چهارمین کنفرانس ملی ایده های نوین مهندسی برق
۲۰و۲۱ آبان ماه ۱۳۹۴ - دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)

پنهان نگاری دیجیتال تصویر بر مبنای تبدیل موجک گسسته جهت افزایش شفافیت و مقاومت در برابر حملات

مهرزاد رشیدی، فرساد زمانی بروجنی
دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)، گروه فنی و مهندسی کامپیوتر، اصفهان، ایران
m.rashidi@khuisf.ac.ir
s.zamani@khuisf.ac.ir

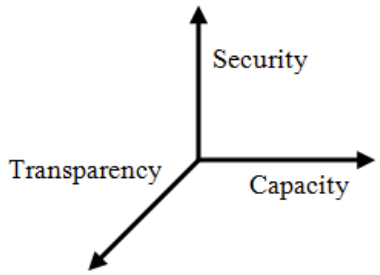
چکیده – با افزایش روز افزون تبادل اطلاعات از طریق شبکه های اجتماعی و بستر اینترنت مهم ترین مسئله ای که اهمیت فراوان پیدا کرده است محرمانه ماندن رابطه می باشد. پنهان نگاری در بسترهای دیجیتال موضوعی است که تقریبا در یک دهه اخیر توجه بسیاری از محققین را به خود جلب کرده است. هدف از پنهان نگاری مخفی کردن نامحسوس اطلاعات پیام در داخل سیگنال میزبان است که به صورت یک رسانه پوششی مانند صوت، ویدئو، متن و به ویژه تصویر می باشد. بنابراین باید روشی استفاده شود که در برابر دستکاری های عمدی و غیرعمدی مقاوم باشد. برای دست یافتن به این هدف اکثر الگوریتم های ارائه شده به منظور مقاوم سازی و حفظ کیفیت و شفافیت پنهان سازی در حوزه های مختلف پیاده سازی شده اند.مقصود از انجام این مقاله برقراری ارتباط پنهان داده توسط سیگنال تصویر می باشد به صورتیکه دشمن از ماهیت این ارتباط آگاه نگردد. به بیان دیگر پنهان نگاری تصویر به منظور افزایش شفافیت و مقاومت در برابر حملات مورد بحث قرار می گیرد و روشهایی که بهترین راه را ارائه کرده اند بیان می شوند.

کلید واژه- افزایش شفافیت پنهان نگاری، پنهان نگاری، تبدیل موجک گسسته، مقابله با حملات

۱- مقدمه

با توجه به گسترده شدن استفاده از کامپیوتر و سیستمهای ارتباطی و اتصال به شبکه های جهانی در دهه های اخیر ایجاد کانالی امن برای داشتن ارتباط و تبادل داده محافظت شده بیش از پیش احساس می شود. برای بدست آوردن این حفاظت دو راه وجود دارد: ۱- پنهان نگاری و ۲- رمزنگاری، که در پنهان نگاری اطلاعات یا پیغام اصلی در یک پیغام یا هر رسانه‌ی پوششی مانند صوت، تصویر، متن یا ویدئو پنهان می گردد؛ ولی در رمزنگاری افراد از ارسال اطلاعات محرمانه باخبرند فقط نمی توانند آن اطلاعات را بخوانند[4]. این ضعف رمزنگاری باعث شد که پنهان نگاری اطلاعات برای ارسال کنندگان مورد توجه قرار گیرد. تصاویر یکی از مهم ترین رسانه های پوششی مورد استفاده در پنهان نگاری می باشد چرا که درک بصری انسان از تغییرات در تصاویر محدود است. از میان انواع ساختارهای تصویری، فرمت JPEG بیشترین فرمتی است که در بین کاربران برای تبادل اطلاعات استفاده می شود[5]. این فرمت متداول ترین روش برای ذخیره سازی تصاویر به دو دلیل می باشد:۱-توانایی حفظ کیفیت بصری تصویر ۲-ایجاد امکان فشرده سازی با نرخ بالا[7].

پنهان سازی اطلاعات به دو دسته پنهان نگاری و نهان نگاری تقسیم می شود. هدف از پنهان نگاری مخفی ماندن خود ارتباط است بنابراین زمانی در پنهان شکنی می توانیم بگوییم حمله کننده موفق عمل کرده است که بتواند به وجود ارتباط یا پیام مخفی پی ببرد، درصورتی که هدف از نهان نگاری پنهان کردن خود پیام می باشد. همانطور که در ابتدا اشاره کردیم تصاویر یکی از پرطرفدارترین رسانه های تبادل اطلاعات در اینترنت می باشند و از آن به عنوان پوشش دهنده پیام بهره می برند[2]. برای ارزیابی و مقایسه الگوریتم های پنهان نگاری شاخص هایی تعریف شده اند، که با استفاده از آنها میتوان روش متناسب با کاربرد مورد نظر را انتخاب کرد. شش شاخص مقاومت، ظرفیت، امنیت، شفافیت، قابل کشف نبودن و پیچیدگی توسط Petitcolas تعریف شده اند [3]و[6]. باید توجه داشت که امکان بهینه سازی تمام شاخص ها همزمان وجود ندارد و با بهبود یکی، امکان تضعیف یک یا چند شاخص دیگر وجود خواهد داشت. طبق شکل 1شاخص ظرفیت همواره با دو شاخص شفافیت و امنیت در نزاع است[6].

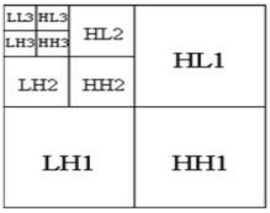


شکل ۱: ارتباط بین امنیت، ظرفیت و شفافیت

در این مقاله برای ارزیابی ویژگی شفافیت و مقاومت، مقایسه ای با روشهای ارائه شده‌ی تاکنون صورت می گیرد و در قسمت دوم بر تحقیقات انجام شده مروری خواهیم داشت که مزایا و معایب هر روش بررسی می شود. در قسمت سوم روشی که بهترین راه حل برای شفافیت و مقاومت را ارائه نموده است بیان می شود، و در آخر نیز نتیجه گیری بیان می گردد.

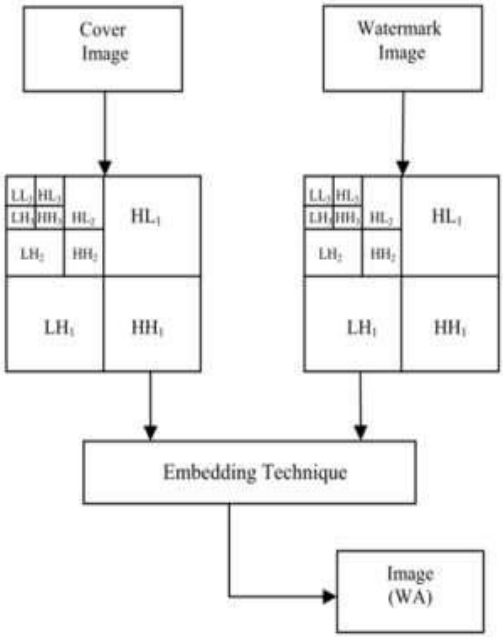
۲- پیشینه تحقیقات

زهره زراعتی دیزچه و همکاران در تحقیقی به عنوان " نهان نگاری مبتنی بر موجک با انتخاب بهینه زیر باند فرکانسی به منظور افزایش شفافیت و مقاومت " با روش پیشنهادی تبدیل موجک گسسته (DWT) به نتایج زیر دست یافتند[6]: ایده اساسی در DWT برای سیگنال یک بعدی به این صورت است که سیگنال حوزه زمان (یا مکان) به دو قسمت فرکانس بالا و فرکانس پایین تقسیم می شود. در تبدیل DWT دو بعدی در سطح یک تصویر دارای چهار ناحیه LL، HL، LH و HH می باشد که بخش تقریبی از تصویر اصلی را قسمت LL پوشش می دهد و سه زیر باند باقی مانده نشان دهنده جزییات افقی (HL)، عمودی (LH) و مورب (HH) می باشد[6]. در سطح دو تبدیل قسمت LL1 نیز به چهار ناحیه مشابه سطح یک تقسیم می شود در سطح سه نیز ناحیه LL2 هم به چهار قسمت تقسیم شده و این روند تا سطح دلخواه ادامه دارد. همانطور که در شکل ۲ نشان داده شده است ساختار حوزه تبدیل موجک دارای ساختار هرمی شکل می باشد.

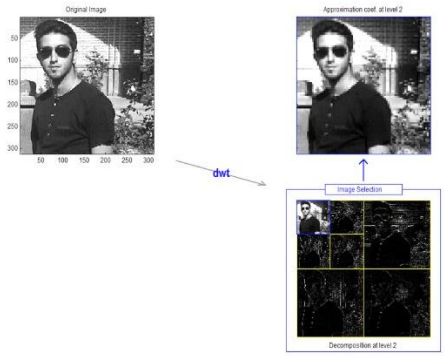


شکل ۲: ساختار تبدیل موجک تصویر

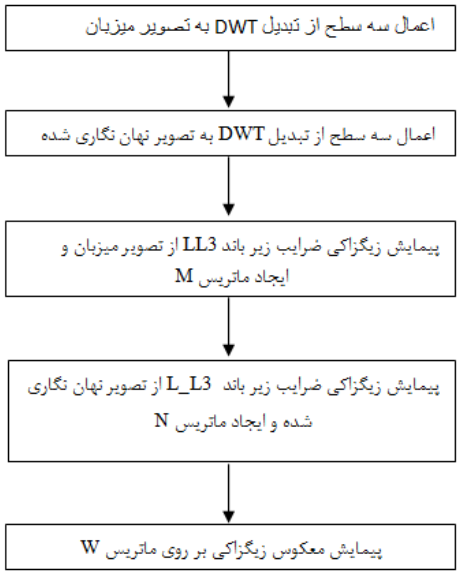
الگوریتم پیشنهادی مقاله فوق طی مراحل زیر در تصویر گنجانه درج می شود[6]: ۱) اعمال سه سطح از تبدیل DWT به تصویر پوشانه ۲) اعمال سه سطح از تبدیل DWT به تصویر گنجانه ۳) پیمایش زیگراکی ضرایب زیرباند LL3 از تصویر پوشانه و ایجاد ماتریس M ۴) تعبیه زیر باندLL3 از تصویر گنجانه در ماتریس M با استفاده از ضریب آلفا ۵) پیمایش معکوس زیگراکی زیر باند تغییر یافته ۶) اعمال معکوس DWT برروی تصویر شامل زیر باند تغییریافته برای تولید تصویر گنجانه، که در شکل ۳ فرآیند تعبیه گنجانه و در شکل ۵ فرآیند استخراج آن نمایش داده شده است.



شکل ۳: فرآیند تعبیه گنجانه



شکل ۴: پیاده سازی فرآیند تعبیه در تبدیل موجک گسسته

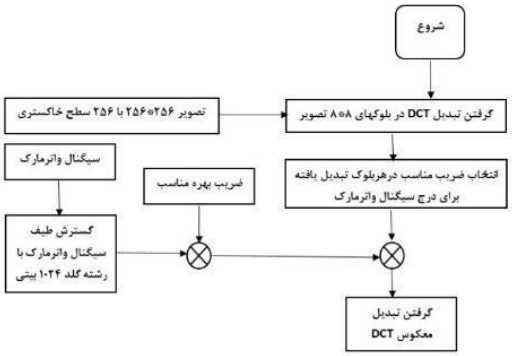


شکل ۵: فرآیند استخراج گنجانه

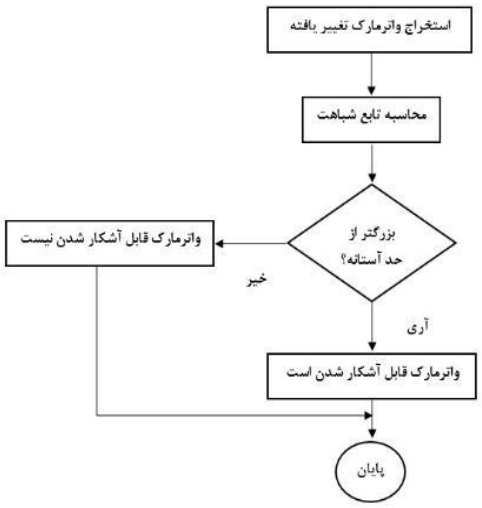
لیلی احسان، فاطمه ادریسی و همکاران در تحقیقی به عنوان "نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه تبدیل گسسته کسینوسی" با روش پیشنهادی کاکس که نتایج زیر را بدست آوردند[8]: در این روش سیگنال نهان نگاری در مهمترین مولفه های تصویر از نظر بینایی انسان، قرار داده می شود. ابتدا تبدیل DCT تصویر صورت می گیرد و سپس پیام طیف گسترده در مهمترین مولفه های طیفی تصویر قرار داده می شود. برای ایجاد امکان مقاومت بیشتر از بلوکهای 8*8 تصویر، تبدیل DCT صورت می گیرد سپس در هربلوک 8*8 که به صورت تصادفی انتخاب می گردد ضریب مورد نظر از سیگنال نهان نگاری درج می گردد. در مقاله تحقیقی خانم احسان و همکاران درج نهان نگاری در ابتدا سیگنال پیام را به یک سیگنال دو قطبی تبدیل می کند و هربیت آن را در یک رشته ۱۰۲۴ بیتی ضرب می کند. سیگنال طیف گسترده نهان نگاری از حاصل جمع بیت های بدست آمده بر روی تمام سیگنال پیام انجام می گیرد. فرمول زیر نحوه آشکارسازی سیگنال نهان نگاری را نمایش می دهد:

$$Sim(X,X_*) = \frac{x.x*}{\sqrt{x*.x*}} \qquad (۱)$$

رابطه بالا برای اندازه گیری شباهت بین سینگال اصلی نهان نگاری و سیگنال استخراج شده است. طبق آمار بدست آمده گرچه افزایش ضریب بهره، مقاومت نهان نگاری را در برابر اکثر حملات به خصوص آنهایی که با افزودن نویز و عبور از فیلترهای مختلف همراهند به نحو قابل ملاحظه ای افزایش می دهد ولی در برابر حملات مربوط به بریدن بخشی از تصویر تأثیر چندانی در بالابردن مقاومت سیگنال ندارد[8]. علت آن هم این است که در حمله با کمبود نواحی سیگنال نهان نگاری مواجه هستیم و بالا بردن ضریب بهره کمکی به افزایش مقاومت سیگنال نهان نگاری نمی کند. افزایش ضریب بهره تا میزان a=2، گرچه هیچ تأثیر کیفی جدی برروی تصویر ندارد ولی مقاومت سیگنال را به طور موثری در برابر حملات افزایش داده است[8]. الگوریتم پیشنهادی مقاله فوق در شکل های شماره ۶ و ۷ به نمایش گذاشته شده اند:



شکل ۶ : فرآیند درج سیگنال نهان نگار در تصویر



شکل ۷: فرآیند استخراج نهان نگاری از تصویر پوشانه

۳- گزینش روش مناسب

مطابق با مقایسه های انجام گرفته بین دو روش بیان شده و اطلاعات آماری بدست آمده از روش های فوق روش مبتنی بر روش موجک گسسته DWT در برابر حملات مقام تر و از نظر حفظ شفافیت تصویر بهتر عمل کرده است. این روش یکی از روشهای حوزه تبدیل می باشد که نسبت به حوزه مکان دارای مقاومت، امنیت و شفافیت بهتری است. در روشهای پنهان نگاری در حوزه تبدیل، ضرایب براساس قانون مشخصی تغییر می کنند. معمولا در حوزه تبدیل پنهان نگاری مقاومت بیشتری در برابر حملات از خود نشان می دهد. در روش ذکر شده خانم زهره زراعتی دیزچه و همکاران در صورتیکه هیچ گونه تغییری در تصویر گنجانه ایجاد نشود تصویر پنهان شده به صورت قابل ملاحظه و کامل قابل استخراج می باشد. همانطور که گفته شد در تبدیل موجک گسسته، سیگنال از یکسری فیلترهای بالاگذر برای آنالیز فرکانسهای بالا و از یکسری فیلترهای پایین گذر برای آنالیز فرکانسهای پایین، عبور داده می شود. بیشترین انرژی تصویر در زیر باندهایی با فرکانس پایین LL_x تمرکز دارد. در هربار تجزیه یک باند فرکانسی از سیگنال اصلی جدا شده و باقیمانده در سیگنال تقریب ذخیره می شود، بنابراین در حالت کلی می توان سیگنال اصلی را از حاصل جمع سیگنالهای بدست آمده محاسبه کرد. بنابراین درج گنجانه در زیرباندهایی با فرکانس پایین مقاومت را به طور چشم گیری افزایش می دهد ولی ممکن است کیفیت تصویر را از نظر شفافیت کم کند[6]. برای برطرف کردن کاهش شفافیت پس از تعبیه در این زیرباند تصویر گنجانه را در ضریبی کوچکتر از یک ضرب کرده و سپس در این زیرباند تعبیه می شود. برای بررسی میزان شفافیت گنجانه از معیار PSNR (نرخ حداکثر سیکنال به نویز) استفاده می گردد، که در آن Max_1 بیشترین مقدار روشنایی تصویر و MSE متوسط مربعات خطا می باشد. همچنین برای بررسی نرخ شباهت بین تصویر گنجانه اصلی و استخراج شده از معیار SR استفاده شده است، که در زیر فرمول های موارد ذکر شده بیان می شود[6]:

$$PSNR= 10\log_{10}\frac{Max_1^2}{MSE} \qquad (۲)$$

$$MSE= \frac{1}{min}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)] \qquad (۳)$$

که m و n ابعاد تصویر و I تصویر پوشانه و K تصویر گنجانه شده می باشد.

$$SR= \frac{S}{S+D} \qquad (۴)$$

که در آن S تعداد پیکسل های یکسان بین دو تصویر و D تعداد پیکسل های متفاوت بین دو تصویر را نشان می دهد.

۴- نتیجه‌گیری

پیشرفت در فناوریهای ارتباطی به خصوص در اینترنت و شبکه های اجتماعی باعث می شود که هر فرد اطلاعات خود را به اشتراک گذاشته و در پس این اشتراک گذاری نگران حفاظت حقوق معنوی خود می باشد[6] . بنابراین بحث حفاظت از اطلاعات و محرمانه ماندن آنها برای مولفان حائز اهمیت خواهد بود. از اینرو ارتباطات پنهان و محرمانه در طول تاریخ دارای اهمیت بسیار شده است[1]. در مقاله ارائه شده جهت حفظ شفافیت و مقاومت طبق روش انتخابی ذکر شده در قسمت سوم که همان روش بر پایه‌ی موجک گسسته DWT می باشد با انتخاب ضریب آلفای مناسب علاوه بر شفافیت، مقاومت بالایی هم حاصل خواهد شد که طبق نتایج بدست آمده از آزمایشات

مختلف و آلفاهای انتخابی مختلف به این نتیجه دست یافتند که اگر مقدار آلفای انتخابی برابر با 0.01 باشد به بهترین جواب مطلوب خواهیم رسید[6]، و همچنین با بررسی های مقادیر بدست آمده به این نتیجه نیز رسیده اند که هرچه مقدار SR در فرمول شماره ۴ به عدد یک نزدیکتر باشد عملکرد بهتری خواهیم داشت، و شفافیت و مقاومت تصویر بیشتر خواهد بود در صورتیکه با روش تبدیل گسسته کسینوسی ارائه شده در قسمت سوم فقط به مقاومت تصویر دست یافته ایم.

مراجع

[1] G. Sahoo and R.K. Tiwari " Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", IJCSNS International Journal of Computer Science and Network Security, VOL. 8 No. 1 January 2008.

[2] Kumar, Arvind, and Km Pooja. "Steganography-A Data Hiding Technique." International Journal of Computer Applications 2010.

[3] Fabien A.P. Petitcolas and Ross J. Anderson. "Evalution of copyright marking systems", In Proceeding of IEEE International Conference on Multimedia Computing and Systems '99, volume 1, pages 574-579, Florence, Italy, June 1999.

[4] Eric Cole & Ronald D. Krutz ,"Hiding in Plain Sight: Steganography and the Art of Covert Communication" , Wiley Publishing, Inc. 2003.

[۵] قنبری، ص؛ قنبری، ن؛ کشتگری، م: "پنهان شکنی در تصاویر با استفاده از ماتریس هم رخدادی و شبکه عصبی"، نشریه مهندسی برق و مهندسی کامپیوتر : شماره ۳، ۱-۶، ۱۳۹۰.

[۶] زراعتی، ز؛ مقدم چرکری، ن: "نهان نگاری مبتنی بر موجک با انتخاب بهینه زیرباند فرکانسی به منظور افزایش شفافیت و مقاومت"، همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات، ۱۳۹۳.

[۷] نقش نیل چی، ا.ح؛ نادعلی، ان، ا : "شیوه ای جدید در پنهان نگاری مقاوم داده در تصاویر JPEG"، نشریه مهندسی برق و مهندسی کامپیوتر: شماره ۱، ۱-۹، ۱۳۸۵.

[۸] احسان، ل؛ ادریسی، ف: "نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه تبدیل گسسته کسینوسی". انجمن گروه فنی دانشکده صدا و سیما و گروه مهندسی برق دانشگاه تربیت مدرس : ۱-۸، ۱۳۸۵.