نهان نگاری مقاوم صحبت در حضور تبدیل LPC

رقیه دوست[i]؛ حسن آقایی نیا[ii]؛ حسین شمسی[iii]

چکیده

پارامتر مهمی که در نهان نگاری[1] باید تأمین شود، مقاومت[2] آن در برابر انواع تبدیلات، فشرده سازی‌ها و نویزهای عمدی و غیر عمدی، است. بدین منظور معمولاً واردسازی[3] علامت پیوند[4] در یک حوزه تبدیل مناسب و با تکنیکی خاص صورت می‌گیرد. هدف این مقاله، یافتن روشی مناسب جهت نهان نگاری در صحبت است، به طوری که در برابر تبدیل LPC مقاوم باشد. به دلیل خواص مطلوب کدهای شبه نویز طیف گسترده از نوع طول ماکزیموم[5]، این کدها را به منظور تولید علامت پیوند مورد استفاده قرار دادیم. با بررسی اثری که تبدیل LPC و عکس آن بر روی این نوع از علامت پیوند می گذارد روش جدیدی در آشکارسازی علامت پیوند در گیرنده به دست آوردیم. به این ترتیب، بدون اینکه فرآیند واردسازی علامت پیوند مستلزم حوزه ی تبدیل خاص و تکنیک پیچیده‌ای باشد، هدف ذکر شده محقق می‌شود.

کلمات کلیدی

نهان نگاری، علامت پیوند، مقاومت، طیف گسترده، تبدیل LPC

Robust Speech Watermarking Against the LPC Transform

Roghayeh Doost; Hassan Aghaeinia: Hossein Shamsi

ABSTRACT

An important parameter in watermarking that must be considered is its robustness against various transforms, compressions, intentional and non-intentional noise. To achieve this, usually an appropriate transform domain and special techniques are employed for watermark insertion. The goal of this paper is to find an appropriate method for speech watermarking that is robust against the LPC transform. Because of beneficial characteristics of the m-sequence pseudo noise (PN) code, as a spreading code used in spread spectrum systems, m-sequence PN code is employed for watermark generation in this paper. Surveying the effects of the LPC transform and its inverse transform on the spread spectrum watermark, in this paper a novel method is proposed to detect the spread spectrum watermark in the receiver. So using no complex techniques or special transform domain in watermark insertion, the above goal is achieved.

KEYWORDS:

Watermarking, watermark, robustness, spread spectrum, LPC transform

[i] دانشجوی دکتری، دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر، rdoost@aut.ac.ir

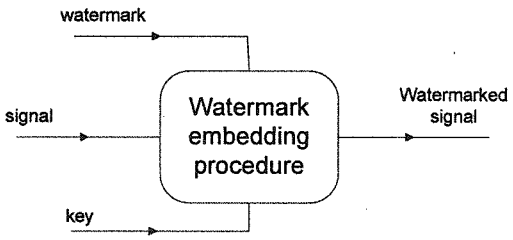
[ii] هیئت علمی، دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر، aghaeini@aut.ac.ir

[iii] دانشجوی دکتری ، دانشکده مهندسی برق دانشگاه تهران، hshamsi@ut.ac.ir

۱- مقدمه

طی سالهای اخیر نهان نگاری از موضوعاتی بوده که بسیار مطالعه شده است[۱]. اساس روش نهان‌نگاری اضافه کردن یک سری اطلاعات بر روی اطلاعات اصلی است، به طوری که اطلاعات نهان نگاری شده از لحاظ ادراکی با اطلاعات نخستین تفاوتی نداشته، و علامت پیوند چه از لحاظ ادراکی و چه از لحاظ آماری قابل آشکارسازی نباشد.

فرآیند کلی نهان نگاری را می‌توان در شکل ۱ مشاهده کرد [۲].



شکل(۱) : فرآیند کلی وارد سازی علامت پیوند

در بیشتر روش‌های آشکارسازی، در نهان نگاری به شیوه‌ی طیف گسترده، تابع همبستگی و یا فیلتر تطبیقی استفاده می شود. در [۳] به نحوی مناسبی این روش تحلیل شده است. البته روش هایی می‌توان یافت که خارج از این حیطه قرار دارند. از جمله روشی که دراین تحقیق به کار رفته است.

۲- تبدیل LPC

بیشتر کدک های موجود با نرخ بیت کم و مخصوصاً انواعی که در مخابرات سیار استفاده می شوند، به دلیل کیفیت قابل قبول روش LPC در نرخ بیت کم، بر اساس این روش طراحی می‌شوند. بنابراین این کدک از اهمیت خاص برخوردار است. این کدک بر اساس خواص با صدا یا بی صدا بودن صحبت طراحی شده است [۴]. در بخش مربوط، اثرات این تبدیل بر روی رشته ی علامت پیوند بررسی می‌شود. با بررسی این اثرات روشی برای آشکارسازی علامت پیوند، به دست می‌آید، در حالیکه صحبت نهان نگاری شده تحت این تبدیل قرار گرفته باشد.از نرم افزار LPC ارائه شده در [۵] جهت شبیه سازی‌های این تحقیق استفاده می‌کنیم.

۳- تولید و واردسازی علامت پیوند

در این تحقیق به دلیل خواص مطلوب و مورد نظر کدهای شبه نویز طول ماکزیموم، از این کد به منظور تولید *watermark* استفاده می‌گردد. طول کد مذکور را L_D می‌نامیم و قطعه های صحبت را با همین طول تشکیل می‌دهیم. به منظور برآورده سازی کیفیت ادراکی[۶] به میزان لازم، هر یک از چیپ های کد شبه نویز را در ضریبی ضرب می‌کنیم. به این ترتیب در یک کد شبه نویز، ضریب چیپ k ام عبارت است از:

$$f(k)=\sqrt{\frac{aud_m(k)^2}{E_{aud_m}}} \qquad (۱)$$

که در آن m شماره ی قطعه ی صحبت، $aud_m(k)$ مؤلفه kام در قطعه مذکور و E_{aud_m} انرژی این قطعه است.

$$E_{aud_m}=\sum_{k=0}^{L_D-1} aud_m{}^2(k) \qquad (۲)$$

ضریب بالا موجب می‌شود که مؤلفه ی علامت پیوند متناظر با مؤلفه ضعیف تر در قطعه صحبت، دارای دامنه کمتر و در مورد مؤلفه‌های قویتر صحبت دارای دامنه‌ی بیشتر باشد. به این ترتیب از شنیده شدن مؤلفه هایی از علامت پیوند، که با مؤلفه‌های ضعیف صحبت جمع شده اند جلوگیری می‌شود. در ضمن انرژی هر علامت پیوند باید در حدی باشد که با توجه به میزان انرژی هر قطعه، شنیده نشود. به این منظور ضریب زیر را در علامت پیوند هر قطعه ضرب می‌کنند.

$$a=0.1\sqrt{E_{aud_m}} \qquad (۳)$$

ضریب ۰،۱، به روش سعی و خطا و به منظور جلوگیری از شنیده شدن علامت پیوند به دست آمد.

حال اگر کد شبه نویز اولیه را *DS* بنامیم، مؤلفه ی kام علامت پیوند، قبل از ضرب واحد اطلاعاتی، عبارت است از:

$$w(k)=a.f(k).ds(k) \qquad (۴)$$

اطلاعات را رشته‌ای از صفر ویک در نظر می‌گیریم: *Data*=1 0 ... 0 1 0 1 1 1 0. به هرقطعه یک بایتری از ارقام اطلاعات بالا با ضرب در علامت پیوند اخیر اضافه می‌شود.

$$WAUD_m=AUD_m+Data(m).W_m \qquad (۵)$$

در رابطه ی (۵)، $Data(m).W_m$ علامت پیوند تولید شده برای قطعه mام، AUD_m و $WAUD_m$ به ترتیب قطعه mام صحبت اصلی و صحبت نهان نگاری شده می‌باشند. به طور ساده تر می توان گفت که اگر *Data(m)=0* باشد هیچ علامت پیوندی به آن قطعه اضافه نمی شود و اگر *Data(m)=1* باشد علامت پیوند W_m به آن قطعه اضافه می‌شود.

مزایای این روش واردسازی، عبارت است از ساده بودن عملیات ساخت و واردسازی علامت پیوند و کم بودن پیچیدگی محاسبات. هم چنین تمام اعمال وارد سازی در حوزه زمان

انجام می‌شود و به این ترتیب مدت زمان نسبتاً کمی را لازم دارد. در بلوک دیاگرام شکل ۲ این روش به تصویر کشیده شده است. خروجی عملگر ضرب نقطه ای در این شکل، برداری است که هر مؤلفه‌ی آن حاصلضرب مؤلفه‌های متناظر دو بردار ورودی است.

٤- آشکارسازی علامت پیوند توسط روشی جدید

در این روش، سیگنال اصلی در آشکارسازی موجود است. سیگنال دریافتی را $RAUD$ می‌نامیم.

$$W_m' = RAUD_m - codec(AUD_m) \qquad (۶)$$

حال با توجه به اینکه سیگنال دریافتی نهان نگاری شده باشد یا خیر، یکی از دو کمیت زیر را در آشکارساز خواهیم داشت:

$$RAUD_m = codec(WAUD_m + NOISE) \qquad (۷)$$

برای حالتی که قطعه مورد نظر دارای علامت پیوند باشد و نیز:

$$RAUD_m = codec(AUD_m + NOISE) \qquad (۸)$$

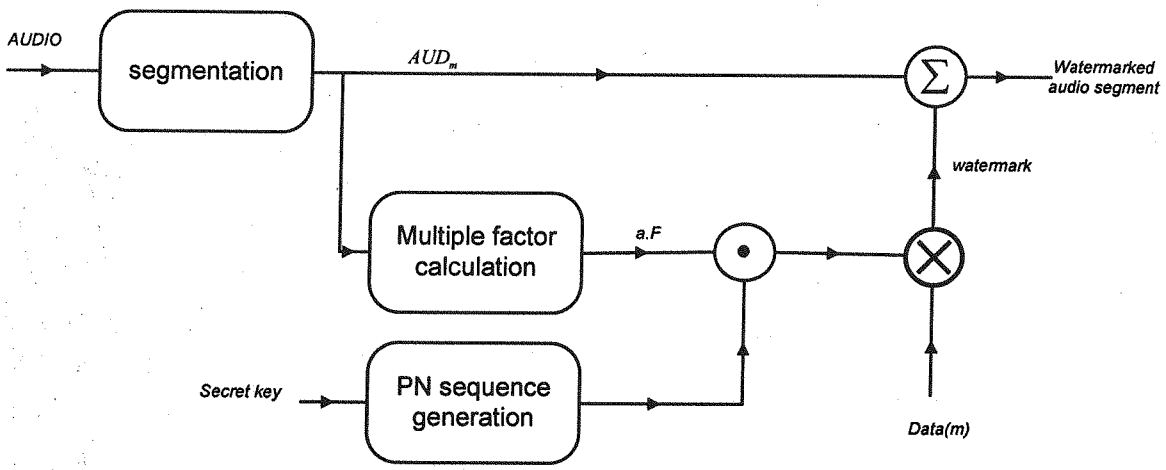
برای حالتی که قطعه مورد نظر بدون علامت پیوند باشد. در رابطه های (۷) و (۸)، $codec$ بیانگر تبدیل و عکس تبدیل صورت گرفته است، که در این تحقیق LPC می‌باشد. برای مدل کردن کانال، نویز گوسی مدل گردیده و اثرات آن در بخش مربوط $codec$ قرار گرفته است:

$$err_m = codec(W_m) - W_m \qquad (۹)$$

کمیتی که به طور مستقیم در این روش آشکارسازی مورد بررسی می شود عبارت است از:

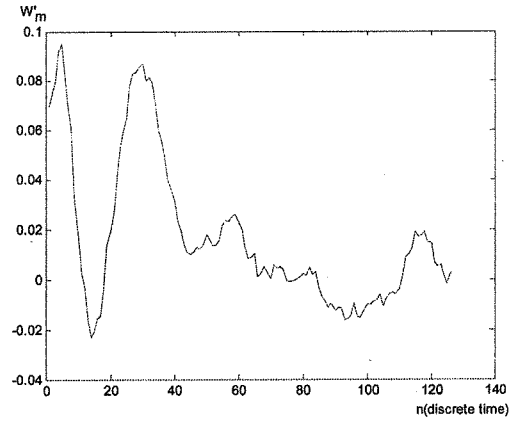
$$MW_m' = W_m' - err_m \qquad (۱۰)$$

شاید در اینجا به نظر برسد که ساده ترین و بهترین راه آشکارسازی این است که کمیت اخیر را با W_m، که آن را در گیرنده مجاز داریم ضرب کنیم و با روش معمول همبستگی و با استفاده از یک حد آستانه مجاز وجود علامت پیوند را آشکار سازی نماییم. ولی باید توجه کنیم که حدود تغییرات err_m در محدوده تغییرات خود W_m یا W_m' است. این تغییرات زیاد موجب خطای زیادی در آشکارسازی می‌شود. برای واضح تر شدن مطالب، به شکل های ۳ تا ۷ توجه نمائید. همانطور که در این شکل ها مشاهده می‌شود، در حالتی که علامت پیوند در قطعه وجود نداشته باشد، شکل MW_m'، تا حد زیادی شبیه err_m است و اگر علامت پیوند موجود باشد، شکل مذکور شبیه به W_m می‌باشد. بین این دو شکل تفاوت قابل استفاده ای وجود دارد و بدین قرار در err_m نمونه‌های ابتدایی دارای دامنه‌ی نسبتاً بزرگی هستند.



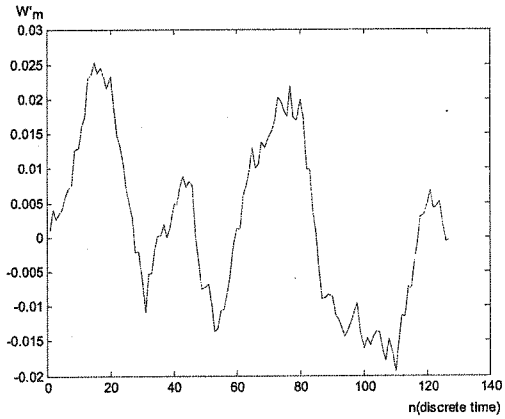
شکل۲ : بلوک دیاگرام وارد سازی

بررسی می‌شود. نکته قابل توجه دیگر اینکه، قطعاتی که به منظور وارد سازی علامت پیوند ایجاد می‌شوند با قطعاتی که مورد پردازش این تبدیل و عکس آن قرار می‌گیرند هم زمان هستند. کمیت مورد توجه دیگر، اختلاف علامت پیوند اصلی وارد شده در قطعه و علامت پیوندی است که تحت تبدیلات



شکل(۳) : W'_m در حالتی که علامت پیوند موجود است

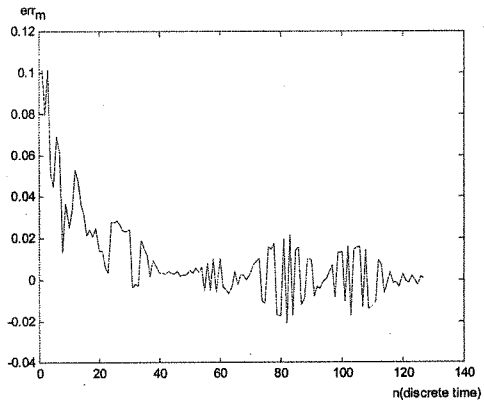
از همین خاصیت در آشکارسازی علامت پیوند استفاده می‌شود. به این ترتیب که در آشکارساز، MW'_m ایجاد می‌شود و سپس k نمونه‌ی ابتدای آن با هم جمع شده و با یک آستانه مناسب مقایسه می‌شوند. البته حد آستانه هم با کمک جمع همین تعداد نمونه از err_m به دست می‌آید. به این ترتیب وجود یا عدم وجود علامت پیوند در قطعه مورد نظر، آشکار می‌شود. در بلوک دیاگرام شکل ۸ این روش ارائه شده است.



شکل(۴): W'_m در حالیکه علامت پیوند موجود نیست

۵- نتایج شبیه سازی

با مقادیر مختلف k ، و طول قطعه برابر ۱۲۷، نرخ خطا برای kهای مختلف مطابق جدول ۱ به دست آمد. بدین ترتیب مشخص شد که هرچه k کوچکتر باشد خطا کمتر خواهد بود. ولی k را برابر با ۲ انتخاب نمودیم نه ۱، به این ترتیب نمونه های بیشتری در آشکارسازی دخیل می‌شوند و در مورد برخی از قطعه‌ها، تصمیم گیری تنها از روی یک نمونه کار پرخطری بوده و خصوصاً زمانی که علامت پیوند موجود نیست با خطای غیر قابل قبولی مواجه می‌شویم. پس انتخاب با این احتیاط، و با توجه به اینکه خطای آشکارسازی در حالت k برابر ۱ یا ۲ تفاوت چندانی ندارد، انجام شد.



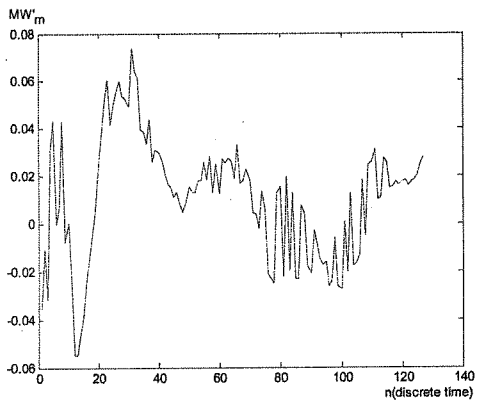
شکل(۵): err_m، اختلاف بین W_m و $codec(W_m)$

۵-۱- تغییرات *BER* بر حسب توان نویز

با زیاد شدن توان نویز انتظار می رود که تخریب علامت پیوند بیشتر و در نتیجه آشکارسازی آن با خطای بیشتری مواجه شود [٦]. با صحبت یکسان و طول‌های ۱۲۷ و۵۱۱ و ۲۰۴۷ برای علامت پیوند، نتایج زیر به دست آمد. منظور از SNR در جداول ۲ تا ٤ نسبت توان صحبت به نویز می باشد. منحنی حاصل از سه جدول اخیر همزمان در شکل ۱۰ رسم شده اند. دیده می‌شود که در اثر افزایش SNR کاهش BER را در هر مورد خواهیم داشت. ولی از همین شکل مشخص است که در صورتی می‌توان با قاطعیت گفت افزایش طول علامت پیوند موجب کاهش BER می‌شود که نسبت سیگنال به نویز از آستانه ای بالاتر باشد.

۵-۲- کیفیت ادراکی

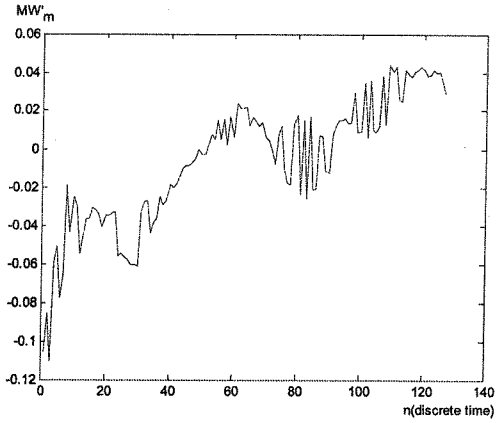
این کیفیت به دو طریق کیفی و کمی قابل اندازه گیری است. روش کیفی آن، این است که صدای نهان نگاری شده و در پی آن صدای اولیه را در معرض شنیدن قرار دهند. تفاوت



شکل(۶): MW'_m در حالیکه علامت پیوند موجود است

محسوس و قابل توجهی بین این دو نیست. به این ترتیب از لحاظ کیفیت ادراکی این نهان نگاری قابل قبول است، چرا که وجود علامت پیوند از طریق شنیدن حدس زده نمی‌شود.

در حالت سنجش کمی نیز از رابطه ی *SNR* با تعریف زیر



شکل(۷): MW'_m در حالیکه علامت پیوند موجود نیست

استفاده شود [۶].

$$SNR = 10\log_{10}\left(\frac{\sum_{n=0}^{N-1} AUD^2(n)}{\sum_{n=0}^{N-1}(WAUD(n)-AUD(n))^2}\right) = 10\log_{10}\left(\frac{E_{AUD}}{\sum_{n=0}^{N-1} W^2(n)}\right) \quad (11)$$

صحبتی که در اینجا نهان نگاری می‌شود *AUD* و تعداد نمونه‌های آن *N* است. برای سهولت سیگنالی را که از کنار هم گذاشتن علامت پیوند هر قطعه ایجاد می‌شود را *W* نام گذاری کردیم. *SNR* برای علامت پیوند با هر طولی و صدای *s2ofwb* و دیگر شرایط یکسان برابر *dB* ۲۰ به دست آمد. علت یکسان بودن این کمیت برای طول‌های متفاوت هم ناشی از نحوه تولید هر علامت پیوند است. برای به دست آوردن *SNR* بیشتر باید ضریب علامت پیوند اضافه شده را کاهش داد و البته به منظور بهبود و جبران *BER* می‌بایست طول علامت پیوند افزایش یابد، که در پی آن کاهش ظرفیت نهان نگاری را خواهیم داشت.

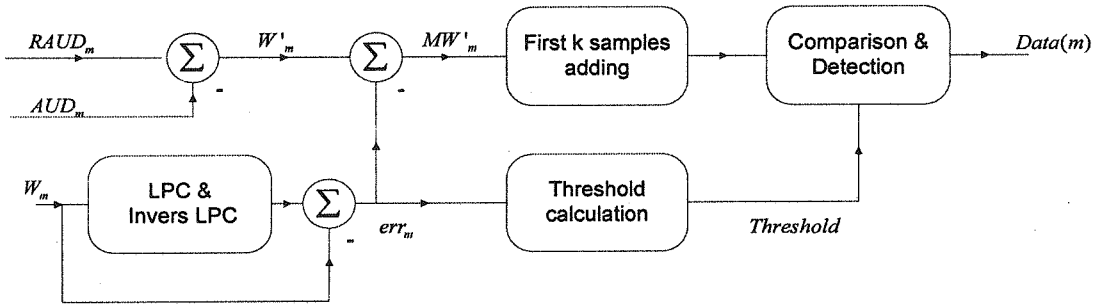
۵-۳- پیچیدگی محاسباتی

منظور از پیچیدگی محاسباتی، میزان پردازش لازم برای واردسازی و یا آشکارسازی علامت پیوند در صدا است. راه‌های گوناگونی به منظور تعیین کمی این مقدار وجود دارد، ولی یکی از راه های ساده و معمول آن اندازه گیری مدت زمان لازم برای اجرای آن برنامه توسط ریزپردازنده مورد استفاده می‌باشد[۶]. با ریزپردازنده پنتیوم چهار و توسط نرم افزار *MATLAB 6.5* زمان لازم برای واردسازی و آشکارسازی علامت پیوندها با طول‌های مختلف، مطابق جدول ۵ است.

علت تحلیلی سیرهای صعودی و نزولی زمان واردسازی وآشکارسازی را می‌توان این گونه بیان کرد که، در واردسازی علامت پیوند بیشتر زمان مربوط، صرف تولید علامت پیوند می‌شود. به این ترتیب با افزایش طول علامت پیوند این زمان و زمان واردسازی بیشتر می‌شود. در آشکارسازی نیز با افزایش طول علامت پیوند، تعداد قطعاتی که باید مورد فرآیند آشکارسازی قرار گیرند کاهش می‌یابد و در نتیجه زمان لازم برای آشکارسازی کم می‌شود. البته دیده می‌شود که در طول‌های بالا زمان آشکارسازی حالت صعودی و در طول‌های پایین زمان واردسازی حالت نزولی دارد که می‌توان علت آن را با عکس تحلیل بالا برای هر یک از این زمانها پذیرفت. یعنی نهایتاً در مدت زمان آشکارسازی و واردسازی، هم طول قطعات و هم تعداد قطعات اثر گذارند، ولی در آشکارسازی تعداد قطعات و در واردسازی طول آنها مؤثرتر هستند[۷].

۶- نتیجه

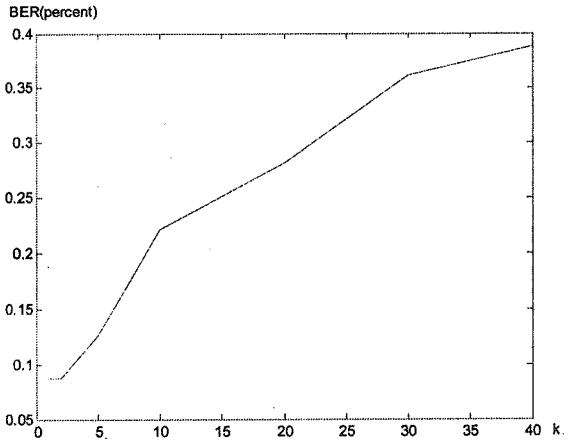
در الگوریتم یاد شده، روش بسیار ساده‌ای به منظور واردسازی علامت پیوند به کارگرفته شد و بدون اینکه تبدیلی بر روی سیگنال اولیه صورت گیرد علامت پیوند مستقیماً به آن اضافه شد. این در حالی است که معمولاً به منظور مقاوم سازی نهان نگاری، علامت پیوند را در حوزه تبدیلی به سیگنال، اضافه می نمایند. ولی در این الگوریتم ما این مقاومت را از طریق بهبود روش آشکارسازی علامت پیوند که مختص نبدیل LPC است ایجاد کردیم. البته در کنار کم بودن پیچیدگی محاسباتی و مدت زمان لازم در واردسازی علامت پیوند، زیاد بودن پارامترهای یاد شده را در آشکارسازی علامت پیوند خواهیم داشت.



شکل(۸) : بلوک دیاگرام آشکارسازی

جدول(۱) : تغییرات BER بر حسب k

k	BER
۴۰	۰،۳۸۷۹
۳۰	۰،۳۶۱۵
۲۰	۰،۲۸۲۳
۱۰	۰،۲۲۱۶
۵	۰،۱۲۶۶
۲	۰،۰۸۷۱
۱	۰،۰۸۷۱



شکل (۹) :تغییرات BER بر حسب k

جدول(۲) : تغییرات BER بر حسب سیگنال به نویز، با طول علامت پیوند ۱۲۷

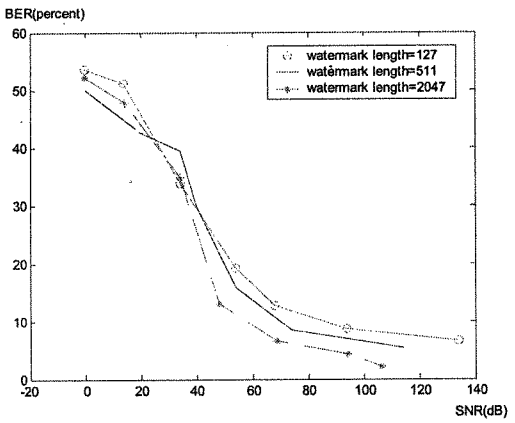
SNR(dB)	BER
۱۳۳،۷۹۷۵	۰،۰۶۶۰
۹۳،۸۹۸۳	۰،۰۸۷۱
۶۷،۸۲۱۹	۰،۱۲۶۶
۵۳،۸۷۷۱	۰،۱۹۲۶
۳۳،۸۲۸۶	۰،۳۳۷۷
۱۳،۸۴۵۲	۰،۵۱۱۹
-۰،۱۸۳۷	۰،۵۳۵۶

جدول(۳): تغییرات BER بر حسب سیگنال به نویز با طول علامت پیوند ۵۱۱

SNR(dB)	BER
۱۱۳،۸۹۸۶	۰،۰۵۳۲
۷۳،۸۵۰۴	۰،۰۸۵۱
۵۳،۸۸۹۶	۰،۱۵۹۶
۳۹،۹۰۷۴	۰،۲۹۷۹
۳۳،۸۵۶۲	۰،۳۹۳۶
۱۹،۸۵۹۵	۰،۴۲۵۵
۰،۲۴۸۶	۰،۵۰۰۰

جدول(۴) : تغییرات BER بر حسب سیگنال به نویز با طول علامت پیوند ۲۰۴۷

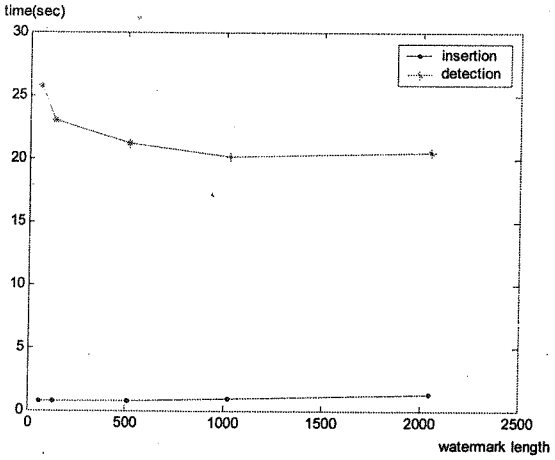
SNR(dB)	BER
۱۰۶،۱۷۶۸	۰،۰۲۱۵
۹۴،۱۲۵۷	۰،۰۴۳۵
۶۸،۷۱۵	۰،۰۶۵۰
۴۸،۱۱۵۹	۰،۱۳۰۴
۳۴،۱۶۳۱	۰،۳۴۷۸
۱۴،۱۱۳۴	۰،۴۷۸۳
-۰،۲۲۹۴	۰،۵۲۱۷



شکل(۱۰) : تغییرات BER بر حسب SNR

جدول(۵) : تغییرات زمان واردسازی و آشکارسازی علامت پیوند بر حسب طول آن

Watermark length	Insertion timing(sec)	Detection timing(sec)
۶۳	۰،۷۵۱۰	۲۵،۷۸۳۰
۱۲۷	۰،۷۳۵۰	۲۳،۰۶۲۰
۵۱۱	۰،۷۵۰۰	۲۱،۱۴۱۰
۱۰۲۳	۰،۹۲۱۰	۲۰،۰۹۱۰
۲۰۴۷	۱،۲۶۶۰	۲۰،۴۶۶۰
mean	۰،۸۸۴۶	۲۲،۱۰۸۶



شکل(۱۱): زمان واردسازی وآشکارسازی بر حسب طول علامت پیوند

۷- مراجع

[۱] Chiristine I.Podilchock ; Edward J.Delp,"Digital Watermarking: Algorithm and application",IEEE Signal processing Magazine, Pages:33-35, 2001.

[۲] Mitchell D.swanson; Ahmed H.Tewfik,"*Multimedia Data-Embedding and Watermarking Technologies*", proceedings of the IEEE,Vol.86, pages: 1064-1069, 1998.

[۳] Darko Kirovski; Henrique S.Malvar,"*Spread Spectrum Watermarking of Audio Signal*",IEEE Transactions on Signal Processing,Vol.51,NO.4,Pages:1021,April 2003.

[۴] .A.RAZI," *Survey & Simulation of Speech Coding Standard & Techniques for Mobiles Systems* " Amirkabir university of technology, Electrical Engineering Department, M.Sc.Dissertation, page:18, 2001.

[۵] http://www.yov408.com/html/tutorials.php.

[۶] J.D.Gordy; L.T.Bruton."*Performance Evaluation of Digital Audio Watermarking Algorithms*",Proc.43P[rdP] IEEE Midwest Symp. On Circuits and Systems,Lansing MI,Pages:456-459, 2000.

[۷] دوست، رقیه؛ پایان نامه کارشناسی ارشد "بهبود نهان نگاری صحبت در مخابرات سیار "،حسن آقائی نیا، دانشگاه صنعتی امیرکبیر، ۱۳۸۱.

۸- زیرنویس ها

۱. watermarking

۲. robustness

۳. insertion

۴. watermark

۵. m-sequence

۶. perceptual quality