

## طراحی یک روش جدید برای نهان‌نگاری صوت با الگوریتم کلونی مورچگان در حوزه تبدیل

نجمه احمدی<sup>۱</sup>، مرتضی زلف پور آرخلو<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد، دانشکده مهندسی، دانشگاه آزاد اسلامی واحد سپیدان، سپیدان، ایران.

<sup>۲</sup> استادیار، دانشکده مهندسی، دانشگاه آزاد اسلامی واحد سپیدان، سپیدان، ایران.

نام نویسنده مسئول:

نجمه احمدی

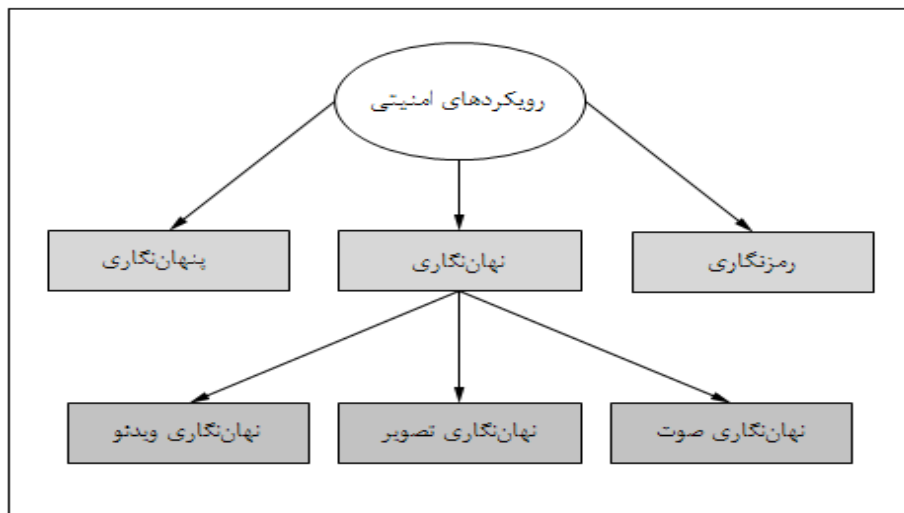
### چکیده

نهان‌نگاری یک سیگنال پنهان است که مستقیماً در داخل داده جاسازی می‌شود و همیشه در آن باقی می‌ماند و باعث بالا رفتن امنیت داده‌ها می‌شود. تکنیک نهان‌نگاری با توجه به نوع رسانه استفاده شده به سه دسته نهان‌نگاری صوت، نهان‌نگاری تصویر و نهان‌نگاری ویدئو تقسیم‌بندی می‌شود. در نهان‌نگاری صوت معمولاً یک داده نهان‌نگار تصویری در یک سیگنال صوتی مخفی می‌گردد. در این مقاله، یک روش جدید برای نهان‌نگاری صوت ارائه شده است. در روش ترکیبی پیشنهادی از الگوریتم‌های بهینه‌سازی کلونی مورچگان، تجزیه مقادیر منفرد، تبدیل موج گسسته، تبدیل فوریه گسسته و تبدیل کسینوسی گسسته بهره برده شده است. ابتدا استراتژی حل مساله و تعیین فلوجارت کلی مساله بیان شده و پس از طراحی روش نهان‌نگاری صوت پیشنهادی، روش مورد نظر توسط نرم‌افزار متلب پیاده‌سازی گردیده و نتایج حاصل از پیاده‌سازی روی چند دیتابیس تست شده و مورد بحث و بررسی قرار گرفته است. نتایج بدست آمده نشان داد که روش نهان‌نگاری صوت پیشنهادی در برابر تست‌های شنیداری، عینی و استحکام و مقاومت از عملکرد مطلوبی برخوردار می‌باشد.

**واژگان کلیدی:** نهان‌نگاری، نهان‌نگاری صوت، الگوریتم کلونی مورچگان، الگوریتم تجزیه مقادیر منفرد

## مقدمه

با توجه به گسترش روز افزون اینترنت به عنوان محیطی مناسب برای انتقال سریع و آسان انواع اطلاعات، مفهوم امنیت اطلاعات بیش از پیش مورد توجه قرار گرفته است. اطلاعات مخابره شده در اینترنت دارای کاربردهای گوناگونی همانند کاربردهای تجاری، نظامی و علمی هستند که نیازمند حفاظت جدی در همه کاربردها می‌باشند. روش‌های مختلفی برای حفاظت از اطلاعات ارسالی در شبکه اینترنت وجود دارد که از جمله مهم‌ترین آن‌ها می‌توان به رمزنگاری (کریپتوگرافی)، پنهان‌نگاری (استگانوگرافی) و پنهان‌نگاری (واترمارکینگ) اشاره نمود [۱]. رمزنگاری علمی است که در آن پیام سری بگونه‌ای دچار تغییر و بهم‌ریختگی می‌شود که توسط یک شخص سوم یا همان مهاجم فرضی قابل فهم و درک نباشد. پنهان‌نگاری علمی است که در آن پیام سری در یک رسانه پوششی با استفاده از رویکردی مشخص، جانمایی می‌شود بگونه‌ای که مهاجم فرضی قادر به تشخیص وجود پیام سری در رسانه پوششی نمی‌باشد. پنهان‌نگاری شاخه‌ای از علم پنهان‌نگاری است که به عنوان یک روش مناسب برای حفاظت کپی‌رایت و جلوگیری از تکثیر غیر قانونی شناخته می‌شود. استفاده از تکنیک پنهان‌نگاری در شبکه اینترنت به دلیل حفاظت از اطلاعات در برابر جعل و کپی برداری از اهمیت بسیار بالایی برخوردار است. بطور کلی پنهان‌نگاری از دو فاز اصلی جانمایی و استخراج تشکیل شده است. در فاز جانمایی، داده پنهان‌نگار که می‌تواند یک لوگو، شماره آی دی و یا امضاء نویسنده باشد در یک رسانه پوششی مخفی می‌گردد، بگونه‌ای که تاثیری بر کیفیت رسانه پوششی ایجاد ننماید. در فاز استخراج، مالک می‌تواند برای بیان حق کپی‌رایت، داده پنهان‌نگار را از رسانه پوششی، آشکار نماید. تکنیک پنهان‌نگاری بسته به نوع رسانه پوششی استفاده شده به سه دسته پنهان‌نگاری صوت، پنهان‌نگاری تصویر و پنهان‌نگاری ویدئو تقسیم‌بندی می‌گردد [۲]. در شکل ۱، شمای کلی رویکردهای امنیتی در شبکه اینترنت نشان داده شده است.



شکل ۱: رویکردهای امنیتی در شبکه اینترنت

همانطور که مشخص است، تمرکز اصلی در این مقاله بر روی پنهان‌نگاری صوت می‌باشد. در پنهان‌نگاری صوت تلاش خواهد شد که یک داده پنهان‌نگار در سیگنال‌های صوتی مخفی و پنهان گردد. اساس و مبنای کار در پنهان‌نگاری صوت، خصوصیات شنوایی انسان می‌باشد. یک روش پنهان‌نگاری صوت باید بتواند در برابر استخراج غیر مجاز داده پنهان‌نگار، از بین بردن داده پنهان‌نگار، تغییر داده پنهان‌نگار و مخدوش کردن داده پنهان‌نگار مقاوم باشد و در برابر این حملات از استحکام لازم و کافی برخوردار باشد. بطور کلی، روش‌های مختلف پنهان‌نگاری صوت را می‌توان به دو گروه روش‌های مبتنی بر حوزه زمان و روش‌های مبتنی بر حوزه تبدیل تقسیم‌بندی نمود [۳]. پیاده‌سازی روش‌های پنهان‌نگاری صوت مبتنی بر حوزه زمان ساده‌تر و راحت‌تر است، ولیکن، استحکام این دست از روش‌ها در برابر حملات مختلف کمتر می‌باشد. در طرف مقابل، پیاده‌سازی روش‌های پنهان‌نگاری صوت مبتنی بر حوزه تبدیل دشوار است، ولی میزان مقاومت این دست از روش‌ها در برابر حملات مختلف بالا می‌باشد. هدف اصلی از این مقاله طراحی یک روش ترکیبی جدید برای پنهان‌نگاری صوت مبتنی بر حوزه تبدیل می‌باشد. در روش ترکیبی پیشنهادی از الگوریتم بهینه‌سازی کلونی مورچگان (ACO)، الگوریتم تجزیه مقادیر منفرد (SVD)، تبدیل ویولت گسسته (DWT) و تبدیل کسینوسی گسسته (DCT) بهره برده خواهد شد.

<sup>1</sup> Ant Colony Optimization

<sup>2</sup> Singular Value Decomposition

<sup>3</sup> Discrete Wavelet Transform

این مقاله در پنج بخش سازمان‌دهی شده است. در بخش دوم مروری بر مهم‌ترین کارهای انجام شده در زمینه نهان‌نگاری صوت صورت خواهد پذیرفت. در بخش سوم یک روش ترکیبی جدید برای نهان‌نگاری صوت مبتنی بر حوزه تبدیل طراحی خواهد شد. در بخش چهارم، روش طراحی شده پیاده‌سازی گشته و نتایج حاصل از پیاده‌سازی مورد بحث و بررسی قرار خواهند گرفت. نهایتاً در بخش پنجم نتیجه‌گیری از مطالب عنوان شده ارائه خواهد شد.

## ۱- مطالعات انجام شده

همانطور که عنوان شد، روش‌های مختلف نهان‌نگاری صوت به دو گروه روش‌های مبتنی بر حوزه زمان و روش‌های مبتنی بر حوزه تبدیل تقسیم‌بندی می‌شوند. از آنجاییکه روش‌های نهان‌نگاری صوت مبتنی بر حوزه تبدیل از سطح امنیت بالاتری نسبت به روش‌های نهان‌نگاری صوت مبتنی بر حوزه زمان برخوردار هستند، لذا تمرکز اصلی بر روی این دست از روش‌ها می‌باشد. در واقع، در این بخش برخی از مهم‌ترین و جدیدترین روش‌های نهان‌نگاری صوت مبتنی بر حوزه تبدیل ارائه خواهند شد. در سال ۲۰۱۱ نوامی و همکارانش یک روش جدید نهان‌نگاری صوت مبتنی بر حوزه تبدیل ارائه نمودند [۴]. در روش ارائه شده توسط آن‌ها از الگوریتم تجزیه مقادیر منفرد و توابع آشوبگون بهره برده شده است. در این روش، داده نهان‌نگار یک تصویر دیجیتالی می‌باشد که این تصویر دیجیتالی توسط توابع آشوبگون رمزگذاری می‌گردد. تصویر رمز شده بدست آمده توسط الگوریتم تجزیه مقادیر منفرد در یک سیگنال صوتی مخفی و پنهان می‌شود. این روش بدلیل استفاده از توابع آشوبگون جهت رمزگذاری داده نهان‌نگار تصویری از سطح امنیت بسیار بالایی برخوردار است. در سال ۲۰۱۱ پنگ و همکارش یک روش جدید نهان‌نگاری صوت مبتنی بر حوزه تبدیل ارائه نمودند [۵]. در روش ارائه شده توسط آن‌ها از الگوریتم ژنتیک بهره گرفته شده است. در این روش با بکارگیری الگوریتم ژنتیک امکان بهینه‌سازی چند پارامتر مختلف فراهم شده است. به عبارت دیگر، در این روش الگوریتم ژنتیک تعادلی بین دو پارامتر شفافیت و امنیت برقرار نموده است. الگوریتم ژنتیک به صورت اتوماتیک جانمایی بهینه برای هر فریم از یک سیگنال صوتی را فراهم می‌آورد. نتایج بدست آمده از اجرای این روش نشان داد که علاوه بر جانمایی بهینه داده نهان‌نگار در سیگنال صوتی، سرعت اجرای الگوریتم نیز در مقایسه با سایر روش‌ها افزایش یافته است. در سال ۲۰۱۱ بهات و همکارانش یک روش نهان‌نگاری صوت مبتنی بر حوزه تبدیل ارائه نمودند [۶]. در روش پیشنهاد شده توسط آن‌ها از الگوریتم تجزیه مقادیر منفرد و مدولاسیون اندیس کوانتیزاسیون بهره برده شده است. در این روش بیت‌های نهان‌نگار با استفاده از تکنیک مدولاسیون اندیس کوانتیزاسیون در مقادیر منفرد بلوک‌های سیگنال صوتی جانمایی می‌شوند. در فاز استخراج، بیت‌های نهان‌نگار بدون نیاز به سیگنال صوتی اصلی می‌توانند استخراج شوند. در سال ۲۰۱۳ میشرای و همکارش یک روش نهان‌نگاری صوت مبتنی بر حوزه تبدیل ارائه نمودند [۷]. در این روش از دو تابع ریاضی تجزیه مقادیر منفرد و تبدیل ویولت گسسته استفاده شده است. در این روش، فازهای جانمایی و استخراج به کمک الگوریتم تجزیه مقادیر منفرد و با استفاده از تبدیل ویولت گسسته صورت می‌پذیرد. در سال ۲۰۱۶ لالیتا و همکارانش یک روش جدید نهان‌نگاری صوت مبتنی بر حوزه تبدیل با ظرفیت بالا طراحی نمودند [۸]. در روش پیشنهاد شده توسط آن‌ها از الگوریتم تجزیه مقادیر منفرد، تبدیل ویولت گسسته و تبدیل کسینوسی گسسته استفاده شده است. در این روش، فازهای جانمایی و استخراج به کمک الگوریتم تجزیه مقادیر منفرد صورت می‌پذیرد. سپس با کمک الگوریتم تجزیه مقادیر منفرد و با استفاده از تبدیل ویولت گسسته و تبدیل کسینوسی گسسته سعی در بالا بردن سطح امنیت نموده است، بگونه‌ای که کمترین تغییرات در سیگنال صوتی ایجاد شود. نقطه اشتراک روش‌های معرفی شده آن است که همگی در حوزه تبدیل عملیات جانمایی و استخراج را انجام می‌دهند. در جدول ۱، نتایج مقایسه بین روش‌های معرفی شده نشان داده شده است. برای مطالعه بیشتر در خصوص روش‌های نهان‌نگاری صوت مبتنی بر حوزه تبدیل می‌توانید به مراجع [۹،۱۰،۱۱] مراجعه نمایید.

جدول ۱: مقایسه روش‌های نهان‌نگاری صوت

شماره	نام نویسنده اول	سال انتشار	نوع حوزه	تکنیک‌های استفاده شده
۱	نوامی	۲۰۱۱	تبدیل	تجزیه مقادیر منفرد، توابع آشوبگون
۲	پنگ	۲۰۱۱	تبدیل	الگوریتم ژنتیک
۳	بهات	۲۰۱۱	تبدیل	تجزیه مقادیر منفرد، مدولاسیون اندیس کوانتیزاسیون
۴	میشرای	۲۰۱۳	تبدیل	تجزیه مقادیر منفرد، تبدیل ویولت گسسته

تجزیه مقادیر منفرد، تبدیل ویولت گسسته، تبدیل کسینوسی گسسته	تبدیل	۲۰۱۶	لالیتا	۵
---	-------	------	--------	---

## ۲- روش پیشنهادی

در این بخش، یک روش ترکیبی برای نهان‌نگاری صوت در حوزه تبدیل ارائه خواهد شد. در روش ترکیبی پیشنهادی از الگوریتم بهینه‌سازی کلونی مورچگان، الگوریتم تجزیه مقادیر منفرد، تبدیل ویولت گسسته و تبدیل کسینوسی گسسته استفاده می‌شود. نکته قابل توجه آن است که در روش نهان‌نگاری پیشنهادی، داده نهان‌نگار یک تصویر باینری خواهد بود.

## ۲-۱- فاز جانمایی

در این بخش، فاز جانمایی نهان‌نگاری صوت مبتنی بر الگوریتم تجزیه مقادیر منفرد، تبدیل ویولت گسسته و تبدیل کسینوسی گسسته بیان خواهد شد. در این فاز داده نهان‌نگار، تصویر باینری  $W$  می‌باشد که قرار است در سیگنال صوتی  $F$  پنهان و مخفی گردد. در ادامه مراحل فاز جانمایی بیان خواهند شد.

گام ۱: داده نهان نگار  $W$  که دارای ابعاد  $M \times M$  است به بردار تک بعدی  $G$  به طول  $M \times M$  تبدیل می‌شود. بردار  $G$  در رابطه شماره یک نشان داده شده است.

$$G = \{G_1, G_2, G_3, \dots, G_{M \times M}\} \quad (1)$$

گام ۲: سیگنال صوتی  $F$  به فریم‌هایی که با یکدیگر تداخل ندارند، تقسیم‌بندی می‌شود. فریم‌های سیگنال صوتی  $F$  در رابطه شماره دو نشان داده شده است.

$$F = \{F_1, F_2, F_3, \dots, F_{M \times M}\} \quad (2)$$

گام ۳: تبدیل ویولت گسسته به هر یک از فریم‌های سیگنال صوتی  $F$  اعمال می‌شود و ضرایب فرکانس پایین و ضرایب فرکانس بالا تخمین زده می‌شود.

گام ۴: تبدیل کسینوسی گسسته به ضرایب تخمین زده شده، اعمال می‌شود و در نتیجه اعمال تبدیل کسینوسی گسسته، ماتریس  $X$  ایجاد می‌گردد.

گام ۵: یک الگوریتم تجزیه مقادیر منفرد به ماتریس بدست آمده در گام قبل (ماتریس  $X$ ) اعمال می‌گردد. این مسئله در رابطه شماره سه نشان داده شده است.

$$X = U_X \cdot S_X \cdot V_X^T \quad (3)$$

گام ۶: گام‌های سه و چهار بر روی داده نهان‌نگار  $W$  اعمال می‌شود و ماتریس نهان‌نگار  $W_c$  ایجاد می‌گردد. سپس یک الگوریتم تجزیه مقادیر منفرد به ماتریس نهان‌نگار  $W_c$  اعمال می‌شود. این مسئله در رابطه شماره چهار نشان داده شده است.

$$W_c = U_{W_c} \cdot S_{W_c} \cdot V_{W_c}^T \quad (4)$$

گام ۷: توابع درهم سازی یک طرفه برای ماتریس‌های  $U_{W_c}$  و  $V_{W_c}$  محاسبه می‌گردد. این مسئله در روابط شماره پنج و شش نشان داده شده است.

$$H_U = \text{hash}(U_{W_c}) \quad (5)$$

$$H_V = \text{hash}(V_{W_c}) \quad (6)$$

گام ۸: ماتریس‌های  $U_{W_c}$  و  $V_{W_c}$  و همچنین مقادیر درهم ساز  $H_U$  و  $H_V$  در کلید خصوصی ذخیره می‌شوند.

گام ۹: بر اساس رابطه شماره هفت، ماتریس  $S_Y$  ساخته می‌شود. در این رابطه  $\alpha$  عامل قدرت نهان‌نگار می‌باشد که رابطه میان کیفیت بصری و استحکام از طرح نهان‌نگاری را کنترل می‌کند.

$$S_Y = S_X + \alpha \cdot S_{W_c} \quad (7)$$

گام ۱۰: بر اساس رابطه شماره هشت، ماتریس  $Z_W$  ساخته خواهد شد.

$$Z_W = U_X \cdot S_Y \cdot V_X^T \quad (8)$$

گام ۱۱: معکوس تبدیل کسینوسی گسسته و سپس معکوس تبدیل ویولت گسسته به ماتریس  $Z_W$  اعمال می‌گردد و سپس

سیگنال صوتی نهان‌نگاری شده  $X_W$  تولید می‌شود. این مسئله در رابطه شماره نه نشان داده شده است.

$$X_W = DWT^{-1} (DCT^{-1} (Z_W)) \quad (9)$$

## ۲-۲- فاز استخراج

در این بخش، فاز استخراج نهان‌نگاری صوت مبتنی بر الگوریتم تجزیه مقادیر منفرد، تبدیل ویولت گسسته و تبدیل کسینوسی گسسته بیان خواهد شد. نکته‌ای که باید به آن اشاره نمود آن است که روش نهان‌نگاری صوت پیشنهادی یک روش کور نمی‌باشد. لذا برای اجرای فاز استخراج به سیگنال صوتی اصلی نیاز است.

گام ۱: در اولین گام باید تست ایمنی اجرا شود. یعنی فرض بر آن است که یک مهاجم قصد انجام عملیات استخراج را دارد. مهاجم برای اجرای عملیات استخراج باید دو مقدار درهم ساز  $H_U$  و  $H_V$  را بدست آورد. اگر مقادیر درهم ساز بدست آمده از طرف مهاجم  $H_{\bar{U}}$  و  $H_{\bar{V}}$  فرض شود و ماتریس‌های  $U_{WC}$  و  $V_{WC}$  به صورت  $\tilde{U}_W$  و  $\tilde{V}_W$  در نظر گرفته شوند، شرط ذیل مورد بررسی قرار می‌گیرد.

$$\begin{cases} \text{if } H_U = H_{\bar{U}} \text{ and } H_V = H_{\bar{V}} & \text{go to step 1} \\ \text{if } H_U \neq H_{\bar{U}} \text{ or } H_V \neq H_{\bar{V}} & \text{stop} \end{cases} \quad (10)$$

گام ۲: تبدیل ویولت گسسته به سیگنال صوتی اصلی  $F$  و سیگنال صوتی نهان‌نگاری شده  $X_W$  اعمال می‌گردد و ضرایب فرکانس پایین و ضرایب فرکانس بالا تخمین زده می‌شود.

گام ۳: تبدیل کسینوسی گسسته به ضرایب تخمین زده شده از سیگنال صوتی اصلی  $F$ ، اعمال می‌شود و ماتریس  $X_I$  ایجاد می‌گردد. همچنین، تبدیل کسینوسی گسسته به ضرایب تخمین زده شده از سیگنال صوتی نهان‌نگاری شده  $X_W$ ، اعمال می‌شود و ماتریس  $X_{IW}$  ایجاد می‌گردد.

گام ۴: یک الگوریتم تجزیه مقادیر منفرد به ماتریس  $X_I$  اعمال می‌گردد. این مسئله در رابطه شماره یازده نشان داده شده است.

$$X_I = U_{X_I} \cdot S_{X_I} \cdot V_{W_I}^T \quad (11)$$

گام ۵: یک الگوریتم تجزیه مقادیر منفرد به ماتریس  $X_{IW}$  اعمال می‌گردد. این مسئله در رابطه شماره دوازده نشان داده شده است.

$$X_{IW} = U_{X_{IW}} \cdot S_{X_{IW}} \cdot V_{W_{IW}}^T \quad (12)$$

گام ۶: ماتریس  $S_{W_C}$  از طریق رابطه شماره سیزده محاسبه می‌گردد.

$$S_{W_C} = \frac{S_{X_{IW}} - S_{X_I}}{\alpha} \quad (13)$$

گام ۷: نهان‌نگار رمز شده تخمین زده شده  $\hat{W}_C$ ، به وسیله محاسبه رابطه شماره چهارده بدست می‌آید.

$$\hat{W}_C = \tilde{U}_{W_C} \cdot S_{W_C} \cdot \tilde{V}_{W_C}^T \quad (14)$$

## ۲-۳- بهبود با الگوریتم بهینه‌سازی کلونی مورچگان

در این بخش، روش نهان‌نگاری صوت پیشنهادی با استفاده از الگوریتم بهینه‌سازی کلونی مورچگان بهبود خواهد یافت. در ادامه، مراحل اعمال الگوریتم بهینه‌سازی کلونی مورچگان به روش پیشنهاد شده بیان خواهد شد.

گام ۱: گام اول مربوط به مقداردهی اولیه به پارامترها می‌باشد. در واقع، اندازه کلونی، دنباله فرومون اولیه، نرخ انحلال ( $\sigma$ ) و تعداد نسل به عنوان معیار برای توقف الگوریتم باید مقداردهی شوند.

گام ۲: با استفاده از رابطه شماره پانزده یک جمعیت اولیه از مورچه‌ها به صورت تصادفی تولید می‌شود که مجموعه‌ای از راه‌حل‌های بالقوه را تشکیل می‌دهند. هر مورچه به صورت  $X = \{x_1, x_2, \dots, x_n\}$  نشان داده می‌شود. در رابطه زیر،  $x_i^*$  مختصات  $i$ ام از بهترین نقطه یافت شده به وسیله بهینه‌ساز درون فضای طراحی در تکرار فعلی است و  $\sigma_i$  شاخص تراکم مورچه‌ها برای مختصات  $i$ ام از فضای طراحی می‌باشد. در تکرار اول،  $x_i^*$  مطابق با یک توزیع یکنواخت با  $\sigma_i$  گرفته شده، حداقل ۳ مرتبه بزرگتر از طول فاصله جستجو انتخاب می‌شود.

$$f_{\text{pheromone}}(x_i) = e^{-\frac{(x_i - x_i^*)^2}{\sigma_i^2}} \quad (15)$$

گام ۳: برای هر مورچه  $X$  از جمعیت باید مراحل ذیل به ترتیب اعمال شوند.

۱. تولید داده نهان نگار  $X_w$  بر اساس فاز جانمایی و با استفاده از مورچه  $X$  به عنوان عامل قدرت نهان نگار. با توجه به این مسئله، رابطه شماره هفت در فاز جانمایی باید به رابطه شماره شانزده تبدیل شود. در رابطه شماره شانزده،  $\text{diag}(\alpha)$  ماتریس قطری ایجاد شده از مورچه  $X$  می‌باشد.

$$S_Y = S_X + \text{diag}(\alpha) \cdot S_{W_C} \quad (16)$$

۲. محاسبه همبستگی نرمال  $NC(X, X_w)$  بین تصویر اصلی و تصویر نهان نگاری شده  $X$  و  $X_w$

۳. اعمال یک حمله نهان نگار خارج از یک مجموعه از  $T$  حمله انتخاب شده روی تصویر نهان نگاری شده  $X_w$ . این منجر می‌شود

به  $T$  حمله مختلف تصاویر نهان نگاری شده  $\{\tilde{X}_w\}$  برای هر تصویر نهان نگاری شده اصلی  $I_w$

۴. استخراج نهان نگارهای  $\tilde{W}_i$  از تصاویر نهان نگاری شده حمله شده  $\tilde{X}_w$  با استفاده از فاز استخراج  $i$  که  $i = \{1, 2, \dots, T\}$

۵. محاسبه ضرایب همبستگی نرمالیزه شده بین نهان نگار اصلی  $W$  و مجموعه‌ای از نهان نگارهای استخراج شده  $\{\tilde{W}_i\}$ .

۶. ساخت بردار از مقادیر هدف،  $F(X)$ ، بر اساس رابطه شماره هفده

$$F(X) = \begin{pmatrix} \overline{NC(X, X_w)} \\ \overline{NC(W, \tilde{W}_1)} \\ \overline{NC(W, \tilde{W}_2)} \\ \vdots \\ \overline{NC(W, \tilde{W}_T)} \end{pmatrix} \quad (17)$$

۷. ارزیابی بردار مقادیر هدف مطابق با روش وزندهی نمائی برای بهینه‌سازی چندهدفه بر اساس رابطه شماره هجده

$$F_{obj}(X) = \sum_{i=1}^{T+2} (e^{p \cdot \omega} - 1) \cdot e^{p \cdot (F(X) - F_i)} \quad (18)$$

گام ۴: پیدا کردن بهترین مورچه  $X_{best} = \{x_1^*, x_2^*, \dots, x_n^*\}$  به عنوان برداری که کوچکترین مقدار هدف  $F_{obj}$  را دارد.

گام ۵: بروزرسانی توزیع دنباله فرمون با استفاده از رابطه شماره پانزده. در این مرحله شاخص تراکم برای  $i$  امین بعد  $\sigma_i$  به وسیله

رابطه شماره نوزده محاسبه می‌گردد. در این رابطه،  $y$  نشان‌دهنده  $i$  امین ستون از ماتریس کلونی  $C$ ،  $\bar{y}$  مقدار میانگین از بردار  $y$  و  $m$  تعدادی از اندازه کلونی می‌باشد.

$$\sigma_i = \sqrt{\frac{1}{m} \sum_{i=1}^m y_i - \bar{y}} \quad (19)$$

گام ۶: ذخیره بهترین مورچه  $X_{best}$  بین این نسل و یک نسل قدیمی.

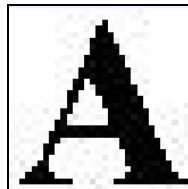
گام ۷: اگر تعداد نسل به مقدار بهینه برسد فرآیند از عوامل مقیاس‌بندی ضربی (MSF) خاتمه یافته است، در غیر اینصورت به

مرحله بعد می‌رود.

گام ۸: با استفاده از رابطه شماره پانزده یک جمعیت جدید از مورچه‌ها تولید می‌شود و سپس بازگشت به گام سوم خواهد داشت.

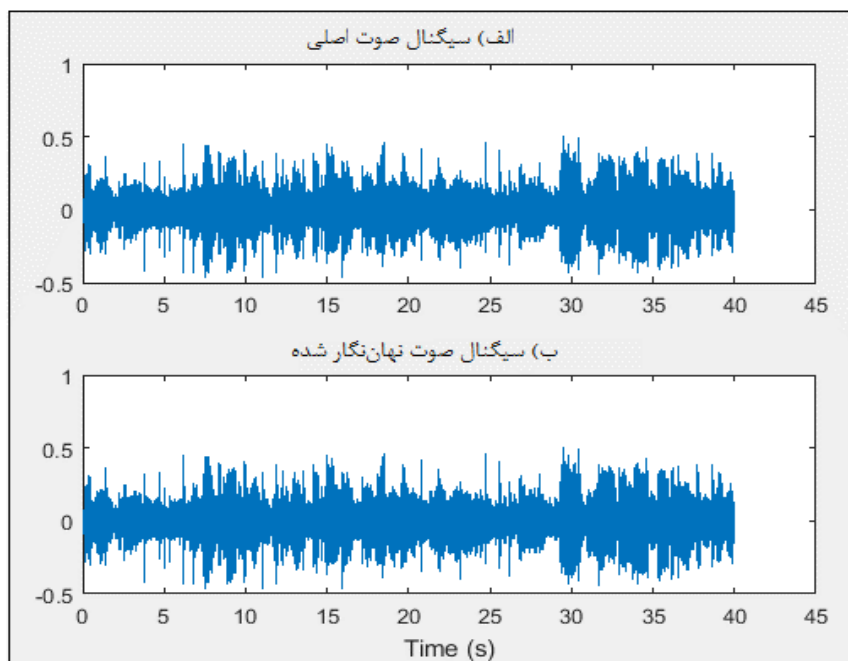
### ۳- پیاده سازی و ارزیابی روش پیشنهادی

در بخش قبل، یک روش ترکیبی برای نهان نگاری صوت مبتنی بر حوزه تبدیل طراحی گردید. در این بخش روش نهان نگاری صوت پیشنهادی توسط نرم افزار متلب پیاده سازی گشته و نتایج حاصل از پیاده سازی مورد ارزیابی قرار خواهد گرفت. به منظور پیاده سازی روش نهان نگاری صوت پیشنهادی، سه سیگنال صوتی مونو ۱۶ بیتی (پاپ، محلی و جاز) نمونه گیری شده در ۴۴,۱ کیلوهرتز در نظر گرفته شده است. فرمت فایل های صوتی به صورت WAV می باشد. همچنین، هر فایل صوتی شامل ۲۶۲,۱۴۴ نمونه (مدت زمان ۵,۹۴ ثانیه) است که هر سیگنال صوتی به فریم هایی با سایز ۲۵۶ نمونه تقسیم شده است. در هر فریم از سیگنال صوتی، یک بیت از داده نهان نگار مخفی می شود. داده نهان نگار یک تصویر باینری با ابعاد ۳۲×۳۲ می باشد که در شکل ۲ نشان داده شده است.



شکل ۲: داده نهان نگار تصویری

داده نهان نگار مورد نظر در سیگنال های صوتی معرفی شده بر اساس الگوریتم طراحی شده، مخفی می گردد. در شکل ۳، چهل ثانیه از سیگنال صوتی اصلی و سیگنال صوتی نهان نگاری شده، نشان داده شده است. همانطور که مشخص است، جزئی بودن تغییرات در سیگنال صوتی نهان نگاری شده نسبت به سیگنال اصلی کاملاً مشهود می باشد. به منظور ارزیابی دقیق این مسئله تست های مختلفی بر روی روش پیشنهادی اعمال خواهد شد.



شکل ۳: سیگنال صوتی اصلی و سیگنال صوتی نهان نگاری شده

### ۳-۱- تست شنیداری

به منظور تست شنیداری روش نهان نگاری پیشنهادی، صوت اصلی و صوت نهان نگاری شده به صورت تصادفی برای یک گروه ۱۰ نفره متشکل از افرادی با سنین مختلف، پخش گردید. در واقع، با انجام این تست تلاش می شود تا کیفیت ادراکی از سیگنال صوتی نهان نگاری شده، ارزیابی گردد. هر یک از نفرات بر اساس میزان کیفیت ادراکی از عدد یک الی پنج به روش نهان نگاری پیشنهادی نمره دادند. نمره یک نشان دهنده کیفیت پایین و نمره پنج نشان دهنده کیفیت بالا می باشد. متوسط نمرات نفرات تحت عنوان MOS بیان می گردد. در

جدول ۲ نتایج بدست آمده از اجرای تست شنیداری نشان داده شده است. همانطور که مشخص است، با توجه به متوسط نمرات نفرات می-توان عنوان داشت که روش نهان‌نگاری صوت پیشنهادی از نقطه نظر تست شنیداری از عملکرد بالایی برخوردار است.

جدول ۲: نتایج بدست آمده در تست شنیداری

نوع سیگنال صوتی	تعداد نفرات شرکت‌کننده در تست	MOS
پاپ	۱۰ نفر	۴/۹
جاز	۱۰ نفر	۵
راک	۱۰ نفر	۵

### ۳-۲- تست عینی

تست عینی یکی دیگر از تست‌های مرسوم در ارزیابی روش‌های نهان‌نگاری صوت می‌باشد. کیفیت عینی یک سیگنال صوتی نهان-نگاری شده با SNR نشان داده می‌شود که از طریق رابطه شماره بیست قابل محاسبه است. در این رابطه،  $x(n)$  و  $x^*(n)$  به ترتیب سیگنال صوتی اصلی و سیگنال صوتی نهان‌نگاری شده می‌باشند. نکته قابل توجه آن است که مقدار بدست آمده برای SNR باید بالای ۲۰ دسی بل باشد تا به سطح استاندارد IFPI برسد.

$$SNR = 10 \cdot \log_{10} \frac{\sum_{n=1}^L x^*(n)}{\sum_{n=1}^L [x(n) - x^*(n)]} \quad (20)$$

در جدول ۳ نتایج بدست آمده از اجرای تست عینی نشان داده شده است. همانطور که مشخص است، نتایج بدست آمده برای معیار SNR بسیار بالا می‌باشد که نشان‌دهنده عملکرد مطلوب روش نهان‌نگاری صوت پیشنهادی است. در واقع، روش نهان‌نگاری صوت پیشنهادی از نقطه نظر تست عینی به استانداردهای مورد نظر رسیده است.

جدول ۳: نتایج بدست آمده در تست عینی

نوع سیگنال صوتی	تعداد فریم‌های هر سیگنال	SNR
پاپ	۱۰۲۴	۳۹/۰۸
جاز	۱۰۲۴	۴۱/۸۰
راک	۱۰۲۴	۴۲/۱۴

### ۳-۳- تست استحکام

پس از بررسی کیفیت سیگنال صوتی نهان‌نگاری شده، با اعمال یک سری از عملیات پردازش سیگنال، مقاومت و استحکام روش نهان‌نگاری پیشنهادی مورد بررسی قرار خواهد گرفت. به منظور بررسی میزان استحکام روش نهان‌نگاری صوت پیشنهادی باید دو معیار NC و BER مورد ارزیابی قرار گیرند. معیار NC نشان‌دهنده میزان همبستگی بین داده نهان‌نگار اصلی و داده نهان‌نگار استخراج شده می‌باشد. اگر مقدار بدست آمده برای معیار NC نزدیک به یک باشد، بدین مفهوم است که شباهت بین داده نهان‌نگار اصلی و داده نهان‌نگار استخراج شده بسیار زیاد است و اگر مقدار بدست آمده برای معیار NC نزدیک به صفر باشد، بدین مفهوم است که شباهت بین داده نهان-نگار اصلی و داده نهان‌نگار استخراج شده بسیار کم است. همچنین معیار BER نشان‌دهنده دقت آشکارسازی داده نهان‌نگار پس از اعمال حملات مختلف می‌باشد. نتایج بدست آمده از اجرای تست استحکام بر روی سیگنال‌های پاپ، جاز و محلی به ترتیب در جداول شماره چهار، پنج و شش نشان داده شده است. با توجه به نتایج بدست آمده، روش نهان‌نگاری صوت پیشنهادی در برابر حملات مختلف دارای مقاومت بالایی است. زیرا، مقدار بدست آمده برای معیار NC در تمام حالات بالای ۰/۹۴ است و همچنین مقدار بدست آمده برای معیار BER در همه حالات کمتر از ۰/۳ است. این موارد در جداول ۴، ۵ و ۶ نشان داده شده است.

جدول ۴: نتایج بدست آمده در تست استحکام بر روی سیگنال صوتی پاپ

نوع سیگنال صوتی	نوع حملات	NC	BER (%)
پاپ	بدون حمله	۱	۰
	اضافه کردن نویز ۲۰۰	۰/۹۹	۰/۶۳



۰/۶۱	۰/۹۹	اضافه کردن نویز ۹۰۰	
۰	۱	تقویت	
۲/۴	۰/۹۷	متراکم سازی	
۰/۲	۰/۹۶	برش نمونه	
۰/۷۶	۰/۹۴	اکو	
۰	۱	باز نمونه‌گیری	
۰/۵	۰/۹۴	فیلتر پایین گذر RC	
۰/۵	۰/۹۴	فیلتر بالا گذر RC	

جدول ۵: نتایج بدست آمده در تست استحکام بر روی سیگنال صوتی جاز

BER (%)	NC	نوع حملات	نوع سیگنال صوتی
۰	۱	بدون حمله	جاز
۰/۶۱	۰/۹۹	اضافه کردن نویز ۲۰۰	
۰/۵۸	۰/۹۸	اضافه کردن نویز ۹۰۰	
۰	۱	تقویت	
۲/۰۵	۰/۹۹	متراکم سازی	
۰/۰۲	۰/۹۶	برش نمونه	
۰/۴۴	۰/۹۵	اکو	
۰	۱	باز نمونه‌گیری	
۱	۰/۹۴	فیلتر پایین گذر RC	
۱	۰/۹۴	فیلتر بالا گذر RC	

جدول ۶: نتایج بدست آمده در تست استحکام بر روی سیگنال صوتی محلی

BER (%)	NC	نوع حملات	نوع سیگنال صوتی
۰	۱	بدون حمله	محلی
۰/۳	۰/۹۹	اضافه کردن نویز ۲۰۰	
۰/۲۹	۰/۹۸	اضافه کردن نویز ۹۰۰	
۰	۱	تقویت	
۲/۹	۰/۹۸	متراکم سازی	
۱/۳	۰/۹۶	برش نمونه	
۱/۲	۰/۹۵	اکو	
۰	۱	باز نمونه‌گیری	
۰/۹	۰/۹۷	فیلتر پایین گذر RC	
۱/۱	۰/۹۷	فیلتر بالا گذر RC	

#### ۴- نتیجه گیری

در این مقاله، یک روش ترکیبی جدید برای نهان نگاری صوت در حوزه تبدیل ارائه شده است. روش نهان نگاری صوت پیشنهادی یک روش کور نمی‌باشد. در واقع، در روش نهان نگاری صوت پیشنهادی برای اجرای فاز استخراج، سیگنال صوتی اصلی مورد نیاز است. روش نهان نگاری صوت پیشنهادی توسط نرم افزار متلب پیاده سازی گردید. نتایج بدست آمده از اجرای تست‌های شنیداری، عینی و استحکام نشان داد که روش طراحی شده از عملکرد مطلوبی برخوردار است. به عنوان پیشنهادی برای کارهای آتی می‌توان عنوان داشت که، بجای استفاده از الگوریتم بهینه سازی کلونی مورچگان از دیگر الگوریتم‌های بهینه سازی همانند الگوریتم جستجوی گرانشی استفاده نمود.

#### ۵- پیشنهادات

در مطالعات آینده، می‌توان برخی از حملات مدرن مانند محوشدگی کانال، جیترو و حمله حذف بسته در نظر گرفته شود زیرا این حملات منحصر به شبکه های مختلف مانند GSM (شبکه جهانی برای ارتباطات همراه) و CDMA (دسترسی چندگانه تقسیم کد) مربوط می‌شوند. بعلاوه، مدل شنوایی می‌تواند اتخاذ شود تا به غیر قابل مشاهده بودن از روش پیشنهاد شده را بهبود بخشد. از این گذشته، کاهش پیچیدگی های محاسباتی از روش های پیشنهاد شده و همچنین استحکام از الگوریتم پیشنهادی می‌تواند به وسیله ی الگوریتم های بهینه سازی دیگر نظیر الگوریتم خفاش انجام شود.

## منابع و مراجع

- [1] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, (2010), "Digital image steganography: survey and analysis of current methods", International Journal of Signal Processing, vol. 90, pp. 727-752
- [2] S. Saranya, P. Elayaraja, (2016), "An efficient and secure watermarking scheme for audio signal authentication", International Journal of Innovative Research in Technology Science & Engineering,, vol. 2, pp. 9-15.
- [3] D. Megias, J. S. Ruiz, M. Fallahpour, (2010), "Efficient self-synchronized blind audio watermarking system based on time domain and FFT amplitude modification", International Journal of Signal Processing, vol. 90, pp. 3078-3092
- [4] W. A. Nuaimy, M. A. M. E. Bendary, A. Shfik, F. Shawki, A. E. A. E. azm, N. A. E. Fishawy, S. M. Elhalafawy, S. M. Diab, B. M. Sallam, A. E. Samie, H. B. Kazemian, (2011), "An SVD audio watermarking approach using chaotic encrypted images", International Journal of Digital Signal Processing, vol. 21, pp. 764-779
- [5] H. Peng, J. Wang, (2011), "Optimal audio watermarking scheme using genetic optimization", Annals of telecommunications, vol. 66, pp. 307-318
- [6] V. Bhat, I. Sengupta, A. Das, (2011), "An audio watermarking scheme using singular value decomposition and dither-modulation quantization", Multimedia Tools and Applications, vol. 52, pp. 369-383.
- [7] J. Mishra, M. V. Patil, J. S. Chitode, (2013), "an effective audio watermarking using DWT-SVD", International journal of computer applications, vol. 70, pp. 6-11
- [8] N. V. Lalitha, P. V. Prasad, S. U. M. Rao, (2016), "Performance Analysis of DCT and DWT Audio Watermarking based on SVD", International Conference on Circuit, Power and Computing Technologies, Nagercoil, India.
- [9] B. Lei, I. Y. Soon, F. Zhou, Z. Li, H. Lei, (2012), "a robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition", Signal processing, vol. 92, pp. 1985-2001.
- [10] B. Lei, I. Y. Soon, E. L. Tan, (2013), "robust SVD-Based audio watermarking scheme with differential evolution optimization", IEEE Transaction on audio, speech, and language processing,, vol. 21, pp. 2368-2378. [11] A. A. Haj, A. Mohammad, L. Bata, (2011), "DWT-Based audio watermarking", International Arab Journal of Information Technology, Vol. 8, pp. 326-333.