوق معنوی مالک و همچنین محافظت از خود محصول چند رسانه ای در برابر اعمال تغییرات می باشد. به طور کلی یک سیتم نهان نگاری دیجیتال به صورت ارسال ایمن، مقاوم و نامحسوس اطلاعاتی در محیط سیگنال میزبان تعریف می گردد. اگر سیگنال میزبان از نوع صوت باشد، اصطلاح نهان نگاری صوت مطرح می شود. در این پایان نامه ابتدا الگوریتمهای پیشین در زمینه نهان نگاری صوتی مورد تجزیه و تحلیل قرار گرفته و سپس دو گروه کلی تعریف و کلیه الگوریتمها در این دو گروه قرار داده می شوند. در نهایت با بهره بردن از این مطالعه، دو الگوریتم مقاوم جدید از نوع کور ارائه گردیده است.

الگوریتم اول موقعیت های مناسب یک سیگنال صوت در حوزه زمان را جهت نهفتن واتر مارک می یابد. این نواحی به حوزه تبدیل منتقل می شوند. با استفاده از یک کلید رمز و الگوریتم خوشه بندی تعدادی از نمونه های هر ناحیه به طور تصادفی انتخاب می شوند. نمونه های انتخاب شده به نمونه های نظیر در حوزه زمان نگاشته می شوند و نهایتاً این گروه نمونه ها توسط یک الگوریتم مبتنی بر تکرار تغییریافته و بدین وسیله واترمارک در این نواحی نهان می گردد. این الگوریتم با استفاده از خواص پوشش زمانی ناشنیدنی بودن واترمارک نهفته شده را تضمین می نماید.

الگوریتم دوم از ایده پرش فرکانسی استفاده می کند. دو مجموعه جداگانه از فرکانسها برای ارسال بیت ″۰″ ویا ″۱″ مورد استفاده قرار می گیرند. این فرکانسها چنان انتخاب می شوند که واترمارک نهان شده را در برابر حملات مقاوم و ناشنیدنی گرداند. برای نهفتن هر بیت واترمارک در یک قسمت از سیگنال صوت، یک جفت فرکانسی به طور تصادفی انتخاب می شود. یکی از این دو فرکانس، براساس بیت پیام و بر اساس محتویات فرکانسی آن قسمت از سیگنال برگزیده می شود. سپس یک سیگنال حامل سینوسی در این فرکانس ساخته می شود. دامنه این سیگنال سینوسی (سیگنال واترمارک) بر اساس خواص فیلترهای بحرانی مدل کننده سیستم شنیداری انسان شکل داده شده و سپس با قسمت نظیر خود در سیگنال صوت جمع می شود. خاصیت مبتنی بر محتوا بودن الگوریتم فوق، امکان فراهم نمودن ماکزیمم شفافیت، مقاومت و ظرفیت را فراهم نموده است.

نتایج حاصل از شبیه سازی و تست الگوریتمهای پیشنهادی با انواع گوناگون سیگنالهای صوتی و تحت حملات مختلف، مقاومت بالای این الگوریتمها را نشان می دهد.

فهرست

فهرست شکلها

فهرست جدولها

کلمات کلیدی

Detecting	آشکارسازی
Extracting	استخراج
Patchwork algorithm	الگوریتم کار چند تکه
Cropping	برش
Real time	بلا درنگ
Frequency hopping	پرش فرکانسی
Audio masking	پوشش صوت
Modification	تغییرات
Quantization	چندی سازی
Carrier	حامل
Threshold	حد آستانه
Clustering	خوشه بندی
Human auditory system(HAS)	سیستم شنیداری انسان
Imperceptibility-Transparency	شفافیت
Audio	صوت
Spread spectrum	طیف گسترده
Modification factor	فاکتور اصلاح
Secret key	کلید رمز
Blind	کور
Cluster center	مرکز خوشه
Robustness	مقاومت
Watermarking	نهان نگاری
Embedding	نهانگی
Watermark	واترمارک

۱

مقدمه

۱-۱. مقدمه

به لحاظ اهمیتی که علم پنهان سازی اطلاعات[۱] در ارتباط با تجارت الکترونیک و مسائل مربوط به ایجاد امنیت برای عرضه محصولات نرم افزاری و الکترونیکی روی شبکه اینترنت دارد، همچنین به لحاظ آشنایی با انواع ارتباطات مخفی و پوشیده ای که به مدد این علم قابل حصول می باشند، در این قسمت به معرفی و بررسی این علم پرداخته می شود.

پنهان سازی اطلاعات شا خه ای چند گانه از دانش می باشد که پردازش سیگنال (پردازش تصویر) را با مخدوش سازی اطلاعات (رمز نگاری) [۲] ، نظریه مخابرات ، نظریه رمزگذاری[۳] ، فشرده سازی سیگنال و نظریه درک انسانی از محیط را ترکیب می کند[1].

استفاده ازپنهان سازی اطلاعات دارای سابقه ای طولانی است. سربازان یونانی برای انتقال پیام به جای آنکه طبق روال عادی آن زمان، روی موم کشیده شده بر لوح ، پیام را بنویسند، پیام را روی خود لوح می نوشتند وسپس آن را با موم می پوشاندند و حال از این لوح مثل یک لوح عادی استفاده می کردند و روی آن یک پیام عادی می نوشتند. یا اینکه برای ارسال پیام از میان نیروهای دشمن سر بردگان را می تراشیدند و روی پوست سرآنها نقشه یا پیام را خال کوبی می کردند و مدتی بعد که سراین بردگان بلند می شد و روی پیام را می گرفت، آنها می توانستند به راحتی از میان سرزمینها و اراضی مربوط به دشمن عبورکنند و در مقصد با تراشیدن مجدد موی

[۱] Information hiding
[۲] Cryptography
[۳] Coding

سرآنان پیام استخراج می شد. همچنین استفاده از جوهرهای نامرئی از زمانهای بسیار دور در نقاط مختلف دنیا مرسوم بوده است[2]. در حال حاضر نیز تکنیکی مشابه در ردیابی انتشارات الکترونیکی مورد استفاده قرار می گیرد که به عدد سریال می توان اشاره کرد. در واقع کاربرد این علم در امور تجاری بسیار زیاد است و در کشورهایی که متعهد به اجرای قانون حق تکثیر می باشند، خدمات خوبی برای صاحبان تولیدات الکترونیکی روی شبکه اینترنت ارائه نموده است. در کشور ما در حال حاضر متأسفانه به دلیل عدم رعایت قانون ذکر شده، شاید اهمیت کاربردی این علم زیاد مورد توجه نباشد. لیکن با پیشرفت تکنولوژی اطلاعات[1] در آینده ای نه چندان دور توجه بیشتر به آن گریزناپذیر خواهد بود.

علاوه بر این استفاده از پنهان سازی اطلاعات در امور ارتباطات گاهاً گریزناپذیر است. یعنی به لحاظ ارتباط این علم با مسائل امنیتی در برقراری ارتباطات پوشیده، توجه ارگانها و نهادهای ذیربط و ذینفع را می طلبد و غفلت از آن زیان های جبران ناپذیری را متصور می سازد.

در کنار واژه پنهان سازی اطلاعات واژه دیگری باعنوان مخدوش سازی(رمزنگاری) مطرح می باشد. البته پنهان سازی اطلاعات با مخدوش سازی(رمزنگاری) اطلاعات تفاوت زیادی دارد . در رمزنگاری برای جلوگیری از دسترسی غیرمجاز به محتوای پیام از مخدوش نمودن آن استفاده می شود. بطوریکه این پیام مخدوش و غیرقابل درک شده ولی توسط شخص مجاز و با استفاده از یک کلید رمز[2] قابل بازسازی است و اطلاعات به راحتی استخراج می شود. لیکن همین امر برای شخص غیرمجازی که تنها به اطلاعات رمز شده و الگوریتم رمزنگاری دسترسی دارد، بدون داشتن کلید ناممکن است[3]. از آنجا که ارسال پیام رمزشده روی کانال عمومی صورت می پذیرد این امر موجب شکل گیری موج عظیمی از حملات مختلف روی این سیستم شده است. بطوریکه می توان گفت جنگ سختی میان طراحان الگوریتمهای رمزنگاری از یک طرف و تحلیل گران این الگوریتمها از طرف دیگر همواره وجود داشته و دارد. طراحان برای افزایش امنیت ومحافظت از

[1] IT (Information Technology)
[2] Secret Key

محرمانگی پیام سعی در پیچیده تر کردن الگوریتم جهت مقاومت در برابر انواع پردازشهای مختلف را دارند و تحلیلگران با نبوغ و استفاده از نقاط ضعف الگوریتمها راههای نفوذ را جستجو می کنند. بنابراین اگر به گونه ای احتمال انجام شدن تحلیل روی الگوریتم کاهش یابد، این کار منجر به افزایش حفاظت از محرمانگی و تمامیت پیام خواهد شد .ایده استفاده از پنهان سازی اطلاعات راهی است در جهت نیل به هدف فوق که در ۱۹۸۳ توسط سیمونز تحت عنوان مسئله زندانیان مطرح شد[4]:

آلیس و باب زندانی هستند و برای طرح نقشه فرار، آلیس میخواهد پیامی را برای باب ارسال کند. ارتباط آلیس و باب از طریق ارسال و دریافت نامه هایی با محتوای مجاز که توسط ویلی زندانبان چک می شود، ممکن می شود. بدیهی است در صورتی که ویلی ارسال پیامی غیرمجاز را تشخیص دهد، به سرپرست زندان اطلاع خواهد داد و این موجب قطع ارتباط آلیس و باب خواهد شد. بنابراین آلیس باید پیام خود را در قالب یک پیام عادی و پنهان شده در آن برای باب ارسال نماید. بطوریکه سوءظن ویلی برانگیخته نشود و باب هم قادر به فهم کامل پیام آلیس باشد .

بنابراین می توان گفت که درپنهان سازی اطلاعات پیام در یک محیط دیجیتال(میزبان) به گونه ای نهفته می شود که این میزبان می تواند به عنوان یک محتوای دیجیتال معمول توزیع و مورد استفاده قرارگیرد؛ حال آنکه حامل یک پیام مخفی می باشد. پنهان سازی اطلاعات به دو شیوه انجام می شود :

- پوشیده نگاری[۱]
- نهان نگاری[۲]

توجه به پنهان سازی اطلاعات از هر دو منظر فوق دارای اهمیت است. چرا که با فراهم شدن زمینه های IT در کشور لزوم استفاده از قانون حق تکثیر و حفظ حقوق مربوط به مالکیت محصولات نرم افزاری و تولیدات الکترونیکی اعم از موسیقی ، آثار هنری ، کتابهای الکترونیکی و ...

[۱] Steganography
[۲] Watermarking

شناخت و استفاده از علم نهان نگاری را ایجاب می کند.از طرفی شناخت پوشیده نگاری نیز از جنبه های کنترلی برای پلیس اینترنتی جهت جلوگیری و شناخت معبری برای ارتباطات غیر مجاز و مشکوک نیز دارای اهمیت است .

همچنین پنهان سازی اطلاعات در ترکیب با رمزنگاری قدرت بسیار بالایی را در مقابل حملات مختلف پدید می آورد[5].

۱-۲. پوشیده نگاری

متشکل از دو کلمه stego به معنی مخفی و graphos به معنای نوشته می باشد که روی هم معنی نوشته مخفی را تداعی می کند. در این پایان نامه از ترجمه پوشیده نگاری برای آن استفاده شده است .

هدف اصلی از پوشیده نگاری، مخفی کردن اصل و حقیقت برقراری ارتباط است. فرستنده یک پیام سرّی را در یک محتوای دیجیتال (تصویر، صوت، فیلم) نهان می کندوتنها گیرنده می تواند این پیام را استخراج کند. از آنجا که نهفتن پیام به گونه ای صورت می گیرد که کیفیت میزبان کاملاً محفوظ باقی می ماند، تمامی کسانی که به کانال ارتباطی دسترسی دارند متوجه ارسال محتوای دیجیتال می گردند. لیکن هرگز متوجه پیام مخفی شده در این محیط نخواهند شد[6]. در مقایسه با رمز نگاری، پوشیده نگاری از امنیت بیشتری بر خوردار است. زیرادر رمزنگاری دسترسی به محتوای پیام برای فرد غیرمجاز ناممکن می گردد. لیکن در پوشیده نگاری موجودیت پیام انکار می شود. هدف رمزنگاری حفظ محرمانگی و تمامیت پیام است که با رمز کردن آن حاصل می شود. پوشیده نگاری ضمن اینکه همین اهداف را با پنهان نمودن پیام دنبال می کند، انتخاب جا و ترتیب پنهان نمودن بیتهای پیام را در لا به لای بیتهای میزبان با بهره گیری از نوعی رمز تحقق می بخشد. همچنین در بعضی موارد، پیام قبل از جاسازی داخل میزبان با استفاده از الگوریتمهای رمزنگاری به صورت رمز درآورد شده و سپس عمل پنهان سازی انجام داده می شود.

در واقع می توان گفت با استفاده از پوشیده نگاری در حقیقت سه لایه حفاظتی بسیار محکم در دسترسی به پیام ایجاد خواهد شد: اول اینکه وجود ارتباط نامحسوس است و این هدف اصلی در پوشیده نگاری است و بنابراین گذشتن از اولین مانع کار چندان ساده ای نخواهد بود. در صورتیکه وجود اطلاعات در یک میزبان مورد سوءظن واقع شود، مرحله دوم پیدا کردن الگوریتم پنهان سازی است. به این معنی که باید جا و ترتیب پنهان شدن اطلاعات معلوم شود. لیکن در این مرحله نیز چون از یک کلید بنام stego_key برای جاسازی پیام استفاده شده، برای آشکارسازی دانستن این کلید ضروری است و بنابراین گذشتن از این مرحله نیز با دشواری همراه خواهد بود. چنانچه دو مرحله قبلی با موفقیت پشت سر گذاشته شوند، اکنون به متن رمزی دسترسی پیدا شده است که تازه در این مرحله مسائل مربوط به رمزنگاری مطرح می گردند[7].

۱-۳. نهان نگاری :

علامات نهان نگاری اطلاعاتی هستند که داخل محصول الکترونیکی جاسازی می شوند و یا به عبارت بهترترکیب می شوند، بطوریکه از مقاومت بسیار بالایی برخوردار می باشند و معمولاً این اطلاعات شامل آرم یا علامت مخصوص شرکت یا مالک است که به آن لوگو گفته می شود.

نهان نگاری بسیار شبیه پوشیده نگاری می باشد. چرا که در هر دو روش سعی بر مخفی نمودن اطلاعات در یک میزبان می باشد. فرقی که پوشیده نگاری با نهان نگاری دارد این است که در پوشیده نگاری آنچه مهم است پیامی است که داخل میزبان پنهان شده و میزبان در حقیقت سدی برای محافظت از پیام است. لیکن در نقش زمینه آنچه که مهم است میزبان است و پیام برای محافظت از میزبان داخل آن جاسازی شده است. اما از آنجا که در پوشیده نگاری اصل ارسال پیام مخفی می باشد، لذا این روشها نیازی به مقاومت در برابر حملات احتمالی در مسیر انتقال ندارند. اما در نهان نگاری وجود پیام مخفی در سیگنال میزبان اعلام می گردد و حتی الگوریتمی که جهت نهان سازی پیام مورد استفاده قرار گرفته است در اختیار عموم از جمله