



بهبود امنیت در واترمارکینگ اصوات دیجیتال

فاطمه ایل بیگی^۱، سعید شعراف تبریزی^۲

^۱دانشجوی کارشناسی ارشد دانشگاه بین المللی امام رضا(ع)، filbeigi@imamreza.ac.ir

^۲استادیار دانشگاه بین المللی امام رضا(ع)، shaerbaf@imamreza.ac.ir

چکیده

واترمارکینگ یا پنهان نگاری صوتی تکنیک پنهان سازی داده در یک سیگنال صوتی (سیگنال میزبان) به منظور دستیابی به اهدافی مانند حفاظت یا محدود کردن حق کپی، پنهان کردن اطلاعات، ردیابی اطلاعات و... است. در این مقاله یک روش پنهان نگاری صوتی مقاوم غیر کور جهت دستیابی به شفافیت بالا بر اساس تبدیل کسینوسی گسسته، تبدیل موجک گسسته و تجزیه نقاط منفرد ارائه شده است. در این روش یک تصویر باینری (واترمارک) با استفاده از تبدیل موجک گسسته^۱ و تبدیل کسینوسی گسسته^۲ در سه درایه از ماتریس مقادیر ویژه^۳ که بیشترین مقدار را دارند جایگذاری میشود که این امر باعث بالا رفتن امنیت ارسال میشود چراکه به جای ارسال یک نمونه از هر بیت سه نمونه از آن ارسال میشود و اگر در اثر عواملی یک یا دو بیت از تصویر در هر ارسال از بین بروند بیت سوم صحیح به مقصد می رسد و در نتیجه تصویر واترمارک حفظ می شود. نتایج شبیه سازی ها نشان دهنده شفافیت بالای سیگنال صوتی واترمارک شده و مقاومت بسیار خوب این تکنیک در مقابل حملات مختلف پردازش سیگنال میباشد که کیفیت سیگنال صوتی را در برابر حملات حفظ می کند.

واژه های کلیدی: واترمارکینگ صوت، تجزیه به مقادیر

منفرد، تبدیل موجک گسسته، استخراج غیر کور

۱. مقدمه

با رشد سریع فناوری دیجیتال و به ویژه اینترنت و شبکه های اجتماعی، محصولات دیجیتال چندرسانه ای (تصویر، صوت، ویدئو و...) به آسانی از طریق این شبکه بین افراد مختلف به اشتراک گذاشته شوند، این گونه انتقال اطلاعات می تواند مشکلاتی مانند دستکاری، کپی برداری و توزیع غیر مجاز آثار برای ناشرانی که نمی خواهند آثارشان بدون اجازه خودشان پخش شود ایجاد کند. پنهان نگاری روشی است که در آن یک سیگنال پنهان نگاره یا واترمارک در سیگنال میزبان قرار میگیرد. پنهان نگاره میتواند یک متن، تصویر یا صوت باشد که به صورت پنهان یا آشکار در سیگنال صوتی میزبان پنهان می شود.

لازمه اجرای صحیح یک الگوریتم پنهان نگاری صوتی سه معیار شفافیت، مقاومت و ظرفیت است. که در تقابل با یکدیگر می باشند و بسته به نیاز کاربر تعیین می شوند الگوریتم واترمارکینگ نمی تواند تمام ویژگی های لازم برای تمامی کاربردها را داشته باشد و بسته به کاربرد، بهترین الگوریتم های واترمارکینگ انتخاب می شوند. منظور از شفافیت نداشتن تفاوت محسوس بین کیفیت شنیداری سیگنال صوتی واترمارک شده با سیگنال صوتی اصلی است. مقاومت برای یک سیستم پنهان نگاری توانایی آشکارسازی واترمارک برای استخراج واترمارک تعبیه شده پس از اعمال حملات مختلف که برای برداشتن واترمارک صورت گرفته، است. همچنین به تعداد بیت پنهان شده در یک ثانیه از سیگنال صوتی ظرفیت گفته میشود.

تاکنون روش های متعددی در زمینه پنهان نگاری ارائه شده است به عنوان مثال تائو وهمکاران [15] در سال ۲۰۱۰ یک روش پنهان نگاری صوتی براساس دامنه فرکانسی lwt ارائه دادند که در این روش واترمارک درون ضرایب lwt قرار میگیرند. در [7] روشی با استفاده از مکانیسم پوشش فرکانسی برای پنهان کردن متن در سیگنال صحبت پیشنهاد شده است. در این روش هر نمونه از پیام مخفی در یک بخش فرکانسی سیگنال میزبان به شرط رسیدن به یک سطح آستانه مشخص، مخفی می شود، با این کار کیفیت خوب سیگنال واترمارک شده تضمین می شود زیرا تعداد بیت های جایگزین شده در سیگنال میزبان محدود به سطح اعوجاج می شود

روشی دیگر با استفاده از پوشش موجک مؤثر در [18] پیشنهاد شده است. ابتدا از هر دو سیگنال میزبان و سیگنال پیام مخفی تبدیل موجک گرفته می شود سپس ضرایب موجک بر اساس یک آستانه به دو دسته بامعنی و بدون معنی تقسیم می شوند. ضرایب بامعنی پائین نمی توانند انرژی بامعنی برای سیگنال فراهم آورند بنابراین آنها صفر در نظر گرفته می شوند. در عمل اگر زمان غیر خاموشی سیگنال پیام مخفی کمتر یا مساوی زمان غیر خاموشی سیگنال میزبان باشد، پیام مخفی مشابه پیام سیگنال میزبان اصلی به نظر می رسد

گروهی از نویسندگان [13] یک روش تطبیقی با استفاده از تبدیل موجک و آنتروپی ارائه داده اند اما این طرح مقاومت پایینی در برابر حملاتی مثل فیلتر کردن و نمونه برداری مجدد دارد.

در این مقاله سعی شده است سیستم واترمارکینگ مقاوم با شفافیت بالا و ظرفیت قابل قبول طراحی شود. علت جایگذاری در سه درایه

¹Discrete Wavelet Transform

²Discrete Cosine Transform

³Singular value decomposition