تاریخ دریافت مقاله: ۹۶/۰۴/۱۱
تاریخ پذیرش مقاله: ۹۶/۰۵/۲۱

مروری بر روش‌های پنهان‌نگاری در متن

هدیه ساجدی*
استادیار دانشکده ریاضی، آمار و علوم کامپیوتر، پردیس علوم، دانشگاه تهران
پست الکترونیکی: hhsajedi@ut.ac.ir

شبنم رهبریعقوبی
کارشناس ارشد دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی قزوین، واحد علوم و تحقیقات
پست الکترونیکی: shrahbar2006@yahoo.com

چکیده

در عصر فناوری و پیشرفت علم، جایگاه اطلاعات و حفظ امنیت داده‌ها از اهمیت ویژه‌ای برخوردار می‌باشد. حتی دولت‌های قدرتمند از نفوذ رخنه‌گرها و جاسوسان در امان نیستند و همواره مهم‌ترین و حساس‌ترین اطلاعات آن‌ها، در حال شنود و در معرض افشا شدن می‌باشد. پنهان‌نگاری یکی از روش‌های اصلی در بهبود امنیت و حفاظت از داده‌ها است. هدف پنهان‌نگاری، انتقال پیام در کانال‌های ارتباطی در قالب متن، تصویر، صوت، ویدیو و غیره به‌طور مخفیانه می‌باشد. از بین قالب‌های مذکور، برای ذخیره‌سازی فایل متنی حافظه کمتری مورد نیاز است. پنهان‌نگاری متن، یکی از پیچیده‌ترین روش‌های پنهان‌نگاری می‌باشد. روش‌های پنهان‌نگاری مبتنی بر متن را می‌توان در متن‌های صفحات وب و متن‌های ساده استفاده کرد. در این مقاله به بررسی روش‌های موجود پنهان‌نگاری متن پرداخته می‌شود و عملکرد آن‌ها مورد مقایسه قرار می‌گیرد.

واژه‌های کلیدی: متن‌های فارسی، پنهان‌نگاری، صفحات وب.

* نویسندهٔ مسئول

۱- تعریف پنهان نگاری

پنهان‌نگاری معادل فارسی واژهٔ استگانوگرافی است که در اصل کلمه‌ای یونانی بوده و از دو کلمه Steganos به معنای «پنهان کردن» و Graphy به معنای «نوشتن» تشکیل شده است. ترجمه کلمه به کلمه این لغت «نوشته مخفی» است که البته برداشت این معنی از استگانوگرافی چندان متداول نیست و بیشتر به مفهوم پنهان‌سازی اطلاعات در یک رسانه پوشش به‌کار می‌رود، به گونه‌ای که توسط اشخاص غیرمجاز قابل تشخیص نباشد.

به‌طور کلی موضوعاتی که پنهان‌سازی اطلاعات دربرگیرنده آن‌ها می‌باشد عبارت‌اند از: ۱- موارد مربوط به حق مالکیت تولیدات نرم‌افزاری و الکترونیکی شامل نهان‌نگاری[1] و اثر انگشت که جنبه تجاری از این علم هستند.۲- استفاده از پنهان‌سازی در ارسال و دریافت پیام به صورت غیرمحسوس [۱].

توجه به پنهان‌سازی اطلاعات از هر دو جنبه بالا دارای اهمیت است. چرا که با فراهم شدن زمینه‌های فناوری

1-Watermarking

اطلاعات در کشـــور، لزوم اســـتفاده از قانون حق تکثیر و حفظ‌حقوق مربـــوط به مالکیت محصـــولات نرم‌افزاری و تولیدات الکترونیکی اعم از موسیقی، آثار هنری، کتاب‌های الکترونیکی وغیره، شناخت و استفاده از این علم را ایجاب می‌کنـــد. همچنین پنهان‌ســـازی در ترکیب بـــا رمزنگاری مقاومت بســـیار بالایی را در مقابل حمـــلات مختلف پدید می‌آورد. شناخت پنهان‌ســـازی از جنبه‌های کنترلی برای پلیس اینترنتـــی جهت جلوگیری و شـــناخت معبری برای ارتباطات غیرمجاز و مشکوک نیز دارای اهمیت است.

۲- تاریخچه پنهان‌نگاری

اســـتفاده از پنهان‌ســـازی اطلاعات در گذشـــته دارای ســـابقه‌ای طولانی است. اولین اســـتفاده‌های پنهان‌نگاری توسط هرودوت که یک مورخ یونانی است به ثبت رسیده و ماجرای آن به یونان باستان باز می‌گردد. سربازان یونانی برای انتقال پیام سر بردگان را می‌تراشیدند و روی پوست سر آنان نقشه یا پیام را خال‌کوبی می‌کردند و مدتی بعد که موی سر این بردگان بلند می‌شد و روی پیام را می‌پوشاند آن‌ها می‌توانستند به راحتی از میان سرزمین‌ها و اراضی مربوط به دشمن عبور کنند و در مقصد با تراشیدن مجدد موی سر آنان پیام استخراج می‌شد.

همچنین اســـتفاده از جوهرهای نامرئـــی از زمان‌های بســـیار دور در نقـــاط مختلف دنیا مرســـوم بوده اســـت. جوهرهـــای نامرئـــی یکـــی از عمومی‌تریـــن ابزارها برای پنهان‌نگاری هســـتند. در روم باستان از جوهرهایی مانند آبلیمو برای نوشتن پیام استفاده می‌کردند. سپس متن پیام در معرض حرارت تیره و نمایان می‌شد. جوهرهای نامرئی در جنگ جهانی دوم نیز مورد استفاده قرار می‌گرفتند.

یکـــی از پیشـــگامان پنهان‌نـــگاری و رمزنـــگاری، جان تریدمیوس[۲](۱۴۶۲-۱۵۲۶)، یک روحانی آلمانی بود. کتاب وی حاوی جداولی از تصاویر بود که پیام در آن پنهان شده بود. اولین کتاب در مورد پنهان‌نگاری توســـط گاســـپاری اسکاتی[۳] با عنوان اســـتگانوگرافیکا[۴] در سال ۱۶۶۵ نوشته شده اســـت [۲]. پنهان‌نگاری در قرن‌های ۱۵ و ۱۶ توسعه یافت. به دلیل این که اکثر نویســـندگان این کتاب‌ها از ایجاد تفرقه بین احزاب و فرقه‌ها می‌ترســـیدند؛ نام خود را مانند داســـتان‌ها در میان کتـــاب مخفی می‌کردنـــد [۳]. یکی از رســـاله‌هایی که در این زمینه نوشـــته شده توسط بیشاپ جان ویلکینس[۵] است که بعدها در کالج ترینیتی[۶] به استادی رســـید. او روش‌هایی را از کد گذاری پیام‌ها در آهنگ‌ها تا جوهرهای نامرئی پیشنهاد داد. همچنین او اولین طرح‌ها را در رمزگشایی با استفاده از تناوب کلمات ساخت.

در جنگ جهانی دوم توجه زیادی به پنهان‌نگاری شـــد و تجربیات زیادی در این مورد کســـب شـــد. در اوایل جنگ از جوهرهای نامرئی استفاده می‌شد ولی پس از آن از حروف و متن‌های معمولی برای مخفی کردن پیام اصلی استفاده کردند. این متن‌ها درباره اتفاقات بسیار ساده و پیش‌پا افتاده بودند که توجه هیچ کس را جلب نمی‌کردند، بنابراین بدون این‌که کسی مشکوک بشود آن متن‌ها انتقال داده می‌شدند [٤].

از طرح‌بنـــدی متن‌ها نیز برای مخفـــی کردن اطلاعات اســـتفاده می‌شـــد. به وســـیله تنظیم کردن مکان خط‌ها و کلمه‌های متن، پیام نشـــانه‌گذاری شـــده و قابل شناسایی می‌شود. از وسایلی مانند سوزن نیز برای مشخص‌کردن لغات مورد نظر استفاده می‌شد.

همان‌طور که به دلیل پیشـــرفت فناوری، مخفی کردن اطلاعات با حجم زیاد بدون نمایان شدن انجام می‌گرفت، علم آشکار کردن متون مخفی نیز در حال پیشرفت بود. یک مســـئول اف‌بی‌آی از اختراع ریزنقطه[۷] به وسیله آلمانی‌ها به‌عنوان «شاهکار جاسوسی دشمن» یاد کرد. میکرودات عکس‌های بسیار کوچکی بودند، که اطلاعات مختلفی مانند عکـــس و متن را در خود جای می‌دادنـــد. این عکس‌ها به اندازه یک نقطه بودند، بنابراین افراد می‌توانستند با آن‌ها یک متن ساده بنویسند.

2- John Trithemius

3- Gaspari Schotti
4- Steganographica
5- Bishop John Wilkins
6- Trinity
7-Microdot

در حقیقت فضای فرستادن متن‌ها به این روش‌ها آن چنان بود که محدودیت‌های زیادی برای ارسال متن و حتی عکس اعمال می‌شد؛ محدودیت‌هایی که امروز بسیار بی‌معنی هستند. به‌عنوان مثال در آمریکا پست کردن شطرنج، نقشه‌های بافندگی، تکه‌های روزنامه و حتی نقاشی کودکان ممنوع بود. حتی فرستادن گل در انگلستان و آمریکا ممنوع شد.

پس از آن محدودیت‌ها، در قرن بیستم پنهان‌نگاری شکوفا شد. با پیشرفت علم کامپیوتر پنهان‌نگاری پیشرفت چشمگیری داشت. روش‌های قدیمی مخفی کردن در عکس با ورود کامپیوترهای پر قدرت قوت گرفتند. در طول دهه ۱۹۸۰ مارگارت تاچر که از نشت اطلاعات و اسناد کابینه‌اش بسیار ناراحت بود توانست با استفاده از یک پردازشگر کلمات، مشخصات هر وزیر را در فاصله بین کلمات به نحوی ثبت کند و از این طریق وزرای خائن را ردیابی نماید. در حال حاضر نیز روشی مشابه در ردیابی انتشارات الکترونیکی مورد استفاده قرار می‌گیرد که از آن میان می‌توان به شماره ردیف[8] اشاره کرد. امروزه پنهان‌نگاری با پیشرفت نرم‌افزارها گسترش یافته و نهان‌نگاری نیز به‌عنوان یک روش نزدیک به پنهان‌نگاری مورد توجه واقع شده است [۵].

۳- پنهان نگاری در متن

با بهره‌گرفتن از قوه درک انسان می‌توان داده‌ها را در فایل‌های مختلف پنهان کرد بدون این‌که بیننده یا شنونده آن متوجه شود. برای مثال، پوشش فرکانسی فایل‌های صوتی پدیده‌ای است که زمانی رخ می‌دهد که دو صوت با فرکانس‌های مشابه و همزمان پخش می‌شوند. شنونده تنها صوت بلندتر را می‌شنود و صوت دیگر پوشش داده می‌شود. به‌طور مشابه، پوشش زمانی، مواقعی رخ می‌دهد که یک سیگنال ضعیف بلافاصله بعد یا قبل از یک سیگنال قوی‌تر و در زمانی که شنونده نیاز به صرف زمان برای تنظیم کردن سیستم شنوایی خود جهت شنیدن سیگنال جدید دارد ظاهر می‌شود. این موارد امکانی برای ذخیره کردن اطلاعات به‌طور پنهان در یک فایل را فراهم می‌آورند [۶].

روش‌های زیادی برای پنهان‌سازی در تصویر، ویدئو و صوت ارایه شده است [۷]. پنهان‌سازی در متن را می‌توان سخت‌ترین نوع پنهان‌سازی به حساب آورد و علت آن را نیز می‌توان نداشتن اطلاعات افزونه در فایل‌های متنی در مقایسه با تصویر و صدا دانست. ساختار داده‌های متنی همان چیزی است که مشاهده می‌شود در حالی که به‌طور مثال در یک تصویر ساختار متفاوت است و به دلیل این‌که پنهان‌سازی باید طوری انجام گیرد که اطلاعات پنهان شده قابل مشاهده نباشند این کار در متن مشکل‌تر می‌باشد. پنهان‌سازی در متن به دلیل این‌که استفاده از داده‌های متنی در مقایسه با بقیه داده‌ها بیشتر است و با توجه به هزینه پایین استفاده و چاپ آن و همچنین نیاز به حافظه کمتر، قابل توجه است [۸].

برای پنهان‌سازی اطلاعات در یک فایل متنی، می‌توان به سادگی بعضی خصوصیات آن را تغییر داد. این خصوصیات می‌تواند قالب‌بندی متن یا خصوصیات حروف باشد. ممکن است بنظر برسد تغییر این خصوصیات برای خواننده متن واضح است اما کلید این مشکل این است که سند متنی را طوری تغییر دهیم که توسط چشم انسان قابل تشخیص نباشد، اما کامپیوتر بتواند آن را کشف و رمزگشایی کند [۶].

شکل ۱ روش‌های مختلف و موجود پنهان‌نگاری پیام در متن‌های انگلیسی، فارسی و صفحات وب را به اختصار نشان می‌دهد. در بخش‌های بعدی این روش‌ها با جزییات بیشتری مورد بررسی قرار می‌گیرند.

۳-۱- روش های پنهان نگاری در متن‌های انگلیسی

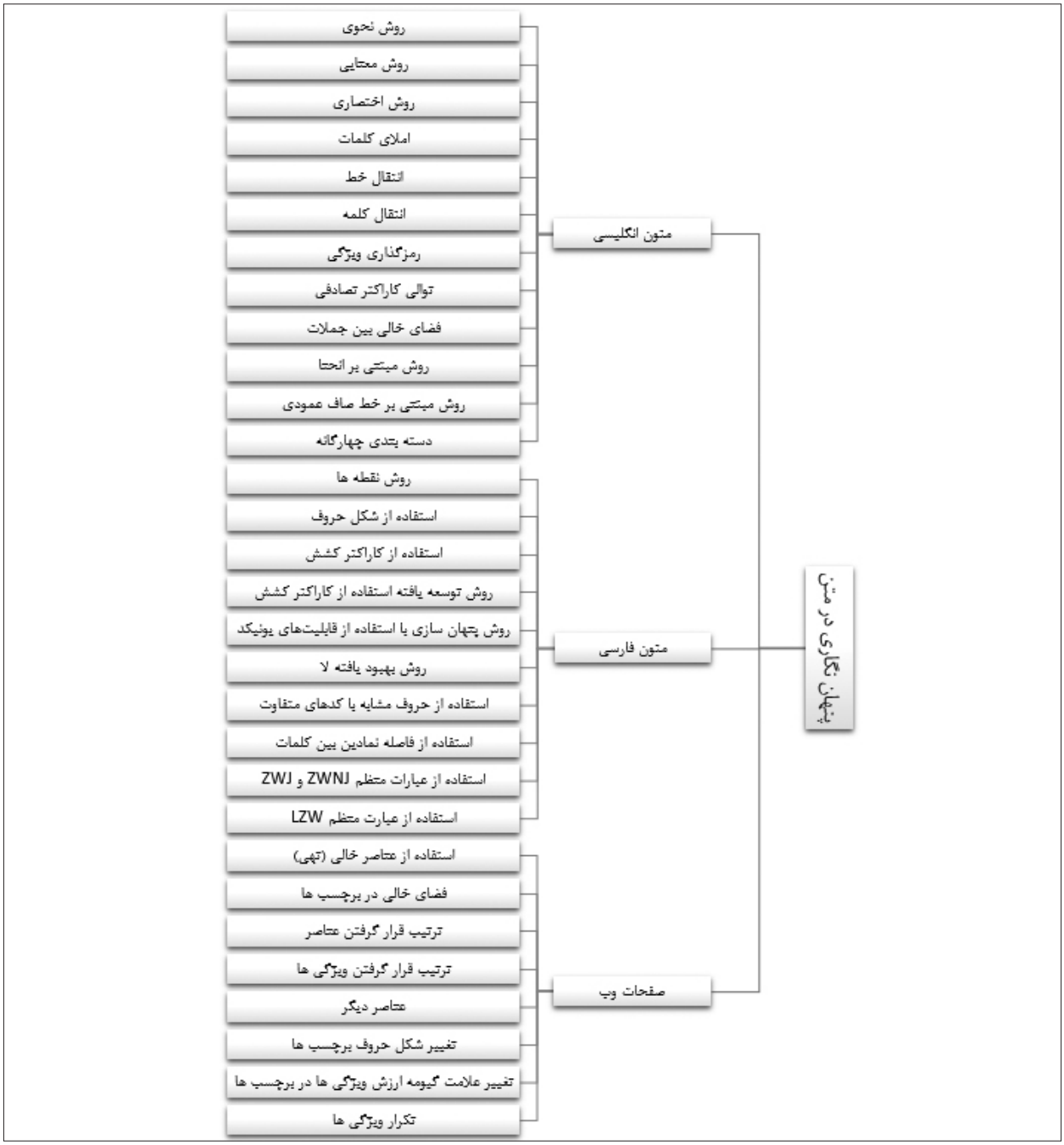
در این بخش روش‌های موجود پنهان نگاری اطلاعات در متن‌های انگلیسی مورد بررسی قرار می‌گیرند.

-روش نحوی[9] [۹]

در این روش از ساختار و قواعد نحوی متن برای پنهان‌سازی داده استفاده می‌شود؛ به‌طوری که با قرار دادن نقطه‌گذاری در متن پوششی مانند (.)، (،) و غیره

8- Serial number

9- Syntactic Method



شکل ۱: روش‌های مختلف و موجود پنهان‌نگاری پیام در متن‌های انگلیسی، فارسی و صفحات وب

در محل مشخص، اطلاعات پنهان‌سازی می‌شود.

-روش معنایی[10] [۱۰]

در این روش از مترادف کلمات برای پنهان‌سازی داده استفاده می‌شود و کلمه مورد نظر با مترادف آن جایگزین می‌شود. اما در برخی از مواقع معنی واقعی فایل متنی تغییر می‌کند.

10- Semantic Method

-روش اختصاری[11] [۱۱]

در این روش از جایگزینی مخفف کلمات برای پنهان‌سازی داده استفاده می‌شود. حجم بسیار کمی از داده‌ها در این روش می‌توانند مخفی شوند.

-املای کلمات[12] [۱۲]

کشورهای مختلف دارای فرهنگ لغات متنوعی هستند.

11- Abbreviation or acronym Method
12- Word Spelling

به‌عنـــوان مثـــال ازکلمات مشـــابه در زبان‌های انگلیســـی بریتانیایی و انگلیسی آمریکایی که دارای املاهای متفاوتی می‌باشند، می‌توان برای پنهان‌سازی داده استفاده کرد.

-انتقال خط[13] [۱۳]

در این روش خط‌هـــای متن مقداری به‌طور عمودی به ســـمت بالا یا پایین انتقال داده می‌شود. معمولاً این روش برای پنهان‌ســـازی اطلاعات در متن‌های چاپ شده مورد استفاده قرار می‌گیرد.

-انتقال کلمه[14] [۱۲]

در ایـــن روش فاصلـــه افقی بین کلمات بـــا وارد کردن فضای خالی سفید تغییر می‌کند. این روش از نظر زمانی به همان اندازه‌ای که متن پنهان شده برای انسان قابل مشاهده است، وقت‌گیر می‌باشد.

-رمزگذاری ویژگی[15] [۱٤]

در این روش حروف با توجه به ابعاد آن‌ها کشـــیده یا کوتاه می‌شوند. همچنین این روش برای پنهان‌سازی داده از خصوصیات مختلف متن مانند رنگ استفاده می‌کند.

-توالی نویسه‌های تصادفی[16] [۱۵]

در این روش یک رشـــته تصادفی از نویسه‌های مجزا ایجاد شده است که شـــامل همان نویسه‌هایی می‌باشد که برای پوشش در پنهان‌سازی اســـتفاده می‌شود. دو گروه برای عملیات پنهان‌سازی تشـــکیل می شود. اگر بیت پیام مخفی صفر باشد، گروه A و اگر یک باشد از گروه B برای پنهان‌سازی استفاده می‌شود.

- فضای خالی بین جملات[17] [۱۵]

این روش از فضای بین جملات برای پنهان‌سازی متن استفاده می‌کند. اشکال اصلی این روش، قابلیت پنهان‌سازی حجم بسیار کمی از داده‌ها است.

13- Line shifting
14- Word Shifting
15- Feature Coding
16- Random Character Sequence
17- Inter sentence space

-روش مبتنی بر انحنا[18] [۱۵]

این روش بر پایه شکل ظاهری حروف استوار می‌باشد. حروف بر اساس ساختارشان به دو گروه تقسیم می‌شوند. گروه A شامل حروف دارای انحنا و گروه B شامل حروف فاقد انحنا می‌باشد. این دو دسته از حروف برای پنهان‌سازی بیت صفر و یک مورد استفاده قرار می‌گیرند.

- روش مبتنی بر خط صاف عمودی[19] [۱۵]

در ایـــن روش حروف بر اســـاس داشـــتن خط‌صاف عمودی گروه‌بندی می‌شـــود. گروه A شامل کلماتی است که دارای خط عمودی و گروه B شـــامل کلماتی اســـت که فاقد خط‌صاف عمودی هستند. این دو دسته از کلمات برای پنهان‌سازی بیت صفر و یک مورد استفاده قرار می گیرند.

-دسته بندی چهارگانه[20] [۱۵]

در این روش حروف به چهار گروه بر اســـاس انحنا، خط‌صاف افقی متوسط، یک خط‌عمودی صاف و خط‌های عمـــودی صاف چندگانه تقســـیم بندی می‌شـــود. ظرفیت پنهان نگاری در این روش نسبت به روش‌های مشابه قبل بیشتر است.

۲-۳- روش های پنهان نگاری در متن‌های فارسی

روش‌های پنهان‌نگاری پیام در متن‌های فارســـی در این بخش به‌صورت خلاصه شرح داده می‌شوند.

- روش نقطه ها [۱۰]

این روش جزء روش‌های مبتنی بر خصوصیات است. در الفبای فارســـی تعـــداد زیادی از حـــروف دارای نقطه هستند. ۱۸ حرف از ۳۲ حرف که ۳ حرف دو نقطه، ۵ حرف ســـه نقطه و ۱۰ حرف یک نقطـــه دارند. از بین چهار حرف فارسی که با عربی متفاوت است سه حرف نقطه‌دار هستند. بنابراین در عربی ۱۵ حرف از ۲۸ حرف نقطه‌دار هســـتند. پس می‌توان گفت تعداد نقطه‌ها در هر متن فارسی یا عربی قابل توجه است.

18- Method based on curves
19- Approach Based on Vertical Straight Line
20- Quadruple categorization

در این روش اطلاعاتی که باید مخفی شوند ابتدا فشرده می‌شوند. سپس در متن مورد نظر اولین حرف نقطه‌دار پیدا می‌شـــود. با پیدا کردن آن به سراغ اطلاعات فشرده شده می‌رویم که این اطلاعات به صورت بیت‌های ۰ و ۱ هستند. بیت به بیت اطلاعات خوانده می‌شود اگر مقدار بیت ۰ بود، حرفی که از متن برای پنهان‌ســـازی انتخاب شـــده، بدون تغییر باقی می‌ماند. اما اگر ۱ بود نقطه مربوط به حرف به ســـمت بالا کمی جابه‌جا می‌شود. این روش تکرار می‌شود تا همه اطلاعات در متن مخفی شـــوند. برای منحرف کردن توجه خوانندگان بعد از مخفـــی کردن همه اطلاعات، نقاط مربوط به بقیه حروف به صورت تصادفی تغییر می‌کنند. برای حروفی که دو یا سه نقطه دارند، همه نقاط تغییر مکان می‌دهنـــد؛ به دلیل این‌که تغییـــر دادن یک نقطه از بین نقاط دیگر یک حرف توجه افراد را جلب می‌کند.

اســـتخراج اطلاعات: برای استخراج اطلاعات، برنامه با شناخت مقدار بیت پنهان شـــده براساس مکان نقاط روی حروف شروع می‌شـــود. به‌وسیله قرار دادن همه بیت‌های استخراج شده کنار یکدیگر، اطلاعات فشرده شده به‌دست می‌آید. ســـپس این اطلاعات از حالت فشرده خارج شده و پیام محرمانه اصلی به‌دست می‌آیند.

-استفاده از شکل حروف [۱۶]

در این روش که جزء روش‌های پنهان‌نگاری اســـت و بـــر روی تصاویر متن کار می‌کنـــد، از چهار حرف (ر ز ژ و) استفاده می‌شود. این حروف شیب خاصی در شکلشان دارند و می‌توان از این شیب برای پنهان‌نگاری داده استفاده کرد. از بین این چهار حرف، سه‌تای آن‌ها در الفبای عربی هم موجود است، بنابراین بجز متن‌های فارسی در متن‌های عربی نیز می‌توان از این روش استفاده کرد.

ســـه حـــرف (ر ز ژ) تنهـــا در تعـــداد نقاط بـــا یکدیگر متفاوت‌انـــد بنابراین در این روش متغیری که برای شـــیب این سه حرف در نظر گرفته می‌شود از متغیر شیب مربوط به حرف (و) جدا می‌شود. الگوریتم از چهار متغیر استفاده می‌کند که دو متغیر اول مربوط به شیب حروف (ر ز ژ) و حـــرف (و) در تصویر متن اصلی و دو متغیر دیگر مربوط به شیب تغییر یافته حروف (ر ز ژ) و حرف (و) در تصویر متن نهان‌نگاری شده است.

روش پنهان‌سازی با استخراج حروف شیب‌دار (حروف ذکر شده در بالا) از تصویر متن اصلی شروع می‌شود. اگر بیت مورد نظر برای پنهان‌ســـازی ۰ بود تغییری در شیب حرف ایجاد نمی‌شـــود اما اگر بیت مورد نظر ۱ بود شیب حرف تغییر می‌کند. این روش ادامه می‌یابد تا همه اطلاعات، مخفی شوند.

اســـتخراج اطلاعات: شـــیب تمـــام حروف شـــیب‌دار اندازه‌گیری شـــده و اختلاف آن با متغیر مربوط به شـــیب اصلی حروف مقایســـه می‌شود. اگر اختلافی وجود داشت یعنـــی بیـــت پنهان شـــده در این حرف ۱ اســـت و در غیر اینصورت بیت ۰ می‌باشد.

- استفاده از نویسهٔ کشش [۱۷]

در استاندارد یونیکد حرفی با کد شانزدهی ۰۶۴۰ موجود اســـت. این حرف به‌عنوان یک حرف مازاد تنها برای اهداف ســـاختاری و چیدمانی استفاده می‌شود. این حرف در همه جا قابل استفاده نیست و تنها در فضای بین حروف متصل شونده عربی استفاده می‌شود به عبارت دیگر بعد از حروف آخر کلمات یا قبل از حروف اول کلمات قرار نمی‌گیرد. وقتی این حرف بین دو حرف متصل شونده قرار می‌گیرد اندکی بین دو حرف کشش ایجاد می‌کند. از این نویسه برای اهداف پنهان‌ســـازی استفاده شده اســـت که در ادامه توضیح داده می‌شـــود. برای پنهان‌کردن یک رشته بیتی به‌عنوان مثال با مقـــدار «۱۱۰۰۱۰» از کم ارزش‌تریـــن بیت که در این مثال ۰ اســـت، الگوریتم آغاز می‌شـــود. اگر بیت مربوطه ۰ بود، در اولین حرف بدون نقطه‌ای که بعد از آن امکان اضافه کردن حرف کشـــش وجود داشته باشـــد؛ بیت را با اضافه کردن حرف کشش مخفی می‌کند. اگر بیت مربوطه ۱ بود، در اولین حرف نقطـــه‌داری که بعد از آن امـــکان اضافه کردن حرف کشش وجود داشته باشـــد بیت را مخفی می‌کند. به عبارت دیگر بیت ۰ را با اضافه کردن حرف کشـــش بعد از حروف

بدون نقطه و بیت ۱ را با اضافه کردن حرف کشش بعد از حروف نقطه‌دار پنهان‌سازی می‌کند.

استخراج اطلاعات: استخراج اطلاعات در این روش عکس عمل پنهان‌سازی است. اگر بعد (قبل) از حرف نقطه‌دار حرف کشش وجود داشت، بیت پنهان شده ۱ است و اگر بعد (قبل) از حرف بدون نقطه حرف کشش وجود داشت، بیت پنهان شده ۰ است.

-روش توسعه یافته استفاده از نویسهٔ کشش [۱۸]

ایده اصلی این روش افزایش ظرفیت پنهان‌سازی با استفاده از همه موقعیت‌های ممکن برای استفاده از نویسه کشش در حروف عربی است. ۲۸ حرف در زبان عربی وجود دارد که بعضی از این حروف بیشتر از یک شکل دارند برای مثال حرف «ا» شش شکل متفاوت دارد {ا آ ؤ إ أ ئ}. به این صورت ۲۸ حرف عربی می‌توانند با ۳۵ شکل مختلف ظاهر شوند. در این روش تمام مکان‌های بین حروف که امکان اضافه کردن نویسه کشش قبل یا بعد از آن‌ها وجود دارد با استفاده از تمام شکل‌های حروف عربی بررسی شده است. در این روش که در واقع توسعه یافته روش قبلی است، پنهان‌سازی و استخراج پیام نیز مانند قبل است. این روش MSCUKAT نامیده شده است.

-روش پنهان‌سازی با استفاده از قابلیت‌های یونیکد [۱۹]

در استاندارد یونیکد، برای حروف عربی دو حالت ذخیره‌سازی کد وجود دارد یک کد که نماینده حرف است و بستگی به موقعیت حرف در کلمه ندارد. نوع دیگر ذخیره‌سازی کد بستگی به موقعیت حرف در کلمه دارد و به چهار نوع ظاهر می‌شود و برای هر نوع یک کد جدا وجود دارد [۲۰]. در یونیکد تنها کد نماینده حرف در فایل متنی ذخیره می‌شود و برنامه بر حسب موقعیت حرف در کلمه شکل صحیح را نشان می‌دهد. اگرچه می‌توان کد شکلی را نیز ذخیره کرد. از این ویژگی یونیکد در این روش پنهان‌سازی استفاده شده است.

برای پنهان‌سازی بیت ۰، کد نماینده حروف در هر کلمه ذخیره می‌شود و برای بیت ۱، کد شکلی حروف در کلمه ذخیره می‌شود. نمی‌توانیم از کد شکلی و کد نماینده حروف در یک کلمه با یکدیگر استفاده کنیم به دلیل این‌که برنامه نمی‌تواند شکل حروف را در کلمه به‌طور صحیح تشخیص دهد.

استخراج اطلاعات: کد حروف کلمه بررسی می‌شود. اگر کدهای ذخیره شده کلمه، کد نماینده حروف باشد نتیجه گرفته می‌شود که کد ۰ مخفی شده اما اگر با شکل حرفی ذخیره شده باشد کد ۱ مخفی شده است.

- روش بهبود یافته لا [۲۱]

کلمه «لا» یک نویسه با کد FEFB در استاندارد یونیکد است. می‌توان به صورت دیگری نیز کلمه لا را نشان داد که به صورت (حرف ل+نویسه فاصله بین حروف با کد شانزدهی ۰۶۴۰+حرف ا) است که به صورت «لـا» نشان داده می‌شود.

برای پنهان‌سازی بیت ۱ از نویسهٔ «لا» و برای بیت ۰ از « لـا» استفاده می‌شود. این روش در نمونه قبلی لا استفاده می‌شده است اما به دلیل مشکلاتی که این روش داشته است از قبیل افزایش حجم فایل و به دلیل گذاشتن فاصله بین «ل» و «ا» کلمه را پهن تر کرده و ظاهر متن را غیرطبیعی می‌کند [۲۲]. در روش بهبود یافته به جای وارد کردن کد فاصله بین «ل» و «ا» کد شکلی آن‌ها آورده می‌شود و کلمه به صورت «لـا» نشان داده می‌شود.

استخراج اطلاعات: عکس عمل پنهان‌سازی است و اگر در متن «لا» باشد بیت مخفی شده ۱ و اگر «لـا» باشد بیت مخفی شده ۰ است. این روش مشکلات روش قبلی لا را برطرف کرده است.

- استفاده از حروف مشابه با کدهای متفاوت [۸]

بین بعضی از حروف عربی و فارسی مثل «ی» و «ک» در شکل ظاهری آن‌ها تفاوت وجود دارد. برای مثال «ی» در فارسی به صورت «ی» و «ی» در عربی به صورت «ي» و حرف «ک» نیز در فارسی به صورت

«ک» و در عربی به صورت«ك» نشان داده می‌شود.

از این قابلیت می‌توان برای پنهان‌سازی استفاده کرد. این روش به این صورت است: برای پنهان کردن بیت ۱ از شـــکل عربی حروف و برای بیت ۰ از شـــکل فارسی آن‌ها استفاده می‌شود.

– استفاده از فاصله نمادین بین کلمات [۱۹]

در فارســـی و عربی، فاصله‌ای بین کلمات وجود دارد. در بعضی کلمات مثل «رفته‌ام» یک فاصله کم بین دو قسمت یـــک کلمه وجود دارد. این فاصلـــه به‌عنوان فاصله نمادین شناخته می‌شـــود. درسیســـتم یونیکد فاصله معمولی کد شانزدهی ۰۰۲۰ را دارد ولی فاصله نمادین یا نیم‌فاصله که کد zwnj نیز نامیده می‌شود کد C۲۰۰ را دارد.

مخفی کردن اطلاعات در این روش به این صورت است که اگر در کلمه‌ای فاصله نمادین وجود داشـــت، یکی از دو فرم فاصله را بســـته به اطلاعاتی کـــه می‌خواهیم در متن پنهان کنیم انتخاب می‌کنیم. برای پنهان کردن بیت ۱ فاصله معمولی را بعد از فاصله نمادین در کلمه اضافه می‌کنیم و اگـــر بخواهیم بیت ۰ را پنهان کنیم، فاصله نمادین را تغییر نمی‌دهیم.

اســـتخراج اطلاعات: اگر در کلمـــه‌ای از فاصله نمادین اســـتفاده شده بود یعنی بیت ۰ در آن پنهان شده و اگر هم از فاصله نمادین و هم فاصله معمولی استفاده شده باشد، بیت ۱ در آن پنهان شده است.

– استفاده از عبارات منظم zwnj و zwj[21] [۲۳]

در سیســـتم یونیکد نویســـهٔ zwj با کد D۲۰۰ و نویسهٔ zwnj با کد C۲۰۰ جزء نویســـه‌های شفاف هستند. نویسهٔ zwj وقتـــی بیـــن دو حرف قرار می‌گیـــرد باعث اتصال دو حرف به یکدیگر می‌شود و نویسهٔ zwnj برخلاف آن هنگام قـــرار گرفتن بین دو حرف آن دو را از یکدیگر جدا می‌کند. بـــرای مثال «م zwj ح» به صورت «مـــح» و «م zwnj ح» به صورت «م ح» دیده می‌شود.

این روش با بهبود روش [۱۹] اطلاعات را به جای پنهان کـــردن یک بیت درون حرف‌ها، درون کلمات پنهان می‌کند. در این حالت نویســـهٔ zwj معادل بیت ۱ و zwnj معادل بیت ۰ هستند. برای پنهان‌سازی، یک گروه از zwj و zwnj ها با اندازه بلوک مشـــخص به کلمات اضافه می‌شود. از دو نوع عبارت منظم برای پنهان‌ســـازی استفاده می‌کند. یک حرف غیرمتصل یا نویسهٔ فاصله +zwnj+ گروهی از zwj یا zwnj ها+ یک حـــرف غیرمتصل یا نویســـهٔ فاصله. حروف غیر متصل در زبان عربی شامل (د، ذ، ر، ز، و، ا) هستند.

– استفاده از عبارت منظم LZW [۲۴]

ساتیرو ایسیک[22] درسال۲۰۱۲روش پنهان‌نگاری متن‌مبتنی بر فشرده‌ســـازی LZW را ارائه کردند که در آن عوامل امنیت و ظرفیت در نظر گرفته شده است. در این روش از رمزگذاری LZW برای بالا بردن ظرفیت و امنیت، استفاده می‌شود. علاوه براین کلیدهای پنهان‌نگاری ایجاد می‌شوند و رمزگذاری مبتنی بر ترکیبات برای بالا بردن امنیت و تأمین موارد تصادفی دلخواه به کار می‌رود. در این روش اطلاعات پنهان شده بدون استفاده از کلیدهای پنهان‌نگاری به راحتی قابل رمزگشایی نمی‌باشند. همچنین روال رمزگشـــایی توســـط رمزگذاری LZW پیچیده می‌باشد.

۳-۳-روش های پنهان نگاری متن در صفحات وب

روش‌هـــای مختلفی برای پنهان کـــردن متن داخل کد منبـــع فایـــل XML وجود دارد، که در حـــال حاضر برای پنهان‌ســـازی متـــن در HTML نیز مورد اســـتفاده قرار می‌گیـــرد. در این روش‌ها، از برچســـب‌های خاص برای پنهان‌نگاری استفاده می‌شود [۲۵].

– استفاده از عناصر خالی (تهی)[23] [۲۶]

در ایـــن روش ممکن اســـت بعد از برچســـب شـــروع بلافاصله برچسب پایان نوشته شود و یا از برچسب‌های خالی استفاده شـــود. با این دو عمل می‌توان داده‌ها را در کدهـــای HTML مخفی نمود. در مثال زیر، یک بیت از داده بعد از هر برچسب پایانی یا عناصر خالی پنهان می‌شود:

21- zero-width joiner(zwj)

22- Satir & Isik

23- Representation of empty elements

Example 1.

stego key:

<img></img>... 0

<img/>... 1

stego data:

<img src=«foo1.jpg«></img>

<img src=«fooS.jpg«></img>

Embedded data:

01110

- فضای خالی در برچسب ها[24] [۲۷]

در این روش با اضافه کردن فضای خالی در برچسب‌ها، امکان پنهان کردن داده‌ها را فراهم می‌کند. در زیر یک مثال از روش پنهان کردن اطلاعات با قرار دادن یا حذف کردن یک فضا ارائه شده است. فضای خالی در برچسب‌ها هیچ تاثیری در شکل ظاهری صفحات وب ندارد.

Example 2.

stego key:

<tag>, </tag>, or <tag/>... 0

<tag >, </tag >, or <tag />... 1

stego data:

<user ><name>Alice</name ><id >01 </id></user>

<user><name >Bob</name><id>02</id ></user >

Embedded data:

101100 010011

- ترتیب قرار گرفتن عناصر[25] [۲۷]

در ایـــن روش اطلاعات با تغییـــر در نحوه قرار گرفتن برچسب‌ها در کدها پنهان می‌شود. در مثال زیر هر بیت با استفاده از دو عنصر پنهان می‌شود.

Example 3.

stego key:

<user><name>NAME</name><id>ID</id></user>... 0

<user><id>ID</id><name>NAME</name></user>... 1

stego data:

<user><name> Alice</name><id>01 </id></user>

<user><id>02</id><name>Bob</name></user>

Embedded data:

01

- ترتیب قرار گرفتن ویژگی ها[26] [۲۶]

در این روش اطلاعـــات محرمانه با تبادل نظم ظاهری ویژگی‌هـــای موجود در عناصـــر در کدهای HTML پنهان می‌شوند.

Example 4.

stego key:

<event month= ‘MONTH’ date= ‘DATE’ >EVENT</event>... 0

<event date= ‘DATE’ month= ‘MONTH’ >EVENT</event>... 1

stego data:

<event month=‘JUL’ date=‘4’>Independence day</event>

<event date=‘24’ month=‘DEC’>Christrnas</event>

Embedded data:

01

- استفاده از چند عنصر[27] [۲۷]

در این روش از دو یا چند عنصر به صورت تودرتو استفاده می‌شـــود. در مثال زیر با استفاده از برچسب‌های درونی[28] و بیرونی[29] ارزش هر بیت اطلاعات مشخص می‌شود.

Example 5.

stego key:

<favorite><fruit>SOMETHING</fruit></favorite>... 0

<fruit><favorite>SOMETHING</favorite></fruit>... 1

stego data:

<fruit><favorite>orange</favorite></fruit>

<favorite><fruit>apple</fruit></favorite>

Embedded data:

10

- تغییر شکل حروف برچسب ها[30] [۲۸]

در ایـــن روش با تغییر در بزرگـــی و کوچکی حروف

24- White spaces in tags
25- Appearing order of the elements
26- Appearing order of the attributes
27- Elements containing other elements
28- inner
29- outer
30- Change Case of letter in tag

در برچســـب‌ها، داده‌ها به صورت بیت‌های صفر و یک در کد پنهان می‌شـــوند، حروف بزرگ برای پنهان کردن بیت ۱ و حـــروف کوچک برای پنهان‌ســـازی بیت صفر. در این روش پیام محرمانه ابتدا تبدیل به کد اسکی می‌شود و بعد از آن به کد دودویی تبدیل می‌شـــود و ســـپس با استفاده از خاصیـــت فوق پیام محرمانـــه در کدهای HTML پنهان می‌شود.

Example 6.

Stego key:

Uppercase …1

Lowercase …0

Stego data:

<hTml>

<body bColor='gRay'>

<table> <tR>

<Td width='200' align='center'>test</td></tr>

< td wiDth='200' align='center' height='50'> Hiding information</td></tr>

</table>

</bodY></Html>

Embedded data:

10110110011001

- تغییر علامت گیومه ارزش ویژگی ها در برچسب ها[۳۱] [۲۹]

در این روش با تغییر در تعداد گیومه‌ها در برچسب‌ها داده‌ها پنهان می‌شود. برای مثال دو تا گیومه نماد بیت یک و یک گیومه نماد بیت صفر است.

Example 7.

Stego key:

<td width='200'> ….1

<td width='200'> ….0

Stego data:

<html>

<body bColor='gray'>

<table> <tr>

<td width='200' align='center'>test <font color='red' size='5'></td><tr>

<td width='200' align='center' hight='50'> Hiding information</td></tr>

</table>

</body></html>

Embedded data:

1010110

- تکرار ویژگی ها[۳۲] [۲۸]

در ایـــن روش داده‌هـــای محرمانـــه با تکـــرار ویژگی برچســـب‌ها در متـــن کدهـــای HTML پنهان می‌شـــوند. در مثـــال زیـــر یـــک بیـــت داده با تکـــرار ویژگـــی پنهان شده است.

Example 8.

Stego key:

<td width='200'> ….1

<td width'200' width='200'> ….0

Stego data:

<html>

<body bColor='gray'>

<table> <tr>

<tdwidth='200'width='200'align='center'align='center'>

test <font color='red' size='5'size='5'> </td></tr>

<td width='200' align='center' height='50'height='50'>

Hiding information</td></tr>

</table>

</body></html>

Embedded data:

10010110

۴- تحلیل و بررسی روش‌های پنهان نگاری

در این بخش به مقایســـه و تحلیـــل روش‌های معرفی شـــده در بخش‌های پیشـــین خواهیم پرداخـــت. در جدول ۱ به بررســـی و مقایســـه نقاط قـــوت و ضعف روش‌های پنهان‌نگاری در متن‌های انگلیسی پرداخته می‌شود.

جدول ۲ به اختصار به بررسی مزایا و معایب روش‌های پنهان‌نگاری در متن‌های فارسی می‌پردازد.

۵-جمع بندی

در این مقاله به بررســـی و مقایسه روش‌های موجود

31- Change quotation marks of attributes value in tags

32- Repeat attributes

جدول ۱: نقاط قوت و ضعف روش‌های پنهان نگاری در متن‌های انگلیسی

روش	مزایا	معایب
انتقال خط [۱۳]	این روش برای متن چاپی مناسب است.	هنگامی که از برنامه تشخیص و شناسایی نویسه استفاده می‌کنیم، اطلاعات پنهان شده، از بین می‌رود.
انتقال کلمه [۱۲]	روش انتقال کلمه به دلیل تغییر جزئی در فاصله کلمات، احتمال کشف کمتری دارد.	الگوریتم مربوط به انتقال کلمه، به راحتی قابل تشخیص است.
روش نحوی [۹]	-	با استفاده از پویشگر هوشمند به راحتی می‌توان اطلاعات پنهان شده را کشف نمود.
روش معنایی [۱۰]	این روش بهتر از روش‌های نحوی، انتقال خط و انتقال کلمه است. به دلیل این که توسط برنامه‌های تشخیص و شناسایی نویسه، قابل تشخیص نمی‌باشد.	پویشگر هوشمندی که دانش زیادی در مورد کلمات مترادف و یا متضاد دارد، می‌تواند پیام محرمانه را کشف کند.
روش اختصاری [۱۱]	-	حجم بسیار کمی از داده‌ها را می توان در این روش پنهان کرد.

جدول ۲: بررسی نقاط قوت و ضعف روش‌های پنهان نگاری در متن‌های فارسی

روش	مزایا	معایب
روش نقطه ها [۱۰]	۱- مخفی کردن حجم زیادی از اطلاعات به دلیل وجود تعداد زیاد حروف نقطه دار در فارسی و عربی ۲- از بین بردن اطلاعات مخفی شده دشوار است. ۳- به علت نبود یک برنامه تشخیص حروف نوری (1OCR) قوی برای زبان‌های فارسی و عربی، متن چاپی به آسانی به متن عادی تبدیل نمی‌شود. ۴- استفاده از متن چاپی با اسکن	۱- از بین رفتن اطلاعات در تایپ دوباره ۲- استفاده از تنها یک فونت قالب ثابت برای متن خروجی ۳- مشکل در استفاده برای متونی که چاپ و دوباره اسکن شده‌اند به دلیل عدم وجود یک برنامه OCR خوب برای زبان‌های فارسی و عربی
استفاده از شکل حروف [۱۶]	۱- شفاف تر از روش‌های جابه جایی خط و کلمه است. به دلیل این‌که از بعضی حروف در آن استفاده می شود و نه همه آن‌ها، برای سیستم بینایی انسان نامحسوس است. ۲-داشتن ظرفیت پنهان‌سازی بالاتری در مقایسه با بقیه روش‌ها ۳- دسته بندی در روش‌های کور. به عبارت دیگر رمزگشا به یک کپی از سند اصلی نیاز ندارد تا اطلاعات مخفی شده را استخراج کند.	
استفاده از نویسهٔ کشش [۱۷]	۱- این روش هر سه خصوصیت ظرفیت، امنیت و مقاومت که جنبه‌های لازم برای پنهان‌سازی هستند را به برآورده می‌کند. ۲- عدم تغییر در محتوای نوشتاری به دلیل استفاده از قابلیت‌های یونیکد	۱- افزایش حجم فایل، برای پنهان‌سازی هر بیت، یک نویسه به متن اضافه می شود.
روش پنهان‌سازی با استفاده از قابلیت‌های یونیکد [۱۹]	۱- ظرفیت ذخیره سازی این روش تقریباً با روش نقطه‌ها برابر است. ۲- ظرفیت پنهان‌سازی مناسبی دارد و یک بیت را در هر کلمه مخفی می‌کند.	
استفاده از فاصله نمادین بین کلمات [۱۹]	۱- ظرفیت پنهان‌سازی این روش در حدود ۴ بیت در هر کیلوبایت است. ۲- عدم وابستگی به هیچ فونت و فرمتی ۳- استفاده از قالب‌های بسیاری مانند HTML یا Word	۱- افزایش زیاد اندازه متن

پنهان‌نگاری در متن اعم از متن‌های انگلیسی، متن‌های فارسی و صفحات وب پرداخته شد. با وجود آن‌که هر یک از روش‌های پنهان‌نگاری با یک روش تحلیلی قابل کشف است اما از آنجا که می توان اطلاعات محرمانه را در رسانه‌های مختلف مانند تصویر، صوت، ویدیو، موسیقی و غیره پنهان نمود، بررسی تمام رسانه‌های موجود از نظر دارا بودن اطلاعات محرمانه کار ساده‌ای نیست. اما چنانچه تمرکز بر روی متن یا برچسب‌های کد صفحات وب باشد

کشف اطلاعات ساده‌تر خواهد بود. باید به این نکته توجه داشت که اســتفاده از کلیدهای محرمانه و تصادفی‌سازی اطلاعات محرمانه قبل از پنهان‌سازی کشف اطلاعات را با چالش بزرگتری مواجه می‌کنــد. حتی برای افزایش امنیت اطلاعــات می‌توان اطلاعات را قبل از مخفی کردن توســط روش پنهان‌نگاری رمزنگاری کرد.

منابع

[۱] ع. احمــدی باغکی، «پنهان‌ســازی اطلاعات،» ماهنامــه الکترونیکی ارتباط علمی، جلد چهارم، شماره اول، ۱۳۸۳.

[2] J. C. Judge, «Stegangoraphy: Past, Present, Future,« SANS Institute Publications, 2001.

[3] K. Rabah, «Steganography-The Art of Hiding Data,« Information Technology Journal, vol. 3, no. 3, pp. 245-269, 2004.

[4] T. Jamil, «Steganography: the Art of Hiding Information in Plain Sight,« IEEE, vol. 18, no. 1, pp. 10-12, 1999.

[5] M. H. Shirali-Shahreza and M. Shirali-Shahreza, «A Survey of Information Hiding,« in Handbook of Research on Secure Multimedia Distribution, 2009, pp. 241-256.

[6] J. Cummins, P. Diskin, S. Lau and R. Parlett, «Steganography and Digital Watermarking,« The University of Birmingham, 2003.

[7] C. Dhanani, K. P. Panchal and M. Scholar, «Steganography Using Web Documents as a Carrier: a Survey,« International Journal of Engineering Development and Research (IJEDR), pp. 172-179, 2013.

[8] M. H. Shirali-Shahreza and M. Shirali-Shahreza, «Arabic/ Persian Text Steganography Utilizing Similar Letters With Different Codes,« The Arabian Journal for Science and Engineering, vol. 35, pp. 213-222, 2010.

[9] W. Bender, D. Gruhl, N. Morimoto and A. Lu, «Technique For Data Hiding,« IBM Systems Journal, vol. 35, no. 4, pp. 316-336, 1996.

[10] M. Shirali-Shahreza and M. H. Shirali- Shahreza, «A New Approach to Persian/ Arabic Text Steganography,« Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ ACIS International Conference on, pp. 310-315, 2006.

[11] M. Shirali-Shahreza and M. H. Shirali- Shahr, «Text Steganography in Chat,« IEEE, 2007.

[12] M. Shirali-Shahreza, «Text Steganography by Changing Words Spelling,« ICACT, 2008.

[13] y. w. Kim, K. Moon and I. Oh, «A Text Watermarking Algorithm Based on Word Classification and Inter-word Space Statistics,« IEEE, pp. 775-779, 2003.

[14] M. Shirali-Shahreza and M. H. Shirali- Shahreza, «Text Steganography in SMS,« Convergence Information Technology, pp. 2260-2265, 2007.

[15] S. Dulera, D. Jinwala and A. Dasgupta, «Experimenting With the Novel Approaches in Text Steganography,« International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 6, 2011.

[16] R. Davarzani and K. Yaghmaie, «Farsi Text Watermarking Based on Character Coding,« International Conference on Signal Processing Systems, pp. 152-156, 2009.

[17] A. Gutub and et. al, «Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking,« in International Conference on Security and Cryptography - SECRYPT, Barcelona, Spain, 2007.

[18] A. Al-Nazer and A. Gutub, «Exploit Kashida Adding to Arabic e-Text for High Capacity Steganography,« in Third International Conference on Network and System Security, Gold Coast, Queensland, Australia, Australia, 2009.

[19] M. Shirali-Shahreza, «Pseudo-Space Persian/Arabic Text Steganography,« IEEE/ACIS International Conference, pp. 864-868, 2008.

[20] M. Shirali-Shahreza and S. Shirali-Shahreza, «Persian/ Arabic Unicode Text Steganography,« Fourth International Conference on Information Assurance and Security, pp. 62-66, 2008.

[21] M. H. Shirali-Shahreza and M. Shirali-Shahreza, «An Improved Version of Persian/Arabic Text Steganography Using «La« Word«,« 6th National Conference on Telecommunication Technologies and IEEE, pp. 372-376, 2008.

[22] M. Shirali-Shahreza, «A New Persian/Arabic Text Steganography Using «La« Word«,« in Advances in Computer and Information Sciences and Engineering, Springer Netherlands, 2008, pp. 339-342.

[23] A. F. Al Azawi and M. A. Fadhil, «An Arabic Text Steganography Technique Using Zwj and Zwnj Regular Expressions,« International Journal and Academic Research, vol. 3, pp. 419-423, 2011.

[24] E. Satir and H. Isik, «A Compression—based Text Steganography Method,« The Journal of Systems and Software, vol. 85, no. 10, pp. 2385-2394, 2012.

[25] M. Garg, «A Novel Text Steganography Technique Based on Html Documents,« International Journal of Advanced Science and Technology, vol. 35, pp. 129-138, 2011.

[26] P. K. Aggarwal, Dharmendra, P. Jain and T. Verma, «Adaptive approach for Information Hiding in WWW Pages,« IEEE, pp. 113-118, 2014.

[27] S. Inoue, K. Makino, I. Murase, O. Takizawa, T. Matsumoto and H. Nakagaw, «A Proposal on Information Hiding Methods using XML,« 1st Workshop on NLP and XML, 2001.

[28] G. Xiaojun, C. Guang, Z. Chengang, Z. Aiping, P. Wubin and T. Dinhtu, «Make Your Webpage Carry Abundant Secret Informatin Unawarely,« IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, pp. 541-548, 2013.

[29] Y. Yang and Y. Yang, «An Efficient Webpage Information Hiding Method Based on Tag Attributes,« Proceedings of the 7th International Conference on Fuzzy Systems and Knowledge Discovery (IEEE), vol. 3, pp. 1181-1184, 2010.