دانشگاه زنجان
دانشکده مهندسی
گروه برق

گرایش : الکترونیک

عنوان : افزایش ظرفیت روش پنهان نگاری اختلاف مقادیر پیکسل ها با استفاده از روش GLM

استاد راهنما : دکتر چرمی

نگارش : مهدی صفرپور

تابستان 92

فهرست مطالب

خلاصه- در اکثر روش های پنهان نگاری افزایش ظرفیت موجب کاهش کیفیت تصویر می شود . برهمین اساس در این متن ما پیشنهاد می کنیم دو روش موجود به نام های اختلاف مقادیر پیکسل ها با روش GLM[1] ترکیب شوند تا یک روش پنهان نگاری ترکیبی با ظرفیت بالا بدون کاهش کیفیت تصویر به دست آید. نتایج آزمایشات نشان دهنده ی این است که روش پیشنهادی ظرفیت بیشتری دارد و نتایج آن قابل درک نیست. در مقایسه با روش اصلی PVD[2] از نظر کیفیت بر مبنای معیار سیگنال به نویز کیفیت در مبنای دسی بل حدود 2 درصد کاهش یافته در صورتی که ظرفیت حدود 25 درصد افزایش یافته است.

کلمات کلیدی- استگانوگرافی و پنهان نگاری و مخفی سازی داده ها GLM و PVD

معرفی

دنیای دیجیتال امروز بیشتر و بیشتر متکی به اطلاعات و مخابرات می شود که به دلیل رشد فزاینده کامپیوتر های دیجیتال و اینترنت است. از این رو امنیت دیجیتال اهمیت بیشتر از هر موقع می یابد و محققات در تلاشند تا روش هایی را توسعه دهند که دنیا را یک محل امن تر بکند.این دانش به چند شاخه تقسیم می شود.

پنهان نگاری یا استگانوگرافی هنر و علم برقراری ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوششی است به گونه‌ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. پنهان نگاری خود شاخه ای از دانشی به نام ارتباطات پوشیده است. دانش ارتباطات پوشیده خود شامل چندین شاخه از جمله رمز نگاری، ,واترمارکیگ و ... می باشد.

روش های نهان نگاری برای محافظت از حقوق مالکیت از محصولات چند رسانه ای توسعه یافته اند ، در واقع این تکنیک برای محافظت از خود رسانه طراحی شده است، بنابراین مقدار داده های جاسازی شده است تا مهم نیست اما به جای آن نیرومندی که به معنی مصونیت از داده های جاسازی شده در برابر اعوجاج سود با اهمیت است [2].

راه دیگری برای ارتباط امن رمزنگاری است. در روش های رمزنگاری اغلب هدف برای مخفی کردن داده ها را از طریق تغییر شکل پیام را به یک پیام بی معنی است. نقطه ضعف این است که پیام غیر معمول قابل توجه است و وجود ارتباطات مخفی را نشان می دهد ، بنابراین روش رمزنگاری ممکن است پیام محافظت می کند ولی نشان دهنده وجود ارتباط مخفی است.

تفاوت اصلی رمزنگاری و پنهان نگاری آن است که در رمز نگاری هدف اختفاء محتویات پیام است و نه به طور کلی وجود پیام، اما در پنهان 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. به عنوان مثال اگر شخصی به متن رمزنگاری شده‌ای دسترسی پیدا کند، به هر حال متوجه می‌شود که این متن حاوی پیام رمزی می‌باشد. اما در پنهان نگاری شخص سوم ابدا از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند. در موارد حساس ابتدا متن را رمزنگاری کرده، آنگاه آن را در متن دیگری پنهان نگاری می‌کنند.

---

[1] GRAY LEVEL MODIFICATION
[2] PIXEL VALUE DIFFERENCING

از سوی دیگر تکنیک های steganographic قصد انتقال اطلاعات را از طریق یک رسانه اند بدون این که کسی متوجه حتی وجود ارتباطات مخفی شود. این با تعبیه داده ها در یک محیط مانند یک تصویر یا یک ویدیو کار می کند. نهان نگاری داده به صورت تغییر پیام مخفی نیست، بلکه پنهان کردن پیام از طریق تغییر رسانه است. نهان نگاری داده، نوع مشابه به نهان نگاری است، اما بر خلاف روش های نهان نگاری، در روش steganographic مقدار از داده های جاسازی شده دارای اهمیت است و نیرومندی دوم می آید [3].

استگانوگرافی که یک کلمه یونانی است به معنی مخفی‌سازی اطلاعات درون پوششی است به صورتی که شک دیگران را برانگیخته نکند و معمولا در ارتباطات مخفی استفاده می‌شود. استگانوگرافی دیجیتالی به معنای استفاده از پوشش دیجیتال مانند فایل‌های صوتی و تصویری برای مخفی کردن اطلاعات بیتی است.

روش های Steganographic هستند عمدتا به روش های مبتنی بر دامنه فضایی و بر اساس دامنه فرکانس طبقه بندی می شود. در میان روش تفاضل ارزش پیکسل و روش اصلاح سطح خاکستری [5] را می توانیم ذکر کنیم. روش PVD پیشنهاد شده توسط Wu و Tsai و که ذخیره سازی مقدار زیادی از داده ها و تصویر stego غیر قابل مشاهده (تصویر که شامل اطلاعات محرمانه) را فراهم می کند. روش GLM پیشنهاد شده توسط Potdar و همکاران است [5]، اطلاعات محرمانه به مقادیر پیکسل تصویر نگاشت می کند (و جاسازی نمی کند). این استفاده از مفهوم ارزش های زوج و فرد و برای نشان دادن 0 و 1 و از جریان بیتی مخفی در تصویر است. ما هر دو روش در بخش بعدی مورد بحث قرار می دهیم. در این کار، ما با استفاده از روش GLM برای افزایش ظرفیت از روش PVD یک روش ترکیبی به دست می آوریم.

معمولا برای ارزیابی عملکرد تعبیه یک طرح جدید، دو معیار به مورد قبول است. ظرفیت داده های مخفی جاسازی شده و کیفیت تصویر stego. این ظرفیت به معنای چه مقدار داده ها در بیت و یا بایت را می توان در یک تصویر با استفاده از یک روش فرض شده و با کیفیت از stego تصویر تعبیه شده است نشان می دهد که چقدر تصاویر پس از تعبیه و یا چه مقدار اعوجاج تصویر به چشم انسان محسوس است تحریف است و توسط اندازه گیری PSNR برآورد شده است.

استگانوگرافی چیست؟

استگانوگرافی عمل مخفی سازی اطلاعات به صورت محرمانه در داخل چیزی است که به صورت معمول نشان داده میشود. استگانوگرافی اغلب برای علم رمز شناسی پیچیده و گیج کننده است به این خاطر که هر دو(چیز) در روشی که برای حفاظت اطلاعات مهم استفاده میشوند، شبیه به یکدیگر هستند. تفاوتهای بین آن دو این است که استگانوگرافی اطلاعات را مخفی میکند، اما هیچ اطلاعات مخفی شده ای را هرگز نشان نمیدهد. اگر شخص یا افرادی آن شیئ که اطلاعات درون آن مخفی شده است را ببینند ، هیچ عقیده ای در وجود داشتن اطلاعات مخفی در آن ندارند ، بنابراین آنها اقدام به رمزگشایی اطلاعات نمیکنند. استگانوگرافی از لغت یونانی استگانوس (پوشاندن) و گرافتوس (نوشتن) گرفته شده است. در دنیای امروزی استگانوگرافی به اطلاعات یا فایل مخفی شده در یک عکس دیجیتالی ، فایل تصویری یا صوتی

دانشجویان محترم:

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

اطلاق میشود. آنچه که استگانوگرافی اساسا انجام میدهد، از احساسات بشر بهره میجوید. احساسات بشری برای پیداکردن فایلهایی که در آنها اطلاعات مخفی وجود دارد ، تربیت نشده است ، با این حال برنامه های قابل دسترس زیادی وجود دارد که میتواند این کار را انجام دهد و آنالیزگراستگ نامیده میشود .(برنامه تشخیص استفاده از استگانوگرافی(رایج ترین استفاده استگانوگرافی در مخفی کردن یک فایل درون فایل دیگر است. زمانی که اطلاعات یا یک فایل درون یک فایل حامل مخفی میشود، داده ها معمولا با کلمه عبور رمزگزاری میشوند. اصطلاحات استگانوگرافی فایل حامل: فایلی که اطلاعات مخفی شده را درون خود نگه میدارد.

آنالیزگر استگ: فرایندی که اطلاعات مخفی درون یک فایل را تشخیص میدهد.

وسیله استگ: وسیله ای که در اطلاعات مخفی وجود دارد.

بیت های فراوانی: قسمتهایی از اطلاعات درون یک فایل که میتواند بدون صدمه به فایل در آن عمل اوررایت یا تغییر فایل را انجام دهد.

محل حمل (داده): اطلاعاتی که مخفی میشوند.

تاریخچه استگانوگرافی

در کل تاریخ ، استگانوگرافی برای ارتباط اطلاعاتی رمزی در بین مردم استفاده شده است.

بعضی مثالهای استفاده از استگانوگرافی در گذشته:

1-در جنگ جهانی دوم ، جوهر مخفی برای نوشتن اطلاعات محرمانه در کاغذ مورد استفاده قرار گرفت به طوری که آن تکه کاغذ برای یک آدم معمولی به عنوان کاغذ خالی سفید محسوب میشد.

در آن از موادی مانند ادرار، شیر، سرکه و آب میوه استفاده شده بود ، زیرا وقتی هر کدام از این عناصر گرم میشد ، تیره و رفته رفته از دید انسان نامرعی میشد.

2-در یونان باستان بعد از انتخاب پیکهای خبری و تراشیدن سر آنها ، سپس پیغامی را روی سر او مینوشتند.

از آنجایی که پیغام نوشته شده بر روی سر نمایان بود ، موهای پیک باید بلند میشد . بعد از اینکه موها به حالت اولیه بلند شدند ، پیک برای تحویل دادن پیام، فرستاده میشد و گیرنده بعد از تراشیدن سر پیک، پیغام را دریافت میکرد.

چگونه عمل میکند؟

روشهای عددی برای مخفی سازی اطلاعات در فایلهای عکسی، تصویری و صوتی وجود دارد.

کمترین بایت مهم) و است (LSB) . معمول ترین آنها روش در زیر در مورد این دو روش بحث شده است:

LSB زمانی که فایلها ایجاد میشوند ، همیشه بایتهایی در فایل وجود دارند که واقعا به آنها نیازی نیست ، یا حداقل مهم نیستند. این مناطق میتوانند با اطلاعاتی که باید در فایل مخفی شود ، بدون صدمه و تغییر در فایل ، تعویض شوند.

این به فرد اجازه میدهد که اطلاعات را در یک فایل مخفی کند و مطمئن باشد که هیچ کسی نمیتواند تغییرات اعمال شده در فایل را تشخیص دهد. در تصاویری که کیفیت بالا و تعداد رنگ استفاده شده بالایی دارند و در فایلهای صوتی که صداهای LSB روش متفاوتی را درون خود دارند، بهترین عملکرد را دارد.

معمولا باعث افزایش حجم فایل نمیشود، اما بسته به حجم اطلاعاتی که باید درون فایل مخفی شوند، فایل LSB روش

منابع

[1] A.Cheddad, J.Condell,and K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," Journal of Signal Processing, pp.727-752, 2010.

[2] H.Nyeem,“Developing a digital image watermarking model” In International Conference on Digital Image Computing Techniques And Applications (DICTA), pages468-473,2011

[3] C.A.Stanley,”Pairs of Values and the Chi-squared Attack”,http://www.math.iastate.edu/thesisarchive/MSC/StanleyMSCSS05.pdf , Department of Mathematics”, Iowa State University May 1, 2005

[4] D.C.Wu. and W.H.Tsai, , “A Steganographic Method for Images by Pixel-Value Differencing,” Pattern Recognition Letters 24, pp. 1613 – 1626, 2003.

[5] V.Potdar and E.Chang , ”Gray level modification steganography for secret communication.” In IEEE International Conference on Industrial Informatics, pages 355–368, Berlin, Germany, 2004

[6] K.Chang., C. Chang., P.S. Huang., and T.Tu,: “A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing”, Journal of Multimedia ,VOL. 3, NO. 2, JUNE 2008

[7] S.L.Li, K.C. Leung, L.M.Cheng, and C.-K. Chan,“Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing,” First International Conference on Innovative Computing, Information and Control (ICICIC'06), Vol. 3, pp. 58-61, 2006.

[8] A.T.Al-Taani. and AM.AL-Issa. A novel steganographic method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3, 2009.

[9] R.Yadhav ,”Information Security Using Blend of Steganography and Cryptography”, International Journal of Computer Technology and Applications., Vol 2 (6), 2023-2036

[10] S.Mohamed ”Automatic evaluation of real-time multimedia quality: a neural network approach”. Rennes: University of Rennes I; 2003.

[11] A.N.Netravali and BG.Haskell. ” Digital pictures: representation, compression, and standards”. 2nd ed. New York, NY:Plenum Press; 1995.