وزارت علوم، تحقیقات و فناوری
موسسه آموزش عالی غیردولتی-غیرانتفاعی سجاد

پایان‌نامه کارشناسی ارشد برق
گرایش مخابرات

موضوع:

واترمارکینگ برگشت‌پذیر تصویر

ارائه‌دهنده:
سیمین کوشاراد

استاد راهنما:
دکتر هدتنی

مهر ۸۹

بسم الله الرحمن الرحیم

چکیده

با توجه به پیشرفت علوم کامپیوتر و اینترنت طی دهه‌های اخیر، ارسال و ذخیره‌ی داده‌ی دیجیتال، خیلی راحت شده است، بطوریکه در این وضعیت نسخه‌برداری از داده‌ها بدون هیچ افت کیفیت و با هزینه‌ای بسیار اندک امکان‌پذیر می‌باشد. در این شرایط، حفظ امنیت برای داده‌ی دیجیتال یک امر ضروری است. تکنولوژی پنهان‌سازی داده، یکی از روش‌هایی است که از داده‌ی دیجیتال در حین ارسال محافظت می‌کند.

واترمارکینگ دیجیتال یکی از زیر شاخه‌های این تکنولوژی است، بدین منظور، این پایان‌نامه بطور خاص بر روی سسیتم واترمارکینگ بحث می‌کند و با ذکر جنبه‌هایی از این سیستم و بررسی اثر کدهای تصحیح خطا بر روی سیستم واترمارکینگ، در نهایت به شبیه‌سازی روش واترمارکینگ برگشت‌پذیر تصویر می‌پردازد.

واترمارکینگ برگشت‌پذیر تصویر یک نوع خاص از واترمارکینگ می‌باشد، که در صنایع حساسی من جمله پزشکی و نظامی کاربرد دارد.

کلید واژه‌ها: امنیت اطلاعات، پنهان‌سازی اطلاعات، واترمارکینگ، کدهای تصحیح خطا، واترمارکینگ برگشت‌پذیر تصویر

قدردانی:

با کمال احترام از استاد ارجمندم، جناب آقای دکتر عابد هدتنی که همواره راهنمایی‌هایشان بیانگر بهترین مسیر برای انجام مراحل پایان‌نامه‌ام بوده است و از لحظه لحظه‌ی حمایت و کمک خانواده‌ام، مخصوصاً پدر و مادر عزیزم تشکر می‌نمایم.

فهرست مطالب

عنوان	صفحه

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فصل اول

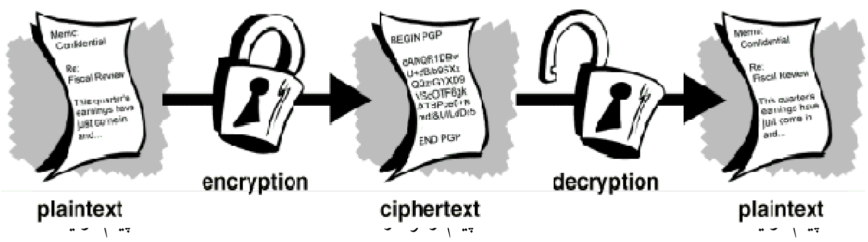
واترمارکینگ از دیدگاه کلی

۱-۱- مقدمه:

مبادله اطلاعات برای انسان همواره یک نیاز محسوب می‌شود و او برای رفع این نیاز به یک محیط نیازمند است. از جمله اطلاعات، اطلاعات محرمانه می‌باشد، برای انتقال اینگونه از اطلاعات محیطی لازم است، که در آن علاوه بر انتقال اطلاعات بصورت محرمانه، نباید امکان تخریب و یا حذف اطلاعات وجود داشته باشد، بدین منظور دو روش رمزنگاری[1] و پنهان‌سازی اطلاعات[2] معرفی می‌شود.

در روش اول، پیام محرمانه از طریق عملیات رمزگذاری با استفاده از کلید محرمانه به پیام رمزداری تبدیل می‌شود، که این پیام از نظر ظاهر با پیام اولیه فرق می‌کند، در نتیجه، پیام محرمانه، قابل تشخیص نمی‌باشد، این امر باعث می‌شود، که امکان دستیابی به پیام محرمانه، غیرعملی باشد.

لازم بذکر است، نحوه‌ی عملیات رمزگذاری بعنوان کلید محرمانه به حساب می‌آید، که برای تأکید بر امنیت سیستم استفاده می‌شود. شکل ۱-۱ یک نمونه از سیستم رمزنگاری را نشان می‌دهد.



شکل ۱-۱ : فرایند رمزنگاری[1]

[1] - cryptography
[2] - information hiding

در مرحله‌ی رمزگشایی، تنها گیرنده‌ی مورد نظر قادر به آشکارسازیی پیام محرمانه می‌باشد، که این کار با آگاهی از عملیات رمزگذاری صورت می‌گیرد، در واقع رمزگشا باید از کلید محرمانه آگاهی لازم را داشته باشد.

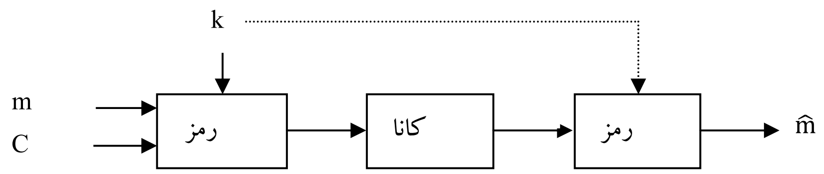
عیب عمده‌ی این روش را می‌توان این چنین بیان نمود، بعد از آشکارسازیی پیام محرمانه، امکان استفاده‌ی غیرمجاز از این پیام برای گیرنده‌های دیگر نیز بوجود می‌آید، این عیب باعث می‌شود که روش مذکور در برابر حملات عمدی کارائی لازم را نداشته باشد، بدین منظور برای غلبه بر این محدودیت، روش دوم مورد توجه بیشتری قرار می‌گیرد[1].

ایده‌ی استفاده از پنهان‌سازی اطلاعات در سال 1983 توسط سیمونز[1] تحت عنوان مسئله‌ی زندانیان[2] مطرح شد [4]-[2] .

مدل کلی از سیستم پنهان‌سازی اطلاعات در شکل ۱-۲ نشان داده شده است، با توجه بشکل، پیام محرمانه m بطور نامحسوس در داده‌ی بی‌ضرری با عنوان پنهان‌ساز یا میزبان C که تنها قادر به حمل پیام محرمانه می‌باشد، جاسازی می‌شود.

فرایند جاسازی با استفاده از کلید محرمانه k صورت می‌گیرد، که رمزگذار از آن مطلع است. حاصل این عملیات، داده‌ی مرکب S که حاوی پیام محرمانه است، می‌باشد.

بعد از انتقال داده‌ی مرکب از کانال و اعمال حملات مختلف بر روی آن، پیام تخریب یافته Y بوجود می‌آید. هدف از حملات مختلف، تخریب و یا دسترسی به پیام محرمانه می‌باشد، که سیستم باید در برابر این حملات مقاوم باشد، زیرا هدف یک سیستم پنهان‌سازی این است که بتواند در نهایت به داده‌ی محرمانه و یا تخمینی از آن دست یابد.



شکل ۱-۲ : نمای کلی از سیستم پنهان‌سازی اطلاعات

[1] - Simmons
[2] - prisoner's problem

در مرحله‌ی رمزگشایی، تنها گیرنده‌ی موردنظر با استفاده از پیام مرکب تخریب‌یافته و با داشتن کلید محرمانه، قادر به آشکارسازی پیام محرمانه $\hat{m}$ که تخمینی از پیام اولیه است، می‌باشد.

بنابراین باتوجه به مطالب بیان شده، هدف سیستم رمزنگاری، پنهان کردن محتواست، در حالیکه، هدف سیستم پنهان‌سازی اطلاعات، پنهان نمودن اطلاعات محرمانه می‌باشد.

۱-۲- تاریخچه‌ی پنهان‌سازی اطلاعات:

ایده مخابره مخفیانه از خود مخابرات، قدیمی‌تر می‌باشد. قبل از اسب، تلفن و ایمیل، پیام‌ها با پای پیاده ارسال می‌شدند. که برای پنهان کردن پیام، دو راه وجود داشت، راه اول این بود که پیغام‌آور، پیام را بخاطر بسپارد و راه دوم اینکه او پیام را در یک پیک، پنهان کند، قدمت پنهان‌سازی اطلاعات، به سال1499 بر می‌گردد، برای مطالعه‌ی بیشتر مراجع [11]-[5] معرفی می‌شوند.

۱-۳- شرایط لازم برای طراحی سیستم پنهان‌سازی اطلاعات:

شرایط لازم برای طراحی سیستم پنهان‌سازی اطلاعات در شکل ۱-۳ نشان داده شده است، که عبارتند از:

۱- شفافیت[1]

۲- قدرت[2]

۳- ظرفیت[3]

این سه شرط با یکدیگر ناسازگارند و ارتباط تنگاتنگی با هم دارند، بعبارتی افزایش یک شرط، شرط دیگر را بخودی خود، تضعیف می‌کند. بدین منظور یک سیستم پنهان‌سازی بهینه باید بین این سه شرط، یک تعادل برقرار نماید.

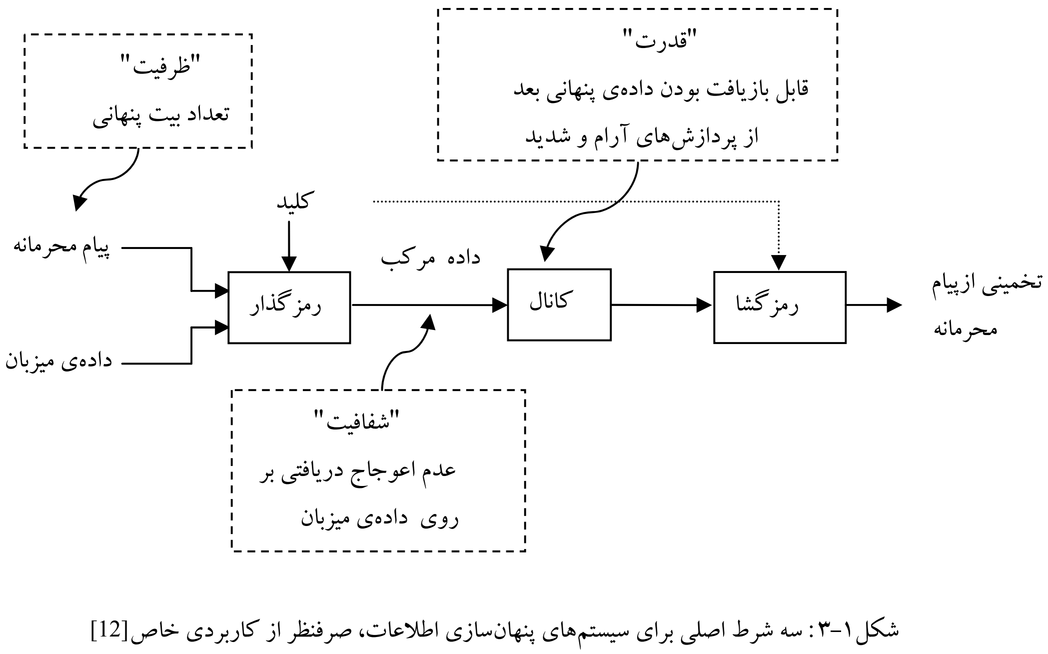
[1] - transparency
[2] - resistance
[3] - capacity

۱-۳-۱- شفافیت:

با جاسازی پیام محرمانه در داده‌ی میزبان، نباید هیچ‌گونه اختلال قابل احساسی در این داده ایجاد شود، بعبارت دیگر داده‌ی مرکب باید بطور واضح و شفاف دریافت شود، زیرا هدف از پنهان‌سازی، انتقال پیام بصورت نامحسوس می‌باشد، و هرچقدر شباهت داده‌ی میزبان در هر دو حالت حاوی و عاری از پیام محرمانه، بیشتر باشد، امنیت سیستم در سطح بالاتری قرار می‌گیرد، این شرط یکی از مهمترین شرط‌های سیستم پنهان‌سازی می‌باشد.

۱-۳-۲- قدرت:

با توجه به اینکه در سیستم پنهان‌سازی، داده‌ی محرمانه باید قابل بازیافت باشد، در نتیجه سیستم باید در برابر حملات غیر عمدی مثل نویز محیط و پردازش‌های عمدی از جمله فشرده‌سازی، تغییر اندازه، برش و ... که بر روی داده‌ی مرکب اعمال می‌شود، مقاوم باشد، زیرا هدف این پردازش‌ها تخریب و یا حذف داده‌ی محرمانه‌ی جاسازی‌شده می‌باشد.



شکل۱-۳: سه شرط اصلی برای سیستم‌های پنهان‌سازی اطلاعات، صرفنظر از کاربردی خاص[12]

۱-۳-۳- ظرفیت:

به میزان حجم پیامی که در داده‌ی میزبان، جاسازی می‌شود، ظرفیت گویند. این تمایل در سیستم پنهان‌سازی اطلاعات وجود دارد که بتوان تا حد امکان، داده‌ی محرمانه‌ی بیشتری در داده‌ی میزبان، جاسازی نمود، بطوریکه دیگر شرایط نیز برقرار باشد.

برحسب کاربردهای مختلف، شرایط متفاوتی برای قدرت و ظرفیت لازم است، اما اغلب کاربردها نیازمند برقراری شرط شفافیت می‌باشند.

۱-٤- تکنیک‌های پنهان‌سازی اطلاعات:

موضوعاتی که پنهان سازی اطلاعات را در بر می‌گیرند عبارتند از:

۱- موارد مربوط به حق مالکیت تولیدات نرم افزاری و الکترونیکی، شامل واترمارکینگ[1] و اثر انگشت[2] که جنبه تجاری از این علم هستند.

۲- استفاده از پنهان سازی در ارسال و دریافت پیام به صورت نامحسوس که ازآن با نام استگانوگرافی[3] یاد می‌شود.

با توجه به این موضوعات، تکنیک‌های پنهان‌سازی اطلاعات شامل موارد زیر می‌باشند:

۱- کانال‌های مخفی[4]

۲- استگانوگرافی

۳- نشانه‌گذاری حق‌نشر[5]

---

[1] - watermarking
[2] - fingerprinting
[3] - steganography
[4] - covert channels
[5] - copyright marking

۱-٤-۱- کانال‌های مخفی:

یک کانال مخفی می‌تواند، بعنوان یک کانال مخابراتی تعریف شود بطوریکه، انواع زیادی از اطلاعات را با استفاده از روشی انتقال دهد، که در اصل این روش برای انتقال این نوع از اطلاعات انتخاب نشده است. بنابراین، پیام پنهانی بطور ناگهانی مخابره می‌شود، در حالیکه تنها فرستنده و گیرنده از این پیام مطلع می‌باشند[5].

۱-٤-۲- استگانوگرافی:

استگانوگرافی یک کلمه‌ی یونانی است و بمعنای نوشته مخفی می‌باشد، این روش همه‌ی موجودیت پیام را پنهان می‌کند. استگانوگرافی، پیام‌ها را در داده‌ی میزبان، سریعتر و ساده‌تر از رمزنگاری پنهان می‌نماید، در نتیجه این تکنیک دارای کاربرد وسیعتری نسبت به رمزنگاری می‌باشد.

استگانوگرافی برای مخابره مخفی بصورت نقطه به نقطه بین دو قسمت کاربرد دارد، در نتیجه در برابر تغییرات قوی نمی‌باشد، یا دارای قدرت محدودی است[5],[6].

۱-٤-۳- نشانه‌گذاری حق‌نشر:

تکنیک نشانه‌گذاری حق نشر در برابر حملات، توانایی لازم برای مقاومت را دارد. در نشانه گذاری‌های قوی، بدلیل آنکه نشانه یا در واقع پیام محرمانه در مؤلفه‌های خیلی مهم از داده‌ی میزبان، جاسازی می‌شود، بنابراین حذف این نشانه‌ها، غیرعملی می‌باشد. واترمارکینگ زیر شاخه‌ای از نشانه‌گذاری حق‌نشر قوی است[6],[7]، که موضوع اصلی مورد بحث در این پایان‌نامه می‌باشد.

۱-۵- واترمارکینگ:

کلمه‌ی واترمارک از نظر لغوی بمعنی اثر آب می‌باشد، دلیل این نام‌گذاری بدین صورت بیان می‌شود، که در کارخانه‌های سنتی تولید کاغذ، الیاف نم‌دار را بوسیله‌ی مهر سختی تحت فشار قرار می‌دادند، تا نم الیاف بر روی کاغذ ایجاد اثری نماید، که از این اثر برای حک مهر کارخانه بر روی کاغذ استفاده می‌کردند. قدیمیترین کاغذ واترمارک‌شده بسال 1292 بر می‌گردد، که اصل آن در شهر کوچک Fabriano در ایتالیا وجود دارد[5],[6].

واترمارک بسرعت در ایتالیا و سپس در اروپا گسترش یافت، اگر چه در ابتدا برای مشخص نمودن برچسب کاغذ، که جنبه قانونی داشت، استفاده می‌شد، اما خیلی سریع در کاربردهای دیگری نیز ظاهر شد.

۱-۵-۱- کاربردهای واترمارکینگ:

از جمله کاربردهای واترمارکینگ می‌توان بموارد زیر اشاره نمود[7]-[5] .

۱- حمایت از حقوق ناشر

۲- اثرانگشت بمنظور پیگیری مجرمین

۳- حفاظت از کپی

۴- تعیین صحت اسناد

۵- نظارت بر پخش عمومی

۱-۵-۲- ساختار واترمارکینگ:

همه‌ی روش‌های واترمارکینگ، بلوک‌های ساختمانی مشابهی دارند. همانطور که در شکل ۱-۴ نشان داده شده است، این سیستم‌ها از یک سیستم جاسازی و یک سیستم استخراج واترمارک تشکیل شده‌اند، در این سیستم‌ها برای تأکید بر امنیت

از کلید استفاده می‌شود، تا بواسطه آن بتوان از حملاتی که قصد تخریب و یا حذف داده‌ی محرمانه را دارند، جلوگیری نمود.

با توجه بشکل، برای طراحی سیستم‌های واترمارکینگ، سه مرحله را می‌توان در نظر گرفت، که در ادامه بیان می‌شوند[8].

۱- **طراحی داده‌ی واترمارک W:** برای این منظور، پیام محرمانه m، با استفاده از کلید محرمانه k به داده‌ی واترمارک W تبدیل می‌شود.

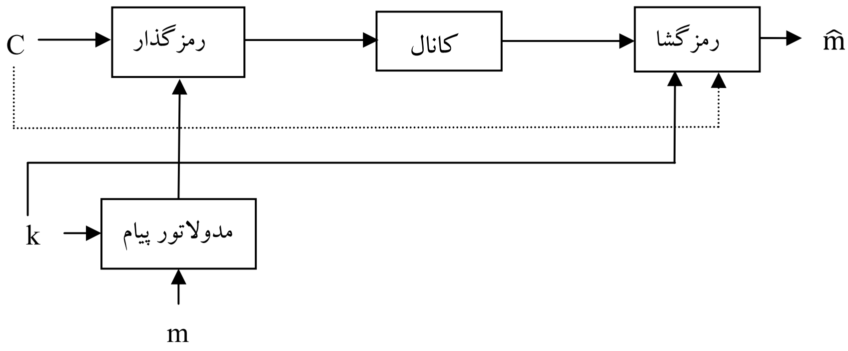
$$W = f_0(m,k) \tag{۱-۱}$$

۲- **طراحی روش جاسازی:** داده‌ی واترمارک W با استفاده از فرایند رمزگذاری در داده‌ی میزبان C، جاسازی می‌شود و حاصل، داده‌ی واترمارک‌شده S خواهد بود، که از آن بعنوان داده‌ی مرکب یاد می‌شود.

$$S = E(C,W) \tag{۲-۱}$$

داده‌ی مرکب با عبور از محیط نویزدار (کانال) به داده‌ی مرکب تخریب‌یافته Y تبدیل می‌شود.

۳- **طراحی روش استخراج:** در مرحله‌ی رمزگشایی، داده‌ی واترمارک از خروجی نویزدار کانال به دو صورت آشکارسازی می‌شود، یک روش با استفاده از کلید محرمانه و با کمک از داده‌ی میزبان، بصورت رابطه (۱-۳) و روش دیگر بدون کمک از داده‌ی میزبان، بصورت رابطه (۱-۴) انجام می‌گیرد. پیام آشکارشده در مرحله‌ی رمزگشایی ممکن است، تخمینی از پیام محرمانه باشد.



شکل۱-۴ : مدل کلی سیستم واترمارکینگ

$$\hat{m} = D(C, Y, k) \qquad (۱-۳)$$

$$\hat{m} = D(Y, k) \qquad (۱-۴)$$

۱-۵-۳- انواع طبقه‌بندی واترمارکینگ:

در ادامه بطور مختصر طبقه‌بندی‌های موجود در سیستم واترمارکینگ بیان می‌شود.

۱-۵-۳-۱- طبقه‌بندی بر اساس حوزه‌ی کاری:

بر اساس اینکه واترمارک در کدام حوزه‌ی پردازش در داده‌ی میزبان جاسازی شود، دو نوع واترمارکینگ بوجود می‌آید.

۱- واترمارکینگ در حوزه مکان

۲- واترمارکینگ در حوزه فرکانس