علوم و مهندسی کامپیوتر
نشریه علمی پژوهشی انجمن کامپیوتر ایران
مجلد ۵، شماره ۳، ۱۳۸۶
صفحات ۳۹-۴۴
مقاله کوتاه

نشانه‌گذاری بلادرنگ فایل‌های صوتی MP3

امیرمنصور پزشک کمال پوررضایی

پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

چکیده

رمزنگاری یا درهم‌ریزی داده‌های صوتی جهت کنترل انتشار آثار صوتی کافی نبوده و باید از روش‌های نشانه‌گذاری شفاف به منظور جلوگیری از توزیع غیرمجاز این آثار و حفظ حقوق پدیدآورندگان و ناشران آنها بهره‌گیری نمود. نشانه‌گذاری فایل‌های فشردهٔ MP3 قرار گرفته در اینترنت نیازمند نوع ویژه‌ای از نشانه‌گذاری بصورت جایگذاری مستقیم اطلاعات در رشته ـ بیت تشکیل دهندهٔ MP3 می‌باشد. در این مقاله روشی نوین جهت نشانه‌گذاری داده‌های صوتی فشرده MP3 مطرح شده است. ویژگی‌های بارز روش پیشنهادی مقاله در مقایسه با راهکارهای مشابه، امکان بازیابی مستقیم اطلاعات نشانه‌گذاری شده از سیگنال فشرده و عدم حساسیت در مقابل همزمان نبودن فریم‌های MP3 در دو وضعیت جایگذاری و بازیابی داده‌ها می‌باشند.

کلمات کلیدی: نشانه‌گذاری شفاف صدا، نشانه‌گذاری شفاف رشته - بیت، تصدیق هویت مالک اثر، فشرده‌سازی MP3، مخفی‌سازی داده.

۱- مقدمه

دستیابی به نرخ‌های بالاتر انتقال داده به‌همراه استفاده از فرمت‌های فشردهٔ صدا و ویدئو موجب گسترش روز افزون تبادل داده‌های چندرسانه‌ای در اینترنت شده است. این امر به نوبهٔ خود باعث آزادی عمل بیشتر سارقان دیجیتالی[۱] در کپی و توزیع غیرمجاز آثار چندرسانه‌ای و بخصوص آثار صوتی گردیده و بنابراین مسئلهٔ حفظ حقوق دستاوردهای معنوی[۲] را بیش از پیش ضروری می‌سازد. روش‌های نشانه‌گذاری شفاف[۳] با مخفی نمودن اطلاعات حق کپی[۴] در فایل صوتی امکان کنترل کپی و نیز پیگیری نسخه‌های کپی شده و تأیید پدیدآورندگان یا ناشران اصلی آثار صوتی را میسر می‌سازند. فرمت فشردهٔ MP3 برای فایل‌های صوتی بعنوان فراگیرترین روش تبادل داده‌های صوتی در اینترنت مورد استفاده می‌باشد. بکارگیری تکنیک نشانه‌گذاری شفاف برای این داده‌ها باید به‌صورت بلادرنگ[۵] و با ایجاد حداقل بار پردازشی اضافه برای سرورهای تحویل‌دهندهٔ آنها باشد. اکثر روش‌های مطرح شده برای نشانه‌گذاری شفاف صدا،[۳، ۴ و ۵] عمل مخفی‌سازی اطلاعات در فایل‌های صوتی MP3 را پس از دکود کردن آنها (خارج ساختن از فرمت فشرده) انجام می‌دهند و بنابراین نمی‌توان از این روش‌ها استفاده نمود.

بر مبنای ملاحظات ذکر شده، در این مقاله روشی کارا جهت جایگذاری مستقیم اطلاعات در حوزهٔ فشرده یا به‌عبارت بهتر رشته- بیت[۶] MP3 ارائه می‌گردد. یک روش نشانه‌گذاری رشته- بیت توسط مؤسسهٔ FhG-IIS که از پایه‌گذاران تکنیک فشرده‌سازی MP3 نیز می‌باشد مطرح شده است. [۱] در این روش، اگرچه جایگذاری داده‌ها در حوزهٔ رشته- بیت صورت می‌گیرد جهت بازیابی این داده‌ها لازم است که ابتدا سیگنال از حالت فشرده خارج شده و سپس آشکارسازی صورت گیرد. همزمانی واحدهای تولید دنبالهٔ تصادفی بین بخش‌های نشانه‌گذار و آشکارساز اطلاعات بزرگترین چالش در طراحی سیستم‌های نشانه‌گذاری می‌باشد.

سیستم پیشنهادی مقاله با رفع نیاز به همزمان بودن فریم‌های رشته - بیت MP3 علاوه بر کاهش چشمگیر پیچیدگی آشکارساز، امکان آشکارسازی مستقیم در حوزهٔ فشرده[۷] را نیز فراهم ساخته است. از اینرو سیستم پیشنهادی مذکور اولین سیستم نشانه‌گذاری رشته - بیت MP3 می‌باشد که هر دو عمل جایگذاری اطلاعات و بازیابی آنها را در حوزهٔ فشرده انجام می‌دهد. در اینجا به تشریح الگوریتم‌های پیشنهادی مقاله برای جایگذاری اطلاعات در رشته - بیت MP3 و بازیابی مجدد آنها می‌پردازیم.

۲- تشریح الگوریتم نشانه‌گذار رشته - بیت MP3

بخش اصلی رشته- بیت MP3 شامل نیم- فریم‌های[۸] ۵۷۶ نمونه‌ای،ix از ضرایب کوانتیزه تبدیل MDCT سیگنال صدای PCM می‌باشد. ضرایب واقع در این بردار که در واقع نوع توصیف سیگنال اصلی در حوزهٔ فرکانس هستند، به ۲۱ محدودهٔ فرکانسی غیر یکنواخت متناظر با باندهای بحرانی تقسیم می‌گردند.[۶] الگوریتم نشانه‌گذار بخشی از نمونه‌های بردار ix را متناسب با بیت نشانه به گونه‌ای تغییر می‌دهد که اعوجاج حاصل از افزایش نویز کوانتیزاسیون همچنان زیر سطح منحنی آستانهٔ پوشیدگی JND[9] هر یک از ۲۱ باند بحرانی قرار گیرد. ایده بکار رفته در الگوریتم توزیع یکنواخت اعوجاج در تمامی باندهای بحرانی و با در نظر گیری معیار امنیت می‌باشد.

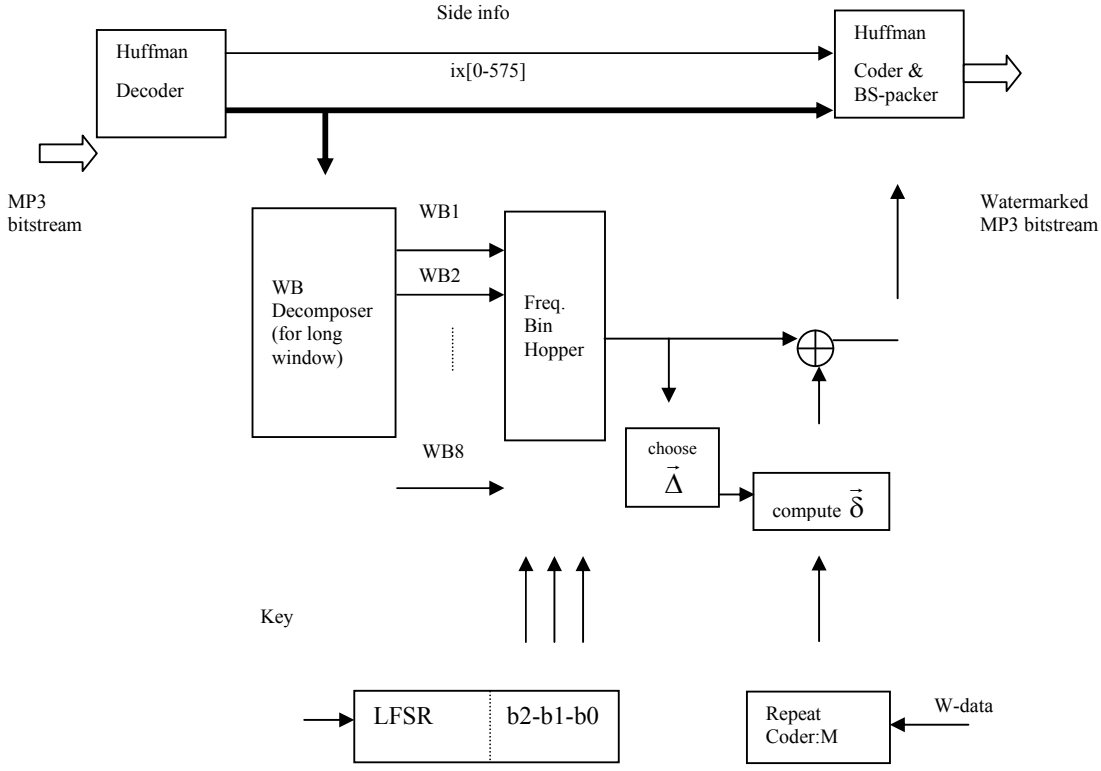
نشانه‌گذار با شروع از اولین نیم- فریم بزرگ به تغییر نمونه‌های بردار ix براساس بیت نشانه می‌پردازد. با توجه به حساسیت زیاد نمونه‌های واقع در پنجره‌های کوتاه، الگوریتم از دستکاری نیم- فریم‌های پنجره کوتاه صرف‌نظر می‌کند. از آنجا که هر بیت نشانه در تعداد زیادی از نیم- فریم‌ها قرار می‌گیرد، این امر تاثیر ناچیزی در پایداری داده‌های نشانه ایجاد می‌کند.

شکل ۱ بلاک دیاگرام نشانه‌گذار نیم- فریم را نشان می‌دهد. نمونه‌های واقع در ۲۱ باند بحرانی به ۸ قسمت تقریباً مساوی تقسیم شده و بخش‌های متناظر در باندهای ۱ تا ۲۱ در ۸ باند نشانه‌گذاری WB_1 تا WB_8 قرار می‌گیرند. از آنجایی که ۸ باند بحرانی ابتدایی کمتر از ۸ نمونه دارند توزیع آنها در ۸ باند WB_1 تا WB_8 به گونه‌ای صورت گرفته است که باندهای متداخل WB_i و WB_j بیش از دو نمونه مشترک نداشته باشند. بدین ترتیب باندهای نشانه WB_1 تا WB_8، مجموعه ix را به ۸ زیرمجموعه تقریباً متعامد ۵۶ عضوی افراز می‌کنند. سه بیت کم ارزش یک LFSR که با مقدار کلید نشانه‌گذاری، K مقداردهی اولیه شده است WB_k. یکی از ۸ باند WB_1 تا WB_8 را از بردار ix هر نیم- فریم به‌طور تصادفی برمی‌گزیند. ۵۶ نمونه طیفی موجود در این باند در بخش مدولاتور به‌صورت زیر تغییر می‌یابند. ابتدا هر یک از بیت‌های بردار داده‌های نشانه W توسط کدینگ کانال تکرار 1:M به M بیت یکسان d تبدیل شده و سپس هر بیت d یکی از نیم- فریم‌ها را مدوله می‌کند.

جهت اینکار مطابق رابطه زیر یکی از دو کد ۲۱ بیتی C1 یا C0 با توجه به یک یا صفر بودن d انتخاب شده و مطابق رابطهٔ زیر در بردار Δ پارامتر دامنه مدولاسیون ضرب می‌گردد.

$$\vec{\delta} = [2(d \cdot C\vec{1} + (\vec{l}_{21} \wedge d) \cdot C\vec{0}) - \vec{l}_{21}] * \vec{\Delta}$$

در این رابطه * به مفهوم ضرب نقطه‌ای دو بردار می‌باشد. سپس قدر مطلق خطوط طیفی واقع در اشتراک باند نشانهٔ WB_k و باند بحرانی iام به اندازهٔ درایهٔ iام بردار $\vec{\delta}$ که برابر یکی از دو مقدار $\pm\Delta_i$ می‌باشد، افزایش یا کاهش می‌یابند.



شکل ۱- بلاک دیاگرام نشانه گذار نیم ـ فریم‌ها

بردار Δ متشکل از عناصر صحیح Δ_i به گونه‌ای تعیین می‌شود تا نمونه‌های فرکانسی بزرگتر تغییرات کمتری متحمل شده و در نتیجه نویز اعمالی به باندهای بحرانی همسان گردد. در پایان مقادیر تغییر یافته WB_k به‌صورت هافمن کد شده و در صورتیکه طول نیم- فریم کد شدهٔ جدید از طول نیم- فریم اصلی تجاوز نکند، کدهای حاصله در رشته- بیت قرار می‌گیرند. بدین ترتیب بسته به مقدار d انرژی بخش مشترک باند نشانهٔ WB_k و هر یک از ۲۱ باند بحرانی افزایش یا کاهش می‌یابد. خواهیم دید که آشکارساز نشانه با بررسی این تغییرات انرژی اعمال شده به زیر - باندهای WB_k به تشخیص بیت‌های نشانه می‌پردازد.

۳- تعیین پارامترهای نشانه‌گذار

در اینجا به نقش و چگونگی تعیین پارامترهای مدولاتور می‌پردازیم. بردارهای ۲۱ بیتی C1 و C0 متعامد بوده $C0 = \overline{C1}$ و به‌صورت عمومی (در اختیار همه) بکار می‌روند. در ظاهر درجه آزادی فراوانی در انتخاب آنها وجود دارد، ولی باید در نظر داشت که در صورت بکارگیری نشانه‌گذاری به‌صورت چند لایه باید تمامی جفت C1- C0های لایه‌ها متعامد باشند. بردار ۲۱ نمونه‌ای $\vec{\Delta}$ متشکل از مقادیر مثبت یک تا Δ_{max} می‌باشد. با انتخاب Δ_{max} به‌عنوان پارامتر مصالحه بین پایداری و شفافیت الگوریتم، مقادیر بردار $\vec{\Delta}$ به گونه‌ای انتخاب می‌گردند که معیار حداقل اعوجاج و عدم تغییر طول رشته- بیت نهایی پس از کدینگ هافمن نمونه‌های تغییر یافته تأمین گردد. فرض بر اینست که عناصر $\vec{\Delta}$ حتی‌المقدور نزدیک به Δ_{max} انتخاب می‌گردند.

بنابراین کنترل مشخصه‌های پایداری و شفافیت صرفاً با تعیین Δ_{max} صورت می‌گیرد. بگونه‌ایکه هر چقدر این پارامتر کوچکتر شود به جهت اعمال تغییرات کمتر در ویژگی‌های بردار ix، سیگنال حاصله متحمل اعوجاج کمتری شده و در نتیجه شفافیت بالاتری خواهیم داشت. از طرفی هر چقدر Δ_{max} بزرگتر می‌شود، اعوجاج اعمال شده به نمونه‌ها افزایش می‌یابد. طبیعی است سیگنال در این حالت مقاومت بیشتری در مقابل حملات مختلف از قبیل افزودن نویز به سیگنال PCM (پس از دکود شدن رشته- بیت) از خود نشان می‌دهد. می‌بینیم که در این حالت پایداری افزایش یافته ولی شفافیت کاهش یافته است. M پارامتر کدینگ تکرار به مصالحه بین پایداری و نرخ نشانه‌گذاری می‌پردازد. به‌طوریکه با افزایش M نرخ کاهش یافته ولی پایداری افزایش می‌یابد.

طول LFSR و در نتیجه طول کلید K تأثیر مستقیم در میزان امنیت سیستم دارد. در سیستم‌های نشانه‌گذاری نیز باید همانند رمزنگاری از طول کلیدهای بزرگ جهت داشتن امنیت کافی استفاده نمود. در واقع جهت مخدوش نمودن یک نشانه با کلید مجهول K، حمله کننده می‌تواند تمام فضای کلید را جستجو نموده و پس از خواندن اطلاعات نشانه به جایگذاری اطلاعات دلخواه خود با همان کلید بپردازد. (جایگزینی اطلاعات یک لایه با لایه بعدی بعلت مشابهت کلید).

بر مبنای این ملاحظات مقادیر پارامترهای M و Δ_{max} به‌ترتیب برابر ۲۴ و ۳ و طول LFSR برابر ۶۴ در نظر گرفته شد.

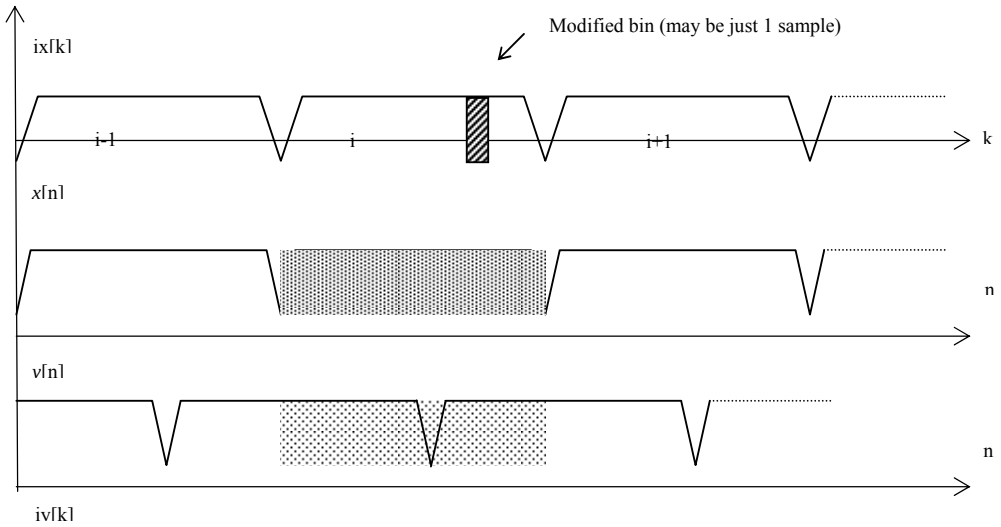
۴- آشکارساز نشانه

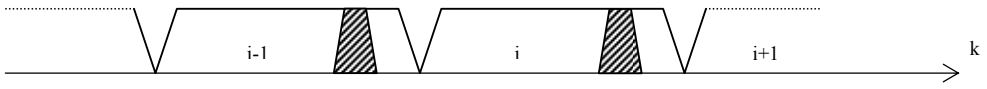
قسمت آشکارساز به بازیابی بیت‌های مخفی شده در رشته- بیت می‌پردازد. ترکیب نشانه‌گذار و آشکارساز باید به گونه‌ای عمل کنند که اطلاعات نشانه پس از تبدیلات متوالی بین حوزه فشرده و خطی (PCM) قابل بازیابی باشند. همچنین مسأله پایداری ایجاب می‌کند که پردازش‌های صورت گرفته بر سیگنال در حالت PCM از قبیل افزودن نویز یا فیلتر کردن موجب از بین رفتن علائم نگردد. در اینجا ابتدا به تحلیل اثر عدم تطابق پنجرهٔ نیم- فریم‌های نشانه‌گذار و آشکارساز پرداخته و سپس به تشریح الگوریتم بازیافت بیت می‌پردازیم.

۴-۱- بررسی مسأله انتقال پنجره

مهمترین مسأله در ارسال اطلاعات در بستر رشته بیت MP3 اینست که اطلاعات نشانه بدون نیاز به تبدیل رشته- بیت به یک سیگنال PCM قابل بازیابی باشند. این امر بخصوص در زمانی که رشته- بیت به‌صورت PCM در آمده و دوباره فشرده شده است اهمیت می‌یابد. در واقع شرط اصلی برای بلادرنگ بودن الگوریتم آشکارساز نشانه در همین نکته نهفته است. از این دیدگاه نقطه ضعف مهم الگوریتم FhG ([۱]) این است که سیگنال همواره باید به حوزهٔ زمانی (PCM) برده شود تا بیت‌های نشانهٔ قابل بازیابی شوند.

در انتقال مجدد رشته- بیت دکود شده MP3 به حالت فشرده پنجره‌های زمانی ۵۷۶ نمونه‌ای اعمال شده در انکودرها منطبق نیستند. در اینجا نشان می‌دهیم که با تغییر خطوط فرکانسی طیف کوانتیزه در نیم- فریم‌های نشانه‌گذار این تغییرات کماکان در فریم‌های انتقال یافته آشکارساز نیز وجود دارند.





شکل ۲- وضعیت پنجره‌های نیم ـ فریم در نشانه‌گذار و آشکارساز

شکل ۲ نیم- فریم‌های بکار رفته در نشانه‌گذار و آشکارساز را در حالتی که ماکزیمم انتقال ($\frac{576}{2}=288$) بین آنها وجود دارد نشان می‌دهد. $ix_n(i)$ و $x_n(i)$ سیگنال‌های MP3 و PCM نشانه‌گذار در نیم- فریم iام و $iy_n(i)$ و $y_n(i)$ سیگنال‌های متناظر در نیم- فریم iام آشکارساز می‌باشند. $WB_{k,m}$ اشتراک باند نشانه‌گذاری kام موجود در نیم- فریم i با باند بحرانی mام می‌باشد که با بردار $\Delta^E(i)$ شامل عناصر هم‌علامت تغییر یافته است.

این تغییرات محدود طیف کوانتیزه در حوزه فرکانس به تغییر کل نمونه‌های زمانی x_n واقع در همان پنجره منجر می‌شود. تغییرات نمونه‌های زمانی x_n که در واقع تبدیل معکوس فرکانس- زمان MP3 بردار $\Delta^E(i)$ می‌باشند در نمونه‌های زمانی پنجره‌های i-1 و iام y_n ظاهر می‌شوند. همانطور که شکل نشان می‌دهد این تغییرات در بخش انتهایی نیم- فریم i-1ام و بخش ابتدایی نیم- فریم iام صورت می‌گیرد. با تبدیل مستقیم زمان- فرکانس MP3 نیم- فریم‌های $iy_n(i-1)$ و $iy_n(i)$ نمونه‌های واقع در محدوده طیفی $WB_{k,m}$ در این دو نیم- فریم با مقادیر $\Delta^D(i-1)$ و $\Delta^D(i)$ افزایش یا کاهش می‌یابند (بسته به علامت $\Delta^E(i)$). نکته مهم اینجاست که تغییرات فریم‌های iy_n صرفاً در محدوده‌های مشخص $WB_{k,m}$ نبوده و خطوط فرکانسی مجاور را نیز در بر می‌گیرد. چرا که تغییر مؤلفه‌های طیفی $WB_{k,m}$ در نیم- فریم‌های زمانی $iy_n(i-1)$ و $iy_n(i)$ به‌صورت موضعی و نه در کل طول دو نیم- فریم صورت گرفته است. در واقع هر چقدر که همپوشانی هر یک از دو نیم- فریم $iy_n(i-1)$ و $iy_n(i)$ با نیم- فریم $ix_n(i)$ کمتر می‌گردد خاصیت پخش فرکانسی تغییرات حول $WB_{k,m}$ در آن نیم- فریم بیشتر می‌گردد. همچنین $\Delta^D(\ )$ که به مفهوم تغییرات محدودهٔ $WB_{k,m}$ است برای آن نیم- فریم نیز کاهش می‌یابد. در مقابل با افزایش همپوشانی بین هر یک از دو نیم- فریم $iy_n(i-1)$ و $iy_n(i)$ با نیم- فریم $ix_n(i)$ موجب تیزتر شدن محدودهٔ تغییرات حول $WB_{k,m}$ و در نتیجه افزایش $\Delta^D(\ )$ می‌گردد.

در اینجا به ارتباط کمی Δ^E با Δ^Dها می‌پردازیم. با فرض مثبت بودن عناصر Δ^E انرژی افزوده شده به بازهٔ $WB_{k,m}$ در نیم- فریم $ix(i)$ باید برابر یا بزرگتر از انرژی افزوده شده به فریم‌های $iy_n(i-1)$ و $iy_n(i)$ باشد (به علت خاصیت پخشی تغییرات). پس داریم:

$$\left[\Delta_m^D(i-1)\right]^2+\left[\Delta_m^D(i)\right]^2\le\left[\Delta_m^E(i)\right]^2 \qquad (۱)$$

که در آن $[.]^2$ به مفهوم مجموع مربعات کل عناصر بردار می‌باشد. با گرفتن مجموع دو طرف نابرابری روی کلید ۲۱ زیر بخش باند نشانه‌گذاری، این نابرابری را برای کلیه عناصر واقع در باند نشانه‌گذاری خواهیم داشت:

$$\left[\Delta^D(i-1)\right]^2+\left[\Delta^D(i)\right]^2\le\left[\Delta^E(i)\right]^2 \qquad (۲)$$

برابری در حالتی صورت می‌گیرد که به علت تطابق کامل پنجره‌های آشکارساز با نشانه‌گذار $\Delta^D(i-1)$ صفر شده و $\Delta^D(i)$ برابر $\Delta^E(i)$ گردد. از طرفی بیشترین تفاضل دو طرف نابرابری در هنگام انتقال ماکزیمم بین پنجره‌ها (به میزان $\frac{576}{2}=288$) رخ می‌دهد. بررسی‌ها نشان دادند که در این حالت انرژی منتقل شده به باند نشانه‌گذاری در فریم‌های $iy(\ )$ برابر انرژی منتقل شده به خطوط فرکانسی مجاور به علت خاصیت پخشی تغییرات می‌باشد پس داریم:

$$2\times\left[\Delta^D(i)\right]^2+\left[\Delta^D(i)\right]^2\approx\left[\Delta^E(i)\right]^2$$

و در نتیجه:

$$\Delta^D(i-1)+\Delta^D(i)=2\times\left[\Delta^D(i)\right]>\left[\Delta^E(i)\right]\quad\left(=\sqrt{3}\left[\Delta^D(i)\right]\right) \qquad (۳)$$

$[.]$ به‌مفهوم مجموع عناصر بردار می‌باشد. بنابراین در بدترین حالت نابرابری ۲ به این نتیجه رسیدیم که مجموع تغییرات صورت گرفته در نیم- فریم‌های مجاور آشکارساز از تغییر نیم- فریم متناظر آنها در نشانه‌گذار بیشتر است. در حالت کلی خواهیم داشت:

$$\left[\Delta^D(i-1)\right]+\left[\Delta^D(i)\right]\ge\left[\Delta^E(i)\right] \qquad (۴)$$

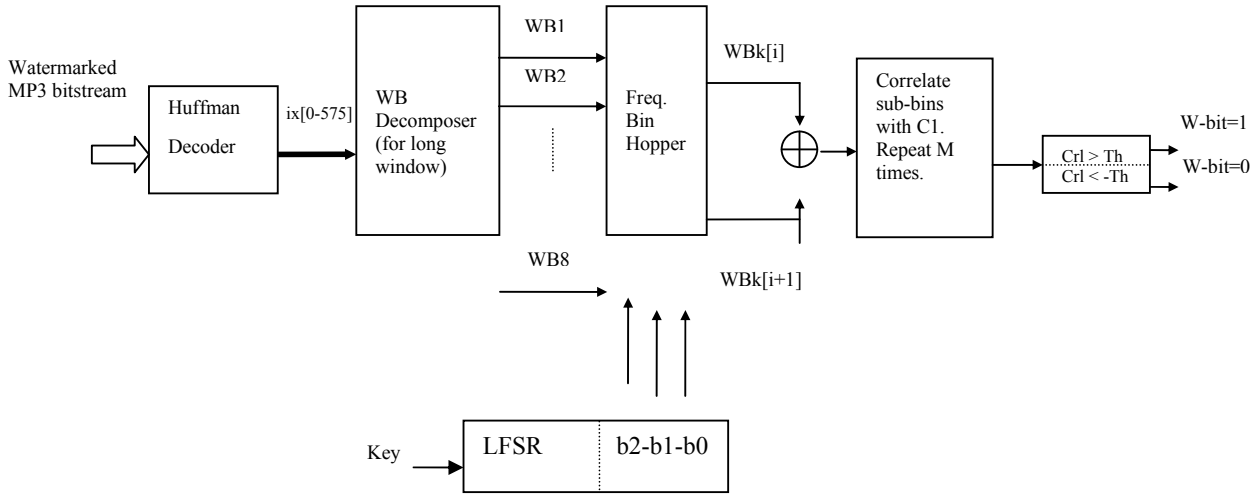
توجه شود که این رابطه بمعنای داشتن بهره بهتر در هنگام عدم تطابق نیم- فریم‌ها نیست. در واقع از آنجا که آشکارساز به مجموع‌گیری باندهای نشانه‌گذاری فریم‌های مجاور پرداخته است مقدار نویز ناشی از تداخل سیگنال اصلی را بیشتر نموده است.

۴-۲- الگوریتم آشکارساز نشانه

شکل ۳ بلاک دیاگرام آشکارساز را نشان می‌دهد. ابتدا رشته- بیت ورودی همانند نشانه‌گذار از حالت فشرده هافمن خارج شده و بردار ۵۷۶ نمونه‌ای ضرایب کوانتیزه طیفی ix به بلاک بعدی اعمال می‌شود. بلاک بعد ix را به باندهای نشانه‌گذار WB_1 تا WB_8 تجزیه می‌کند. یکی از این باندها باید برای هر دو نیم- فریم مجاور انتخاب شود. طبیعی است که آشکارساز باید از همان الگوی انتخاب تصادفی WBiها که در نشانگذار توسط یک LFSR با کلید K انجام می‌شد پیروی کند. برای این منظور آشکارساز از همان LFSR و واحد انتخاب‌گر باند نشانه بکار رفته در نشانه‌گذار استفاده می‌کند.

پس از اینکه آشکارساز نمونه‌های دو باند $WB_k(i-1)$ و $WB_k(i)$ را از فریم‌های i-1 و i بدست آورد به استخراج دو بردار ۲۱ عنصری از ۲۱ زیر بخش بکار رفته در هر باند نشانه به‌صورت زیر می‌پردازد.

$$A_x^{(i)}(k,m)=\frac{\left|WB_{k,m}(i)\right|}{\left\|WB_{k,m}(i)\right\|} \qquad (۵)$$



شکل ۳- بلاک دیاگرام آشکارساز نشانه

همانطورکه دیده می‌شود $A_x(k,m)$ به متوسط‌گیری اشتراک باند نشانه kام با هر یک از باندهای بحرانی m می‌پردازد. جهت مجموع‌گیری از تغییرات مطابق بحث بخش پیش، آشکارساز بردارهای $\vec{A}_x k^{(i-1)}$ و $\vec{A}_x k^{(i)}$ را با هم جمع می‌کند و بردار $\vec{B}_x k^{(i)}$ را بدست می‌آورد.

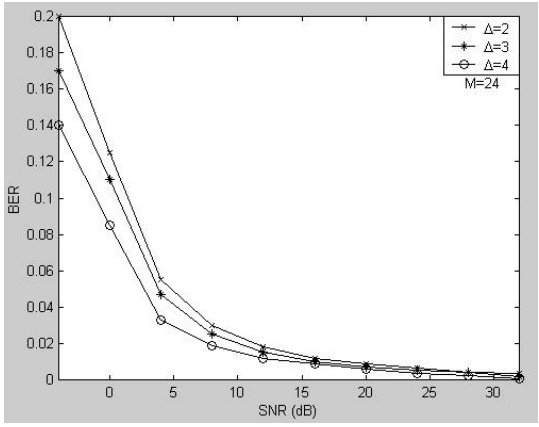
در مرحله بعد بردار $\vec{B}_x k^{(i)}$ در بردار ۲۱ بیتی کد C1 متشکل از عناصر $\pm\Delta$ ضرب شده و مجموع مقادیر حاصلضرب روی هر M نیم- فریم که آنرا Corr می‌نامیم تعیین می‌گردد. M پارامتر کدینگ تکرار اعمال شده در نشانه‌گذار می‌باشد.

طی آخرین مرحله مقدار Corr با آستانه‌های Th $(Th > 0)$ و Th- مقایسه در صورت بزرگتر از Th بودن مقدار بیت 1 و در صورت کوچکتر از Th- شدن مقدار بیت 0 به‌عنوان بیت نشانه قرار گرفته در M نیم- فریم آشکار می‌گردد. مقادیر آستانه‌های مثبت و منفی جهت داشتن کمترین احتمال خطا برابر $\mathrm{Th} = \pm\frac{\alpha.21.M.\Delta^2}{2}$ انتخاب می‌شوند.

۵- نتایج پیاده‌سازی

در اینجا به تشریح نتایج پیاده‌سازی الگوریتم‌های طراحی شده برای نشانه‌گذاری و بازیابی اطلاعات در (از) رشته- بیت MP3 می‌پردازیم. ۵ فایل نمونهٔ MP3 از ۵ ژانر مختلف که به صورت استریو کد شده بودند انتخاب شده و با پیام‌های ۴۰۰ بیتی (۲۰۰ بیت در هرکانال) نشانه‌گذاری شدند. سپس رشته- بیت‌های نشانه‌گذاری شده دکود شده و توسط یک نرم‌افزار ویرایشگر صدا تحت پردازش‌های مختلفی قرار گرفته و دوباره فشرده شدند. سیگنال‌های فشردهٔ حاصله به آشکارساز اعمال شدند تا ۴۰۰ بیت نشانه از هر یک بازیابی شود. شکل ۴ نتیجهٔ اعمال نویز گوسی سفید با توان‌های مختلف (حتی بیش از توان سیگنال) را در سه حالت Δ نشان می‌دهد. در حالت $\Delta = 3$ با افت توان نویز در انتهای نمودار مقدار خطا به حد تقریبی ۰/۰۰۲ نزدیک می‌شود. در واقع با توجه به استفاده از دو مدولاسیون طیف گسترده (DSSS وFHSS) در سیستم انتظار هم می‌رفت که الگوریتم پایداری بالایی در برابر نویز سفید داشته باشد.

جدول ۱، خطای متوسط رخ داده در آشکارسازی ۴۰۰ بیت بازیابی شده برای ۵ فایل را بر حسب نوع پردازش خاص اعمالی به سیگنال نشان می‌دهد. میزان خطا در حالت بدون پردازش سیگنال PCM برابر ۰،۰۰۲ شد. روی‌هم‌رفته مقادیر جدول حاکی از پایداری خوب سیستم نشانه‌گذاری طراحی شده می‌باشد.



شکل ۴- نمودار خطا بر حسب شدت نویز گوسی سفید

جدول ۱- خطای متوسط آشکارسازی بر حسب نوع پردازش اعمالی

	AWGN (PSD_n=PSD_{sig})	LPE, F_{cut}=4khz	Equalizer, fc_1=1khz, fc_2=7khz, G_p,G_s=-6db	Requa-ntization, to 8 bit	MP3 Reencoding to 64 Kbp
BER	0.11	0.105	0.08	0.045	0.007

۶- نتیجه‌گیری

در این مقاله روشی کارا جهت جایگذاری مستقیم اطلاعات در رشته- بیت MP3 مطرح گردید. ویژگی‌های بارز روش پیشنهادی مقاله در مقایسه با راهکارهای مشابه، امکان بازیابی مستقیم اطلاعات نشانه‌گذاری شده از سیگنال فشرده و عدم حساسیت در مقابل همزمان نبودن فریم‌های MP3 در دو وضعیت جایگذاری و بازیابی داده‌ها می‌باشند. همچنین نقطه قوت دیگر سیستم حاضر بار پردازشی بسیار اندک آن برای سرور تحویل دهندهٔ فایل می‌باشد به‌طوریکه امکان نشانه‌گذاری موازی تعداد زیادی فایل MP3 توسط سرور فراهم می‌گردد. نتایج بررسی مقاومت سیستم در برابر پردازش‌ها و حملات مختلف اعمالی به آن حاکی از پایداری رضایت‌بخش داده‌های نشانه‌گذاری شده با سیستم طراحی شده می‌باشند.

مراجع

[1] J. Herre, and C. Neubauer, "Audio Watermarking in the Bitstream Domain," *Watermarking Workshop*, 1999.

[2] B. Girod, and F. Hartung, "Digital Watermarking of MPEG-2 Coded Video in the Bitstream Domain," *ICASSP-97*, Vol. 4, pp. 2621-2624, Apr. 1997.

[3] M. Swanson, B. Zhu, and A. Tewfik, "Current State of the Art Challenges and Future Directions for Audio Watermarking," *ICMCS-99*, pp. 19-24, 1999.

[4] D. Kirovski, and H. Malvar, "Robust Spread-Spectrum AudioWatermarking," *ICASSP'2001*, Vol. 3, pp. 1345-1348, 2001.

[5] M. Arnold, "Audio Watermarking: Features, Applications and Algorithms," *IEEE ICMCS'99*, Vol. 2, pp. 1013-1016, 1999.

[6] D. Pan, "A Tutorial on MPEG/audio Compression," *IEEE Multi Media Mag.*, pp. 60-74, 1995.

[7] ISO/IEC, JTC1/SC29/WG11 MPEG, "Information Technology – Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to 1.5 Mbit/s – part 3: Audio," IS11172-3, 1992 ("MPEG-1").

امیرمنصور پزشک در سال ۱۳۳۶ در شهر تهران متولد شد. تحصیلات تا مقطع دیپلم را در همان شهر سپری و دیپلم متوسطه خود را در سال ۱۳۵۳ دریافت کرد. وی تحصیلات خود در مقطع کارشناسی را در رشته مهندسی برق ـ الکترونیک در دانشگاه صنعتی امیـرکبیر (سال ۱۳۵۷)، کارشناسی ارشد را در رشتـه سیستم انفورماتیک در دانشگاه پیروماری کوری پاریس (سال ۱۳۶۰) و دورهٔ دکترای خود را در رشته میکروالکترونیک و میکروکامپیوتر در همین دانشگاه به پایان رسانید . نامبرده از سال ۱۳۶۷ در سمت عضو هیأت علمی دانشکده مهندسی برق دانشگاه صنعتی شریف به تدریس و تحقیق مشغول می‌باشد. ایشان علاوه بر تدریس، راهنمایی دهها پروژه کارشناسی و کارشناسی ارشد و نیز هدایت تعداد زیادی پروژه‌های صنعتی را بر عهده داشته است. از دیگر فعالیت‌های ایشان راه‌اندازی آزمایشگاه‌های مدار مجتمع، رادار و جنگال در پژوهشکده الکترونیک و آزمایشگاه میکروپروسسور در دانشکده مهندسی برق دانشگاه صنعتی شریف می‌باشد.

آدرس پست‌الکترونیکی ایشان عبارت است از:

pezeshk@sharif.edu

کمال پوررضایی در سال ۱۳۵۳ در شهر میبد متولد شد. تحصیلات تا مقطع دیپلم را در همان شهر سپری و دیپلم متوسطه خود را در سال ۱۳۷۱ دریافت کرد. وی تحصیلات خود در مقطع کارشناسی را در رشته مهندسی برق - الکترونیک در دانشگاه صنعتی امیرکبیر (سال ۱۳۷۵) و کارشناسی ارشد را در رشته مخابرات - رمز در دانشگاه صنعتی شریف (سال ۱۳۸۳) به پایان رسانید. نامبرده از سال ۱۳۸۳در سمت مدیر بخش تحقیق و توسعه شرکت علم و صنعت نوید به فعالیت مشغول است. زمینه‌های تخصصی مورد علاقه ایشان پردازش سیگنال صدا و شناسایی الگو می‌باشد.

آدرس پست‌الکترونیکی ایشان عبارت است از:

kamalporeza@yahoo.com

---

[1] Digital Pirates
[2] Intellectual Property Rights (IPR)
[3] Watermarking
[4] Copyright
[5] Real-Time
[6] Bit-Stream
[7] Compressed (Bit-Stream) Domain
[8] Granule
[9] Just Noticeable Distortion