Journal of Electronic & Cyber Defence
Vol 2, No. 3, 2014

Robust Steganography Algorithm Text in the Image Using A Spread Spectrum Method

M. Nejati Jahromi[1], H. Akbarian[2*]

1- PhD, Shahid Sattari University
2- Master Student, Shahid Sattari University

(Reccive: 2013/10/26, Accept: 2014/11/14)

Abstract

Due to the epidemic growing of telecommunication systems and new services, the demand for radio frequency spectrum has greatly increased to the extent that the radio frequency spectrum has been a vital source of value to radio communications.

Therefore, managing the efficient use of the frequency spectrum of the different technologies and different services is very difficult. In the past, this was done by assigning a frequency spectrum for each service, But another way to solve this problem is based on the characteristics of a modulation that shares the frequency band without significant interference. This method is called spread spectrum modulation.

Spread spectrum steganography method uses a spread spectrum communication concept in which a narrow-band signal is transferred into a pseudo-noise signal. This method shows a very high ability to withstand adverse interactions.

It also has security advantages of the encryption based on the keys used in the production of different strings pseudo-random orthogonal - such as Gold strings.

To spread the message signal spectrum, the Hadamard matrix is used with appropriate statistical properties of low cross-correlation.

In this paper we have studied Steganography by Hadamard matrix and it is compared with a simple method.

Keywords:

Spread Spectrum Communication, Steganography, Embedding Data, Image Processing

* **Corresponding Author Email:** akbarian.hassan@gmail.com

مجله علمی- پژوهشی «پدافند الکترونیکی و سایبری»
سال دوم، شماره ۳، پاییز ۱۳۹۳؛ ص ۸۳-۷۷

الگوریتم نهان‌نگاری مقاوم پیام متنی در تصویر با استفاده از روش طیف گسترده

منصور نجاتی جهرمی[۱]، حسن اکبریان[۲*]

۱- استادیار، دانشکده تحصیلات تکمیلی، دانشگاه علوم و فنون هوایی شهید ستاری
۲- دانشجوی کارشناسی ارشد مخابرات، دانشکده تحصیلات تکمیلی، دانشگاه علوم و فنون هوایی شهید ستاری
(دریافت: ۹۲/۰۸/۱۹، پذیرش: ۹۳/۰۸/۲۳)

چکیده

امروزه با توجه به رشد روزافزون سیستم‌های مخابراتی و فراگیر شدن سرویس‌های جدید، تقاضا برای طیف فرکانس رادیو به‌شدت افزایش یافته تا جایی که طیف فرکانس رادیویی به‌عنوان یک منبع حیاتی باارزش برای مخابرات رادیویی مطرح می‌شود.

بنابراین مدیریت استفاده بهینه از طیف فرکانسی به‌علت حضور تکنولوژی مختلف و سرویس‌های متفاوت بسیار دشوار است. در گذشته این عمل با اختصاص‌دادن طیف فرکانسی به هر سرویس انجام می گرفت، اما روش دیگری برای حل این مشکل مطرح شده است که متکی به ویژگی‌های یک نوع مدولاسیون است که باند فرکانسی را بدون تداخل قابل ملاحظه ای به اشتراک می‌گذارد. این روش مدولاسیون طیف گسترده نامیده می‌شود. نهان‌نگاری به روش طیف گسترده از یک مفهوم مخابرات طیف گسترده استفاده می‌کند که در آن یک سیگنال باند باریک در داخل یک سیگنال شبه نویز منتقل می‌شود. توانایی این روش در تحمل تداخلات ناخواسته بسیار بالاست. این روش هم‌چنین دارای مزایای امنیت حاصل از رمزنگاری است که بر مبنای کلیدهای استفاده شده در تولید رشته‌های شبه تصادفی متعامد مانند رشته‌های گلد حاصل می‌شود. برای گسترش طیف سیگنال پیام، از ماتریس هادامارد، که دارای خواص آماری مناسبی از نظر همبستگی متقابل پایین هستند، استفاده شده است. در این مقاله به بررسی نهان‌نگاری توسط ماتریس هادامارد برای گسترش پیام پرداخته شده و با روش ساده مقایسه می‌گردد.

واژه‌های کلیدی: مخابرات طیف گسترده، پنهان‌نگاری، جاسازی اطلاعات، پردازش تصویر

۱. مقدمه

ایده‌های اولیه تکنیک طیف گسترده مربوط می‌شود به فعالیت‌های دو مهندس آلمانی از شرکت *Telefunken*[1] در سال ۱۹۳۵ که اقدام به ارسال سیگنال صحبت آغشته به نویزی که توسط یک مولد چرخشی ایجاد شده بود، کردند و در گیرنده با استفاده از مولد چرخشی دیگری که با فرستنده هماهنگ بود موفق به بازسازی صحبت شدند. در اوت ۱۹۴۲ با ثبت روشی به نام مخابرات سری که در آن فرکانس حامل بین فرستده و گیرنده بر طبق الگویی تصادفی تغییر می‌کرد، گامی دیگر در جهت این تکنیک برداشته شد[۱].

در دهه ۵۰ نیز با پیشرفت تکنولوژی الکترونیک، گروه سیستم‌های الکترونیکی سیلوانیا[2] نیز آزمایشاتی پیرامون روش مخابرات سری انجام دادند که از نتایج آن در بحران موشکی کوبا در ۱۹۶۲ استفاده شد. در اوایل دهه ۶۰ نام طیف گسترده وارد ادبیات سیستم‌های مخابراتی گردید. اما محدود به تحقیقات محرمانه نظامی می‌شد. مهم‌ترین این تحقیقات در دانشگاه *MIT* تحت عنوان پروژه[3] (*NOMAC*) به انجام رسید[۲].

سرانجام در اوسط دهه ۸۰، ارتش آمریکا این تکنولوژی را غیرنظامی اعلام کرد که به موجب آن استفاده از طیف گسترده در کاربردهای تجاری مورد بررسی قرار گرفت. در مدتی کمتر از ۲۰ سال رشد این تکنولوژی به حدی بود که استفاده از آن در نسل سوم مخابرات سیار سلولی مورد توافق همگان قرار گرفت[۲۰]. در این مقاله پس از بیان مزایای بهره برداری از طیف گسترده، به معرفی ساختار تبدیل نوین کانتورلت پرداخته شده است. در ادامه الگوریتم پیشنهادی به همراه معرفی عناصر تشکیل‌دهنده آن و نحوه به‌کارگیری طیف گسترده در آن و هم‌چنین فرایند جاسازی و استخراج پیام سرّی در تصویر اصلی شرح داده شده است. در بخشی دیگر چگونگی ارزیابی و سنجش کاربرد این الگوریتم بر روی تصاویر مختلف بیان گردیده است. در پایان نیز با استناد به نتایج به‌دست‌آمده، به مقایسه این روش با روش‌های قبلی دیگر از جمله تبدیل ویولت و تبدیل کسینوس گسسته و... پرداخته شد.

۲. مزایای طیف گسترده

آنچه که موجب رشد روزافزون طیف گسترده شده است تنها به قابلیت طیف گسترده در استفاده اشتراکی از پهنای باند یا خاصیت ضد تداخلی آن برنمی‌گردد، بلکه مزایای دیگر طیف گسترده که استفاده از آنها کیفیت بهتری را در کانال‌های ارتباطی جدید به دست

* رایانامه نویسنده مسئول: akbarian.hassan@gmail.com

1. George Antheil , Hedy Lamarr
2. Sylvania Electronic system Division
3. Noise Modoulation and Correlation

می‌دهد نیز در گسترش کاربرد آن تاثیر زیادی داشته است. اکثر روش‌های مدولاسیون برای انتقال اطلاعات در کانال‌هایی با نویز سفید گوسی جمع شونده[1] بهینه هستند. اما کاربردهای جدید کانال‌هایی را معرفی نموده‌اند که با این مدل قابل بیان نیستند. به‌عنوان مثال در کانال‌های چند مسیره که چندین مسیر انتقال بین فرستنده و گیرنده وجود دارد نظیر آنچه که در مخابرات سیار سلولی اتفاق می‌افتد، سیگنال اصلی با نمونه‌هایی از خود که با تأخیر متفاوت به گیرنده می‌رسند تداخل نموده و موجب ایجاد پراکندگی[2] و یا رنگ‌باختگی[3] می‌گردد. طیف گسترده در این موارد نیز موفق عمل کرده و کیفیت بهتری را در مقایسه با سایر روش‌ها ارائه می‌نماید[۳].

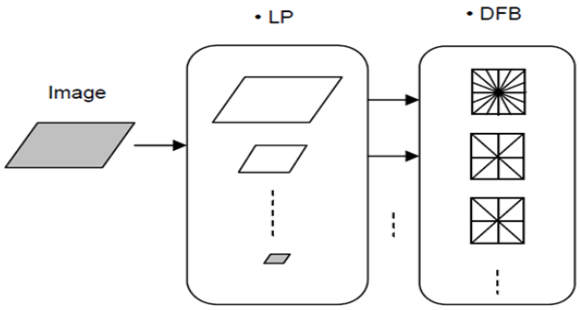
۳. تبدیل کانتورلت

به‌طور کلی عملیات نهان‌نگاری شامل دو مرحله می‌باشد. در مرحله اول اطلاعات مورد نظر جهت نهان‌نگاری بر روی رسانه گنجانده می‌شود و سپس در مرحله دوم این اطلاعات از رسانه نهان‌نگاری شده بازیابی می‌گردد. در حوزه تبدیل (فرکانس)، روش‌های مختلفی وجود دارد. یکی از این روش‌ها، تبدیل کانتورلت است[۷]. تبدیل کانتورلت یکی از چندین تبدیل پیشرفته در سال‌های اخیر است که با بهبود نمایش تنکی تصویر در سرتاسر تبدیل ویولت به‌دست می‌آید. تبدیل کانتورلت با کمک فیلتر بانک‌ها از یک حوزه گسسته شروع شده و سپس از طریق یک چارچوب تحلیلی مالتی رزولوشن به یک حوزه پیوسته همگرا می‌شود. تبدیل موجک مانند هرم لاپلاسین (LP) که یک تبدیل چند مقیاسه است و برای تسخیر نقاط ناپیوسته تصویر یعنی همان لبه‌های تصویر به‌کار می‌رود را با یک فیلتر بانک جهت‌دار که برای ارتباط نقاط ناپیوستگی به یک ساختار خطی به کار می‌رود ترکیب می‌کنیم. به چنین ترکیبی «فیلتر بانک جهتدار هرمی» (PDFB) و به بسط حاصل از آن تبدیل کانتورلت می‌گویند[۱۷ و ۱۸].

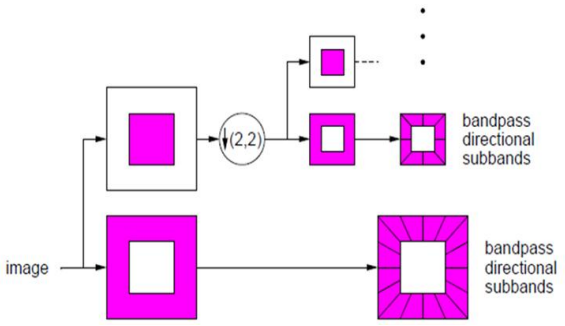
تبدیل کانتورلت یک نمایش چندمقیاسه و چند جهتی از یک تصویر را نمایش می‌دهد. این تبدیل شامل یک ساختار فیلتربانک دوبل برای به‌دست آوردن بسط پراکنده جهت تصاویر دارای خطوط تراز هموار می‌باشد.

در فیلتربانک دوبل، هرم لاپلاسی (LP) ابتدا جهت نقاط نامنظم استفاده می‌شود و سپس توسط یک فیلتربانک جهتی (DFB) جهت اتصال نقاط نامنظم و ناپیوسته در میان ساختارهای خطی دنبال می‌شود. تعداد جهت‌های مورد نیاز می‌تواند توسط کاربر مشخص گردد. از آنجایی که کانتورلت‌ها لبه‌های بیشتری را تخصیص می‌دهند، جهت کاربرد مخفی‌سازی اطلاعات مناسب‌تر می‌باشند، به‌طوری که اطلاعات بیشتری می‌تواند در نواحی فرکانس بالا بدون خرابی قابل درک تصویر اصلی مخفی گردد. همان‌طور که پیشتر گفته شد، این تبدیل از ترکیب هرم لاپلاس و بانک فیلتر جهت‌دار تشکیل شده است.

در حوزه فرکانس هرم لاپلاس تصویر دوبعدی را به دو زیرباند بالاگذر و پایین‌گذر تجزیه کرده و DFB که در باند بالاگذر به کار می‌رود در حقیقت زیرباندهای بالاگذر را به زیرباندهای جهت‌دار تقسیم می‌کند. شکل ۲ این ترکیب را نشان می‌دهد [۱۶].



شکل ۱. فلوگراف تبدیل کانتورلت. تصویر ابتدا توسط هرم لاپلاسین به زیرباندهایی تقسیم شده و سپس هر جزء تصویر توسط فیلتربانک جهتی، تجزیه می‌شود.



شکل ۲. تجزیه کانتورلت - هرم لاپلاسی توسط فیلتربانک جهتی دنبال می‌شود.

۴. طراحی الگوریتم نهان‌نگاری

الگوریتم پیشنهادی برای نهان‌نگاری دیجیتال تصویر ثابت به روش طیف گسترده در حوزه‌ی تبدیل کانتورلت، در شکل‌های ۳ نشان داده شده‌اند.

به‌عنوان سیگنال پیام از جمله " this is a watermark " استفاده شده است که در ۳ تصویر آزمایش استاندارد خاکستری ۵۱۲×۵۱۲ پیکسل به‌نام‌های بابون (تصاویر فرکانس بالا)، فلفل‌ها (تصاویر با نواحی یکنواخت و در عین حال دارای لبه‌های برجسته) و لنا (تصویر هموار)، با فرمت png که قبلاً هیچ‌گونه عمل فشرده‌سازی، بر روی آن‌ها صورت نگرفته است، درج می‌شود.

برای درج نهان‌نگاره، ابتدا سیگنال پیام به یک سیگنال ۲ قطبی تبدیل شده و سپس برای گسترش طیف سیگنال پیام، از ماتریس هادامارد، که دارای خواص آماری مناسبی از نظر همبستگی متقابل پایین هستند، استفاده شده است و سیگنال ۱۵۲ بیتی پیام

1. AWGN (Additive White Gaussian Noise)
2. Dispersion
3. Fading

{۱۵۲= (حرف) ۱۹ × ۸} با استفاده از ماتریس هادامارد از مرتبه ۱۰۲۴ به یک رشته ۱۰۲۴ بیتی، گسترده شده است. بنابراین در هر یک از نقاط ناهموار یکی از عناصر سگنال گسترش یافته جای می‌گیرد.

۴. ۱. ایجاد رشته تصادفی

الگوهای $Pi, i=1,2,3,\ldots,R$ که در نهان‌نگاری به روش طیف گسترده استفاده می‌شوند چنانچه دارای خصوصیاتی باشند فرایند تشخیص بهبود می‌یابد و خطای کمتری در هنگام بازیابی خواهیم داشت. می‌توان شرایط زیر را برای آن‌ها در نظر گرفت [۱]:

۱) $Pi, i=1,2,3,\ldots,R$ می‌بایست با میانگین صفر باشد.

۲) همبستگی فاصله‌ای[1] $\langle P_i, P_j \rangle$, $i\neq j$ بایستی حداقل باشد. به صورت ایده‌آل رشته‌های P_i و P_j بایست وقتی $i\neq j$ است، متعامد باشند.

روشی که ما در این پایان‌نامه برای ایجاد رشته‌های تصادفی[2] از آن استفاده کرده‌ایم استفاده از ماتریس هادامارد است که شرایط فوق را دارا می‌باشد. نکته اصلی که باید در این انتقال به آن توجه کرد این است که ابعاد ماتریس هادامارد توانی از دو می‌باشد. لذا در آزمایشات مربوط به ارزیابی روش، طول بردار طیف گسترده همواره توانی از دو می‌باشد.

۴. ۱. ۱. ضرب سیگنال پیام در ماتریس هادامارد

یک ماتریس هادامارد از مرتبه ۱۰۲۴ انتخاب کرده و برای برقراری شرایط بند ۲-۱-۱ ماتریس P را به‌صورت زیر در نظر می‌گیریم:

$$P=\text{Hadamard}\ (2:1+152\ ,1:1024) \qquad (۱)$$

P ماتریس از مرتبه ۱۰۲۴×۱۵۲ (از سطر ۲ تا سطر ۱۵۳ ماتریس هادامارد) می‌باشد.

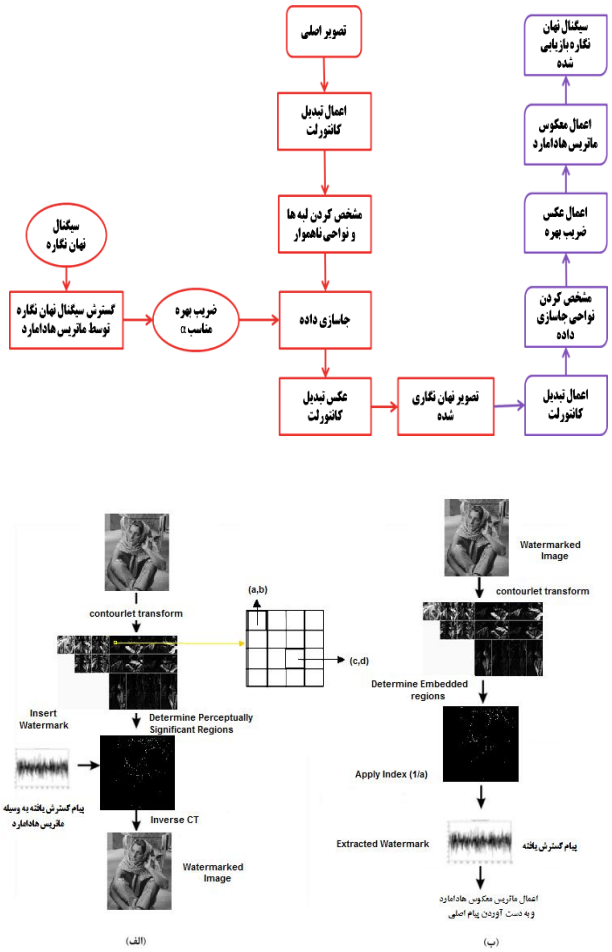
گسترش طیف را به‌صورت زیر انجام می‌دهیم:

$$W_{(1\times1024)} = [\ \text{پیام سیگنال}\ ]_{(1\times152)} \times [P]_{(152\times1024)} \qquad (۲)$$

۴. ۱. ۲. تعیین ضریب بهره α

α پارامتری است که در هنگام گنجاندن هرچه مقدارآن کمتر باشد، PSNR یعنی شباهت بین تصویر نهان‌نگاری شده و تصویر اصلی افزایش می‌یابد اما در عوض مقاومت تصویر نهان‌نگاری شده در مقابل اعمال خرابکاری کمتر خواهد شد. بنابراین در هنگام گنجاندن نهان‌نگاره می‌بایست سعی کرد تا بهترین مقدار برای آن در نظر گرفته شود که هم شفافیت تصویر نهان‌نگاری حفظ شود و هم مقاومت الگوریتم ارائه شده در حد مطلوبی باقی بماند.

1. Spatial Correlations
2. Pseudorandom Sequences



شکل ۳. بلوک دیاگرام و نمایه تصویری روند نمای درج و استخراج نهان‌نگاره

شکل ۳ یک تصویر را نشان می‌دهد که به یک سطح هرمی و زیرباندهای ۱۶ جهتی تجزیه شده است (ضرایب بالا سفید رنگ هستند). به‌دلیل مسئله اختلاط زیرباندها در تبدیل ویولت، دستکاری یک ضریب در زیرباند قطری، مقدار ضرایب وابسته در جهت‌های دیگر را تغییر می‌دهد. تأثیرپذیری تبدیل کانتورلت در تجزیه تصویر برای جهت‌ها به‌طور جداگانه استفاده می‌گردد. از این رو دستکاری مقدار یک ضریب در زیرباندهای کانتورلت نسبت به تغییر یک ضریب در زیرباندهای ویولت، بر کیفیت تصویر تأثیر کمتری دارد. علاوه‌بر این اکثر الگوریتم‌های پنهان‌شکنی[3] رایج به حوزه فضایی (مکانی)، ویولت و تبدیل *DCT* محدود می‌شود. از این‌رو تشخیص تصاویر پوششی از تصاویر نهان‌سازی (ساخته شده به‌وسیله جاسازی داده در ضرایب کانتورلت آنها) به‌وسیله این الگوریتم‌های پنهان‌شکنی ساده نیست.

۵. فرایند جاسازی

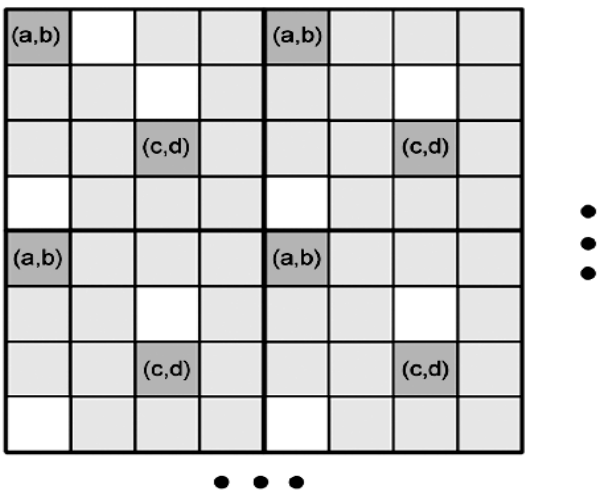
فرایند جاسازی پس از گسترش پیام سرّی با استفاده از ماریس هادامارد، طبق مراحل زیر انجام می‌شود:

3. Steganalysis

مرحله اول: تصویر اصلی توسط یک سطح هرمی و ۱۶ تبدیل کانتورلت جهتی تجزیه می‌شود.

مرحله دوم: نواحی از زیرباندها که اطلاعات می‌تواند جاسازی شود، مشخص می‌شوند. سپس ضرایب کانتورلت بالاتر در این نواحی را که برای جاسازی استفاده می‌شود، تعیین می‌گردد.

مرحله سوم: در این مرحله مکان دو ضریب در هر بلوک برای جاسازی انتخاب می‌گردد. دو ضریبی برای جاسازی مناسب هستند که هر دوی آنها به مجموعه ضرایب بالاتر متعلق باشند. هر بیت از پیام سرّی توسط مقایسه و اینکه آیا مقادیر دو ضریب کانتورلت در ناحیه ناهموار نیازمند تعویض می‌باشد و یا خیر، پنهان می‌گردند. اگر ضریب *(a,b)* بزرگ‌تر یا مساوی ضریب *(c,d)* باشد، بلوک ۴×۴ بیت یک را کد می‌کند و در غیر این‌صورت بیت صفر را کد می‌نماید. اگر مقادیر دو ضریب مطابق با بیت کدشده نباشند، جایگزین خواهند شد. دستکاری مقدار ضرایب ممکن است منجر به از دست دادن اطلاعات جاسازی شده در تبدیل کانتورلت معکوس شود. به‌علاوه، ممکن است بر روی مقدار ضرایب همجوار تأثیر گذاشته و در نتیجه موجب از دست رفتن اطلاعات جاسازی شده در این همسایگی گردد. برای به‌دست آوردن سطح بالایی از تشابه بین تصاویر نهان‌نگاری شده و تصاویر اصلی، و هم‌چنین داشتن کمترین تلفات در اطلاعات استخراج شده، هر ضریب انتخاب شده برای جاسازی باید از ضرایب دیگر انتخاب شده فاصله داشته باشند. با توجه به این ویژگی، ما هر بیت را در ضریبی از بلوکی به اندازه ۴×۴ جاسازی می‌کنیم. در این مدل، ضریب انتخاب شده کمترین نزدیکی را به دیگر ضرایب انتخاب شده دارا می‌باشد. شکل ۴ بخشی از یک زیرباند کانتورلت را نشان می‌دهد که دارای تعدادی بلوک ۴×۴ می‌باشد. همان‌طور که در شکل مشخص است، ضرایب انتخاب شده برای جاسازی بطور قابل ملاحظه‌ای از دیگر ضرایب در نظر گرفته شده دور می‌باشند.



شکل ۴. یک بخش از زیرباند کانتورلت با تعدادی بلوک ۴×۴. ضرایب منتخب (نشان داده شده در خاکستری تیره) برای جاسازی حداقل یک پیکسل از دیگر ضرایب دور می‌باشد.

۶. فرایند استخراج

مرحله اول: تجزیه تصویر نهان‌نگاری شده به‌وسیله تبدیل کانتورلت.

مرحله دوم: شناسایی ضرایب بالای کانتورلت که پیام سرّی گسترش یافته در آنها جایگزین شده است.

مرحله سوم: تشکیل فرایند معکوس جاسازی و اعمال ضریب $\frac{1}{\propto}$ با استفاده از همان ضریبی که استفاده شده است.

مرحله چهارم: بازیابی اطلاعات جاسازی شده با مقایسه ضرایب *(a,b)* و *(c,d)* در هر بلوک ۴×۴. اگر ضریب *(a,b)* بزرگ‌تر یا مساوی ضریب *(c,d)* بود، بیت پنهان شده ۱ است و در غیر این صورت صفر می‌باشد. در پایان این مرحله پیام گسترش یافته به وسیله ماتریس هادامارد بازیابی می‌شود که با اعمال معکوس ماتریس هادامارد پیام سرّی اصلی به دست می‌آید.

۷. معیارهای سنجش

نحوه آشکارسازی سیگنال نهان‌نگاره در شکل ۳ نشان داده شده است. چون احتمال دارد که سیگنال پیام استخراج شده W^*، با سیگنال نهان‌نگاره اولیه W، برابر نباشد. میزان مشابهت W و W^* را می‌توان با رابطه زیر اندازه گرفت:

$$Sim(W, W^*) = \frac{W.W^*}{\sqrt{W^*W^*}} \quad (۳)$$

الف) اندازه‌گیری خطا

جهت اندازه‌گیری خطا بین نهان‌نگاره‌ی اصلی و نهان‌نگاره‌ی بازیابی شده از NC که به صورت زیر تعریف می‌شود استفاده می‌کنیم.

اگر نهان‌نگاره اصلی را M و نهان نگاره بازیابی شده را 'M در نظر بگیریم و تعداد سطر و ستون‌های نهان‌نگاره را M_{length} و M_{Width} فرض کنیم آنگاه NC از رابطه زیر محاسبه می‌شود:

$$NC = \frac{\sum_{i=1}^{M_{length}} \sum_{j=1}^{M_{width}} [M(i.j)M'(i,j)]}{\sum_{i=1}^{M_{length}} \sum_{j=1}^{M_{width}} [M(i.j)]^2} \quad (۵)$$

NC، بیانگر میزان تطابق نهان‌نگاره بازیابی شده با نهان‌نگاره اصلی است.

ب) معیار شفافیت

جهت مشخص نمودن شباهت بین تصویر اصلی و تصویر نهان‌نگاری شده نیز از PSNR[1] استفاده می‌کنیم. اگر تصویر اصلی را

1. Power Signal to Noise Ratio

H و تصویر نهان‌نگاری شده را 'H در نظر بگیریم و تعداد سطرها و ستون‌های تصاویر H_{length} و H_{width} باشند، PSNR با استفاده از MSE[1] به‌صورت زیر تعریف می‌شود:

$$MSE = \frac{\sum_{i=1}^{H_{length}} \sum_{j=1}^{H_{width}} [H(i.j)H'(i,j)]^2}{H_{length}.H_{width}} \quad (۶)$$

$$PSNR = 10 \log \left[\frac{255^2}{MSE} \right] \quad (۷)$$

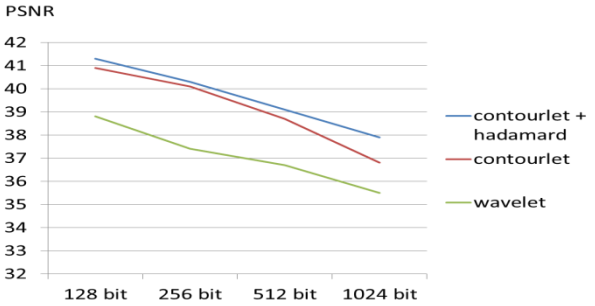
PSNR، بیانگر میزان شباهت تصویر نهان‌نگاره‌ی شده با تصویر اصلی است.

در شکل ۴ تصاویر اصلی و نهان‌نگاری شده نشان داده شده است. میزان PSNR مربوط به تصاویر مختلف در مقابل شکل‌ها نشان داده شده است.

شکل ۴. مقایسه بین تصاویر اصلی و تصاویر نهان‌نگاری شده

۸. نتایج آزمایش‌ها

در شکل ۵ مقایسه بین تغییرات *PSNR* روش‌های تبدیل کانتورلت (با استفاده از ماتریس هادامارد و بدون استفاده از ماتریس هادامارد) و تبدیل موجک با ظرفیتهای مختلف پیام سری نشان داده شده است. نتایج شبیه‌سازی‌ها نشان‌دهنده شفافیت بیشتر تبدیل کانتورلت با استفاده از ماتریس هادامارد نسبه به تبدیل کانتورلت ساده و تبدیل ویولت می‌باشد.



شکل ۵. میزان تغییرات PSNR مربوط به تصویر نهان‌نگاری شده لنا در روش‌های تبدیل ویولت، تبدیل کانتورلت با استفاده از ماتریس هادامارد و تبدیل کانتورلت ساده

نتایج حاصل از نهان‌نگاری با ظرفیت‌های مختلف پیام سری و افزایش ضریب بهره از ۰٫۰۱ به ۰٫۰۵، در جدول ۱ نشان داده شده است همان‌طور که مشاهده می‌شود، شفافیت مدل استفاده‌کننده از ماتریس هادامارد نسبت به مدل کانتورلت ساده از شفافیت بهتری برخوردار می‌باشد. هم‌چنین مقاومت حاصل از تکنیک ماتریس هادامارد نسبت به مدل ساده کانتورلت خیلی بهتر شده است. با افزایش ضریب بهره و هم‌چنین ظرفیت پیام سری، به مقاومت نهان‌نگاری افزوده می‌شود و از شفافیت آن کاسته می‌شود. در جدول ۲ لیست حملاتی که جهت سنجش مقاومت الگوریتم پیشنهادی به تصویر نهان‌نگاری شده با جاسازی پیام ۱۵۲ بیتی اعمال می‌گردد، آورده شده است. همه حملات برای α= ۰٫۰۱ آزمایش شده است.

جدول ۱. محاسبه نتایج نهان‌نگاری حاصل ازمدل کانتورلت با استفاده از ماتریس هادامارد و مدل کانتورلت ساده

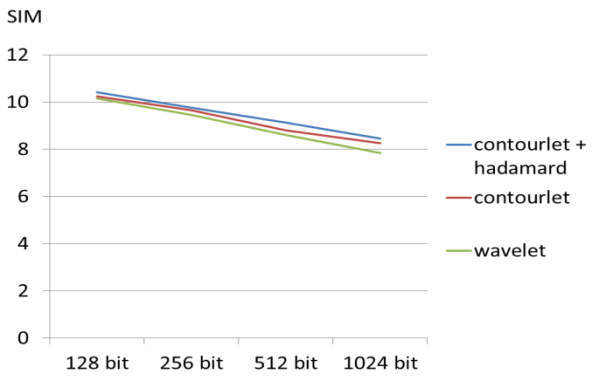
نوع تصویر		PSNR	SNR	SIM	NC
Barbara	Contourlet	34.5167	20.7750	9.9513	1
	Contourlet+hadamard	34.9486	21.5413	10.2834	1
peppers	Contourlet	36.3813	20.5580	10.2471	1
	Contourlet+hadamard	36.7351	21.4243	10.4218	1
Lena	Contourlet	36.0594	19.5282	10.8467	1
	Contourlet+hadamard	35.8017	20.3945	11.0105	1
Baboon	Contourlet	33.6427	19.3562	9.9778	1
	Contourlet+hadamard	33.3325	20.2225	10.0951	1

1. Mean Squared Error

جدول ۲. حملات مختلف آزمایش شده بر روی تصویر نهان‌نگاری شده

نوع خرابکاری	لنا مدل کانتورلت با استفاده از ماتریس هادامارد PSNR NC	لنا مدل کانتورلت ساده PSNR NC	فلفل‌ها مدل کانتورلت با استفاده از ماتریس هادامارد PSNR NC	فلفل‌ها مدل کانتورلت ساده PSNR NC	بابون مدل کانتورلت با استفاده از ماتریس هادامارد PSNR NC	بابون مدل کانتورلت ساده PSNR NC
بدون خرابکاری	۱ ۴۱٫۱۸۱۳ This is a watermark	۱ ۴۱٫۰۲۳۰ This is a watermark	۱ ۴۱٫۳۱۰۲ This is a watermark	۱ ۴۱٫۰۰۱۲ This is a watermark	۱ ۴۰٫۹۹۰۵ This is a watermark	۱ ۴۰٫۷۶۱۶ This is a watermark
افزودن نویز گوسی(m=0 , v=0.005) و عبور از فیلتر وینر	۱ ۳۲٫۹۳۲۰ This is a watermark	۱ ۳۱٫۱۵۸۳۱ This is a watermark	۱ ۳۶٫۱۳۲۵ This is a watermark	۱ ۳۵٫۸۳۲۷ This is a watermark	۱ ۳۲٫۹۳۲۰ This is a watermark	۱ ۳۱٫۱۵۲۴ This is a watermark
افزودن نویز فلفل نمکی (D=2%) و عبور از فیلتر میانه	۱ ۳۲٫۸۲۱۴ This is a watermark	۱ ۳۲٫۳۹۱۷ This is a watermark	۱ ۳۶٫۸۹۷۸ This is a watermark	۱ ۳۶٫۵۱۲۰ This is a watermark	۱ ۳۱٫۰۶۹۹ This is a watermark	۱ ۳۰٫۶۸۵۶ This is a watermark
فشرده‌سازی JEPG با Q=۵۰%	۱ ۳۶٫۶۹۳۲ This is a watermark	۰٫۹۸۹۶ ۳۵٫۸۳۰۱ This is a watermark	۱ ۳۴٫۶۱۴۶ This is a watermark	۱ ۳۴٫۴۲۷۳ This is a watermark	۱ ۳۱٫۶۲۲۶ This is a watermark	۰٫۹۶۹۷ ۳۱٫۵۷۲۸ This is a watermark
بریدن ۱/۸ از تصویر نهان‌نگاری شده	۱ ۲۲٫۸۳۷۱ This is a watermark	۱ ۲۲٫۱۰۴۴ This is a watermark	۱ ۲۵٫۴۳۲۶ This is a watermark	۱ ۲۵٫۰۹۵۷ This is a watermark	۱ ۲۹٫۰۰۱۸ This is a watermark	۱ ۲۸٫۳۶۲۹ This is a watermark
تغییر مقیاس و اندازه‌ی تصویر از ۵۱۲×۵۱۲ به ۲۵۶×۲۵۶	۱ ۳۱٫۷۵۷۷ This is a watermark	۱ ۲۹٫۱۸۹۳ This is a watermark	۱ ۳۱٫۴۷۸۳ This is a watermark	۰٫۸۷۸۸ ۳۱٫۶۵۲۱ This is a watermark	۰٫۹۳۹۴ ۳۱٫۴۱۶۲ This is a watermark	۰٫۸۷۸۸ ۳۱٫۳۷۲۲ This is a watermark

همان‌طور که از نتایج شکل ۶ مشخص است، میزان شباهت پیام بازیابی شده نسبت به پیام اصلی در روش تبدیل کانتورلت به همراه گسترش پیام توسط ماتریس هادامارد نسبت به دو روش دیگر (کانتورلت و ویولت) بهتر بوده و هم‌چنین هرچه حجم پیام متنی کمتر باشد، این تغییرات کمتر بوده و وضوح پیام بازیابی شده بهتر است. این فرایند نشان‌دهنده مقاومت بالای روش پیشنهادی در برابر حملات عمدی و غیر عمدی می‌باشد.



شکل ۶. میزان تغییرات *SIM* مربوط به تصویر نهان‌نگاری شده فلفل‌ها در روش‌های تبدیل ویولت، تبدیل کانتورلت با استفاده از ماتریس هادامارد و تبدیل کانتورلت ساده

۹. نتیجه‌گیری

استفاده از مدل استفاده کننده از ماتریس هادامارد نسبت به مدل کانتورلت ساده دارای *PSNR* یا به‌عبارت دیگر دارای شفافیت بیشتری می‌باشد. با توجه به این که همیشه بین شفافیت تصویر نهان‌نگاری شده و مقاومت مصالحه‌ای وجود دارد اما با بررسی مقاومت روش ارائه شده در مقابل اعمال خرابکاری‌های مختلف مشاهده می‌شود که مدل استفاده کننده از ماتریس هادامارد دارای مقاومت بهتری در برابر اعمال نویزهای مختلف می‌باشد.

از این نتایج چنین برمی‌آید که درج هر بیت از سیگنال طیف گسترده‌ی نهان‌نگاره در ضریبی از تبدیل کانتورلت که از نظر *JPEG* ارزش بیشتری دارد، سبب مقاوم شدن بسیار زیاد سیگنال نهان‌شده در تصویر، در برابر فشرده‌سازی‌های *JPEG* می‌شود.

با توجه به مزایای تبدیل کانتورلت، در نواحی لبه‌ها نویز کمتری ایجاد کرده و شفافیت بیشتری نسبت به تبدیل موجک خواهد داشت. استفاده از تبدیل فوق سبب بهبود در شفافیت تصویر نهان‌نگاری شده می‌گردد.

به‌دلیل استفاده از طیف گسترده الگوریتم ارائه شده از امنیت خوبی برخوردار می‌باشد. هم‌چنین به‌دلیل استفاده از ماتریس هادامارد برای گسترش طیف پیام، فرایند تشخیص بهبود می‌یابد و خطای کمتری در هنگام بازیابی خواهیم داشت.

۷. مراجع

[1] Joseli Mayer, Anderson Vieria Silveria Silverio, Jose Carlos M. Bermudez, “On the Design of Pattern Sequences for Spread Spectrum Image Watermarking” International Telecommunications Symposium- ITS 2002.

[2] Gary C. Kessler, An Overview of Steganography for the Computer Forensics Examiner, Burlington, Vermont, June 2011.

[3] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview Of Image Steganography, Proceedings of the Fifth Annual Information Security South Africa Conference(ISSA2005), Sandton, South Africa, June/July 2005.

[4] A. Cheddad, J. Condell, “Digital Image Steganography: Survey and Analysis of Current Methods” Signal Processing, Vol.90, Issue3, pp.727-752, 2010.

[5] Mrs. Kavitha, K. Kadam, “Steganography Using Least Signicant Bit Algorithm” Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.

[6] Atallah M. Al-Shatnawi, “A New Method in Image Steganography with.

[7] Improved Image Quality” Applied Mathematical Sciences, Vol. 6, no. 79, pp. 3907 - 3915, 2012.

[8] E. Hussein, “ A Comparative Study of Digital Watermarking Techniques in Frequency Domain” International Journal of Computer Applications, Volume 52– No.20, pp.43-50, August 2012.

[9] G.L. Varco and W.Puech, “DCT-based data hiding for securing ROI of color image,” in proc. Of the IEEE International Conference on Image Processing(ICIP), Genova,Italy, vol.2,no.2,pp. 1086-1089, 2005.

[10] Avisha Khanna et al,"Lossless Compression based on Curvelet-IWT" Int.J.Computer Technology & Applications,Vol 3 (1), pp. 431-436, feb. 2012.

[11] E. Candes, L. Demanet, D. Donoho , L.Ying, "Fast Discrete Curvelet Transforms", Caltech, March 2006.

[12] P.Tao, S. Dexter, A. M. Eskicioglu, "Robust Digital Image Watermarking in Curvelet Domain", Dept. of Computer Science, Graduate Center & Brooklyn College, City University of NewYork, 2006.

[13] L. Ying, L. Demanet and Emmanuel Cand`es, " 3D Discrete Curvelet Transform", Applied and Computational Mathematics, MC 217-50, Caltech, Pasadena, 2007.

[14] A. Mertins, " Wavelet, Filter Banks, Time Frequency Transforms and Applications", translated by: Dr. M. H. Moradi, Amir Kabir University, 2006. (in Persian)

[15] V. Natarajan, “Blind Image Steganalysis Based on Contourlet Transform” International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[16] S. Masaebi, “A New Approach for Image Hiding Based on Contourlet Transform”, International Journal of Electrical and Computer Engineering (IJECE) Vol.2, No.5, pp. 699-708, October 2012.

[17] P-P. Niu, et al, “A novel color image watermarking scheme in nonsampled contourlet-domain” ELSEVIER Expert Systems with Applications38, pp.2081-2098, 2011.

[18] D. Liu, “An Adaptive Watermarking Scheme Based on Nonsubsampled Contourlet Transform for Color Image Authentication” IEEE computer society, 2008.

[19] T. Bhattacharya, N. Dey, “A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum” International Journal of Modern Engineering Research (IJMER), Vol.1, Issue1, pp.157-161, 2012.

[20] C. Xie, Y.Cheng, Y. Chen, “Spread-Spectrum Steganalysis and PN Sequence Estimation” IEEE 3rd International Congress on Image and Signal Processing (CISP 2010), pp. 4143-4147, 2010.