# ارائه یک روش واترمارکینگ صوت مقاوم در برابر حمله نویز با استفاده از تبدیل موجک گسسته

فاطمه السادات قنادی[۱]، سعید نصری[۲] و علیرضا نقش[۳]
[۱]دانشکده مهندسی برق، واحد نجف آباد، **دانشگاه آزاد اسلامی**، نجف آباد، ایران.
[۲]دانشکده مهندسی برق، واحد نجف آباد، **دانشگاه آزاد اسلامی**، نجف آباد، ایران.
[۳] دانشکده مهندسی برق، واحد نجف آباد، **دانشگاه آزاد اسلامی**، نجف آباد، ایران.

**چکیده – در این مقاله هدف ارائه یک الگوریتم واترمارکینگ مقاوم صوت در برابر حمله نویز با استفاده از تبدیل موجک گسسته می‌باشد. برای دستیابی به این هدف اطلاعات در ضرایب فرکانس پایین تعبیه می‌گردد. این مشخصه‌های فرکانس پایین ابتدا توسط روش تبدیل ویولت استخراج می‌گردند، و رشته بیت پیام بر روی این نمونه‌ها که شامل بخش اعظمی از انرژی فرکانس پایین سیگنال هستند درج می‌گردد تا الگوریتم واترمارکینگ ارائه شده، در مقابل حملات از حداکثر مقاومت بهره مند گردد. در الگوریتم جدید رشته بیت پیام توسط کدهای کانولوشن، کدگذاری می‌گردد. یکی از ویژگی‌های این کدها مقاومت زیاد در مقابل نویز و اعوجاج کانال است. روش پیشنهادی در مقایسه با دیگر روش‌های ارائه شده در حوزه تبدیل موجک دارای سرعت استخراج واترمارک بالاتر و خطای کمتر در ظرفیت برابر می باشد.**

کلید واژه- واترمارکینگ، تبدیل موجک گسسته، مقاومت، نویز

## ۱. مقدمه

در سال‌های اخیر فنّاوری رسانه‌های دیجیتال[۱] پیشرفت چشم‌گیری داشته است. این فنّاوری در مقایسه با سیستم‌های آنالوگ قدیمی، برتری و نتایج بسیاری همچون، انتقال سریع اطلاعات و کپی بدون از دست دادن هیچ بخشی از منبع را دسترس عموم قرار می‌دهد. همچنین یکی دیگر از برتری‌های بسیار مهم رسانه‌های دیجیتال قابلیت پردازش و ویرایش آسان آن‌ها می‌باشد. به‌صورت موازی رشد این صنعت در اینترنت و وایرلس نیز مشهود است و با موفقیت و مقبولیت بسیار گسترده‌ای مواجه شده است. از سویی دیگر این رشد برخی از مشکلات و مسائل را نیز به همراه آورده است.

قابلیت کپی سریع بدون هیچ‌گونه محدودیت در تعداد کپی و یا از دست رفتن اطلاعات سبب به وجود آمدن قانون کپی رایت[۲] شده است. در این بین پنهان‌سازی[۳] به‌عنوان راه حلی برای اثبات حق و حقوق مؤلف ارائه شده است. سیگنال واترمارک، سیگنالی محرمانه و غیر قابل مشاهده است که در داخل اطلاعات اصلی تعبیه می‌گردد. این تعبیه به گونه‌ای است که تا هنگامی‌که داده اصلی از نظر کیفیت، در سطحی قابل قبول قرار دارد، سیگنال واترمارک نیز در آن قابل کشف و آشکارسازی باقی می‌ماند. در این مقاله، به‌منظور دستیابی به مشخصه‌هایی هر چه قوی‌تر، از تبدیل ویولت و استخراج اطلاعات فرکانس پایین استفاده شده است. بر اساس توضیحات داده شده می‌توان دریافت، که مساله اساسی، ارائه روشی برای پنهان‌سازی است که بتواند به بهترین نحو ممکن و به‌صورتی متعادل، تمامی ملاک‌های ارزیابی را برآورده سازد. بلوک‌های مختلف به منظور بهبود هر یک از این ملاک‌های

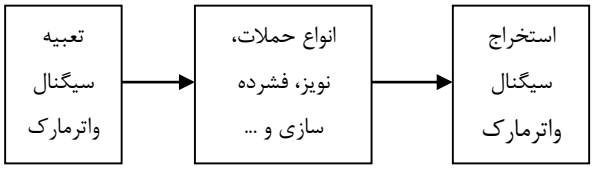
[1]- Digital Multi Media
[2]- Copy Right
[3]- Watermarking

سنجش وجود دارند، ولی مساله مهم ترکیب و به کارگیری این بلوک‌ها به گونه‌ای است که بهترین نتایج حاصل شده و موازنه‌ای قابل قبول بین تمامی ابعاد ارزیابی برقرار گردد.

## ۲. ساختار کلی یک سیستم پنهان‌ساز

روش‌های مختلف پنهان‌سازی را می‌توان بر اساس حوزه‌ای که عمل درج سیگنال پیام در آن انجام می‌شود تقسیم بندی نمود. سه نوع متداول، انجام پنهان‌سازی در حوزه‌های فرکانس، زمان و هیستوگرام می‌باشد.

یک سیستم پنهان‌سازی، مطابق شکل۱ در حالت کلی به‌عنوان ساختاری متشکل از دو قسمت پنهان‌سازی و استخراج است. در قسمت تعبیه و یا پنهان‌سازی دو سیگنال مجزا وجود دارد، یکی سیگنال پذیرنده[1] و دیگری سیگنال پیام که به‌عنوان واترمارک بر روی پذیرنده کد می‌گردد.




شکل ۱: ساختار کلی یک سیستم پنهان ساز

## ۳. تبدیل گسسته ویولت

تبدیل دیگری که برای انجام عمل پنهان‌سازی، بسیار مورد توجه قرار گرفته است تبدیل موجک گسسته (DWT) می‌باشد که در هر دو زمینه پنهان‌سازی صوت و تصویر به کار گرفته می‌شود. DWT تبدیلی است که در مراحل مختلف به سیگنال اعمال می‌شود و سیگنال را در سطوح و باندهای مختلف مورد پردازش قرار می‌دهد. تبدیل ویولت، سیگنال را با رزولوشن‌های متفاوت نمایش می‌دهد. در اغلب موارد ویولت توسط فیلتر بانکی متشکل از فیلترهای پایین گذر و بالا گذر پیاده‌سازی می‌شود[۱].

روند پردازش با تبدیل ویولت گسسته چنین آغاز می‌شود؛ در ابتدا سیگنال از یک فیلتر دیجیتال پائین‌گذر نیم‌باند با پاسخ ضربه h[n] عبور می‌کند، و لذا خروجی فیلتر برابر است با کانولوشن ورودی و پاسخ ضربه فیلتر. در نتیجه این عمل فیلترینگ، تمام مؤلفه‌های فرکانسی که بیشتر از نصف بزرگترین فرکانس موجود در سیگنال باشند حذف می‌شوند. از آنجا که بیشترین فرکانس موجود در سیگنال خروجی فیلتر برابر است با $\pi / 2$ رادیان، نیمی از نمونه‌ها قابل حذف‌اند. لذا با حذف یکی در میان نمونه‌ها، طول سیگنال نصف خواهد شد بدون اینکه اطلاعاتی را از دست داده باشیم. روند مشابهی نیز با استفاده از یک فیلتر دیجیتال بالاگذر نیم باند با پاسخ ضربه g[n] انجام می‌پذیرد. درنتیجه در خروجی اولین مرحله از اعمال تبدیل ویولت، دو نسخه، یکی بالاگذر و دیگری پائین گذر، با طول کاهش‌یافته (نصف شده) از سیگنال اولیه به فرم زیر به دست می‌آیند[۲].

$$y_{high}[k] = \sum_{n} x[n].g[2k-n] \qquad (۱)$$

$$y_{low}[k] = \sum_{n} x[n].g[2k-n]$$

## ۴. روش ارائه شده

در این تحقیق، به منظور دستیابی به مشخصه‌هایی هر چه قوی‌تر، از تبدیل ویولت و استخراج اطلاعات فرکانس پایین استفاده شده است. این مشخصه‌های فرکانس پایین ابتدا توسط روش تبدیل ویولت استخراج می‌گردند، و رشته بیت پیام بر روی این نمونه‌ها که شامل بخش اعظمی از انرژی فرکانس پایین سیگنال هستند درج می‌گردد تا الگوریتم واترمارکینگ ارائه شده، در مقابل حملات نویز از حداکثر مقاومت بهره مند گردد.

مدولا سیون کوانتشی یکی از روش‌های درج ر شته بیت پیام بر روی سیگنال صوت است که از مقاومت خوبی نسبت به حملات نویز بهره‌مند است.یکی دیگر از اهداف این تحقیق

[1] - Host Signal

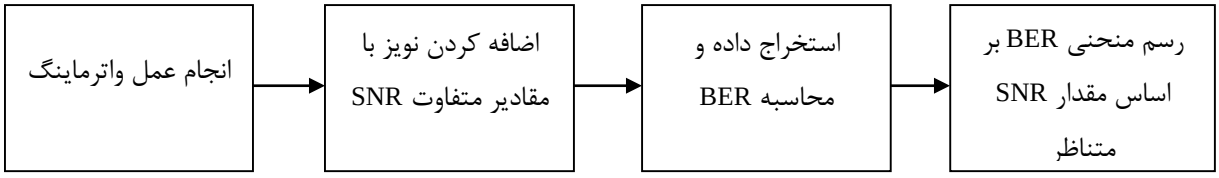
افزایش مقاومت الگوریتم واترمارکینگ، در مقابل انواع حملات است. بدین منظور رشته بیت پیام توسط کدهای کانولوشن، کدگذاری می‌گردد. یکی از ویژگی‌های اساسی این کدها مقاومت زیاد در مقابل نویز و اعوجاج کانال است. این مقاومت، در اثر کدگشایی نرم در هنگام استخراج رشته بیت پیام به وجود می‌آید. کدگشایی نرم از اطلاعاتی فراتر از اطلاعات دودویی در مرحله استخراج بهره می‌گیرد.

به منظور تلفیق هر چه بهتر این الگوریتم کدگذاری با سیستم‌های واترکینگ، در این مقاله، چگونگی استخراج اطلاعات نرم از مدولاتور کوانتشی ارائه شده و این مدولاتور به طریقی مناسب با دکودر نرم ترکیب می‌گردد.

در اثر استفاده از این اطلاعات، مقاومت الگوریتم واترمارکینگ به نحو چشمگیری در مقابل حملات فشرده سازی و نویزی بهبود می‌یابد. در واقع یک دمدولاتور نرم کوانتشی جدید ارائه می‌گردد که می‌تواند با استفاده از اطلاعات نرم، تا حد زیادی مقاومت را بهبود بخشد.

یکی از آسیب‌ها و یا حملاتی که ممکن است به سیگنال‌های واترمارک شده وارد شود، ایجاد اغتشاش و یا نویز در سیگنال واترمارک شده در اثر عواملی مختلف همچون ضبط مجدد صدا و ... می‌باشد.

در شبیه‌سازی این حمله، مطابق شکل۲، ابتدا سیگنال صوت مورد پردازش قرار گرفته و اطلاعات واترمارکینگ در آن تعبیه می‌گردد. سپس این سیگنال از کانال AWGN[1] نویزی با شدت SNRهای متفاوت عبور می‌نماید. در هنگام استخراج اطلاعات از سیگنال نویزی، مقدار BER ایجاد شده در SNR مرتبط محاسبه و ذخیره سازی می‌گردد تا به کمک آن منحنی *BER* برای تخریب از نوع نویز سفید رسم گردد.




شکل ۲: چگونگی شبیه سازی حمله نویز به سیگنال واترمارکینگ

## ۵. پارامترهای استفاده شده در روش پیشنهادی

دو پارامتر مهم در ارزیابی عملکرد روش پیشنهادی، شدت مخفی سازی (SNR) و نرخ خطای بیت (BER) می‌باشد.

### ۵-۱. شدت مخفی سازی

در این قسمت روش محاسبه شدت مخفی سازی مورد بررسی قرار می‌گیرد. دقت محاسبه‌ی این پارامتر در مخفی سازی امری حیاتی است چراکه اگر شدت پنهان‌سازی اطلاعات از آستانه شنوایی بالاتر آثار نامطلوب شنیداری به وجود خواهد آمد و اگر این میزان از آستانه شنوایی پایین‌تر باشد، مقاومت آب نقش نگار در برابر حملات مختلف کاهش خواهد یافت.

در الگوریتم‌های واترمارکینگ، شدت *SNR* سیگنال نتیجه شد از رابطه زیر بدست می‌آید:[۳]

$$SNR = -10\log_{10}\left(\frac{\left\|F - F'\right\|_2^2}{\left\|F\right\|_2^2}\right) \qquad (۲)$$

که در آن $F$ و $F'$ به ترتیب نمونه‌های زمانی سیگنال صوت قبل و بعد از عمل واترمارکینگ، و $\|F\|_2^2$ مجموع مربعات نمونه‌های زمانی سیگنال صوت، قبل از تعبیه اطلاعات می‌باشد. معمولاً شدت مخفی سازی باید بر روی ۲۰dB یا مقادیر بزرگ‌تر از آن تنظیم گردد.

[1] Additive White Gaussian Noise

### ۵-۲. نرخ خطای بیت

نرخ خطای بیت یا نرخ بازیابی، کمیتی است که عملکرد روش پیشنهادی با آن ارزیابی می‌شود و از رابطه (۳) به دست می‌آید.[۳]

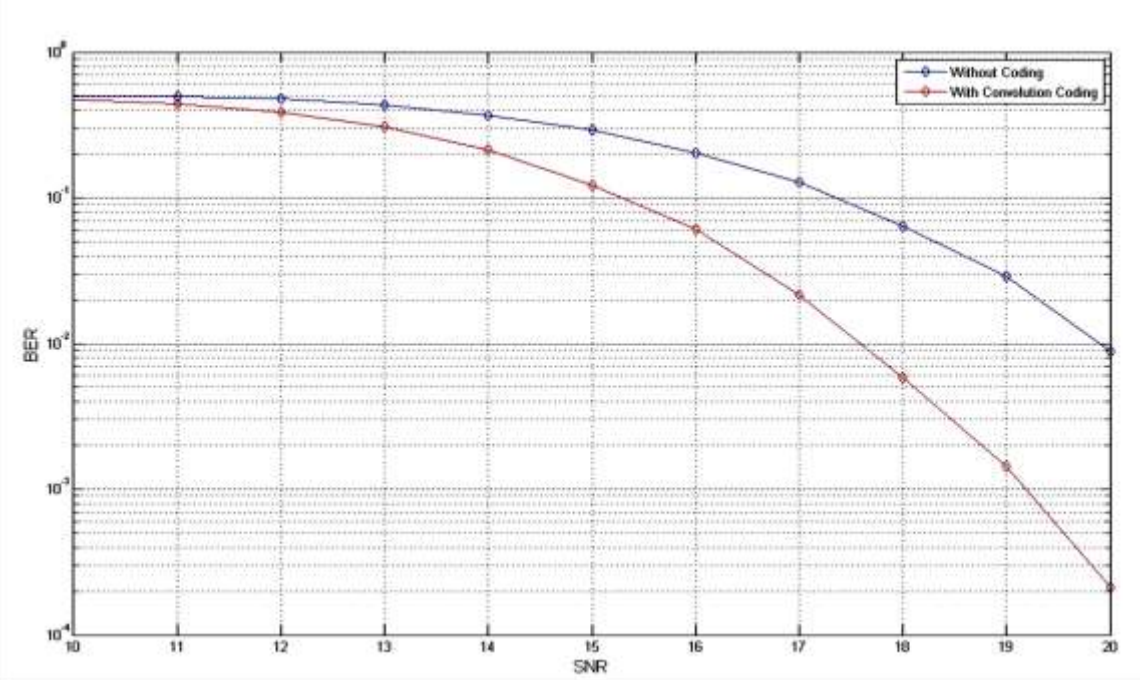
$$BER = \frac{\text{تعداد بیت‌های خطا}}{\text{کل تعداد بیت‌های واتر مارک}} \qquad (۳)$$

### ۶. نتایج

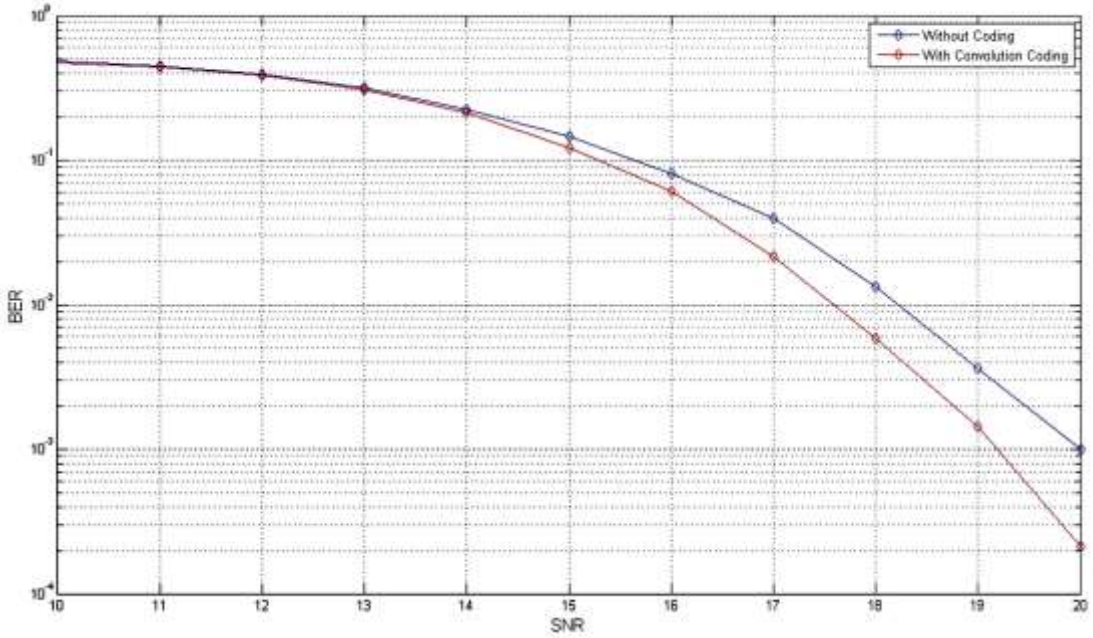
الگوریتم پیشنهادی توسط نرم‌افزار MATLAB 2014a شبیه‌سازی گردیده و بر روی انواع صوت سنتی، آرام، تند و گفتار مورد آزمایش قرار گرفته است. صوت‌های مورد آزمایش دارای نرخ ۴۴۱۰۰ و از نوع فرمت Wav هستند.

در شبیه‌سازی‌های انجام شده در این قسمت، ابتدا ۱۵S ثانیه سیگنال صوت با سطح شدت S= ۰,۳ و نرخ نمونه‌برداری ۴۴۱۰۰ Sample/S مورد پردازش قرار گرفته و اطلاعات واتر مارکینگ در آن تعبیه می‌گردد. سپس این سیگنال از کانال AWGN نویزی با شدت SNRهای متفاوت عبور می‌نماید. در هنگام استخراج اطلاعات از سیگنال نویزی، مقدار BER ایجاد شده در SNR مرتبط محاسبه و ذخیره‌سازی می‌گردد تا به کمک آن منحنی BER برای تخریب از نوع نویز سفید رسم گردد. اطلاعات واترمارکینگ در این شبیه سازی از نوع متن بوده و جمله "This is a signature" در سرتاسر سیگنال صوت درج شده است. همان‌طور که مشاهده می‌شود متن در نظر گرفته شده دارای ۱۹ کاراکتر می‌باشد و هر کاراکتر باید توسط ۸ بیت نمایش داده شود. بنابراین هر جمله دارای ۱۵۲=۸*۱۹ بیت اطلاعات می‌باشد. پس از انجام عمل تعبیه اطلاعات، ویولت معکوس به تمامی‌ضرائب اعمال شده و سیگنال صوت مجددا بازسازی می‌گردد.

آزمایش نویز بر روی دو نوع سیگنال صوت متفاوت توسط روش جدید ارائه شده و نتایج این شبیه‌سازی در زیر نمایش داده می‌شود.




شکل۳: منحنی BER حاصل شده پس از اعمال حمله نویزی به سیگنال صوت ۱ واتر مارک شده با نرخ نمونه‌برداری ۴۴۱۰۰ و سطح مخفی سازی S= ۰,۳




شکل۴: منحنی BER حاصل شده پس از اعمال حمله نویزی به سیگنال صوت ۲ واتر مارک شده با نرخ نمونه‌برداری ۴۴۱۰۰و سطح مخفی سازی۰,۳ =S

منحنی BER حاصل از به‌کارگیری هر دو روش پنهان‌سازی در شکل‌های ۳ و ۴ نمایش داده شده است. در این دو شکل، منحنی آبی رنگ، شبیه‌سازی به کمک روش تبدیل ویولت ساده و منحنی قرمز رنگ شبیه‌سازی با روش جدید ارائه شده را نمایش می‌دهد. به‌خوبی می‌توان دریافت که الگوریتم ارائه شده در کانال‌های نویزی عملکردی به‌مراتب بهتر را نشان می‌دهد. بهبود عملکرد سیستم، در مقابله با نویز اضافه شونده به‌مراتب بهتر می‌باشد. با توجه به منحنی‌های خطای بیت، مقدار خطا در صوت شماره ۱ به اندازه ۲dB و در صوت شماره ۲ به اندازه ۱dB بهبود یافته است.

## ۷. نتیجه گیری

پنهان‌سازی دارای کاربردهای متنوع و کلیدی در حوزه‌هایی همچون حفظ حقوق مولفین، ارسال و دریافت امن اطلاعات می‌باشد.

یک سیستم پنهان‌سازی، شامل دو قسمت اصلی درج اطلاعات پیام بر روی سیگنال پذیرنده و استخراج این اطلاعات از سیگنال پذیرنده است. قبل از مرحله استخراج اطلاعات ممکن است تغییراتی در سیگنال ایجاد گردد که مرحله استخراج را با مشکلاتی روبرو ساخته و به اطلاعات درج شده نیز آسیب وارد می‌شود. ازاین‌رو مقالات تحقیقی، به مقاوم‌سازی روش‌های پنهان‌سازی در مقابل این حملات پرداخته‌اند.

در این مقاله درج اطلاعات از طریق مدولاسیون کوانتشی در حوزه ویولت مورد تمرکز قرار گرفت و به افزایش مقاومت آن در برابر حملات نویز پرداخته شد و در این راستا، رشته بیت پیام توسط کدهای کانولوشن کدگذاری گردیند. کدهای کانولوشن در فنّاوری‌هایی نظیر ارتباطات رادیویی، موبایل، مخابرات ماهواره و پخش دیجیتالی تصاویر کاربرد دارد.

یکی از مزایای استفاده از کد کانولوشن، توانمندی این مدل کد برای کنترل خطاهای قطاری رخ داده در زنجیره اطلاعات است.

در هنگام حملات از نوع نویز، کدهای کانولوشن به‌طور قابل قبول خطا را حذف می‌نمایند.همان‌طور که در منحنی‌های خطا مشاهده گردید، الگوریتم ارائه شده قابلیت بهبود تا حد ۲dB را از خود نشان می‌دهد.

## مراجع


[1] N.V.Lalitha, Ch.Srinivasa, "**DWT-Arnold transform based audio watermarking**", IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics, PP. 196-199, December 2013

[2] A.Padungdit, "**Image watermarking using joined wavelet and time domain**", ICT International Conference, No.3, PP. 47–50, March 2014

[3] S.Wu, J.Huang, "**Efficiently self-synchronized audio watermarking for assured audio data transmission**", IEEE Transaction on Broadcasting, Vol. 51, No. 1, PP 69-76, MARCH 2005