

یک روش نهان نگاری چندلایه برگشت پذیر و قابل تطبیق در حوزه موجک

مهدی صادقی^{۱*}، احمد عقیفی^۲

۱- کارشناسی ارشد، گروه برق، دانشگاه آزاد اسلامی، واحد اراک ۲- استادیار، مجتمع دانشگاهی برق الکترونیک، دانشگاه صنعتی مالک اشتر (دریافت: ۹۱/۰۷/۵، پذیرش: ۹۱/۱۲/۲۱)

چکیده

در این مقاله، یک روش نهان نگاری چندلایه برگشت پذیر پیشنهاد شده است که پیام، در ضرایب فرکانس بالای تبدیل موجک حقیقی به حقیقی هار و به ترتیب، در باند قطری، عمودی و سپس افقی جاسازی می شود. عملیات جاسازی، یک فرآیند دو فازی بوده و براساس قدم-مطلق اختلاف بین پیکسل های متوالی، انجام می شود. به عبارت دیگر، ابتدا لبه های تیزتری برای جاسازی انتخاب شده و نواحی نرم، بدون تغییر باقی می ماند و با افزایش نرخ جاسازی، لبه های بیشتری آزاد می گردند. فاز دوم نیز در برخی حالت ها، تغییرات فاز اول را خنثی می کند. نتایج آزمایش-ها، ظرفیت و سیگنال به نویز بالاتر روش پیشنهادی نسبت به روش نشان می دهد. علاوه بر آن، نسبت به جیا، سیگنال به نویز بالاتری داشته و مشخصات آماری تصویر نهان نگاره، مانند هیستوگرام، میانگین، واریانس، چولگی و کشیدگی، مطابقت بیشتری با تصویر پوشش دارد.

واژه های کلیدی: نهان نگاری، نهان کاوی، برگشت پذیر، رمزگذاری، نشانه گذاری، امنیت

۱. مقدمه

امروزه، ایجاد امنیت در تبادل پیام های متنی، صوتی و تصویری از طریق شبکه های مختلف ارتباطی، یکی از مهم ترین دغدغه های بشر و سامانه های تبادل اطلاعات می باشد. در این مسیر، استفاده از روش هایی که بتوانند ضمن ایجاد امنیت بالا، کمترین تأثیر منفی در ارتباطات و شبکه های ارتباطی را ایجاد و همچنین، کمترین افزونگی را بر کانال های ارتباطی تحمیل نماید، از ویژگی های اصلی روش های ایجاد امنیت می باشد. نهان نگاری^۱، هنر ارتباطات مخفی است، طوری که فقط فرستنده و گیرنده، از ارتباطات مخفی باخبر باشند [۱]. برای انجام این کار، پیام (معمولا متن یا تصویر) درون تصویر دیگری جاسازی می شود به طوری که اطلاعات نهان شده، قابل رویت نبوده و به سادگی، وجود پیام نهان شده قابل کشف نباشد.

بنابراین، نهان نگاری به عنوان رهیافتی برای پنهان نمودن ارتباطات و همچنین، جلوگیری از آسیب های امنیت ناشی از آشکار بودن ارتباطات به کار می رود. روش های نهان نگاری چندلایه، اطلاعات را در چندین لایه مختلف درون تصویر مخفی می کنند. این لایه ها می توانند از ترکیب روش های نهان نگاری حوزه زمان یا حوزه

امروزه، ایجاد امنیت در تبادل پیام های متنی، صوتی و تصویری از طریق شبکه های مختلف ارتباطی، یکی از مهم ترین دغدغه های بشر و سامانه های تبادل اطلاعات می باشد. در این مسیر، استفاده از روش هایی که بتوانند ضمن ایجاد امنیت بالا، کمترین تأثیر منفی در ارتباطات و شبکه های ارتباطی را ایجاد و همچنین، کمترین افزونگی را بر کانال های ارتباطی تحمیل نماید، از ویژگی های اصلی روش های ایجاد امنیت می باشد. نهان نگاری^۱، هنر ارتباطات مخفی است، طوری که فقط فرستنده و گیرنده، از ارتباطات مخفی باخبر باشند [۱]. برای انجام این کار، پیام (معمولا متن یا تصویر) درون تصویر دیگری جاسازی می شود به طوری که اطلاعات نهان شده، قابل رویت نبوده و به سادگی، وجود پیام نهان شده قابل کشف نباشد.

بنابراین، نهان نگاری به عنوان رهیافتی برای پنهان نمودن ارتباطات و همچنین، جلوگیری از آسیب های امنیت ناشی از آشکار بودن ارتباطات به کار می رود. روش های نهان نگاری چندلایه، اطلاعات را در چندین لایه مختلف درون تصویر مخفی می کنند. این لایه ها می توانند از ترکیب روش های نهان نگاری حوزه زمان یا حوزه

علاوه بر آن، سیگنال به نویز از لایه دوم تا پنجم، ثابت می‌ماند. به عبارت دیگر، با وجود جاسازی پنج لایه و رسیدن به ظرفیت $3/28 \text{ bps}$ ، سیگنال به نویز همچنان بالاتر از 54 dB است.

از جمله روش‌های حوزه موجک برگشت پذیر، می‌توان به یوسفی [۹]، چن [۱۰] و وو [۱۱] اشاره کرد. اساس روش یوسفی، مبتنی بر پیدا کردن چند نقطه پیک، درون هیستوگرام باندهای فرکانس بالای تبدیل موجک حقیقی به حقیقی $CDF(2,2)$ است. پس از شیفت دادن، بیت پیام، درون نقاط پیک جاسازی می‌شود. مشخص است که هرچه تعداد نقاط پیک بیشتری پیدا شود، ظرفیت بیشتر شده ولی سیگنال به نویز، کاهش می‌یابد. در سال ۲۰۰۹، چن [۱۰] روش [۱۲] چنگ^۸ را با تغییراتی به حوزه تبدیل موجک اعمال کرده است. جاسازی در هر چهار باند تبدیل موجک حقیقی به حقیقی $CDF(2,2)$ انجام می‌شود. این روش در جاسازی یک لایه، به ظرفیت 1 bps و سیگنال به نویز 45 dB دست یافت. در سال ۲۰۱۱، وو [۱۱]، روش [۱۳] لیانگ^۹ را با تغییراتی به حوزه موجک منتقل کرده است. پیام، درون نقطه پیک هیستوگرام قدرمطلق اختلاف پیکسل‌های متوالی جاسازی می‌شود. جاسازی در هر چهار باند تبدیل موجک حقیقی به حقیقی $CDF(9,7)$ انجام می‌شود.

در این مقاله، یک روش نهان‌نگاری چندلایه برگشت پذیر در حوزه موجک پیشنهاد شده است که جاسازی پیام را از بلوک‌های لبه آغاز می‌کند. نتایج آزمایش‌ها، بالاتر بودن ظرفیت و سیگنال به نویز روش پیشنهادی نسبت به [۱۱] وو را نشان می‌دهد. علاوه بر آن، نسبت به جیا^{۱۰}، سیگنال به نویز بالاتر و امنیت بهتری دارد. مقاله به صورت زیر سازمان‌دهی شده است. در بخش ۲، الگوریتم فرستنده و گیرنده روش جیا مورد بررسی قرار گرفته و بخش ۳، تبدیل موجک حقیقی به حقیقی هار را معرفی کرده است. روش حوزه موجک پیشنهادی، در بخش ۴ تشریح شده و نتایج شبیه‌سازی در بخش ۵ آورده شده است. در انتها، نتیجه‌گیری مقاله در بخش ۶ آمده است.

۲. بازبینی روش جیا [۲]

برای جاسازی پیام، تصویر پوشش به بلوک‌های 1×2 پیکسلی غیرهمپوشان تقسیم می‌شود. برای بلوک‌هایی که مقدار پیکسل دوم آنها زوج است، بیت متناظر در نقشه جاسازی فاز اول، یک شده و مقدار پیکسل، به علاوه بیت پیام می‌شود.

دو فن به کار گرفته شده، در اکثر روش‌های برگشت پذیر حوزه زمان، بسط تفاضلی و شیفت هیستوگرام هستند. دسته اول، ظرفیت بیشتری را فراهم می‌کند؛ در حالی که دسته دوم، سیگنال به نویز بهتری به دست می‌دهد [۴]. در سال ۲۰۰۸، لین^۱ یک روش برگشت پذیر مبتنی بر شیفت هیستوگرام برای استفاده در نشانه-گذاری ارائه کرد [۵].

در این روش، از قدرمطلق اختلاف بین پیکسل‌های همسایه برای تشکیل هیستوگرام تفاضلی، استفاده شده است. بیت پیام نیز در نقطه پیک، جاسازی می‌شود. متأسفانه، به علت استفاده از پیمانیه 256 ، مقداری نویز فلفل و نمک^۲ در این روش وجود دارد. علاوه بر آن، در بعضی حالت‌ها، توانایی بازبازی تصویر پوشش وجود ندارد [۶]. در سال ۲۰۱۰، ونگ^۳ بهبودی بر روش لین ارائه کرده است [۷]. در این روش، پس از تشکیل هیستوگرام اختلاف بین پیکسل مرکزی و پیکسل‌های همسایه، دو نقطه پیک و صفر درون آن پیدا می‌شود.

در ادامه، پیکسل‌هایی که بین نقاط پیک و صفر قرار دارند، به طور مناسب شیفت یافته و بیت پیام، در نقاط پیک جاسازی می‌شود. این روش، نسبت به روش لین و Ni، ظرفیت و سیگنال به نویز بهتری دارد [۸]. مشخص است که ارسال نقاط پیک و صفر برای بازبازی در گیرنده، الزامی است. به عنوان مثال، برای یک تصویر 512×512 که به بلوک‌های 4×4 تقسیم شده است، در روش لین، نیاز به ارسال 16384 نقطه پیک هست [۶]. برای حل این مشکل، زاوو^۴ و زنگ^۵ به ترتیب از هیستوگرام اختلاف پیکسل‌های متوالی با ثابت نگه داشتن پیکسل اول و هیستوگرام اختلاف پیکسل مرجع و سایر پیکسل‌ها، در حالی که پیکسل مرجع ثابت است، برای جاسازی داده، استفاده کردند [۶ و ۴].

زنگ، بیت پیام را در مقادیری که برابر مثبت / منفی آستانه هستند، جاسازی می‌کند؛ در حالی که زاوو، از اختلاف‌هایی که برابر لایه جاسازی هستند، استفاده می‌کند. کاربرد ذکر شده، برای این روش نهان‌نگاری است و مزیت مشترک این دو روش، عدم ارسال نقاط پیک و صفر به گیرنده است. در سال ۲۰۱۰، جیا یک روش چندلایه برگشت پذیر پیشنهاد کرده است که عملیات جاسازی این روش، فقط در پیکسل دوم بلوک‌های 1×2 پیکسلی و در دو فاز انجام می‌شود. با استفاده از فنی، فرآیند جاسازی فاز دوم در بعضی حالت‌ها، قادر به خنثی کردن تغییرات فاز اول می‌باشد.

6- Wu
7- Chen
8- Chan
9- Liang
10- Jia

1- Lin
2- Salt & Peeper
3- Wang
4- Zhao
5- Zeng

جدول ۱. تحلیل روش جیا [۲]

		even			odd	
Secret Data	1 st Embedding	0	1	1	-	-
	2 st Embedding	-	0	1	0	1
y''		y	$(y+1)-1$	$y+1$	$y-1$	y

۳. تبدیل موجک حقیقی به حقیقی هار

ضرایب تبدیل‌های موجک، اعشاری هستند؛ لذا، وقتی ورودی (همانند تصاویر) شامل مجموعه‌ای از اعداد حقیقی باشد، هیچ تضمینی برای حقیقی ماندن خروجی صافی‌ها وجود ندارد. به همین دلیل، بازیابی تصویر پوشش امکان‌پذیر نیست. با استفاده از تبدیل موجک حقیقی به حقیقی هار، می‌توان از حقیقی بودن خروجی صافی‌ها اطمینان یافت [۱۴].

یکی از تبدیل موجک‌هایی که اعداد حقیقی را به اعداد حقیقی نگاشت می‌کند (یعنی ورودی حقیقی و خروجی حقیقی دارد)، تبدیل S می‌باشد. این تبدیل، همان نسخه حقیقی تبدیل موجک هار می‌باشد [۱۴]. خروجی‌های نرم (S) و جزئیات (d) برای L امین ضریب فرکانس پایین و فرکانس بالا، به ترتیب توسط روابط (۱) و (۲) محاسبه می‌شوند.

$$S_{1,L} = [(S_{0,2L} + S_{0,2L+1}) / 2] \quad (1)$$

$$D_{1,L} = S_{0,2L+1} - S_{0,2L} \quad (2)$$

که در آن، $S_{0,2L}$ و $S_{0,2L+1}$ نمونه‌های متوالی تصویر پوشش هستند. تبدیل معکوس نیز، توسط روابط (۳) و (۴) به دست می‌آید [۱۵].

$$S_{0,2L} = S_{1,L} - [d_{1,L} / 2] \quad (3)$$

$$S_{1,2L+1} = S_{1,L} + [(d_{1,L} + 1) / 2] \quad (4)$$

روابط بالا، یک بعدی هستند؛ لذا، برای اعمال به تصاویر، نیاز به تعمیم آنها هست. تعمیم تبدیل S به دوبعد، در روابط (۵) تا (۸) آمده است [۱۴].

$$A_{1,j} = [(x_{2i,2j} + x_{2i+1,2j}) / 2] \quad (5)$$

$$H_{1,j} = x_{2i,2j+1} - x_{2i,2j} \quad (6)$$

سایر بلوک‌ها در این فاز استفاده نمی‌شوند. نحوه خواندن بلوک‌ها نیز به ترتیب می‌باشد. به عبارت دیگر، از گوشه بالا سمت چپ شروع شده و تا گوشه پایین سمت راست ادامه می‌یابد. این روند تا رسیدن به انتهای تصویر ادامه دارد و خروجی این فاز، به عنوان ورودی فاز بعد در نظر گرفته می‌شود.

در فاز دوم، فرد بودن مقدار پیکسل‌های دوم هر بلوک، به عنوان شرط ورود به فرآیند جاسازی در نظر گرفته می‌شود. برای این بلوک‌ها، بیت متناظر در نقشه جاسازی فاز دوم، یک شده و مقدار پیکسل منهای ممتد بیت، پیام می‌شود. این روند نیز تا رسیدن به انتهای تصویر ادامه دارد که خروجی این فاز، همان تصویر نهان‌نگاره است.

برای استخراج پیام و بازیابی تصویر پوشش، تصویر نهان‌نگاره به بلوک‌های 1×2 پیکسلی غیرهمپوشان تقسیم می‌شود. در ادامه، بیت متناظر با هر بلوک در نقشه جاسازی فاز دوم چک می‌شود. چنانچه این بیت برابر یک باشد، این بلوک حاوی بیت پیام بوده در غیر این صورت، باید بلوک دیگری خوانده شود.

اگر مقدار پیکسل دوم بلوک حاوی پیام زوج باشد، بیت استخراج شده صفر بوده و مقدار پیکسل، یک واحد افزایش می‌یابد. در غیر این صورت، بیت یک استخراج شده و مقدار پیکسل، بدون تغییر باقی می‌ماند. با پایان این مرحله، پیام جاسازی شده در فاز دوم، استخراج شده و تصویر خروجی فاز اول نیز بازیابی می‌شود. این تصویر، به عنوان ورودی به مرحله بعد فرستاده می‌شود.

در مرحله دوم، بلوک‌هایی که بیت متناظر در نقشه جاسازی فاز اول آنها یک است، مورد استفاده قرار می‌گیرند. اگر مقدار پیکسل دوم بلوک حاوی پیام زوج باشد، بیت استخراج شده صفر بوده و مقدار پیکسل، بدون تغییر باقی می‌ماند. در غیر این صورت، بیت استخراج شده یک بوده و مقدار پیکسل، یک واحد کاهش می‌یابد. با پایان این مرحله، پیام جاسازی شده در فاز اول، استخراج شده و تصویر پوشش بازیابی می‌شود.

جدول ۱ تحلیلی از این روش را نشان می‌دهد. همان‌طور که مشاهده می‌شود، اگر مقدار پیکسل دوم بلوک زوج و بیت یک در فاز اول جاسازی شده باشد، با جاسازی بیت صفر در فاز دوم، تغییر فاز اول خنثی می‌شود. علاوه بر آن، چنانچه تماماً صفر در فاز اول و تماماً یک در فاز دوم جاسازی شود، هیچ تغییری در مقادیر تصویر پوشش ایجاد نمی‌شود.

ستون زام این زیرباند باشد. در ادامه، کلیه مقادیر ماتریس‌های L1 و L2 با ابعاد $MBand * (Nband/2)$ ، صفر قرار داده می‌شود. دو متغیر TNew و Told که برای انتخاب لبه‌ها به کار می‌روند، به ترتیب برابر ۳۰ و ۲۵۶ قرار داده و برای هر کدام از زیرباندها، مرحله (۳) انجام می‌شود.

۳. زیرباند مورد نظر به بلوک‌های 1×2 پیکسلی غیرهمپوشان تقسیم شده و بلوک‌ها، به صورت متوالی خوانده می‌شوند. اگر پیکسل دوم بلوک یا $IBand(i,j+1)$ زوج بوده و قدرمطلق اختلاف بین دو پیکسل بلوک در رابطه (۱۳) صدق کند، احتمالاً پیکسل دوم بلوک، در فاز اول جاسازی استفاده شده و به مرحله (۴) وارد می‌شود؛ در غیر این صورت، زوج پیکسل دیگری خوانده می‌شود.

$$abs(IBand(i,j+1)-IBand(i,j)) \geq TNew \ \& \quad (13)$$

$$abs(IBand(i,j+1)-IBand(i,j)) < Told$$

۴. مقدار پیکسل دوم بلوک بعلاوه بیت پیام شده و مجدداً شرط (۱۳) برای مقادیر به دست آمده، چک می‌شود. اگر این شرط برقرار باشد، $L1(i, \frac{j+1}{2}) = 1$ قرار داده شده و بلوک حاصل، به جای بلوک متناظر، زیرباند خروجی فاز اول قرار می‌گیرد؛ یعنی:

$$StegoBand1(i,j) = IBand(i,j), \quad (14)$$

$$StegoBand1(i,j+1) = IBand(i,j+1) \oplus Messagebit$$

در غیر این صورت، همان بیت، درون زوج پیکسل دیگری باید جاسازی شود. این روند تا زمانی که تمام بلوک‌های زیرباند مورد نظر خوانده شود، ادامه می‌یابد. زیرباند خروجی این مرحله یا همان Stegoband1، به عنوان ورودی فاز دوم در نظر گرفته شده و به مرحله (۵) می‌رویم.

۵. در فاز دوم، اگر مقدار $StegoBand1(i,j+1)$ فرد بوده و رابطه (۱۵) برقرار باشد، احتمالاً پیکسل دوم بلوک در فاز دوم استفاده شده و به مرحله (۶) می‌رویم. در غیر این صورت، زوج پیکسل دیگری خوانده می‌شود.

$$abs(StegoBand1(i,j+1)-StegoBand1(i,j)) \geq TNew \ \& \quad (15)$$

$$abs(StegoBand1(i,j+1)-StegoBand1(i,j)) < Told$$

۶. مقدار پیکسل دوم بلوک، طبق رابطه (۱۶) تغییر یافته و مجدداً شرط (۱۵) برای مقادیر به دست آمده، چک می‌شود. اگر این شرط برقرار باشد، $L2(i, \frac{j+1}{2}) = 1$ قرار داده و مقادیر به دست آمده طبق رابطه (۱۷) به جای بلوک متناظر، زیرباند نهان‌نگاره قرار می‌گیرند.

$$V_{i,j} = X_{2i+1,2j} - X_{2i,2j} \quad (7)$$

$$D_{i,j} = X_{2i+1,2j-1} - X_{2i,2j} \quad (8)$$

در روابط بالا، x بیانگر نمونه‌های تصویر پوشش، A تخمین تصویر (یا باند CA)، H باند افقی (یا باند CH) و V باند قطری (یا باند CV) می‌باشد. مقادیر تصویر پوشش نیز، توسط روابط (۹) تا (۱۲) محاسبه می‌شوند [۱۴].

$$X_{2i,2j} = A_{i,j} - [H_{i,j}/2] \quad (9)$$

$$X_{2i,2j+1} = A_{i,j} + [(H_{i,j}+1)/2] \quad (10)$$

$$X_{2i,2j+1} - X_{2i,2j+1} + V_{i,j} - H_{i,j} \quad (11)$$

$$X_{2i+1,2j+1} = X_{2i+1,2j} + D_{i,j} - V_{i,j} \quad (12)$$

۴. روش پیشنهادی

هرچه قدرمطلق اختلاف بین دو پیکسل متوالی بیشتر باشد، بلوک مورد نظر به ناحیه لبه اختصاص داشته و می‌تواند تغییرات بیشتری را تحمل کند [۱۵]. با استفاده از این ایده، روش پیشنهادی، جاسازی پیام را از بلوک‌هایی که اختلاف زیادی دارند، شروع می‌کند. به عبارت دیگر، در ابتدا لبه‌های تیزتری برای جاسازی پیام انتخاب می‌شود. در صورتی که نتوان پیام مورد نظر را جاسازی کرد، بلوک‌هایی با اختلاف کمتر یا لبه‌های نرم‌تر، آزاد می‌گردند.

برای اطمینان از بازیابی تصویر پوشش، از جاسازی در بلوک‌هایی که اختلاف آنها خارج از محدوده (Told, TNew) باشند و یا پس از جاسازی پیام، خارج از این محدوده بی‌افتند، صرف‌نظر می‌شود. مشخص است که هرچه مقادیر Told و TNew بزرگ تر باشند، لبه‌ها تیزتر بوده و در مقابل، ظرفیت کاهش می‌یابد.

فرآیند جاسازی روش پیشنهادی به صورت زیر است:

۱. از تصویر پوشش، تبدیل موجک حقیقی به حقیقی هار (یک سطحی) گرفته می‌شود. در این صورت، چهار زیرباند تقریب (CA)، عمودی (CV)، افقی (CH) و قطری (CD) به دست می‌آید. باتوجه به اینکه چشم انسان به فرکانس‌های پایین حساسیت بیشتری دارد، از جاسازی در ضرایب فرکانس پایین جلوگیری می‌شود [۱۶].

۲. جاسازی، به ترتیب در باندهای قطری، عمودی و افقی انجام می‌شود. فرض کنید $IBand$ ، زیرباند مورد نظر با ابعاد $MBand * Nband$ و $IBand(i,j)$ ، پیکسل واقع در سطر i ام و

۴. اگر $L1\left(i, \frac{j+1}{2}\right)=1$ بوده و شرط (۱۵) برقرار باشد، آن وقت بیتی درون پیکسل دوم این بلوک جاسازی شده و به مرحله (۵) می‌رویم و در غیر این صورت، زوج پیکسل دیگری خوانده می‌شود.

۵. اگر مقدار پیکسل دوم بلوک زوج باشد، بیت استخراج شده صفر بوده و بازیابی به صورت زیر انجام می‌شود:

$$\text{RecBand}(i,j)=\text{RecBand2}(i,j); \quad (21)$$

$$\text{RecBand}(i,j+1)=\text{RecBand2}(i,j+1)$$

اگر مقدار پیکسل دوم بلوک فرد باشد، بیت استخراج شده یک بوده و بازیابی به صورت زیر انجام می‌شود:

$$\text{RecBand}(i,j)=\text{RecBand2}(i,j); \quad (22)$$

$$\text{RecBand}(i,j+1)=\text{RecBand2}(i,j+1)-1$$

اگر طول پیام استخراج شده برابر طول پیام جاسازی شده در فرستنده باشد، فرآیند استخراج پیام و بازیابی تصویر پوشش به اتمام می‌رسد و در غیر این صورت، پس از انجام تغییرات طبق رابطه (۲۳)، مجدداً به مرحله (۲) برگشت داده می‌شود.

$$\text{TOld}=\text{TNew}; \text{TNew}=\text{TNew}-5 \quad (23)$$

۶. پیام‌های استخراج شده در هر باند، به همان ترتیبی که جاسازی شده است، کنار هم قرار داده می‌شود تا پیام، به صورت کامل استخراج شود.

۷. باندهای بازیابی شده باهم ترکیب شده و با گرفتن عکس تبدیل موجک حقیقی به حقیقی هار، تصویر پوشش بازیابی شده به دست می‌آید. دقت کنید که باند RCA به علت عدم استفاده در فرآیند جاسازی، به طور مستقیم در این مرحله استفاده می‌شود. بعد از جاسازی در باندهای فرکانس بالای تبدیل موجک، احتمال اینکه پس از گرفتن تبدیل موجک معکوس، بعضی از پیکسل‌ها خارج از بازه [۰-۲۵۵] بی‌افتند، وجود دارد. به این حالت سرریز / پاریز می‌گویند و باید از آن جلوگیری نمود [۹]. برای حل این مشکل، مقادیر کوچک‌تر از آستانه (α_0) ، به α_0 و مقادیر بزرگ‌تر از $255-\alpha_0$ ، به $255-\alpha_0$ تغییر می‌یابند و مکان و مقدار چنین پیکسل‌هایی، به صورت کلید رمز به گیرنده ارسال می‌شوند. α_0 نیز با استفاده از نتایج آزمایش‌ها روی پایگاه داده مورد نظر، به دست می‌آید؛ البته، واضح است که مقدار اولیه آن صفر است. چنانچه مقدار α_0 انتخابی، حتی

در غیر این صورت، همان بیت، درون زوج پیکسل دیگری باید جاسازی شود.

$$D = \begin{cases} \text{StegoBand1}(i,j+1)-1 & \text{if Message bit}=0 \\ \text{StegoBand1}(i,j+1) & \text{if Message bit}=1 \end{cases} \quad (16)$$

$$(17)$$

$$\text{StegoBand}(i,j)=\text{StegoBand1}(i,j); \text{StegoBand}(i,j+1)=D$$

حال اگر تعداد بیت‌های جاسازی شده برابر طول پیام باشد، فرآیند جاسازی به اتمام می‌رسد و در غیر این صورت، پس از انجام تغییرات طبق رابطه (۱۸)، به مرحله (۳) برگشته و فرآیند جاسازی تکرار می‌شود.

$$\text{TOld}=\text{TNew}; \text{TNew}=\text{TNew}-5 \quad (18)$$

فرآیند استخراج و بازیابی پیام، به صورت زیر می‌باشد:

۱. پس از گرفتن عکس تبدیل موجک حقیقی به حقیقی از تصویر نهان نگاره، چهار زیرباند RCA, RCH, RCV, RCD به دست می‌آید. دو متغیر $\text{TNew}=30$ و $\text{TOld}=255$ قرار داده می‌شود. زیرباندهای تصویر نهان نگاره به همان ترتیب جاسازی فرستنده، به مرحله (۲) برده شده تا پیام مربوطه استخراج و زیرباند متناظر تصویر پوشش، بازیابی شود.

۲. تصویر نهان نگاره، به بلوک‌های 2×1 پیکسلی غیرهمپوشان تقسیم می‌شود. اگر $L2\left(i, \frac{j+1}{2}\right)=1$ بوده و شرط (۱۵) برقرار باشد، آن وقت بیتی درون پیکسل دوم این بلوک جاسازی شده و به مرحله (۳) می‌رویم و در غیر این صورت، زوج پیکسل دیگری خوانده می‌شود.

۳. اگر مقدار پیکسل دوم بلوک زوج باشد، بیت استخراج شده صفر بوده و بازیابی به صورت زیر انجام می‌شود:

$$\text{RecBand2}(i,j)=\text{StegoBand}(i,j); \quad (19)$$

$$\text{RecBand2}(i,j+1)=\text{StegoBand}(i,j+1)+1$$

اگر مقدار پیکسل دوم بلوک فرد باشد، بیت استخراج شده یک بوده و بازیابی به صورت زیر انجام می‌شود:

$$\text{RecBand2}(i,j)=\text{StegoBand}(i,j); \quad (20)$$

$$\text{RecBand2}(i,j+1)=\text{StegoBand}(i,j+1)$$

پس از خواندن کلیه بلوک‌های تصویر نهان نگاره، به مرحله (۴)

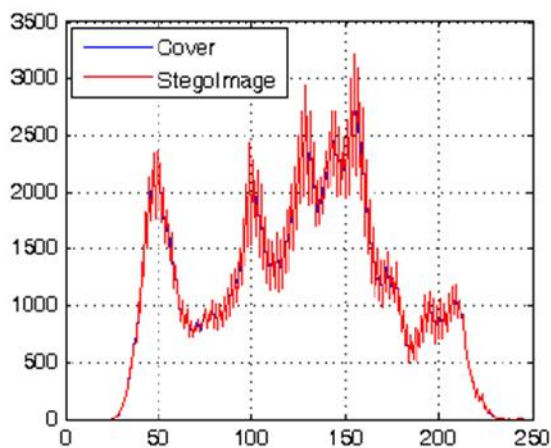
می‌رویم.

جدول ۲. مقایسه سیگنال به نویز روش پیشنهادی و جیا در ظرفیت یکسان

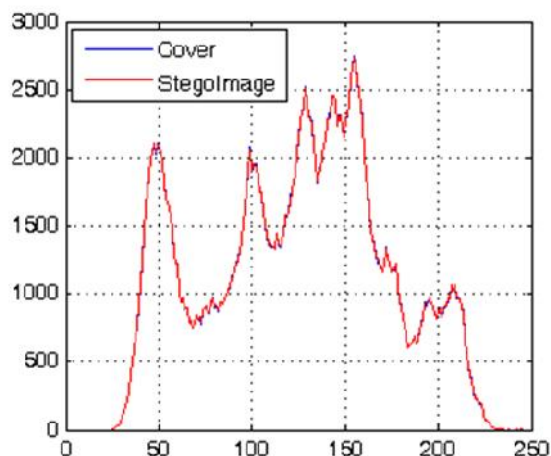
تصویر	روش پیشنهادی جاسازی فقط در باند CD			روش جیا		
	ظرفیت	PSNR	RMSE	در ظرفیت یکسان	PSNR	RMSE
Lena	۳۷۷۲۸	۶۱/۹۶۷۱	۰/۲۰۳۳۲۲	۳۷۷۲۸	۵۹/۵۵۷۷	۰/۲۶۸۳۱۸
Baboon	۳۸۱۱۳	۶۱/۸۳۶۴	۰/۲۰۶۴۰۴	۳۸۱۱۳	۵۹/۵۱۶۷	۰/۲۶۹۵۸۸
F16	۳۸۳۲۲	۶۱/۸۲۶۷	۰/۲۰۶۳۳۵	۳۸۳۲۲	۵۹/۴۹۱۱	۰/۲۷۰۳۸۶
Peepers	۳۷۳۲۵	۶۱/۹۸۷۱	۰/۲۰۲۸۵۳	۳۷۳۲۵	۵۹/۶۰۲۲	۰/۲۶۶۹۵۰
Boat	۳۷۳۸۹	۶۱/۹۵۶۳	۰/۲۰۳۵۷۵	۳۷۳۸۹	۵۹/۵۹۶۳	۰/۲۶۷۱۲۹
Average	۳۷۷۷۵/۲	۶۱/۹۱۴۷	۰/۲۰۴۶	۳۷۷۷۵/۲	۵۹/۵۵۲۸	۰/۲۶۸۵۰

۲.۵. بررسی مشخصات آماری

پیام تصادفی، مطابق روش پیشنهادی فقط درون زیرباند قطری تصویر لنا جاسازی شده است. همان تعداد بیت (یعنی ۳۷۷۲۸ بیت)، مطابق روش جیا در همان تصویر جاسازی شد. هیستوگرام تصویر پوشش و نهان نگاره برای تصویر لنا در روش جیا و روش پیشنهادی به ترتیب در شکل های ۱ و ۲ آمده است.



شکل ۱. هیستوگرام تصویر پوشش و نهان نگاره روش جیا



شکل ۲. هیستوگرام تصویر پوشش و نهان نگاره روش پیشنهادی

برای یک تصویر باعث سرریز / پاریز شود، مقدار آن یک واحد افزایش داده شده و این کار تا زمانی که مشکل سرریز / پاریز حل شود، ادامه می یابد.

۵. نتایج آزمایش

تمام تصاویر مورد استفاده در آزمایش ها، مقیاس خاکستری و با ابعاد 512×512 هستند. پیام جاسازی شده، توسط مولد عدد شبه-تصادفی، تولید شده است.

۱.۵. بررسی کارایی روش پیشنهادی

پیام تصادفی، فقط در زیرباند قطری به اندازه ظرفیت روش Jia جاسازی انجام می شود. نتیجه در جدول ۲ آمده است. همان طور که مشاهده می شود، روش پیشنهادی در ظرفیت یکسان، حدود ۲/۳ dB افزایش سیگنال به نویز دارد. در ادامه، پیام در تمام زیرباندهای فرکانس بالای تبدیل موجک، مطابق روش پیشنهادی جاسازی می شود. جدول ۳ نتایج مقایسه روش پیشنهادی با وو را نشان می دهد. همان طور که مشاهده می شود، ظرفیت تقریباً 0.20 bpp و سیگنال به نویز حدود ۱۰ dB بهبود یافته است.

جدول ۳. مقایسه نتایج روش پیشنهادی با روش وو

تصویر	روش پیشنهادی		روش وو	
	ظرفیت	PSNR	در ظرفیت یکسان	PSNR
Lena	۱۱۴۳۸۷	۵۵/۱۶۳۷	۴۲۳۴۶	۴۴/۲۵
Baboon	۱۱۳۷۲۲	۵۵/۲۱۲۹	۱۴۸۳۴	۴۴/۲۷
Barbara	۱۱۸۷۶۱	۵۵/۰۷۰۳	۴۰۵۲۳	۴۴/۳۲
Peepers	۱۱۳۵۱۳	۵۵/۲۰۸۶	۳۶۹۵۲	۴۴/۲۲
Boat	۱۱۳۴۴۳	۵۵/۲۱۵۸	۳۳۸۵۰	۴۴/۲۳
Average	۱۱۴۷۶۵.۲	۵۵/۱۷۴۳	۳۳۷۰۱	۴۴/۲۵۸

۶. نتیجه گیری

در این مقاله، یک روش چندلایه برگشت پذیر پیشنهاد شده است. از آنجا که میزان اختلاف بیشتر بین پیکسل های متوالی، مشخص کننده لبه یا نرم بودن بلوک مورد نظر است، ابتدا از پیکسل های با اختلاف بزرگ تر مساوی ۳۰ یا لبه های تیزتر برای جاسازی پیام استفاده شد. چنانچه پیام مورد نظر نتواند جاسازی شود، بلوک هایی با اختلاف کمتر برای جاسازی پیام آزاد می گردند. تنها بلوک هایی که مقدار پیکسل دوم آنها زوج بوده و قدرمطلق اختلاف بین دو پیکسل قبل و بعد از فرآیندهای جاسازی قبلی در محدوده (TNew, Told) باشد، برای جاسازی استفاده می شوند. با توجه به بالاتر بودن سیگنال به نویز، تطبیق بیشتر مشخصات آماری و در نتیجه، امنیت بیشتر، انتخاب بلوک های لبه بیشتر برای جاسازی پیام روش پیشنهادی نسبت به جیا، اولویت بالاتری دارد. علاوه بر آن، نسبت به روش وو، ظرفیت و سیگنال به نویز بالاتری دارد.

۷. مراجع

- [1] Cox. I. J, Miller. M. L, Bloom. J. A, Fridrich. J, and Kalker T, Digital Watermarking and Steganography, 2nd ed., R. Adams, Ed. Burlington, USA: Morgan Kaufmann, 2008.
- [2] Jia. L, Shin. S. H, and Yoo. K-Y, "A reversible data hiding scheme using inverse embedding methods in double-embedding strategies," in Informatics and Systems (INFOS), Cairo, pp. 1-7, 2010.
- [3] Li. L, and Luo. B, "A Color Images Steganography Method by Multiple Embedding Strategy Based on Sobel Operator," in International Conference on Multimedia Information Networking and Security, Hubei, pp. 118-121, 2009.
- [4] Zhao. Z, Luo. H, Lu. Z. M, and Pan. J. S, "Reversible data hiding based on multilevel histogram modification and sequential recovery," International Journal of Electronics and Communications, vol. 65, no. 10, pp. 814-826, Oct. 2011.
- [5] Lin. C. C, Tai. W. L, and Chang. C. C, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognition, vol. 41, no. 12, pp. 3582-3591, Dec. 2008.
- [6] Zeng. X. t, Li. Z, and Ping. L. d, "Reversible data hiding scheme using reference pixel and multi-layer embedding," AEU - International Journal of Electronics and Communications, vol. 66, no. 7, p. 532-539, Jul. 2012.
- [7] Wang. S. J, Weng. C. Y, and Goyal. D, "Multilevel Data Hiding for Embedding Reversibility upon Improving Histogram Shifting," in International Computer Symposium (ICS), Tainan, pp. 137-141, 2010.
- [8] Ni. Z, Shi. Y.Q, Ansari. N, and Su. W, "Reversible Data Hiding," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, vol. 16, no. 3, pp. 354-362, Mar. 2006.

همان طور که مشاهده می شود، نوسانات شدیدی در هیستوگرام تصویر نهان نگاره روش جیا وجود دارد، در حالی که در ظرفیت یکسان، مطابقت بیشتری بین هیستوگرام تصویر نهان نگاره و پوشش در روش پیشنهادی بوده و نوسانات وجود ندارد. بنابراین، روش پیشنهادی با توجه به حفظ بیشتر هیستوگرام، امنیت بیشتری نسبت به روش جیا دارد. برای بررسی بیشتر، سایر مشخصات آماری تصویر پوشش و نهان نگاره یعنی میانگین، واریانس، کشیدگی و چولگی، برای پنج تصویر Lena Baboon, F16, Peepers, Boat, Toldmin محاسبه می شود. منظور از Toldmin، حداقل مقدار Told است که در فرآیند جاسازی استفاده می شود. در ادامه، متوسط قدرمطلق اختلاف بین مشخصات آماری تصویر پوشش با مقدار متناظر آن در تصویر نهان نگاره، به عنوان معیار مقایسه امنیت به کار می رود. جدول ۴، نحوه محاسبه برای مشخصه آماری میانگین را نشان می دهد. جدول ۵ نیز مقایسه ای بین متوسط قدرمطلق اختلاف مشخصات آماری روش پیشنهادی و روش جیا را نشان می دهد. همان طور که مشاهده می شود، انحراف مشخصات آماری روش پیشنهادی از تصویر پوشش، نسبت به روش جیا کمتر بوده و لذا، امنیت آن بهتر است.

جدول ۴. قدر مطلق اختلاف میانگین تصویر پوشش و

نهان نگاره در روش پیشنهادی

Told = 0			
Mean	Cover	Stego	Abs(def)
Lena	۱۲۴/۰۴۲۵۱۱	۱۲۴/۰۴۲۵۱۵	۰/۰۰۰۰۰۴
Baboon	۱۲۹/۶۱۴۵۱۳	۱۲۹/۶۱۴۴۶۰	۰/۰۰۰۰۵۳
F16	۱۷۹/۱۷۸۹۰۹	۱۷۹/۱۷۸۳۲۶	۰/۰۰۰۰۵۸۳
Peepers	۱۲۰/۲۱۶۴۲۳	۱۲۰/۲۱۶۲۲۱	۰/۰۰۰۰۲۰۲
Boat	۱۲۹/۷۰۷۹۶۶	۱۲۹/۷۰۸۳۰۲	۰/۰۰۰۰۳۳۶
Average	۱۳۶/۵۵۲۰۶۴	۱۳۶/۵۵۱۹۶۵	۰/۰۰۰۰۲۳۶

جدول ۵. مقایسه مشخصات آماری روش پیشنهادی و جیا در ظرفیت

یکسان و Toldmin متغییر

Told = 20				
	Mean	Var	kurtosis	skewness
Proposed	۰/۰۰۰۲۴۱۰۹	۰/۰۲۶۱۲۵۶۱	۰/۰۰۰۰۴۹۷۴	۰/۰۰۰۰۲۰۷۴
Jia	۰/۰۱۲۶۰۹۸۶	۰/۳۰۹۵۴۳۸۸	۰/۰۰۰۱۹۸۳۰	۰/۰۰۰۰۲۰۱۸۷
Told = 10				
Proposed	۰/۰۰۰۱۹۲۲۶	۰/۰۱۵۷۷۳۶۱	۰/۰۰۰۰۳۲۲۷	۰/۰۰۰۰۱۲۳۰
Jia	۰/۰۲۷۲۱۳۲۹	۰/۴۹۹۱۳۴۶۳	۰/۰۰۰۴۷۷۸۲	۰/۰۰۰۳۲۴۴۴
Told = 0				
Proposed	۰/۰۰۰۲۳۵۷۵	۰/۰۴۰۶۰۸۹۸	۰/۰۰۰۰۶۹۹۴	۰/۰۰۰۰۲۲۲۲
Jia	۰/۰۷۲۰۸۰۲۳	۰/۸۵۵۲۰۲۳۰	۰/۰۰۰۷۷۸۲۷	۰/۰۰۰۴۱۷۰۲

- [13] Tai. W. L, Yeh. C. M, and Chang. C. C, "Reversible data hiding based on histogram modification of pixel differences," IEEE Transaction on Circuits and Systems for Video Technology, vol. 19, no. 6, pp. 906-910, Jun. 2009.
- [14] Ramani. K, Prasad. E. V, and Varadarajan. S, "STEGANOGRAPHY USING BPCS TO THE INTEGER WAVELET TRANSFORMED IMAGE," International Journal of Computer Science and Network Security (IJSNS), vol. 7, no. 7, pp. 293-302, Jul. 2007.
- [15] Wu. D. C and Tsai. W-H, "A steganographic method for image by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, p. 1613-1626, Jun. 2003.
- [16] Shejul. A. A, Kulkarni. U. L, "A DWT based Approach for Steganography Using Biometrics," in International Conference on Data Storage and Data Engineering, Bangalore, pp. 39-43, 2010,
- [9] Yousefil. S, Rabiee. H. R, Yousefi. E, and Ghanbari. M, "Reversible Date Hiding Using Histogram Sorting and IntegerWavelet Transform," in International Conference on Digital Ecosystems and Technologies, Cairns, pp. 487-490, 2007.
- [10] Chen. K. K. and Wang. J. J, "A Novel Reversible Data Hiding Based on Exploiting Modification Direction Algorithm," in International Conference on Multimedia Information Networking and Security, Hubei, pp. 514-518, 2009.
- [11] Wu. X and Zheng. X, "Reversible Data Hiding Based on Histogram Shifting Using Difference Integer Wavelet Coefficients," in International Conference on Business Computing and Global Informatization, Shanghai, pp. 383-386, 2011.
- [12] Chang. C. C, Kieu. T. D, and Chou. Y. C, "Reversible data hiding scheme using two steganographic images," in IEEE Region 10 Conference TENCON, Taipei, pp. 1-4, 2007.