



نهای نگاری در تصاویر

تألیف :

ابوالفضل قره سوفر

علی رفیعی شهرکی

انتشارات دانشگاه علوم دریایی امام خمینی (ره)

۱۳۹۷



- سرشناسه : قره‌سوفلو، ابوالفضل، ۱۳۶۵ -
- عنوان و نام پدیدآور : نهان‌نگاری در تصاویر / تألیف ابوالفضل قره‌سوفلو، علی رفیعی شهرکی.
- مشخصات نشر : نوشهر: دانشگاه علوم دریایی امام خمینی (ره)، ۱۳۹۷.
- مشخصات ظاهری : ۱۶۵ ص.: مصور، جدول، نمودار.
- شابک : ۹۷۸-۶۰۰-۷۹۴۱-۵۸-۴
- وضعیت فهرست نویسی : فیفا
- یادداشت : در نام: ۱۵۷ - ۱۶۵.
- موضوع : رمزنگاری
- موضوع : cryptography
- موضوع : فایل‌های تصویری - تدابیر ایمنی
- موضوع : Images files -- Security measures
- موضوع : تعقیب‌نگاری رقیمی
- موضوع : Digital watermarking
- شناسه افزوده : رفیعی شهرکی، علی، ۱۳۶۴ -
- شناسه افزوده : دانشگاه علوم دریایی امام خمینی (ره)
- شناسه افزوده : Imam Khomeini Naval University of Noshahr
- رده بندی کنگره : ۱۳۹۷ ۴۶۶ن۹ / ۱۰۳ Z
- رده بندی دیویی : ۶۵۲/۸
- شماره کتابشناسی ملی : ۴۷۹۸۴۶۷
- نام کتاب : نهان‌نگاری در تصاویر
- تألیف : ابوالفضل قره‌سوفلو، علی رفیعی شهرکی
- ناشر : دانشگاه علوم دریایی امام خمینی (ره)
- نوبت چاپ : چاپ اول
- تاریخ انتشار : ۱۳۹۷
- تیراژ : ۵۰۰
- قیمت : ۲۰۰۰۰۰ ریال
- حروفچینی، چاپ و صحافی : انتشارات دانشگاه علوم دریایی امام خمینی (ره)

پیشگفتار

از زمانی که انسان ها قادر به ارتباط با یکدیگر شدند امکان برقراری ارتباط مخفیانه یک خواسته مهم افراد بوده است. گسترش روز افزون اینترنت و رشد سریع استفاده از آن، انسانها را به سوی جهان دیجیتال و ارتباط از طریق داده های رقومی سوق داده است. در این میان امنیت ارتباطات یک نیاز مهم است و هر روزه نیاز به آن بیشتر احساس می شود. به طور کلی دو شیوه ارتباط نهانی وجود دارد. در روش اول که رمزنگاری است اطلاعات به طریقی رمز می شود که برای شخص ثالث قابل فهم نیست اما فرستنده و گیرنده با استفا از کد مشترک می توانند اطلاعات مورد نظر را رمزگشایی کنند. نهان نگاری شیوه دوم ارتباط محرمانه است. در نهان نگاری علاوه بر مخفی ماندن اطلاعات، وجود ارتباط محرمانه باید مخفی بماند. در واقع در نهان نگاری هنر و علم نهان کردن ارتباطات است و هدف آن، مخفی کردن وجود هر گونه ارتباط بین فرستنده و گیرنده است. اغلب اوقات تصور می شود که با کد کردن پیام مورد مبادله، ارتباط امن است اما در عمل بعضی ایرادات تنها رمز کردن کافی نیست و به همین دلیل روش هایی برای نهان کردن داده به جای کد کردن آن ارائه شده است.

نهان نگاری از لحاظ لغوی به معنی «نوشته استتار شده» است و به راز نهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوششی است به گونه ای که کمترین تغییر قابل آشکاف را در آن ایجاد نماید و نتوان موجودیت پیام نهان در رسانه را حتی به صورت احتمالی آشکار ساخت.

اگر چه رمز نگاری و احراز هویت نیز مفاهیمی مشابه نهان نگاری دارند، اما تفاوت هایی بین آن ها وجود دارد. در رمز نگاری دسترسی به محتوا پیام برای فرد غیر مجاز ناممکن می گردد. لیکن در نهان نگاری موجودیت پیام انکار می شود. هدف رمز نگاری حفظ محرمانگی و تمامیت پیام است که با رمز کردن آن حاصل می شود. نهان نگاری هم همین اهداف را با نهان نمودن پیام دنبال می کند. بعلاوه در نهان نگاری انتخاب جا و ترتیب نهان نمودن پیام نیز با بهره گیری از نوعی رمز در چینش بیت های پیام لا به لای بیت های میزبان صورت می پذیرد. همچنین می توان پیام را قبل از جاسازی داخل میزبان با استفاده از الگوریتم های رمز نگاری به صورت رمز در آورد و سپس عمل نهان سازی را انجام داد. بطوریکه می توان گفت با استفاده از نهان نگاری در حقیقت سه لایه حفاظتی بسیار محکم در دسترسی به پیام ایجاد خواهد شد: اول اینکه وجود ارتباط نامحسوس است و این هدف اصلی در نهان نگاری است و بنابراین گذشتن از اولین مانع کار چندان ساده ای نخواهد بود. در صورتیکه وجود اطلاعات

در یک میزبان مورد سوء ظن واقع شود مرحله دوم پیدا کردن الگوریتم نهان نگاری است و باید جا و ترتیب نهان شدن اطلاعات مشخص شود. لیکن در این مرحله نیز چون از یک کلید به نام stego-key برای جاسازی پیام استفاده شده است دانستن این کلید ضروری است و بنابراین گذشتن از این مرحله نیز با دشواری همراه بود و چنانچه دو مرحله قبلی با موفقیت پشت سر گذاشته شوند، اکنون به متن رمز شده دسترسی پیدا شده است که در این مرحله مسائل مربوط به رمز نگاری مطرح می گردند. از طرف دیگر با عمل اضافه کردن نشانه ای در عکس، ویدئو یا صدا برای نشان دادن هویت آن اثر نیز نهان نگاری یا راز هویت می گویند. البته نهان نگاری و احراز هویت کمی با یکدیگر تفاوت دارند، وقتی نشانه تجاری یا مشخصه ای در یک اثر مانند عکس، ویدئو یا صدا به شکل مخفیانه ذخیره می شود به آن نهان نگاری می گویند، با مخفی کردن شماره سریال یا یک مشخصه از یک چیز در چیز مشابه دیگر را احراز هویت می نامند. هر وی این روش ها برای جلوگیری از دزدی آثار بکار می روند، از دومی برای پیدا کردن ناقصین کپی رایت و از اولی برای اثبات آن استفاده می شود.

از سوی دیگر در برابر نهان نگاری، دانش تحلیل زبان نگاری، هنر کشف وجود ارتباط نهان، قرار دارد که هدف آن تمیز دادن بین رسانه های حاوی اطلاعات از رسانه عادی است. همانگونه که نهان نگاری از اهمیت بسیاری برخوردار است داشتن دانش تحلیل نهان نگاری نیز بسیار مهم و ضروری است چرا که علی رغم امتیازهای مثبتی که نهان نگاری دارد امکان سوء استفاده از آن برای مقاصد خرابکارانه نیز وجود دارد.

با پیشرفت فناوری امکان مخفی کردن اطلاعات با حجم زیاد افزایش یافت. آسانی ها میکروودات ها را که عکس های بسیار کوچکی در اندازه یک نقطه بودند و اطلاعات مختلفی مانند عکس و متن را در خود جای می دادند، اختراع کردند.

اندازه بسیار کوچک این عکس ها امکان نوشتن یک متن ساده با آن ها را فراهم می کند و اینگونه بر روی خطوط یک کلمه می توان اطلاعات زیادی را جاسازی کرد.

در آن زمان بازار فرستادن متن ها به این روش ها آتچنان گرم شده بود که محدودیت های زیادی برای ارسال متن و حتی عکس اعمال می شد. محدودیت هایی که امروزه بسیار بی معنی می باشند. در آمریکا پست شطرنج، نقشه های بافندگی، تکه های روزنامه و حتی نقاشی کودکان ممنوع بود. حتی فرستادگان گل در انگلستان و آمریکا ممنوع شد.

اما در قرن بیستم که حقیقتاً نهان نگاری شکوفا شد. در زمان کامپیوتر نهان نگاری پیشرفت حیرت انگیزی داشت. روش های قدیمی مخفی کردن در عکس با ورود کامپیوترهای پر قدرت نیرو گرفتند. و روز به روز بر تعداد مقالات و محققینی که در این زمینه فعالیت میکردند افزوده شد. در سالهای اخیر، با توجه به پیشرفت قابل توجه ارتباطات دیجیتال نظیر اینترنت نگاه دوباره ای به نهان نگاری در رسانه های دیجیتال شده است. این شاخه از علم، کاربردهای متعددی نظیر حق رونوشت، امنیت تجارت الکترونیکی، سرویس های بلادرنگ، ارتباطات نهانی، محفوظ نگه داشتن اطلاعات خاص نظیر اطلاعات بیمار در تصاویر پزشکی و... پیدا کرده است.

تألیف:

ابوالفضل قره سوفلو، علی رفیعی شهرکی

فصل اول: مفهوم نهان نگاری و رمز نگاری

سیر تاریخی نهان نگاری اطلاعات یا استگانوگرافی.....	۱۶
مدل کلاسیک نهان نگاری.....	۱۸
مسأله زندانی.....	۲۰
اصل کرکاف در نهان نگاری.....	۲۶
سه استاندارد اصلی امنیت شده.....	۲۷
تاریخچه رمز نگاری.....	۲۹
اصول ششگانه کرکف در رمز نگاری.....	۳۰
رمز نگاری پیشرفته.....	۳۱
پروتکل رمز نگاری.....	۳۴
الگوریتم رمز نگاری.....	۳۵
رمز نگاری کلید متقارن.....	۳۷
رمز نگاری کلید نامتقارن.....	۳۸
مقایسه رمز نگاری کلید متقارن و کلید نامتقارن.....	۳۸
تجزیه و تحلیل رمز.....	۳۹
رمزهای جانشینی.....	۴۰
افزونگی.....	۴۰
رمز نگاری به صورت سخت افزاری.....	۴۲
الگوریتم های کلید عمومی.....	۴۲
امضاهای دیجیتالی.....	۴۴
تفاوت نهان نگاری و رمز نگاری.....	۴۶
کاربردهای نهان نگاری.....	۴۷
نقطه ضعف نهان نگاری.....	۴۹

صفحه	عنوان
۵۰	نهان نگاری و امنیت
۵۳	دسته بندی روش های نهان نگاری از نظر مقاومت
۵۵	مروری کلی بر نهان نگاری

فصل دوم: روش های نهان نگاری

۷۸	نهان نگاری در تصویر
۷۸	تعریف تصویر
۷۹	فشرده سازی تصویر
۸۲	نشان گذاری
۸۳	تفاوت های نهان نگاری و نشان گذاری
۸۴	انواع سیستم های نشان گذاری
۸۶	دسته بندی کلی روش های نهان نگاری
۹۰	دسته بندی روش های نهان نگاری تصویر از نظر حوزه
۹۴	LSB و تصاویر دارای جعبه رنگ
۹۹	نهان نگاری JPEG
۱۰۵	روش LSB در تصاویر رنگی ۲۴ بیتی

فصل سوم: پیاده سازی روش LSB

۱۱۲	مقدمه
۱۱۳	تابع $LSB \rightarrow Encode$
۱۱۷	تابع $LSB \rightarrow Decode$
۱۲۰	تابع numtobin
۱۲۱	تابع bintonum

۱۲۱.....	تابع psnr
۱۲۲.....	نتایج پیاده سازی

فصل چهارم: نهان کاوی (تحلیل نهان نگاری)

۱۲۸.....	مقدمه
۱۲۹.....	انواع نهان کاو
۱۳۰.....	نهان کاوی مبتنی بر یادگیری نظارتی
۱۳۲.....	نهان کاوی مبتنی بر تشخیص کوا
۱۳۴.....	نهان کاوی آماری پارامتری
۱۳۶.....	روش های نهان کاوی ترکیبی
۱۳۶.....	انواع حملات نهان کاوی
۱۳۷.....	معیارهای ارزیابی کارایی روش های نهان کاوی
۱۳۹.....	ارزیابی نهان کاو مبتنی منحنی ROC
۱۴۰.....	روش های حمله نهان نگاری
۱۴۵.....	بررسی چند تکنیک نهان کاوی در حوزه مکان
۱۵۴.....	بازیابی پیام
۱۵۴.....	انکار نهان نگاری
۱۵۵.....	ابزارهای موجود برای تحلیل نهان نگاری

منابع و مآخذ

۱۵۷.....	منابع
----------	-------