نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۲، تابستان ۱۴۰۰؛ ص ۲۲۸- ۲۱۷

علمی– پژوهشی

طراحی الگوریتم مخفی‌سازی پیام اصلاح‌شده در نهان‌نگاری تصویر مبتنی بر فشرده‌سازی روش AMBTC

محمدعلی شمع‌علیزاده بایی

استادیار دانشکده علوم مهندسی دفاعی، دانشگاه افسری و تربیت پاسداری امام حسین(ع)

(دریافت: ۱۳۹۹/۰۷/۱۲، پذیرش: ۱۴۰۰/۰۲/۲۵)

چکیده

امروزه نهان‌نگاری تصویر، از راه‌های مهم حفاظت از امنیت اطلاعات در شبکه‌های الکترونیکی و به‌خصوص اینترنت است. برای کاهش بار ترافیکی در شبکه‌ها سعی می‌شود از فنون فشرده‌سازی تصویر در کنار نهان‌نگاری استفاده شود. یکی از شیوه‌های نهان‌نگاری در حوزه تصاویر فشرده، نهان‌نگاری مبتنی بر AMBTC بهبودیافته است. این الگوریتم مبتنی بر روش‌های پیشرفته ریاضی طراحی شده است، اما برای مخفی‌سازی بیت‌های پیام در هر سطح بیتی، از کدهای فشرده هر تصویر، از جایگزینی مستقیم استفاده می‌کند، که احتمال تخریب هر بیت در این روش $\frac{۱}{۲}$ است. در این مقاله، به‌جای جایگزینی مستقیم در سطوح بیتی کدهای فشرده، از عملگر xor برای مخفی‌سازی بیت‌های پیام پیشنهاد شده است، که این احتمال را به $\frac{۱}{۴}$ کاهش می‌دهد. نتیجه این اصلاح، بهبود کیفیت بصری تصاویر نهانه، بدون تأثیر بر هیستوگرام آن‌ها است. ارزیابی طرح پیشنهادی با آزمایش معیارهایی چون PSNR، MSE و SSIM، بهبود طرح اصلاح‌شده را برای ۱۰۰۰ تصویر طبیعی نشان می‌دهد.

کلیدواژه‌ها: فشرده‌سازی مبتنی بر AMBTC، نهان‌نگاری مبتنی بر AMBTC بهبودیافته، کمترین تخریب، مخفی‌سازی با عملگر xor.

Designing a Modified Version of the Message Hiding Algorithm in Image Steganography, Based on the AMBTC Compression Method

M. A. Shamalizadeh Baei
Imam Hossein University
(Received: 03/10/2020; Accepted: 15/05/2021)

Abstract

Today, image steganography is one of the most important ways to protect information security in electronic networks, especially the Internet. To reduce the traffic load in the networks, we try to use image compression techniques along with steganography. One of the methods of steganography in the field of compressed images is the AMBTC-based image steganography. This algorithm is based on advanced mathematical methods, but uses a direct replacement to hide the message bits at each bit level of the compressed code of each image. The probability of destroying each bit in this method is %50. In this paper, instead of directly replacing the compressed code bit levels, the xor operator is suggested to hide message bits, which reduces this probability to %25. The result of this correction is the improvement of the visual quality of the hidden images, without affecting their histograms. Evaluation of the proposed design by the testing criteria such as PSNR, MSE and SSIM on 1000 natural images, shows the superiority of the modified design.

Keywords: AMBTC-Based Compression, AMBTC-Based Steganography, Minimal Degradation, Message Hiding, Xor Operator.

*Corresponding Author E-mail: Ma.shamalizade@ihu.ac.ir

۱- مقدمه

علم و هنر مخفی‌سازی پیام در یک رسانه مانند تصویر را نهان‌نگاری و برعکس علم و هنر تحقیق و بررسی وجود پیام در تصویر را نهان‌کاوی گویند. هر تصویر اصلی قبل از مخفی‌سازی پیام را پوشانه و تصویری که پس از مخفی‌سازی پیام در پوشانه به‌دست می‌آید را نهانه گویند [۱].

نهان‌نگاری تصاویر به دو حوزه مکان و حوزه تصاویر فشرده تقسیم می‌شود. نهان‌نگاری در حوزه مکان با دست‌کاری مستقیم پیکسل‌های تصویر صورت می‌گیرد. در حوزه تصاویر فشرده از تبدیلاتی چون، تبدیل فوریه کسینوسی گسسته، تبدیل موجک گسسته، تبدیل آفینی و تبدیل تجزیه یکتا روی تصویر استفاده‌شده و سپس، مخفی‌سازی بیت‌های پیام به روش‌های گوناگون صورت می‌گیرد [۱ و ۲].

BTC[1] و بعد از آن AMBTC[2] روش‌های دیگر فشرده‌سازی تصویر هستند، که مزیت‌های فراوانی همانند کارایی، هزینه محاسباتی پایین و سادگی در پیاده‌سازی را دارند که علاقه‌مندان زیادی را به خود جذب کرده‌اند. به همین دلیل نهان‌نگاری در این حوزه از تصاویر فشرده نیز طرفداران زیادی دارد.

BTC یک روش فشرده‌سازی با اتلاف ساده و کارآمد تصویر است [۳]. این روش، به‌دلیل هزینه محاسباتی پایین و زمان پردازشی بسیار مناسب است. ایده اصلی روشBTC به خاطر فرمول اندازه‌گیری پیکسل‌ها در هر بلوک است به‌طوری‌که برخی از گشتاورهای آماری بلوک‌های کوچک تصاویر سطوح سیاه‌وسفید حفظ شده و کیفیت بصری تصویر فشرده قابل‌قبول باقی می‌ماند.

بعد از BTC، روش AMBTC، که نوعی از BTC است، توسط لما و میچل برای بهبود عملکرد آن ارائه شد [۴]. روش AMBTC ازنظر محاسباتی ساده‌تر از روش BTC است درحالی‌که اولین گشتاور مطلق همراه با گشتاور متوسط را پشتیبانی می‌کند. تفاوت عمده بین AMBTC و BTC محاسبه دو سطح کوانتیزاسیون (پردازش تصویر) در طول مراحل کدگذاری است. بااین‌حال، فرایند کدگشایی تصویر درروش AMBTC همانند روش‌های سنتی BTC است.

در این مقاله اصلاح یک طرح نهان‌نگاری تصویر بهبودیافته بر اساس روش فشرده‌سازی AMBTC ارائه می‌شود. هدف از طرح پیشنهادی، بهبود طرح مخفی‌سازی پیام از طریق اصلاح روش مخفی‌سازی و بهبود کیفت بصری در تصویر نهانه، با حفظ امنیت آماری(هیستوگرام) است. طرحی که قصد اصلاحش را داریم، تصویر را به بلوک‌های صاف و ناصاف(پیچیده) ۴ × ۴ تقسیم کرده، پس از فشرده‌سازی هر بلوک، بیت‌های پیام را در همه بیت-های سطوح بیتی فشرده شده متناظر بلوک‌های صاف، بدن هیچ شرطی جایگزین می‌کند. لذا همان‌طوری که انتظار می‌رود این روش جایگزینی بی‌قیدوشرط، بیشترین تخریب سطوح بیتی را به همراه دارد. بنابراین، در طرح پیشنهادی داده‌ها را طوری در بلوک‌های پوشانه مخفی‌سازی می‌کنیم که تخریب ناشی از این کار تا حد امکان کمینه گردد. برای این کار، با مخفی‌سازی بیت‌های پیام با استفاده از عملگر xor، حداقل تخریب سطوح بیتی صورت می‌گیرد.

در ادامه این مقاله، در بخش دوم روش تحقیق، در بخش سوم پیش‌زمینه تشریح می‌شود. همچنین در بخش چهارم، طرح پیشنهادی مقاله، در بخش پنجم معیارهای سنجش و ارزیابی، بخش ششم پیاده‌سازی تجربی و در بخش هفتم نتیجه‌گیری خواهد شد.

۲- پیشینه تحقیق

هوانگ و همکاران [۵] یک طرح نهان‌نگاری تصویر مبتنی بر BTC با ظرفیت بالایی ارائه دادند. این طرح قابل‌برگشت است، یعنی تصویر پوشانه اصلی می‌تواند به‌صورت کامل از تصویر نهانه بازیابی شود. در این طرح آن‌ها یک حد آستانه برای دسته‌بندی نوع هر بلوک به‌عنوان سطح صاف[3] یا ناصاف (پیچیده[4]) در تصویر تعریف کرده و داده‌های محرمانه را در بیت‌های سطوح بیتی بلوک‌های صاف به‌صورت مشابه مخفی‌سازی نمودند. در طرح هوانگ وقتی حد آستانه‌بالا باشد بیت‌های بیشتری قابل مخفی‌سازی است، اما کیفیت بصری تصویر نهانه به‌صورت قابل‌توجهی کاهش می‌یابد. درنتیجه می‌تواند سوءظن مهاجمان را افزایش داده و منجر به شکست طرح نهان‌نگاری شود.

برای توسعه طرح هوانگ، چانگ و همکاران [۶] یک نهان‌نگاری تصویر قابل‌برگشت با تأکید بر روی تصاویر رنگی فشرده BTC پیشنهاد دادند، که قابلیت برگشت‌پذیری این طرح و طرح‌های مشابه دیگر ظرفیت آن‌ها را پایین نگه‌داشته است. جدیدترین طرح بهبودیافته دیگر در زمینه تصاویر فشرده رنگی توسط لیائو و همکارانش ارائه شده است [۷].

هرچند طرح‌های قابل برگشت برای برخی کاربردها در حوزه‌های نظامی و پزشکی بسیار مهم هستند اما آن‌ها معمولاً از ظرفیت پایین که منجر به محدودیت کاربرد آن‌ها می‌شود، رنج می‌برند.

[1] Block Trunction Coding
[2] Absolut Moment Block Trunction Coding
[3] Smooth
[4] Complex

برای غلبه بر مسائل موجود در طرح هوانگ و همکاران، چن و همکاران [۸] نیز یک طرح بهبودیافته‌ای را پیشنهاد دادند که داده‌ها را در سطوح بیتی با دو سطح کوانتیزه یکسان مخفی‌سازی می‌کند. در این طرح ظرفیت مخفی‌سازی در مقایسه با طرح هوانگ و همکاران کمی بهبود دارد.

برخلاف طرح‌های نهان‌نگاری برگشت‌پذیر دیگر، ویسان و همکاران [۹] یک طرح برگشت‌پذیر مبتنی بر AMBTC پیشنهاد دادند که از پیچیدگی محاسباتی پایینی برخوردار است و در آن داده‌ها به‌طور مستقیم درون کدهای فشرده، مخفی‌سازی می‌شوند، اما ظرفیت مخفی‌سازی آن پایین است. همچنین چین چن چانگ و همکاران [۱۰] روش برگشت‌پذیر دیگری در همان حوزه پیشنهاد کردند، که از کدگذاری محلی مشترک برای مخفی‌سازی اطلاعات استفاده می‌کند. این روش از عملگر xor برای محاسبه اختلاف بین مقدار فعلی و مقدار انتخاب شده استفاده می‌کند. نتایج تجربی نشان می‌دهد که این روش از ظرفیت مخفی‌سازی رضایت بخشی، که متناسب با تصویر نهانه نیز می‌باشد، برخوردار است.

چی چنگ و همکارانش [۱۱] یک طرح نهان‌نگاری پرظرفیت در حوزه‌ی تصاویر فشرده‌ی مبتنی بر AMBT ارائه کردند. در این طرح، ترکیب رشته داده‌ی محرمانه به‌صورت آماری تجزیه تحلیل‌شده و یک فرهنگ لغت جستجوی رمزگذار و رمزگشای منحصربه‌فرد برای تنظیم مقادیر پیکسل‌ها پیشنهاد شد، که در مراحل مخفی‌سازی و استخراج مورداستفاده قرار می‌گیرد. این فرهنگ لغت باعث ارتقای ظرفیت نهان‌نگاری می‌شود، چراکه داده‌های محرمانه با استفاده از این روش کدگذاری مبتنی بر فرهنگ لغت، فشرده‌سازی می‌شوند.

دانهو و ویسان [۱۲] نیز طرح قابل‌برگشت قبلی خود را بهبود دادند. در این طرح بهبودیافته هنگامی‌که داده‌ها در یک بلوک صاف مخفی سازی می‌شوند، دو سطح کوانتیزاسیون بلوک صاف برای به حداقل رساندن تخریب بین بلوک تصاویر نهانه و پوشانه مجدداً محاسبه می‌شود، درنتیجه کیفیت بصری می‌تواند بهبود یابد. از سوی دیگر، بلوک‌های ناصاف یا پیچیده نیز برای مخفی‌سازی داده‌ها مورداستفاده قرار می‌گیرند، که در بعضی از طرح‌های دیگر انجام‌نشده است. برای این کار یک بیت پیام را در هر یک از بلوک‌های ناصاف با جابجایی دو سطح کوانتیزاسیون و سطح بیتی مربوطه مخفی‌سازی می‌کنند(تعویض مقادیر a_i و b_i و IB_i با $\sim IB_i$). چنین راهبرد مخفی‌سازی می‌تواند ظرفیت را بدون ایجاد هیچ‌گونه تخریبی در کیفیت بصری تصویر افزایش دهد. در فرآیند فشرده‌سازیAMBTC، ابتدا هر تصویر ورودی به مجموعه‌ای از بلوک‌های ناهمپوشان B_i از پیکسل‌ها مثلاً ۴ × ۴ تقسیم می‌شود. سپس هر بلوک B_i با استفاده از دو سطح کوانتیزاسیون a_i و b_i و سطح تک‌بیتی IB_i فشرده‌سازی می‌شود. برای هر بلوک B_i، مقدار میانگین $\overline{x}$ و سطوح کوانتیزاسیون a_i و b_i به شرح زیر محاسبه می‌شود:

$$\bar{x} = \frac{1}{M}\sum_{i=1}^{M} x_i \qquad (۱)$$

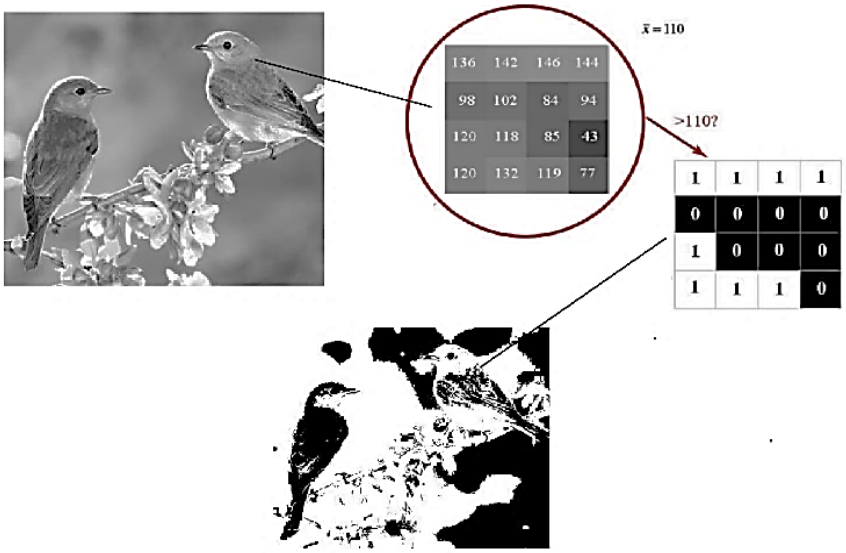
$$a_i = \frac{1}{M-q}\sum_{x_i < \bar{x}} x_i \qquad (۲)$$

$$b_i = \frac{1}{q}\sum_{x_i \geq \bar{x}} x_i \qquad (۳)$$

که در آن x_i نشان‌دهنده شدت روشنایی پیکسل i ام هر بلوک B_i، M نشان‌دهنده تعداد کل پیکسل‌های آن بلوک و q نشان‌دهنده تعداد پیکسل‌هایی است که سطح سیاه‌وسفید آن بزرگ‌تر یا مساوی با مقدار متوسط $\bar{x}$ است می‌باشد. برای بلوک هر B_i، هنگامی‌که مقدار پیکسل بزرگ‌تر یا مساوی $\bar{x}$ است، مقدار ۱ و در غیر این صورت ۰ در سطح بیتی IB_i به‌صورت یک بلوک متناظر در نظر گرفته می‌شود.

در طول فرآیند خارج‌سازی از حالت فشرده نیز دو سطح کوانتیزاسیون a_i و b_i و یک سطح بیتی IB_i برای بازسازی بلوک تصویر مورد نیاز است. شکل (۱). نمونه‌ای از فرایند محاسبه سطح تک‌بیتی برای یک بلوک از تصویر را نشان می‌دهد.

برای هر تصویر فشرده مبتنی بر AMBTC، هر بلوک B_i، مثلاً با ابعاد ۴ × ۴، دارای ۱۶ پیکسل x_i است، که متناظر آن سطح بیتی IB_i، ۱۶ بیت به همراه دو مقدار کوانتیزه‌ی a_i و b_i هرکدام با ۸ بیت است. درمجموع حافظه مصرفی IB_i در هر بلوک فشرده برابر ۳۲ بیت است. بنابراین، برای ۱۶ پیکسل از یک بلوک B_i با ابعاد ۴ × ۴، نرخ فشرده‌سازی روش AMBTC، bpp ۲ است، که برابر روش سنتی BTC است.



شکل۱. نمایش فرایند فشرده‌سازی یک تصویر به روش AMBTC و عکس آن روی یک تصویر.

البته همان‌طوری که در طرح هوانگ و همکاران بیان شد، در روش AMBTC اولین گشتاور مطلق همراه با میانگین را به‌جای استفاده از انحراف استاندارد در روش BTC حفظ می‌کند، به‌طوری‌که روش AMBTC محاسبات تعیین ناصاف بودن هر بلوک را در مقایسه با روش BTC نیاز ندارد [۵].

۳- روش تحقیق

۳-۱- روش AMBTC بهبودیافته

طرح مخفی‌سازی پیام مبتنی بر AMBTC بهبودیافته، شامل یک الگوریتم نهان‌نگاری تصویر با کاهش تخریب بر اساس AMBTC است [۸]. در این طرح هر بلوک صاف، ۱۶ بیت پیام و هر بلوک ناصاف، فقط یک بیت پیام را در خود مخفی می‌کند. البته مخفی‌سازی در هر بلوک ناصاف بدون هیچ‌گونه تغییر و فقط بر طبق یک قاعده قراردادی صورت می‌گیرد. بلوک‌های صاف با کدهای فشرده AMBTC، که برای مخفی سازی عمده بیت‌های پیام استفاده می‌شوند، ۱۶بیت را در بیت‌های هر سطح بیتی به‌صورت نظیر به نظیر جایگزین می‌کند. این راهبرد به دلیل جایگزینی بی‌قیدوشرط بیت‌های پیام در سطح بیتی می‌تواند باعث تخریب کیفیت بصری تصویر نهانه شود. لذا، در این طرح به‌منظور کاهش تخریب هر بلوک صاف دو سطح کوانتیزاسیون a_i و b_i مجدداً محاسبه می‌شوند. بدین ترتیب که پس از جایگزینی بیت‌های پیام در سطح بیتی IB_i، سطح بیتی جدید IB_i' به دست می‌آید.

بنابراین، در این روش بیت‌های سطوح بیتی IB_i' به دو گروه G_0 و G_1 طبقه‌بندی می‌شود، به این صورت که اگر مقدار بیت در IB_i' برابر با ۰ باشد، پیکسل متناظر با آن در B_i به‌عنوان گروه اول (G_0) و بقیه در گروه دوم (G_1) طبقه‌بندی می‌شوند. در این روش، D_i را برای اندازه‌گیری میزان تخریب بین هر بلوک تصویر اصلی و بلوک بازسازی شده نهانه (a_i بجای صفرها و b_i بجای یک‌ها) که شامل بیت‌های پیام مخفی است در نظر می‌گیریم. برای این کار فرض می‌کنیم که نتیجه محاسبه مجدد سطوح کوانتیزاسیون یک بلوک صاف B_i، پس از مخفی‌سازی بیت‌های پیام، به ترتیب a_i' و b_i' باشد در این صورت می‌توان نوشت:

$$D_i=\frac{1}{N}\left(\sum_{x_i \in G_0}(x_i-a_i')^2+\sum_{x_i \in G_1}(x_i-b_i')^2\right) \quad (۴)$$

که در آن x_i نشان دهنده مقدار پیکسل i ام بلوک تصویر اصلی صاف B_i و N نشان‌دهنده تعداد کل پیکسل‌ها در آن بلوک است. برای به دست آوردن بهترین کیفیت بصری از هر بلوک بازسازی شده نهانه، کوانتیزاسیون جدید a_i' و b_i'، باید برای به حداقل رساندن تخریب D_i تعیین شوند . مشتقات جزئی اول و دوم D_i با توجه به متغیرهای a_i' و b_i' به‌صورت زیر محاسبه می‌شوند.

$$\frac{\partial D_i}{\partial a_i'}=-\frac{2}{N}\sum_{x_i \in G_0}(x_i-a_i') \quad (۵)$$

$$\frac{\partial D_i}{\partial b_i'}=-\frac{2}{N}\sum_{x_i \in G_1}(x_i-b_i'). \quad (۶)$$

$$\frac{\partial^2 D_i}{\partial a_i'^2}=\frac{2}{N}\sum_{x_i \in G_0}1. \quad (۷)$$

$$\frac{\partial^2 D_i}{\partial b_i'^2}=\frac{2}{N}\sum_{x_i \in G_1}1. \quad (۸)$$

ازآنجایی‌که $\frac{\partial^2 D_i}{\partial a_i'^2}>0$ و $\frac{\partial^2 D}{\partial b_i'}>0$، حداقل D_i زمانی رخ می‌دهد که در آن مشتقات جزئی مرتبه اول آن با توجه به متغیر

a'_i و b'_i صفر هستند. تنظیم مشتقات جزئی مرتبه اول $\frac{\partial D_i}{\partial a'_i}=0$ ،$\frac{\partial D_i}{\partial b'_i}=0$ و عملکرد دستگاه معادلات به شرح زیر است:

$$\frac{\partial D_i}{\partial a'_i} = -\frac{2}{N}\sum_{x_{i\in G_0}}(x_i - a'_i) = 0 \quad (۹)$$

$$\frac{\partial D_i}{\partial\, b'_i} = -\frac{2}{N}\sum_{x_{i\in G_1}}(x_i - b'_i) = 0 \quad (۱۰)$$

حاصل دو معادله فوق عبارت است از:

$$a'_i = \frac{1}{\sum_{x_i\in G_0}1}\sum_{x_i\in G_0}x_i = \frac{1}{N-q}\sum_{x_i\in G_0}x_i \quad (۱۱)$$

$$b'_i = \frac{1}{\sum_{x_i\in G_1}1}\sum_{x_i\in G_1}x_i = \frac{1}{q}\sum_{x_i\in G_1}x_{i.} \quad (۱۲)$$

که در آن $q=\sum_{x_i\in G_1}1$ نشان‌دهنده تعداد پیکسل‌هایی است، که ارزش آن در B'_iبرابر ۱ است و $N=(\sum_{x_i\in G_0}1+\sum_{x_i\in G_1}1)$ نشان می‌دهد که تعداد کل پیکسل‌ها در B'_i است. دو سطح کوانتیزاسیون محاسبه‌شده به‌عنوان سطوح کوانتیزاسیون جدید در بلوک صاف B_i برای به حداقل رساندن تخریب بلوک اصلی و بلوک بازسازی‌شده نهانه استفاده می‌شود.

توجه داشته باشید که دو سطح کوانتیزاسیون a'_i و b'_i جدید a_i و b_i باید همان ویژگی صاف بودن را تعیین کنند. اگر ویژگی صاف بودن یک بلوک تغییر کند، یعنی شرط $|a_i - b_i| \le \text{thr}$ به $|a'_i - b'_i| > \text{thr}$ تبدیل شود، که ممکن است موجب قضاوت نادرست برای استخراج داده‌های مخفی توسط گیرنده پیام شود. بنابراین، برای جلوگیری از این امر و تضمین این‌که تمام بیت‌های مخفی بتوانند با موفقیت استخراج شوند، در این مورد خاص، هنوز هم از سطوح کوانتیزاسیون قدیمی a_i و b_i به‌جای سطوح جدید a'_i و b'_i استفاده می‌شود.

در طرح بهبودیافته دانهو و ویسان، هنگامی‌که بیت‌های پیام در سطوح بیتی بلوک‌های صاف به‌طور مستقیم جایگزین می‌شوند، لذا برای کاهش تخریب در کیفیت تصویر، این دو سطح کوانتیزاسیون مجدداً محاسبه می‌شوند [۹]. اما بااین‌وجود، ازآنجایی‌که در این روش، بیت‌های پیام بدون در نظر گرفتن هیچ‌گونه شرط و تطبیقی به‌صورت بیت به بیت و مستقیم در سطوح بیتی IB_i جایگزین می‌شوند، احتمال تغییر مقدار شدت روشنایی هر پیکسل زیاد است. برای کاهش این احتمال، در طرح پیشنهادی اصلاح‌شده این مقاله، استفاده از روش مخفی‌سازی xor پیشنهاد می‌شود [۱ و ۲]. این کار باعث می‌شود عمل بازسازی چنین بلوک‌های صاف، پس از مخفی‌سازی پیام از چند گام جلوتر شروع شده و درنتیجه از برآیند میزان تخریب ناشی از مخفی‌سازی پیام کاسته شود. دستورالعمل و تجزیه‌وتحلیل کارایی این روش در بخش ۳- ۲ می‌آید.

۳-۲- مخفی‌سازی پیام با عملگر xor

این روش از یک جدول شاخص با گروه‌های چهار پیکسلی استفاده می‌کند و سه بیت پیام را در پیکسل‌های هر گروه مخفی‌سازی می‌کند. عملگر xor تضمین می‌کند که پیام محرمانه در پوشانه با کمترین تعداد تغییرات پیکسلی پنهان شود. بنابراین، هر سه بیت پیام مانند m_1, m_2, m_3 در ۴ بیت یعنی I_1, I_2, I_3 و I_4 (در اینجا سطر اول IB) مخفی می‌شوند.

$$IB=\begin{bmatrix} I_1 & I_2 & I_3 & I_4 \\ I_5 & I_6 & I_7 & I_8 \\ I_9 & I_{10} & I_{11} & I_{12} \\ I_{13} & I_{14} & I_{15} & I_{16} \end{bmatrix}$$

در گام اول سه عمل xor زیر به‌صورت زیر اجرا می‌شود:

$$\begin{aligned} k_1 &= I_1 \oplus I_2 \\ k_2 &= I_3 \oplus I_4 \\ k_3 &= I_1 \oplus I_3 \end{aligned} \quad (۱۳)$$

در گام دوم برای مخفی‌سازی سه بیت پیام m_1, m_2, m_3 سه بیت محاسبه‌شده k_1, k_2, k_3 با بیت‌های پیام m_1, m_2 و m_3 مقایسه می‌شوند. نتایج این مقایسه که می‌تواند یکی از هشت احتمال باشد که تشخیص می‌دهد که کدام‌یک از چهار بیت I_1, I_2, I_3 و I_4 باید تغییر کنند، جدول (۱) نشان می‌دهد که مخفی‌سازی ۳ بیت پیام در چهار پیکسل پوشانه، حداکثر به‌احتمال ۰/۲۵ آن‌ها را تغییر می‌دهد. این یعنی احتمال تخریب هر پیکسل پوشانه ۰/۲۵ است، این درحالی است که روش جایگزینی مستقیم دارای احتمال تخریب ۰/۵ است. بنابراین انتظار داریم با به‌کارگیری این فن، کیفیت تصویر نهانه بهبود داشته باشد.

و برای استخراج بیت‌های پیام از پیکسل‌های تصویر نهانه ، با فرض اینکه q_1 ، q_2، q_3 و q_4 بیت‌های سطر اول ماتریس سطح بیتی نهانه I_s باشند داریم:

$$\begin{aligned} m_1 &= q_1 \oplus q_2 \\ m_2 &= q_3 \oplus q_4 \\ m_3 &= q_1 \oplus q_3 \end{aligned} \quad (۱۴)$$

جدول۱- شرایط مخفی‌سازی

عمل	شرط			
بدون تغییر	$m_۳ = k_۳$	$m_۲ = k_۲$	$m_۱ = k_۱$	
$\sim I_۲$	$m_۳ = k_۳$	$m_۲ = k_۲$	$m_۱ \neq k_۱$	
$\sim I_۴$	$m_۳ = k_۳$	$m_۲ \neq k_۲$	$m_۱ = k_۱$	
$\sim I_۳ , \sim I_۴$	$m_۳ \neq k_۳$	$m_۲ = k_۲$	$m_۱ = k_۱$	
$\sim I_۲ , \sim I_۴$	$m_۳ = k_۳$	$m_۲ \neq k_۲$	$m_۱ \neq k_۱$	
$\sim I_۳$	$m_۳ \neq k_۳$	$m_۲ \neq k_۲$	$m_۱ = k_۱$	
$\sim I_۱$	$m_۳ \neq k_۳$	$m_۲ = k_۲$	$m_۱ \neq k_۱$	
$\sim I , \sim I_۴$	$m_۳ \neq k_۳$	$m_۲ \neq k_۲$	$m_۱ \neq k_۱$	

۴- طرح پیشنهادی

در این طرح، که در اینجا اصلاح AMBTC بهبودیافته نامیده می‌شود، ابتدا تصویر سیاه‌وسفید اصلی(پوشانه) f به بلوک‌های نا همپوشان B_i با ابعاد k × k پیکسل تقسیم می‌شود (مثلاً ۴ یا ۳ = k) . برای هر بلوک B_i، دو سطح کوانتیزاسیون a_i و b_i با استفاده از معادلات (۲ و ۳) محاسبه می‌شود. طی فرآیند فشرده‌سازی AMBTC، هر بلوک B_i می‌تواند با استفاده از دو سطح کوانتیزاسیون a_i و b_i و سطح بیتی BI_i فشرده‌سازی شود. در این طرح نیز هر بلوک B_i با توجه به یک آستانه از پیش تعیین‌شده، به‌عنوان یک بلوک صاف و یا ناصاف طبقه‌بندی می‌شود. اصلاحیه پیشنهادی در این طرح دو مورد است. مورد اول تعیین آستانه تصمیم‌گیری thr برای شناسایی بلوک‌های صاف یا ناصاف است. مورد دوم استفاده از عملگر xor حین مخفی‌سازی پیام در بلوک‌های صاف است.

نخست برای محاسبه مقدار آستانه تصمیم‌گیری، قدرمطلق تفاضل دو سطح کوانتیزاسیون a_i و b_i در بلوک B_i به‌صورت زیر محاسبه می‌شود:

$$d_i = |a_i - b_i| \quad (۱۵)$$

یکی از مسائلی که در این قسمت باقی می‌ماند تعیین یک آستانه تصمیم‌گیری، جهت تشخیص نواحی صاف از ناصاف یا پیچیده است. برای این کار پیشنهاد می‌شود ابتدا d_i برای همه بلوک‌های B_i محاسبه‌شده سپس d_iها را به‌صورت صعودی مرتب می‌کنیم. شکل(۲) را ببینید.

d_1	d_2	d_3	…	$d_{\|M\|}$	…	d_{l-1}	d_l

شکل۲. محاسبه آستانه تصمیم‌گیری

که در آن |M| طول پیام M است. لذا قرار می‌دهیم $thr = d_{|M|}$ که آستانه تصمیم‌گیری برای انتخاب بلوک صاف یا هموار خواهد بود. بعد از به‌دست آوردن آستانه تصمیم، بلوک‌هایی که در شرط $d_i > thr$ صدق کنند را صاف و بقیه را ناصاف می‌نامیم.

پس طبقه بندی بلوک‌های تصویر، داده‌ها در بلوک‌های صاف طبق الگوریتمی که در ادامه می‌آید با استفاده از عملگر xor در درآیه‌های ماتریس بیتی IB_i، که از بیت‌های ۰ یا ۱ تشکیل‌شده‌اند، مخفی خواهند شد. البته همان‌طوری که قبلاً اشاره شد، هر سه بیت متوالی m_i از رشته پیام M در چهار عنصر بیتی یک سطر از ماتریس بیتی IB_i، طبق جدول (۱) مخفی خواهد شد. در ضمن برتری طرح پیشنهادی اصلاح شده نسبت به طرح قبلی که توسط دانهو و ویسان ارائه شد به این مفهوم برمی‌گردد، چراکه این عملگر به تطبیق مقدار بیت‌های پیام در پوشانه (ماتریس بیتی IB_i) و بیت‌های پیام تأکید دارد. لذا انتظار داریم تأثیر مستقیم بر کیفیت نهانه و درنتیجه به معیارهای کیفی مانند MSE و PSNR و SSIM داشته باشد.

در طرح پیشنهادی این مقاله، مانند طرح دانهو و ویسان، برای بلوک ناصاف هیچ عملیاتی مورد نیاز نیست، به دلیل این‌که در این طرح برعکس AMBTC اصلی، که هر بلوک ناصاف یک بیت مخفی‌سازی می‌کند، هیچ ظرفیتی در نظر گرفته نمی‌شود. در ضمن آستانه‌ی محاسبه شده به روش گفته‌شده، توان افزایش یا کاهش ظرفیت مخفی‌سازی پیام، مطابق با طول پیام، را دارد. فرض کنید که داده‌های رمزگذاری شده ما یک‌رشته بیت به‌صورت مجموعه M زیر باشد. $M = \{M(i) \mid M(i) \in \{۰،۱\}. i = ۱.۲.۳. \dots, n\}$ در این صورت، یک سطح سیاه‌وسفید تصویر اصلی f برای ساخت تصویر نهانه فشرده AMBTC که رشته بیت M در آن مخفی سازی شده، انتخاب می‌شود. بدون از دست دادن کلیت مسئله، ابعاد هر بلوک ۴ × ۴ در نظر گرفته می‌شود. الگوریتم مخفی‌سازی پیام پیشنهادی، که آن را اصلاح بهبودیافته AMBTC می‌نامیم، به‌صورت زیر خواهد بود.

۴-۱- الگوریتم ۱: الگوریتم مخفی‌سازی پیام

ورودی: بیت‌های پیام که به‌صورت رشته بیت M و تصاویر خاکستری (پوشانه) $W \times H$ است.

خروجی: کدهای فشرده Is مطابق تعریف AMBTC.

گام اول: فرض Is = ∅

گام دوم: تصویر خاکستری f را به بلوک‌های ناهمپوشان ۴ × ۴ تقسیم کنید.

گام سوم: از چپ به راست و از بالا به پایین، هر بلوک B_i تصویر f با استفاده از روش AMBTC پردازش کرده و دو سطح کوانتیزاسیون a_i و b_i و یک سطح بیتی IB_i را به‌دست آورید.

گام چهارم: قدر مطلق تفاضل $d_i = |a_i - b_i|$ را برای هر دو سطح کوانتیزاسیون a_i و b_i از بلوک B_i محاسبه کنید.

گام پنجم: حد آستانه thr را بر اساس روش گفته‌شده در بخش تعیین آستانه مطابق با طول پیام محاسبه کنید.

گام ششم: اگر $d_i > thr$ باشد، بلوک B_i به‌عنوان یک بلوک پیچیده یا ناصاف طبقه‌بندی می‌شود، که در آن یک بیت M(i) از M می‌تواند مخفی‌سازی شود، که دو حالت در نظر می‌گیریم.

حالت اول: اگر M(i) برابر با ۱ باشد، سطح بیتی IB_i جابه جاشده و دو سطح کوانتیزاسیون عوض می‌شوند، به‌طوری‌که $\{b_i, a_i, \overline{B_i}\}$ به‌جای $\{a_i, b_i, B_i\}$ قرار داده، سپس $\{b_i, a_i, \overline{B_i}\}$ به Is اضافه می‌شود.

حالت دوم: اگر M(i) برابر با ۰ باشد، هیچ عملیاتی موردنیاز نیست و کدهای فشرده اصلی $\{a_i, b_i, IB_i\}$ را به Is اضافه کنید. درنهایت، M(i)ها را از M حذف کنید و برای رسیدگی به بلوک پردازش نشده بعدی به مرحله ۳ برگردید.

گام هفتم: اگر $di < thr$ باشد، بلوک B_i به‌عنوان یک بلوک صاف طبقه بندی می‌شود، که در آن ۹ بیت M(i) از M با استفاده از عملگر xor ، مطابق جدول (۱)، در سطح بیتی I_s مخفی‌سازی می‌شوند. روش مخفی‌سازی در اینجا برخلاف روش اصلی که با جایگزینی مستقیم بیت‌ها است، در اینجا با استفاده از فن مخفی‌سازی با عملگر xor انجام می‌شود، که در آن مکان‌های سطح بیتی IB_i با M(i) جایگزین می‌شوند. پس از جایگزینی ۹ بیت M(i) در ۴ سطر هر بلوک (۳ بیت پیام در ۴ سطح بیتی هر سطر)، مجدداً یک سطح بیتی جدید IB_i' و مقادیر کوانتیزه جدید a_i' و b_i' را طبق فرمول‌های ۱۲ و ۱۳، جهت حداقل کردن تخریب کیفیت تصویر محاسبه می‌کنیم.

گام هشتم: اگر $|a_i' - b_i'| \leq$ thr باشد، این بدان معناست که دو سطح کوانتیزاسیون دوباره محاسبه‌شده می‌توانند به‌عنوان ویژگی صاف بودن بلوک B_i باشند، لذا این مقادیر a_i' و b_i' می‌توانند به‌عنوان دو سطح کوانتیزاسیون جدید برای بلوک B_i استفاده شوند. سپس $\{a_i', b_i', IB_i'\}$ را به Is اضافه می‌کنیم.

اگر $|a_i' - b_i'|$ > thr باشد، دو سطح کوانتیزاسیون قدیمی a_i و b_i که ویژگی صاف و همواری بلوک Bi را نشان می‌دهند، بدون تغییر باقی می‌ماند و کدهای فشرده $\{a_i.b_i.IB_i'\}$ به Is اضافه می‌شوند. درنهایت، برای رسیدگی به بلوک‌های پردازش نشده به مرحله ۳ برمی‌گردیم.

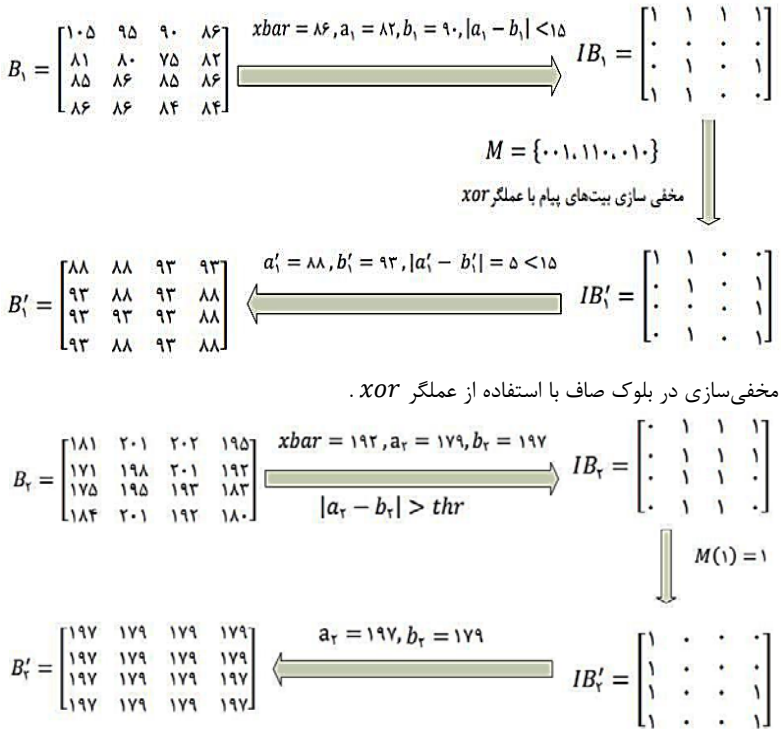
گام نهم: گام‌های۶ تا ۸ را تا زمانی که همه بلوک‌های تصویر به‌طور کامل پردازش شوند تکرار می‌کنیم، کدهای نهانه فشرده Is طبق تعریف AMBTC ساخته می‌شود.

به‌این‌ترتیب تصویر خروجی فشرده Is ، متشکل از $\frac{N\times N}{4\times 4}$ تا چهارتایی، که هرکدام شامل دو سطح کوانتیزاسیون با ۱۶ بیت و یک سطح بیتی IB_i با ۱۶ بیت هستند، ساخته می‌شوند. تصویر نهانه ساخته‌شده توسط این طرح در فرمت فشرده است، که می‌تواند کارآمدی انتقال و ذخیره‌سازی داده‌ها را بهبود بخشد. در ضمن، هرکسی می‌تواند تصویر AMBTC را از کدهای فشرده نهانه با استفاده از فرآیند کدگشایی به دست آورد. در طی این فرآیند، دو سطح کوانتیزاسیون برای بلوک صاف برای به حداقل رساندن تخریب کیفیت تصویر، مجدداً محاسبه می‌شود. بنابراین، کیفیت بصری تصویر نهانه توسط طرح پیشنهادی بهبود می‌یابد.

علاوه بر این، با تنظیم آستانه، thr، بار مفید و میزان کیفیت بصری تصویر نهانه را کنترل کرد. واضح است که با افزایش آستانه، ظرفیت نهان‌نگاری افزایش می‌یابد، ولی به دلیل افزایش تخریب کیفیت تصویر نهانه، امنیت طرح نهان‌نگاری کاهش می‌یابد.

برای توضیح روند ساخت تصویر نهانه‌ی مربوط به طرح نهان‌نگاری پیشنهادی به مثال زیر توجه کنید. بدون از دست دادن کلیت مسئله فرض کنید آستانه thr=۱۵ محاسبه‌شده باشد. همان‌طوری که در شکل(۳) نشان داده شد، یک‌رشته بیت $M = \{۱۰۰,۱۱۰,۰۱۰,۱۰۰\}$ به‌عنوان داده رمز شده در نظر می‌گیریم که thr آن ۱۵ است. ابتدا بلوک‌های اصلی $B_۱$ و $B_۲$ با استفاده از روش AMBTC فشرده‌شده و کدهای فشرده $\{۸۸/۹۳.IB_1\}$ به دست می‌آیند. برای بلوک B۱، ازآنجاکه $|a_۱ - b_۱| = < thr$ است، بلوک B_1 به‌عنوان یک بلوک صاف طبقه‌بندی می‌شود. بنابراین، ۹ بیت از M را می‌توان درسطرهای بلوک IB_1 مخفی‌سازی کرد. به‌طوری‌که هر سه بیت پیام در چهار بیت از هر سطر، طبق جدول مقایسه‌ای شماره ۱، با استفاده از عملگر xor مخفی‌سازی شده، ابتدا $IB_۱'$، سپس $a_۱' = ۸۸$ و $b_۱' = ۹۳$ با استفاده از معادلات (۱۲) و (۱۳) و درنتیجه $B_۱'$ محاسبه می‌شود.

اما ازآنجایی‌که قدر مطلق تفاضل این دو مقدار کمتر از مقدار آستانه thr است، این بدان معنی است که، ویژگی صاف بودن بلوک $B_۱$ حفظ شده است. بنابراین، دو مقدار محاسبه‌شده $a_۱'$ و $b_۱'$ را می‌توان به‌جای $a_۱$ و $b_۱$ به‌عنوان دو سطح کوانتیزاسیون برای بلوک B۱ مورد استفاده قرارداد. این یعنی $\{a_۱'.b_۱'.IB_۱'\}$ جایگزین $\{a_۱.b_۱.IB_۱\}$ می‌شود.



شکل۳. مخفی‌سازی در بلوک صاف با استفاده از عملگر xor .

شکل۴. مخفی‌سازی در بلوک ناصاف با شرط $M(۱) = ۱$.

از طرفی، با توجه به شکل (۴)، برای بلوک B_2، ازآنجایی‌که $|a_۲ - b_۲| = |۱۹۷ - ۱۹۷| = ۱۸ > thr$ است، بلوک $B_۲$ به‌عنوان یک بلوک ناصاف یا پیچیده طبقه‌بندی می‌شود. که مطابق الگوریتم فوق، با توجه به این‌که $M(۱) = ۱$، $\{b_۲, a_۲, \overline{IB_۲}\}$ جایگزین $\{a_۲, b_۲, IB_۲\}$ می‌شود .

روند استخراج داده‌ها در مقایسه با فرآیند ساخت تصویر نهانه نسبتاً ساده است. جزئیات مربوط به روند استخراج داده‌ها در الگوریتم زیر نشان داده‌شده است.

۴-۲- الگوریتم۲: الگوریتم استخراج

ورودی: کدهای فشرده AMBTC نهانه Is که متشکل از $\frac{N\times N}{۴\times ۴}$ چهارتایی $\{a_i . b_i . IB_i\}$، آستانه thr و طول پیام است.

خروجی: یک‌رشته بیت پیام M^E.

گام اول: فرض کنید $M^E = \emptyset$.

گام دوم: برای هر مجموعه سه‌تایی $\{a_i, b_i, IB_i\}$ در I_s، $d_i = |a_i - b_i|$ را محاسبه می‌کنیم.

گام سوم: اگر di > thr باشد، یک بیت $M(i)$ را می‌توان استخراج کرد. اگر $a_i < b_i$، $M(i)$ می‌تواند به عنوان '۱' استخراج شود؛ در غیر این صورت، $M(i)$ به‌عنوان '۰' استخراج می‌شود. سپس،بیت $M(i)$ استخراج شده را به M^E اضافه کنید و برای رسیدگی به مجموعه سه‌تایی پردازش نشده به مرحله۲ برگردید.

گام چهارم: اگر $d_i \le$ thr باشد، ۹ بیت $M(i)$ را می‌توان از سطح بیتی IB_i (سه بیت از هر سطر با استفاده از روابط (۱۴) استخراج کرد. سپس، $M(i)$ را به M^E اضافه کرده و برای به‌کار بردن مجموعه سه‌تایی پردازش نشده بعدی به گام دوم برمی‌گردیم.

گام پنجم: مراحل ۲ تا ۴ را تکرار کنید تا زمانی که همه مجموعه سه‌تایی به‌طور کامل پردازش شوند، و دنباله بیتی M^E که حاوی داده‌های کدگذاری شده است تولید شوند .

پس از استخراج تمام داده‌های رمزگذاری شده M^E توسط الگوریتم فوق، روند نهایی کدگشایی اطلاعات محرمانه اصلی با استفاده از یک کلید مربوطه انجام می‌شود.

برای مشاهده‌ی روند استخراج مثال مربوط به شکل(۳) را به خاطر بیاورید، برای بلوک نهانه ۱، مقدار اختلاف مطلق دو سطح کوانتیزاسیون a_1 و b_1 کوچک تر از مقدار آستانه است، ازاین‌رو، ۹ بیت از {۰۰۰۰، ۰۰۰۱، ۰۱۰۱، ۱۰۰۰} را می‌توان از سطح بیتی بلوک نهانه ۱، با به‌کارگیری معادلات (۱۴) استخراج کرد. برای بلوک نهانه ۲، مقدار اختلاف مطلق دو سطح کوانتیزاسیون a_2 و b_2، یعنی $|a_۲ - b_۲| = |۱۹۷ - ۱۹۷| = ۱۸ >$ thr است. ازاین‌رو، یک بیت را می‌توان از بلوک ۲ استخراج کرد. ازآنجاکه $a_۲ > b_۲$ است، سطح بیتی مخفی به‌عنوان '۱' استخراج می‌شود.

۵- معیارهای سنجش و ارزیابی

چندین آزمایش برای ارزیابی عملکرد هر طرح پیشنهادی در نهان‌نگاری وجود دارد. دسته‌ای از این آزمایش‌ها به سنجش کیفی و ظاهری تصاویر نهانه و تفاوت یا تشابه آن‌ها با پوشانه را مورد ارزیابی قرار می‌دهند.

در سنجش آزمایش‌ها، حداکثر نسبت سیگنال به نویز (PSNR[1]) برای ارزیابی کیفیت تصویر نهانه به‌کار می‌رود. PSNR بیشتر، نشان‌دهنده کیفیت و ظاهر طبیعی‌تر تصویر نهانه C نسبت به پوشانه S است. که به‌صورت زیر تعریف می‌شود:

$$\mathrm{PSNR} = 10log_{10}\frac{255^2}{MSE} \qquad (۱۶)$$

PSNR اختلاف بین تصاویر پوشانه و نهانه را محاسبه می‌کند. هر چه این مقدار بزرگ‌تر باشد یعنی تصویر نهایی به تصویر اصلی نزدیک‌تر بوده و فشرده‌سازی(در اینجا نهان‌نگاری) کیفیت بهتری ارائه می‌دهد و هر چه به صفر نزدیک‌تر باشد نشان‌دهنده این است که تصویر نهایی اطلاعات بیشتری را از دست داده است و شباهت کمتری با تصویر اصلی دارد.

میانگین مربعات خطا(MSE [2]) نیز نشان‌دهنده تفاوت بین تصویر پوشانه C و تصویر نهانه S است، که به‌صورت زیر تعریف می‌شود:

$$MSE = \frac{1}{W \times H}\sum_{i=1}^{N}\sum_{j=1}^{N}(C_{i.j} - S_{ij})^2 \qquad (۱۷)$$

در این تعریف W وH نشان‌دهنده ابعاد تصویر I است. همان‌طوری که از فرمول‌های(۱۶) و (۱۷) ملاحظه می‌شود، با افزایش MSE تفاوت دو تصویر بیشتر شده و درنتیجه از کیفیت تصویر نهانه (PSNR) کاسته می‌شود.

علاوه بر برآورد معیارهای کیفی PSNR و MSE معیار دیگری نیز وجود دارد، که به اندازه‌گیری شاخص ساختاری و تشابه (SSIM) معروف است و برای اندازه‌گیری شباهت بین تصاویر پوشانه و نهانه استفاده می‌شود. مقدار SSIM در فاصله [۰ ,۱] است. مقدار ۰ به معنای این است که دو تصویر کاملاً متفاوت و ۱ به معنای دقیق و یکسان بودن دو تصویر است.

معیار دیگری که در ارزیابی طرح‌های نهان‌نگاری بکار می‌رود، ارزیابی آماری طرح است. به‌این‌ترتیب که هیستوگرام پوشانه و نهانه را در کنار هم قرار داده و مقایسه می‌کنند. تشابه بیشتر هیستوگرام‌ها دلیل بر موفقیت در طراحی الگوریتم نهان‌نگاری است، که احتمال سوءظن رقبا مبنی بر وجود پیام مخفی در نهانه را کاهش می‌دهد.

[1] Peak Signal to Noise Ratio
[2] Main Squar Error

۶- پیاده‌سازی و نتایج تجربی

در این بخش نتایج تجربی الگوریتم پیشنهادی ارائه می‌شوند. با مقایسه نتیجه‌ی پیاده‌سازی طرح پیشنهادی با روش‌های دیگر، کارایی و برتری این طرح نشان داده می‌شود. ابزار آزمایش نرم‌افزار متلب ۲۰۱۹ است و تصاویر مورداستفاده از پایگاه داده BOWS می‌باشد. اندازه تمام تصاویر۵۱۲×۵۱۲ است. برای درک بهتر از چگونگی تأثیر تصاویر مختلف بر روی کارایی طرح نهان‌نگاری پیشنهادی، تعدادی از نتایج در قالب نمودار در این پژوهش نشان داده می‌شود. لذا، در ادامه نتایج حاصل از آزمایش‌ها در قالب جداول و اشکال نشان داده می‌شوند.

همان‌طور که در بخش۳ گفته شد، شاخص thr نشان‌دهنده آستانه است که برای تعیین این‌که آیا بلوک صاف و هموار است یا نه استفاده می‌شود. درواقع شاخص thr بار مفید و کیفیت تصویر را تحت تأثیر قرار می‌دهد.

در ادامه این بخش به ارزیابی الگوریتم پیشنهادی، که الگوریتم AMBTC اصلاح‌شده نامیدیم، نسبت به الگوریتم اصلی که کار دانهو و ویسان است، از جنبه‌های مختلف می‌پردازیم.

۶-۱- ارزیابی میزان تخریب طرح پیشنهادی

همان‌طوری که در بخش قبل دیدیم، PSNR، MSE و SSIM برای اندازه‌گیری کیفیت بصری تصاویر نهانه در آزمایش‌های نهان‌نگاری استفاده می‌شوند. به‌طورکلی امنیت در نهان‌نگاری شامل دو جنبه است، که یکی غیرقابل مشاهده بودن و دیگری غیرقابل‌کشف بودن است. برای بررسی غیرقابل مشاهده بودن، معیارهایی چون PSNR، MSE و SSIM که به تفاوت یا تشابه پوشانه و نهانه دلالت دارند، معیارهای خوبی هستند. در جدول (۲) سه معیار فوق برای پوشانه و نهانه به‌دست‌آمده با اجرای الگوریتم پیشنهادی در این مقاله و الگوریتم پیشنهادی توسط دانهو و ویسان محاسبه و ثبت شده است. البته این کار روی ۵ تصویر ۵۱۲ × ۵۱۲ با آستانه‌ی ۲۰ و طول پیام‌های ۳۰۰۰۰ و ۵۰۰۰۰ بیت، پیاده‌سازی گردید. سپس معیارهای ارزیابی PSNR، MSE و SSIM ، محاسبه شده است. همان‌طوری که انتظار می‌رفت، با توجه به کاهش تخریب سطوح بیتی در حین جاسازی بیت‌های پیام، در همه موارد و برای ۵ تصویر معروف آورده شده در جدول (۲)، MSE یا میانگین مربعات خطا کاهش‌یافته و با توجه به رابطه MSE و PSNR، طبق رابطه (۱۶)، مقدار PSNR دارای افزایش و SSIM یا تشابه نهانه و پوشانه در هر مورد افزایش را نشان می‌دهد، که نشان از بهبود طرح اصلاح شده پیشنهادی را دارد.

برای اطمینان از نتیجه فوق، میانگین مقادیر همان سه شاخص با آستانه تصمیم‌گیری و طول بیت‌های پیام متفاوت روی ۱۰۰۰ تصویر طبیعی به‌عنوان پوشانه برای روش‌های دانهو و ویسان و روش پیشنهادی شبیه‌سازی گردیده و در جدول (۳) ثبت‌شده است. نتیجه این مرحله از آزمایش نیز مشابه نتیجه‌ی جدول (۲)، به کیفیت بصری تصاویر نهانه و تشابه بیشتر نهانه با پوشانه در مقایسه با روش دانهو و ویسان دلالت دارد.

جدول۲. ارزیابی الگوریتم مخفی‌سازی پیشنهادی با محاسبه PSNR، MSE و SSIM با آستانه ۲۰

شماره تصویر	تصویر	معیار	n= ۳۰۰۰۰ bit		n= ۵۰۰۰۰ bit	
			دانهو و ویسان	پیشنهادی	دانهو و ویسان	پیشنهادی
۱		PSNR	۴۴/۷۱۰	۴۵/۱۷۲	۳۸/۵۹۹۷	۳۸/۹۱۲۳
		MSE	/۸۶۳۸	۰/۷۴۵۷	۲/۹۹۳۰	۲/۶۲۴۱
		SSIM	۰/۹۹۵۲	۰/۹۹۶۹	۰/۹۸۵۶	۰/۹۹۰۱
۲		PSNR	۵۱/۸۱۷۳	۵۵/۲۸۵۷	۴۹/۱۶۲۳	۵۱/۴۶۱۸
		MSE	۰/۲۶۹۴	۰/۰۷۵۷	۰/۴۲۲۵	۰/۱۵۷۹
		SSIM	۰/۹۹۵۱	۰/۹۹۷۷	۰/۹۹۲۴	۰/۹۹۶۱
۳		PSNR	۳۸/۰۵۱۵	۳۹/۳۱۱۸	۳۴/۰۰۳۹	۳۵/۱۱۱۶
		MSE	۳/۹۹۲۷	۳/۱۲۴۵	۹/۳۴۰۱	۷/۲۶۲۹
		SSIM	۰/۹۷۸۳	۰/۹۸۵۰	۰/۹۵۴۸	۰/۹۶۹۲
۴		PSNR	۳۵/۶۹۲۴	۳۶/۲۸۲۶	۳۴/۰۴۲۹	۳۵/۱۱۱۹
		MSE	۴/۷۸۱۴	۳/۸۶۸۲	۷/۹۴۵۴	۵/۷۳۰۹
		SSIM	۰/۹۷۷۲	۰/۹۸۴۶	۰/۹۵۵۹	۰/۹۷۲۸
۵		PSNR	۴۵/۰۹۱۹	۵۹/۸۲۷۲	۴۲/۸۶۷۶	۵۰/۴۰۴۹
		MSE	۱/۵۳۹۲	۰/۰۲۳۹	۲/۵۰۴۴	۰/۲۷۳۴
		SSIM	۰/۹۸۳۳	۰/۹۹۹۰	۰/۹۷۱۷	۰/۹۹۵۹

جدول۳. میانگین نتیجه پیاده‌سازی طرح‌های دانهو و پیشنهادی روی ۱۰۰۰ تصویر از پایگاه BOWS

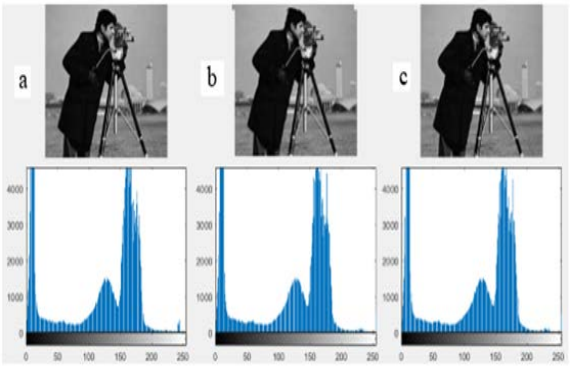
thr	میانگین معیارها	بار ۴۰۰۰۰ بیت		بار ۸۰۰۰۰ بیت	
		دانهو و ویسان	طرح پیشنهادی	دانهو و ویسان	طرح پیشنهادی
۱۰	PSNR	۴۰/۲۳۲۱	۴۱/۰۵۰۵	۳۴/۶۱۸۱	۳۵/۰۲۸۳
	MSE	۷/۲۴۸۳	۶/۷۶۵۴	۱۱/۸۸۹۸	۱۰/۸۶۹۸
	SSIM	۰/۹۶۳۷	۰/۹۶۸۹	۰/۹۳۵۵	۰/۹۴۶۷
۲۰	PSNR	۴۰/۹۶۳۰	۴۲/۲۳۴۳	۳۴/۸۲۲۹	۳۵/۷۸۶۵
	MSE	۵/۵۳۴۳	۴/۳۲۶۸	۱۲/۶۹۱۵	۹/۷۷۰۵
	SSIM	۰/۹۶۸۷	۰/۹۷۷۵	۰/۹۲۶۹	۰/۹۴۷۸
۳۰	PSNR	۴۰/۸۴۵۲	۴۲/۵۰۲۷	۳۴/۵۶۳۰	۳۶/۰۱۵۳
	MSE	۴/۵۶۸۲	۳/۴۷۹۹	۱۱/۵۱۶۹	۸/۸۹۶۹
	SSIM	۰/۹۶۸۹	۰/۹۷۹۴	۰/۹۲۳۶	۰/۹۴۸۵

۶-۲- ارزیابی امنیت آماری

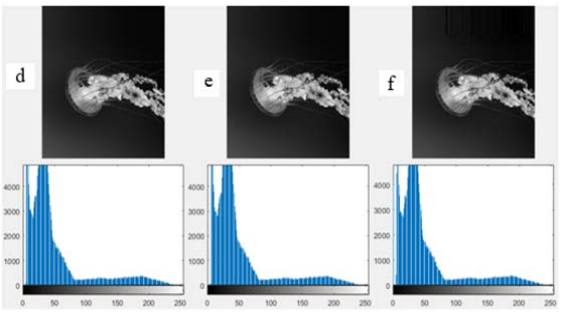
برای ارزیابی امنیت پیام جاسازی‌شده توسط الگوریتم‌های نهان‌نگاری از حملات مختلفی استفاده می‌شود. یکی از این حملات، حمله بصری (بینایی) است که در آن سعی می‌شود وجود پیام محرمانه در یک تصویر از طریق دقت در تصویر یا هیستوگرام آن، با چشم غیرمسلح یا رایانه، حدس زده شود. سپس با به‌کارگیری روش‌های خلاقانه یا روش‌های نهان‌کاوی دیگر وجود پیام در تصویر به اثبات برسد.

در شکل (۵) دو تصویر اصلی پوشانه a و d و حالت فشرده‌شده آن‌ها یعنی b و e و همین‌طور نهانه به‌دست‌آمده در تصویر فشرده را به همراه هیستوگرام تک‌تک آن‌ها با مخفی‌سازی ۳۰۰۰۰ بیت پیام طبق الگوریتم دانهو و ویسان و الگوریتم پیشنهادی نشان می‌دهد. همان‌طوری که در این تصاویر و هیستوگرام آن‌ها دیده می‌شود، تفاوتی بصری بین این تصاویر پوشانه و نهانه و همین‌طور در هیستوگرام‌های آن‌ها قابل‌تشخیص نیست.

همان‌طور که در الگوریتم ارائه‌شده ملاحظه گردید، در AMBTC اصلاح‌شده، در هر بلوک صاف، بیت‌های پیام را در کلیه بیت‌های سطوح بیتی (IB_i) مخفی‌سازی می‌شود. درواقع یک بلوک صاف بلوکی است که دو سطح کوانتیزاسیون مربوطه شباهت بیشتری داشته باشند. درنتیجه می‌توان گفت سطوح صاف‌تر نسبت به بقیه سطوح صاف، پس از مخفی‌سازی پیام، کمتر جلب‌توجه می‌کند. لذا، چنین سطوح بیتی را می‌توان با بیت‌های پیام جایگزین کرد. درهرصورت، راهبرد طراحی‌شده توسط دانهو و ویسان برای هر بلوک صاف، تخریب کیفیت تصویر را به همراه دارد. لذا، در این طرح با استفاده از عملگر xor، که سطح تخریب برای هر بیت را از $\frac{1}{2}$ به $\frac{1}{4}$ کاهش می‌دهد، انتظار داریم کیفیت بصری تصویر نهانه بهبود داشته باشد.



شکل ۵. a و d تصاویر اصلی، b و e تصاویر اصلی فشرده، c وe تصاویر نهانه فشرده و هیستوگرام‌های آن‌ها با نرخ جاسازی ۳۰۰۰۰ بیت پیام



ادامه شکل ۵. a و d تصاویر اصلی، b و e تصاویر اصلی فشرده، c وe تصاویر نهانه فشرده و هیستوگرام‌های آن‌ها با نرخ جاسازی ۳۰۰۰۰ بیت پیام

۷- نتیجه‌گیری

نهان‌نگاری، فنی است که امنیت اطلاعات را از طریق رسانه‌های دیجیتالی مانند تصاویر فراهم می‌سازد. این مقاله، که بر اساس روش‌های ریاضی قوی استوار است، با تجزیه‌وتحلیل الگوریتم نهان‌نگاری AMBTC بهبودیافته، روش مخفی‌سازی پیام را بهبود داده است. در این مقاله بجای مخفی‌سازی مستقیم پیام درون کدهای فشرده AMBTC، که در روش‌های دیگر صورت می‌گیرد، از عملگر xor و شرایط تطبیقی و مقایسه‌ای استفاده می‌شود، که می‌تواند باعث کار آیی بهتر انتقال داده‌ها و کاهش سوءظن مهاجمان در ارتباطات تصویری شود. چراکه فن بکار گرفته‌شده برای مخفی‌سازی پیام، احتمال تخریب تصویر را از ۰/۵ به ۰/۲۵ کاهش می‌دهد. در این طرح تمام بلوک‌های صاف و ناصاف، برای مخفی‌سازی پیام استفاده می‌شوند. هر بلوک صاف نه بیت و هر بلوک ناصاف یک بیت را در خود مخفی می‌کند. طرح اصلاح‌شده پیشنهادی مزایای طرح AMBTC بهبودیافته مانند پیچیدگی محاسباتی پایین و سهولت در اجرا را به ارث می‌برد و با ظرفیت مخفی‌سازی یکسان، کیفیت بصری خوبی را به‌دست می‌آورد. نتایج تجربی روی طرح پیشنهادی، با برآورد معیارهای ارزیابی چون PSNR، MSE و SSIM برای تصاویر نهانه با حجم بار مفید یکسان، نسبت به برخی از طرح‌هایی که قبلاً گزارش‌شده است، از کیفیت بصری بهتری برخوردار است. از طرفی آزمون هیستوگرام هم نشان داده است که، این طرح مخفی‌سازی پیام، امنیت آماری را هم حفظ می‌کند.

۸- مرجع‌ها

[1] Bohem, R. “Advanced Statistical Steganalysis”; Springer-Verlag Berlin Heidelberg, 2010.

[2] Shamalizadeh Baei, M. A. “Designing a Combinatorial Image Steganography Algorithm Based on Game Theory”; Adv. Defence Sci. & Technol. 2020, 2, 133-145, (In Persian).

[3] Guo, J. M.; Lin, C. Y. “Parallel and Element-reduced Error-Diffused Block Truncation Coding”; IEEE Trans. Commun. 2010, 58, 1667–1673.

[4] Lema, M.; Mitchell, O. “Absolute Moment Block Truncation Coding and Its Application to Color Images”; IEEE Trans. Commun. 1984, 32,1148–1157.

[5] Hong, W.; Chen, T. S.; Shiu, C. W. “Lossless Steganography for AMBTC-Compressed Images”; Int. Cong. Image Signal Processing 2008, 2, 13–17.

[6] Chang, C. C.; Lin, C. Y.; Fan, Y. H. “Lossless Data Hiding for Color Images Based on Block Truncation Coding”; Pattern Recog. 2008, 41, 2347–2357.

[7] Liao, X.; Yu, Y.; Li, B.; Li, Z.; Qin, Z. “A New Payload Partition Strategy in Color Image Steganography”; IEEE Trans. Circuits Syst. Video Technol., in press, 2019.

[8] Chen, J.; Hong W.; Chen, T. S.; Shiu, C. W. “Steganography for BTC Compressed Images Using no Distortion Technique”; Imaging Sci. J. 2010, 58, 177–185.

[9] Sun, W.; Lu ZM.; Wen Y. C.; Yu F. X.; Shen RJ. “High Performance Reversible Data Hiding for Block Truncation Coding Compressed Images”; Signal, Image Video Process 2013, 7, 297–306.

[10] Chin-Chen, C.; Tung-Shou, C.; Yu-Kai, W.; Yan-Jun, L. “A Reversible Data Hiding Scheme Based on AMBTC compression using xor Operator”; Multimed. Tools Appl. 2017, 2019, 3, 113–124..

[11] Jung-Yao, Y.; Chih-Cheng, C.; Po-Liang, L.; Ying-Hsuan, H. “High-Payload Data-Hiding Method for AMBTC Decompressed Images”; MDPI, 2020, 1, 212–219.

[12] Ou, D.; Sun, W. “High Payload Image Steganography with Minimum Distortion Based on Absolute Moment Block Truncation Coding”; Multimed Tools Appl. 2014, 74, 9117–9139