دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

اصالت سنجی اسناد الکترونیکی با استفاده از روش‌های پنهان نگاری و واترمارکینگ

پریسا دانشجو [۱]، مصطفی مظفری [۲]

دانشیار،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران[۱]، Daneshjoo.p@wtiau.acir

دانشگاه آزاد واحد تهران غرب[۲] ، m.mozafari@protonmail.com

خلاصه

همه سازمان‌ها باید سوابق تصمیمات و معاملات تجاری خود را برای پاسخگویی به خواسته‌های مشتریان یا ذی‌نفعان شرکت، نگه دارند. با توجه به افزایش روزافزون اسناد الکترونیکی و همچنین تبدیل اسناد کاغذی به الکترونیکی، استفاده از فن‌آوری اطلاعات و ارتباطات، نحوه انجام کار در سازمان‌ها را تغییر می‌دهد و منجر به وابستگی بسیار بیشتر به سوابق الکترونیکی می‌شود. مدیریت اسناد الکترونیکی به سازمان‌ها کمک می‌کند تا از اطلاعات به طور موثرتری بهره برداری و از نیازهای عملیاتی فوری برای اطلاعات تجاری پشتیبانی کنند. یک سیستم مدیریت سوابق الکترونیکی باید بتواند این سوابق را در طول چرخه حیات خود، از نظر ضبط, یکپارچگی، اصالت, امحا و در دسترس بودن، مدیریت کند. با این حال، یکی از مشکلات، اصالت سنجی و حفظ آثار معنوی فایل‌های الکترونیکی است. برای رفع چنین مشکلاتی می‌توانیم از روش‌های نوین در این زمینه استفاده کنیم که یکی از این روش‌ها، استفاده از پنهان‌نگاری و واترمارکینگ است. پنهان‌نگاری در دهه گذشته بسیار مورد استفاده قرار گرفته‌است. روش‌های پنهان‌نگاری و واترمارکینگ طراحی شده‌اند تا توالی‌های اطلاعات پنهان را در اشیاء الکترونیکی برای اهداف مختلف تعبیه کنند. این روش‌ها در حوزه‌های امنیتی و حفاظتی برای پنهان نگه‌داشتن پیام اصلی یا حفظ معنوی آثار به کار می‌روند. مقاله حاضر ابتدا به مطالعه مفاهیم EDMS پرداخته و **در مرحله بعد، تحقیقات فعلی در زمینه روش‌های جاسازی اطلاعات در اسناد الکترونیکی را مورد برررسی قرار داده‌است.**

کلمات کلیدی: سیستم مدیریت اسناد الکترونیکی، اسناد الکترونیکی، اصالت سنجی، پنهان نگاری، واترمارکینگ

۱ مقدمه

با اینکه سوابق کاغذی هنوز هم وجود دارند و برای آینده قابل پیش‌بینی تولید می‌شوند - و ابزارها و سیستم‌های مدیریت آنها به خوبی تثبیت شده‌اند-، نگرانی کلی در مورد توانایی سازمان‌ها برای مدیریت و حفظ آن دسته از سوابق الکترونیکی که برای پشتیبانی کسب و کار لازم است، همچنان وجود دارد. سازمان‌ها برای پشتیبانی از پرونده‌ها، ارائه خدمات و پاسخگویی و تعهدات سازمان نیازمند بایگانی هستند. مدیریت سوابق الکترونیکی از نیازهای اطلاعاتی میان مدت و بلند مدت کسب و کار پشتیبانی و حافظه شرکت را ایجاد و نگهداری می‌کند. ساختار بایگانی شرکتی را مدیریت می‌کند که سوابق در آن طبقه بندی می‌شوند. پس از طبقه‌بندی سوابق باید مشخص شود که چه مدت باید نگهداری شوند یا برخی از این سوابق به صورت دائمی در آرشیو(بایگانی) حفظ و در نهایت چگونه باید امحا شوند؟

اسناد الکترونیکی سازمان‌ها که در EDMS ایجاد می‌شوند برای تایید مالکیت اسناد در حال گردش خود و ارسال اسناد سازمانی به سازمان‌های دیگر و همچنین با هدف ارایه به محاکم قضایی در صورت هر گونه سرقت مالکیت معنوی یا اصالت سنجی اسناد نیازمند یک روش برای اصالت سنجی هستند.

با توجه به قوانین موجود، از اسناد الکترونیکی در آمریکا با عنوان «سوابق الکترونیک»، در قانون آنسیترال و ایران با عنوان «داده پیام» و در فرانسه با عنوان «سند الکترونیک» یاد می‌شود. اما نظر مشترک این است که، همگی کاربرد و جایگاه سند را مستقیماً یا به صورت معادل یا در حکم آن برای این نوع اسناد پذیرفته‌اند. شاید بتوان گفت روش فرانسویان با توجه به پیوند آن با قوانین کشور و نیز فرهنگ حقوقی آن، مدبرانه‌تر و کامل‌تر است.

قانون جرایم رایانه‌ای ایران، بدون این‌که تعریف خاصی برای محتوای حافظه رایانه در نظر بگیرد، در ماده ۵۰، این اسناد را قابل استناد خوانده است.

«اگر داده‌های رایانه‌ای به وسیله طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده و سیستم رایانه‌ای یا مخابراتی مربوطه به گونه ای عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، می‌توان به آنها استناد نمود.»

براین اساس، برای شناسایی جعلی بودن سند باید داده یا علائمی در اسناد -در سامانه‌های رایانه‌ای یا مخابراتی- وجود داشته باشد. از پنهان‌نگاری و واترمارکینگ برای مخفی کردن یک قطعه و یا برای اضافه کردن جزئیاتی به اسناد می‌توان استفاده کرد.

۲ سیستم مدیریت اسناد الکترونیکی(Electronic Document Management System)

بسیاری از سازمان‌های جهانی استراتژی(راهبرد) و عملیات خود را از طریق چهارچوب سیستم مدیریت یکپارچه (IMS) مبتنی بر ISO هماهنگ کرده‌اند که امکان ادغام سیستم‌های مدیریت کیفیت، محیط زیست، سلامت و ایمنی را فراهم می‌کند. در چنین شرایطی، داشتن یک سیستم مدیریت اسناد الکترونیکی قوی (EDMS) ضروری است، به ویژه در شرکت‌های جهانی که در آن حجم زیادی از اسناد تولید شده توسط فرایندها، از طریق فرهنگ‌های کاری مختلف جریان می‌یابد. سیستم‌های مدیریت یکپارچه (IMS) به عنوان یک رویکرد فرایندگرا برای حمایت از سازمان‌ها در ترکیب سیستم‌های مدیریت کیفیت، محیط زیست، سلامت و ایمنی در انطباق با استانداردهای ISO 9001، ISO 14001 و OHSAS 18001 توجه فزاینده ای را به خود جلب کرده‌اند.(Eriksson & Hansson, 2003; Rasmussen, 2007; Tambo, 2012; Oliveira, 2013).

در حوزه مدیریت اسناد، سیستم مدیریت اسناد الکترونیکی(EDMS) به عنوان مفهومی برای کاهش استفاده از کاغذ ایجاد شده‌است.(Agarkar, Borle, Deshmukh & Bhagat, 2012؛ Ralph, 1995). EDMS دارای ابزارهای ضروری برای شرکت‌ها به‌منظور مستندسازی فرایندهای تجاری و مدیریت جریان داخلی اطلاعات است. EDMS نقش‌های متعددی در ذخیره‌سازی، بایگانی، مدیریت، تایید و کنترل جریان اسناد IMS برای تسهیل گردش کار سازمانی دارد(Bae & Kim, 2002). استانداردهای فردی و همچنین پیاده‌سازی‌های شرکتی بر نقش حیاتی کنترل اسناد در IMS تأکید دارند(موئهلن، ۲۰۰۴).

اسناد مورد استفاده یا تولید شده توسط فرایندها باید برای کاهش عدم انطباق مربوط به سند، ارائه اطلاعات به روز، مدیریت «منبع واحد حقیقت» [۱] و اطمینان از اینکه فقط اسناد تایید شده از طریق سازمان مورد استفاده واقع شود، کنترل شوند. بنابراین، به منظور رعایت استانداردهای IMS، کارایی یک سیستم مدیریت اسناد مستقر در سازمان‌های مربوطه، بسیار حیاتی است.

۲-۱ نحوه اجرا EDMS

مدیریت الکترونیکی اسناد نتیجه اجرای فرایند یا پروژه‌های آرشیو الکترونیک یا بایگانی الکترونیکی و داده آمایی (ورود اطلاعات) مربوط به اسناد در نرم افزارهای مربوطه بوده و چندین سال است که توسط سازمان‌ها و موسسات مختلف درحال اجرا و بهره‌برداری است. مدیریت اسناد الکترونیکی حوزه‌ای پیچیده و بی‌نهایت گسترده است. این حوزه مدیریتی باید ضرورت‌هایی را برای هماهنگی بین اجزای تشکیل دهنده سامانه و کارکرد بهتر آن در نظر گیرد.

در دیدگاه مدیریت الکترونیکی اسناد، ابتدا می بایست مدارک و اسناد موجود در سازمان آرشیوی خود را شناسایی و نحوه مدیریت اسناد را بر اساس استانداردها تعریف کنیم. سیاست‌های سازمانی و اهمیت تاریخی و پیشینه هویتی اسناد موجود جزء دیگر تشکیل دهنده این نظام است. فرایند مدیریت بر اطلاعات و میزان اهمیت ذاتی اسناد یک سازمان را می‌توان نقطه آغازین سامانه مدیریت اسناد الکترونیکی در نظر گرفت. همچنین به منظور بالا بردن بازدهی و کارائی اطلاعات و اسناد تولید شده در گذشته، حال و آینده سازمان، آرشیو اسناد با به کارگیری استانداردها و سیاستگذاری‌های مناسب بسیار ضروری به نظر می‌رسد. مدیریت اسناد الکترونیکی را می‌توان یافتن راهی برای خلق، شناسایی، کسب، اشتراک و توزیع اسناد الکترونیکی به افراد نیازمند آن دانست. این خود، عاملی برای شرکت‌های نرم‌افزاری به منظور ورود به بازار و ارایه سیستم‌های EDMS است که می‌تواند آن‌ها را به سودآوری برساند، اما این عمل باید با دقت و در نظر گرفتن تمام جوانب انجام شود.

سیستم مدیریت اسناد الکترونیکی، نرم‌افزاری قدرتمند برای متمرکز سازی و مدیریت اسناد الکترونیک است. هدف سیستم مدیریت اسناد و آرشیو الکترونیک، ارائهٔ یک منبع واحد و ثابت از داده‌ها و اطلاعات حقیقی و صحیح است که می‌تواند کنترل نسخه‌های اسناد و انطباق را تسهیل کند و در نهایت منجر به کارایی و بازگشت سرمایه شود. امروزه نرم افزارهای مختلفی با عنوان «مدیریت اسناد الکترونیکی» به بازار عرضه شده است که برای کار در بایگانی‌های اسناد طراحی شده‌اند.

این سیستم با رعایت ملاحظات امنیتی و مجوزهای دسترسی، امکان دستیابی از راه دور به اسناد را در اختیار کاربران خود قرار داده و با ثبت تمامی وقایع رخداده در سیستم امکان ممیزی عملکرد کاربران را به مدیر سیستم می‌دهد.

1. Single Source of truth

۲-۲ مزایای EDMS

مزایای قابل توجه EDMS شامل کاهش هزینه‌ها، بهبود امنیت، ذخیره سازی اسناد الکترونیکی به صورت متمرکز و کارایی کلی کسب و کار است. پیاده‌سازی این سیستم به معنای صرفه‌جویی زیاد در زمان رویه‌های روزمره مانند چاپ یا بایگانی اسناد و همچنین جست‌وجوی یک سند کاغذی است. برچسب‌ها، کلمات کلیدی و ابرداده‌ها به کاربران EDMS اجازه می‌دهند یک سند را در عرض ۱-۲ دقیقه پیدا کنند. به طور کلی، سیستم‌های مدیریت اسناد برای افزایش ذخیره‌سازی داده‌ها و بهبود تجربه کلی طراحی شده‌اند و دیگر مزایای آنها به شرح ذیل است :

- پشتیبان‌گیری یا بازیابی سریع و آسان
- کنترل نسخه
- بهبود در گردش کار
- کاهش زمان
- همکاری بهتر بین تیم
- فضای ذخیره‌سازی کمتر
- انعطاف‌پذیری
- ادغام با سیستم‌های اتوماسیون اداری

۲-۳ مشکلات EDMS

فرایند انتقال از اسناد کاغذی به DMS یا حتی مهاجرت از یک DMS به DMS دیگر، ممکن است چالشی به نظر برسد. آشکارترین مشکل، آموزش مجدد کارکنان و دادن زمان به آنها برای تطبیق با سیستم، عملکردها و رابط کاربری آن است. برای مدیران اجرایی غیرفنی و شرکت‌هایی که در بخش فن‌آوری اطلاعات درگیر نیستند، ممکن است کار با پشتیبانی ۲۴ ساعته و به‌روزرسانی‌های دائمی که همه سیستم‌های مدیریت اسناد نیاز دارند، سخت باشد. با این حال، اگر راه حلی را خریداری کنید، ارائه دهنده خدمات از آن مراقبت خواهد کرد، و اگر یک DMS سفارشی دارید، همیشه می‌توانید یک متخصص پشتیبانی فنی استخدام کنید (یا او را ساعتی به کار بگیرید).

این سیستم‌ها باید به مرور و با پیاده‌سازی امکانات آنها، از قبیل جریان گردش سندهای قابل طراحی، آرشیو الکترونیکی، به‌روز نگهداشتن اسناد و امکان گزارش‌گیری از محتویات آنها و منطبق بر ساز و کارهای اداری سازمان‌ها وارد بازار شوند تا به این ترتیب، بتوانند با گذشت زمان تحولی در فرهنگ اداری سازمان‌ها به‌وجود آورند و راه را برای تولید و راه‌اندازی سیستم‌های مدیریت اسناد و محتوا در آینده هموار کنند. در غیر این صورت، راه‌اندازی این سیستم‌ها در سازمان‌ها با صرف وقت و هزینه ای بسیار بالا همراه خواهد بود.

Doc Flow ۲

۳ واترمارکینگ

واترمارکینگ نوعی تکنیک علامت‌گذاری الکترونیکی است که به‌طورعمده برای شناسایی مالکیت و همچنین برای احراز هویت یا یکپارچگی استفاده می‌شود. در ابتدا به صورت الکترونیکی توسط اندرو تیرکل و همکاران در سال ۱۹۹۲ ابداع شد. عملکرد یک واترمارک الکترونیکی مشابه عملکرد امضای الکترونیکی است. واترمارک الکترونیکی برچسبی است که به عنوان مثال امکان شناسایی نویسنده یک شیء الکترونیکی یا تأیید صحت و یکپارچگی این شیء را فراهم می‌کند. واترمارک‌های الکترونیکی اغلب برای محافظت از نویسندگی فایل‌های چند رسانه‌ای[۳]، کنترل یکپارچگی داده‌ها و تأیید اعتبار منابع این داده‌ها استفاده می‌شود. در حال حاضر، استفاده از چنین روش‌هایی برای محافظت از داده‌ها، به نوع متفاوت مرتبط می‌شود.

واترمارکینگ می‌تواند برای مثال متن، لوگو، کد هش یا اطلاعات دیگر باشد. در بیشتر موارد از روش‌های واترمارک الکترونیکی برای محافظت از خود تصویر روی جلد[۴] استفاده می‌شود، نه از اطلاعات جاسازی شده، زیرا اطلاعات جاسازی شده یک پیام مخفی نیست، بلکه برای شناسایی صاحب تصویر یا کنترل یکپارچگی تصویر استفاده می‌شود. استخراج چنین اطلاعاتی در صورتی اتفاق می‌افتد که تأیید نویسندگی[۵] یک تصویر، تأیید صحت آن، ارزیابی وجود هرگونه تحریف تصادفی یا عمدی ضروری باشد. گسترده‌ترین واترمارک‌های الکترونیکی در زمینه حفاظت از حق چاپ برای محتوای الکترونیکی، به ویژه، تصاویر الکترونیکی استفاده می‌شود. اما روش‌های واترمارک الکترونیکی را می‌توان در زمینه‌های دیگر نیز مورد استفاده قرار داد، به عنوان مثال، برای جاسازی داده‌های بیمار در تصاویر پزشکی. بسیاری از الگوریتم‌های جاسازی نه فقط به تشخیص تغییرات در تصویر می‌پردازند، بلکه به محلی‌سازی و بازیابی ناحیه آسیب‌دیده نیز اجازه می‌دهند.

نامحسوس بودن و استحکام، دو شرط اساسی برای تکنیک‌های واترمارک هستند. واترمارکینگ می‌تواند شکننده، قوی یا نیمه شکننده باشد. واترمارک شکننده نمی‌تواند پس از کوچکترین تغییر در واترمارک، آن را استخراج کند. در نتیجه، آنها معمولاً فقط برای اهداف احراز هویت قابل استفاده هستند. از سوی دیگر، تکنیک واترمارک قوی قادر است واترمارک را حتی پس از ایجاد تغییراتی در آن، با دقت استخراج کند. بنابراین، این تکنیک‌ها معمولا برای حفاظت از حق چاپ استفاده می‌شود. در نهایت، تکنیک واترمارک نیمه شکننده از واترمارک‌های قوی و شکننده بهره می‌برد. این تکنیک‌ها در درجه نخست هم برای یکپارچگی و هم برای احراز هویت استفاده می‌شوند. علاوه بر این، تکنیک‌های واترمارک نیمه شکننده قادر به تشخیص و بازیابی مناطق دستکاری شده[۶] هستند.

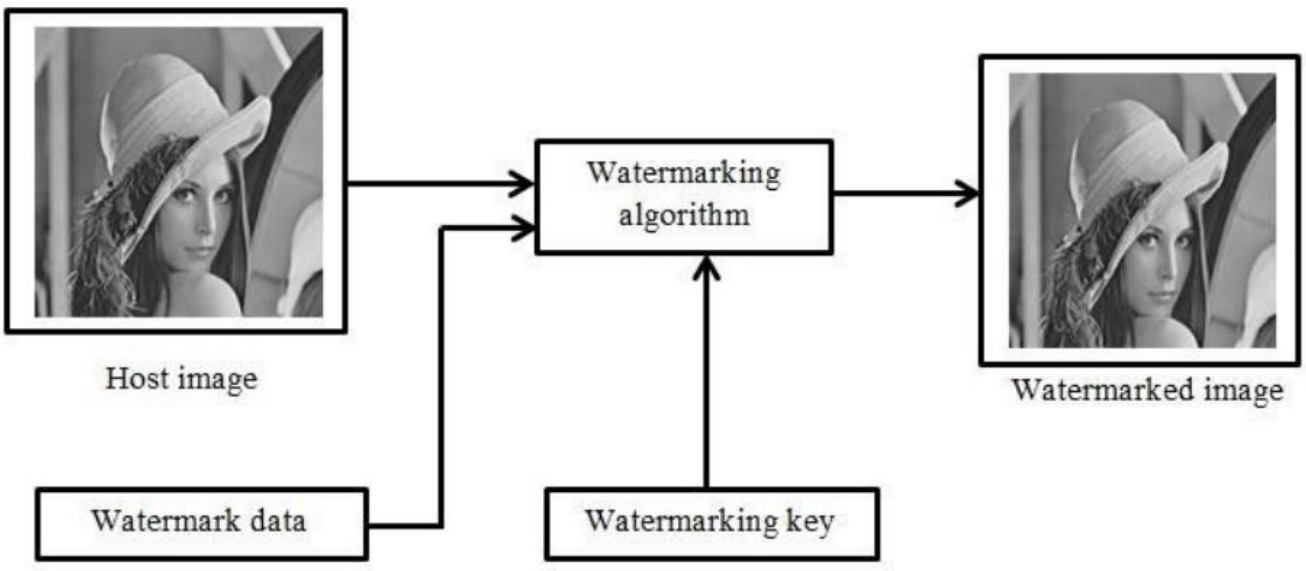
Authorship of multimedia files۳

Cover ۴

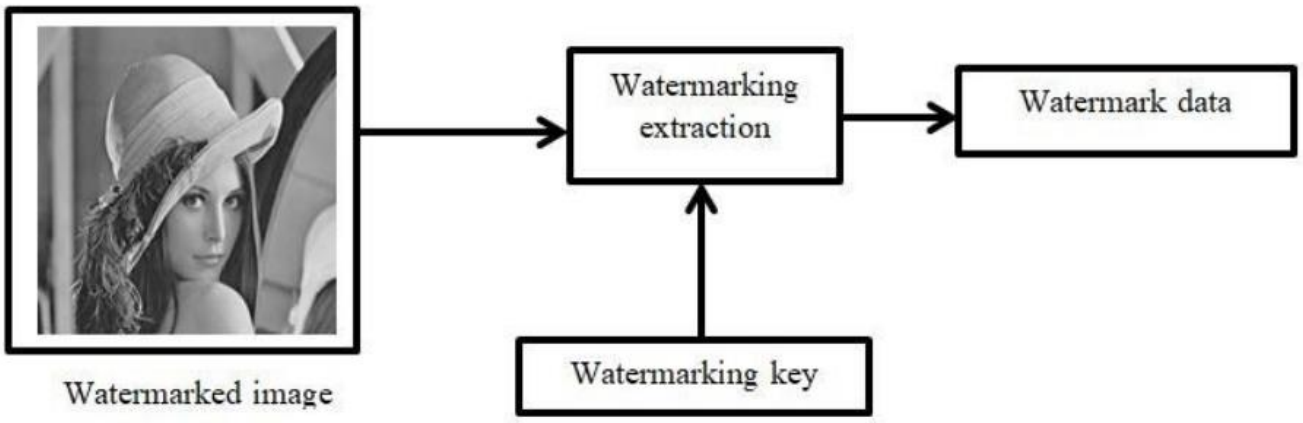
Authorship۵

Tempered۶

شکل ۱ و ۲ روش درج و استخراج واترمارک را به صورت تصویری نشان می‌دهد.



شکل ۱ نحوه درج کردن واترمارک



شکل ۲ نحوه استخراج واترمارک

مقالات [۱]، [۲] نمونه‌هایی از مقالات مروری در مورد تکنیک‌های واترمارک الکترونیکی هستند.

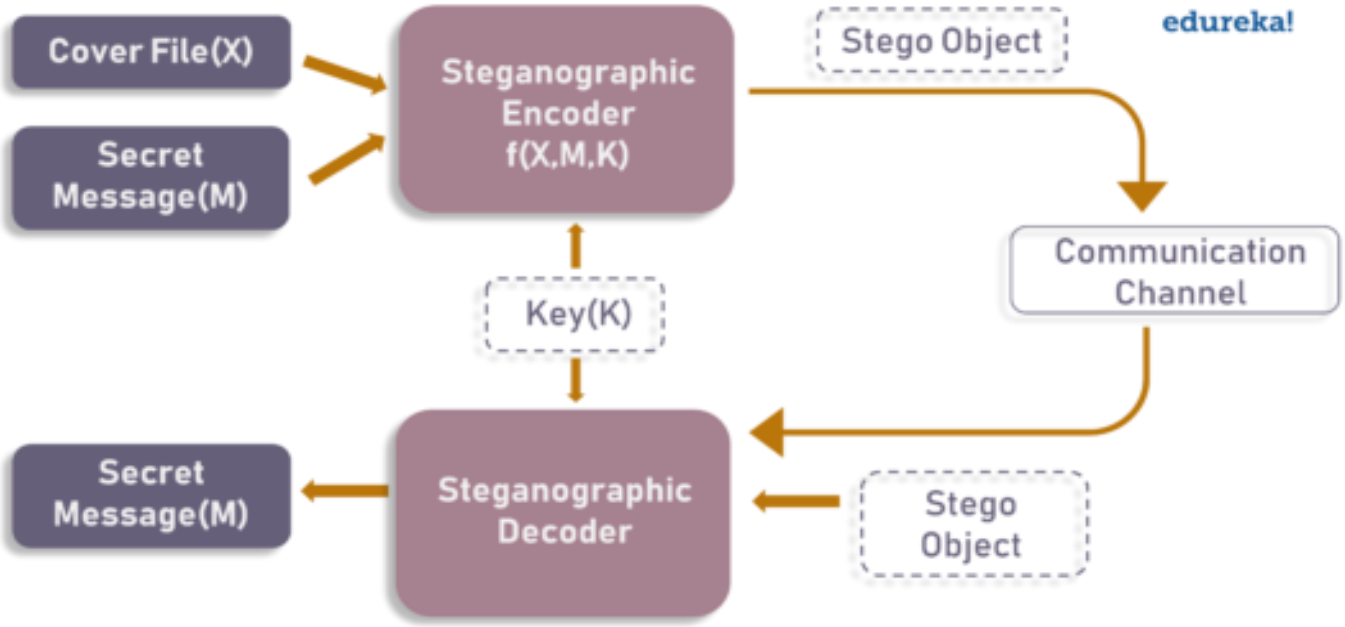
۴ پنهان‌نگاری

پنهان‌نگاری، هنر ارتباط با اطلاعات نامرئی است و نقشی مهم در امنیت اطلاعات ایفا می‌کند. اصطلاح پنهان‌نگاری یک کلمه یونانی و در لغت به معنای «نوشتن پنهان» است که از دو کلمه Stego به معنی «پنهان» و Graphein به معنای «نوشتن» تشکیل شده است.

پنهان‌نگاری، اطلاعات را به گونه‌ای مخفی می‌کند که هیچ شخص ثالثی به جز گیرنده نداند که یک پیام مخفی در داخل اطلاعاتی که منتقل می‌شود پنهان شده‌است. مزیت اصلی این تکنیک این است که شخصی دیگر -به جز گیرنده‌ای که قصد دریافت اطلاعات را دارد- نمی‌تواند به وجود اطلاعات مخفی در پیامی که از طریق یک کانال منتقل می‌شود مشکوک شود. بنابراین، پنهان‌نگاری، وجود اطلاعات یا پیام مخفی را برای شخص سوم جدا از فرستنده و گیرنده نامرئی می‌کند.

نامرئی بودن داده‌ها و ظرفیت جاسازی تصویر دو الزام اولیه هستند که به طور گسترده در تکنیک‌های مختلف پنهان‌نگاری مورد تحقیق قرار گرفته‌اند.

همانطور که در تصویر مشاهده می‌کنید، هر دو فایل جلد(x) و پیام مخفی(m) به عنوان ورودی به رمزگذار پنهان‌نگاری وارد می‌شوند. تابع رمزگذار Steganographic، f(x,m,k) پیام مخفی را در یک فایل جلد جاسازی می‌کند. شیء حاصل Stego که بسیار شبیه به فایل جلد شماست، این کدگذاری را کامل می‌کند. برای بازیابی پیام مخفی، شیء Stego به رمزگشای پنهان‌نگاری وارد می‌شود.



شکل ۳ ساختار کلی فرایند تعبیه و استخراج پنهان نگاری

۴-۱ انواع روش‌های پنهان نگاری

۴-۱-۱ پنهان‌نگاری در متن

پنهان‌نگاری متن، اطلاعاتی را در داخل فایل‌های متنی پنهان می‌کند که شامل مواردی مانند تغییر قالب متن موجود، تغییر کلمات در متن، ایجاد توالی کاراکترهای تصادفی یا استفاده از گرامرهای بدون زمینه برای تولید متون قابل خواندن است. تکنیک‌های مختلفی که برای پنهان کردن داده‌ها در متن استفاده می‌شود عبارتند از:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

۴-۱-۲ پنهان‌نگاری در تصویر

مخفی کردن داده‌ها با قرار دادن شیء پوششی در تصاویر را پنهان‌نگاری تصویر می‌گویند. در پنهان‌نگاری الکترونیکی، تصاویر به طور گسترده‌ای مورد استفاده قرار می‌گیرند، زیرا تعداد زیادی بیت در نمایش الکترونیکی یک تصویر وجود دارد. راه‌های زیادی برای پنهان کردن اطلاعات در داخل یک تصویر وجود دارد. رویکردهای رایج عبارتند از:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter

- Coding and Cosine Transformation

۴-۱-۳ پنهان‌نگاری در صدا

در پنهان‌نگاری صوتی، پیام مخفی در یک سیگنال صوتی جاسازی می‌شود که توالی باینری فایل صوتی مربوطه را تغییر می‌دهد. پنهان کردن پیام‌های مخفی در صدای الکترونیکی در مقایسه با سایرین، مانند پنهان‌نگاری تصویر، فرایندی بسیار دشوارتر است. روش‌های مختلف پنهان‌نگاری صوتی عبارتند از:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

این روش، داده‌ها را در فایل های صوتی wav، au و حتی mp3 مخفی می‌کند.

۴-۱-۴ پنهان نگاری در ویدیو

در پنهان‌نگاری ویدیویی می‌توانید نوع داده‌ها را در قالب ویدیوی الکترونیکی پنهان کنید. پنهان کردن مقدار زیادی داده در داخل ویدیو مزیت این نوع نهان‌نگاری به شمار می‌رود و در واقع یک جریان متحرک از تصاویر و صداها است. شما می‌توانید این پنهان‌نگاری را به عنوان ترکیبی از پنهان‌نگاری تصویر و پنهان نگاری صوتی در نظر بگیرید. دو دسته اصلی از پنهان نگاری ویدئویی عبارتند از:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

۴-۱-۵ پنهان نگاری در پروتکل

این تکنیک، جاسازی اطلاعات در پروتکل‌های کنترل شبکه است که در انتقال داده‌ها مانند TCP، UDP، ICMP و غیره استفاده می‌شود. به عنوان مثال، می‌توانید اطلاعات را در سربرگ[۷] یک بسته TCP/IP در برخی از فیلد(قسمت)ها که اختیاری هستند، پنهان کنید.

۵ تفاوت واترمارکینگ و پنهان نگاری

در برخی موارد تفاوت بین این دو برای پنهان کردن داده‌ها در اشیاء الکترونیکی صرفاً در هدف کاربرد نهفته است، زیرا بسیاری از الگوریتم‌ها برای آماده ساختن نهان‌نگاری و جاسازی واترمارک الکترونیکی مبتنی بر عملیات مشابه هستند. با این وجود، بسیاری از الگوریتم‌های خاص وجود دارند که به صراحت فقط برای پنهان‌نگاری یا واترمارکینگ الکترونیکی اعمال می‌شوند. در چنین مواقعی، تفاوت‌های اصلی در الزامات اثربخشی جاسازی داده‌ها است. به طور کلی، نیاز اصلی برای اثربخشی الگوریتم‌های پنهان‌نگاری، نامرئی بودن تعبیه است، زیرا ایده پنهان‌نگاری در نامرئی بودن تعبیه نهفته است. در این میان، الگوریتم‌های پنهان کردن واترمارک الکترونیکی اغلب به عنوان الگوریتم‌های جاسازی قوی توسعه داده می‌شوند که می‌توانند داده‌های جاسازی شده را حتی پس از اعوجاج[۸] یک شیء الکترونیکی شناسایی کنند. اگرچه، نویسندگان مختلف در حال توسعه الگوریتم‌هایی با شاخص‌های کیفیت اضافی هستند که امکان به‌کارگیری چنین الگوریتم‌هایی را در عمل گسترش می‌دهند.

تعداد زیادی الگوریتم خاص برای جاسازی واترمارک الکترونیکی وجود دارد که -همانطور که در برنامه‌های پنهان‌نگاری فرض می‌شود-، برای آماده‌سازی حجم زیادی از داده‌ها مناسب نیستند. گاهی اوقات نیازی به استخراج کامل واترمارک داخلی نیست. کافی است متقاعد شود که واترمارک خاصی در این تصویر وجود دارد. نامرئی بودن و ظرفیت جاسازی برای تکنیک‌های واترمارکینگ مانند پنهان‌نگاری، مهم به‌شمار می‌روند، اما در برخی موارد واترمارک‌ها قابل مشاهده هستند و همیشه به ظرفیت بالایی نیاز نیست.

۶ نتایج بررسی

در حال حاضر، روش‌های پنهان‌نگاری و واترمارکینگ الکترونیکی به طور فعال در حال توسعه هستند و بسیاری از محققان از کشورهای مختلف، الگوریتم‌های جدید را که در ویژگی‌های کیفی متفاوت هستند، ارائه می‌کنند.

با پیشرفت در سامانه‌های مدیریت اسناد الکترونیکی، امکانات بسیار زیادی در خصوص اصالت سنجی اسناد الکترونیکی فراهم خواهد شد. در این راستا، یکی از بحث‌ها و سوالات مطرح شده در زمینه «مناسب بودن پنهان‌نگاری به عنوان ابزاری برای پنهان کردن اطلاعات» این است: زمانی که روش‌هایی دیگر مانند رمزنگاری، قوی‌تر به نظر می‌رسند، آیا پنهان‌نگاری روشی مناسب برای نگهداری اطلاعات دریافت‌کننده مورد نظر به شمار می‌رود؟

استفاده از امضای الکترونیکی، یک تکنیک رمزنگاری رایج برای احراز هویت متن است. از آنجا که مفهوم اصلی ارتباطات پنهان‌نگاری در محرمانه بودن انتقال نهفته‌است، بنابراین، برنامه‌هایی که ارتباطات مبتنی بر رمزگذاری محدود است، مناسب‌تر است. در هنگام استفاده از پنهان‌نگاری می‌توان برای نمایش اطلاعات پنهان شده در فایل از کلید رمز استفاده کرد که باعث ارتقاء امنیت اطلاعات رمزگذاری شده می‌شود.

شرکت‌های دارای نرم افزار مدیریت اسناد می‌توانند در هنگام ثبت سند در سیستم یا بانک اطلاعاتی از روش‌های مورد اشاره برای اصالت سنجی اسناد سازمان‌ها استفاده کنند. سازمان‌ها در صورت استفاده نکردن از سامانه‌های مدیریت اسناد الکترونیکی می‌توانند در قالب یک نرم افزار با استفاده از تکنیک‌های پنهان‌نگاری یا واترمارکینگ، اسناد مورد نیاز خود را برچسب‌گذاری و اطلاعات مورد نیاز را به منظور اصالت سنجی در اسناد پنهان کنند تا در صورت نیاز آن را برای شناسایی اسناد جعلی مورد استفاده قرار دهند.

۷ نتیجه گیری و آینده نگری

تحقیقات بیشتر باید به سمت پتانسیل(ظرفیت)هایی برای پیاده‌سازی عمیق‌تر EDMS در معماری سیستم‌های اطلاعات شرکت‌ها هدایت شود تا از گنجاندن مستقیم IMS نه تنها در فرایندهای تجاری استراتژیک، بلکه در شیوه‌های کاری روزانه با ادغام واضح‌تر با سیستم‌های مهندسی و فروش محصول اطمینان حاصل شود.

اکثر قریب به اتفاق الگوریتم‌های تعبیه‌سازی مدرن، منجر به نامحسوس بودن تعبیه می‌شوند. بنابراین، محققانی که در این زمینه کار می‌کنند لازم است برای دستیابی به سایر شاخص‌های کارایی تعبیه که عبارتند از: برگشت‌پذیری، استحکام، و مقاومت در برابر آنالیز پنهان‌نگاری اهتمام ورزند. بررسی‌ها نشان داد که فعالیت در این زمینه در حال انجام است، اما هنوز مشکلات زیادی وجود دارد که به کشف راه حل‌های اصلی جدید نیاز دارد.

پنهان‌نگاری، در امنیت جایگاه خود را دارد. قرار نیست جایگزین رمزنگاری شود، اما مکمل آن است. پنهان کردن یک پیام با روش‌های پنهان‌نگاری احتمال شناسایی پیام را کاهش می‌دهد. با این حال، اگر آن پیام نیز رمزگذاری شده باشد، در صورت کشف، باید کرک شود (لایه دیگری از حفاظت).

---

7 Header

8 Distortions

پنهان‌نگاری بخشی از برنامه‌های مختلف صنعتی دارای IoT، شهرهای هوشمند، تصویربرداری پزشکی، برنامه‌های نظامی و غیره است. برای جلوگیری از حمله و ارائه محرمانه بودن داده‌ها، یک دیدگاه امنیتی چند سطحی انعطاف پذیر باتوجه به پنهان کردن اطلاعات و رمزنگاری پیشنهاد شده است. احراز هویت متن، نقش حیاتی در دفاع از هویت و محتوای الکترونیکی در برابر انواع مختلف جرایم سایبری دارد.

با استفاده از مکانیزم‌های امنیتی در حوزه امنیت اطلاعات و به کارگیری این مکانیزم‌ها در انواع سامانه‌های مدیریت فایل یا سند الکترونیکی می‌توانیم مشکلات پیش روی سامانه‌های مدیریت فایل‌ها و اسناد را شناسایی و رفع کنیم یا آنها را کاهش دهیم.

۸ منابع

[۱] A. F. Qasim, F. Meziane, and R. Aspin, ‘‘Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review,’’ Comput. Sci. Rev., vol. 27, pp. 45–60, Feb. 2018, doi: 10.1016/j.cosrev.2017.11.003.

[۲] S. Kumar, B. K. Singh, and M. Yadav, ‘‘A recent survey on multimedia and database watermarking,’’ Multimedia Tools Appl., vol. 79, nos. 27–28, pp. 20149–20197, Jul. 2020, doi: 10.1007/s11042-020- 08881-y.

[۳] Integrated management systems and workflow-based electronic document management: An empirical study (Hang Thu Pho; Tambo, Torben)

[۴] Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions(Oleg Evsutin.)

[۵] Steganography A Data Hiding Technique(Naga Ranijth Kumar Kesa)

[۶] Digital image steganography and steganalysis: A journey of the past three decades(Aditya Kumar Sahu* and Monalisa Sahu)

[۷] A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique(Kshetrimayum Jenita Devi)

[۸] Steganography: Past, Present, Future : Published by SANS Institute (James C. Judge)

[۹] https://www.edureka.co/blog/steganography-tutorial

[۱۰] https://www.thecloudtutorial.com/edms-electronic-document-management/

[۱۱] https://procoders.tech/blog/advantages-of-electronic-document-management-system/