دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش:الکترونیک

عنوان:پنهانگاری اطلاعات در تصاویر با فرمت jpeg

استاد راهنما:مصطفی چرمی

نگارش:پوریا کرمی

تیر ماه ۱۳۹۲

فهرست مطالب

فصل اول :

کلیات پنهان سازی اطلاعات

۱-۱)مقدمه

رمز نگاري از دير باز به عنوان يك ضرورت براي حفاظت از اطلاعات خصوصي در مقابل دسترسي هاي غير مجاز در تجارت، سياست و مسايل نظامي وجود داشته است. به طور مثال تلاش براي ارسال يك پيام سرّي بين دو هم پيمان به گونه اي كه حتي اگر توسط دشمن دريافت شود نيز قابل درك نباشد. در ساليان اخير رمز نگاري و تحليل رمز از يك هنر پا را فراتر گذاشته و يك علم مستقل شده است و در واقع به عنوان يك وسيله عملي براي ارسال اطلاعات محرمانه روي كانال هاي غير امن همانند اينترنت، تلفن، ماكرويو و ماهواره ها شناخته مي شود. البته با پيشرفت تكنولوژي اطلاعات، نياز به روش هاي ديگري احساس شد كه در آن ها همانند رمز نگاري، وجود اطلاعات محرمانه و پنهاني، علني و واضح نباشد يكي از اين دسته روش ها، تكنيك هاي پنهان نگاري هستند.

پنهان نگاري به علم ارتباطات غير قابل مشاهده اشاره مي كند. بر خلاف رمزنگاري، كه هدف امنيت اطلاعات است، پنهان نگاري به دنبال مخفي كردن خود پيام از ديد ديگران است. در پنهان نگاري، معمولاً سه عامل مورد بررسي قرار مي گيرد و سعي مي شود كه با توجه به كاربرد و پيش فرض ها و ديگر شرايط موجود، هر يك از اين سه عامل در حد مورد نياز رعايت شوند. اين عوامل عبارتند از :

1) ظرفيت

2) نا محسوس بودن [1]

3) مقاومت [2]

1) **ظرفیت :** این عامل، مشخص کننده ي ظرفت پنهان سازي روش پیاده شده است، به این صورت که همیشه سعي مي شود در يك الگوريتم پنهان نگاري، تا جاي ممكن ظرفيت را براي پنهان كردن داده ها در شيء پوشانه افزايش داد.البته بايد توجه داشت كه اين افزايش بايد به گونه اي متعادل انجام گيرد. به طور كلي، روش هاي مختلف پنهان نگاري سعي مي كنند كه ظرفيت پنهان نگاري را تا جاي ممكن، با حفظ ديگر عوامل افزايش دهند.

2) **نامحسوس بودن :** مشخص كننده توانايي الگوريتم پنهان نگاري در نهان كردن داده ها در شي ميزبان است، به طوري كه باعث جلب توجه نشود، به عبارت ديگر، بايد به گونه اي عمل پنهان سازي انجام گيرد كه كيفيت اوليه شي ميزبان، تا حد ممكن حفظ شود و اين حفظ كيفيت اوليه شي ميزبان باعث شود كه داده هاي مخفي شده كمتر مشخص شوند. به همين دليل نامحسوس بودن و كيفيت تقريباً بيانگر يك مفهوم هستند. البته روش هاي ديگري نيز براي ايجاد امنيت به طور مستقل وجود دارند، مانند رمز نگاري داده ها، كه به دليل رمزنگاري به صورت مستقل از كيفيت شيي گنجانه عمل مي كند، مي توان آن را صرفاً روشي براي امنيت بيشتر در صورت شكست خوردن روش پنهان نگاري در نظر گرفت .

۳) مقاومت : در پنهان نگاري مقاومت عبارت است از ايستادگي الگوريتم نسبت به روش هاي مختلف پنهان شكني [3] . به عبارت ديگر، روش هاي پنهان نگاري بايد تا جاي ممكن به گونه اي طراحي و پياده سازي شوند كه توانايي ايستادگي ومقاومت را در مقابل روش هاي مختلف پنهان شكني، كه به منظور آشكار سازي داده هاي مخفي شده به كار مي روند، داشته باشند.

---

1. Imperceptibilitg
2. Robustness
1. Stegan nalysis

براي مثال، هيستوگرام يا توزيع هاي آماري، از جمله روش هاي متداول براي پنهان شكني هستند.

به طور كلي، در طراحي يك سيستم پنهان نگاري مناسب بايد سعي شود كه با توجه به كاربردها و نيازهاي موجود، و هم چنين تهديدهاي بالقوه، تعادلي را بين 3 عامل ياد شده برقرار كرد. البته بايد به اين نكته توجه داشت كه پارامترهاي ياد شده را مي توان به صورت سه رأس يك مثلث در نظر گرفت كه در تقابل با يكديگر هستند. يعني افزايش هر يك از عوامل، منجر به كاهش عامل ديگر مي شود .

بنابراين بايد سعي كرد تعادل را در بين عوامل نامبرده برقرار كرد.

شكل ۱-۱. مثلث پنهان‌نگاری و عوامل اصلی.

تأكيد اصلي ما بر بررسي دو عامل متقابل ظرفيت و نامحسوس بودن در روش هاي پنهان نگاري مختلف قرار دارد. در روش هاي بررسي شده، دو عامل ظرفيت پنهان سازي داده ها و نا محسوس بودن (كيفيت) تصاوير گنجانه را با توجه به مقدار PSNR به دست آمده براي آن ها در نظر مي گيريم، و بيشينه كردن اين دو ويژگي در روش هاي پنهان نگاري نامبرده و هم چنين پياده سازي نرم افزاري روش هاي ياد شده از اهداف مورد نظر خواهد بود. در ضمن، بر اساس مشخصاتي كه براي يك سيستم پنهان نگاري تعريف شده است، در صورتي كه عمليات انجام گرفته نامحسوس باشند، معمولاً حمله به سيستم منتفي مي شود و امنيت سيستم

ارتقاء مي يابد و مقاومت سيستم نسبت به حملات از حالت بحراني (از نظر اهميت) خارج مي شود. ولي اين عامل در روش هاي نشانه گذاري هم چنان داراي اهميت بالايي است.

در رمز نگاري، براي جلوگيري از دسترسي غير مجاز به محتواي پيام، آن را تغيير مي دهند، به طوري كه اين پيام غيرقابل درك، براي اشخاص مجاز با استفاده از يك كليد سرّي قابل بازسازي است و اطلاعات به راحتي استخراج مي شوند. ولي براي افراد غير مجاز ، دستيابي به اطلاعات رمز شده بدون داشتن كليد و الگوريتم رمز نگاري تقريباً غير ممكن است.

اشكال عمده ي رمز نگاري اين است كه اگر شخص ثالثي در خلال ارسال اطلاعات پي به وجود اطلاعات محرمانه ببرد، حتي اگر به دليل رمز نگاري قوي نتواند به اين اطلاعات سرّي دست پيدا كند، مي تواند از رسيدن پيام به مقصد جلوگيري كند، بيائيد از ديدگاه ديگري به مسئله نگاه كنيم. اگر بتوان اطلاعات را به گونه اي فرستاد كه شخص ثالث متوجه فرآيند فرستادن اطلاعات سري نشود، اين كار باعث افزايش امنيت و محرمانه ماندن پيام خواهد شد.

در واقع، پنهان نگاري به دنبال اين امر است. در ادامه ي اين فصل، ابتدا تاريخچه كوتاهي از پنهان نگاري و مخفي كردن اطلاعات را بيان مي كنيم و سپس مفاهيم كلي مربوط به اين زمينه و تعاريف مربوط ارائه مي شوند. سپس به چند نمونه از روش هاي پنهان نگاري در حوزه مكان اشاره خواهيم كرد.

۱-۲) تاريخچه : استفاده از مخفي سازي اطلاعات داراي سابقه اي طولاني است. سربازان يوناني براي انتقال پيام به جاي آن كه طبق روال عادي پيام را روي موم كشيده شده بر روي لوح بنويسند، پيام را روي خود لوح حك مي كردند و سپس آن را با موم مي پوشاندند و روي موم يك پيام عادي را مي نوشتند.

همان طور كه مورخ مشهور يوناني هردوتس در سال 499 قبل از ميلاد نوشته بود، در ميانه ي جنگ با ايراني ها فرمانروا ميلتوس خواست پيامي را به دوستش آريستاگروس بفرستد تا يوناني ها را تحريك كند كه عليه فرمانروايي ايراني شورش كنند. به منظور فريب دادن نگهبانان ايراني، او سر معتمد ترين خدمتكار خود را تراشيد و پيام را روي آن خالكوبي كرد.

پس از اين كه موهاي وي رشد كرد، او مي توانست بـه راحتـي از سرزمين هـاي دشمن عبور كنـد و در مقصـد بـا تراشـيدن موهـاي سـر وي پيغـام اسـتخراج مـي شـد. همچنـين، اسـتفاده از جوهرهاي نامرئي از زمان هاي بسيار دور در نقاط مختلف دنيا مرسوم بوده است. اين گونـه روش ها ، يعني نوشتن مخفي در جنگ جهاني اول نيز مورد استفاده آلماني ها قرار گرفت.

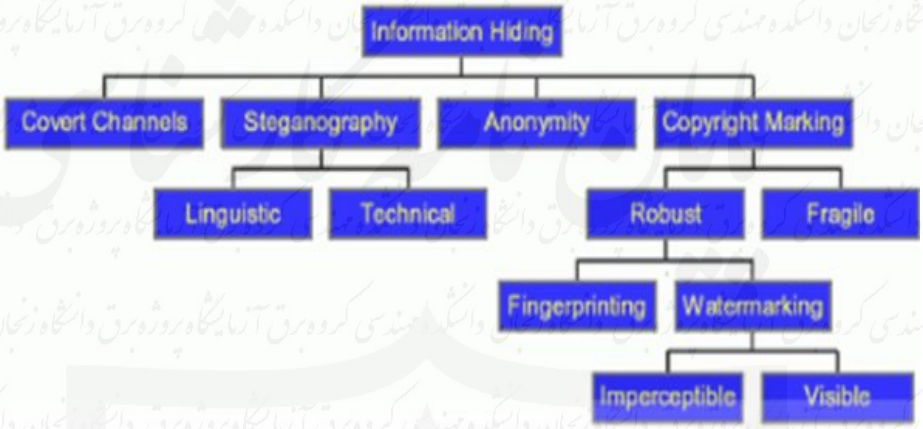
در طول دهه ي 1980 مارگارت تاچر كه از نشت اطلاعات و اسناد محرمانـه كابينـه اش بسيار ناراحت بود، توانست با استفاده از يك پردازشگر كلمات ، مشخصـات هر وزير را در فاصله بين كلمات به نحوي ثبت و وزراي خائن را از اين طريق شناسايي كند

يكي از پيشگامان پنهان نگاري و رمزنگاري ، ژوهانس ترتيميوس[1] (1462 – 1526) يك روحاني آلماني بود. اولين كار وي بر روي پنهان نگاري " Steganographia " نـام داشت كه درباره ي سيستم هاي جادو و پيشگويي توضيحاتي داده بود. هم چنين در آن كتـاب (شكل 1-2) درباره سيستم هاي پيچيده رمز نگاري هم مطالبي يافت مي شد. اين كتـاب در زمـان وي منتشر نشد، زيرا وي از فاش شدن اسرارش مي ترسيد .

شكل ۱-۲. Johannes Trithemius و نمونه ای از كتاب هايش.

[1] . Johannes Trithemius

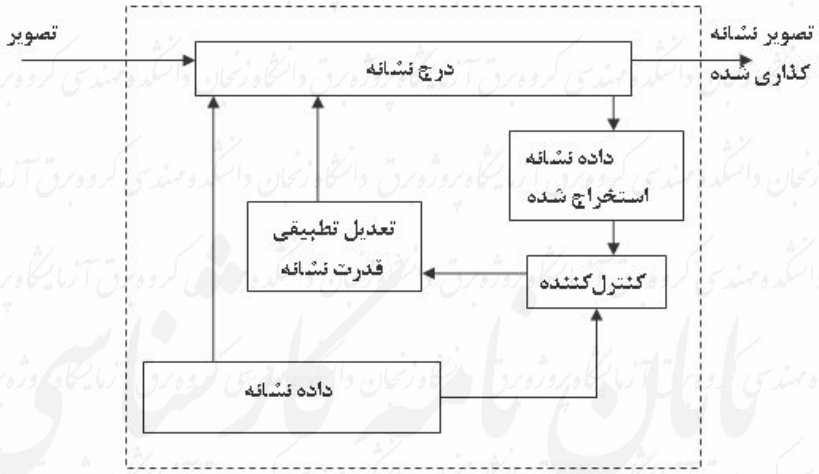
هم چنين در شكل 1-3 مي توانيد ديا‌گرامي رسمي را ، كه در اولين كارگاه بين المللي پنهان سازي براي روش هاي مختلف پنهان سازي داده ها ارائه شده، مشاهده كنيد.



شكل ۱-۳. طبقه بندی روش‌های مختلف پنهان سازی داده‌ها.

۱-۳)مدل كلاسيک ارتباط مخفی :

مدل كلاسيك ارتباط مخفي براي اولين بار توسط آقاي سيمونز در سال 1984 به صورت مسئله ارتباط زنداني ها بيان شد و اين مدل معروف به عنوان مدل استگانوگرافي بيان شد. در اين مدل كه در شكل 1-4 نمايش داده شده است، Bob , Alice دو زنداني هستند كه در دو سلول مختلف به سر مي برند. آن ها به دنبال طراحي نقشه اي براي فرار مي باشند و ليكن متاسفانه تمام ارتباطات آن ها توسط wendy كه نگهبان ناظر آن هاست كنترل مي شود. اين دو زنداني اگر توسط پيام رمز شده با يكديگر ارتباط برقرار كنند، نگهبان مظنون شده و مانع از برقراري ارتباط ميشود، بنابراين تنها راه ارتباط اين دو زنداني، ارسال پيام هاي مفهوم و با معني در لفافه يك سري پيام عادي و بي خطر است، به گونه اي كه هيچ گونه شك wendy را كه پيام ها را كنترل مي كند، برنيانگيزد! براي مثال Bob مي تواند با ترسيم و ارسال يك نقاشي از يگ گاو آبي در چمنزار سبز پيام خود را در لفافه مفهوم رنگ براي Alice ارسال كند. در اين صورت wendy هم كه از مفهوم رنگ ها كاملاً بي اطلاع است، به تصوير به عنوان يك



شکل 2-16

۲-۷)جمع بندی ونتیجه گیری:

در اين پروژه اهميت استفاده از دو بيومتريک به جاي يک بيومتريک و هم چنين بحران امنيت بيومتريک هابررسي شد.يکي از روش هاي جلوگيري از حمله به بيومتريک به خصوص هنگامي که بيومتريک از طريق شبکه يا توسط فرد(روي کارت شناسايي هوشمند)منتقل مي شود نشانه گذاري بيو متريک است.بنابراين براي افزايش کارايي وامنيت سيستمهاي شناسايي فردبه طور همزمان، پيشنهاد شد که از دو بيو متريک که يکي در ديگري نشانه گذاري شده است استفاده شود.

همان طور که گفته شد روش هاي قبلي چندان موفق عمل نکردنددر پايان روش جديدي معرفي شدکه در اين روش عمل بازيابي اطلاهات درج شده با 100درصد

موفقيت انجام مي گيردو مي توان بدون هيچ گونه نگراني ازكاهش كيفيت،اطلاعات رادر تصوير پنهان كرد.همان طور كه گفته شد وزن دار كردن پيكسل هاواضافه كردن بيت هاي مرجع به ترتيب باعث راحت تر شدن عمل تخمين بدون حضورتصوير اوليه وبازيابي اطلاعات درج شده با موفقيت كامل شد.كه ازمزيت هاي اين روش مي باشند.

به عنوان كار پيشنهادي مي توان حلقه ي فيدبک قسمت نشانه گذار و تعديل كننده قدرت نشانه گذاري را به نحو هوشمندي طراحي كردكه باعث تغيير مقدارq در هر پيكسل نسبت به پيكسل ديگرشودتا باعث افزايش كيفيت هر چه بيشتر تصوير شود و امكان بازيابي غلط بيت ها به طور كامل ازبين برود.

دانشجویان محترم:

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

مراجع :

[1] www.ICAO.int

[2] Ratha N.K., Connell J.H., and Bolle R.M.,“Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” *IBM Systems Journal*, vol. 40, no. 3, pp.614-634, 2001A.

[3] Pankanti S. and Yeung M.M., “VerificationWatermarks on Fingerprint Recognition andRetrieval,” *Proc. SPIE*, vol. 3657, pp. 66-78, 1999.

[4] . Jain A.K and Uludag U., “Hiding BiometricData,” *IEEE Transactions on PatternAnalysis andMachine Intelligence*, Vol. 25, NO. 11, pp. 1494-1498, November 2003.

[5] Noore A., Tungala N., Houck M.M.**, “**Embeddingbiometric identifiers in 2D barcodes for improvedsecurity,**”** *ELSEVIER, Computers and Security*,vol. 23, pp.679-686,2004.

[6]Katzenbeisser S. and Petitcolas A.-P.,"Information Hiding Techniques forSteganography and Digital Watermarking,"Artech House, January 2000, ISBN: 1580530354

[7] Langelaar G., Setyawan I. and Lagendijk R.,"Watermarking digital image and video data: Astate-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, p. 20-46,September 2000

[8] Meerwald P. and Uhl A., "A survey of waveletdomainwatermarking algorithms," inProceedings of SPIE, Electronic Imaging,Security and Watermarking of MultimediaContents III, P. W. Wong and E. J. Delp, eds.,4314, SPIE, San Jose, CA, USA, Jan. 2001A.

[9] Kutter M., Jordan F., and Bossen F.. "Digitalsignature of color images using amplitudemodulation". *In Proc. SPIE, Storage andRetrieval for Image and Video Databases V*, vol.3022, pages 518{526, 1997

[10] Kutter M. and Petitcolas A., "A fair benchmarkfor image watermarking systems" , *Proceedingsof Electronic Imaging’99, Security*

andWatermarking of Multimedia Contents, vol. 3657,p. 226–239, San Jose, California, U.S.A..

[11]. احمديان پويا و رحمتي محمد،"مقاوم سازي پنهان سازي اطلاعات اثر انگشت در تصوير چهره"،پايان نامه كارشناسي ارشد،دانشكده كامپيوتر و فناوري اطلاعات،دانشگاه صنعتي امير كبير تهران