

بررسی کار آیی یک روش نهان نگاری تصویر مبتنی بر چرخش در حوزه تبدیل موجک

عزیزاله جمشیدی^۱، سجاد طباطبائی^۲، محمدعلی اخائی^۳

۱- مربی، گروه برق دانشگاه آزاد اسلامی واحد ماهشهر، jamshidi801@gmail.com

۲- مربی، گروه برق دانشگاه آزاد اسلامی واحد ماهشهر، sdtatababee@yahoo.com

۳- دانشجوی دکتری برق، دانشگاه صنعتی شریف، akhaiee@yahoo.com

چکیده

در این مقاله یک روش جدید کور مبتنی بر چرخش برای پنهان نگاری در حوزه تبدیل موجک پیشنهاد شده است. مهمترین ویژگی این روش بهینه بودن گیرنده در حضور نویز سفید گوسی و نیز پایداری آن نسبت به حمله بهره می باشد. به این منظور یک متغیر پایدار در برابر بهره معرفی شده است و تابع توزیع آن بکمک ریاضی محاسبه گردیده است. با داشتن تابع توزیع تجمعی گیرنده بهینه در برابر نویز به کمک الگوریتم بیشینه همانندی طراحی و پیاده سازی شده است. عملکرد این گیرنده مورد تحلیل قرار گرفته و احتمال خطای آن به صورت دقیق محاسبه شده است. برای درج بیشترین مقدار نهان نگاره از الگوریتم بهینه سازی چند هدفه استفاده شده است. به این منظور مصالحه مناسبی بین احتمال خطای الگوریتم و شفافیت نهان نگاره که توسط پارامتر اندیس کیفیت ارزیابی می شود بر قرار شده است. برای ارزیابی صحت مدل پیشنهادی و نیز احتمال خطای تحلیلی، روش بر روی سیگنال گوسی مصنوعی شبیه سازی شده است و سپس الگوریتم بر روی سیگنال های تصویر آزموده شده اند. نتایج شبیه سازی بر روی سیگنال های مصنوعی حاکی از درستی روابط ریاضی منتج شده و صحت مدل بکار برده شده می باشد. همچنین نتایج تجربی بر روی تصاویر از مقاومت بسیار خوب الگوریتم نهان نگاری معرفی شده در برابر حملات متداول نظیر نویز، فشرده سازی JPEG، و بهره خبر می دهد. همچنین در شرایط برابر از نظر نرخ درج و شفافیت، روش پیشنهادی پایداری بهتری نسبت به روش های گذشته دارد.

واژه های کلیدی

نهان نگاری مبتنی بر چرخش، تبدیل موجک، گیرنده بیشینه همانندی، بهینه سازی چندهدفه، تحلیل عملکرد.

۱- مقدمه

می تواند مشکلات جدی برای مؤلفانی که نمی خواهند آثارشان بدون اجازه خودشان پخش شود ایجاد کند. به همین دلیل حفاظت از اطلاعات دارای حق کپی امری ضروری است. یکی از بهترین روش ها برای پاسخ گویی به مشکلات فوق نهان نگاری می باشد که دارای کاربردهای زیادی از جمله مخابرات مخفی، زمان بندی پخش

با گسترش روزافزون اینترنت به عنوان محیطی برای انتقال سریع و آسان انواع اطلاعات (صوتی، تصویر، فیلم و غیره) این امکان برای افرادی که خواستار به اشتراک گذاشتن اطلاعات خود هستند به وجود آمده است. با وجود مزایای آن، این گونه انتقال اطلاعات

QIM را زایل می‌کند. همچنین پایداری روش AQIM به‌خوبی QIM نمی‌باشد. روش RDM نواقص ذکر شده را تا حد خوبی مرتفع کرده است اما در روش آنها تابع نرم p به‌صورت دلخواه انتخاب شده است. این موضوع مقاومت الگوریتم را تا حدی تحت الشعاع قرار داده است. لذا ما به دنبال روشی هستیم که علاوه بر امنیت پایداری بالایی نیز داشته باشد و در برابر حمله بهره به‌طور کامل مقاوم باشد. تابع گیرنده نیز با توجه به نظریه بیشینه همانندی انتخاب گردد تا بیشترین پایداری نسبت به نویز سفید گوسی حاصل گردد.

در این مقاله ما یک روش کور برپایه روش [۱۸] در حوزه تبدیل موجک پیشنهاد می‌کنیم. روش ما در واقع بهبود و تعمیم روش [۱۸] می‌باشد. به این منظور تصویر به بلوک‌های غیرهمپوشان تقسیم شده و از هر بلوک تبدیل موجک گرفته می‌شود. نمونه‌های شامل فرکانس‌های پایین بر مبنای یک کلید محرمانه در کنار یکدیگر قرار می‌گیرند و هر چهار نمونه تشکیل یک پاره خط را می‌دهند. عمل درج نهان نگاره با عوض کردن شیب این پاره‌خطها صورت می‌پذیرد. تابع توزیع شیب پاره خط محاسبه گردیده و به کمک گیرنده بیشینه شباهت عمل آشکارسازی صورت می‌پذیرد. یکی از کارهایی که به‌عنوان تعمیم روش [۱۸] صورت پذیرفته محاسبه احتمال خطای سیستم به‌صورت دقیق است که شبیه‌سازی‌ها بر روی سیگنال مصنوعی گوسی آن را تأیید می‌کند. همچنین به‌منظور رعایت مصالحه میان شفافیت نهان‌نگاره و پایداری آن در برابر حملات از الگوریتم بهینه‌سازی چندهدفه استفاده شده است. این در حالی است که در روش [۱۸] اندازه زاویه یک مقدار ثابت انتخاب شده است. در این حالت میزان شفافیت به روش اندیس کیفیت تصویر [۱۹] به‌صورت خودکار محاسبه شده و پایداری نیز به کمک روابط احتمال خطای منتج شده محاسبه می‌گردد. با این کار روش معرفی شده مقاومت بسیار بالایی در برابر حملات متداول دارد.

بقیه مقاله به شرح زیر است. ابتدا مدل سیستم پیشنهادی در بخش دو مورد ارزیابی قرار می‌گیرد. در بخش سوم به بررسی روش پیشنهادی می‌پردازیم و گیرنده آن را مورد بحث قرار می‌دهیم. عملکرد الگوریتم در بخش چهارم مورد تحلیل و بررسی قرار می‌گیرد. در بخش پنجم مسدله بهینه‌سازی شفافیت و پایداری نهان‌نگاره را ارزیابی می‌کنیم. نتایج شبیه‌سازی هم بر روی سیگنال مصنوعی و هم بر روی تصاویر طبیعی در فصل ششم به نمایش در می‌آیند. فصل هفتم متعلق به نتیجه‌گیری و کارهای آینده است.

برنامه‌ها، اثبات مالکیت و غیره است [۱]-[۴]. نهان‌نگاری روشی است که در آن اطلاعات مالک (سیگنال الگو یا نهان‌شونده) به‌گونه‌ای نامحسوس در سیگنال اصلی یا میزبان نهان می‌شود و به این صورت سیگنال الگوگذاری شده یا نهان‌نگاری شده ایجاد می‌شود. این نهان کردن الگو نباید باعث کاهش کیفیت اطلاعات اصلی شود. به اقتضای کاربرد نهان نگاری به‌صورت‌های مقاوم، نیمه‌شکننده و شکننده انجام می‌پذیرد [۳]. در این میان کاربردهای روش‌های مقاوم از مابقی بیشتر است. همچنین از نقطه نظر آشکارسازی روش‌های نهان‌نگاری به سه گونه کور، نیمه‌کور و بینا تقسیم می‌شوند [۴]. در سیستم‌های کور نیازی به سیگنال تمیز برای آشکارسازی نیست درحالی‌که در نیمه‌کور و بینا به بخشی یا کل سیگنال تمیز احتیاج است.

یکی از مهمترین حملات که در کانال مخابراتی بوفور اتفاق می‌افتد حمله بهره است. در ساده‌ترین مدل‌های کانال این پدیده قابل مشاهده است. بسیاری از روش‌های متداول نظیر بیت کم‌ارزش (LSB) [۵]-[۶]، کوانتیزاسیون اندیس مدولاسیون (QIM) [۷]-[۹]، روش دو تکه (Patchwork) [۱۰]-[۱۱] و غیره در برابر این حمله ناتوانند. معرفی تبدیل یا حوزه‌ای که در برابر بهره بی‌تغییر باشد از چالش‌های مسأله نهان‌نگاری است که تاکنون بسیاری به بررسی آن پرداختند [۱۲]-[۱۷]. کلیه روش‌های پیشنهادی به چهار دسته مهم تقسیم می‌شوند. ۱- استفاده از پیشرو در سیگنال نهان نگاری شده [۱۲]. در این حالت در فواصل معین سیگنال‌های از پیش تعیین قرار داده می‌شوند و با بررسی آنها در گیرنده میزان بهره تخمین زده شده و جبران می‌گردد. ۲- استفاده از کدهای مخروطی [۱۳] با گیرنده‌های منطبق بر شباهت [۱۴]. در این حالت از کدهایی استفاده می‌گردد که بخاطر ساختار مخروطی که دارند نسبت به بهره با هر ضریبی ثابت هستند. ۳- استفاده از کوانتیزاسیون زاویه‌ای (AQIM) [۱۵]-[۱۶]. در این حالت الگوریتم کوانتیزاسیون اندیس مدولاسیون بر روی زاویه حاصل از دو نمونه (مثلاً مجاور) در یک حوزه خاص صورت می‌پذیرد. ۴- معرفی یک تابع تقسیمی مبتنی بر تابع نرم p و اعمال روش‌های مبتنی بر کوانتیزاسیون بر روی این تابع. این روش به لرزش مدولاسیون تقسیمی معروف است (RDM) [۱۷].

راه حل اول امنیت الگوریتم را به‌شدت کاهش می‌دهد. اساس نهان‌نگاری این است که دشمن متوجه هیچ چیز مشکوکی در سیگنال ارسالی نشود. وجود سیگنال پیشرو شک دشمن را برمی‌انگیزد. اگرچه روش دوم و سوم امنیت را حفظ می‌کنند، اما پیچیدگی محاسباتی بالایی را به روش‌های مبتنی بر کوانتیزاسیون تحمیل می‌کنند به‌گونه‌ای که سادگی فرستنده و گیرنده در طرح

۲- مدل سیگنال پیشنهادی

در اینجا مدل سیستمی را که برای نهان نگاری مورد استفاده قرار می گیرد توضیح داده می شود. ما فرض می کنیم که یک سیگنال تصادفی گوسی با میانگین صفر و واریانس σ^2 داریم. در هر سناریو چهار نمونه از سیگنال مورد نظر (سیگنال میزبان) مورد استفاده قرار می گیرد. این چهار نمونه به صورت $u=[u_1, u_2, u_3, u_4]$ نمایش داده می شوند. ما این چهار نمونه را به دو زوج نمونه $p=[u_1, u_2]$ و $q=[u_3, u_4]$ در یک فضای دوبعدی تقسیم می کنیم. شیب خطی که این دو نقطه را بهم وصل می کند به صورت زیر بیان می شود.

$$c = \frac{u_4 - u_2}{u_3 - u_1} \quad (1)$$

اگر صورت و مخرج رابطه بالا را به صورت a و b نشان دهیم خواهیم داشت $a, b \sim N(0, 2\sigma^2)$. برای حالتی که a و b مستقل هستند پارامتر c که حاصل تقسیم دو مولفه گوسی با میانگین صفر و مستقل از هم می باشد با توزیع گوسی به صورت زیر قابل بیان است:

$$f_c(c) = \frac{1}{\pi} \frac{\frac{\sigma_a}{\sigma_b}}{c^2 + \left(\frac{\sigma_a}{\sigma_b}\right)^2} \quad (2)$$

در حالتی که دو متغیر گوسی دارای همبستگی باشند تابع توزیع مشترک آن به صورت زیر است:

$$f_{ab}(a, b) = \frac{1}{2\pi\sigma_a\sigma_b\sqrt{1-r^2}} e^{-\frac{1}{2(1-r^2)}\left(\frac{a^2}{\sigma_a^2} - \frac{2rab}{\sigma_a\sigma_b} + \frac{b^2}{\sigma_b^2}\right)} \quad (3)$$

بنابراین تابع توزیع تجمعی c به صورت:

$$\begin{aligned} F_c(c) &= P\left\{\frac{a}{b} \leq c\right\} \\ &= P\{a \leq bc, b \geq 0\} \\ &= \int_0^{\infty} \int_{-\infty}^{bc} f_{ab}(a, b) da db \\ &+ \int_{-\infty}^0 \int_{bc}^{\infty} f_{ab}(a, b) da db \end{aligned} \quad (4)$$

بنابراین تابع چگالی احتمال آن به صورت:

$$f_c(c) = F_c'(c) = \int_{-\infty}^{+\infty} |b| f_{ab}(bc, b) db \quad (5)$$

با جایگزینی (۴) در (۵) و در نظر گرفتن این نکته که تابع $f_{ab}(a, b)$ نسبت به a و b زوج است داریم:

$$\begin{aligned} f_c(c) &= \frac{1}{2\pi\sigma_a\sigma_b\sqrt{1-r^2}} \int_0^{\infty} b e^{-\frac{b^2}{2\sigma_b^2}} db \\ &= \frac{\sigma_0^2}{\pi\sigma_a\sigma_b\sqrt{1-r^2}} \end{aligned} \quad (6)$$

که در آن $\sigma_0^2 = \frac{1-r^2}{(c/\sigma_a)^2 - (2rc/\sigma_a\sigma_b) + (1/\sigma_b^2)}$ است. در نتیجه:

$$f_c(c) = \frac{1}{\pi} \frac{\sigma_a\sigma_b\sqrt{1-r^2}}{\sigma_b^2\left(c - \frac{r\sigma_a}{\sigma_b}\right)^2 + \sigma_a^2(1-r^2)} \quad (7)$$

همچنین تابع توزیع تجمعی آن به صورت زیر قابل محاسبه است.

$$F_c(c) = \frac{1}{2} + \frac{1}{\pi} \tan^{-1} \frac{\sigma_b c - r\sigma_a}{\sigma_a\sqrt{1-r^2}} \quad (8)$$

از این تابع توزیع تجمعی در ادامه برای بدست آوردن گیرنده بهینه و احتمال خطای آن استفاده خواهیم کرد.

۳- روش پیشنهادی مبتنی بر چرخش

۳-۱- درج نهان نگاره

برای درج نهان نگاره در تصویر، سیگنال میزبان به بلوک های مساوی و غیرهمپوشان تقسیم می گردد. در هر یک از این بلوک ها یک بیت پیغام مخفی نهان می گردد. در واقع هر یک از این بلوک ها حامل های ما در سیستم پنهان نگاری مذکور هستند. در هر بلوک ما چهار ضریب تقریب تبدیل موجک آنرا انتخاب می کنیم. به این منظور به هر بلوک تبدیل موجک دوبعدی اعمال می گردد. پس از بدست آوردن چهار ضریب تقریب اندیس آنها به صورت تصادفی انتخاب می گردد و به وسیله یک کانال امن به گیرنده ارسال می شود. این کار برای بالا بردن امنیت انجام شده است. به عبارت دیگر به چهار نمونه بدست آمده ۴! اندیس می توان اختصاص داد. به کمک کلید رمز در هر بلوک ما یکی از این ۲۴ حالت ممکن را انتخاب می کنیم.

حال فرض کنید اندیسها اختصاص یافته و بردار $u=[u_1, u_2, u_3, u_4]$ انتخاب گردیده اند. همان طور که در مدل بیان شد $p=[u_1, u_2]$ و $q=[u_3, u_4]$ در فضای دوبعدی هستند. شکل (۱) این دو نقطه را بر خط فاصل بین آنها را نشان می دهد.

ساده سازی راه حل به صورت زیر خلاصه می گردد.

$$p_{\perp} = \begin{pmatrix} \frac{u'_1 + ku'_2}{k^2 + 1} \\ \frac{ku'_1 + k^2 u'_2}{k^2 + 1} \end{pmatrix}, \quad (11)$$

$$q_{\perp} = \begin{pmatrix} \frac{u'_3 + ku'_4}{k^2 + 1} \\ \frac{ku'_3 + k^2 u'_4}{k^2 + 1} \end{pmatrix}$$

در قدم آخر تنها کافی است تا ما پاره خط تصویر شده را به محل اولش انتقال دهیم. در نتیجه مجموعه نقاط جدید $p_w = [u''_1, u''_2]$ و $q_w = [u''_3, u''_4]$ بعد از انتقال حاصل می گردند.

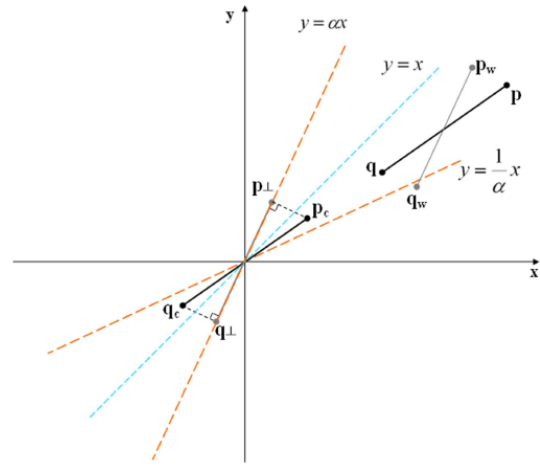
$$p_w = \begin{pmatrix} u''_1 \\ u''_2 \end{pmatrix} = \begin{pmatrix} \frac{u'_1 + ku'_2 + u_1 + u_3}{k^2 + 1} \\ \frac{ku'_1 + k^2 u'_2 + u_2 + u_4}{k^2 + 1} \end{pmatrix} \quad (12)$$

$$q_w = \begin{pmatrix} u''_3 \\ u''_4 \end{pmatrix} = \begin{pmatrix} \frac{u'_3 + ku'_4 + u_1 + u_3}{k^2 + 1} \\ \frac{ku'_3 + k^2 u'_4 + u_2 + u_4}{k^2 + 1} \end{pmatrix}$$

بنابراین با جای گذاری (۹) در (۱۲) کل روند به صورت زیر قابل بیان است. که در آن $T(k)$ یک ماتریس تبدیل است.

$$\begin{pmatrix} u''_1 \\ u''_2 \\ u''_3 \\ u''_4 \end{pmatrix} = T(k) \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} \quad (13)$$

$$T(k) = \frac{1}{2k^2 + 2} \times \begin{pmatrix} k^2 + 2 & k & k^2 & -k \\ k & 2k^2 + 1 & -k & 1 \\ k^2 & -k & k^2 + 2 & k \\ -k & 1 & k & 2k^2 + 1 \end{pmatrix} \quad (14)$$



شکل ۱- تصویر مراحل درج نهان نگاره بکمک چرخش نقاط

فرض می کنیم زاویه شیب این خط θ باشد. نقطه وسط این پاره خط در نقطه $\left[\frac{u_1 + u_3}{2} + \frac{u_2 + u_4}{2} \right]$ قرار دارد. اگر ما این پاره خط را به نقطه مبدأ منتقل کنیم به دو نقطه جدید p_c و q_c می رسیم. منظور از p_c و q_c نقاط مرکزی شده اند که به صورت زیر قابل بیان هستند.

$$p_c = \begin{pmatrix} u'_1 \\ u'_2 \end{pmatrix} = \begin{pmatrix} \frac{u_1 - u_3}{2} \\ \frac{u_2 - u_4}{2} \end{pmatrix}, \quad q_c = \begin{pmatrix} u'_3 \\ u'_4 \end{pmatrix} = \begin{pmatrix} \frac{u_3 - u_1}{2} \\ \frac{u_4 - u_2}{2} \end{pmatrix} \quad (9)$$

حال برای درج نهان نگاره ما این پاره خط را بر روی دو خط L_0 و L_1 تصویر می کنیم بر حسب این که چه بیتی نهان شده باشد. در نتیجه پاره خط مرکزی شده بعد از درج صفر روی خط L_0 و بعد از درج یک روی خط L_1 تصویر می شود. شکل (۱) این فرایند را به طور ریز توضیح می دهد. ما به نقاط تصویر شده p_{\perp} و q_{\perp} می گوئیم. شیب زاویه خط L_0 که متناظر با بیت پیام صفر است، مقدار α انتخاب می شود اگر θ (شب پاره خط متواصل بین p و q اولیه) مثبت باشد. در غیر این صورت $-\alpha$ انتخاب می گردد. به طور مشابه شیب خط L_1 $\frac{1}{\alpha}$ یا $-\frac{1}{\alpha}$ انتخاب می گردد.

محل نقطه تصویر شده p_{\perp} در موقعی که بر روی یک خط دلخواه با شیب k تصویر می شود با تقاطع دو خط حاصل می شود. بدین منظور معادله زیر باید حل شود.

$$\begin{cases} y = kx \\ y - u'_2 = -\frac{1}{k}(x - u'_1) \end{cases} \quad (10)$$

و یک روند مشابه نیز برای q_{\perp} صورت می پذیرد. بعد از

که در آن

نگاری روی k ثابت کرده‌ایم طبق رابطه (۱۵) داریم:

$$k = \frac{u_4'' - u_2''}{u_3'' - u_1''} \Rightarrow u_4'' - u_2'' = k(u_3'' - u_1'') \quad (17)$$

بنابراین اگر تعریف کنیم $v = u_3'' - u_1''$ می‌توان (۱۶) را به صورت زیر بازنویسی کرد.

$$c = \frac{kv + n_4 - n_2}{v + n_3 - n_1} \quad (18)$$

حال ما می‌خواهیم همبستگی بین صورت و مخرج را حساب کنیم. در واقع همان‌طور که دیده می‌شود در صورت و مخرج پارامتر v وجود دارد. لذا حتماً یک همبستگی بالا بین صورت و مخرج موجود است. برای محاسبه ابتدا تابع توزیع v را باید محاسبه کنیم. با استفاده از (۱۴) و (۱۶) می‌توانیم بگوییم:

$$v = u_3'' - u_1'' = \frac{1}{k^2 + 1} (-u_1 - ku_2 + u_3 + ku_4) \quad (19)$$

از آنجا که سیگنال میزبان u گوی و مستقل است پارامتر v هم متغیر گوی با میانگین صفر و واریانس $\sigma_v^2 = \frac{2}{1+k^2} \sigma_u^2$ می‌باشد. در نتیجه تابع توزیع در متغیر تصادفی a و b به صورت $a \sim N(0, k^2 \sigma_v^2 + 2\sigma_n^2)$ و $b \sim N(0, \sigma_v^2 + 2\sigma_n^2)$ می‌باشد. ضریب همبستگی بین a و b مطابق رابطه زیر قابل بیان است:

$$r = \frac{k \sigma_v^2}{\sqrt{(k^2 \sigma_v^2 + 2\sigma_n^2)(\sigma_v^2 + 2\sigma_n^2)}} \quad (20)$$

حال ما داریم $c = \frac{a}{b}$ که a و b دو متغیر گوسی وابسته با میانگین صفر است. مطابق بحث بخش قبل تابع توزیع متغیر c به صورت رابطه (۷) قابل بیان است. با داشتن تابع توزیع متغیر شیب پاره خط، براحتی می‌توان گیرنده بهینه ML را برای آشکارسازی بکار برد.

$$\text{decision} = \begin{cases} 1 & f_C(c|1) - f_C(c|0) > 0 \\ 0 & f_C(c|1) - f_C(c|0) < 0 \end{cases} \quad (21)$$

که $f_C(c|0)$ و $f_C(c|1)$ به ترتیب تابع توزیع متغیر c به شرط درج بیت یک و صفر می‌باشد. در اینجا بدون از دست دادن کلیت مساله فرض می‌کنیم که متغیر c مثبت است. خواهیم دید که بحث ما در مورد c های منفی نیز درست خواهد بود. لذا داریم:

$$f_C(c) = \frac{1}{\pi} \frac{\sigma_{a|1} \sigma_{b|1} \sqrt{1-r_1^2}}{\sigma_{b|1}^2 (c - \frac{r_1 \sigma_{a|1}}{\sigma_{b|1}})^2 + \sigma_{a|1}^2 (1-r_1^2)} \quad (22)$$

$$k = \begin{cases} \alpha & \text{for '1' embedding when } \theta \geq 0 \\ \frac{1}{\alpha} & \text{for '0' embedding when } \theta \geq 0 \\ -\alpha & \text{for '1' embedding when } \theta < 0 \\ -\frac{1}{\alpha} & \text{for '0' embedding when } \theta < 0 \end{cases} \quad (15)$$

بنابراین فرآیند درج نهان نگاره که در (۱۳) آمده است به راحتی قابل پیاده‌سازی است. در این تبدیل k براساس شیب اولیه پاره خط θ و بیت پیغام مخفی به صورت زیر انتخاب می‌شود، سپس از سیگنال نهان‌نگاری شده $u'' = [u_1'', u_2'', u_3'', u_4'']$ بعد از آنکه اندیس آنها به حالت اول (به وسیله کلید رمز) درآمد، تبدیل معکوس موجک دوبعدی گرفته می‌شود.

۳-۲- استخراج نهان نگاره

برای استخراج نهان نگاره در هر بلوک ما از گیرنده بهینه استفاده می‌کنیم. فرض کنید $y = [y_1, y_2, y_3, y_4]$ ضرایب تقریب با اندیس‌های مناسب باشند. این ضرایب آلوده به نویز جمع‌شونده سفیده شده‌اند. در نتیجه $y = u'' + n$ که $n \sim N(0, \sigma_n^2)$ بدین معنی که متغیر تصادفی n یک متغیر تصادفی گوسی با میانگین صفر و واریانس σ_n^2 می‌باشد.

همان‌طور که در [۲۰] نشان داده شده است ضرایب تقریب تصویر می‌توانند با دقت خوب با توزیع گوسی مدل شوند. ما از این مدل در تحلیل‌گیرنده بهینه خود بهره می‌بریم. همچنین فرض می‌کنیم نمونه‌ها مستقل با توزیع یکسان باشد.

از آنجا که اعمال ماتریس $T(k)$ یک عمل خطی است و این عملگر توزیع گوسی را گوسی نگه می‌دارد، همچنین نویز جمع‌شونده هم گوسی است، لذا سیگنال نهان‌نگاری شده بدست آمده هم گوسی خواهد بود. همچنین به دلیل استقلال نویز و نمونه‌های نهان‌نگاری شده، واریانس سیگنال دریافت شده به صورت $\sigma_y^2 = \sigma_u^2 + \sigma_n^2$ می‌باشد.

حال از مدل معرفی شده در قسمت قبل استفاده می‌کنیم. چهار ضریب بدست آمده از سیگنال دریافتی را با $p_r = [y_1, y_2]$ و $q_r = [y_3, y_4]$ در یک فضای دوبعدی انتخاب کرده و شیب خط واصل بین آنرا حساب می‌کنیم.

$$c = \frac{y_4 - y_2}{y_3 - y_1} = \frac{u_4'' - u_2'' + n_4 - n_2}{u_3'' - u_1'' + n_3 - n_1} \quad (16)$$

از آنجا که ما شیب نقاط سیگنال میزبان را بعد از اعمال نهان

$$P_e^+ = \frac{1}{2} + \left[\tan^{-1} \frac{\sigma_b |1 - r \sigma_a|}{\sigma_a |1 - r| \sqrt{1 - r^2}} - \tan^{-1} \frac{-\sigma_b |1 - r \sigma_a|}{\sigma_a |1 - r| \sqrt{1 - r^2}} - \tan^{-1} \frac{\sigma_b |0 - r \sigma_a|}{\sigma_a |0 - r| \sqrt{1 - r^2}} + \tan^{-1} \frac{-\sigma_b |0 - r \sigma_a|}{\sigma_a |0 - r| \sqrt{1 - r^2}} \right] \quad (26)$$

که در آن $r = r_0 = r_1$ همان طور که در (۲۳) آمده است. در رابطه مذکور داریم $\sigma_a |1 - r \sigma_a| = \sigma_b |1 - r \sigma_a|$ و $\sigma_a |0 - r \sigma_a| = \sigma_b |0 - r \sigma_a|$ بنابراین اگر تعریف کنیم $d = \frac{\sigma_a |1 - r \sigma_a|}{\sigma_b |1 - r \sigma_a|}$ به صورت زیر ساده می شود.

$$P_e^+ = \frac{1}{2} + \frac{1}{\pi} \left(\tan^{-1} \frac{d^{-1} - r}{\sqrt{1 - r^2}} + \tan^{-1} \frac{d^{-1} + r}{\sqrt{1 - r^2}} - \tan^{-1} \frac{d + r}{\sqrt{1 - r^2}} - \tan^{-1} \frac{d - r}{\sqrt{1 - r^2}} \right) \quad (27)$$

با یک بحث مشابه می بینیم که احتمال خطا هنگامی که شیب پاره خط منفی است همانند P_e^+ محاسبه می گردد. به عبارت دیگر $P_e^- = P_e^+$ در نتیجه $P_e = \frac{1}{2} (P_e^+ + P_e^-) = P_e^+$ در شکل (۴) نتایج محاسبات تئوری با نتایج تجربی در $\sigma_n = 40$ مقایسه شده است. همان گونه که دیده می شود محاسبات با مشاهدات تطابق خوبی دارند. برای ارزیابی عملکرد ما از دو پارامتر نسبت نهان نگاره به توان نویز (WNR) و نسبت توان سیگنال میزبان به توان نهان نگاره (DWR) استفاده می کنیم. این پارامترها به صورت زیر تعریف می شوند:

$$DWR = 10 \log \frac{E \{ \|x_i\|^2 \}}{E \{ \|x_i' - x\|^2 \}} \quad (28)$$

$$WNR = 10 \log \frac{E \{ \|x_i' - x\|^2 \}}{E \{ \|v_i - x_i'\|^2 \}} \quad (29)$$

در این روابط x سیگنال میزبان است و x' و v به ترتیب سیگنال نهان نگاری شده و دریافتی بعد از کانال می باشند.

$$f_c(c) = \frac{1}{\pi} \frac{\sigma_{a|0} \sigma_{b|0} \sqrt{1 - r_0^2}}{\sigma_{b|0}^2 (c - \frac{r_0 \sigma_{a|0}}{\sigma_{b|0}})^2 + \sigma_{a|0}^2 (1 - r_0^2)} \quad (23)$$

که در آن

$$\sigma_{a|1}^2 = \frac{2\alpha^2}{1 + \alpha^2} \sigma_u^2 + 2\sigma_n^2, \quad \sigma_{b|1}^2 = \frac{2}{1 + \alpha^2} \sigma_u^2 + 2\sigma_n^2,$$

$$\sigma_{a|0}^2 = \frac{2}{1 + \alpha^2} \sigma_u^2 + 2\sigma_n^2, \quad \sigma_{b|0}^2 = \frac{2\alpha^2}{1 + \alpha^2} \sigma_u^2 + 2\sigma_n^2,$$

$$r_1 = r_0 = \frac{\alpha \sigma_u^2}{\sqrt{(\alpha^2 \sigma_u^2 + (1 + \alpha^2) \sigma_n^2)(\sigma_u^2 + (1 + \alpha^2) \sigma_n^2)}}$$

این پارامترها با جایگزینی k (رابطه ۱۴) در واریانس های متغیرهای a و b نیز همبستگی بین آنها (u) بدست آمده اند. با قرار دادن (۲۳) و (۲۴) در رابطه (۲۱) و بعد از مقداری ساده سازی به راه ساده زیر می رسیم:

$$\text{decision} = \begin{cases} 1 & c^2 > 1 \\ 0 & c^2 < 1 \end{cases} \quad (24)$$

همانطور که دیده می شود آشکار ساز بهینه مستقل از α عمل می کند. همچنین واضح است که برای c های منفی نیز بحث به همین گونه است. (تنها می بایست علامت v_1 و v_0 عوض شود).

۴- تحلیل عملکرد

در اینجا می خواهیم احتمال خطای سیستم پیشنهادی را در حضور نویز بدست آوریم. خطا هنگامی رخ می دهد که بیت یک نهان کرده باشیم و صفر آشکار شده باشد و بالعکس. با توجه به تقارن موجود در این دو نوع خطا ما به بررسی یکی از آنها می پردازیم. ابتدا به بررسی احتمال خطا هنگامی که شیب پاره خط واصل (p, q) مثبت است می پردازیم. لذا طبق رابطه (۲۴) احتمال خطا به صورت زیر نوشته می شود.

$$P_e^+ = \frac{1}{2} P(c^2 < 1 | 1) + \frac{1}{2} P(c^2 < 1 | 0) \\ = \frac{1}{2} P(-1 < c < 1 | 1) + \frac{1}{2} P(c < -1 \text{ or } c > 1 | 0) \quad (25) \\ = \frac{1}{2} \{ F_C | 1(1) - F_C | 1(-1) + 1 - F_C | 0(1) \\ + F_C | 0(-1) \}$$

با جایگزینی $F_c(r)$ در (۸) خواهیم داشت.

۵- بهینه‌سازی زاویه چرخش

زاویه چرخش θ که در واقع شیب پاره‌خط را تعیین می‌کند، نقش اساسی در عملکرد الگوریتم پیشنهادی دارد. در واقع مقدار آن از دو دیدگاه قابل ارزیابی است. ۱- نامرئی بودن: با افزایش θ ، اعوجاج بیشتری به سیگنال میزبان اعمال می‌گردد که ممکن است وجود نهان‌نگاره را محسوس سازد. ۲- مقاومت: با افزایش θ ، الگوریتم در برابر حملات مختلف مقاوم‌تر خواهد بود. از آنجا که یک مصالحه بین نامرئی بودن و مقاومت وجود دارد، ما در اینجا از یک روش بهینه‌سازی چند هدفه برای تعیین مقدار مناسب θ استفاده خواهیم کرد.

به‌منظور نشان دادن تأثیر θ در میزان اعوجاج اعمالی در تصویر، ما از اندیس اندازه‌گیری کیفیت در تصویر که در [۱۹] و [۲۰] ارائه شده است بهره می‌بریم. در این رهیافت اندازه‌گیری کیفیت، هر گونه اعوجاج با در نظر گرفتن مدل بینایی انسان برحسب سه عامل. ۱- کاهش شباهت، ۲- اعوجاج روشنایی و ۳- اعوجاج وضوح، بیان می‌شود. این مدل ارزیابی کیفیت از تمام مدل‌های ارزیابی پیشین نظیر MSE، PSNR و غیره بهتر عمل می‌کند و تطابق بسیار خوبی با تست‌های دیداری دارد.

اگر تصویر اصلی و نهان‌نگاری شده با x و y نشان داده شوند. اندیس اندازه‌گیری کیفیت Q به‌صورت زیر تعریف می‌شود.

$$Q = \frac{(\hat{x}\hat{y} + C_1)(2\sigma_{xy} + C_2)}{[(\hat{x})^2 + (\hat{y})^2 + C_1](\sigma_x^2 + \sigma_y^2 + C_2)} \quad (30)$$

که در آن \hat{x} ، \hat{y} ، σ_x^2 و σ_y^2 به ترتیب میانگین و پراش x و y هستند. پارامترهای C_1 و C_2 بر طبق زیرند:

$$C_1 = (K_1 L)^2, \quad C_2 = (K_2 L)^2$$

که L بازه دینامیکی تغییرات نمونه‌های تصویر است (۲۵۵) برای ۸ بیت) و $K_1, K_2 \ll 1$. بدین معنی که این پارامترها بسیار کوچک‌تر از یک هستند. (در این کار $K_1 = 0.01$ و $K_2 = 0.03$ لحاظ شده است). دامنه تغییرات Q بین $[-1, 1]$ است. مقدار یک تنها وقتی بدست می‌آید که مقادیر $y_i = x_i$ برای تمام i ها باشد.

از آنجا که تصویر به‌طور کلی یک سیگنال غیرایستاد است و کیفیت آن در جاهای مختلف متفاوت است، این کار معقول است که اندازه‌گیری به‌صورت محلی صورت پذیرد و سپس به‌صورت آماری با هم جمع شود. در [۱۹] پیشنهاد شده است که اندازه‌گیری کیفیت در بلوک‌های جدا صورت پذیرد Q_j ، و

اندیس کیفیت نهایی از جمع حسابی Q_j ها مطابق با (۳۱) صورت پذیرد.

$$Q = \frac{1}{M} \sum_{j=1}^M Q_j \quad (31)$$

با این حال از آنجا که قضاوت انسان عموماً بر روی بدترین بلوک‌ها صورت می‌پذیرد یا به بیان دیگر، چشم انسان کیفیت را از بلوک‌های خراب می‌فهمد، ما تصمیم گرفتیم که از میانگین هندسی بجای میانگین حسابی استفاده کنیم. بنابراین اندیس کیفیت نهایی مطابق زیر محاسبه می‌شود.

$$Q = \left(\prod_{j=1}^M Q_j \right)^{\frac{1}{M}} \quad (32)$$

بنابراین با تعریف اندیس اندازه‌گیری کیفیت ما دو تابع هدف داریم: که $f_D(\theta)$ بیانگر نقش θ در مسیر اعوجاج است و به‌صورت $f_D(\theta) = 1 - D(\theta)$ تعریف می‌شود و $f_E(\theta)$ که بیانگر مقاومت الگوریتم است و از روی روابط احتمال خطا در (۲۷) محاسبه می‌گردد. تابع $f_D(\theta)$ یک تابع یکنوا و صعودی از θ است. در حالی که تابع $f_E(\theta)$ تابع نزولی اکید است. هدف ما در اینجا پیدا کردن θ بهینه برای کمینه‌کردن هر دو تابع هدف است. از آنجا که این دو تابع، ماهیتاً با هم تفاوت دارند ما نمی‌توانیم آنها را به‌صورت وزن‌دار جمع کنیم. برای این منظور از روش بهینه‌سازی چندهدفه کسب هدف Gembichi [۲۲] استفاده می‌کنیم. در این روش برای بهینه‌سازی m تابع که بین آنها مصالحه وجود دارد، یکسری هدف در نظر گرفته می‌شود $F^* = [F_1^*, F_2^*, \dots, F_m^*]$ و با در نظر گرفتن یکسری وزن $w = [w_1, w_2, \dots, w_m]$. نقطه یا ناحیه بهینه بدست می‌آید. روش کسب هدف بصورت زیر بیان می‌گردد.

$$\min_{\lambda \in \mathbb{R}} \text{subject to } F_i(x) - w_i \lambda \leq F_i^*, \quad (33)$$

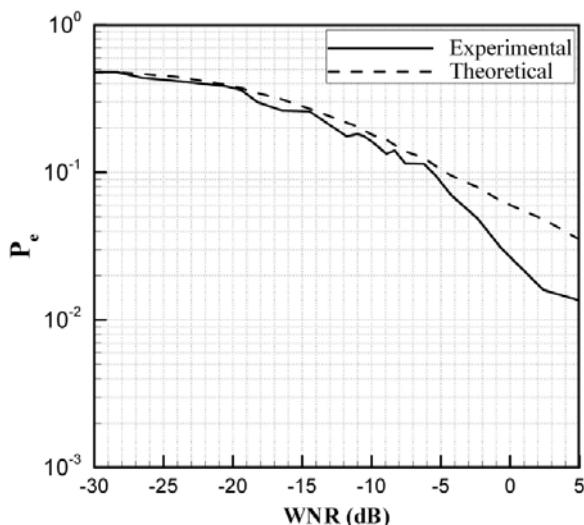
$$i = 1, 2, \dots, m, \quad x \in \Omega$$

که در آن Ω ناحیه حصول در فضای پارامتر x و λ متغیر کمکی بدون علامت است. بردار وزن w در واقع طراح را قادر به برقراری مصالحه مناسب بین اهداف می‌گرداند. عبارات دیگر اگر ما بتوانیم یک هدف را با مقادیر بیشتر تحمل کنیم، وزن کمتری را به آن تخصیص می‌دهیم و بالعکس.

شکل (۲) بصورت هندسی روش کسب هدف را برای دو تابع هدف نشان می‌دهد. در این شکل $F(\Omega)$ یک ناحیه قابل

۶- نتایج تجربی

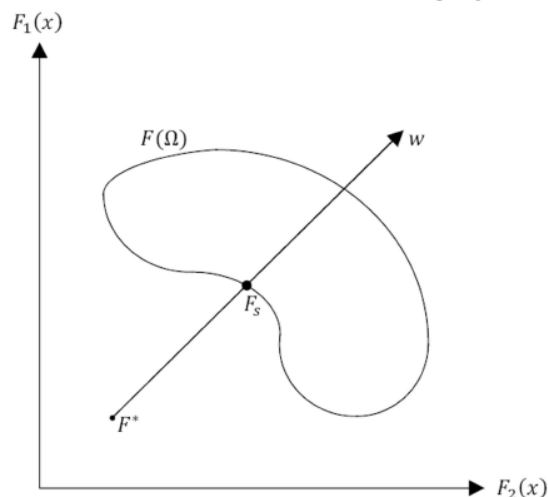
ما برای ارزیابی روش پیشنهادی خود آزمایش‌های بسیاری را روی تصاویر گوناگون انجام دادیم و عملکرد الگوریتم نهان نگاری را در برابر حملات متداول به بوته آزمایش گذاشتیم. در تجربه نخست برای تست صحت روش و نیز درستی روابط ریاضی استخراج شده، ما عملکرد روش را بر روی سیگنال مصنوعی گوسی (دقیقاً مدل فرض شده) در حضور نویز سفید گوسی آزمودیم. توان نهان نگاره با DWR اندازه‌گیری می‌شود ۲۲db می‌باشد. نتایج روش برای نویزهای متفاوت که با نسبت توان نهان نگاره به توان نویز (WNR) سنجیده می‌شود در شکل (۴) آمده است. همچنین نتایج با روش کوانیزاسیون زاویه ای که در [۱۵] آمده و نیز کدهای مخروطی در [۱۴] مقایسه شده است. همان‌طور که می‌بینیم نتایج روش پیشنهادی بهتر از AQIM می‌باشد. این موضوع بهبود عملکرد طرح دورانی را به کوانیزاسیون برداری به خوبی نشان می‌دهد.



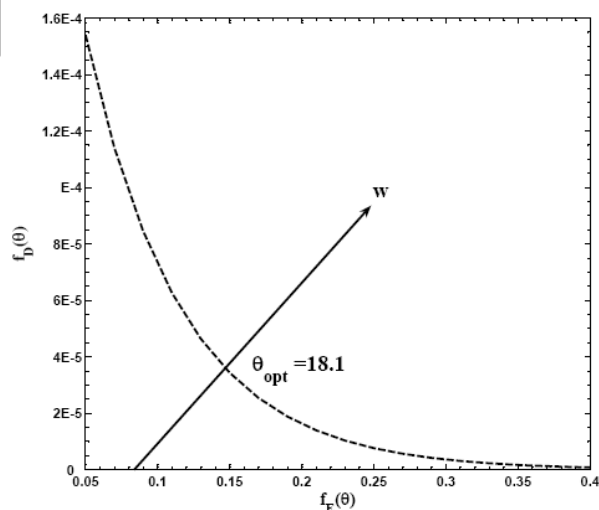
شکل ۴ - مقایسه احتمال خطای تئوری با نتایج تجربی در $\sigma_n=40$

حال شبیه‌سازی را برای تصاویر واقعی تصاویر انجام می‌دهیم. در این راستا از موجک با فیلترهای متقارن Daubechies استفاده می‌کنیم. درج نهان نگاره در سطح دوم ضرایب تقریب در هر بلوک صورت می‌پذیرد. نتایج با میانگین‌گیری روی ۵۰ اجرای متفاوت صورت پذیرفته است. به این منظور تصاویر زیادی نظیر هواپیما، دزد دریایی، قایق و پل با اندازه 512×512 مورد استفاده قرار گرفته‌اند. تصاویر پاک و نهان نگاری شده با بلوک‌های 16×16 که شامل مجموعاً ۱۳۸ بیت نهان نگاره هستند در شکل (۶)، (۷) به نمایش درآمده‌اند. همچنین زاویه θ که در قبل معرفی شد بنا به تصویر بین

دسترس در فضای توابع هدف است. کمترین مقدار λ در F_s رخ می‌دهد، جایی که بردار $F^* + w\lambda$ مرز پایینی فضای اهداف را قطع می‌کند.



شکل ۲- روش بهینه سازی کسب هدف



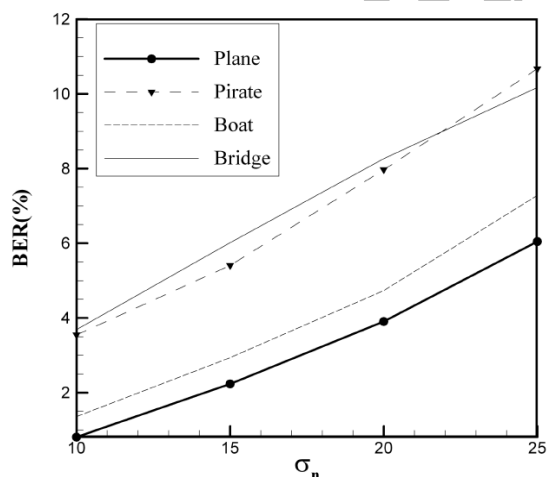
شکل ۳- پیاده سازی روش بهینه سازی کسب هدف برای بدست آوردن θ بهینه

در شکل (۳) روش کسب هدف بر روی تصویر باربارا نشان داده شده است. در این شکل مقدار $f_E(\theta)$ بر حسب $f_D(\theta)$ رسم شده است در حالی که پارامتر θ بر حسب وزن تغییر می‌کند. با توجه به این شکل دیده می‌شود که با انتخاب بردار وزن به صورت $[0.16 \ 0.14]$ برای $(f_D(\theta), f_E(\theta))$ ، نقطه بهینه $\theta = 18/1$ درجه بدست آمده است. روند مشابهی برای بدست آوردن θ بهینه برای هر تصویر طی شده است.

همانگونه که مشهود است الگوریتم دوران در مقابل نویز به شدت مقاوم است. مهمترین دلیل این مقاومت بهینه بودن الگوریتم آشکارسازی است. حمله دوم در اینجا بررسی می شود فشرده سازی به روش JPEG است. مقاومت بالا نسبت به این حمله در این نکته نهفته است که اطلاعات نهان نگاری در ضرایب تقریب نهفته شده اند. لذا الگوریتم JPEG که عموماً روی مؤلفه های فرکانس بالای تصویر کار می کند نمی تواند روش پیشنهادی را تخریب کند.



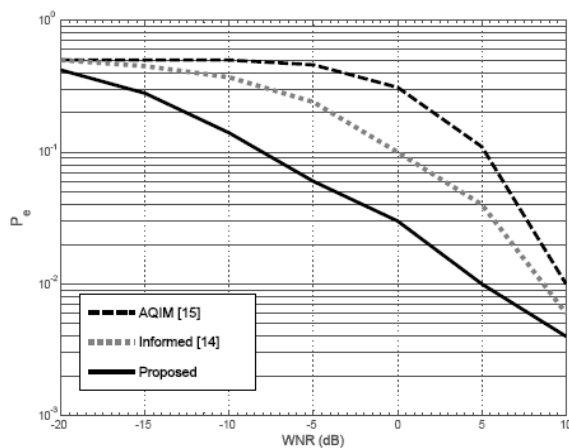
شکل ۷- چپ تصویر اصلی و راست تصویر نهان نگاری شده (تصاویر قایق و پل)



شکل ۸ - حمله نویز به زای واریانس های متفاوت

در حمله سوم فیلتر میانه و فیلتر گوسی بر روی الگوریتم نهان نگاری اعمال شده اند. جدول (۱) درصد احتمال خطای بیت را نشان می دهد که نتایج حاصل نشان دهنده این است که روش ارائه

۱۶ تا ۲۰ درجه انتخاب شده است. این مقادیر برحسب رابطه بهینه سازی (۳۳) بدست آمده اند؛ به گونه ای که هم پایداری خوبی در برابر حملات داشته باشد و هم شفافیت نهان نگاره حفظ شود. همان طور که در شکل (۶) هویدا است، نامحسوس بودن نهان نگاره به خوبی لحاظ شده است. پارامتر بیشینه نسبت سیگنال به نویز (PSNR) در تصاویر مربوط به ترتیب ۴۰/۴۰، ۴۰/۴۵، ۳۹/۹ و ۴۰/۸ می باشند.



شکل ۵ - مقایسه احتمال خطای روش پیشنهادی با روش [۱۴] و [۱۵]



شکل ۶- چپ تصویر اصلی و راست تصویر نهان نگاری شده (تصاویر هواپیما و دزد دریایی)

اولین حمله ای که اینجا مورد بررسی قرار می گیرد نویز سفید گوسی است. شکل (۸) و (۹) نتایج شبیه سازی را نشان می دهد.

[۱۵] در برابر این نوع حملات می باشد. درحالی که روش پیشنهادی مقاومت خود را حفظ می کند. در جدول (۳) نیز روش پیشنهادی با روش ارائه شده در [۲۳] مقایسه شده است. نتایج این جدول نشان می دهند که روش معرفی شده مقاومت بهتری نسبت به [۲۳] بعد از اعمال فیلتر میانه دارد.

جدول ۳- مقایسه روش پیشنهادی با [۲۳] بعد از اعمال فیلتر میانه ۳×۳

روش	تصویر		
	باربارا	میمون	فلفل
[۲۲]	۲۴/۹۵	۳۱/۶۵	۲۹/۳۵
پیشنهادی	۸/۰	۱۰/۸۸	۴/۲۵
			۲۵/۶۰
			۱/۹۵

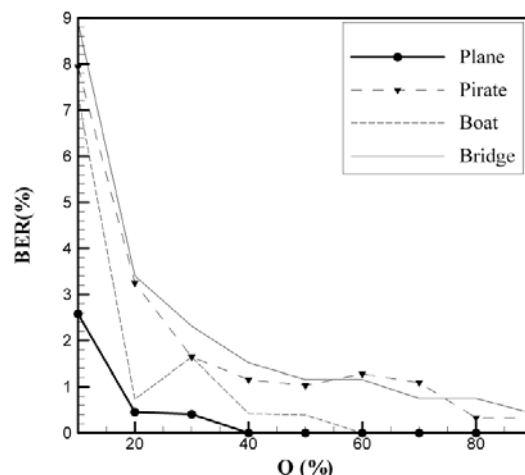
۷- نتیجه گیری

در این مقاله یک روش کور نهان نگاری مبتنی بر چرخش شیب پاره خط حاصل از چهار نمونه تصادفی از ضرایب تقریب بلوک های غیرهمپوشان تصویر معرفی گردید و مورد تحلیل و بررسی قرار گرفت. با فرض گوسی بودن نمونه های تقریب تابع چگالی تجمعی و احتمال شیب پاره خط محاسبه گردید و گیرنده بهینه در حضور نویز برای آن طراحی شد. برای بهینه بودن توان نهان نگاره که وابسته به میزان چرخش شیب پاره خط داشت از روش بهینه سازی چندهدفه استفاده شد. برای ارضای شرط شفافیت از اندیس اندازه گیری کیفیت و برای مقاومت در برابر حملات روابط تحلیلی احتمال خطا مورد استفاده قرار گرفت. در نتیجه این بهینه سازی، درج نهان نگاره در ضرایب تقریب موجک و نیز بهینه بودن گیرنده روش بسیار مقاومی پدید آمد که بر روش های پیشین برتری دارد. نتایج شبیه سازی ها بهتر بودن عملکرد الگوریتم پیشنهادی را بر سایر روش ها تأیید می کند. همچنین بدلیل ماهیت شیب پاره خط که با تغییر ضریب بهره بدون تغییر باقی می ماند روش نسبت به حمله بهره نیز مقاوم است. کار آینده می تواند تعمیم عمل درج نهان نگاری به چندنشانه ای (M-array) به جای باینری باشد.

۸- مراجع

- [1] Chun-Shien Lu; **Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property**, Idea Group Publishing, 1st ed., 2002

شده مقاومت بالایی نسبت به این نوع حملات دارد. دلیل این امر نیز نهان نگاری در ضرایب حاوی فرکانس پایین است.



شکل ۹- حمله فشرده سازی بازای ضریب کیفیت های گوناگون

جدول ۱- نتایج شبیه سازی بعد از فیلتر گوسی و میانه

تصویر	فیلتر گوسی		
	۳×۳	۵×۵	۷×۷
هواپیما	۲/۶۹	۰/۳۹	۱/۱۹
دزد دریایی	۵/۲۳	۱/۶۶	۲/۷۷
قایق	۱۳/۱۳	۱/۷۳	۲/۶۹
پل	۱۳/۱۴	۱/۱۱	۲/۸۰

در نهایت ما روش پیشنهادی را با دو روش کور و جدید مقایسه نموده ایم [۱۵] و [۲۳]. همان طور که جدول (۲) و (۳) نمایش می دهد الگوریتم دوران بطور محسوس دارای عملکرد بهتر از این دو روش است.

جدول ۲- مقایسه روش پیشنهادی با [۱۵] در حضور نویز

روش	σ_n					
	۱	۲	۳	۴	۵	۶
[۱۵]	۱/۰	۲/۰	۳/۰	۴/۰	۱۵/۰	۲۵/۰
پیشنهادی	۰/۰	۰/۰	۰/۱۲	۰/۱۲	۰/۴۳	۱/۲۵
						۱/۰۵

چنان که دیده می شود با افزایش نویز روش [۱۵] دچار شکست می گردد به عبارتی احتمال خطای بیت به سمت ۵۰ در صد میل می کند که این موضوع نشان دهنده شکست الگوریتم ارائه شده در

- [15] C. Chen, X. Wu; “**An Angel QIM Watermarking Based on Watson Berceptual Model**,” in Proc. International Conference on Image and Graphics, Chengdu, Sichuan, China, 2007.
- [16] F. Ourique, F. Perez-Gonzalez; “**Angel QIM: A Novel Watermarking Embedding Scheme Robust Against Amplitude Scaling Distortion**”, in Proc. ICASSP 2005, Vol.2, No. 1, pp. 797 - 800, 2005.
- [17] F. Perz-Gonzalez, C. Mosquera, M. Barni, A. Abrado; “**Rational Dither Modulation: A High Rate Rata-Hiding Method Invariant to Gain Attacks**”, IEEE Trams. Signal Process. Vol. 53, No. 10, pp. 3960 - 3975, Oct 2005.
- [18] S.M.E. Saheaeian, M.A. Akhaee, F. Marvasti; “**Blind Image Watermarking Based on Sample Rotation with Optimal Detector**”, Accepted in 17th European Signal Processing Conference (EUSIPCO), Glasgow, Scotland, UK, 2009.
- [19] Z. Wang, A.C. Bovik; “**Image Quality Assessment: From Error Visibility to Structural Similarity**”, IEEE Trans. on Image Process., Vol. 13, No. 4, pp. 600–612, 2004
- [20] Z. Wang, A.C. Bovik; “**A Universal Image Quality Index**”, IEEE Signal Processing Letters, Vol. 9, No. 3, pp. 81 – 84, 2002.
- [21] M.A. Akhaee, S.M.E. Sahraeian, B. Sankur, F. Marvasti; “**Robust Scaling Based Image Watermarking Using Maximum Likelihood Decoder with Optimum Strength Factor**”, IEEE Trans. on Multimedia, Vol. 11, No.4, pp. 431 - 444, Aug 2009
- [22] F. Gembicki , Y. Haimes; “**Approach to Performance and Sensitivity Multiobjective Optimization: The Goal Attainment Method**”, IEEE Transactions on Automatic control, Vol. 20, No. 6, pp. 769 - 771, 1975.
- [23] Y. Wang, J.F. Doherty, R.E. Van Dyck; “**A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images**”, IEEE Transactions on Image Processing, Vol. 11, No. 2, pp. 77 – 88, 2002.
- [2] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn; “**Information Hiding—A Survey**”, Proc. IEEE, Vol. 87, No. 7, pp. 1062–1078, 1999.
- [3] I.J. Cox, M.L. Miller, J.A. Bloom; **Digital Watermarking** (1st Ed.). San Francisco: Morgan Kaufmann, 2002.
- [4] J. Seitz; **Digital Watermarking for Digital Media**, Information Science Publishing, 1st ed., 2005.
- [5] A. Ker; **Improved Detection of LSB Steganography in Grayscale Images**, in Proc. Information Hiding Workshop 3200, Springer LNCS, pp. 97 – 115, 2004.
- [6] J.Mielikainen, “**LSB Matching Revisited**”, IEEE signal processing letters, Vol. 13, No. 5, pp. 285-287, May 2006.
- [7] B. Chen, G. Wornell; “**Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding**”, IEEE Trans. Inf. Theory, Vol. 47, No. 4, pp. 1423 - 1443, May 2001.
- [8] J. J. Eggers, R. Bauml, R. Tzschoppe, B. Girod; “**Scalar Costa Scheme for Information Embedding**”, IEEE Trans. Signal Process., Vol. 4, No. 51, pp. 1003 - 1019, Apr. 2003.
- [9] Q. Zhang, N. Boston; “**Quantization Index Modulation Using E8 Lattice**”, in Proc. 41th Annual Allerton Conf. on Communication, Control and Computing, Allerton, IL, USA, 2003.
- [10] K. Yeo, H. J. Kim; “**Modified Patchwork Algorithm: A Novel Audio Watermarking Scheme**”, IEEE Trans. Speech Audio Process., Vol. 11, No. 4, pp. 381 – 386, Jul 2003
- [11] K. Yeo, H.J. Kim; “**Generalized Patchwork Algorithm for Image Watermarking**”, Multimedia Syst. Vol. 9, No. 3, pp. 261 - 265, 2003
- [12] J.J. Eggers, R. Bauml, B. Girod; “**Estimation of Amplitude Modifications Before SCS Watermark Detection**”, in Proc. SPIE Security Multimedia Content P. W. Wong and E. J. Delp, Eds. San Jose, CA, Vol. 4675, No. 1, pp. 387 - 398, Jan 2002
- [13] J.H. Conway, N.J.A. Sloane; **Sphere Packing, Lattices, and Groups**, New York: Springer-Verlag, 2nd ed.,1999
- [14] M.L. Miller, G.J. Doerr, I. J. Cox; “**Applying Informed Coding and Embedding to Design Robust, High Capacity, Watermark**”, IEEE Trans. Image Process., Vol. 13, No. 16, pp. 792 - 807, June 2004.