دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش: مخابرات

عنوان: مروری بر روش های متداول پنهان نگاری و پنهان شکنی

استاد راهنما: دکتر محمد مصطفوی

نگارش: مرتضی حسن آبادی

تیر ۱۳۹۰

تقدیمبه:

پدرومادرفداکارمکهوجودشانراوقفآموختنمنمودند

چکیده:

پنهان نگاری هنر پنهان سازی اطلاعات در اطلاعات دیگر است به گونه ای که نتوان گفت اصلا اطلاعاتی وجود دارد. حامل های مختلفی برای پنهان نگاری وجود دارد اما محبوب ترین آنها تصاویر دیجیتال است. اخیرا پنهان نگاری در بین گروه های خرابکار و تروریستی برای پنهان سازی نقشه هایشان بسیار شایع شده است و متعقبا کشف تصاویری که حاوی پنهان نگاری هستند نیز بسیار اهمیت پیدا کرده است.

در بین روش های مختلف کشف پیام پنهان که پنهان شکنی نامیده می شود، روش های فراگیر یا کور که به نوع پنهان شکنی خاصی وابسته نیستند مناسب تر به نظر می رسند لذا ما در این پایان نامه به بررسی و شبیه سازی یکی از مهمترین این روش ها که روش فرید نام دارد پرداخته ایم و نتایج قابل قبولی را به دست آورده ایم.

کلمات کلیدی: پنهان نگاری، پنهان شکنی، استگانوگرافی، روش فرید.

فهرست مطالب :

موضوع **صفحه**

فصل اول

مقدمه

۱-۱) معرفی پنهان نگاری و پنهان شکنی

پنهان نگاری هنر ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوششی است به گونه ای کهکمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت [۱]. تفاوت اصلی رمزنگاری و نهان نگاری آن است که در رمز نگاری هدف اختفاء محتویات پیام است و نه به طور کلی وجود پیام، اما در نهان نگاری هدف مخفی کردن هر گونه نشانه‌ای از وجود پیام است. در مواردی که تبادل اطلاعات رمز شده مشکل آفرین است باید وجود ارتباط پنهان گردد[۲].

به صورت کلی در سیستم‌های اختفاء اطلاعات سه عنصر اصلی ظرفیت، امنیت و مقاومت دخیل هستند. در روش‌های پنهان نگاری عناصر ظرفیت و امنیت اهمیت اصلی را دارند. تصاویر مهمترین رسانه مورد استفاده به خصوص در اینترنت هستند و درک تصویری انسان از تغییرات در تصاویر محدود است. تصاویر نوعی رسانه پوششی مناسب در پنهان نگاری محسوب می‌شوند و الگوریتم های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر ارائه شده است.

به طور کلی روش های پنهان نگاری در تصویر از الگوریتم جاسازی[۱] و الگوریتم استخراج[۲] بیت‌ها تشکیل شده‌اند. به تصویر مورد استفاده برای پنهان نگاری، پوشانه[۳] و به تصویری که در اثر قرار دادن پیام به وسیله الگوریتم جاسازی به دست می آید، تصویر میزبان[۴] می‌گوییم.

---

۱ Embedding
۲ Extraction
۳ Cover medium
۴ Stego image

الگوریتم‌های پنهان نگاری به صورت عمومی از افزونگی در فضای مکانی[1] یا افزونگی در فضای تبدیل[2] استفاده می‌کنند[۱]. در هر کدام از این فضاها به شیوه‌های گوناگونی می‌توان داده‌ها را پنهان کرد که یکی از ساده‌ترین روشها، استفاده از بیت‌های کم ارزش فضای مورد نظر است.توانایی کشف پیام در تصویر به طول پیام پنهان بستگی دارد.واضح است که هرچه مقدار اطلاعاتی که در یک تصویر قرار می دهیم کمتر باشد امکان کمتری هست که نشانه‌های قابل کشف به وجود آید.

پنهان شکنیدانش کشف حضور اطلاعات پنهان است، مادر پنهان شکنی بهدنبالکشفوتشخیصفایلهاوسیگنالهایحاملپیاممخفیهستیم.در سال‌های ابتدایی پیدایش دانش پنهان نگاری و پنهان شکنی روش‌های بصری نیز مطرح گشتند که یک نمونه از آن در [۳] دیده می‌شود اما بعد از گذشت مدتی از تکامل این دانش این روش‌ها منسوخ گردید. بدین ترتیب روش‌های نهان‌نگاری دشمنِ خود را سیستم بینایی انسان قرار دادند و نسبت به حملات آماری کاری انجام ندادند. معمولا با تحلیل-های آماری می‌توان وجود پیام پنهان را در آنها آشکار کرد.روشهایزیادیبرایتشخیصپنهان نگاریوجوددارند که یکی از ابتدایی ترین روش ها مشاهدهآنفایلومقایسهبادیگرکپی هایآنفایلازطریقپیداکردنآندراینترنت است،

معمولاکپیهایچندگانهایازتصاویردراینترنتوجوددارند،بهطوریکهشمامیتوانیدچنداز آنهاراجهتمقایسهبافایلمشکوکبهکارگیرید .

[1] Spatial domain
[2] Transform domain

۱-۲) تاریخچه پنهان نگاری و پنهان شکنی

اولین استفاده های پنهان نگاریتوسط Herodotus یک مورخ یونانی به ثبت رسیده و ماجرای آن به یونان باستان باز می گردد. وقتی حاکم یونان Histiaeusبه دست داریوش در شوش در قرن پنجم پیش از میلاد زندانی شده بود می بایست پیغامی مخفیانه به بردار خوانده اش در Miletus بفرستد . برای همین منظور موی سر غلامش را تراشید و پیغامی را روی فرق سرش خال کوبی کرد . وقتی موهای غلام به اندازه کافی رشد کرد او را عازم مقصد کرد .

داستان دیگری که از یونان باستان به ما رسیده مربوط به همین پادشاه است ، وسیله نوشتن در آن زمان لوح هایی بوده که روی آن با موم پوشانیده شده بود . یکی از حکام برای اطلاع دادن به وی مبنی بر اینکه کشورش مورد تاخت و تاز قرار خواهد گرفت و برای اینکه این پیغام پیدا نشود مومِ روی لوح ها را پاک کرد و متنش را بر روی لوحِ چوبی حک کرد سپس دوباره موم بر روی آن زد و لوح مانند لوح های استفاده نشده تبدیل شد . سپس بدون اینکه در بازرسی ها برای متن و لوح مشکلی پیش آید به مقصد رسید .

جوهر های نامرئی یکی از عمومی ترین ابزارها برای پنهان نگاری هستند . در روم باستان از جوهر هایی مانند آبلیمو برای نوشتن بین خطوط استفاده می کردند . وقتی متن ها را حرارت می دادند متن آن تیره و نمایان می شد . جوهر های نامرئی در جنگ جهانی دوم نیز مورد استفاده قرار می گرفتند .

یکی از پیشگامان steganography و cryptography ، Johannes Trithemius - ۱۴۶۲ تا ۱۵۲۶ ،یکروحانیآلمانیبود . اولین کار وی بر روی steganography ، *Steganographia*نام داشت که درباره سیستم های جادو و پیشگویی توضیحاتی داده بود ، همچنین در آن کتاب درباره سیستم های پیچیده رمزنگاری هم مطالبی یافت می شد . این کتاب در زمان وی منتشر نشد ، زیرا او از فاش شدن اسرارش می ترسید .

فصل پنجم

نتیجه گیری

نتیجه گیری

در چند سال گذشته علاقه فزاینده ای به استفاده از تصاویر به عنوان رسانه پوششی برای ارتباطات پنهان نگاری شده به وجود آمده است. وسیله های زیادی در حوزه عمومی برای پنهان نگاری بر پایه تصویر وجود ندارند، هرچند برخی از آنها تک کاره و خام هستند. با توجه به این مطلب کشف ارتباطات پنهانی که تصاویر را به کار می گیرند به موضوع مهمی تبدیل شده است. در این پایان نامه ما به مرور برخی مفاهیم اساسی در ارتباط با پنهان نگاری و پنهان شکنی پرداخته ایم.

اگرچه ما تعدادی از مفاهیم امنیت و ظرفیت را پوشش داده ایم. اما هیچ روش معین و دقیقی برای فرموله کردن روابط در مسئله پنهان نگاری وپنهانشکنی از نقطه نظر عملی وجود ندارد. برای مثال این موضوع فهمیده می شود که هرچقدر اطلاعاتی که در تصویر پوشانه جاسازی می شود کمتر باشند، سیستم ایمن تر می شود. اما به علت مشکلاتی که در مدل سازی آماری ویژگی های تصویر وجود دارد، سبک و سنگین کردن بین ظرفیت و امنیت هنوز به صورت تئوری بررسی نشده و در یک چاچوب تحلیلی فرموله نشده است.

ما همچنین تعدادی از الگوریتم های جاسازی که با قدیمی ترین آنها که روش LSB است شروع می شود، را مرور کردیم. از برخی جهات LSB به نظر غیرقابل شکست می آمد اما زمانی که تصاویر طبیعی بهتر درک شدند و مدل های جدیدتری تولید شدند، LSB راه را برای روش های قدرتمندتر که تلاش داشتند تغییرات ایجاد شده در آمارگان تصویر را به حداقل برسانند، هموار کرد. اما با پیشرفت های بیشتر در درک قواعد آماری و افزونگی های تصاویر طبیعی بیشتر این الگوریتم ها با موفقیت پنهان شکنی شدند.

در مسئله پنهان شکنی همانطور که در قبل بحث شد دو روش وجود دارد روش های خاص و روش های فراگیر پنهان شکنی. هرچند پیدا کردن حملاتی به روش جاسازی معین، در مورد روش های جاسازی

بهتر مفید هستند اما به نظر می رسد کاربرد عملی آنها محدود با شد. از آنجایی که در مورد تصاویر داده شده ممکن است ما نوع جاسازی را ندانیم و یا حتی با روش های جاسازی آشنا نباشیم، بنابراین به نظر می رسد روش های پنهان شکنی فراگیر راه حل واقعی باشند چرا که باید بتوانند تصاویر پنهان نگاری شده را حتی وقتی که روش جاسازی جدیدی به کار گرفته می شود کشف کنند.

با توجه به این مطالب ما بخش اعظم کار خود در این پایان نامه را به بررسی و شبیه سازی یکی از مهم ترین روش های پنهان شکنی فراگیر یعنی روش فرید اختصاص دادیم. در اینجا ذکر این نکته لازم به نظر می رسد که نتایج به دست آمده در این پایان نامه اختلافاتی نیز با نتایج اصلی مبتکر طرح دارد ولی این اختلافات در نتیجه گیری کلی ما از این روش پنهان شکنی فراگیر، بی تاثیر است.

منابع و مراجع

[۱] Wayner, p., *Disapearing Cryptography*, ۲nd Edition , by Elsivier Science (USA), ۲۰۰۲.

[۲] Anderson, R.J, Petitcolas, F.A.P., "*On the Limits of Steganography*", IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and privacy Protection, Vol. ۱٦(٤), pp. ٤٧٤-٤٨١, May ۱۹۹۸.

[۳] Fridrich, J., Goljan, M., Du, R., "*Steganalysis Based on JPEG Compatibility*", Proc. SPIE Multimedia System and Applications IV, Denver Vol. ٤٥۱۸, pp. ۲۷٥-۲۸۰, Colorado, ۲۰۰۱.

[٤] Westfeld, A., "F٥__ A SteganographicAlgorithm: High Capacity Despite Better Steganalysis", Proc. ٤th Int'l Information Hiding Workshop, Springer-Verlog Vol.۲۱۳۷, Berlin Heidelberg New York , pp.۲۸۹-۳۰۲, ۲۰۰۱.

[٥] N. Provos, "Defending against statistical steganalysis," *۱۰th USENIX Security Symposium*, ۲۰۰۱.

[٦] F. Alturki and R. Mersereau, "Secure blind image steganographic technique using discrete fourier transformation," *IEEE International Conference onImage Processing, Thessaloniki, Greece.*, ۲۰۰۱.

[۷] A.D. Ker, "Steganalysis of LSB Matching in Grayscale Images.", IEEE Signal Processing Letters, vol. ۱۲(٦), pp. ٤٤۱–٤٤٤, ۲۰۰٥.

[۸] J. Harmsen and W. Pearlman, "Higher-order statistical steganalysis of palette images," in Proc. SPIE Security Watermarking Multimedia Contents, vol. ٥۰۲۰, E. J. Delp III and P. W. Wong, Eds., ۲۰۰۳.

[۹] A. Westfeld, "Detecting low embedding rates," in Proc. Inf. Hiding Workshop, Springer LNCS, vol. ۲۵۷۸, ۲۰۰۲.

[۱۰] A. Westfeld and A. Pittman, "Attacks on steganographic systems," ۳rd International Workshop on Information Hiding., ۱۹۹۹.

[۱۱] R. Machado, “Ezstego,” http://www.stego.com, ۲۰۰۱.

[۱۲] M. Kwan, “Gifshuffle,” http://www.darkside.com.au/gifshuffle/.

[۱۳] N. F. Johnson and S. Jajodia, “Steganalysis of images created using current steganography software,” in David Aucsmith (Eds.): Information Hiding, LNCS ۱۵۲۵, Springer-Verlag Berlin Heidelberg., pp. ۳۲-۴۷, ۱۹۹۸.

[۱۴] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, “Quantitivesteganalysis of digital images: Estimating the secret message lenght,” ACM Multimedia Systems Journal, Special issue on Multimedia Security, ۲۰۰۳

[۱۵] A. Westfeld, “F۵a steganographic algorithm: High capacity despite better steganalysis,” ٤th International Workshop on Information Hiding., ۲۰۰۱.

[۱۶]D.Upham, “Jpeg-jsteg,” ftp://ftp.funet.fi/pub/crypt/steganography/jpeg-jsteg-v٤.di®.gz.

[۱۷]Y. Wang and P. Moulin, “Steganalysis of block-dct image steganography,”*IEEE Workshop On Statistical Signal Processing*, ۲۰۰۳.

[۱۸] A.D. Ker, “Steganalysis of LSB Matching in Grayscale Images.”, IEEE Signal Processing Letters, vol. ۱۲(٦), pp. ٤٤١–٤٤٤, ۲۰۰۵.

[۱۹] J. Harmsen and W. Pearlman, "Higher-order statistical steganalysis of palette images," in Proc. SPIE Security Watermarking Multimedia Contents, vol. ۵۰۲۰, E. J. Delp III and P. W. Wong, Eds., ۲۰۰۳.

[۲۰] I. Avcibas, N. Memon, and B. sankur, “Steganalysis using image quality metrics."*Security and Watermarking of Multimedia Contents, San Jose, Ca.*, February ۲۰۰۱.

[۲۱] S. Lyu and H. Farid, “Detecting hidden messages using higher-order statistics and support vector machines," *۵th International Workshop on InformationHiding.*, ۲۰۰۲.

[۲۲] R. Duda and P. Hart, “Pattern classification and scene analysis," John Wiley and Sons., ۱۹۷۳.

[۲۳] C. Burges, “A tutorial on support vector machines for pattern recognition, *“Data Mining and Knowledge Discovery.*, pp. ۲:۱۲۱-۱۶۷, ۱۹۹۸.

[۲٤] R.J. Anderson and F.A.P. Petitcolas.On the limits of steganography.*IEEE Journal on Selected Areas inCommunications*, ۱٦(٤):٤٧٤–٤٨١, ۱۹۹۸.

[۲٥] N. Johnson and S. Jajodia. Exploring steganography: seeing the unseen. *IEEE Computer*, pages ۲٦–۳٤,۱۹۹۸.

[۲٦] J. Fridrich and M. Goljan. Practical steganalysis: State of the art. In *SPIE Photonics West, Electronic Imaging*, San Jose, CA, ۲۰۰۲.

[۲۷] N. Johnson and S. Jajodia.Steganalysis of images created using current steganography software. Lecture notes in Computer Science, pages ۲۷۳–۲۸۹, ۱۹۹۸.

[۲۸] E.P. Simoncelli and E.H. Adelson.Subband image coding, chapter Subband transforms, pages ۱٤۳–۱۹۲. Kluwer Academic Publishers, Norwell, MA, ۱۹۹۰.

[۲۹] P.P. Vaidyanathan. Quadrature mirror filter banks, Mband extensions and perfect reconstruction techniques. IEEE ASSP Magazine, pages ٤–٢٠, ١٩٨٧.

[۳۰] R.W. Buccigrossi and E.P. Simoncelli.Image compression via jointstatistical characterization in the wavelet domain.*IEEE Transactions on Image Processing*, ٨(١٢):١٦٨٨–١٧٠١, ١٩٩٩.

[۳۱] R. Fisher. The use of multiple measures in taxonomic problems.*Annals of Eugenics*, ٧:١٧٩–١٨٨, ١٩٣٦.

[۳۲] E.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn.Information hiding a survey.*Proceedings of the IEEE*, ٨٧(٧):١٠٦٢–١٠٧٨, ١٩٩٩.