استگانوگرافی

سعید زمهریرلو

معرفی

استگانوگرافی موضوعی است که به ندرت از طریق هواخواهان امنیتی فن آوری اطلاعات مورد توجه قرار گرفته است .
اغلب مردم از موضوع استگانوگرافی بی خبرند و حتی نمیدانند استگانوگرافی چیست.
امیدوارم از طریق این مقاله به سوالات هر کسی که میخواهد بیشتر راجع به استگانوگرافی بداند ، پاسخ دهم و به مردم بیاموزم که میتوانند پی ببرند که استگانوگرافی دقیقا چیست. آیا استگانوگرافی یک تهدید محسوب میشود؟

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 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 .

www.hajarian.com

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:

۱- 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 .

۲- 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 .

معمول ترین آنها روش LSB (کمترین بایت مهم) و تزریق است .

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 .

روش LSB در تصاویری که کیفیت بالا و تعداد رنگ استفاده شده بالایی دارند و در فایلهای صوتی که صداهای متفاوتی را درون خود دارند، بهترین عملکرد را دارد .

روش LSB معمولا باعث افزایش حجم فایل نمیشود، اما بسته به حجم اطلاعاتی که باید درون فایل مخفی شوند، فایل میتواند به صورت قابل ملاحظه ای دارای افت و اعواج شود .

تزریق

تزریق روش ساده ای است که به طور ساده و مستقیم اطلاعات مخفی را در فایل حامل تزریق میکند .

مشکل اصلی این روش این است که میتواند به میزان قابل ملاحظه ای باعث افزایش حجم فایل شود .

استگانوگرافی در تصاویر

در مخفی سازی اطلاعات در تصاویر معمولا از روش LSB استفاده میشود .

بهترین تصاویر جهت مخفی سازی اطلاعات در آنها ، تصاویر ۲۴ بیت Bitmap هستند . به این دلیل که بزرگترین نوع فایل و با کیفیت ترین فایل تصویری محسوب میشود . وقتی یک فایل تصویری دارای ضرفیت و کیفیت بالای تصویری است ، بسیار راحت میتوان اطلاعات را در آن مخفی کرد .

اگرچه تصاویر ۲۴ بیتی بهترین گزینه برای مخفی سازی اطلاعات هستند ، اما برخی افراد ترجیح میدهند از تصاویر ۸ بیتی یا در حد ممکن از دیگر فرمتهای تصویری برای مخفی کردن اطلاعات در آن استفاده کنند ، به این دلیل که ارسال یک تصویر حجیم در اینترنت ، مستلزم صرف زمان بیشتری میباشد .

مهم است که یادتان باشد اگر شما اطلاعاتی را درون یک فایل تصویری مخفی کردید و فرمت آن فایل به یک فایل تصویری دیگر تغییر یافت ، به احتمال بسیار زیاد اطلاعات مخفی شده در فایل از بین خواهد رفت .

استگانوگرافی در صوت

درزمان مخفی سازی اطلاعات درون یک فایل صوتی ، تکنیک استفاده شده معمولا رمزگزاری سطح پایین بیتی است که چیزی شبیه به LSB است که در تصاویر استفاده میشد .

مشکل رمزگزاری سطح پایین بیتی در این است که معمولا توسط حس شنوایی مردم به صورت مشخص ، قابل تشخیص است ، بنابراین برای کسانی است که میخواهند اطلاعات را در فایل صوتی مخفی کنند، یک روش ریسکی است .

انتشار طیف روش دیگری برای مخفی سازی اطلاعات در فایل صوتی است .

این روش با اضافه کردن صداهای تصادفی به سیگنال ، اطلاعات را در فایل حامل مخفی کرده و طیفی را در طول فرکانس منتشر میکند .

مخفی سازی داده Echo روش دیگری برای مخفی سازی اطلاعات در فایل صوتی میباشد .

این روش از Echoهای فایل صوتی برای مخفی سازی اطلاعات استفاده میکند .

بوسیله اضافه کردن صدای اضافی در داخل یک echo در فایل صوتی، اطلاعات میتواند مخفی شود .

این روش به این دلیل از دیگر روش ها برتر است که میتواند در عمل باعث بهبود کیفیت صدا در داخل فایل صوتی شود .

استگانوگرافی در تصاویر ویدیویی

در مخفی سازی اطلاعات درون فایل ویدیویی ، فرد یا شخصی که اطلاعات را مخفی میکند ، معمولا از روش DCT استفاده میکند .

DCT به صورت اعمال کمی تغییرات در هر تصویر از ویدیو، فقط به اندازه ای که از دید مردم محسوس نباشد، عمل میکند. برای دقیقتر شدن در کار DCT ، DCT با اعمال تغییرات درمقادیر بخشهای معین شده ای از تصویر، معمولا آنها را گرد میکند .

به عنوان مثال اگر بخشی از تصویر دارای مقدار ۶٫۶۶۷ باشد ، آن را به ۷ گرد میکند .

استگانوگرافی در ویدیو همانند استگانوگرافی در تصاویر است ، چون فریم های ویدیو که همان تصاویر هستند را تغییر میدهد .

وقتی تنها اطلاعات کمی در فایل ویدیویی مخفی شد ، معمولا قابل تشخیص نیست، به هر حال هر چقدر اطلاعات بیشتری مخفی شوند ، قابل تشخیص تر خواهند بود .

استگانوگرافی در اسناد

آیا استگانوگرافی میتواند در اسناد استفاده شود؟ بله، درست است !

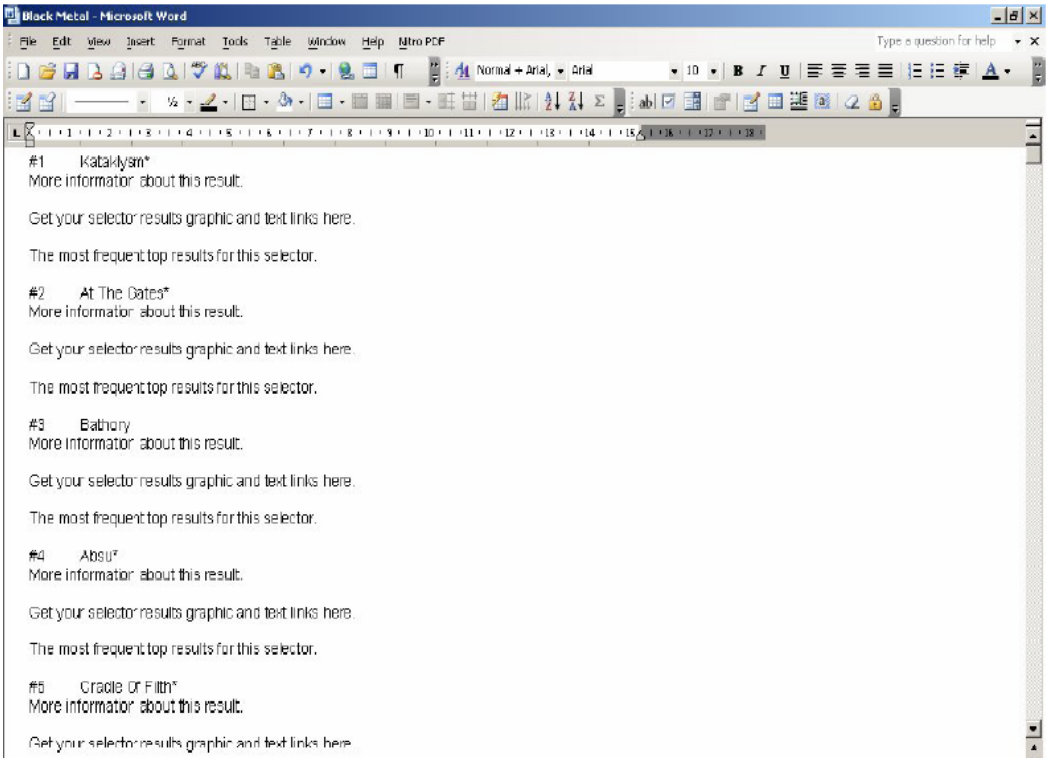
برای استفاده استگانوگرافی در اسناد از اضافه کردن ساده فضای سفید در انتهای خطوط یک سند استفاده میشود .

این نوع از استگانوگرافی بینهایت مؤثر است ، زیرا استفاده از فضای سفید همیشه از دید مردم ، حداقل در بیشتر ویرایشگرهای متنی ، نامرعی باقی میماند .

فضای سفید به طور طبیعی در اسناد ایجاد میشود ، به طوری که عملا روش ممکنی وجود ندارد که مانند این روش، هیچ کس به آن مشکوک نشود .

رایج ترین تکه برنامه برای انجام این نوع استگانوگرافی ، تکه برنامه ای به نام SNOW است .

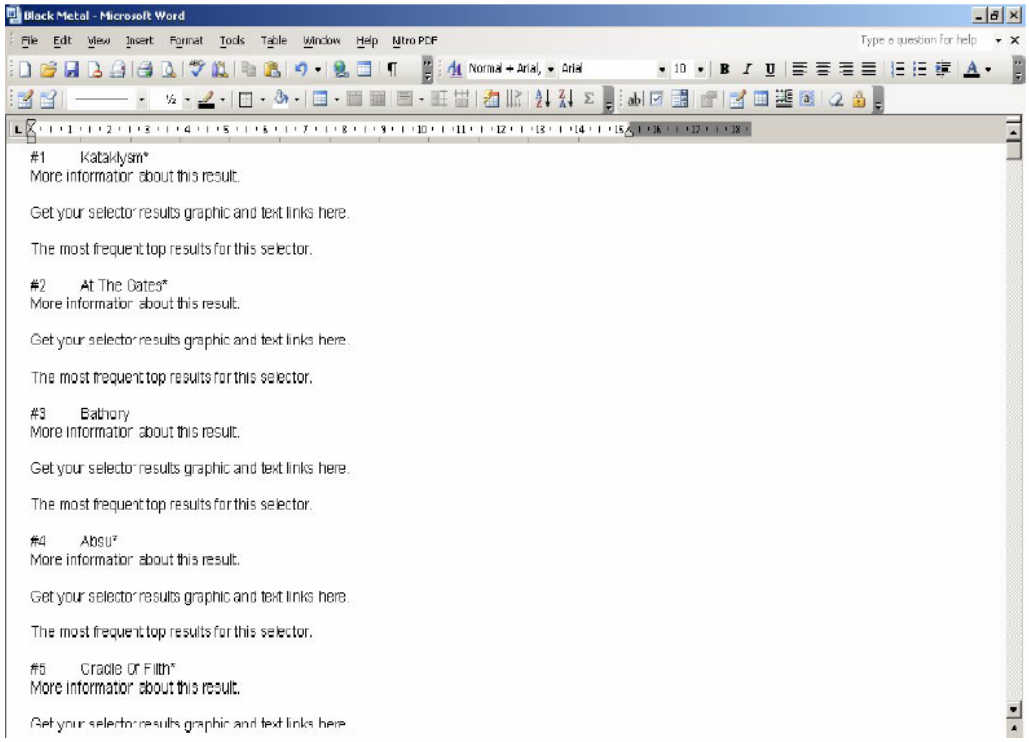
در زیر تصویری از متن، قبل از استفاده از SNOW قرار گرفته است:



اکنون من از SNOW برای مخفی سازی پیغامی در داخل سند استفاده کرده ام .

کاری که من کردم این بود که کلمه Aelphaeis را با کلمه عبور Zone-h را در سند مخفی کردم.

در زیر تصویری از سندی که بعد از استفاده از SNOW نشان داده شده است را ملاحظه میکنید :



همان طور که ملاحظه میکنید ، هیچ تفاوت قابل تشخیصی ، بین دو سند وجود ندارد .

ما با استفاده از SNOW دستور زیر را وارد میکنیم :

snow -C -p "Zone-H" C:\Black_Metal_Steg.doc C:\Hidden_Message.doc

از نظر دانش من ، هیچ راهی برای تشخیص استگانوگرافی در اسناد وجود ندارد .

تشخیص استگانوگرافی

هنر تشخیص استگانوگرافی ، به عنوان آنالیزاستگ یاد میشود ، که برای تشخیص استگانوگرافی موجود در یک فایل استفاده میشود .

روشهای زیادی برای تشخیص استگانوگرافی وجود دارند:

مشاهده آن فایل و مقایسه آن با دیگر کپی آن فایل از طریق پیداکردن آن در اینترنت.

معمولا کپی های چندگانه ای از تصاویر در اینترنت وجود دارند، به طوری که شما میتوانید چند تا از آنها را جهت مقایسه با فایل مشکوک به کار گیرید .

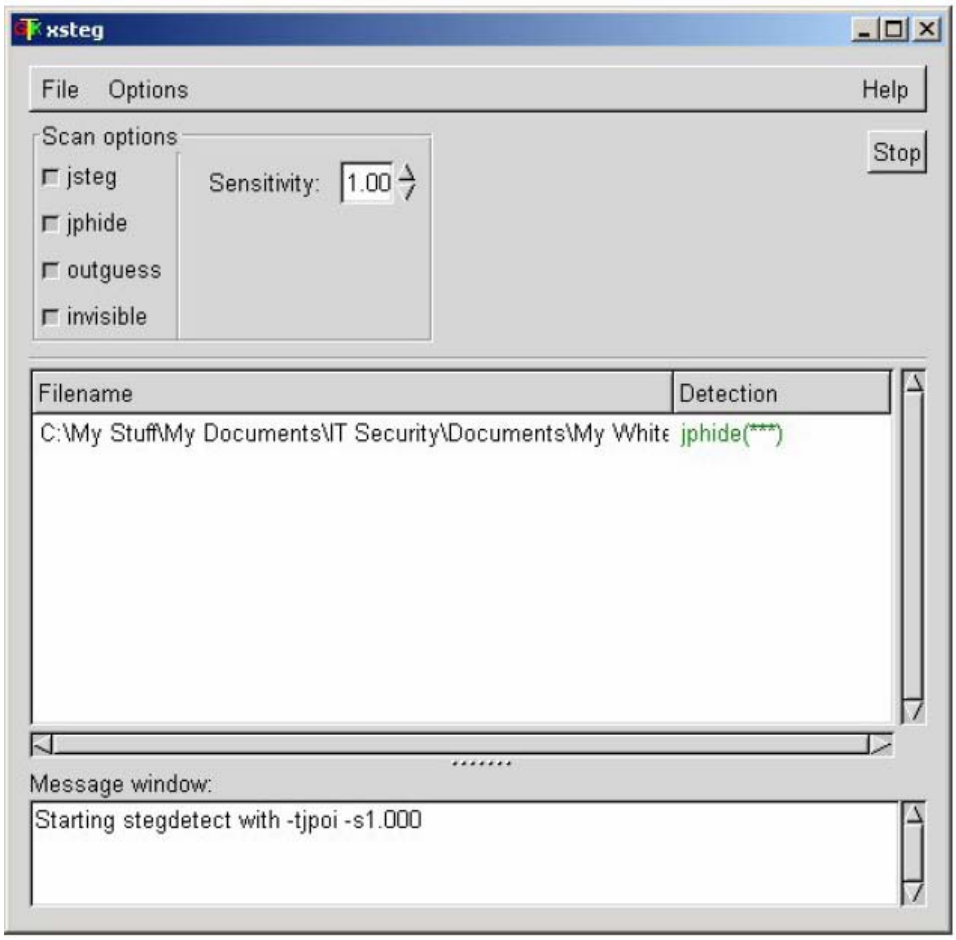
به عنوان مثال اگر شما یک فایل Jpeg را دانلود کردید و فایل مشکوک هم Jpeg بود و دو فایل ، از واقعیت فاصله داشتند ، یکی از دیگری بزرگتر است . احتمال اینکه فایل مشکوک شما اطلاعات مخفی در درون خود داشته باشد زیاد است .

گوش کردن به یک فایل .

این روش مانند روش بالا است و سعی در تشخیص استگانوگرافی در فایل تصویر دارد .

اگر شما سعی در تشخیص استگانوگرافی در یک فایل صوتی دارید ، شما نیازمند این هستید که فایل یکسانی را برای مقایسه پیدا کنید که از همان فرمت صوتی استفاده میکند (برای مثال MP3) . همین روش برای پیدا کردن اطلاعات مخفی در فایل تصویری هم استفاده میشود .

نمونه ای از تصویر نرم افزار تشخیص استگانوگرافی:



ابزارهای استگانوگرافی

MP3Stego

این نرم افزار اطلاعات را در فایل های MP3 مخفی میکند . داده ها ابتدا فشرده شده ، سپس رمزگزاری شده و در فایل قرار میگیرند .

http://www.petitcolas.net/fabien/software/MP3Stego_1_1_17.zip

JPHide and JPSeek

این ها برنامه هایی هستند که برای پنهان سازی اطلاعات در تصاویر Jpeg استفاده میشوند .

نسخه های متفاوتی از این نرم افزار موجود است . به سایت زیر جهت دانلود برنامه رجوع کنید :

http://www.snapfiles.com/php/download.php?id=101911

StegoVideo

این برنامه اجازه میدهد که هر نوع فایلی را در فایل ویدیویی مخفی کنید.

http://compression.ru/video/stego_video/index_en.html

نتیجه:

استگانوگرافی هرگز تهدیدی عمومی برای بشر به شمار نمی آید و من اعتقاد ندارم که ممکن است برای مقاصد شوم مورد استفاده قرار بگیرد .

من عقیده دارم که استگانوگرافی برای مخفی سازی اطلاعات محرمانه و انتقال آنها از محلی به محل دیگر است .

مردم باید بر تاثیرات استگانوگرافی تمرکز کرده ، و بدانند واقعا برای چه از آن استفاده کنند .

منبع:

zone-h
unrestricted information

http://zone-h.org

© Copyright Zone-H.Org 2006