انجمن رمز ایران
Iranian Society of Cryptology

دانشگاه صنعتی خواجه نصیرالدین طوسی
۱۳۰۷

هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹
دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران-ایران

بسمه تعالی

گواهی می شود مقاله با عنوان:

"افزایش ظرفیت استگانوگرافی در فایل های صوتی با استفاده از روش ذخیره غیریکنواخت در ضرایب موجک مترقی"

ونویسندگان: "امید اسلامی، وحید حقیقت دوست، الهام رجبی"

در هفتمین کنفرانس بین المللی انجمن رمز ایران

که در دانشگاه صنعتی خواجه نصیرالدین طوسی در تاریخ ۲۴و۲۵ شهریورماه ۱۳۸۹ برگزار گردید، ارائه شد.

ISCISC'10
7th International ISC Conference on
Information Security and Cryptology
September 15-16, 2010, Tehran, Iran
K.N.Toosi University of Technology

دبیر کنفرانس
دکتر محمود احمدیان

دبیر خانه: تهران، تقاطع خیابان شریعتی و بزرگراه رسالت
دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی خواجه نصیرالدین طوسی
تلفن: ۰۲۱-۸۸۴۶۲۴۹۶ نمابر: ۰۲۱-۸۸۴۶۲۰۶۶

افزایش پیلود استگانوگرافی در فایل‌های صوتی با استفاده از روش ذخیره غیریکنواخت در ضرایب موجک مترقی

امید اسلامی
دانشکده فنی و مهندسی دانشگاه شاهد
eslami.omid@gmail.com

وحید حقیقت‌دوست
دانشکده فنی و مهندسی دانشگاه شاهد
haghigatdoost@shahed.ac.ir

الهام رجبی
دانشکده فنی و مهندسی دانشگاه شاهد
Elham.rajabi86@gmail.com

چکیده

در این مقاله یک روش نوین نهان‌نگاری صوت که اطلاعات را در ضرایب تبدیل موجک LWT مخفی می‌کند، ارائه شده است. در این روش ابتدا فایل صوتی موردنظر به اندازه ۶۴ تائی فریم‌بندی می‌شود. سپس به سیگنال صوتی، تبدیل موجک LWT اعمال می‌گردد. در مراحل بعدی و به منظور افزایش شباهت نتایج به آستانه شنوائی انسان، تبدیل موجک در رده‌های بالاتر و بالطبع زیرباندهای بیشتر اعمال می‌شود. سپس در زیرباندهای مذکور آستانه شنوائی محاسبه شده، توالی داده جانشین بیت‌های کم‌ارزشتر در هر ضریب می‌شوند. سپس با اعمال عکس تبدیل موجک، سیگنال صوتی حاوی اطلاعات مخفی، بازسازی شده و قابل بهره برداری می‌باشد. نتایج تجربی از ظرفیت بالای پنهان نگاری، بازیابی کامل اطلاعات مخفی شده و کیفیت سیگنال صوتی حاوی اطلاعات حکایت می کند.

کلمات کلیدی

پنهان‌نگاری اطلاعات در صوت، تبدیل موجک مترقی، بسته موجک، آستانه شنوائی، نهان‌نگاری موجک سازگار

مقدمه

امروزه با پیشرفت و گسترش رایانه ها و شبکه‌های جهانی و نیز افزایش کارآئی این تکنولوژی در تمامی ابعاد زندگی انسان، استفاده از رایانه‌ها بعنوان دفاتر کاری انسان‌ها و سازمان‌ها و برقراری ارتباط بصورت غیرحضوری بسیار مورد توجه قرار گرفته است. ولیکن یکی از مهمترین نگرانی‌ها و چالش‌ها در این زمینه، امنیت و عدم دسترسی غیرمجاز به اطلاعات شخصی افراد و سازمان‌های مختلف می‌باشد.

دانش نهان‌نگاری اطلاعات ابزاری نیرومند است که امنیت انتقال و ذخیره سازی اطلاعات را بالا می‌برد. در سناریوی نهان‌نگاری، داده محرمانه درون رسانه دیگری نظیر صوت، تصویر و یا ویدئو مخفی می‌شود که به رسانه مذکور اصطلاحاً سیگنال پوشش گفته می‌شود. پس از اتمام فرآیند نهان‌نگاری، سیگنال نهانه تشکیل می‌شود، که این سیگنال جدید می‌تواند انتقال داده شده و یا ذخیره سازی گردد. به طور کلی یک سامانه مخفی سازی اطلاعات باید دارای دو ویژگی اساسی زیر باشد:

شفافیت: بدین معنی که موضوع میزبان پیام در هر دو حالت عاری وحاوی پیام مشابه باشد، یعنی در سیگنال نهانه تفاوت قابل درکی برای حواس انسان وجود نداشته باشد.

ظرفیت: میزان اطلاعاتی را که می‌توان در حداقل حجم از رسانه مورد نظر مخفی‌سازی کرد. ذکر این نکته الزامیست که حجم داده‌ای که می توان در یک میزبان ذخیره کرد دقیقا بستگی به ماهیت میزبان دارد.

در سال‌های اخیر شگردهای مختلفی با اهداف گوناگون برای پنهان نگاری اطلاعات در صوت دیجیتالی ارائه شده است که همه این روش‌ها به نوعی از ضعف سامانه شنوایی انسان (HAS) در نهان‌نگاری بهره می‌جویند. در بسیاری از این روشها از شگرد تغییر بیت‌های کم‌ارزش (LSB) سیگنال صوتی در حوزه زمان و یا حوزه تبدیل استفاده می‌کنند. برخی از این روش‌ها این شگرد را با شگردهای دیگری همچون انتشار خطا [1,2] ، جانشانی خطای کمینه (MER) و اثر خاصیت پوشش‌دهی زمانی [3] ترکیب می‌کنند. در روشهای دیگر پیامهای محرمانه را در بیتهای کم‌ارزش حوزه های تبدیل همچون تبدیل موجک [4] و تبدیل صحیح به صحیح [3] و اخیراً تبدیل موجک صحیح شده [5] مخفی‌سازی می‌کنند. هرچند شگرد تغییر بیت‌های کم‌ارزش در [6] با هدف افزایش مقاومت

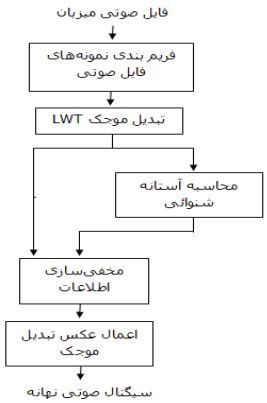
در برابر نویز جمع‌شونده، اصلاح شده است. در گروه دیگری از روشهای نهان‌نگاری در صوت[7,8] ازشگردهای نهان‌نگاری اطلاعات در تصاویر برای مخفی‌سازی اطلاعات استفاده می‌شود.

در این مقاله یک روش نهان‌نگاری مبتنی بر شگرد تغییر بیت‌های کم‌ارزش ارائه می‌شود که بیت‌های کم‌ارزش تبدیل موجک LWT سیگنال صوتی را متناسب با بیت‌های داده تغییر می‌دهد. تعداد بیت‌های قابل تغییر در هر زیر باند با آستانه شنوائی که برای آن زیرباند تعریف می شود، متناسب است. تأکید اصلی در این روش افزایش ظرفیت نهان‌نگاری بدون کاهش کیفیت شنیداری صوت نهانه و بازیابی کامل اطلاعات مخفی شده در صوت است.

فرایند پنهان نگاری اطلاعات

در بلوک دیاگرام **شکل(۱)** مراحل مخفی‌سازی را مشاهده می‌کنید. باتوجه به این نمودار مراحل مختلف مخفی‌سازی بصورت زیر قابل بیان است:

ابتدا نمونه‌های فایل صوتی فریم بندی می‌شوند. سپس به نمونه‌های گسسته در زمان سیگنال پوشش، تبدیل LWT را با فیلتر هار اعمال می‌کنیم، تا ضرایب صحیح بدست آیند. با استفاده از این ضرایب آستانه شنوائی را محاسبه می‌کنیم.

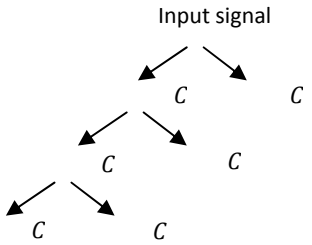


شکل ۱- مراحل مخفی سازی اطلاعات به روش پیشنهادی

روش اعمال تبدیل موجک پاکت

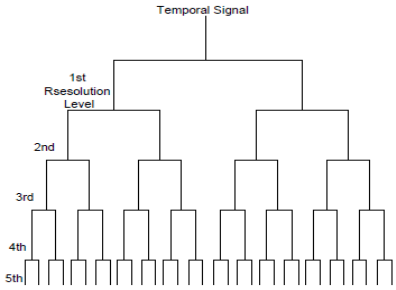
در حالتی‌که تبدیل موجک را به صورت موجک ساده در سطح سوم پیاده سازی کنیم، خروجی آن رشته‌هائی است که شامل ۴ زیرباند خواهد بود که در **شکل(۲)** شامل باندهای (A3,D1,D2 ,D3) تشکیل می‌شود.

همانطور که در این شکل دیده می‌شود در این حالت برای محاسبه تبدیل موجک در سطح سوم، ابتدا این تبدیل در سطح اول محاسبه می‌شود و ضرایب بدست آمده در مرحله بعد تبدیل موجک فقط به ضرایب CA_1 اعمال می‌شود تا ضرایب دیگری حاصل شوند و به‌همین ترتیب با اعمال تبدیل موجک در هر سطح و بعد از جاگذاری این ضرایب، رشته‌ای از ضرایب مشابه رشته مذکور حاصل می‌گردد.



شکل ۲- روش ساخت ضرایب تبدیل موجک ساده از سیگنال زمانی تا رده سوم

حال اگر از قسمتهایی از رشته مذکور که متعلق به سطوح پایین‌تر تبدیل موجک هستند، مجددا تبدیل موجک بگیریم و این کار تا آنجا ادامه دهیم که تمام زیرباندها متعلق به سطح پنجم باشند، نتیجه آن رشتهائی خواهد بود که به ۳۲ زیر باند قابل تفکیک است. این نوع اعمال تبدیل موجک اصطلاحاً موجک پاکت گفته می‌شود. در **شکل(۳)** این موضوع بوضوح مشهود است.

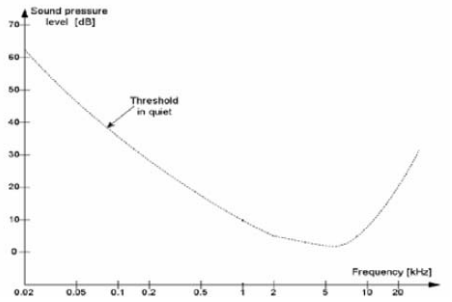


شکل ۳- روش ساخت ضرایب تبدیل موجک پاکت از سیگنال زمانی تا رده پنجم

آستانه شنوایی در حوزه تبدیل موجک

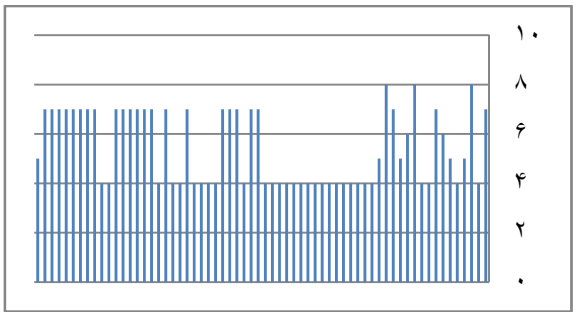
آستانه سکوت شنوایی درحقیقت مرز بین شنیدن و نشنیدن گوش انسان است به‌شرط آنکه هیچ سیگنال قابل شنیده شدن دیگری در محیط اطراف گوش در حال پخش نباشد. در حوزه زمان این آستانه بصورت یکنواخت توزیع می شود ولی در حوزه فرکانس حد این آستانه در فرکانسهای مختلف متفاوت است بطوریکه آستانه شنوایی در فرکانسهای بالا و خیلی پایین، بالاست. ولی در

فرکانسهای میانی میزان آستانه سکوت بسیار پایین است. این فرکانسهای میانی شامل محدوده ۲۰۰۰ تا ۴۰۰۰ هرتزهستند. در نمودار **شکل(۴)** آستانه سکوت شنوایی را در حوزه فرکانس می‌بینیم.



شکل ۴- آستانه سکوت شنوایی در حوزه فرکانس

در کانال انکدر، اطلاعات در ضرایب تبدیل موجک صوت مخفی می‌شود. میزان اطلاعات وارد شده به هر ضریب به حساسیت شنوایی گوش انسان در آن محدوده بستگی دارد. هر چه محدوده فرکانسی زیرباند مورد نظر به فرکانسهای پایین و یا بالا نزدیکتر باشد، بدلیل آنکه گوش انسان حساسیت کمتری نسبت به تغییرات اعمال شده در آنها از خود نشان میدهد، حجم بیشتری از اطلاعات را در این دسته از ضرایب میتوان مخفی کرد. در **شکل(۵)** ظرفیت مخفی‌سازی به ازای هر فریم ۶۴ تائی از فایل صوتی نمایش داده شده است.

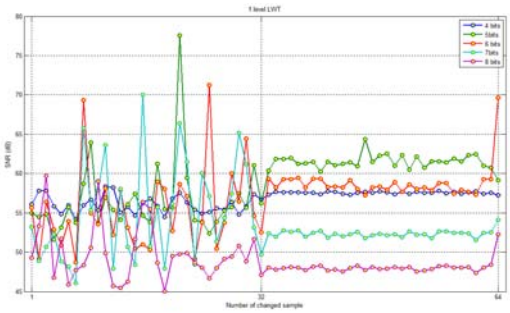


شکل ۵- قابلیت مخفی‌سازی اطلاعات در زیر آستانه شنوائی

این ۶۴ عدد معادل آستانه مطلق شنوایی هستند که به صورت تجربی و با انجام تست های مکرر شنوائی برای افراد مختلف و با روش مذکور بدست آمده‌اند. باید خاطرنشان ساخت که این آستانه فقط به ازای اعمال تبدیل LWT در سطح پنجم معتبر است.

تشریح الگوریتم نهان‌نگاری موجک سازگار

در ابتدا روش پیاده‌سازی را در سطح اول LWT شرح می‌دهیم. همانگونه که در **شکل(۶)** مشاهده می‌کنید، نمودار نمایشگر ۵ منحنی است که همگی میزان SNR نمونه موردنظر در ازای جانشانی n بیت کم ارزشتر و ۳ بیت کم‌ارزشتر مابقی نمونه‌ها می باشد، که در آن n عددی بین ۴ تا ۸ می باشد. از آنجائی که تنها یکبار از صوت اصلی تبدیل LWT گرفته شده است لذا، این نمودار نمایانگر دو زیر باند مجزا می‌باشد که زیر باند اول (نمونه های ۱ تا ۳۲) مربوط به فرکانس‌های بالا و زیرباند دوم (نمونه‌های ۳۳ تا ۶۴) مربوط به فرکانس‌های پائین می‌شود. در هر کدام از زیرباندها ۳۲ نمونه قرار گرفته است.



شکل ۶- نمودار تغییرات SNR درجاسازی LSB غیر یکنواخت ضرایب موجک با جانشانی ۳ بیت پیش‌فرض

با استفاده از اطلاعات بدست آمده، روندی را انتخاب می‌کنیم که بتوان با جانشانی غیریکنواخت اطلاعات در LSB ضرایب موجک به Payload بیشتری از حالت جانشانی ۴بیت LSB یکنواخت برسیم. به‌همین منظور، در اطلاعات SNR پس از حذف تمامی حالات استثنا از دامنه اطلاعات هر نمونه و با در نظر گرفتن آستانه 5dB، در هرنمونه مقدار بیتی را انتخاب می‌کنیم که، اختلاف SNR آن با حالت ۴بیتی کمتر از 5dB باشد. به عبارت دیگر:

۱. تمامی جانشانی بیت‌هائی که SNR بیشتر از حالت جانشانی ۴بیتی دارند را از دامنه هر نمونه حذف می‌کنیم.
۲. در دامنه هر نمونه، بیتی را انتخاب می‌کنیم که SNR آن حداکثر 5dB کمتر از SNR حالت ۴بیتی باشد.
۳. در صورتی که نمونه‌ای با این شرایط امکان انتخاب بیت‌های بالاتر را نداشت، اطلاعات را با ۴ بیت در این نمونه جانشانی می‌کنیم.

ذکر این نکته الزامی‌است که، تعریف این حد آستانه به‌منظور افزایش ظرفیت نهان‌نگاری بوده است و مقدار آن

نیز پس از انجام چندین آزمایش بدست آمده است. روند انتخاب این حد آستانه بدین صورت است که ضمن توجه به خصوصیات گوش انسان و با اعمال حد آستانه مذکور بتوان تعداد بیت‌های بیشتری را در هر نمونه جانشانی کرد. با انجام آزمایشهای گوناگون این نتیجه حاصل شد که 5dB اختلاف قابل درکی برای گوش انسان نیست، ضمن اینکه در نهایت SNR حاصل شده نیز مقدار قابل توجهی دارد.

در **جدول۱** مقایسه‌ای از روش پیشنهادی با روشهای یکنواخت دیگر آورده شده است.

جدول ۱- مقایسه SNR و Payload روش پیشنهادی با روش‌های قبلی

روش	SNR	Payload
روش پیشنهادی	55.13	351
LSBیکنواخت ۴ بیتی	51.2	256
LSBیکنواخت ۵ بیتی	47.22	320

آزمایش قبلی را با همان مشخصات و الگوریتم بر روی فایل صوتی مذکور، در رده های بالاتر موجک پاکت نیز انجام دادیم که نتایج آن در بخش نتایج آورده شده است. SNRهای جانشانی در هر زیرباند، تقریبا برابر هستند و نیز در هر زیرباند، اختلاف زیادی از این نظر مشاهده نمی‌گردد، مگر در موارد استثنا که قبلا بحث شد، که این موضوع در نمودارهای رده‌های بالاتر به وضوح مشهود است.

مقایسه نتایج

جدول۲- مقایسه کارائی روش پیشنهادی در رده‌های مختلف با LSB یکنواخت ضرایب LWT

روش	SNR	Payload	MOS
پیشنهادی 1st LWT	55.13	351	4.4
پیشنهادی 2nd LWT	57.6	349	4.5
پیشنهادی 3rd LWT	58.48	343	4.6
پیشنهادی 4rd LWT	58.43	321	4.6
پیشنهادی 5rd LWT	55.39	363	4.8
LSB4 bit LWT	51.2	256	4.1
LSB 5bit LWT	47.22	320	3.8

با توجه به اعمال روش نهان‌نگاری موجک سازگار و مقایسه نتایج آن در رده‌های مختلف و نیز قیاس آنها با روش‌های دیگر به این نتیجه رسیدیم که در فریم بندی ۶۴ تائی نمونه‌ها و با اعمال تبدیل موجک پاکت در رده پنجم به بالاترین درجه تفکیک فرکانسی می رسیم که نتیجه این بررسی به‌صورت آشکار در اطلاعات **جدول۲** مشهود است.

جمع بندی و نتیجه گیری

دراین مقاله یک روش مؤثر و نوین نهان‌نگاری اطلاعات در صوت ارائه شد. در این روش بیت های داده محرمانه در ضرایب تبدیل موجک مترقی در نواحی که سامانه شنوایی انسان در آن نقاط حساسیت کمتری به تغییرات دارد مخفی می‌شود. استفاده از تبدیل موجک LWT موجب حذف خطای بازیابی شده است. از مزایای این روش، بی‌نیازی به دسترسی به صوت اصلی در زمان بازیابی داده، ظرفیت مخفی سازی بالا، بازیابی کامل و کیفیت شنیداری بالای صوت نهانه را می‌توان نام برد.

با توجه به توضیحات ذکر شده و کارآئی استفاده از رده پنجم ضرایب موجک پاکت، انجام ادامه آزمایشات را در رده مذکور و با استفاده از موجک پاکت که طراحی شد، پیگیری کردیم که نتایج اعمال آن را بر روی ۱۰ فایل صوتی در **جدول۳** می‌توانید مشاهده نمائید.

جدول ۳- نتایج کلی طرح پیشنهادی در آزمایشات گوناگون

	روش پیشنهادی			SNR LSB 4bit	SNR LSB 5bit
	SNR	Payload	MOS		
Classic 1	53.04	341	4.8	51.32	47.31
Classic 2	50.19	355	4.8	53.59	43.87
Country	55.91	353	4.9	50.8	47.56
Country	55.39	363	4.8	51.2	47.22
Jazz 1	57.07	372	5	48.73	45.46
Jazz 2	51.22	410	4.9	47.17	48.71
Pop 1	44.17	379	5	41.83	38.16
Pop 2	43.44	392	5	41.29	38.85
Speech	47.62	336	4.5	55.45	40.81
Speech	45.71	373	4.6	42.91	38.98

با بررسی اطلاعات جدول و با حذف تمامی حالات استثنا می‌توان به این نتیجه رسید که بطور میانگین این روش قابلیت دارا بودن ظرفیتی معادل ۳۶۷ بیت را در هر فریم ۶۴تائی داراست. که با توجه به میانگین مقادیر SNR که عددی معادل ۵۰/۳۷ است، نشان از کارآئی بالای این روش می‌دهد. از نظر کیفی نیز فایل‌های صوتی از کیفیت شنیداری بالائی برخوردارند که با میانگین MOS ، ۴/۸

تطابق این روش با خصوصیات شنوائی انسان مشخص می‌شود.

مراجع

[1] N. Cvejic, T. Seppanen, *"Increasing robustness of LSB audio steganography using a novel embedding method,"* In Proc. IEEE Int. Conf. Info. Tech. : Coding and Computing, Vol. 2, pp. 533-537, April 2004.

[2] N. Cvejic, T. Seppanen, *"Increasing the capacity of LSBbased audio steganography."* IEEE Workshop on Multimedia Signal Processing, pp. 336-338, 2002.

[3] S.S. Agaian, D. Akopian, O. Caglayan, S. A. D'Souza, *"Lossless Adaptive Digital Audio Steganography,"* In Proc. IEEE Int. Conf. Sig., Sys. and Comp., pp. 903-906, 2005.

[4] N. Cvejic, T. Seppanen, *"A wavelet domain LSB insertion algorithm for high capacity audio steganography,"* In Proc. IEEE Digital Signal Processing Workshop, Callaway Gardens, GA, p. 53–55, Oct. 2002.

[5] A. Delforouzi, M. Pooyan, *"Adaptive Digital Audio Steganography Based on Integer Wavelet Transform,"* IEEE Int. conf. Intelligent Information Hiding
and Multimedia Signal Processing (IIH- SP'07), Nov. 2007, Kaoshiung, Taiwan.

[6] K. Gopalan, *"Audio steganography using bit modification,"* Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2003.

[7] P. Bao and X. Ma, *"MP3-Resistant Music Steganography based on Dynamic Range Transform,"* IEEE Int. Sym. Intelligent Signal Processing and Communication Systems, pp. 266-271, Nov. 18-19, 2004, Seoul, Korea.

[8] R. A. Santosa, P. Bao, *"Audio-to-image wavelet transform based audio steganography,"* IEEE Int. Symp. , pp. 209-212, June 2005, Zadar, Croatia.

[9] H. Matsuka, *"Spread Spectrum Audio Steganography using Sub-band Phase Shifting,"* IEEE Int. conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP' 06), pp. 3-6, Dec. 2006, Pasadena, CA, USA.

[10] K. Gopalan, *"Audio steganography by cepstrum modification,"* In Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 5, pp. 481-484, March 2005.