دانشگاه زنجان

دانشکده فنی و مهندسی

گروه برق و کامپیوتر

پنهان نگاری در تصاویر دیجیتال با استفاده از جایگذاری در بیت کم ارزش

پایان نامه جهت دریافت درجه کارشناسی

در رشته مهندسی برق گرایش مخابرات

استاد راهنما:

دکتر محمد مصطفوی

نگارش:

سوسن یوسفلی

اردیبهشت ۱۳۹۴

تقدیم به پدر و مادر عزیزم، آنان که چشمه محبتشان همیشه جوشان است.

چکیده:

نهان نگاری علم پنهان سازی داده درون رسانه های مختلف اعم از صوت و تصویر و ویدئو می باشد که هدف مشترک تمامی آن ها حفاظت از اطلاعات پنهان شده (پیغام) در برابر مهاجمین می باشد. برای رسیدن به این هدف باید کیفیت تصویر حاصل در مقایسه با تصویر اولیه حفظ شود و تصویر حاصل در برابر عملیات نهان کاو ها مقاوم باشد.

در این پژوهش، ابتدا نظریه دانشمندان مختلف را در زمینه نهان نگاری مورد بحث و بررسی قرار می دهیم و نقاط ضعف و قوت هر یک را بازگو می کنیم. سپس با استفاده از الگوریتمی که در فصل های بعد ارائه خواهد شد، پیام مورد نظر را که یک رشته دو بیتی می باشد در دو پیکسل مجاور از تصویر پوششی جاسازی می کنیم. در ادامه با استفاده از یک روش پیشنهادی پیام مورد نظر را درپیکسل های یک رسانه پوششی جاسازی و سپس استخراج می کنیم. مزیت این روش نسبت به روش های قبل این است که ظرفیت جاسازی بالایی دارد. در این روش، با استفاده از پیکسل های پیشنهادی و آستانه از پیش تعیین شده، هر بیت پیام در پیکسلی از تصویر پوششی جاسازی می شود. به این ترتیب فرستنده تمام بیت های پیام را در تعدادی پیکسل جاسازی می کند گیرنده نیز با دانستن الگوریتم جاسازی قادر به استخراج پیام و بازیابی تصویر پوششی خواهد بود.همچنین امنیت و ظرفیت از مباحث بسیار مهم در نهان نگاری هستند که در این مقاله از دید دو دانشند به طور کامل مورد بحث و بررسی قرار می گیرد.

در واقع هدف اصلی از این پژوهش جاسازی حجم زیادی از اطلاعات در تصویر دیجیتال است با این شرط که کیفیت بصری تصویر حفظ شود و احتمال کشف پیام توسط نهان کاو ها به حداقل برسد

واژه های کلیدی: نهان نگاری، رسانه پوششی، گنجانه، پیکسل پیشنهادی، آستانه از پیش تعیین شده، کیفیت بصری تصویر یا نسبت سیگنال به نویز.

فهرست مطالب

عنوان **صفحه**

فصل ۱

مقدمه

۱-۱-نهان نگاری اطلاعات:

پنهان کردن اطلاعات بطور کلی به دو دسته نهان نگاری اطلاعات[۱] و نشان گزاری[۲] اطلاعات تقسیم می شود. اگر چه این دو مورد در پنهان کردن اطلاعات شباهت های زیادی به هم دارند ولی تفاوت های اساسی موجب شده هر یک در زمینه خاص کارآیی داشته باشند.

نهان نگاری عبارتی یونانی است که مشتق شده از دو کلمه پنهان شده[۳] ونوشتن[۴] است و در اصل هنری است که اولین بار یونانیان باستان در مقابل ایرانیان از آن استفاده کردند.

تاریخچه این هنر به پنج قرن قبل از میلاد مسیح و کشور یونان برمی گردد، در آن زمان مردی به نام هیستایاکاس می خواست پیغامی را به صورت محرمانه برای شخص دیگری بفرستد. وی برای فرستادن پیغام موهای سر برده را تراشید و پیغام محرمانه را بر روی پوست سر برده خالکوبی کرد و سپس مدتی صبر کرد تا موهای فرد رشد کرده و به حالت اول برگشت و بعد او را به سمت مقصد روانه کرد. در مقصد، گیرنده دوباره موهای برده را تراشید و پیغام را بر روی پوست سر او مشاهده کرد.

در رمزنگاری[۵] ، محتوای پیام بصورت رمز در فایلی جاسازی می شود. فایل حفاظت شده حاوی پیام، حساس جلوه می کند بطوری که ناظر به وجود پیام مخفی پی می برد و درصدد کشف پیام بر می آید. ولی در نهان نگاری فرستنده پیام رمز شده را در یک رسانه پوششی که جلب توجه نمی کند مخفی کرده و آن را مبادله می کند. در این صورت ناظر به وجود پیام مخفی در رسانه پوششی پی نمی برد.

تفاوت اصلی رمزنگاری و نهان نگاری آن است که در رمز نگاری هدف اختفاء محتویات پیام است نه وجود پیام، اما در پنهان نگاری هدف مخفی کردن هر گونه نشانه ای از وجود پیام است. به عنوان مثال اگر مهاجم به رسانه رمزنگاری شده‌ای دسترسی پیدا کند، متوجه می‌شود که این متن حاوی پیام می‌باشد . اما در نهان نگاری مهاجم به وجود پیام مخفی در متن پی نمی برد. باید دقت شود در موارد حساس، ابتدا پیغام را باید رمزنگاری کرده، سپس پیام رمز شده را در رسانه پوششی که ظاهر مشکوکی ندارد جاسازی کرد تا امنیت اطلاعات حفظ شود.

---

[۱] Steganography
[۲] Watermarking
[۳] Steganos
[۴] Graphia
[۵] Crypography

در مقابل مسئله نهان نگاری، مسئله نهان کاوی[۱] مطرح است . یک نهان کاو تلاش می کند تا وجود پیام را در یک رسانه کشف کند. در رسانه های حامل پیام هر چقدرعملیات نهان کاوی دشوارتر باشد نشان دهنده امنیت بالا در جاسازی اطلاعات است.

از مثال های قدیمی مشهور نهان نگاری می توان به جوهر نامرئی در جنگ جهای اول و پنهان کردن پیام در حروف کلمات انتخاب شده در یک متن ، در جنگ جهانی دوم اشاره نمود.

درج کردن اطلاعاتی خاص مانند یک لوگو در یک داده میزبان که برای حفظ حق کپی انجام می شود، نشان گذاری[۶] نام دارد. تفاوت اصلی سیستم نشان گذاری و نهان نگاری این است که در نهان نگاری هدف درج میزان اطلاعات قابل ملاحظه ای در رسانه پوششی[۲] است و لذا در این سیستم ظرفیت[۳] درمقایسه با مقاومت در برابرحملات اولویت بیشتری دارد. در صورتی که در نشان گذاری هدف رسیدن به سیستمی است که در برابر هرگونه تغییر مقاوم باشد و بنابراین در اینجا مقاومت جزء اهداف اصلی به شمار می رود.

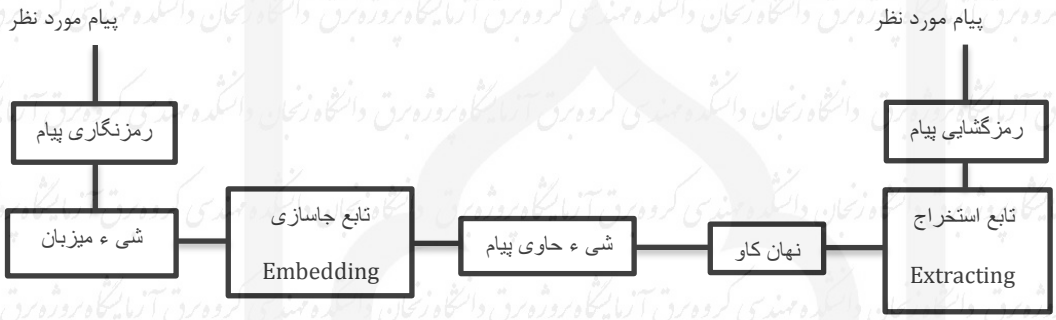
۱-۲-مدل عمومی استگانوگرافی از دید آلیس و باب:

مدل ارتباط غیر قابل شناسایی از طریق نهان نگاری، اولین بار توسط سیمونز در قالب مسئله زندانی ها مطرح شد [۱]. این مسئله به این شکل است که آلیس و باب دو زندانی در دو سلول مجزا و در فکر طراحی یک نقشه فرار هستند. آن ها می توانند از طریق ارسال پیام با هم ارتباط برقرار کنند. این ارتباط پیوسته توسط زندان بانی به نام وندی که فعالیت های مشکوک را کنترل می کند، مورد بررسی قرار می گیرد. اگر ارتباط بین آلیس و باب از نظر وندی مشکوک به وجود پیام باشد، امکان برقراری ارتباط بین آن دو از بین می رود. بنابراین آلیس و باب از نهان نگاری برای ارسال پیام استفاده کردند به این صورت که پیغام مخفی را در یک شی ء پوششی که از نظر وندی مشکوک نباشد جاسازی می کنند. این شی ء پوششی می تواند صوت، تصویر، ویدئو و یا رسانه های دیگر باشد. در ساده ترین حالت زندان بان غیر فعال است و تنها ارتباط بین آلیس و باب را کنترل می کند. اگر زندان بان فعال باشد، می تواند رسانه در حال مبادله را تغییر دهد تا حتی اگر پیغام مخفی در حال مبادله است تخریب شود. اگر زندان بان غیر فعال باشد، تنها ضرورت برای برقراری امنیت نهان نگاری، الگوی جاگذاری[۴] غیر قابل شناسایی می باشد.

---

[۱] Steganalysis
[۲] Cover object
[۳] Capacity
[۴] Embedding

مدل عمومی سیستم نهان نگاری در شکل۱-۱ آمده است. در این سیستم ابتدا آلیس شی ء میزبان x را از منبع پوششی انتخاب می کند، سپس پیام مورد نظر m را که با یک کلید رمز نگاری مشترک رمز شده است، در شی ء میزبان جاسازی می کند و شی ء نهان نگاری شده [۱] حاصل (y) را برای باب ارسال می کند. باب نیز با استفاده از کلید مشترک و تابع استخراج، پیام مخفی شده را از شی ء نهان نگاری شده استخراج می کند. به این ترتیب امنیت سیستم نهان نگاری بستگی به ناتوانی زندان بان وندی در پی بردن به حضور اطلاعات مخفی درشی ء پوششی دارد. در این تعریف، مسئله ای که زندان بان با آن رو به رو است، تشخیص حضور پیام مخفی در اطلاعات مبادله شده بین آلیس و باب است و برای این منظور او می تواند به سابقه ارتباطات و تبادل اطلاعات بین آن دو نیز رجوع کند. به این ترتیب مسئله نهان نگاری و تحلیل آن تعریف می شود.



شکل۱-۱ (مدل عمومی آلیس و باب) [۱]

۱-۳- هدف از انجام پژوهش:

هر روش نهان نگاری دارای نقاط ضعف و قوت مربوط به خود است. بنابراین بهترین روش نهان نگاری روشی است که ضمن بالابودن ظرفیت جاسازی پیام، امکان کشف حضور پیام توسط نهان کاوها به حداقل برسد و لازمه این امر بالابودن کیفیت بصری تصویر[۲] و شباهت نمودار هیستوگرام[۳] رسانه پوششی و گنجانه[۴] به هم و تغییرات ناچیز مشخصات آماری رسانه می باشد. برای داشتن ارتباطی امن در حضور روش های نهان کاوی، نهان نگار باید داده محرمانه را طوری در تصویر پنهان کند که ویژگی های آماری

[۱] Stego Object
[۲] Peak single to noise ratio
[۳] Histogram
[۴] Stego image

تصویر حین فرآیند جاسازی کمترین تغییر را داشته باشد. بعنوان مثال تابع توزیع احتمال پیکسل های رنگی در رسانه پوششی و گنجانه تا حد ممکن شبیه به هم باشند.

۱-۴- نتایج حاصل از پژوهش

روش های مختلفی برای نهان نگاری وجود دارد که هر یک از این روش ها وقتی ارزشمند هستند که علاوه بر امنیت و ظرفیت بالا و حفظ مشخصات آماری، بعد از جاسازی، امکان استخراج درست بیت های پیام وجود داشته باشد و بعد از استخراج پیام بتوان به پیکسل های رسانه پوششی دست یافت.

در این پژوهش نیز سعی شده علاوه بر افزایش کیفیت بصری تصویر، بعد از جاسازی پیام توسط فرستنده در رسانه پوششی، بتوان در بخش گیرنده بیت های پیام را به درستی استخراج کرد و بعد از استخراج پیام از گنجانه به پیکسل های تصویر پوششی دست یافت. این روش نهان نگاری، با استفاده از آستانه از پیش تعیین شده[۱] و پیکسل پیشنهادی[۲] می تواند فرآیند جاسازی و استخراج را به ترتیب در پیکسل های پوششی و گنجانه به درستی انجام دهد.

---

[۱] Threshold

[۲] Predictive pixel

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

منابع و مراجع:

[1] Simmons, G. J . " The prisoner's problem and the subliminal channel" , Advances in Cryptography, pp. 51-67, 1983

[2] Fridrich, J., & Goljan, M. " Digital image steganography using stochastic modulation", Proceedings SPIT, Electronic Imaging, Security and Watermarking of Multimedia, Contents, pp. 191-202, 2003

[3] Mielikainen, J. "LSB Matching Revisited", IEEE Signal Processing, pp. 285-287, 2006

[4] Provos, N., & Honeyman, P. "Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy Magazine, 2003

[5] Westfeld, A. " High capacity despite better steganography (F5 – a Steganographic algorithm)", Information Hiding 4th International Workshop, pp. 289-302, 2001

[6] Fridrich, J., Goljan, M., & Soukal, D."Perturbed quantization steganography using wet paper codes", Proceedings of the 6 th ACM Multimedia & Security Work shop, pp.4-15, 2004

[7] Westfeld, A., & Bohme, R,"Exploiting preserved statistics for steganalysis", Information Hiding, 6th International Workshop, pp.82-96, 2004

[8] Westfeld, A., & Pfitzmann, A." Attacks on Steganographic Systems", '99 Proceedings of the Third International Workshop on Information Hiding, pp.61-76,1999

[9] Wang, C., Li, X., Yang, B., Lu, X., & Liu, C, "A content-adaptive approach for reducing embedding impact in steganography" pp.1762-1765,2010

[11] Chin-Feng Leea, Hsing-Ling Chenb, Hao-Kuan Tsoc. "Embedding capacity raising in reversible data hiding based on prediction of difference expansion" pp. 1864–1872

[12] Filler, T., Judas, J., & Fridrich, J. " Minimizing Additive Distortion in Steganography using Syndrom-Trellis Codes", pp.920-935.2011

[13] Chen, C., & Shi, Y. Q." JPEG image steganalysis utilizing both intrablock and interblock correlations", pp.3029-3032,2008

[14] Cachin, C. " An Inforraphymation- Theoretic model for steganography", pp.306-318, 1998

[15] Mehdi Kharrazi1, Husrev T. Sencar, and Nasir Memon " Image Steganography: Concepts and Practice"