هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی

دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

یک الگوریتم نهان‌نگاری صوتی جدید براساس خوشه‌بندی نمونه ها

سمیه مهدوی جعفری [۱]، سعید رضا صید نژاد [۲]، سعید سریزدی [۳] و وحید جمشیدی [۴]

دانشگاه شهید باهنر کرمان

s.mahdavi.j@gmail.com

کرمان، دانشگاه شهید باهنر کرمان ، گروه مهندسی برق ۲و۳

چکیده

در این مقاله یک روش نهان نگاری صوتی مقاوم در مقابل حملات برش و همزمانی ارائه شده است . تعدادی نواحی مناسب از سیگنال صوت بر اساس خواص حوزه زمانی آن برای نهفتن بیت های واترمارک انتخاب می شوند. این نواحی انتخاب شده به حوزه تبدیل منتقل می شوند. با استفاده از یک کلید رمز و یک الگوریتم خوشه بندی تعدادی نمونه تصادفی از هر ناحیه در حوزه تبدیل انتخاب می شوند. مؤلفه های انتخاب شده در حوزه تبدیل به نمونه های نظیر در حوزه زمان نگاشته می شوند. دامنه نمونه های انتخاب شده در حوزه زمان جهت نهفتن بیت پیام توسط یک الگوریتم مبتنی بر تکرار تغییر می یابند. با استفاده از خواص پوشش زمانی سیستم شنیداری انسان (HAS) نا محسوس بودن واترمارک نهفته شده تضمین شده است. نتایج آزمایشات انجام شده نشانگر مقاومت الگوریتم پیشنهادی در برابر حملات متداول در زمینه نهان نگاری صوتی می باشد.

واژه های کلیدی

نهان نگاری صوتی، سیستم شنیداری انسان، الگوریتم خوشه بندی.

۱- مقدمه

الگوریتم‌های نهان نگاری صوتی عموماً به دو گروه حوزه زمان و حوزه تبدیل تقسیم بندی می شوند. الگوریتم های حوزه تبدیل نسبت به الگوریتم های حوزه زمان در مقابل حملات مقاوم تر می باشند، ولی مقاومت آنها در سیگنالهایی که تعداد مؤلفه های حوزه تبدیلشان بسیار کم می باشد رضایت بخش نیست [۱]. در ضمن این الگوریتم ها نسبت به الگوریتم های حوزه زمان پیچیده تر و زمان بر تر می باشند.

روشهای حوزه زمان عموماً از دو استراتژی استفاده می‌کنند: ۱- اضافه کردن نویز نا محسوس (سیگنال واترمارک) که پیام را حمل می کند، به سیگنال میزبان (روش‌های طیف گسترده[۱] [۲]، پنهان کردن تأخیر[۲] [۳،۴]و غیره[۷-۵]) ۲- دستکاری کردن نمونه‌های سیگنال به منظور نهفتن بیت واترمارک (روش رمزگذاری بیت کم ارزش[۳] [۸]، روش چندی سازی[۴] [۹] و غیره[۱۰،۱۱]). الگوریتم‌های گروه دوم نمونه‌ها را یا بصورت انفرادی و یا بصورت گروهی [GOS] تغییر می‌دهند. الگوریتم هایی که نمونه‌ها را بصورت انفرادی تغییر می‌دهند ظرفیت نهانگی بالایی (یک نمونه برای نهان کردن یک بیت واتر مارک) ارائه می‌دهند، اما در برابر حملات بویژه نویز به شدت آسیب پذیر می‌باشند. در عوض الگوریتم‌هایی که نمونه‌ها را بصورت گروهی تغییر می‌دهند (بطور مثال[۱۱]) معمولاً مقاومت بیشتری در برابر حملات نشان می‌دهند. در [۱۱] تقسیم‌بندی سیگنال صوت از محل اولین نمونه آن اتفاق می‌افتد. این امر الگوریتم را نسبت به همزمانی گیرنده و فرستنده حساس می‌کند. علاوه بر این عملکرد

[1] Spread Spectrum

[2] Echo Hiding

[3] LSB Coding

[4] Quantization

آن در برابر حمله برش تضعیف خواهد شد. گرچه این مسائل با بکار گیری کدهای همزمانی و کدهای تصحیح خطا برطرف می شود، اما این مسئله، الگوریتم را بسیار پیچیده و زمان بر می کند. روش پیشنهادی در این مقاله سعی بر نهفتن پیام در نواحی خاصی از سیگنال میزبان دارد که قابل حذف شدن و یا تغییر یافتن (تحت تأثیر حملات) نباشند. بعلاوه جهت حل مسئله همزمانی بجای استفاده از تعدادی نمونه متوالی از سیگنال میزبان، ما از تعدادی نمونه تصادفی و پخش شده حول سیگنال میزبان، برای نهفتن پیام استفاده می کنیم.

۲- نهفتن واتر مارک!

مراحل کلیدی فرآیند نهفتن واتر مارک در سیگنال صوت در الگوریتم پیشنهادی به شرح زیر می باشند:

انتخاب نواحی مناسب

انتخاب تعدادی از نمونه های هر ناحیه به صورت تصادفی

نهفتن واتر مارک با تغییر دادن دامنه نمونه های انتخاب شده در مرحله قبل.

۲-۱-انتخاب نواحی مناسب

دراکثر الگوریتم های حوزه زمان سیگنال میزبان از ابتدا (از محل اولین نمونه) به پنجره هایی با طول مساوی تقسیم بندی می شود تا در هر پنجره یک بیت نهفته شود. در گیرنده نیز برای آشکارسازی پیام این پنجره ها باز سازی می شوند . حال اگر بنا به دلایلی همزمانی بین گیرنده و فرستنده بهم بخورد عملکرد این الگوریتمها تضعیف خواهد شد. در الگوریتم پیشنهادی بیت های پیام در نواحی خاصی از سیگنال نهفته می شوند تا در صورت عدم همزمانی گیرنده و فرستنده، آشکار سازی پیام دچار مشکل نگردد. نواحی مناسب بر اساس دو ویژگی خاص از سیگنال ابتدایی در حوزه زمان یافت می شوند:

انرژی پیکها

فاصله بین دو پیک مناسب

تمامی حملات ناگزیر از حفظ پیکهای پر انرژی می باشند. زیرا حذف و یا دست کاری آنها سبب بروز نویز شنیداری و یا کاهش کیفیت سیگنال صوت می گردد. لذا این پیکها به عنوان نشانه همزمانی به کار می روند. فضای بین این پیکها به عنوان محلی مناسب برای نهفتن بیت پیام در نظر گرفته می شوند. لیکن تنها نواحی انتخاب می شوند که شامل تعداد کافی نمونه باشند تا بدون ایجاد پیچیدگی محاسباتی، دقت الگوریتم در برابر حملات تضمین گردد.

۲-۱-۱-انرژی پیکها

پیکهای پر انرژی سیگنال صوت ، $X(n)$ ، طی سه مرحله یافت می شوند:

۱. یافتن مقدار قدر مطلق سیگنال صوت

$$X_a(n) = |X(n)| \qquad (۱)$$

۲. نرمالیزه کردن سیگنال $X_a(n)$

$$X_n(n) = \frac{1}{\max(X_a(n))} \times X_a(n) \qquad (۲)$$

با اجرای این مرحله تمامی مقادیر نمونه ها بین صفر و یک قرار می گیرند.

۳. به توان رسانیدن سیگنال منتج

$$X_p(n) = X_n^N(n) \qquad (۳)$$

که در آن N یک عدد صحیح مثبت می باشد. با اجرای این مرحله تفاوت بین پیکهای پر انرژی و نمونه های کم انرژی بیشتر شده و پیکها واضحتر می گردند. N های بزرگ این تفاوت را بیشتر و در نتیجه الگوریتم را در برابر حملات مقاومتر می سازد در حالیکه N کوچکتر تعداد نواحی بیشتر ودر نتیجه ظرفیت نهانگی بیشتری ایجاد می کند. بنابراین یک تعامل بین مقاومت الگوریتم پیشنهادی و ظرفیت نهانگی وجود دارد.

۴. انتخاب پیکهایی که اندازه شان α٪ ازاندازه بزرگترین پیک سیگنال باشد.

مقدار α بر تعداد نواحی انتخابی تأثیر دارد. پس از بررسی نحوه عملکرد سیستم در مقادیر مختلف α ، مقدار۰/۱۴ برای آن در نظر گرفته شد.

در انتهای این مرحله کلیه پیکهای پر انرژی انتخاب و فضای بین هر دو پیک متوالی به عنوان یک کاندید ناحیه مناسب برای نهفتن بیت پیام شناخته می شود. از بین این کاندیدها تنها تعدادمحدودی، در مرحله بعد به عنوان ناحیه مناسب انتخاب می شوند.

۲-۱-۲- فاصله بین دو پیک

هر ناحیه بایستی تعداد نمونه کافی جهت نهفتن یک بیت داشته باشد. تعداد نمونه ها در هر ناحیه نمی تواند از یک حد مشخص تجاوز نماید، زیرا در غیر این صورت الگوریتم خوشه بندی زمانبر خواهد شد. ما تعداد ۱۰۰ نمونه را به عنوان حد پایین انتخاب می کنیم و برای انتخاب حد بالا ما حمله برش[۱] را در نظر می گیریم. برش بیش از ۵۰۰الی۶۰۰ نمونه متوالی سبب بروز نویز شنیداری می گردد. بنابراین اگر تعداد ۷۰۰=۱۰۰+۶۰۰ نمونه به عنوان حد بالای تعداد نمونه های یک ناحیه انتخاب شود، الگوریتم حمله برش را تحمل خواهد کرد. پس از انتخاب نواحی مناسب، پیکهای مرزی به عنوان پرچم شناخته می شوند.

[۱] Cropping

۲-۲- انتخاب تصادفی تعدادی از نمونه های هر پنجره

به دلیل ماهیت مقاومتر حوزه تبدیل نسبت به حوزه زمان، انتخاب نمونه ها در حوزه تبدیل صورت می پذیرد. به این منظور به دامنه نمونه های هر پنجره تبدیل فوریه اعمال می گردد. سپس اندازه مؤلفه های فوریه هر پنجره به یک الگوریتم خوشه بند اعمال می گردد تا گروهی از نمونه ها به صورت تصادفی انتخاب شوند. انتخاب تصادفی نمونه هایی که بایستی مطابق با بیت پیام تغییر یابند ویا به عبارتی پخش بودن آنها در طول پنجره، سبب مقاومت الگوریتم در برابر حملات و همچنین نا محسوس بودن تغییرات اعمالی می گردد. زیرا هر نمونه تغییر یافته در همسایگی حداقل یک نمونه دست نخورده قرار می گیرد و طبق خواص پوشش زمانی[۲] سیستم شنیداری انسان (HAS)[3] توسط آنها پوشیده و نا محسوس می شود.

انتخاب تصادفی نمونه ها بر اساس یک الگوریتم خوشه بندی[۴] و یک کلید رمز صورت می پذیرد. خوشه بندی یک نمونه از الگوریتم های طبقه بندی بدون نظارت می باشد. ورودی این الگوریتم تعدادی داده بدون برچسب می باشد. این الگوریتم داده ها را بر اساس فاصله بینشان طبقه بندی می کند. بنابراین داده های نزدیک به هم متعلق به یک خوشه خواهند شد. برای رسیدن به این منظور از تکنیکها آماری استفاده می شود که متداولترین آنها که اینجا مورد استفاده قرار می گیرد تکنیک K-means می باشد[۱۲].

انتخاب تصادفی نمونه ها در چند مرحله صورت می پذیرد:

۱. محاسبه اندازه ضرایب فوریه پنجره
۲. انتخاب K نمونه تصادفی از بین داده های مرحله ۱به عنوان مراکز خوشه $Z_i(old)$
۳. محاسبه فاصله مؤ لفه فوریه نمونه ها تا مراکز خوشه انتخاب شده و نسبت دادن هر مؤ لفه به نزدیکترین مرکز و ایجاد K خوشه
۴. به روز شدن مقدار مراکز خوشه طبق فرمول

$$Z_i = \frac{1}{N_i} \times \sum_{X_i \in C_i} X_i \qquad (۴)$$

که در آن:
N_i مقدار داده متعلق به خوشه i ام
X_i داده متعلق به خوشه i ام
و C_i خوشه i ام می باشد.

۵. رفتن به مرحله ۲ اگر $Zi(new) - Zi(old) > \varepsilon$ و پایان الگوریتم در غیر اینصورت.

در روش پیشنهادی مقدارK برابر ۳ انتخاب شده است. لذا ۳ خوشه در هر پنجره ایجاد می شود. یک خوشه برای تغییر یافتن، اگر i امین بیت کلید رمز "۱" باشد، یک خوشه برای تغییر یافتن ، اگر i امین بیت کلید رمز "۰" باشد و یک خوشه به عنوان باند محافظ مورد استفاده قرار می گیرند تا حتی در صورت وجود نویزقوی، نمونه های متعلق به خوشه اول وآخر با یکدیگر تداخل پیدا نکنند.

K های بزرگ ضمن اینکه الگوریتم خوشه بند را پیچیده و زمان بر می کنند، خوشه هایی ایجاد می کنند که از فاصله کافی بر خوردار نبوده و دقت روش در برابر حملات را کاهش می دهند. انتخاب عدد۲ برای K نیز سبب می شود تا تحت تأثیر نویز کانال انتقال اعضای دو خوشه در گیرنده با یکدیگر مخلوط شوند و آشکارسازی پیام به درستی صورت نپذیرد.

پس از همگرا شدن الگوریتم خوشه بندی، هر مؤلفه به یک خوشه متعلق خواهد شد. حال مراکز این خوشه ها بر اساس مقدارشان به ترتیب از ۱ تا K مرتب می شوند. اعضای هر خوشه ایندکس آن خوشه را که عددی از۱ تا K می باشد را می پذیرند. حال محل مؤلفه های متعلق به خوشه کوچکتر و محل مؤلفه های متعلق به خوشه بزرگتر در نظر گرفته می شوند و از مؤلفه های خوشه میانی (مؤلفه های باند محافظ) صرفنظر می شود. این مکانها مستقیماً به قدر مطلق نمونه ها در حوزه زمان اعمال می گردند. شکل۱ نحوه اجرای این فرآیند را روی چند نمونه فرضی از سیگنال را نشان می دهد.

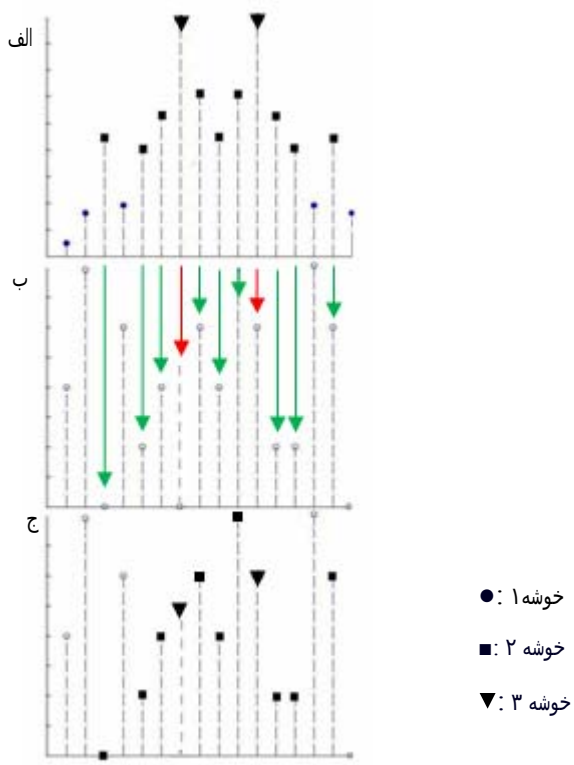
لذا در حوزه زمان دو گروه نمونه بدست می آیند که بر اساس بیت پیام، در فرآیند اصلاح و تغییر (مرحله بعد) شرکت می کنند. یک کلید رمز مشخص می کند کدام گروه از نمونه ها به مرحله بعد بروند. اصطلاحاً اگر بیت i ام کلید رمز صفر باشد نمونه های متعلق به خوشه کوچکتر و اگر بیت i ام کلید رمز یک باشد نمونه های متعلق به خوشه بزرگتر انتخاب وجهت تغییر یافتن به مرحله بعد می روند.

۲-۳- نهفتن واتر مارک (اعمال تغییرات)

مطابق با موقعیت فیزیکی، نمونه ها ی انتخاب شده در هر پنجره، به دو قسمت تقسیم می شود: نمونه های سمت چپ که قبل از نقطه وسط فیزیکی پنجره واقع شده اند و نمونه های سمت راست که بعد از آن قرار دارند.

اگرi امین بیت پیام صفر باشد مجموع نمونه های سمت چپ بایستی از مجموع نمونه های سمت راست بیشتر باشد. اگر شرط برقرار باشد هیچ عملیات خاصی انجام نمی شود، اما اگر شرط برقرار نباشد تک تک نمونه های سمت راست و چپ بایستی تا

[2] Time Masking
[3] Human Auditory System
[4] clustering



شکل۱ : فرآیند اعمال خوشه بندی الف) اندازه مؤلفه های فوریه چند نمونه فرضی از سیگنال و نتیجه اعمال خوشه بندی روی آنها ب) قدر مطلق نمونه های فرضی سیگنال صوت در حوزه زمان ج) اعمال نتایج خوشه بندی (ایندکس های بدست آمده) در مرحله (الف) بر روی نمونهای فرضی سیگنال در مرحله (ب) و یافتن دو گروه تصادفی از نمونه ها

برقرار شدن شرط تغییر یابند.از طرف دیگر اگرi امین بیت پیام یک باشد مجموع نمونه های سمت راست بایستی از مجموع نمونه های سمت چپ بیشتر باشد. اگر شرط برقرار باشد هیچ عملیات خاصی انجام نمی شود، اما اگر شرط برقرار نباشد تک تک نمونه های سمت راست و چپ بایستی تا برقرار شدن شرط تغییر یابند.

اعمال تغییرات به نمونه ها توسط یک الگوریتم مبتنی برتکرار[5] اجرا می شود وفاکتوراصلاح[6] وابسته به خود سیگنال تعریف می شود.

به این منظور در تکرارj ام مجموع نمونه های سمت چپ و مجموع نمونه های سمت راست محاسبه می شوند. اگر شرط برقرار باشد الگوریتم خاتمه می یابد و در غیر اینصورت فرآیند اصلاح تکرار می شود. برای اصلاح مقادیر نمونه های انتخاب شده در تکرار j ام، از نمونه های تضعیف شده تکرار (j-1) ام استفاده می شود. در واقعβ ، فاکتور تضعیف، در مقادیر نمونه های انتخاب شده در تکرار (j-1) ام ضرب می شود (فاکتور اصلاح وابسته به خود سیگنال) و با مقادیر نمونه های انتخاب شده در تکرار (j-1) ام جمع می شود، تا هر نمونه متناسب با مقدار سابق خود تغییر کند و مقادیر جدید نمونه ها در تکرار j ام بدست آید. به طور خلاصه:

اگـر بیـت i ام پیـام صـفر باشـد و قـرار باشـد اصـلاحات و تغییرات صورت پذیرد آنگاه:

*نمونه های سمت چپ در تکرار jام= نمونـه هـای سـمت چـپ در تکرار(j-1)ام+ نمونه های سمت چپ در تکرار(j-1)ام*β*

*نمونه های سمت راست در تکرار jام= نمونه های سمت راسـت در تکرار(j-1)ام- نمونه های سمت راست در تکرار(j-1)ام*β*

برعکس اگر بیت i ام پیام یک باشد و قرار باشد اصلاحات و تغییرات صورت پذیرد آنگاه:

*نمونه های سمت چپ در تکرار jام= نمونـه هـای سـمت چـپ در تکرار(j-1)ام- نمونه های سمت چپ در تکرار(j-1)ام*β*

*نمونه های سمت راست در تکرار jام= نمونه های سمت راسـت در تکرار(j-1)ام+ نمونه های سمت راست در تکرار(j-1)ام*β*

فرآیند فوق آنقدر تکرار می شود تا شرط برقرار شود.

مقدار β سرعت همگرایی الگوریتم فوق را مشخص می کند. β هر چه بزرگتر باشد سرعت الگوریتم بالاتر خواهد بود. در حالیکه β کوچکتر ، نامحسوس بودن تغییرات اعمالی را تضمین می کند. زیرا این امکان فراهم می آید که در گامهای کوچکتر شرط چک شود و به محض برآورده شدن شرط، الگوریتم مبتنی بر تکرار خاتمه می یابد.

از آنجا که برای تغییر نمونه های یک پنجره از شکل خود سیگنال پنجره استفاده می شود، میزان تغییر هر نمونه بر اساس مقدار خود آن نمونه می باشد. این تغییر وفقی و جزئی، نا محسوس بودن تغییرات اعمال شده را تضمین می نماید.

۳- فرآیند آشکار سازی!

از آنجا که روش پیشنهادی از جمله روشهای کور می باشد در فرآیند آشکار سازی به سیگنال ابتدایی نیاز نمی باشد.

با تکرار مراحل ۱و۲ فرآیند نهانگی و استفاده از کلید رمز، پرچمها، نواحی مناسب (پنجره ها) و نمونه های تصادفی انتخاب شده در هر پنجره استخراج می شوند. در هر پنجره نمونه های سمت چپ و سمت راست بر اساس موقعیت آنها نسبت به نقطه وسط پنجره مشخص می شوند. سپس مجموع نمونه های سمت چپ و مجموع نمونه های سمت راست در هر پنجره محاسبه می شوند. قانون تصمیم گیری در مورد بیت نهفته شده در هر پنجره (b) به شرح زیر می باشد:

b=0 اگر مجموع نمونه های سمت چپ از مجموع نمونه های سمت راست بیشتر باشد

b=1 اگر مجموع نمونه های سمت راست از مجموع نمونه های سمت چپ بیشتر باشد

[5] Iterative algorithm

[6] Modification Factor

۴- نتایج آزمایشهای انجام شده!

برای بررسی عملکرد سیستم های پیشنهادی یک تست ناشنوائی وچند تست مقاومت صورت پذیرفت. ما الگوریتم پیشنهادی را با۱۲ کلیپ موسیقی۲۰ ثانیه ای مختلف از انواع پاپ[7] ، راک[8] ، پیانو[9] ، نی(تک نوازی)[10] ، صحبت[11] (زن و مرد) وصوت با بازه های طولانی سکوت (از هر نوع ۲ موسیقی) تست کردیم. اگرچه مقالات پیشین هریک تعداد اندکی از این اصوات را مورد آزمایش قرار دادند، ولی ما در این مقاله مجموعه ای از کلیه این اصوات گردآوری کرده ومورد آزمایش قرار دادیم. جهت تطابق با کیفیت اصوات موجود در CD های رایج، در این کلیپها فرکانس نمونه برداری۴۴/۱کیلو هرتز و هر نمونه با ۱۶ بیت نمایش داده می شود.

۴-۱-تست شنیداری!

ارزیابی کیفیت سیگنال صوت حاوی واترمارک نسبت به سیگنال صوت ابتدائی با معیارهای عددی (به عنوان مثال بر اساس متوسط مجذور خطا یا نسبت سیگنال به نویز) مشکل است. زیرا بر اساس خواص گوش انسان حتی یک صوت با دامنه تغییر مقیاس یافته، ممکن است با وجود متوسط مجذور خطای بالا از کیفیت بسیار عالی برخوردار باشد[۱۱]. بنابراین برای ارزیابی کیفیت صوت، (مطابق با آنچه که در سایر مقلات صورت گرفته است)، یک سری تست غیر رسمی با هد ست انجام شده است. به این منظور کلیپهای صوت ابتدایی و کلیپهای صوت حاوی واترمارک دار به صورت تصادفی برای یک گروه۱۰ نفره متشکل از افرادی با سنهای متنوع و جنس مختلف پخش گردید.

هیچ تفاوتی بین اصوات پخش شده توسط افراد گروه تشخیص داده نشد و در تشخیص نوع صوت نیز، صوت حاوی واترمارک بعضاً با صوت اصلی اشتباه گرفته شد. نتایج این آزمایشات گویای این مسئله است که همانطور که انتظار می رفت واتر مارک اضافه شده بر کیفیت سیگنال صوت اثر نمی گذارد. استفاده از یک الگوریتم مبتنی بر تکرار و سیگنال اصلاح وابسته به سیگنال، امکان نامحسوس بودن واترمارک را در عین مقاومت کافی در برابر حملات را فراهم می آورد. همچنین از آنجا که هرنمونه اصلاح شده و حداقل یک نمونه دست نخورده در یک بازه زمانی کوچک ظاهر می شوند، مطابق با خواص پوشش زمانی سیستم شنیداری انسان، نمونه های دست نخورده، نمونه های تغییر یافته را می پوشانند و به این ترتیب ناشنوایی تغییرات اعمالی را تضمین می نماید.

۴-۲-تست مقاومت!

ضمن حفظ کیفیت سیگنال واترمارک دار شده، با اعمال یک سری از عملیات پردازش سیگنال، مقاومت الگوریتم مورد بررسی قرار گرفت. این حملات بر اساس آنچه که در سایر مقالات ذکر شده است، اتخاب گردیدند. برای مشخص شدن میزان مقاومت روشهای پیشنهادی حملات زیر به کار گرفته شدند.

۱. تغییر مقیاس محور زمان (T1)

ابتدا سیگنال واتر مارک دار شده تا حد ٪۴ در محور زمان منبسط می گردد و سپس تا حد ٪۴ فشرده می گردد.

۲. تغییر نرخ نمونه برداری (T2)

نرخ نمونه برداری سیگنال واتر مارک داده ابتدا به۴۴/۱ کیلو هرتزبه۳۲ کیلو هرتزو سپس به ۴۸ کیلو هرتز و نهایتاً به۴۴/۱کیلو هرتز تغییر می یابد.

۳. فیلتر پایین گذر (T3)

از یک فیلتر پایین گذر مرتبه ۴ باتروورث با فرکانس قطع۴ کیلو هرتزاستفاده گردید.

۴. اضافه کردن نویز (T4)

نویزی با متوسط صفر و تابع چگالی توان گوسی به سیگنال حاوی واترمارک اضافه می شود.

۵. تغییر دامنه سیگنال (T5)

سیگنال واتر مارک دار با ضریب۰/۰۱ تضعیف گردید.

۶. برش (T6)

چندین قسمت ۵۰۰ نمونه ای از محلهای مختلف سیگنال واترمارک دارحذف گردید و سپس آشکارسازی پیام نهفته شده مورد بررسی قرار گرفت. البته برش روی پیکها اجرا نمی شود.

۷. همزمانی (T7)

یک قسمت ۵۰۰ نمونه ای از ابتدای سیگنال حاوی واترمارک حذف گردید.

۸. اضافه کردن اکو (T8)

سیگنال ابتدایی با ۱۰۰میلی ثانیه تأ خیربه سیگنال حاوی واترمارک اضافه می شود.

جدول ۱ میزان بیت خطایی که در آشکارسازی پیام یک پیام ۳۲ بیتی پس از هر یک از این مراحل رخ داده است را نشان می دهد. در این جدول T_0 میزان خطا در آشکارسازی طبیعی و بدون اعمال هیچ گونه حمله ایی و T_1 ,..., T_8 به ترتیب حملات ذکر شده را مشخص می کنند. همانطور که مشاهده می شود روش پیشنهادی قادر به تحمل اکثر حملات به خوبی می باشد ولی در برابر تغییر مقیاس محور زمان و عبور از فیلتر بیت خطای بیشتری نشان می دهد.

طبق پارامترهای انتخابی نرخ نهانگی الگوریتم پیشنهادی (ظرفیت)۱۵بیت بر ثانیه است که با تغییر پارامترهای انتخابی قابل

[7] Pop
[8] Rock
[9] Piano
[10] Pipe (Solo)
[11] Speech

افزایش می باشد.

جدول۱: تعدا د بیتهای خطا تحت حملات مختلف

نوع موسیقی	T0	T1	T2	T3	T4	T5	T6	T7	T8
پیانو۱	0	4	0	8	0	0	0	0	0
پیانو۲	0	6	0	12	1	0	0	0	0
راک۱	1	4	0	9	1	1	1	1	1
راک۲	0	2	0	8	0	0	0	0	0
پاپ۱	1	2	1	9	1	1	1	1	1
پاپ۲	1	5	2	9	1	1	1	1	1
نی(تک نوازی)۱	1	6	1	7	2	1	1	1	1
نی(تک نوازی)۲	0	4	0	10	1	1	1	0	0
سکوت۱	0	2	0	10	0	0	0	0	0
سکوت ۲	0	4	0	8	0	0	0	0	0
صحبت مرد	1	9	1	9	1	1	1	1	1
صحبت زن	0	5	0	9	0	0	0	0	0

۵-نتیجه گیری!

الگوریتم نهانگاری پیشنهاد شده در این مقاله واترمارک را در حوزه زمان و توسط تغییر جزئی دامنه تعدادی از نمونه های سیگنال صوت، نهان می نماید. نمونه هایی که بایستی در معرض تغییرات قرار گیرند، توسط الگوریتم خوشه بندی اعمال شده در حوزه فرکانس، و سپس توسط کلید رمز مشخص می گردند. یکی از نقاط برجسته الگوریتم پیشنهادی ترکیب حوزه زمان و حوزه فرکانس به منظور بهره گیری همزمان از مزایای آن دو حوزه می باشد. الگوریتم نهان نگاری پیشنهادی بر اساس خواص پوشش زمانی سیستم شنیداری انسان بر کیفیت سیگنال صوت ابتدایی اثر نگذاشته و همچنین در برابر حملات متداول پردازش سیگنال مقاوم می باشد. گرچه نرخ بیت خطای الگوریتم پیشنهادی در برابر حمله عبور از فیلتر و تغییر مقیاس محور زمان بیشتر از سایر حملات می باشد.

مراجع

[1] A.N., Lemma, et. al., "A Temporal Domain Audio Watermarking Technique", IEEE Trans. Signal Proc., Vol. 51, No. 4, April 2003.

[2] L.Boney, et. al.,"Digital watermarks for audio signal", International Conference on Multimedia Computing and Systems, Hiroshima, Japan, pp. 473-480,1996.

[3] H. J. Kim, et. al. ,"A Novel Echo-Hiding Scheme With Backward and Forward Kernels", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003.

[4] B.S. Ko, et. al.,"Time-Spread Echo Method for Digital Audio Watermarking", IEEE Transactions on Multimedia, Vol. 7, No. 2, April 2005.

[5] P. Bassia, et. al.,"Robust Audio Watermarking in the Time Domain", IEEE Transactions on Multimedia, Vol. 3, No. 2, June 2001.

[6] Cheng et al., "Spread Spectrum Signaling for Speech Watermarking ",United States Patents, Patent No. US 6,892,175 B1, May 10,2005.

[7] S. Erküçük, et. al.,"A Robust Audio Watermark Representation Based on Linear Chirps", IEEE Transactions on Multimedia, Vol. 8, No. 5, October 2006.

[8] C.H. Yeh, et. al. "Digital watermarking through quasi m-arrays". Proc. IEEE Workshop on Signal Proc. Systems, Taipei, Taiwan, p 456–461, 1999.

[9] H. J. Kim, et. al., "Audio Watermarking Techniques", J-s-Pan Ed. Chap 8, World, Scientific Pub. Co, 2004

[10] M. F. Mansour, et. al., "Audio Watermarking by Time-Scale Modification", Proc. IEEE ICASSP Conf, pp. 1353-1356, 2001.

[11] W-N Lie, et. al., "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification", IEEE Trans. Multimedia, Vol. 8, pp. 46-59, Feb. 2006

[12] H. Spath, "Cluster Dissection and Analysis: Theory, FORTRAN Programs, Examples", translated by J. Goldschmidt, Halsted Press, 1985, 226pp.