Archive of SID

پنهان نگاری وفقی براساس پیچیدگی نسبی پیکسلها در تصاویر دوسطحی

مجتبی مهدوی[1] شادرخ سماوی[2] الهه خدامی[3]

1- کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر ، دانشگاه صنعتی اصفهان
Mahdavi110@gmail.com

2- استاد، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران
Samavi96@cc.iut.ac.ir

3- کارشناسی ارشد، مهندسی کامپیوتر دانشگاه آزاد اسلامی، نجف آباد، ایران
ekhoddami@gmail.com

چکیده: امروزه پنهان نگاری توجه محققین زیادی را به خود جلب کرده است. پنهان نگاری در رسانه‌های مختلفی مانند تصویر, صدا, تصاویر متحرک صورت می‌گیرد. تصویر به عنوان یکی از پراستفاده‌ترین رسانه‌ها مطرح است. یکی از روش‌های نمایش تصویر استفاده از تصاویر دوسطحی است. در این مقاله روشی ارائه شده است که داده‌ها را در تصاویر دوسطحی مخفی می‌نماید. عمل جاسازی داده‌ها در فرآیند تبدیل تصویر طیف خاکستری به تصویر دوسطحی صورت می‌گیرد که باعث بهبود امنیت یا ظرفیت می گردد. جاسازی در نواحی یکنواخت تصاویر دوسطحی شده, می‌تواند بیانگر حضور داده های مخفی باشد. در این مقاله روشی ارائه گردیده است که با بررسی وضعیت هر پیکسل نسبت به پیکسلهای همسایه از جاسازی داده در نواحی یکنواخت اجتناب می شود. اجرای روش پیشنهادی باعث بهبود کیفیت تصویر گنجانه و افزایش امنیت آن گردیده است.

کلمات کلیدی: پنهان نگاری, تصاویر دوسطحی, فلوید استاینبرگ, پنهان شکنی

تاریخ ارسال مقاله: 86/6/23

تاریخ پذیرش مقاله: 88/5/31

نام نویسنده‌ی مسئول: مجتبی مهدوی

نشانی نویسنده‌ی مسئول: دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

www.SID.ir

Archive of SID

1 - مقدمه

پنهان‌نگاری[1] خود شاخه‌ای از علم مخفی‌سازی[2] اطلاعات می‌باشد. مخفی‌سازی اطلاعات خود شامل چندین شاخه از جمله رمزنگاری[3] و ته‌نقش‌نگاری[4] می‌باشد[1].

مفهوم پنهان‌نگاری ممکن است گاهی با رمزنگاری و یا ته‌نقش‌نگاری اشتباه شود. تفاوت رمزنگاری با پنهان‌نگاری در این است که در رمزنگاری وجود ارتباط برای حمله کننده[5] مخفی نیست و تنها محتوای پیام است که از دید حمله کننده مخفی می‌ماند[2]. به بیان دیگر در رمزنگاری خود پیام مهم است. در پنهان نگاری خود ارتباط است که باید پنهان شود. به همین دلیل است که در رمزشکنی[6] زمانی حمله را موفق می‌دانیم که بتوان به تمام یا بخشی از محتوای پیام پی برد ولی در پنهان‌شکنی[7] زمانی حمله کننده موفق به اجرای حمله می‌شود که بتواند به وجود ارتباط (یا پیام مخفی) پی برده و یا به صورتی احتمالی آنرا آشکار نماید[3]. در ته‌نقش‌نگاری، هدف عموما حفاظت از یک رسانه در مقابل انتشار غیر مجاز است این کار عمدتاً به صورت درج یک ته‌نقش[8] معمولاً کوتاه در رسانه صورت می‌گیرد و بنابراین دشمن زمانی موفق به اجرای حمله می‌گردد که بتواند ته‌نقش را از رسانه حذف کند به طریقی که رسانه آسیب جدی نبیند.

رسانه ای که پیام مخفی در آن جاسازی می‌شود را پوشانه[9] می‌گوییم. این رسانه می‌تواند تصویر، صدا، فیلم و حتی صفحه های HTML باشد. به پوشانه پس از جاسازی پیام توسط الگوریتم جاسازی رسانه گنجانه[10]می‌گوییم. به داده‌ای که قرار است در پوشانه جاسازی شود پیام سری گفته می‌شود. به کلیدی که در هنگام جاسازی و استخراج پیام مخفی استفاده می‌گردد، کلید جاسازی می‌گوییم. به تکنیکهایی که به ما در تمایز بین پوشانه و گنجانه کمک میکند پنهان شکنی گوییم[4]. این تمایز باید بدون دانستن کلید جاسازی و حتی در برخی موارد بدون دانستن الگوریتم جاسازی انجام شود. در پنهان-شکنی هدف فقط فهمیدن وجود پیام مخفی است و الزاما کشف محتویات پیام مد نظر نیست.

در این مقاله روشی برای پنهان‌نگاری در تصاویر دوسطحی[11] ارائه شده است. تصاویر دوسطحی به طور گسترده در چاپ کتاب، مجله، روزنامه و چاپگرهای کامپیوتری استفاده می‌شود. تصاویر ارسالی بوسیله فکس، برخی مدارک که به فرمت pdf ذخیره شده‌اند و یا تصاویری که از اسکن متون چاپی به وجود آمده اند از جمله تصاویر دوسطحی هستند. تبدیل تصویر خاکستری به تصویر دوسطحی که مقادیر پیکسلهایش صفر یا 255 (سیاه یا سفید) است فرآیند دوسطحی سازی[12] می‌نامند. برای جاسازی پیام در این دسته از تصاویر روشهایی ابداع شده است که ذیلاً به شرح برخی از آنها می‌پردازیم.

در [5] روشی ارائه شده است که در آن پیکسلهایی برای جاسازی انتخاب می‌گردند که تغییر در آنها قابل تشخیص نباشد. این نقاط بر روی مرز نواحی سیاه و سفید قرار دارند. از آنجا که تصاویر دوسطحی پیچیدگی کمی دارند، جاسازی با در نظر گرفتن محتوا و شکل پوشانه، امنیت را بالا خواهد برد. روش ارائه شده در [5] دارای امنیت دیداری خوبی است ولی ظرفیت آن کم است. منظور از امنیت دیداری آن است که سیستم بینایی انسان قادر به تشخیص وجود داده‌های سری در تصویر نیست.

در مرجع [6] روشی ارائه شده که جاسازی در آن بر اساس زوج یا فرد کردن تعداد یکهای هر بلوک از تصویر دوسطحی است. در این روش کلید به صورت بلوکی $n \times m$ از صفر و یکهاست. زوج یا فرد کردن تعداد یکهای هر بلوک تصویر بر اساس بلوک کلید صورت می-گیرد. از آنجا که از هر بلوک $n \times m$ حداکثر امکان تغییر یک بیت وجود دارد این روش از لحاظ دیداری از امنیت خوبی برخوردار است ولی در همه تصاویر نمی‌توان آنرا به کار برد. اگر در تصاویر کاملاً و یا تقریباً سفید یا سیاه از این روش استفاده شود، امکان لو رفتن کلید برای دشمن وجود دارد. در مرجع [7] روشی ارائه شده که در آن تصویر به بلوکهای هم اندازه $n \times m$ تقسیم شده و از یک کلید $n \times m$ و یک ماتریس وزن دهی $n \times m$ برای جاسازی استفاده می‌شود. در هر بلوک از تصویر r بیت, که کوچکتر یا مساوی $\log_2(m \times n - 1)$ می‌باشد, را می‌توان جاسازی کرد. در نتیجه این روش دارای ظرفیت خوبی است و از طرف دیگر به دلیل استفاده از ماتریس وزن دهی از خطر حدس کلید توسط دشمن مصون است. در همه این روشها ابتدا عمل دوسطحی سازی انجام شده و سپس در تصویر دوسطحی، جاسازی صورت می‌گیرد. در این مقاله ما به ارائه روشی خواهیم پرداخت که عمل جاسازی همراه با دوسطحی‌سازی انجام خواهد شد. در نتیجه تصویر حاصل‌شده نسبت به زمانی که جاسازی بعد از دوسطحی‌سازی صورت می‌گیرد، کیفیت بهتری خواهد داشت.

برای پنهان شکنی روشهایی مانند [5] و [6] که جاسازی را بعد از دوسطحی سازی و در نواحی مرزهای سیاه و سفید انجام می‌دهند روشی در [8] ارائه گردیده است. در روش ارائه شده در [8] داده جاسازی شده به صورت یک اغتشاش در نظر گرفته شده و از فشرده سازی JBIG 2 به عنوان معیاری برای اندازه گیری اغتشاش استفاده شده است. روش ارائه شده در [8] می‌تواند علیه روشهای پنهان نگاری موفق باشد که جاسازی را در مرزهای بلوکهای سیاه و سفید صورت می‌دهند.

در [9] نیز روشی برای شکستن پنهان نگاری‌هایی ارائه شده است که جاسازی را در مرز نواحی سیاه و سفید صورت می‌دهند. معیارهایی که در [9] برای پنهان شکنی ارائه شده است شامل پیچیدگی در مرز نواحی سیاه و سفید, میزان نویزی بودن بلوک و ریزدانگی این بلوک ها است.

www.SID.ir

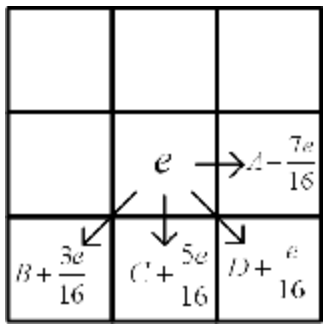
Archive of SID

در [10] روشی برای ته نقش نگاری تصاویر دوسطحی ارائه شده است که می‌تواند با حفظ کیفیت دیداری تصویر خروجی, نشانه ای[13] را جاسازی نماید. در این روش با استفاده از مولد اعداد شبه تصادفی[14] تعدادی از نقاط تصویر انتخاب شده و جاسازی در آنها صورت می‌گیرد. این روش نیز جاسازی را در تصویر دوسطحی شده صورت می‌دهد. این روش نیز توسط [11] شکسته شده است. در [11] ابتدا فیلتر پایین گذری بر روی تصویر مشکوک اعمال می‌گردد و تخمینی از تصویر اولیه را به دست می‌دهد. تصویر حاصل از فیلتر پایین گذر, با استفاده از فیلتر QMF[15] تجزیه شده و تعدادی خصیصه[16] از آن استخراج می-گردد و با استفاده از دسته بندی کننده خطی[17] تصاویر حاوی نشانه مشخص می‌گردد.

برای دوسطحی‌سازی الگوریتم های گوناگونی وجود دارد. یکی از مشهورترین آنها الگوریتم فلوید استاینبرگ[18] است [12] که در این مقاله از آن استفاده شده است.

در روش فلوید استاینبرگ سطح روشنایی هر پیکسل با مقدار آستانه 255/2 مقایسه می‌گردد و اگر بزرگتر از مقدار آستانه بود به 255 و اگر کوچکتر از مقدار آستانه بود به 0 تغییر می‌یابد و بنابراین هر پیکسل را می‌توان با یک بیت نمایش داد. این تغییر مقدار خطایی را در تصویر جدید تولید می‌کند. برای مثال اگر F مقدار اولیه پیکسل باشد و مقدار جدید آن 255باشد، مقدار خطا برابر $e = 255 - F$ خواهد بود. در روش فلوید استاینبرگ این مقدار خطا، در پیکسل‌های مجاور به صورت نشان داده‌شده در شکل 1، منتشر می‌گردد.

مقدار خطا با وزن‌های مختلف بین پیکسل‌های مجاوری منتشر می-گردد که سمت راست یا پایین پیکسل باشند. برای مثال اگر مقدار پیکسل سمت راست پیکسل مذکور A باشد مقدار جدید آن $A + \frac{7e}{16}$ خواهد بود.

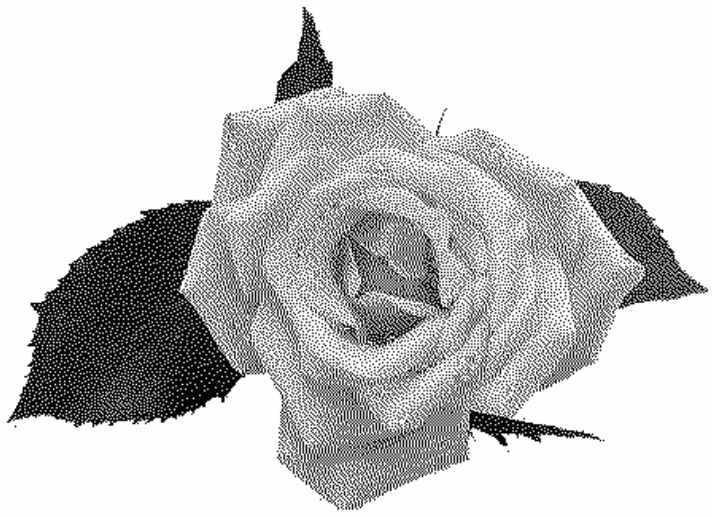


شکل (1): انتشار خطا در روش فلوید استاینبرگ

در روش فلوید استاینبرگ از گوشه سمت چپ و بالای تصویر شروع کرده و پیکسل‌ها را به صورت ردیفی پیمایش کرده و برای هر پیکسل عمل دوسطح سازی و انتشار خطا را صورت می‌دهیم.

شکل 2 تصویر یک گل و شکل 3 دوسطحی شده آن توسط الگوریتم فلوید استاینبرگ را نمایش می‌دهد. همانطور که مشاهده می‌شود این الگوریتم عمل دوسطحی سازی را با کیفیت خوبی انجام می‌دهد. توضیحات بیشتر در مورد این الگوریتم در مرجع [6] آورده شده است.

شکل(2): تصویر گل با نمایش سطح خاکستری



شکل (3): تصویر دوسطحی شدهٔ تصویر گل به روش *Floyd Steinberg*

به طور کلی روش‌های دوسطحی سازی چهار دسته‌اند[13]. در روش تصفیه کلاسیک[19] که قدیمی‌ترین روش دوسطحی سازی است آرایه-ای متناوب از مقادیر سطوح آستانه وجود دارد. مقدار سطح روشنایی هر کدام از پیکسل‌ها که از سطح آستانه در آرایه کمتر باشد به مقدار 0 و اگر بیشتر باشد به مقدار 255 تبدیل می‌گردد[14]. در روش دوسطحی سازی با نویز آبی[20] سعی می‌گردد نویز حاصل از دوسطحی سازی در فرکانس‌های بالاتر قرار گیرد[15]. کارایی این روش بدان جهت است که سیستم بینایی انسان نسبت به نویز فرکانس بالا در تصویر کمتر حساس است. در روش جستجوی مستقیم دودویی[21] سعی می‌شود مقداری برای هر پیکسل در تصویر دوسطحی انتخاب گردد که معیار کیفیت مشخصی را بهینه کند[16]. بهترین کیفیت در بین روش‌های دوسطحی سازی مربوط به روش‌هایی است که بر مبنای جستجوی دودوی عمل می‌کنند. در ادامه، روش پیشنهادی برای جاسازی داده در هنگام تولید تصویر دوسطحی با استفاده از روش فلوید استاینبرگ ارائه می‌گردد. در ادامه این مقاله، در بخش 2 روش پیشنهادی برای پنهان نگاری ودر بخش 3 بهبود آن ارائه شده است. پس از آن در بخش 4 نتایج حاصل از پیاده سازی ارائه گردیده است. در نهایت نتیجه گیری مقاله آورده شده است.

2- روش پیشنهادی *ComB-Steg*

www.SID.ir

Archive of SID

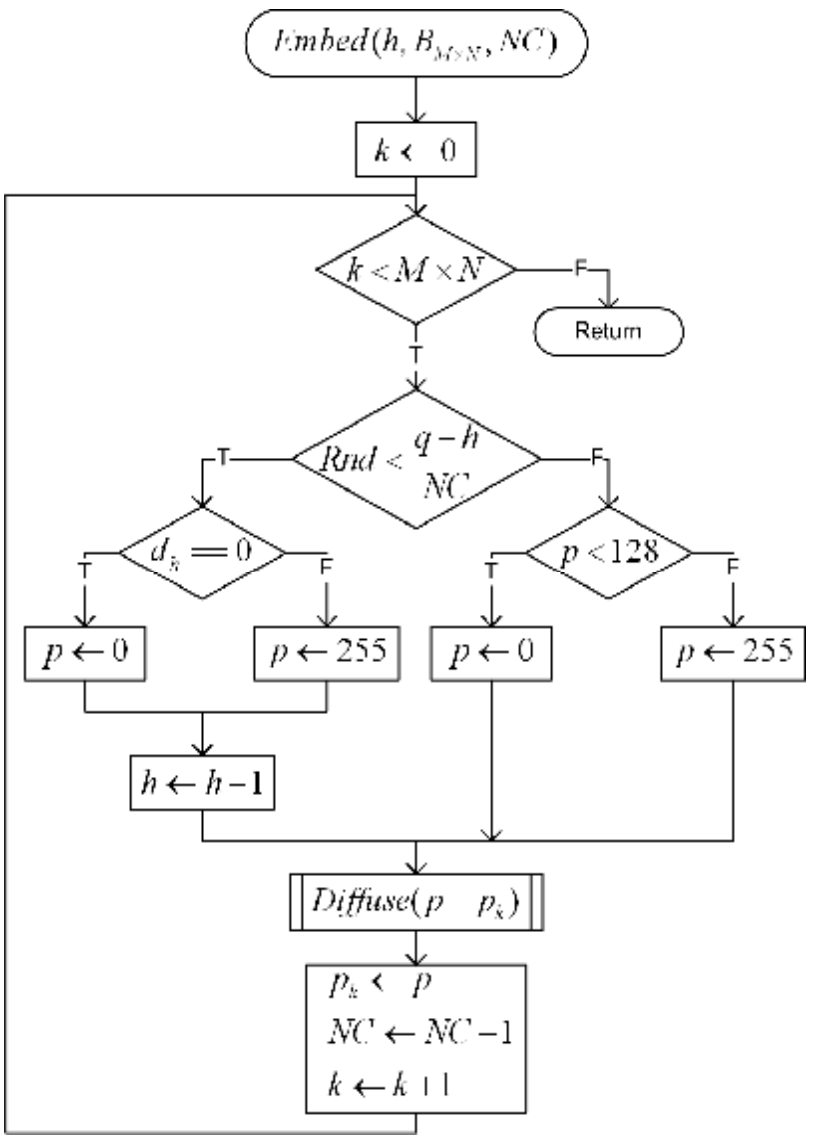
در روشهای ارائه شده در مراجع [4-7] عمل جاسازی بعد از ایجاد تصویر دوسطحی صورت می‌گیرد. جاسازی داده در تصاویر بعد از ایجاد تصاویر دوسطحی باعث به وجود آمدن مقداری نویز نمک فلفل[22] علی الخصوص در نواحی صافی می‌شود که رنگ خاکستری متوسطی[23] دارند[17]. در روشی که ما پیشنهاد می دهیم جاسازی اطلاعات در تصویر همزمان با عمل دوسطحی‌سازی صورت می‌گیرد به طوری که خطای ایجاد شده در اثر جاسازی اطلاعات همانند خطای دوسطحی-سازی در پیکسلهای مجاور انتشار می‌یابد. جاسازی در حین فرآیند دوسطحی سازی نسبت به جاسازی در تصویر دوسطحی شده باعث افزایش کیفیت بصری[24] تصویر نهایی می‌گردد [18] که باعث افزایش امنیت یا ظرفیت خواهد بود.

روش پیشنهادی بر اساس پیچیدگی بلوکهای تصویر عمل جاسازی را انجام می‌دهد. به همین دلیل به آن "پنهان‌نگاری در تصاویر دوسطحی بر اساس پیچیدگی"[25] یا به اختصار *ComB-Steg* می-گوییم.

در ادامه، ابتدا شیوه جاسازی داده‌ها در یک بلوک از تصویر، توضیح داده خواهد شد. سپس چگونگی در نظر گرفتن نواحی پیچیده در هنگام جاسازی را شرح خواهیم داد.

فرض می‌کنیم قرار است q بیت داده در تصویر جاسازی گردد. رشته بیت داده‌ها را به صورت مجموعه $d = \{d_0, \dots, d_{q-1}\}$ در نظر می‌گیریم.

روند نمای کامل جاسازی در حین دوسطحی سازی بدون در نظر گرفتن نواحی پیچیده در شکل 4 نشان داده شده است.



شکل (4): روندنمای کامل جاسازی و دوسطحی سازی همزمان

در شکل 4، فرآیند $Embed$ به عنوان تابعی از اندیس داده‌ای که قرار است جاسازی شود (h) و بلوکی از تصویر (B) به ابعاد $N \times M$ پیکسل و تعداد پیکسل‌هایی که می‌توانند برای جاسازی استفاده شوند (NC) بیان شده است. پیکسل‌های بلوک را یک به یک از سمت چپ و بالا به صورت ردیفی پیمایش می‌کنیم. برای هر پیکسل (p_k) عدد شبه تصادفی با توزیع یکنواخت (Rnd) بین صفر و یک تولید می‌شود و در صورتی که مقدار آن از $\frac{q-h}{NC}$ کمتر باشد یک بیت در آن جاسازی می‌گردد. بدین صورت که اگر بیت مورد نظر (d_h) برابر صفر باشد مقدار جدید پیکسل (p) ، صفر و در صورتی که بیت مورد نظر، یک باشد مقدار جدید پیکسل 255قرار داده می‌شود. سپس به اندیس داده‌هایی که قرار است جاسازی شوند یکی اضافه می‌گردد. در صورتی که با توجه به عدد شبه تصادفی تولید شده، پیکسل مورد نظر برای جاسازی انتخاب نشود، مقدار جدید پیکسل مطابق روش فلوید استاینبرگ 0 یا 255خواهد بود. پس از به دست آوردن مقدار جدید پیکسل، خطای تولید شده $(p - p_k)$ باید مطابق شکل 1 منتشر شود یعنی تابع $Diffuse(p - p_k)$ اجرا شود. سپس تعداد پیکسل‌هایی که ممکن است در آنجا جاسازی شود یکی کم می‌شود. مقایسه عدد شبه تصادفی تولید شده با مقدار $\frac{q-h}{NC}$ باعث می‌شود در پایان جاسازی دقیقا (q) بیت داده و به صورت تقریبا یکنواخت در سطح تصویر جاسازی شوند.

طبیعی است که تبدیل تصویر خاکستری به تصویر دوسطحی مقداری خطا ایجاد می‌کند. ما در این مقاله از SNR[26] به عنوان معیاری برای اندازه‌گیری میزان خطای ایجاد شده استفاده می‌کنیم. معیار SNR روش متداولی برای تعیین میزان خطا است که بیان کننده نسبت توان سیگنال به نویز می‌باشد. برای تصویری با اندازه $U \times V$ پیکسل، SNR به صورت زیر تعریف می شود:

$$SNR(dB) = 10 \lim_{10} \left(\frac{\sum_{i,j} x(i,j)^2}{\sum_{i,j} (x(i,j) - y(i,j))^2} \right) \quad (1)$$

$$\begin{cases} 0 \le i \le U-1 \\ 0 \le i \le V-1 \end{cases}$$

که در آن $x(i,j)$ مقدار پیکسل در سطر i و ستون j در تصویر اصلی می‌باشد و $y(i,j)$ مقدار پیکسل متناظر آن در تصویر تغییر یافته می‌باشد.

منبع تولید خطا، غیر از عمل جاسازی، خود فرآیند دوسطحی‌سازی نیز می‌باشد. حال برای اندازه‌گیری تاثیرات عمل جاسازی نیاز به داشتن یک مبنا وجود دارد. در این مقاله ما معیاری به نام $NSNR$[27] را

Journal of Iranian Association of Electrical and Electronics Engineers - Vol.6- No.1- Spring and Summer 2009

www.SID.ir

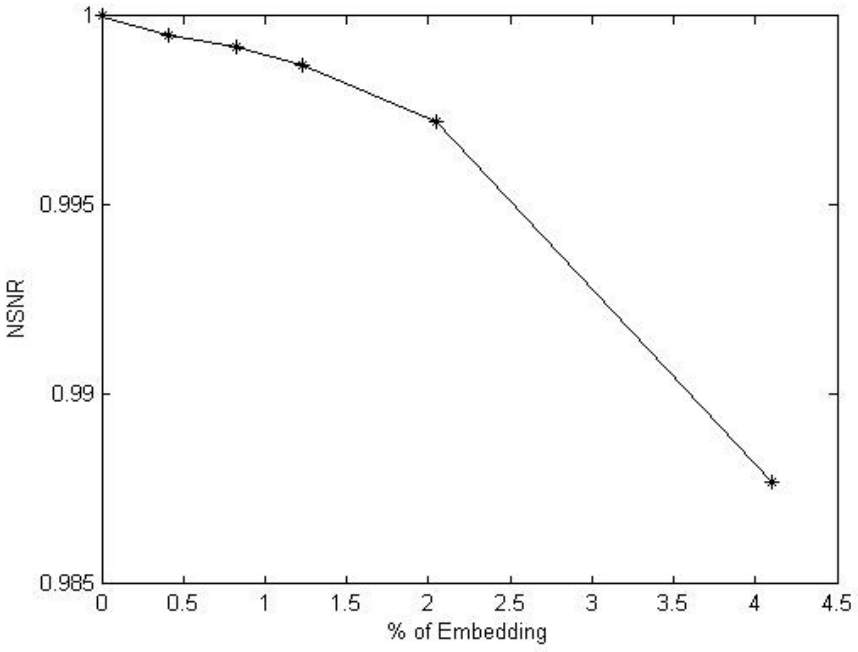
Archive of SID

برای بررسی تاثیرات جاسازی پیشنهاد می‌دهیم. $NSNR$ را به صورت زیر تعریف می‌کنیم.

$$NSNR = \frac{SNR_{stego}}{SNR_{Cover}} \quad (2)$$

در رابطه فوق SNR_{Cover} برابر با SNR به دست آمده از تصویر دوسطحی بدون جاسازی نسبت به تصویر خاکستری و SNR_{stego} برابر با SNR تصویر دوسطحی حاوی داده نسبت به تصویر خاکستری است.

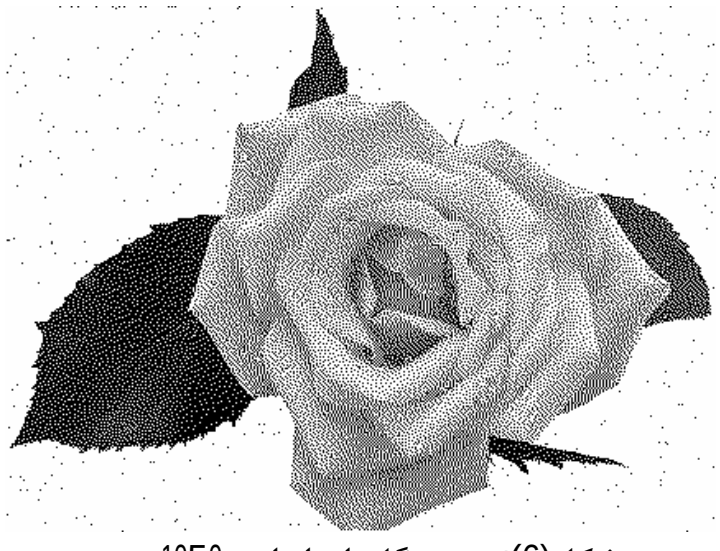
هر چه میزان جاسازی بالا رود، فاکتور $NSNR$ کاهش می‌یابد. شکل5 نمودار تغییرات $NSNR$ برای یک تصویر با درصدهای جاسازی متفاوت را نمایش می‌دهد.



شکل(5): $NSNR$ به دست آمده با درصدهای جاسازی متفاوت برای یک تصویر نمونه

در شکل 6 تصویر گل پس از جاسازی 1050 بیت در آن که معادل 0/7 درصد از کل پیکسلها است، نمایش داده شده است.

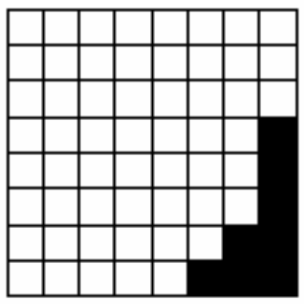
همانطور که مشاهده می‌شود در ناحیه یکرنگ (سفید) تعدادی نقاط سیاه ایجاد شده که در اثر جاسازی بیتهای صفر پیام در آن می‌باشد. عیب این روش امکان حمله دیداری به آن در نواحی یک رنگ می‌باشد.



شکل(6): تصویر گل با جاسازی 1050 بیت

از آنجا که جاسازی در نواحی یک رنگ در معرض حمله حتی حمله دیداری می‌باشد، برای جلوگیری از این حملات می‌توان تصویر را به بلوکهایی با ابعاد مناسب (مثلا 16×16) تقسیم کرده و سپس در بلوکی‌هایی اطلاعات جاسازی کنیم که یکنواخت نباشند. به بلوک هایی که خیلی یکنواخت نیستند بلوکهای پیچیده گوئیم. معیار پیچیدگی که ما استفاده کرده‌ایم معیار پیچیدگی مرز سیاه و سفید[28] می‌باشد که در مرجع [19] بیان شده است.

اگر کل یا اغلب پیکسلهای یک بلوک سیاه یا سفید باشند، آن بلوک ساده است. شکل 7 یک بلوک 8×8 ساده[29] را نمایش می‌دهد. فرض کنید بین هر دو پیکسل بلوک مرزی وجود دارد. در بلوک نمایش داده شده در شکل 7، $(8-1) \times 8 \times 2 = 112$ مرز بین پیکسلها وجود دارد اما فقط هشت‌تای آنها مرز بین پیکسل سیاه و سفید می‌باشد. بقیه مرزها بین دو پیکسل همرنگ (سیاه-سیاه یا سفید-سفید) می‌باشند. بنابراین بلوکی می‌تواند ساده باشد که تعداد مرزهای بین پیکسلهای سیاه و سفید آن کم باشد.



شکل (7): یک بلوک ساده

به طور کلی، تعداد مرزهای بلوکی با اندازه $M \times N$ برابر با $M(N-1) + N(M-1)$ است. این مشاهدات به ما اجازه تعریف معیاری برای پیچیدگی بر مبنای مجموع مرزهای بین پیکسلها-ی سیاه و سفید می‌دهد. فرض کنید T تا مرز پیکسلی در بلوکی وجود دارد و فقط τ تا از آنها بین پیکسل‌های سیاه و سفید هستند آنگاه معیار پیچیدگی به صورت زیر تعریف می‌شود.

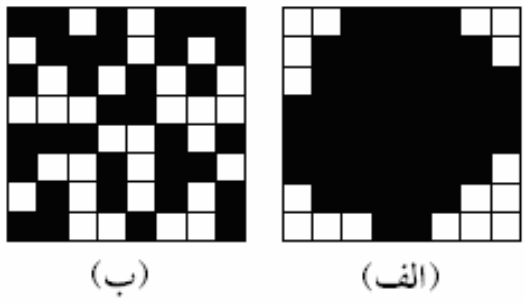
$$\alpha = \frac{\tau}{T} \quad (3)$$

در شکل 7، $\alpha = \frac{8}{112}$ می‌باشد. اگر α بزرگ باشد به معنی آن است که در آن بلوک مرز بین پیکسلهای سیاه و سفید زیاد است و ما می‌توانیم آنرا پیچیده در نظر بگیریم. اگر α کوچک باشد، بلوک ساده است. این معیار در بازه $[0,1]$ قرار دارد. با مقدار آستانه α_0 می‌توان بین بلوکهای ساده و پیچیده تمایز قائل شد. بلوک B را پیچیده گوییم، اگر $\alpha(B) \geq \alpha_0$ باشد. معمولا مقدار α_0 به صورت تجربی برابر 0/3 انتخاب می گردد[19]. شکل 8(الف)، بلوک ساده-

www.SID.ir

Archive of SID

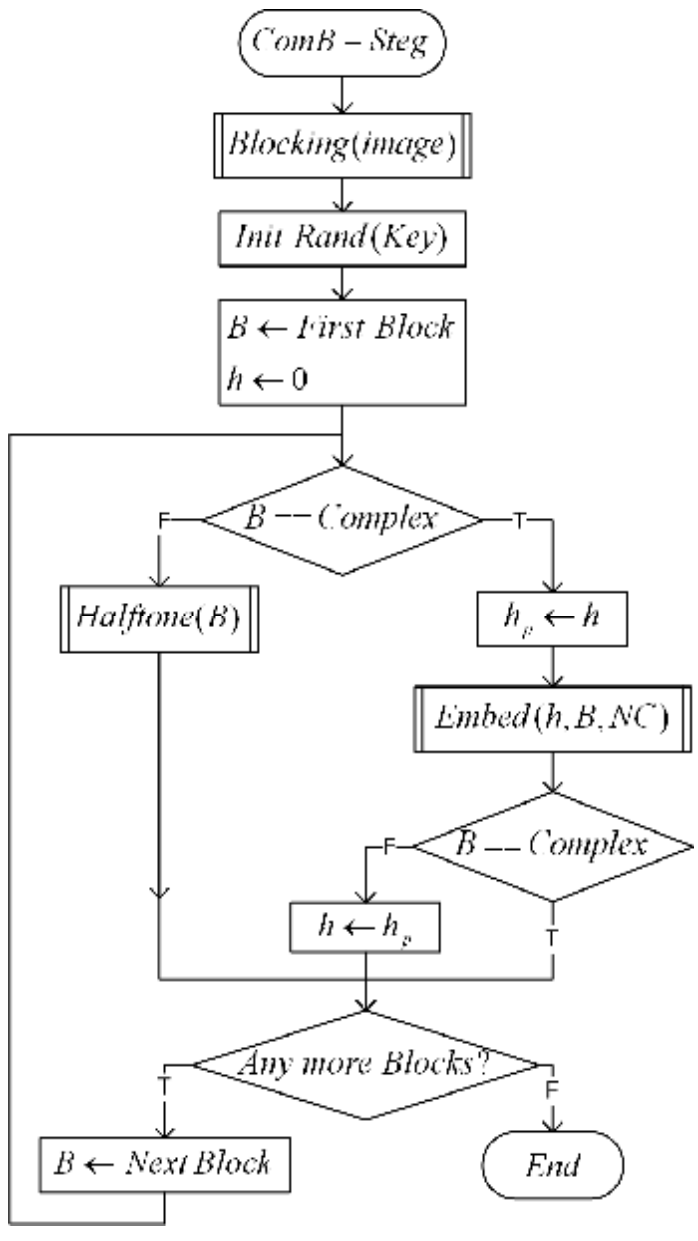
$\left(\alpha = \frac{20}{112}\right)$ و شکل 8(ب) بلوک پیچیده‌ای $\left(\alpha = \frac{72}{112}\right)$ را نمایش می‌دهند.



شکل(8): (الف) یک بلوک ساده، (ب) یک بلوک پیچیده

با استفاده از معیار پیچیدگی بیان‌شده، جاسازی را فقط در نواحی پیچیده انجام می‌دهیم. شکل 9 الگوریتم جاسازی با در نظر گرفتن پیچیدگی بلوک‌ها را نمایش می‌دهد.

مطابق شکل 9، ابتدا تصویر را به بلوکهایی با ابعاد مساوی (16×16) تقسیم کرده، هر بلوک را به روش فلوید استاینبرگ، دوسطحی کرده و سپس پیچیدگی آنرا محاسبه می‌کنیم $(Blocking(image))$. برای آنکه بتوانیم تعداد پیکسل‌هایی که برای جاسازی مناسب اند (NC) را تشخیص دهیم باید تعداد بلوک‌های پیچیده را تعیین کنیم. در صورتی که تعداد بلوک‌های پیچیده $($ تا باشد تعداد پیکسل‌هایی که ممکن است برای جاسازی بکار روند برابر $NC = ($ خواهد بود که در آن $M \times N$ و N M ابعاد بلوک‌ها هستند.

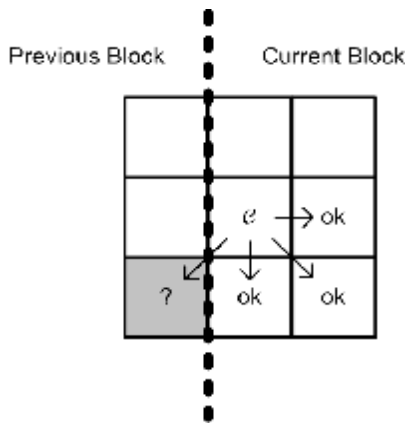


شکل(9): روندنمای روش *ComB-Steg*

پس از بلوک بندی تصویر، PRNG[30] را با کلید جاسازی مقدار دهی می‌کنیم. اکنون برای هر بلوک در صورتی که پیچیده نباشد عمل دوسطحی سازی بدون جاسازی صورت می‌گیرد $(Halftone(B))$ و در صورتی که بلوک پیچیده باشد جاسازی مطابق شکل 4 صورت می‌گیرد.

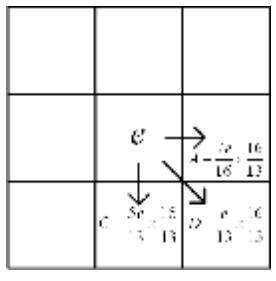
نکته حائز اهمیت این است که در اثر جاسازی داده در بلوک، این امکان وجود دارد که بلوکی که قبل از جاسازی پیچیده بوده، بعد از آن دیگر پیچیده نباشد. این امکان، استخراج[31] داده را با مشکل مواجه می‌سازد. زیرا روال استخراج بدین صورت است که ابتدا تصویر را بلوک‌بندی کرده و سپس مطابق معیار پیچیدگی بلوک‌ها بررسی می‌شود که بلوک پیچیده هست یا خیر. اگر بلوک پیچیده نبود به سراغ بلوک بعد می‌رویم، و اگر بلوک پیچیده بود بیتهای داده را از محلهای شبه تصادفی با همان کلیدی استخراج می‌کنیم که زمان جاسازی به کار رفته است. اگر بلوک قبل از جاسازی پیچیده باشد ولی بعد از آن دیگر پیچیده نباشد، در زمان استخراج فرض بر آن است که داده در آن جاسازی نشده است. البته این مشکل به ندرت رخ می‌دهد. با اینحال برای رفع این مشکل در فرآیند جاسازی داده، پس از جاسازی در هر بلوک باید مجدداً پیچیدگی بلوک گنجانه[32] محاسبه شود. در صورتی که بلوک دیگر پیچیده نباشد باید داده های جاسازی شده در این بلوک در بلوک پیچیدهٔ بعدی دوباره جاسازی شود $(h \leftarrow h_p)$.

در الگوریتم *Comb-Steg*، هنگامی که در لبه چپ بلوک قرار داریم، مطابق روش فلوید استاینبرگ باید 3/16 خطا در پیکسل سمت چپ و پائین منتشر گردد در حالی که عملیات مربوط به بلوک قبلی تمام شده است. شکل 10 این مساله را نشان می‌دهد.



شکل(10): مشکل انتشار خطا در سمت چپ بلوک

به همین دلیل خطا را در لبه سمت چپ بلوک مانند شکل 11 انتشار می‌دهیم. در پیکسلهای دیگر یعنی پیکسلهایی که در مرز سمت چپ بلوک قرار ندارند، خطا را طبق شکل 1 انتشار می‌دهیم. در لبه‌های پایینی بلوک نیز مشکلی وجود نخواهد داشت زیرا انتشار فلوید استاینبرگ رو به بالا صورت نمی‌گیرد.



www.SID.ir

Archive of SID

شکل(11): انتشار خطا در لبه سمت چپ بلوک

شکل 12 تصویر *Cameraman* بدون جاسازی را نشان می‌دهد و شکل 13، تصویر *Cameraman* با جاسازی 1000 بیت داده (معادل 2 درصد) و اندازه بلوک 16 را نمایش می‌دهد.

شکل(12): تصویر Cameraman بدون جاسازی

کیفیت تصویر دوسطحی حاوی داده با کیفیت تصویر دوسطحی‌ای که داده‌ای در آن جاسازی نشده است مشابه است. با این‌حال همانطور که در شکل 13 با کمی دقت می‌توان دید خطوط عمودی که نشان دهنده لبه بلوک‌ها می‌باشند، در پالتوی مرد عکاس قابل مشاهده هستند. این خطوط عمودی می‌تواند موجب کشف وجود داده جاسازی شده به روش *ComB-Steg* گردد.

شکل (13) : تصویر Cameraman با جاسازی 1000بیت و انتشار خطای غیر یکسان در لبه سمت چپ بلوک

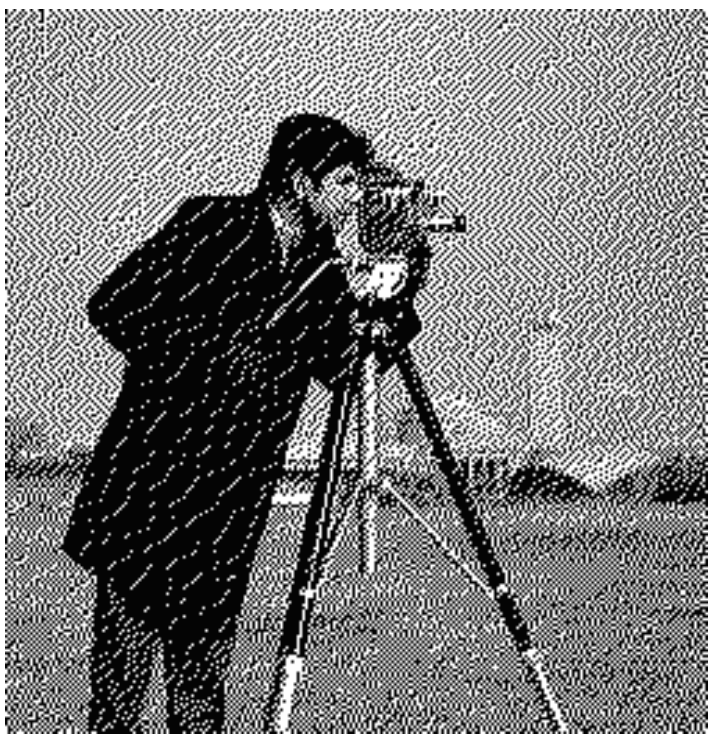
خطوط عمودی موجود در پالتوی مرد عکاس (شکل 13) حذف شده‌اند اما کیفیت تصویر به دست آمده خیلی مطلوب نیست و خطوط مورب در پالتوی مرد عکاس به وجود آمده است که به دلیل عدم استفاده از روش انتشار خطای فلوید استاینبرگ است.

3- بهینه سازی *ComB-Steg*

با توجه به شکل 14 مشاهده می‌شود که کیفیت تصویر به دلیل عدم استفاده از روش فلوید استاینبرگ برای انتشار خطا پایین آمده است. برای رفع این مشکل باید روش خود را طوری تغییر دهیم که بتوان انتشار خطا را برای همهٔ پیکسل‌ها، با روش فلوید استاینبرگ صورت دهیم. به این منظور به جای آنکه پیچیدگی را به بلوک‌های تصویر نسبت دهیم آنرا به پیکسل‌های تصویر (p_k) نسبت می‌دهیم. پیچیدگی پیکسل را $\alpha(p_k)$ می‌نامیم. برای محاسبه $\alpha(p_k)$ از بلوک تصمیم گیر[33] استفاده می‌کنیم که آنرا $DB_{MxN}(p_k)$ می‌نامیم.

این مشکل به این دلیل به وجود آمده است که انتشار خطا در همه پیکسلها یکسان نیست. خطا در پیکسلهای واقع در لبه چپ بلوک طبق شکل 11 انتشار می‌یابد در حالی که خطا در پیکسلهای دیگر طبق شکل 1 منتشر می‌شود. در نتیجه لبه های بلوک به صورت تعدادی خطوط عمودی قابل رؤیت است.

برای رفع این مشکل در همه پیکسلها به صورت یکسان طبق شکل 11 خطا را انتشار دادیم. شکل 14، تصویر *Cameraman* با جاسازی 1000 بیت داده، معادل 2 درصد را نمایش می‌دهد که انتشار خطا در آن در همه پیکسلها به صورت یکسان و طبق شکل 11 انجام شده است.

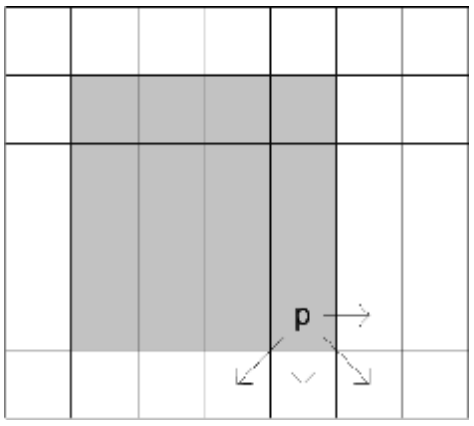


شکل (14) :تصویر Cameraman با جاسازی 1000بیت و انتشارخطای یکسان در همه پیکسلها

www.SID.ir

Archive of SID

بلوک تصمیم گیر برای پیکسل p_k ، بلوکی با اندازه $M \times N$ است که p_k در گوشه سمت راست و پایین آن واقع شده باشد. شکل 15 بلوک تصمیم گیر برای یک پیکسل را نشان می‌دهد.



شکل (15): بلوک تصمیم گیر با ابعاد 4 در 4

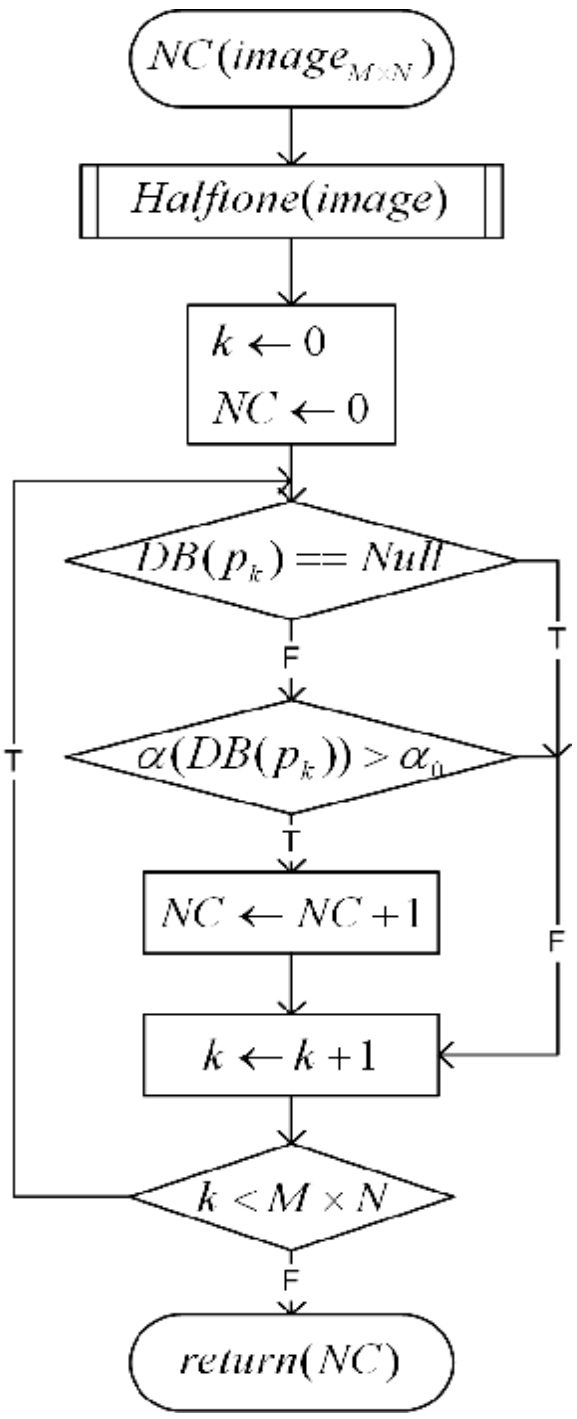
در شکل 15 بلوک تصمیم گیر $DB_{4\times4}(p)$ با رنگ خاکستری برای پیکسل p نشان داده شده است. $\alpha(p_k)$ را برابر $\alpha(DB_{M\times N}(p_k))$ تعریف می‌کنیم که از رابطه 3 به دست می‌آید. پیکسلی را پیچیده گوییم که برای آن شرط $\alpha(p_k) > \alpha_0$ صادق باشد.

برای برخی از پیکسلها که در حواشی بالا و سمت چپ تصویر قرار دارند، بلوک تصمیم گیر وجود ندارد. در این حالت می‌گوییم که $DB_{M\times N}(p_k)$ برابر $Null$ است.

برای آنکه بتوان داده‌ها را به صورت یکنواخت در پیکسل‌های پیچیده جاسازی کرد لازم است تعداد پیکسل‌های پیچیده قبل از شروع جاسازی محاسبه گردد. شکل 16 الگوریتم محاسبه تعداد پیکسل‌های پیچیده را نشان داده است.

مطابق شکل 16، ابتدا تصویر توسط روش فلوید استاینبرگ دوسطحی می‌گردد. سپس برای هر پیکسل چک می‌شود که آیا بلوک تصمیم گیر برای آن وجود دارد یا خیر. در صورتی که وجود داشته باشد چک می‌شود که بلوک تصمیم گیر برای آن پیچیده هست یا خیر. در صورت پیچیده بودن به تعداد پیکسل‌های پیچیده یکی افزوده می‌شود. پس از شمارش تعداد پیکسل¬های پیچیده مجددا به تصویر سطح خاکستری برمی گردیم و عملیات جاسازی را در حین دو سطح سازی اجرا می کنیم.

با توجه به مقدمات فوق، الگوریتم نهایی ارائه شده که به آن *EComB-Steg*[34] می‌گوییم به صورت الگوریتم نشان داده شده در شکل 17 خواهد بود.

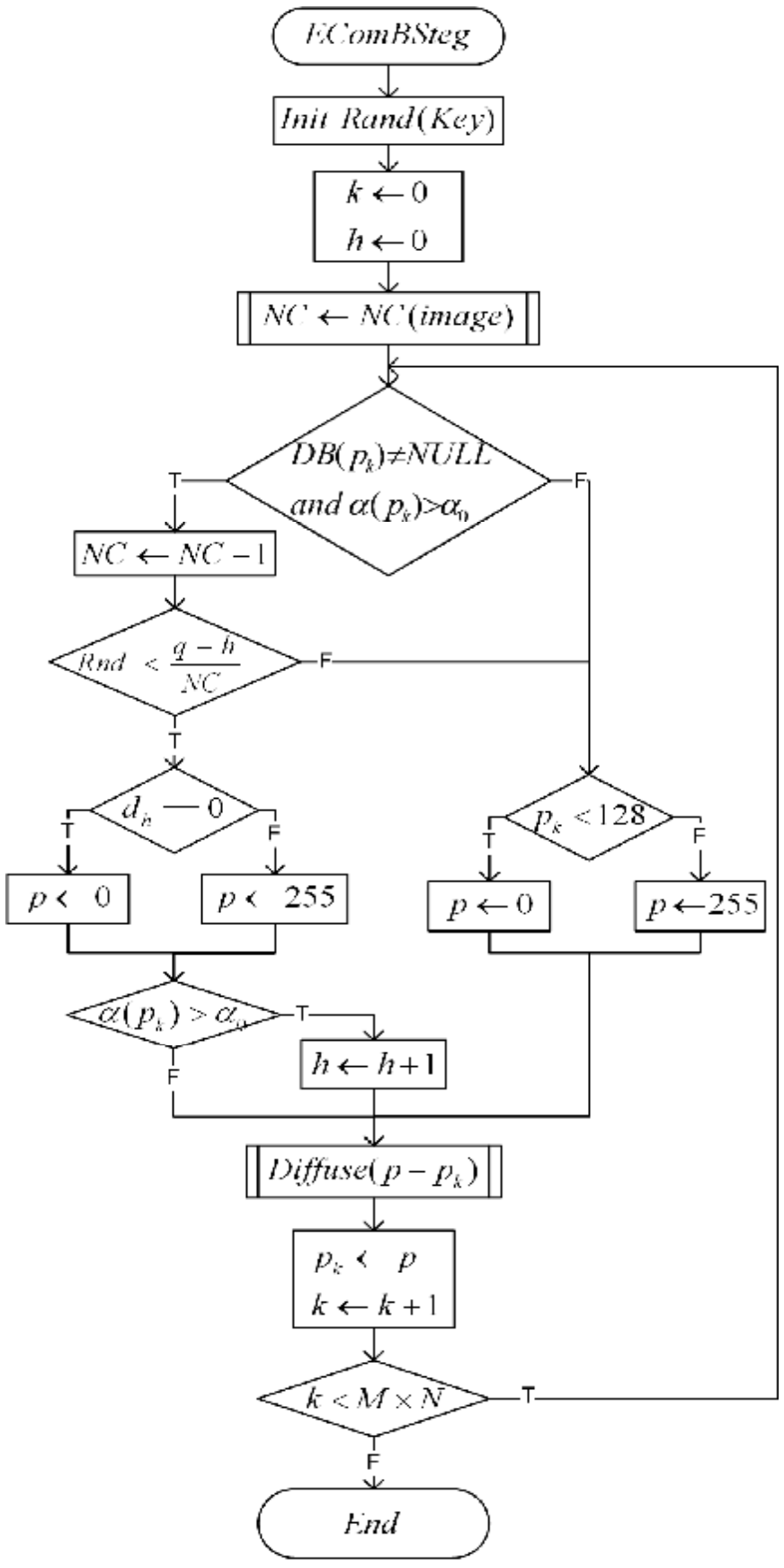


شکل (16): الگوریتم شمردن تعداد پیکسل‌های پیچیده

مطابق الگوریتم نمایش داده شده در شکل 17، ابتدا یک PRNGبا یک کلید مقدار دهی می‌شود. سپس تصویر از گوشه سمت چپ و بالا پیمایش شده و تعداد پیکسل‌های پیچیده تصویر, یعنی NC به دست می‌آید. پس از آن تصویر اصلی (دو سطحی نشده) به صورت ردیفی از گوشه سمت چپ و بالا پیمایش شده و برای هر پیکسل (p_k) عملیات جاسازی یا عملیات دوسطحی سازی صورت می‌گیرد. در صورتی که بلوک تصمیم گیر وجود نداشته باشد یا پیکسل پیچیده نباشد عمل دوسطحی سازی به روش معمول صورت می‌گیرد. در غیر این صورت از تعداد کل پیکسل‌های پیچیده NC یکی کاسته می-شود و برای آن عدد شبه تصادفی‌ای تولید می‌شود. در صورتی که عدد تصادفی از مقدار $\frac{q-h}{NC}$ بیشتر باشد باز هم عمل دوسطحی سازی به روش معمول صورت می‌گیرد. در صورتی که اینطور نباشد یک بیت داده (d_k) در پیکسل جاسازی می‌گردد.

www.SID.ir

Archive of SID



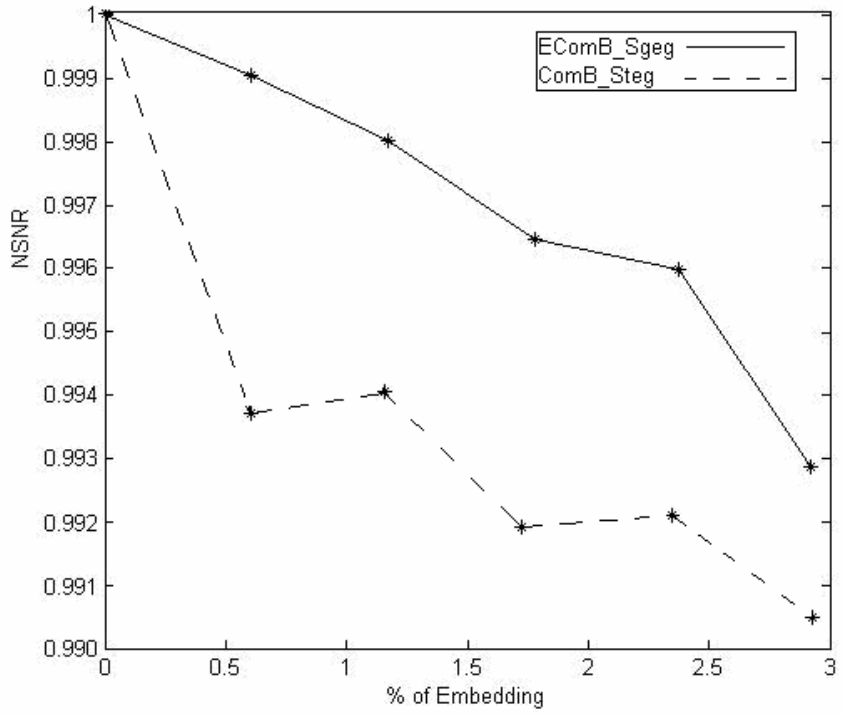
شکل (17): الگوریتم *EComb-Steg*

ممکن است در اثر جاسازی داده، پیچیدگی پیکسل از دست برود و تبدیل به یک پیکسل غیر پیچیده شود و روند استخراج داده‌ها را مختل کند. به همین دلیل پس از جاسازی پیچیدگی پیکسل امتحان می‌گردد و در صورتی که پیکسل هنوز هم پیچیده باشد اندیس داده‌ها یکی اضافه می‌گردد. در صورتی که پیکسل پیچیدگی خود را از دست داده باشد عدد شبه تصادفی تولید شده که برای تصمیم گیری برای جاسازی بکار رفته است برای پیکسل پیچیده بعدی بکار خواهد رفت تا بتوان در هنگام استخراج رشته اعداد تصادفی درستی تولید گردد.

در هر صورت، مقدار خطای ایجاد شده در اثر جاسازی یا دوسطحی سازی در پیکسل‌های مجاور منتشر می‌گردد یعنی تابع $Diffuse(p-p_k)$ اجرا می‌شود.

با این روش انتشار خطا به روش فلوید استاینبرگ، امکان پذیر خواهد بود، زیرا انتشار خطا در پیکسل‌های بلوک تصمیم گیر صورت نمی-گیرد.

در شکل 18 *NSNR* مربوط به تصویر گل با درصد جاسازیهای مختلف با هر دو روش ***ComB-Steg*** و ***EComB-Steg*** نشان داده شده است.



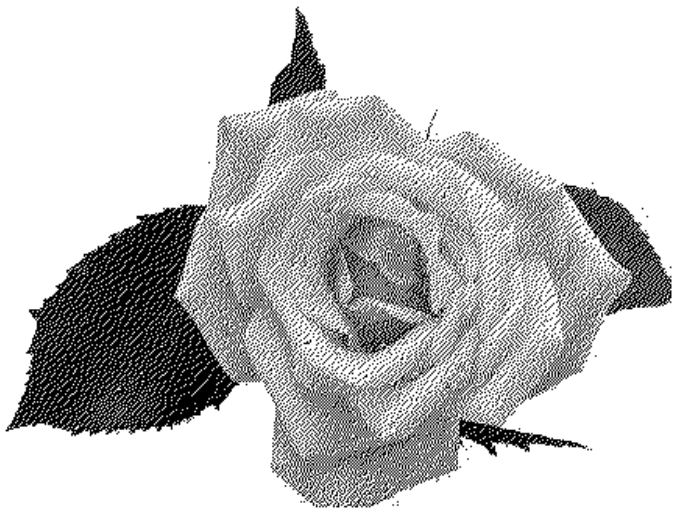
شکل(18): مقایسه *NSNR* تصویر گل با دو روش *ComB-Steg* و *EComB-Steg*

در شکل 18 خط ممتد *NSNR* مربوط به روش بهبود یافته یعنی *EComB-Steg* و خط چین مربوط به روش *ComB-Steg* است. با مقایسه این دو منحنی نتیجه می‌گیریم که روش *EComB-Steg* نسبت به روش اولیه دارای مقدار *NSNR* بزرگتر و در نتیجه خطای کمتری است.

برای استخراج داده‌های جاسازی شده در تصویر گنجانه با داشتن کلید بکار رفته برای مقدار دهی اولیه *PRNG* و طول داده‌های جاسازی شده ابتدا به روشی که در شکل 16 شرح آن رفت تعداد پیکسل‌های پیچیده را به دست می‌آوریم. سپس از گوشه سمت چپ و بالای تصویر شروع کرده و برای هر پیکسل پیچیدگی آنرا با توجه به بلوک تصمیم گیر آن محاسبه می‌کنیم و در صورت پیچیده بودن یک عدد شبه تصادفی توسط *PRNG* تولید می‌کنیم و توسط آن پیکسل‌هایی که حاوی داده هستند را شناسایی می‌کنیم. شکل 19 الگوریتم استخراج داده‌ها را نشان می‌دهد.

www.SID.ir

Archive of SID



شکل(20): تصویر گل با 1691 بیت معادل 1 درصد جاسازی توسط الگوریتم ارتقاء یافته (*EComB-Steg*)

واضح است که نمی‌توان از تمام پیکسل‌های تصویر برای جاسازی استفاده کرد زیرا وجود داده پنهان در تصویر بر ملا خواهد شد. بنابراین لازم است نسبت ماکزیمم تعداد پیکسل‌هایی که می‌توان برای جاسازی استفاده کرد به تعداد کل پیکسل‌ها به دست آید. این نسبت را S می نامیم. در این صورت ظرفیت یک تصویر بر حسب بیت از رابطه زیر به دست خواهد آمد.

$$C = Number\ of\ complex\ pixels \times S$$

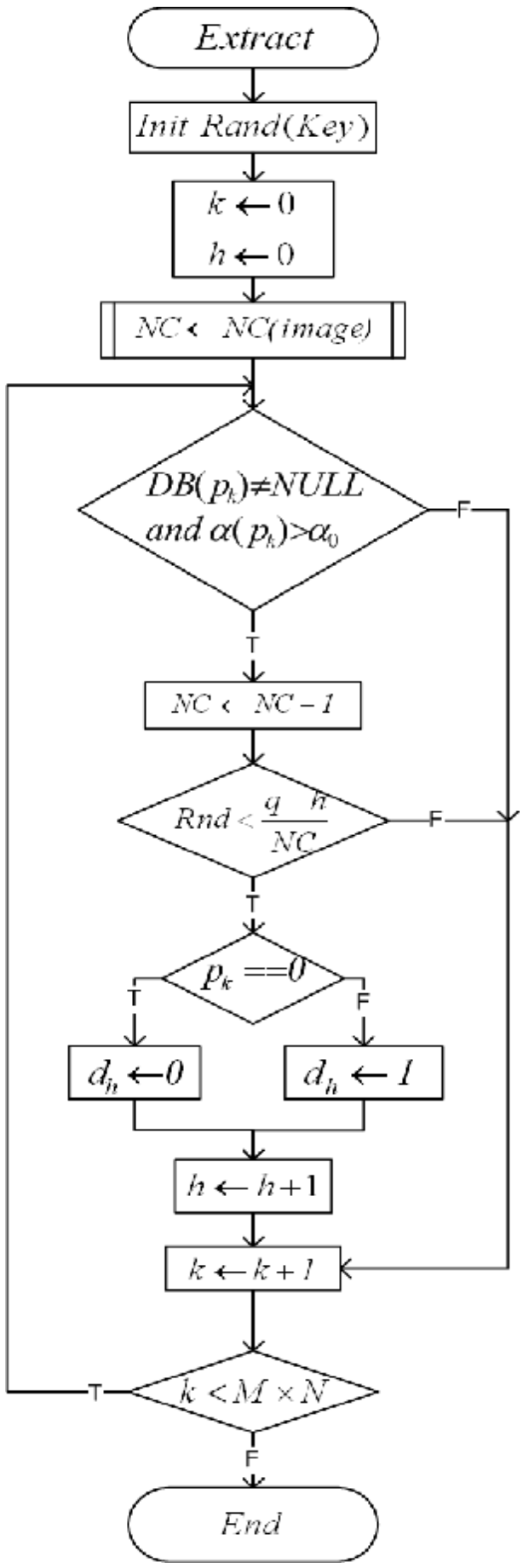
برای به دست آوردن مقدار S، روش *EComb-Steg* بوسیله نرم افزار Matlab v7.1 پیاده‌سازی شد و در هفت تصویر BMP که دارای ابعاد متفاوت بودند، به روش ذکر شده جاسازی انجام دادیم و میزان جاسازی را تا حدی بالا بردیم که تصویر از نظر ظاهری خراب نشود. جدول1 نتایج حاصله برای تخمین S را نشان می دهد.

جدول(1): جاسازی داده در تعدادی تصویر و به دست آوردن معیار کیفیت S

تصویر	S	پیچیدگی	ظرفیت(بیت)
1	0,010	0,695	2500
2	0,007	0,987	7300
3	0,012	1	3200
4	0,008	0,825	5200
5	0,006	0,792	700
6	0,008	0,963	2250
7	0,008	0,966	3100

در جدول 1 منظور از پیچیدگی، نسبت تعداد پیکسل‌های پیچیده به پیکسل‌های ساده است.

مقدار S را به طور کلی کوچکترین S به دست آمده برای این تصاویر نمونه پیشنهاد می‌کنیم. بنابراین $S = 0.006$ مقدار مناسبی برای تعیین ظرفیت تصاویر قبل از خراب شدن تصویر می‌باشد که برای تصاویر دوسطحی شده ظرفیت خوبی است.



شکل (19): الگوریتم استخراج داده ها

4- نتایج پیاده‌سازی

شکل 20 حاصل اجرای روش *EComB-Steg* با اندازه بلوک 8*8 بر روی تصویر گل را نشان می‌دهد.

همانطور که در شکل 20 ملاحظه می‌شود به دلیل استفاده از معیار پیچیدگی در نواحی یک رنگ (سفید) اطراف گل، داده جاسازی نشده است در نتیجه نقاط سیاه رنگ که در شکل 6 وجود داشت از بین رفته‌اند.

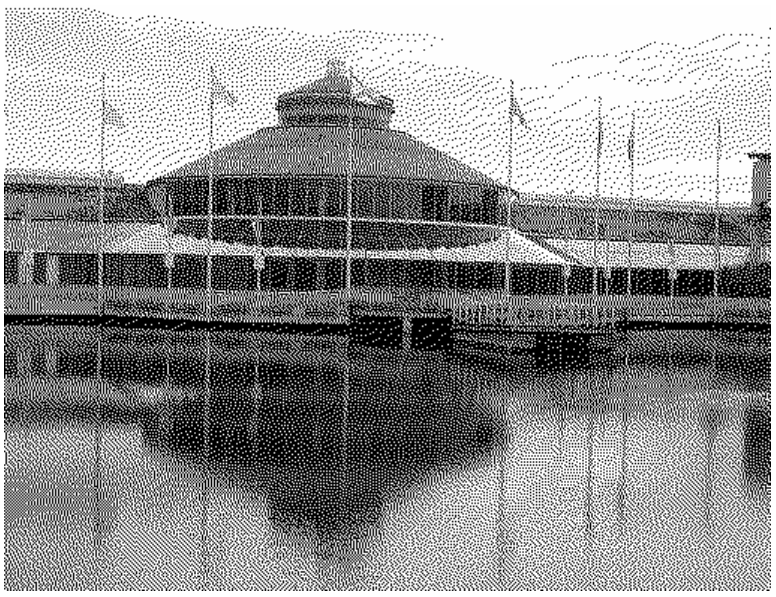
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.6- No.1- Spring and Summer 2009

www.SID.ir

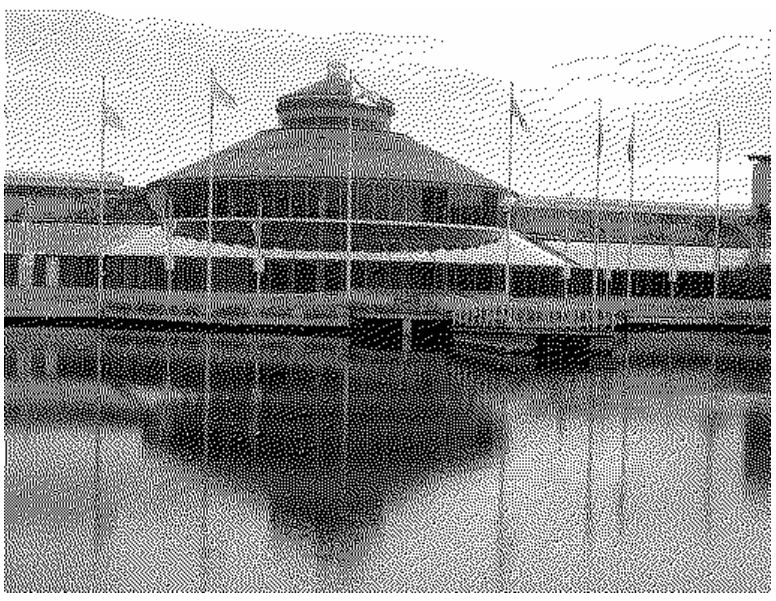
Archive of SID

دو تصویر از این تصاویر در شکل 21 تا شکل 26 آورده شده است. هر تصویر, قبل از دوسطحی سازی, بعد از دوسطحی سازی بدون جاسازی و بعد از دوسطحی سازی و جاسازی نمایش داده شده است.

شکل (21): تصویر اصلی قبل از دوسطحی سازی

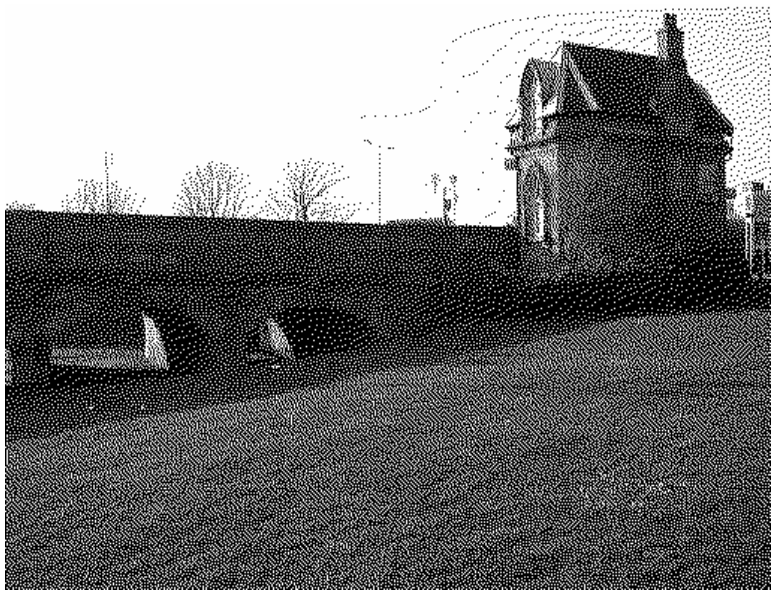


شکل (22): تصویر بعد از دوسطحی سازی بدون جاسازی

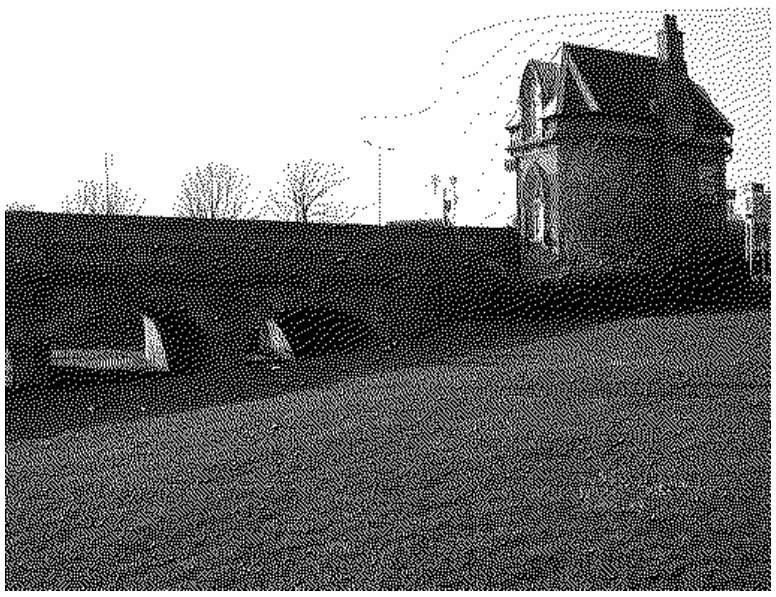


شکل (23): تصویر بعد از دوسطحی سازی و جاسازی

شکل (24): تصویر اصلی قبل از دوسطحی سازی



شکل(25): تصویر بعد از دوسطحی سازی و قبل از جاسازی



شکل (26): تصویر بعد از دوسطحی سازی و جاسازی

با بررسی اشکال فوق متوجه می‌شویم که تفاوت معنی داری بین تصاویر حاوی جاسازی و تصاویری که داده ای در خود مخفی کرده اند دیده نمی‌شود. همچنین حملاتی که در مراجع [8] و [9] و [11] ذکر شده است برای کشف جاسازی بعد از دوسطحی سازی بوده و برای حمله به این روش طراحی نشده اند. پیاده سازی حمله ذکر شده در مرجع [8] نیز صورت گرفت و با توجه به آنکه این حمله اصولا برای این نوع جاسازی موثر نبود تمایزی بین تصویر گنجانه و پوشانه مشاهده نشد.

www.SID.ir

Archive of SID

5- نتیجه گیری

در این مقاله روشی برای پنهان نگاری در تصاویر دوسطحی ارائه گردید. در این روش عمل جاسازی همزمان با دوسطحی سازی انجام می‌شود و خطای حاصله از جاسازی به پیکسلهای مجاور انتشار می‌یابد. با جاسازی در بلوک‌های ساده تصویر امکان کشف پنهان‌نگاری از طریق چشم وجود دارد. در این مقاله معیاری برای تشخیص بلوک‌های ساده بکار بردیم و روشی را پیشنهاد کردیم که مانع از جاسازی در بلوک‌های ساده تصویر می‌گردد. در برخی روشهای پنهان‌نگاری مرحله جاسازی پس از دوسطحی سازی قراردارد که باعث کاهش زیاد ظرفیت می‌گردد. در روش پیشنهادی انتشار خطای حاصل از جاسازی داده در پیکسلهای مجاور سبب حفظ کیفیت تصویر و بهره‌مندی از ظرفیت بالاتری نسبت به روشهای قبلی شده است. روش پیشنهادی از معیار پیچیدگی استفاده کرده است که باعث کاهش چشمگیر خطا و بهبود کیفیت گردیده است. پیاده‌سازی‌های انجام شده صحت و دقت روش را نشان می‌دهد.

مراجع:

[1] R.J. Anderson, F.A.P. Petitcolas, “On the Limits of Steganography,” IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and privacy Protection, Vol. 16(4), pp. 474-481, May 1998.

[2] K. Wong, X. Qi, K. Tanaka, “A DCT-based Mod4 steganographic method,” Signal Processing, Vol. 87, No. 6, pp. 1251-1263, 2007.

[3] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, “Steganalysis of Pixel-Value Differencing Stegano-graphic Method,” Proceedings of IEEE Pacific Rim, pp. 292-295, August 2007.

[4] P. Wayner, “Disappearing Cryptography: Information Hiding: Steganography and Watermarking,” (2nd Edition), Morgan Kaufmann Publishers Inc., San Francisco, CA, 2002.

[5] M. Wu, E. Tang, B. Liu, “Data Hiding in Digital Binary Image,” Proceedings of IEEE International Conference on Multimedia & Expo (ICME'00), pp. 393-396, 2000.

[6] M. Y. Wu. And J. H. Lee, “A novel data embedding method for two-color facsimile images,” Proceedings of international symposium on multimedia information processing, (ICASSP), Vol. 2, pp. 1161-1164, 1998.

[7] Y. C. Tseng, Y. Y. Chen, H.-K. Pan, “A Secure Data Hiding Scheme for Binary Images”, IEEE Transaction on Communications, Vol. 50, No. 8, pp. 1227-1231, 2002.

[8] M. Jiang, N. Memon, E. Wong, “Quantitative Steganalysis of Binary Images,” International Conference on Image Processing, Vol. 1, pp. 29-32, 2004.

[9] X. Yu, Y. Wang, T. Tan, “Steganalysis of Data Hiding In Binary Images,” Proceedings of the 17th International Conference on Pattern Recognition, Vol. 4, pp. 877-880, 2004.

[10] H. Y. Kim and A. Afif, “Secure authentication water-marking for binary images,” Proceedings of the Brazilian Symposium on Computer Graphics and Image Processing, pp. 199-206, Oct. 2003.

[11] M. Jiang, E. K. Wong, N. Memon, X. Wu, "Steganalysis of Halftone Images,” Proceedings of ICASSP, Vol. 2, pp. ii/793- ii/796, 2005.

[12] R. W. Floyd and L. Steinberg, “Adaptive algorithm for spatial grayscale,” Proceedings of SID, vol. 17, no. 2, pp. 75–77 1976.

[13] T. N. Pappas, J. P. Allebach, and D. L. Neuhoff, "Model-based digital halftoning," IEEE Signal Processing Mag., Vol. 20, pp. 14--27, July 2003.

[14] R. Ulichney, “Dithering with blue noise,” Proceedings of the IEEE Vol. 76, pp. 56-79, Jan. 1988.

[15] T. Mitsa and K. Parker, “Digital halftoning using a blue noise mask,” Journal of Optical Society of America, A 9, pp. 1920-1929, 1992.

[16] S. H. Kim and J. P. Allebach, “Impact of human visual system models on model based halftoning,” IEEE Transaction on Image Processing, Vol. 11, pp. 258-269, 2002.

[17] Z. Fan and R. Eschbach, “Limit cycle behavior of error diffusion,” Proceedings of the IEEE International Conference on Image Processing, Vol. 2, pp. 1041-1045, Nov. 1994.

[18] M. S. Fu and O. C. Au, “Data hiding Watermarking for Halftone Images,” IEEE Transactions on Image Processing, Vol. 11, No. 4, pp.477-484, April 2002.

[19] E. Kawaguchi and R. O. Eason, “Principle and applications of BPCS steganography,” Proceedings of SPIE's International Symposium on Voice, Video, and Data Communications, pp. 464-473, Nov. 1998.

زیرنویس‌ها

[1] Steganography
[2] Information hiding
[3] Cryptography
[4] Watermarking
[5] Attacker, Warden
[6] Cryptanalysis
[7] Steganalysis
[8] Watermark
[9] Cover Medium
[10] Stego Medium
[11] Halftone
[12] Halftoning
[13] Mark
[14] Pseudo random number generator (PRNG)
[15] Quadrature mirror filters
[16] Feature
[17] Linear classifier
[18] Floyd Steinberg
[19] Classical screening
[20] Dithering with blue noise
[21] Direct binary search

www.SID.ir

Archive of SID

[22] Salt and pepper noise
[23] Mid-gray smooth regions
[24] Visual quality
[25] Complexity Based Steganography in halftone images (Comb-Steg)
[26] Signal to Noise Ratio
[27] Normalized SNR
[28] Black and White Border Complexity
[29] Simple
[30] Pseudo Random Number Generator
[31] Extract
[32] Stego Block
[33] Decision Block
[34] Enhanced Comb-Steg

www.SID.ir