استگانوگرافی صوتی توانمند با استفاده از تکنولوژی طیف گسترده دنباله مستقیم

ساجد محیسن*[1]، دکتر علی برومندنیا[2].

۱- دانشجوی دانشگاه آزاد اسلامی واحد بوشهر ،واحد علوم و تحقیقات ، ایران،

sajednet@gmail.com

۲- استاد دانشگاه آزاد اسلامی واحد بوشهر ،واحد علوم و تحقیقات، ایران،

broumandnia@gmail.com

چکیده

استگانوگرافی، هنرپنهان کردن این واقعیت است که ارتباط ازطریق پنهان سازی اطلاعات دراطلاعات دیگر صورت می گیرد.بسیاری از فرمت های فایل حامل متفاوت را می توان مورد استفاده قرارداد ، ولیکن تصاویر دیجیتالی با توجه به فراوانی آنها دراینترنت ،به عنوان معروف ورایج ترین نمونه هستند. به منظور پنهان کردن اطلاعات محرمانه در صوت، حیطه متنوعی از تکنیک های استگانوگرافی وجود دارد که بعضی از آنها بسیار پیچیده تر از بقیه بوده و همه آنها ازنقاط ضعف وقوت مربوطه برخوردارند . برنامه های کاربردی متفاوت از مستلزمات تکنیک استگانوگرافی مختلفی برخوردار می باشد.برای مثال،ممکن است بعضی از برنامه های کاربردی مستلزم قابلیت عدم مشاهده مطلق اطلاعات محرمانه باشد،در حالی که دیگر برنامه ها نیاز به مخفی ماندن پیام های محرمانه بزرگ تر داشته باشند. این طرح سعی در ارائه بررسی اجمالی استگانوگرافی،کاربرد و تکنیک های آن دارد.این طرح به منظور ارائه یک رویکرد ایمن تر،پیام را از طریق کلید محرمانه رمزنگاری نموده و سپس آن را به دریافت کننده ارسال می کند.سپس دریافت کننده پیام را رمز گشایی نموده تا به پیام اصلی دست یابد.

کلمات کلیدی: استگانوگرافی ، طیف گسترده ، تکنیک

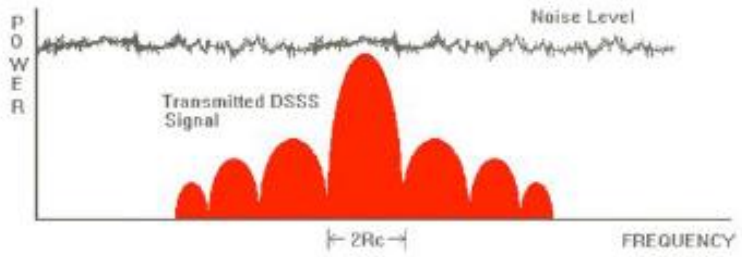
۱–مقدمه

استگانوگرافی برگرفته از لغت یونانی استگانوس به معنای پوشش یا محرمانگی بوده و گرافی (نوشتن یا رسم کردن) می باشد. استگانوگرافی در ساده ترین سطح آن به معنی نوشته پنهان بوده ،حال به صورت جوهر نامرئی بر روی کاغذ یا اطلاعات کپی رایت پنهان شده در یک فایل صوتی باشد.در حالی که رمز نگاری،پیام ها را به شکل کد یا رمز درهم سازی می کند،استگانوگرافی پیام را به طور کامل پنهان می سازد.این دو تکنولوژی ارتباط محرمانه را می توان به طور جداگانه یا باهم مورد استفاده قرارداد. برای مثال در ابتدا پیام را رمز نگاری نموده و سپس آن را در فایل دیگر برای انتقال آن پنهان سازی می کند.در راستای نگرانی جهان در زمینه استفاده از هر نوع ارتباط محرمانه و همچنین با توجه به قوانین اعمالی از

سـوی دولت ها به منظور محدود سـازی استفاده از رمزنگاری ها بنابراین نقش استگانوگرافی بسیار بارز و مهم می شود.آنچه که استگانوگرافی عملا انجام می دهد ،بهره وری از درک انسان می باشد،حس های انسانی به گونه ای آموزش ندیده اند که که در پی فایل هایی باشد که اطلاعات درون آنها پنهان شده است . هرچند یکسری برنامه هایی نیز وجود دارد که می تواند اسـتگانالیز(تشـخیص اسـتفاده از اسـتگانوگرافی) را انجام دهند.رایج ترین کاربرد اسـتگانوگرافی،پنهان سازی یک فایل درون دیگری اسـت. هنگامی که فایل یا اطلاعاتی درون یک فایل حامل پنهان می شود،داده معمولا ازطریق پسورد رمزنگاری می شود.[1]

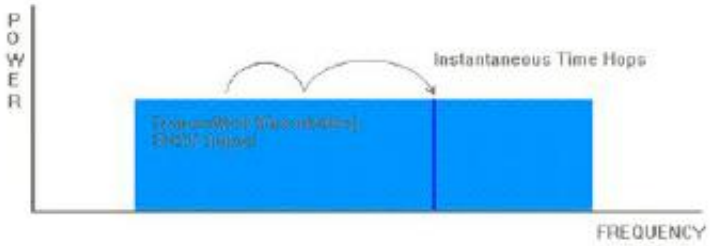
۲- معرفی طیف گسترده

تکنیک طیف گسترده ،از کاربرد گسترده ای در ارتباطات داده ای مانند ارتباطات سیار CDMA (دسترسی چندگانه با تقسیم کدی) برخوردار است .اولین حق امتیاز آن توسط "هدی لامار"و"جورج آنتیل" در سال ۱۹۴۱ و در قبال ارائه ارتباط محرمانه برای اهداف نظامی ثبت شـد[2].تکنیک های طیف گسـترده ،روش هایی هسـتند که انرژی تولیدی در پهنای باند خاص ازطریق آنها به طورعمدی در دامنه فرکانس گسترده شده وسیگنالی با پهنای باند گسترده تری را ایجاد می کند. مجموعه ای از این نوع تکنولوژی ها دراین شـاخه وجود دارد .DSSS طیف گسترده دنباله مستقیم : داده قابل انتقال به قطعات کوچکتر تقسـیم شـده و هر قطعه داده به یک کانال فرکانس در سـراسـر طیف اختصـاص می یابد. انتقال دهنده از یک تکنیک مدولاسیون با فاز متغیر به منظور مدوله سازی هر قطعه داده با توالی بیتی نرخ داده بالاتر بهره می برد[3](شکل۱)



شکل۱ : طیف گسترده دنباله مستقیم

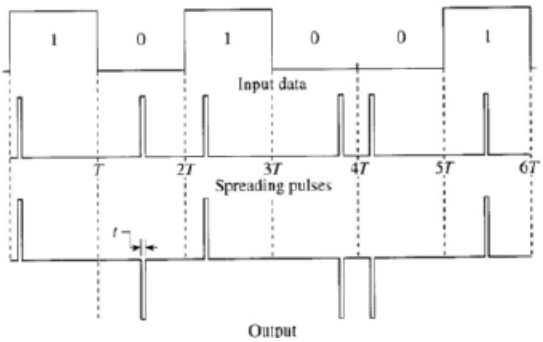
FHSS طیف گسـترده پرش فرکانسی . روشی برای انتقال سیگنال ها ازطریق سوئیچ سازی سریع یک حامل درمیان کانال های فرکانس بسـیار با اسـتفاده از یک توالی شـبه تصـادفی شـناخته شـده برای هر دوی دریافت کننده و انتقال دهنده می باشد[3](شکل۲)



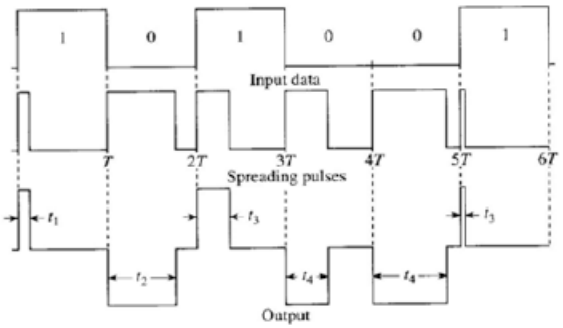
شکل۲: طیف گسترده پرش فرکانسی

طیف گسترده با پرش زمانی.چریپ(chirp) اطلاعات کوتاه با زمان پالس شبه تصادفی یا با موقعیت های تصادفی منتقل می شوند.عموما دو روش برای اجرای این مساله وجود دارد:روشیک : میانه چریپ ها ازطریق تولید کننده کد PN تعیین می شود (شـکل۳)[1].روش دو:چریپ ها به طور همزمان در هر زمان بیت وارد می شود،تولید کننده PN طول مدت خود را تغییر می دهـد(شـکـل۴)[1].دراینجـا ،یـک چریـپ سـیگنـالی اسـت کـه درآن فرکـانس به موازات زمان افزایش یا کاهش می

یابد.کاربردعمومی طیف گسترده با استفاده از چریپ ها،طیف گسترده چریپ(CSS) نامیده می شود . گاهی اوقات نیزمحقق این تکنولوژی ها را باهم تلفیق نموده تا تکنولوژی طیف گسترده الگودار مشخصی به دست آید.



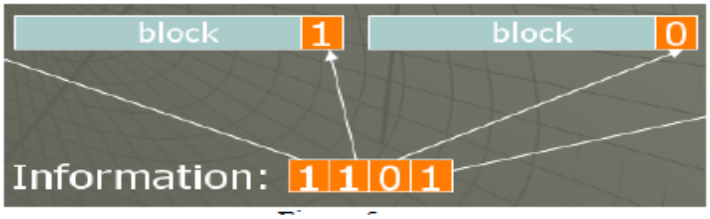
شکل ۳ : میانه چریپ ها



شکل ٤ : چریپ سیگنالی

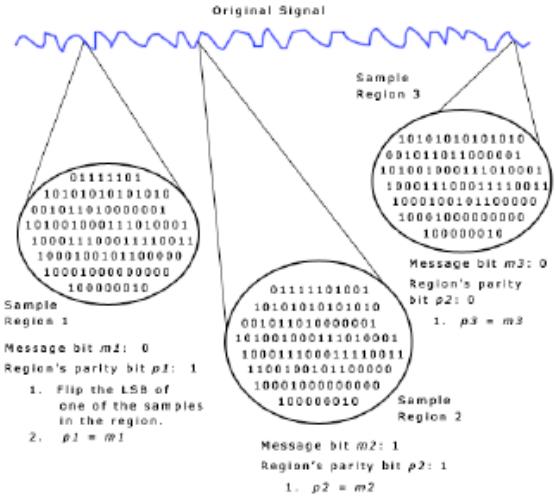
۳– تکنولوژی استگانوگرافی صوتی

استگانوگرافی صوتی،تکنولوژی تعبیه سازی اطلاعات در یک کانال صوتی است.این تکنولوژی برای حفظ یا حمایت کپی رایت دیجیتالی مورد استفاده قرار می گیرد. واترمارکینگ ،تکنیکی است که یک قطعه ازاطلاعات (پیام) را در قطعه دیگر اطلاعات (حامل) مخفی می سازد.این تکنیک کاربرد گسترده ای درتصویردوبعدی،کلیپ صوتی،کلیپ تصویری دارد.بیشتر تحقیق ها مبتنی بر واترمارکینگ تصویر دو بعدی هستند.پنج نوع استگانوگرافی صوتی وجوداردکد دهی(LSB کم ارزش ترین بیت)؛ساده ترین شیوه تعبیه اطلاعات درفایل های صوتی دیجیتالی می باشد. درواقع این نوع کددهی،کددهی بیت هایی با حداقل اهمیت به منظور حمل اطلاعات می باشد.این روش بسیارساده می باشد.بهرحال این تکنیک با توجه به عدم توانمندی از کاربرد کمتری در صنعت واقعی برخورداراست[5](شکل۵).



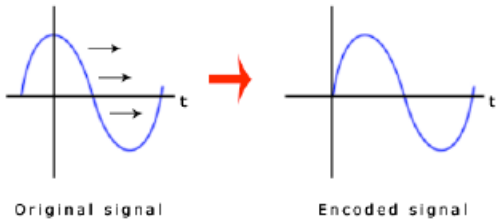
شکل۵ : کم ارزش ترین بیت

کددهی پریتی :دراین روش ،یک سیگنال به قسمت های مجزای نمونه تقسیم شده و هربیت برای پیام محرمانه در بیت پریتی یک قسمت از نمونه رمزنگاری می شود.بهرحال،مهاجمان هنوز هم می توانند الگوی شکستن یا حذف اطلاعات ازرسانه حامل را بیابند.[5](شکل۶)



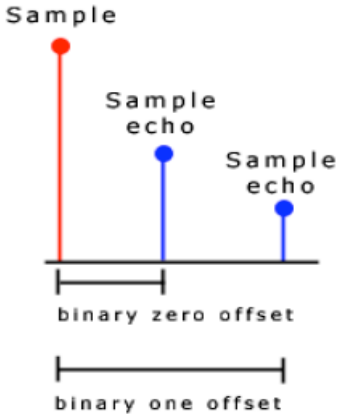
شکل٦ : کددهی پریتی

کددهی فازی:این نوع کدگذاری برای مطرح کردن معایب نویز ناشی از استگانوگرافی صوتی مورد استفاده قرار می گیرد.کددهی فازی مبتنی براین واقعیت است که کمپوننت های فازی صدا همانند نویزبرای گوش انسان قابل درک نیست.عیب این روش هم نرخ پایین انتقال داده می باشد[6].(شکل۷)



شکل۷ : کددهی فازی

پنهان کردن اطلاعات دراکو: اطلاعات ازطریق معرفی یک اکو درسیگنال گسسته درفایل صوتی تعبیه می شود.بدین ترتیب نرخ انتقال داده بالا رفته و درمقایسه با روش های القای نویز از توانمندی بالاتری برخوردارند(شکل۸)

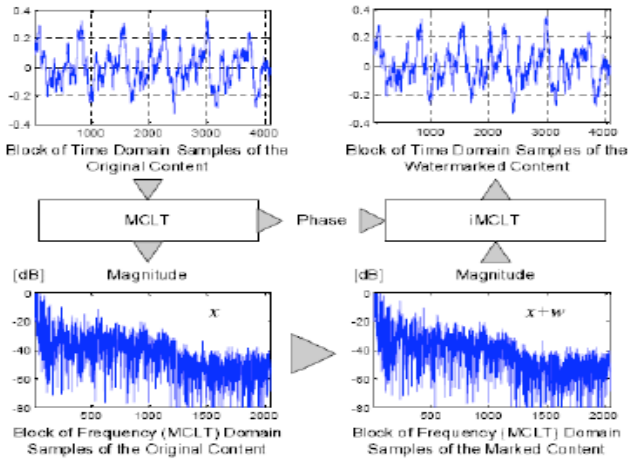


شکل۸ : پنهان کردن اطلاعات دراکو

طیف گسترده:یکی از توانمند ترین تکنیک های واترمارکینگ می باشد.طیف گسترده ،سعی در گسترده سازی اطلاعات در سراسر طیف فرکانس سیگنال صوتی تا حدامکان دارد.نقطه ضعف این تکنولوژی،هزینه بالای آن می باشد.علاوه بر این،با توجه به تضمن الگوریتم های بعضی از الگوریتم های گران قیمت مانند تبدیل فوریه،بنابراین اجرای آن نیز به نوعی هزینه زا و دشوار است.با این حال به عنوان یکی از توانمندترین روش ها تلقی می شود[7].

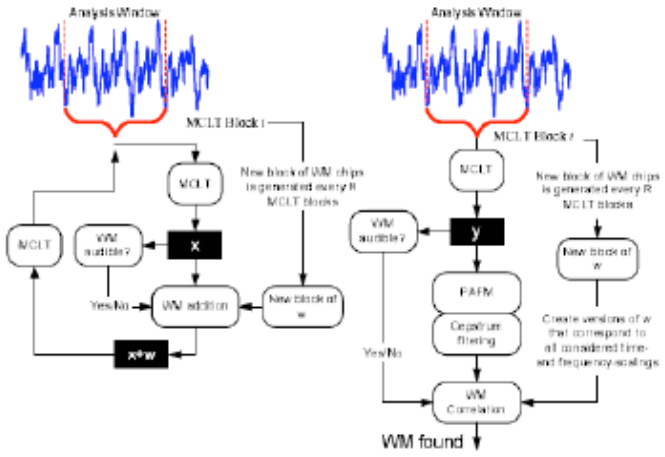
۳- تکنیک ها وروش ها

هیچگونه اجرای رایگان کانال پوشش صوتی را نمی توان به صورت رایگان بر بستر اینترنت یافت.بسیاری از مقالات پژوهشی بر واترمارکینک دیجیتالی برای حمایت ازکپی رایت متمرکز شده اند.بیشتر منابع برای طیف گسترده تصویر یافت شده تا اینکه کانال پوششی صوتی.دلائل احتمال آن هم بدین ترتیب هستند:اکثر تقاضای بازاریابی ناشی ازمساله کپی رایت است.در مقایسه با تصاویر دو بعدی،اجرای کانال پوشش طیف گسترده در موسیقی صوتی با توجه خصوصیات صدای انسان کمی دشوار تر می باشد.دقت کد زدایی پیام ،نیز بعنوان یک مساله قابل ملاحظه می باشد.هزینه ها با توجه به پهنای باندکمتر تعبیه اطلاعات ،بالا می باشد.اجرای آن دشوار و پیچیده است.روند کد دهی،به نوعی زمان بر است.اکثر کدها مبتنی بر C بوده وبه خوبی سازماندهی نشده اند. تکنیک طیف گسترده گزینشی : در اینجا پروژه در طرح DSSS (طیف گستره دنباله مستقیم) به طورمختصرتوصیف می شود.طرح های واترمارکینگ صوتی ،برنواقس سیستم شنیداری انسان (HAS)استناد می کنند.تکنیک های مخفی سازی داده به بررسی این واقعیت می پردازند مبنی براینکه HAS نسبت به تغییرات دامنه ای کوچک در حوزه فرکانس یا زمان غیر حساس می باشد. مزیت SS این است که تشخیص واترمارک مستلزم گزارش اولیه نبوده و استخراج داده پنهان شده با استفاده از تحلیل آماری بهینه تحت بعضی از خاص دشوار می باشد. روش DSSS را می توان با استفاده از نمودار زیر بیان نمود[7] .(شکل۱۰)



شکل ۱۰ : روش DSSS را می توان با استفاده از نمودار زیر بیان نمود

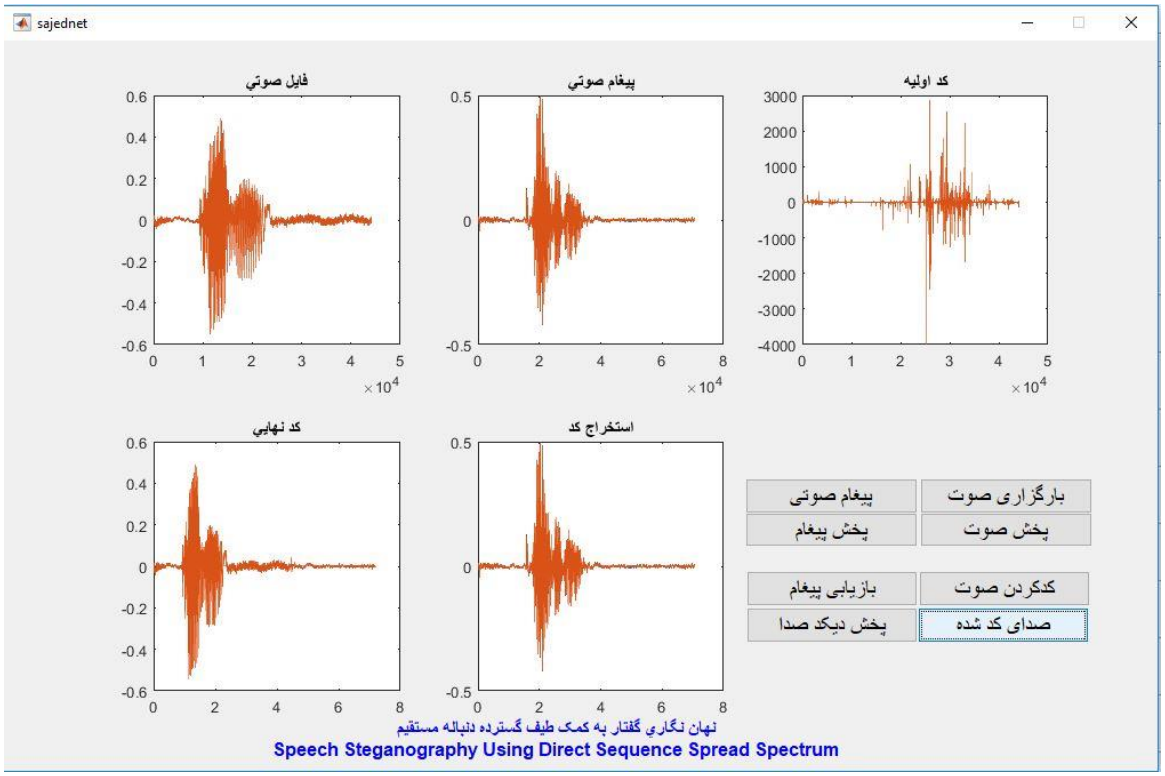
تبدیل همپوشان پیچیده مدوله شده(MCLT) ،برای انتقال اطلاعات صوتی به دامنه اطلاعاتی مورد استفاده قرار می گیرد.دردامنه فرکانس ،اطلاعات با استفاده از الگوریتم خاص در سیگنال تعبیه می شود .درپایان نیز، MCLT معکوس شده (iMCLT) به منظور انتقال مجدد سیگنال به نمونه های دامنه زمانی به کار می رود.نمودار زیر (شکل۱۱)،نشان می دهد که چگونه اطلاعات رمز نگاری و رمز گشایی می شوند. در اینجا از R شبه تصادفی برای ایجاد چریب های واترمارک برای بلوک i استفاده می شود.



شکل ۱۱ : چگونگی اطلاعات رمز نگاری و رمز گشایی

۴–محیط برنامه

یک برنامه اثبات‌کننده نوشـته شـده به زبان متلب که طبق آن تائید می‌شـود کاربران می‌توانند به‌راحتی اطلاعات را در فایل Hz x 2Channel .wav۴۴۱۰۰ رمزگذاری و رمزگشایی کنند.(شکل ۱۲)



شکل ۱۲ : محیط برنامه

5–نتیجه‌گیری

تکنولوژی واترمارکینگ صـوتی و محصـولات مربوطه تنها برای حمایت کپی رایت مورد اسـتفاده قرار می گیرند.رویه کانال پوشـشـی مبتنی بر واترمارکینگ سـیگنال صـوتی را نمی توان چندان در اینترنت یافت.مسـائل امنیتی کامپیوتری در زندگی روزمره امروزی ما بسـیار رایج شده است.این مساله منجربه افزایش قابل ملاحظه تقاضای طراحی سیستم های بسیار امنیتی

شده است.تا کنون هیچگونه رویکرد امنیتنی واحد نتوانسته سیستم را به طور کامل غیر قابل اجتناب سازد.اصل امنیتی طراحی در عمق نیز مساله ای مهم می باشد.این مساله مستلزم آن است که به ارزیابی گسترده و انتخاب مولفه های امنیتی پرداخت.طیف گسترده دنباله مستقیم ،یک تکنولوژی واترمارکینگ توانمند است.استگانوگرافی ،به عنوان شیوه ای ایمن در انتقال داده محرمانه در دنیای دیجیتال امروزی است.در این تحقیق،روش استگانوگرافی با ظرفیت تعبیه صوتی فوق العاده با استفاده از شبیه سازی DSSS پیشنهاد می شود.سیگنال های اصلی و پنهان شده شبیه هم بودند.زیرا حداقل شانس تشخیص پیام های محرمانه مخفی در صدای پنهانی وجود دارد.

۶–قدردانی

اینجانب از جناب آقای دکتر علی برومندنیا بخاطر نظرات و پیشنهاد های ارزشمند و کمک های ارزنده ایشان در تنظیماین مقاله ارائه شده تشکر می نمایم.

۷–مراجع

1. E. Armstrong, A Method of Reducing Disturbances in Radio Signalling by a System of Frequency Modulation, Proc. IRE, Vol. 24, pp. 689-740, May 1936
2. URL: http://inventors.about.com/library/inventors/bllamar.htm
3. URL: http://en.wikipedia.org/wiki/Chip_rate
4. Madhavi Chalamalasetti, Direct Sequence Spread Spectrum, October 2003 URL:http://www.bsnl.in/Telecomguide.asp?intNewsId=21019&strNewsMore=more
5. George R. Cooper, Clare D. McGillem, Modern Communications and Spread Spectrum, McGraw-Hill Book Company, 1986
6. Kaveh Pahlavan and Allen H. Levesque, Wireless Information Networks, Wiley and Sons, March 1995
7. URL: http://www.sss-mag.com/primer.html#vpintro
8. Jack Glas, The principles of Spread Spectrum communication, URL:http://cas.et.tudelft.nl/~glas/ssc/techn/techniques.html
9. Sorin M. Schwartz, Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), Alvarion Professional Education Center (ALPEC), version 7, December 2001.
10. Witold Jachimczyk, Spread Spectrum, http://webpages.charter.net/witek/ss/ss.html
11. Robert C. Dixon, Spread Spectrum Systems with Commercial Applications, third edition, Wiley and Sons, 1994, ISBN 0-471-59342-7
12. URL: http://cbdd.wsu.edu/kewlcontent/cdoutput/TR502/page74.htm
13. URL:http://www.isa.org/InTechTemplate.cfm?Section=General_Information2&template=/TaggedPage/DetailDisplay.cfm&ContentID=49893
14. Robert A. Scholtz, "The Origins of Spread-Spectrum Communications", IEEE Trans. Commun., vol. COM-30, pp. 822-854, May 1982.