نشریه علمی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۱۴۵-۱۳۳

طراحی یک الگوریتم نهان‌نگاری تصویر ترکیبی بر مبنای نظریه بازی‌ها

محمدعلی شمع‌علیزاده بایی*
استادیار، دانشگاه افسری امام حسین(ع)، مجتمع دانشگاهی علوم و فنون دریایی امام خامنه‌ای((مدظله)) گیلان
(دریافت: ۹۷/۱۰/۰۹، پذیرش: ۹۸/۰۳/۲۸)

چکیده
روش‌های نهان‌نگاری تطبیقی با استفاده از یک معیار تطبیق، به‌صورت ترتیبی یا تصادفی به مخفی‌سازی پیام در تصویر می‌پردازند. هدف از امنیت، کاهش احتمال تشخیص وجود پیام است. در این مقاله، نخست با استفاده از نظریه بازی‌ها، نشان داده می‌شود که الگوریتم نهان‌نگاری تطبیقی همراه با یک روند شبه‌تصادفی که الگوریتم نهان‌نگاری ترکیبی نامیده می‌شود، نسبت به الگوریتم نهان‌نگاری تطبیقی محض از امنیت بالاتری برخوردار است. سپس این مطلب در عمل با طراحی الگوریتم‌هایی مبتنی‌بر آنتروپی و عملگر Xor، برای ۵۰۰۰ تصویر طبیعی نشان داده می‌شود. مقایسه دو الگوریتم طراحی‌شده توسط یکی از الگوریتم‌های معروف نهان‌کاوی یعنی SRM، نشان از برتری امنیتی روش تطبیقی ترکیبی در مقایسه با روش تطبیقی محض دارد.

کلیدواژه‌ها: نهان‌نگاری تطبیقی محض، نهان‌نگاری ترکیبی، امنیت، نظریه بازی‌ها

۱. مقدمه
روش‌های نهان‌نگاری تطبیقی به متن پوشانه‌های تصویری توجه ویژه‌ای دارند. مناطق پرنوسان و با تغییرات بیش‌تر تصاویر را مناطق زبر می‌نامیم. این روش‌ها زبرترین مناطق تصویر به مفهوم فوق را شناسایی کرده و به مخفی‌سازی پیام در آن مناطق می‌پردازند [۲-۱].

روش‌های نهان‌نگاری تطبیقی با استفاده از یک معیار تطبیق و به یکی از دو روش ترتیبی و تصادفی به جستجوی مکان‌های مخفی‌سازی پیام در پوشانه‌های تصویری می‌پردازند. روش‌هایی که صرفاً با یک معیار تطبیق و به‌صورت ترتیبی به مخفی‌سازی پیام در تصویر می‌پردازند را روش‌های نهان‌نگاری تطبیقی محض و روش‌هایی که علاوه‌بر معیار تطبیق از یک روند شبه‌تصادفی نیز استفاده کنند را نهان‌نگاری ترکیبی می‌نامیم. یکی از اصول مهم در نهان‌نگاری اصل کهرشف است [۳]. مطابق این اصل همانند رمزنگاری، همه پارامترهای نهان‌نگاری، به‌جز احیاناً کلید مورد استفاده، آشکار است. اگر به این اصل توجه کنیم، نهان‌نگاری تطبیقی محض از امنیت مناسبی برخوردار نیست. چرا که هر تحلیل‌گر از الگوریتم تطبیق یعنی الگوریتم تشخیص مکان‌های مخفی‌سازی پیام باخبر است. بنابراین، نخست در این مقاله با استفاده از نظریه بازی‌ها امنیت در نهان‌نگاری تطبیقی را مورد بررسی قرار می‌دهیم. تصمیم‌گیری در مورد چگونگی انتخاب مناطق مخفی‌سازی پیام در نهان‌نگاری تطبیقی یکی از مسائل کلیدی طرح پیشنهادی در این مقاله است. سپس با استفاده از آنتروپی، معیاری برای شناسایی مناطق زبر و پرنوسان تصویر، طراحی کرده و با استفاده از این معیار و یک الگوریتم مخفی‌سازی پیام، که با عملگر xor ساخته می‌شود، یک الگوریتم نهان‌نگاری تطبیقی با دو رویکرد محض و ترکیبی ارائه شده و مورد ارزیابی قرار می‌گیرد. به این ترتیب نتایج به‌دست‌آمده از نظریه بازی تایید خواهد شد.

در ادامه این مقاله، در بخش ۲ مروری بر روش‌های نهان‌نگاری تطبیقی را خواهیم داشت. در بخش ۳ با استفاده از نظریه بازی به بررسی امنیت در نهان‌نگاری تطبیقی محض و ترکیبی پرداخته و در بخش ۴ با استفاده از آنتروپی محلی گراف متناظر تصویر، معیاری برای شناسایی مناطق زبر و مناسب مخفی‌سازی پیام ارائه می‌شود. سپس با استفاده از این معیار، الگوریتم‌های نهان‌نگاری تطبیقی محض و ترکیبی پیشنهادی در بخش‌های ۵ و ۶ ارائه خواهد شد. در بخش ۷ با پیاده‌سازی آن‌ها روی ۵۰۰۰ تصویر طبیعی، به ارزیابی‌شان پرداخته و در بخش ۸ نتیجه‌گیری می‌شود.

۲. مروری بر روش‌های نهان‌نگاری تطبیقی
روش‌های نهان‌نگاری تطبیقی موجود عموماً روش‌های تطبیقی محض هستند. روش تفاضل مقدار پیکسل‌ها[2] (PVD) [۴] و

*رایانامه نویسنده پاسخگو: ma_shamalizade@gmail.com

2- Pixel Value Difference

بهبودیافته آن (IPVD[1]) [۵] در واقع از اولین روش‌های نهان‌نگاری ترکیبی هستند که با استفاده از یک الگوریتم شبه‌تصادفی زوج پیکسل‌هایی از تصویر را برای مخفی‌سازی پیام انتخاب می‌کند و در صورتی که آن‌ها در معیار لبه مورد نظر صدق کنند، پیام را در اختلاف آن‌ها جاسازی می‌کند. الگوریتم تطبیق لبه مبتنی‌بر کم‌ارزش‌ترین بیت (AE-LSB[2]) در ۲۰۰۸ توسط چنگ- هسینگ یانگ[3] و همکارانش ارائه شد [۶]. این روش با تنظیم نحوه جاسازی به‌صورت مطلوب‌تر، ناهمگونی ایجادشده در هیستوگرام روش PVD را برطرف کرد. ولی مشابه IPVD جاسازی پیام را در یک مکان تصادفی از تصویر به پایان می‌رساند که باعث یک ناهمگونی دیگر در هیستوگرام نهانه می‌شود و در مقابل حمله RS[4] دارای ضعف است [۷]. جی‌ملیکی‌نن[5] در ۲۰۰۶ الگوریتم نهان‌نگاری تطبیقی اصلاح‌شده (LSBMR) را ارائه کرد [۸]. این الگوریتم برخلاف روش‌های پیشین که به‌طور مستقل با تک‌تک پیکسل‌های تصویر سروکار دارند، با یک مولد شبه‌تصادفی، یک زوج پیکسل را به‌عنوان واحد جاسازی انتخاب می‌کند. این الگوریتم نرخ تغییر پیکسل‌ها را از ۰٫۵ bpp به ۰٫۳۷۵ bpp کاهش داده است. لیو[6] و همکارانش در ۲۰۱۰ یک الگوریتم تطبیقی بازبینی‌شده مبتنی‌بر لبه[7] (EAMR) را طراحی کردند [۹]. این‌روش لبه‌ها را با محاسبه اختلاف بین پیکسل‌های متوالی جستجو می‌کند. به دلیل ضعف در انتخاب آستانه، لبه‌های زیادی را از دست می‌دهد. در سال ۲۰۱۴، هوانگ[8] و همکاران الگوریتم نهان‌نگاری تطبیقی اصلاح‌شده مبتنی‌بر لبه توسعه‌یافته[9] (I-EAMR) را پیشنهاد دادند [۱۰]. در سال ۲۰۱۶ هیات الدمور[10] و همکارش در [۱۱] نیز یک الگوریتم تطبیقی محض ارائه کردند که در این روش از اختلاف پیکسل‌های گوشه‌ای پنجره‌های ۳×۳ برای شناسایی پنجره‌های لبه استفاده می‌شود.

۳. نظریه بازی و امنیت در نهان‌نگاری تطبیقی

ایده تلفیق نظریه بازی با امنیت نهان‌نگاری اولین بار در سال ۱۹۹۸ توسط اتینگر[11] مطرح شد [۱۲]. او از بازی مجموع صفر برای رقابت بین مخفی‌کننده داده‌ها و هکر استفاده کرد. نظریه بازی، یک چهارچوب ریاضی است که رقابت بین بازیگران راهبردی با اهداف مختلف را مورد بررسی قرار می‌دهد. در نهان‌نگاری تطبیقی، آلیس[12] موقعیت‌هایی را انتخاب کرده و پیام را مخفی‌سازی می‌کند و ایو[13] سعی می‌کند که این موقعیت‌ها را پیش‌بینی کند تا بتواند هرچه بهتر مکان مخفی‌سازی را شناسایی کند. این وضعیت به‌طور طبیعی با استفاده از نظریه بازی، قابل مدل‌بندی است [۱۱-۹].

در [۱۳] برای اولین بار، با استفاده از نظریه بازی نشان داده شد که اگر نهان‌کاو راهبردی باشد، برای نهان‌نگار هیچ وقت مطلوب نیست که به‌طور قطع در موقعیت‌های کم‌تر قابل پیش‌بینی مخفی‌سازی کند. این مطلب با اصل کهرشف در نهان‌نگاری نیز سازگاری دارد [۳]. تجزیه و تحلیل نهان‌نگاری تطبیقی با نظریه بازی در [۱۴] به یک مدل با دو موقعیت مخفی‌سازی محدود شد که در آن ایو هر بار تنها می‌تواند یک موقعیت را بررسی کند. توسعه دیگری از آن مدل در منبع [۱۶-۱۵] به نهان‌نگار این امکان را داد تا بیت‌های متعدد را در یک دنباله با اندازه دلخواه از تصویر پوشانه تغییر دهد، اما حدود محدودیت‌های قدرت نهان‌کاو را حفظ کرد تا او را ملزم کند که تنها بر اساس بررسی همان یک موقعیت تصمیم‌گیری کند. در این مبحث نشان داده می‌شود که اگر آلیس دقیقاً kبیت از دنباله دودویی تصویر پوشانه را تغییر دهد، در این صورت بهترین راهبرد پاسخ ایو را می‌توان تعیین کرد. در مقابل، هر راهبرد که ایو برای جداسازی اشیاء پوشانه و نهانِ ارائه می‌دهد، درصورتی‌که آلیس از راهبرد ترکیبی نهان‌نگاری تطبیقی و تصادف، به‌طور همزمان استفاده کند، یک راهبرد پاسخ بهتری دارد که تابع جمع‌بندی[14] ساده بازده انتخاب راهبرد توسط ایو را کمینه می‌کند. همچنین، فرمول‌هایی برای تعیین راهبردهای مین ماکس[15] و ماکس مین[16] دو بازیگر در حالت‌های مختلف طراحی می‌شود.

۳-۱. نهان‌نگاری و نظریه بازی

همان‌طوری که می‌دانیم در نهان نگاری، آلیس سعی دارد یک پیام را از طریق یک کانال ارتباطی ارسال کند و ایو می‌خواهد کشف کند که آیا اشیاء تصویری موجود در این کانال حاوی پیامی هستند یا خیر. گاهی اوقات مناسب می‌دانیم، طبیعت را به‌عنوان نیرویی که باعث می‌شود متغیرهای تصادفی به تحقق بپیوندند، در نظر بگیریم و باب دریافت‌کننده پیام است. با این وجود، طبیعت و باب در مفهوم نظریه بازی به‌عنوان بازیکن نیستند، زیرا تصادفی در کارشان نیست. فضای رویدادهای این بازی مجموعه

1- Improvement PVD
2- Adaptive Edge LSB
3- Cheng-Hsing Yang
4- Regular Singular
5- J. Mielikainen
6- Lou
7- Edge adaptive LSBMR
8- Huang
9- Improved EAMR
10- Hayat Al-Dmour
11- Etinger
12- Alice
13- Eve
14- Summation
15- Minmax
16- Maxmin

$\Omega = \{0,1\}^N \times \{C,S\}$ است. هر رویدادی شامل دو قسمت است، یک دنباله دودویی $x \in \{0,1\}^N$ و یک حالت نهان‌نگاری $y \in \{C,S\}$، که در آن C تصویر پوشانه و S تصویر نهانه است. دنباله دودویی نشان‌دهنده چیزی است که ایو در کانال ارتباطی مشاهده می‌کند. حالت نهان‌نگاری بیان می‌کند که آیا پیامی در یک پوشانه مخفی شده است یا خیر. در یک بازی تصادفی هیچ‌یک از این دو حالت برای بازیکنان مشخص نیست، تا وقتی که بازیکنان انتخاب‌های خود را انجام دهند. برای تعریف برد و باخت بازی در یک حالت محدود، همانند جهان واقعی، فرض می‌کنیم که بعضی از رویدادها که توسط طبیعت انتخاب می‌شوند، دارای حالت (x,y) ثابت است.

در این بازی، آلیس یک پیام محرمانه به طول k را در یک دنباله دودویی x (پوشانه) با طول N مخفی می‌کند. طبیعت تعیین می‌کند که آیا تصویر ظاهرشده در آن از نوع پوشانه است یا نهانه؟. ایو دنباله ظاهرشده روی کانال را مشاهده کرده و تصمیم‌گیری می‌کند. باب نیز، اگر پیام پنهانی در یک تصویر دریافتی وجود داشته باشد، آن‌ها را استخراج می‌کند. گزینه آلیس (راهبرد محض)، انتخاب یک زیرمجموعه I از $\{0,1,\dots,N-1\}$ با اندازه k است که نشان‌دهنده موقعیت‌هایی است که او پیام‌های رمزشده را با تغییر مقدار دنباله داده‌شده (پوشانه) در هریک از موقعیت‌های I مخفی می‌کند. گزینه ایو (راهبرد محض)، انتخاب یک زیرمجموعه E_S از $\{0,1\}^N$ است،که نشان‌دهنده مجموعه دنباله‌هایی است که او به‌عنوان اشیاء نهانه طبقه‌بندی می‌کند. لذا، اشیاء متعلق به $E_C = \{0,1\}^N \backslash E_S$ به‌عنوان تصویر پوشانه طبقه‌بندی می‌شوند.

همچنین فرض کنید که آلیس راهبرد محضی از $I \subseteq \{0,\dots,N-1\}$ و ایو هم راهبرد محضی از $E_S \subseteq \{0,1\}^N$ را انتخاب کند. از طرفی طبیعت هم یک دنباله دودویی x و حالت نهان‌نگاری yرا انتخاب کند. در این صورت، اگر ایو x را به‌درستی طبقه‌بندی کند، ۱ را برنده می‌شود و چنانچه طبقه‌بندی او غلط باشد، او ۱ را از دست می‌دهد. مطابق جدول (۱) این بازی با مجموع صفر در نظر گرفته می‌شود.

جدول (۱): نتایج بازی برای (آلیس، ایو)

	حالت‌های نهان‌نگاری	
تصمیم ایو برای x	C	S
$x \in E_C$	$(1,-1)$	$(-1,1)$
$x \in E_S$	$(-1,1)$	$(1,-1)$

۲-۳. تصادفی‌سازی و حالت‌های نهان‌نگاری

در این بازی کاملاً تصادفی ما روی دنباله‌های دودویی و حالت‌های نهان‌نگاری، توزیع‌هایی داریم. همچنین در راهبردهای بازیکنان نیز تصادفی‌سازی را داریم. برای توصیف ماهیت تصادفی این بازی، فرض می‌کنیم $X: \Omega \longrightarrow \{0,1\}^N$ متغیری تصادفی باشد که رویدادی یک دنباله دودویی را به خود می‌گیرد و $Y: \Omega \longrightarrow \{C,S\}$ متغیر تصادفی دیگری باشد که رویدادی یک حالت نهان‌نگاری را به خود می‌گیرد. رویداد $Y = S$ وقتی اتفاق می‌افتد که طبیعت حالت نهان‌نگاری را به‌عنوان نهانه انتخاب می‌کند و این رویداد با احتمال p_S اتفاق می‌افتد. لذا می‌توان نوشت: $pr_\Omega[Y = C] \coloneqq p_C = 1 - p_S$. و از دیدگاه ایو، p_S احتمال این است که او یک دنباله نهانه را در کانال ارتباطی مشاهده می‌کند.

مشابه رمزنگاری، یک قرارداد مشترک در نهان‌نگاری هم داریم و آن این است که ایو یک دنباله نهانه را در کانال‌های ارتباطی دقیقا با احتمال ۵۰ ٪ مشاهده می‌کند. توزیع دنباله‌های دودویی به حالت نهان‌نگاری بستگی دارد. اگر $Y = C$ باشد، در این صورت حالت نهان‌نگاری یک پوشانه است و X بر اساس توزیع تصویر پوشانه C است. اگر $Y = S$ باشد آنگاه حالت نهان‌نگاری یک نهانه است و X بر اساس توزیع تصویر نهانه S است. با داشتن این نمادها می‌توانیم برای هر رویدادی مانند $(X = x, Y = y)$، تعریف زیر را داشته باشیم [۱۵]:

$$Pr_\Omega[(x,y)] = Pr_\Omega[Y = y] Pr_\Omega[X = x | Y = y] = \begin{cases} P_C\, Pr_C[X = x] & ,y = C \text{ اگر} \\ P_S Pr_S[X = x] & ,y = S \text{ اگر} \end{cases} \quad (۱)$$

۳-۳. راهبردهای ترکیبی بازیکنان

به خاطر داشته باشید که یک راهبرد ترکیبی، خود توزیع احتمالی روی راهبردهای محض است. در راهبرد ترکیبی، آلیس به‌طور احتمالی می‌تواند در هر زیرمجموعه مفروضی از موقعیت‌ها، با انتخاب توزیع احتمالی روی زیرمجموعه‌های I با اندازه k، از $\{0,\dots,N-1\}$ مخفی‌سازی کند. در شرح راهبرد ترکیبی، برای هر $I \subseteq \{0,\dots,N-1\}$، فرض می‌کنیم که a_I احتمال این باشد که آلیس در هریک از موقعیت‌های مربوط به I مخفی‌سازی کند. اما در مورد ایو، راهبرد ترکیبی عبارت است از توزیع احتمالی روی همه زیرمجموعه‌های $\{0,1\}^N$، با این فرض که راهبرد ترکیبی ایو، احتمال e_S را به هر زیرمجموعه $S \subseteq \{0,1\}^N$نسبت دهد. بنابراین، تابع دیگر $e: \{0,1\}^N \longrightarrow [0,1]$ را به‌صورت زیر تعریف می‌کنیم:

$$e(x) = \sum_{S \subseteq \{0,1\}^N : x \in S} e_S \quad (۲)$$

$e(x)$ کل احتمال این است که ایو دنباله x را به‌عنوان نهانه طبقه‌بندی می‌کند. توجه کنید که این طرح نمایش راهبرد ترکیبی ایو، رابطه (۲)، نیازمند مشخص کردن 2^N عدد حقیقی است، در حالی‌که نمایش متعارفی راهبرد ترکیبی ایو، با استفاده از نماد e_S، نیازمند مشخص کردن 2^{2^N} عدد حقیقی است، لذا ترجیح می‌دهیم که از طرح نمایش فوق، یعنی(۲)، استفاده کنیم.

۳-۴. توزیع تصاویر پوشانه و نهانه

در تصویر پوشانه C، مقادیر متغیر تصادفی X به‌طور مستقل توزیع می‌شوند، به‌طوری‌که:

$$Pr_C[X = x] = \prod_{i=0}^{N-1} Pr_C[X_i = x_i]. \quad (۳)$$

هرچند که بیت‌ها به‌طور یکسان توزیع نمی‌شوند. برای هر i تعریف می‌کنیم:

$$Pr_C[X_i = 1] = f_i \quad (۴)$$

این یعنی ایو با احتمال f_i مشاهده می‌کند که، بیت i برابر ۱ است. بیش‌تر بودن f_i از $\frac{1}{2}$ نشان می‌دهد که تصویر مشاهده‌شده شباهت زیادی با پوشانه دارد و درصورتی‌که بیت i برابر۱ باشد، آن تصویر پوشانه خواهد بود. بنابراین، چنانچه بیت مشاهده‌شده نزدیک صفر باشد، آن تصویر خیلی شبیه به نهانه خواهد بود و درصورتی‌که صفر باشد، نهانه است. لذا می‌توان گفت $\{f_i\}_{i=0}^{N-1}$ یک دنباله افزایشی یکنواخت در بازه $(\frac{1}{2}, 1)$ است. دقت کنید که این فرض بدون از دست دادن کلیت موضوع است. همچنین در اینجا برای راحتی در محاسبات، قرار می‌دهیم:

$$f_i' = 2f_i - 1 \quad (۵)$$

از مقدار f_i' به‌عنوان اندازه و میزان اریبی[1] پیش‌بینی در موقعیت i تعبیر می‌کنیم. بنابر تعریف f_i می‌دانیم که اگر این اریبی در برخی از موقعیت‌ها نزدیک به صفر باشد، مقدار آن موقعیت قابل پیش‌بینی نیست، در حالی‌که اگر این مقدار نزدیک به ۱ باشد، مقدار آن موقعیت قابل پیش‌بینی‌تر خواهد بود. با جمع‌بندی همه این مسائل، توزیع پوشانه به‌صورت زیر قابل‌تعریف است:

$$\begin{aligned} Pr_C[X = x] &= \prod_{x_i=1} f_i \prod_{x_i=0} (1 - f_i) \\ &= \prod_{i=0}^{N-1} (1 - f_i + x_i f_i') \end{aligned} \quad (۶)$$

توزیع تصویر نهانه $\boldsymbol{S}$ به انتخاب راهبرد مخفی‌سازی آلیس بستگی دارد. فرض کنید $I \subseteq \{0, \dots, N-1\}$، و برای هر $x \in \{0,1\}^N$، x_I نشان‌دهنده دنباله دودویی به‌دست‌آمده از x با تغییر بیت‌ها در همه موقعیت‌ها در I باشد. با فرض این‌که برای هر I با احتمال a_I، آلیس بیت‌های x را در همه موقعیت‌های I تغییر می‌دهد، توزیع تصویر نهانه از روی توزیع تصویر پوشانه با تنظیم احتمالی که برای هر x اتفاق می‌افتد، به‌دست می‌آید. به‌طور رسمی‌تر، فرض کنید که آلیس در هر زیرمجموعه $I \subseteq \{0, \dots, N-1\}$ با احتمال a_I، مخفی‌سازی را انجام می‌دهد. در این صورت داریم:

$$\begin{aligned} \Pr_S[X = x] &= \sum_I a_I \Pr_C[X = x_I] \\ &= \sum_I a_I \prod_{i \notin I} \Pr_C[X_i \\ &= x_i]. \prod_{i \in I} \Pr_C[[X_i \\ &= 1 - x_i] \\ &= \sum_I a_I \prod_{i \notin I} (1 - f_i \\ &+ x_i f_i'). \prod_{i \in I} (f_i - x_i f_i') \end{aligned} \quad (۷)$$

۳-۵. بازده بازی بازیکنان

در بازی کامل، بازده بازی مورد انتظار برای ایو را می‌توان به‌صورت زیر نوشت:

$$\begin{aligned} E[Eve] &= Pr_\Omega[X \in E_S \text{ and } Y = S\ ] \\ &\text{(True positive)} \\ &+ Pr_\Omega[X \in E_C \text{ and } Y = C\ ] \\ &\text{(True negative)} \\ &- Pr_\Omega[X \in E_S \text{ and } Y = C\ ] \\ &\text{(False positive)} \\ &- Pr_\Omega[X \in E_C \text{ and } Y = S] \\ &\text{(False negative} \end{aligned} \quad (۸)$$

و این را می‌توان علاوه‌بر این به‌صورت زیر نیز محاسبه کرد:

$$\begin{aligned} &E[Eve] = ps\ Pr_S[X \in E_S] + pc\ Pr_C[X \in \\ &E_C] - pc\ Pr_C[X \in E_S] - ps\ Pr_S[X \in E_C] = \\ &\sum_{x \in \{0,1\}^N} \big[e(x)\ ps\ Pr_{S(a)}[X = x] + \\ &\big(1 - e(x)\big)\ pc\ Pr_C[X = x] - \big(1 - \\ &e(x)\big)\ ps\ Pr_{S(a)}[X = x] - e(x)\ pcPr_C[X = \\ &x]\ \big] \\ &= \sum_{x \in \{0,1\}^N} (2e(x) - 1)\big(ps.Pr_{S(a)}[X = x] - \\ &pc.Pr_C[X = x]\big). \end{aligned} \quad (۹)$$

عبارت‌های $Pr_C[X = x]$ و $Pr_{S(a)}[X = x]$ به ترتیب در معادلات (۶) و (۷) تعریف شدند. توجه داشته باشید که با نوشتن $S = S(a)$ این مسئله روشن می‌شود که توزیع S به راهبرد ترکیبی آلیس وابسته است. به‌طور خلاصه، بازده بازی ایو عبارت است از احتمال این‌که طبقه‌بندی او درست باشد منهای احتمال این‌که، این کار نادرست باشد. و این بازی به‌صورت یک

1 bias

بازی با مجموع صفر است، به‌طوری‌که بازده بازی آلیس دقیقاً قرینه بازده بازی ایو است.

۳-۶. بهترین پاسخ بازیکنان

با فرض یک راهبرد ثابت e برای ایو، هدف آلیس این است که بازده بازی ایو در رابطه (۹) را به حداقل برساند. هرچند، از آنجایی که او بر توزیع تصویر پوشانه C هیچ کنترلی ندارد، اما هدف می‌تواند به‌صورت کمینه‌سازی عبارت زیر باشد:

$$\sum_{x\in\{0,1\}^N}(2e(x)-1).ps.Pr_{S(a)}[X=x].$$

$$=ps\sum_{x\in\{0,1\}^N}(2\,e(x)-1).\sum_{I\subseteq\{0,1,\dots,N-1\}}a_I.Pr_C[X=x_I] \qquad (۱۰)$$

$$=ps\sum_{I\subseteq\{0,1,\dots,N-1\}}a_I.\sum_{x\in\{0,1\}^N}(2\,e(x)-1).Pr_C[X=x_I]$$

این فرمول برحسب متغیرهای انتخاب آلیس به‌صورت خطی است. بنابراین، او می‌تواند با قرار دادن احتمالات همه عناصرش با کمترین مقدار، آن را مینیمم‌سازی کند. بنابراین، بهترین پاسخ برای آلیس این است که یک بازی با راهبرد محض I بازی کند که رابطه زیر را به حداقل می‌رساند:

$$\sum_{x\in\{0,1\}^N}(2e(x)-1).Pr_C[X=x_I]. \qquad (۱۱)$$

البته، چندین I مختلف می‌توانند به‌طور هم‌زمان این مجموع را به حداقل برسانند. در این حالت، بهترین فضای راهبرد پاسخ آلیس می‌تواند شامل یک راهبرد ترکیبی باشد که احتمالات تصادفی مخفی‌سازی او را در I نشان می‌دهد.

راهبردهای مینی‌ماکس در یک بازی دو نفره، یک راهبرد ترکیبی از یک بازیکن است که بازده او را به حداکثر می‌رساند با فرض این‌که بازیکن رقیب با یک راهبرد محض مطلوب پاسخ خواهد داد، راهبرد ماکس‌مین ایو به‌صورت زیر خواهد بود:

$$\max_{e}\left\{\min_{I}\left(\sum_{x\in\{0,1\}^N}(2e(x)-1)(p_s.Pr_C[X=x_I]-p_C.Pr_C[X=x])\right)\right\} \qquad (۱۲)$$

درحالی‌که راهبرد مینی‌ماکس آلیس عبارت است از:

$$\min_{a}\left\{\max_{E_S}\left(\sum_{x\in E_S}(p_s.Pr_{S(a)}[X=x]-p_S.Pr_{S(a)}[X=x]\right)+\sum_{x\in E_S}(p_C.Pr_C[X=x]-p_S.Pr_{S(a)}[X=x])\right\} \qquad (۱۳)$$

هر راهبرد مینی‌ماکس می‌تواند (به‌صورت بازگشتی) به‌عنوان راه‌حلی برای یک برنامه خطی که در بردارنده ماتریس بازده راهبردهای محض آلیس و ایو است، تعیین شود. متأسفانه، فضای راهبرد محض ایو دارای اندازه 2^{2^N} است. بنابراین، از لحاظ محاسباتی برای پیدا کردن راهبرد مینی‌ماکس و ماکس‌مین با استفاده از این روش حتی برای N کوچک مثلاً ۵ آسان نیست. لذا با توجه به این واقعیت و با توجه به روابط (۹) تا (۱۲) می‌توان نتیجه گرفت که نهان‌نگاری تطبیقی اگر با تصادف همراه باشد مطمئناً از احتمال تشخیص کم‌تری نسبت به نهان‌نگاری تطبیقی محض خواهد بود.

۴. طراحی یک الگوریتم‌نهان‌نگاری تطبیقی محض

همان‌طوری که می‌دانیم، منظور از الگوریتم نهان‌نگاری تطبیقی محض، الگوریتمی با یک معیار تطبیق است که زبرترین مناطق تصویر را توسط آن معیار شناسایی کرده و به مخفی‌سازی پیام در آن‌ها می‌پردازد. در این قسمت با استفاده از معیار شناسایی‌کننده مناطق زبر تصویر که در مرجع [۱۷و ۱۸] ارائه شد، و عملگر ***xor*** یک الگوریتم نهان‌نگاری تطبیقی محض طراحی می‌شود. لذا به‌طور خلاصه مفاهیم اولیه طراحی این الگوریتم را تشریح کرده سپس به طراحی آن اقدام می کنیم.

معیارهای مختلفی برای شناسایی مناطق زبر نسبت به نواحی صاف تصویر وجود دارد. یکی از این معیارها، آنتروپی است. آنتروپی، کاربرد زیادی در زمینه‌های مختلف پردازش تصویر، به‌خصوص نهان‌نگاری و نهان‌کاوی دارد. آنتروپی شانون در حالت کلی مفاهیمی نظیر میانگین اطلاعات موجود و عدم قطعیت را برآورد می‌کند. یکی از تعاریفی که برای آنتروپی تصویر $\mathrm{I}=[\mathrm{I}_{ij}]^{w\times h}$ وجود دارد و بر اساس تعریف کلی آنتروپی شانون است، به‌صورت $H(I)=-\sum_{i=0}^{255}\frac{f_I(i)}{N}\log\frac{f_I(i)}{N}$ است در این تعریف $N=w\times h$ و $f_I(i)$ فرکانس (تکرار) شدت روشنایی $i=0,1,2,\dots,255$ است [۱۷]. همان‌طور که می‌دانید، این تعریف تصاویر صاف و همواری را که از تغییرات کمتری برخوردارند، با آنتروپی کم‌تر و تصاویر ناهموار با تغییرات بیش‌تر را با آنتروپی بیش‌تر شناسایی می‌کند. در ضمن، به دلیل استفاده این تعریف از فرکانس شدت روشنایی پیکسل‌ها، برای ارزیابی ناهمواری یک تصویر کامل مناسب است. لذا تعریف دیگری برای آنتروپی محلی تصویر در مرجع [۱۸] بیان شده است که به‌جای استفاده از فرکانس، از شدت روشنایی تک‌تک پیکسل‌های آن استفاده می‌کند. که معیار شناسایی نواحی صاف از زبر در بسیاری از مراجع پردازش تصویر است. این معیار برای یک پنجره $M\times N$ تصویر به‌صورت زیر تعریف می‌شود:

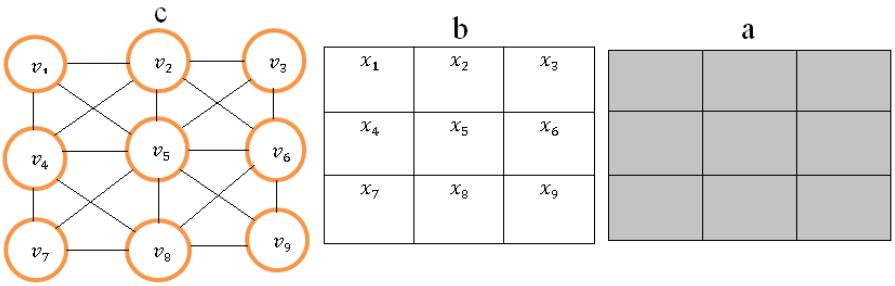
$$H_1^*(\mathrm{W}) = -\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} q_{ij}\, Log\, q_{ij}}{\sigma_w} \quad (۱۴)$$

$$q_{ij} = \frac{I_{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{N} I_{ij}} \quad (۱۵)$$

که در آن، I_{ij} شدت روشنایی پیکسل (i,j)، q_{ij} توزیع احتمال شدت روشنایی I_{ij}، σ_W واریانس پیکسل های پنجره W، H آنتروپی پنجره W از تصویر است [۱۸]. این تعریف آنتروپی، نشان‌دهنده میزان تفرق و پراکندگی شدت روشنایی پیکسل‌های تصویر است. مطابق این تعریف، با توجه به این‌که بیشینه (۱) زمانی اتفاق می‌افتد که $q_{xy} = q_{x'y'}$، لذا، برخلاف روش مبتنی‌بر تعریف شانون، این نشان می‌دهد، تصاویری که شدت روشنایی یکنواخت‌تری (صاف‌تر) دارند، آنتروپی بیش‌تر و در مقابل تصاویری که تغییرات شدت روشنایی آن‌ها زیاد و شدیدتر باشد، دارای آنتروپی کم‌تری هستند.

یعنی مقدار عددی بزرگ‌تر آنتروپی نشان‌دهنده نوسانات و تغییرات کم‌تر و مقادیر عددی کم‌تر، گواه تغییرات و تغییرات بیش‌تر در تصویر خواهد بود. این مطلب نشان می‌دهد که آنتروپی می‌تواند ملاک و معیار مناسبی برای شناسایی مناطق زبر و پرنوسان از تصاویر صاف و هموار باشد.

از آنجایی‌که تعریف فوق شدت روشنایی پیکسل‌های مجاور را در محاسبه معیار زبری هر پنجره تاثیر نداده است، لذا مرجع در مرجع [۱۸] معیار دیگری مبتنی‌بر آنتروپی گراف متناظر هر پنجره به‌صورت زیر طراحی گردیده است. در این تعریف، ابتدا یک پنجره ۳×۳ از تصویر را در یک گراف می‌نگاریم. همچنین، رابطه مجاورت پیکسل‌ها در تصویر نیز به‌طور مشابه به‌صورت ۸- همسایگی در گراف نگاشته می‌شود. شکل (۱) را ببینید. در این تناظر یک‌به‌یک بین یک پنجره از تصویر و یک گراف بدون جهت، متناظر پیکسل‌های p_i و p_j در تصویر، رئوس v_i و v_j در گراف را داریم. برای دو رأس v_i و v_j در گراف، یک یال (i,j) را داریم که رابط دو رأس است [۱۹]. اگر به هر یال این گراف یک عدد مانند $|v_i - v_j|$ اختصاص داده شود، گراف وزن‌دار خواهد شد.



شکل(۱): (a) یک پنجره ۳×۳ از یک تصویر (b) همان پنجره با شدت روشنایی پیکسل‌ها (c) گراف متناظر ۸- همسایگی

حال برای هر j,i که $i \neq j$ و v_i مجاور v_j معیار زبری برای پنجره W به‌صورت زیر تعریف می شود:

$$H_2(W) = -\sum_{(v_i,v_j)} \frac{|v_i - v_j|}{\sum_{(v_i,v_j)}|v_i - v_j|} \log \frac{|v_i - v_j|}{\sum_{(v_i,v_j)}|v_i - v_j|} \quad (۱۶)$$

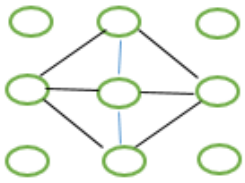
این بدین معنی است که درواقع متناظر هر پنجره ۳×۳ در تصویر، یک گراف وزن‌دار موجود است که در آن وزن یال (i,j) برابر $|v_i - v_j|$ است، که آنتروپی متناظر آن رأس در پنجره موردنظر (D) مطابق فرمول (۲۱) قابل محاسبه است. حال با محاسبه انحراف معیار به‌صورت:

$$\sigma_v^* = Stdev(\{|v_i - v_j|, \forall\, i \neq j\})$$

فرمول (۱۹) را بر انحراف معیار تقسیم می‌کنیم. یعنی:

$$H_2^*(W) = \frac{H_2(D)}{\sigma_v^*} \quad (۱۷)$$

برای انتخاب پیکسل‌های مناسب جاسازی، آنتروپی گراف متناظر آن را $H_2^*[\mathrm{i}]$ که v_i رأس میانی هر پنجره است) بدون در نظر گرفتن چهار پیکسل گوشه‌ای، مطابق شکل (۲) و فرمول (۲۰) محاسبه می‌کنیم. علت شرکت ندادن چهار پیکسل گوشه‌ای هر پنجره، در محاسبات این است که می‌خواهیم پیکسل‌های انتخابی در پوشانه، برای جاسازی و پیکسل‌های انتخابی در نهانه، برای استخراج پیام جاسازی‌شده، یکسان گردد.



شکل (۲): گراف در نظر گرفته‌شده برای تعیین پیکسل‌های مناسب جاسازی

در این محاسبه، مقادیر صفر را که نشان‌دهنده پنجره‌های صاف هستند، حذف کرده و بقیه را تا k رقم اعشار گرد نموده، در آرایه $H_2^*[\mathrm{i}];\ \mathrm{i}=1,2,\dots,\mathrm{l}$ ذخیره می‌کنیم. نکته قابل توجه این است که با توجه به مبحث قبل، پنجره‌های زبرتر دارای آنتروپی محلی کم‌تری هستند، که هنگام جاسازی پیام باید در اولویت قرار گیرند. لذا برای جاسازی پیام M با طول $|M|$ لازم است آستانه‌ای $T>0$ را طوری به‌دست آوریم که تعداد پنجره‌های زبر شمارش‌شده در سراسر تصویر، به‌ازای آن مقدار T یعنی N_W، ظرفیت جاسازی پیامی با طول $|M|$ را داشته باشد. لذا قرار می دهیم:

$$T=H_2^*[p]=arg.\min_{H_2^*[i]}\{|\{H_2^*[i];H_2^*[i]\leq H_2^*[p]\}|\geq\frac{|M|}{K}\} \quad (۱۸)$$

سیستم بینایی انسان نسبت به تغییرات در نواحی لبه‌دار و نویزدار، معروف به نواحی زبر، در مقایسه با نواحی نرم و صاف حساسیت کم‌تری دارد. از طرفی می‌دانیم که، LSB پیکسل‌های این نواحی از یک روند تصادفی برخوردارند. با استفاده از نظریه بازی‌ها در بخش نخست نشان داده شد که نهان‌نگاری تطبیقی همراه با یک روند شبه‌تصادفی از امنیت بیش‌تری نسبت به نهان‌نگاری تطبیقی محض برخوردار است. بنابراین، در ادامه با استفاده از معیار تشخیص زبری ارائه‌شده در بخش قبل و مخفی‌سازی پیام توسط عملگر xor، دو الگوریتم نهان‌نگاری تطبیقی محض و ترکیبی طراحی‌شده، سپس مورد ارزیابی امنیتی قرار می‌گیرند.

۴-۱. الگوریتم مخفی‌سازی پیام

ورودی‌ها: تصویر پوششی C با ابعاد $h\times w$ و پیام محرمانه M.

خروجی‌ها: تصویر نهانه S با ابعاد $h\times w$ و آستانه استخراج پیام از آن یعنی T.

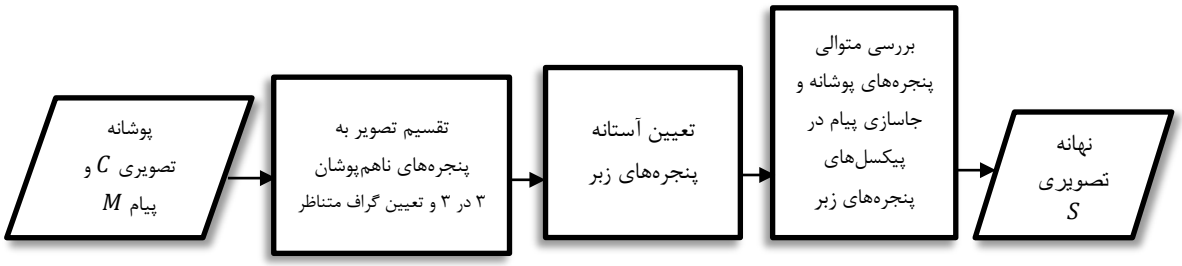
گام ۱. تقسیم پوشانه تصویری به پنجره‌های ۳×۳ ناهم‌پوشان.

گام ۲. محاسبه آنتروپی محلی پنجره‌های ۳×۳ و خذف مقادیر صفر که نشان‌دهنده پنجره‌های صاف هستند سپس بقیه را تا k رقم اعشار گرد نموده، در آرایه $H_2^*[\mathrm{i}];\ \mathrm{i}=1,2,\dots,\mathrm{l}$ ذخیره می‌کنیم.

گام ۳. محاسبه آستانه زبری پنجره‌های تصویر:
با توجه به این‌که مقادیر کم‌تر آرایه $H_2^*[i]$ آن نشان‌دهنده پنجره‌های زبرتر است، با توجه به طول پیام M، آستانه زبری $0<T\leq H_2^*[p]$ را مطابق (۱۸) طوری انتخاب می‌کنیم که $k\times N_W\geq|M|$ باشد (اینجا $k=4$). طوری که تا حد امکان پیام در سراسر تصویر جاسازی شود.

گام ۴. از گوشه چپ بالای تصویر، گراف متناظر هر پنجره ناهم‌پوشان را مطابق شکل (۲) در نظر گرفته، آنتروپی آن H_2^* را حساب کرده، چنانچه $H_2^*\leq T$ باشد، مخفی‌سازی سه بیت پیام m_3,m_2,m_1 را در چهار پیکسل گوشه‌ای پنجره موردنظر طبق دستور *Xor Coding* [۱۱] انجام بده.

گام ۵: آستانه شناسایی پنجره‌های زبر یعنی T و طول پیام جاسازی‌شده یعنی $|M|$ را در مکان خاصی از نهانه جاسازی کرده یا از طریق کانال امن به مقصد ارسال می‌کنیم (شکل ۳).



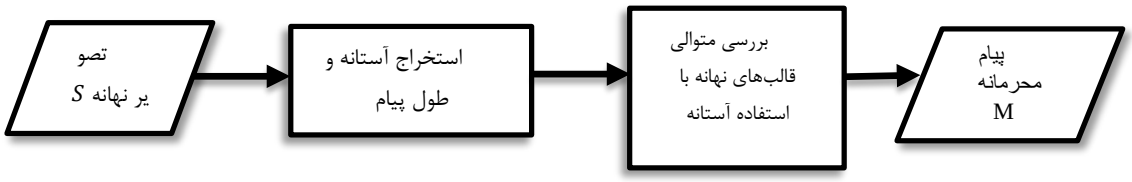
شکل(۳): فرایند مخفی‌سازی پیام در یک پوشانه تصویری طبق الگوریتم نهان‌نگاری تطبیقی محض

۴- ۲. الگوریتم استخراج پیام

شکل(۴) نشان‌دهنده نمودار عملیاتی فرایند استخراج برای یک نهانه تصویری است، که با بازیابی مقدار آستانه آغاز می‌گردد. پنجره‌های زبر تصویر نهانه با استفاده از آستانه زبری T، بازیابی می‌شوند. در ادامه، ۴ پیکسل گوشه‌ای هر پنجره زبر، که آنتروپی گراف متناظر آن مطابق شکل (۲) محاسبه می‌شود، انتخاب گردیده و LSB1 آن‌ها را به ترتیب q_1 ، q_2 ، q_3 و q_4 می‌نامیم و عملیات Xor به‌صورت:

$$\begin{aligned}\mathrm{m}_1&=q_1\oplus q_2\\ \mathrm{m}_2&=q_2\oplus q_3\\ \mathrm{m}_3&=q_1\oplus q_3\end{aligned} \quad (۱۹)$$

جهت بازیابی سه بیت پیام m_1 ، m_2 و m_3 به کار می‌رود.



شکل (۴): فرایند استخراج پیام نهان‌نگاری تطبیقی محض

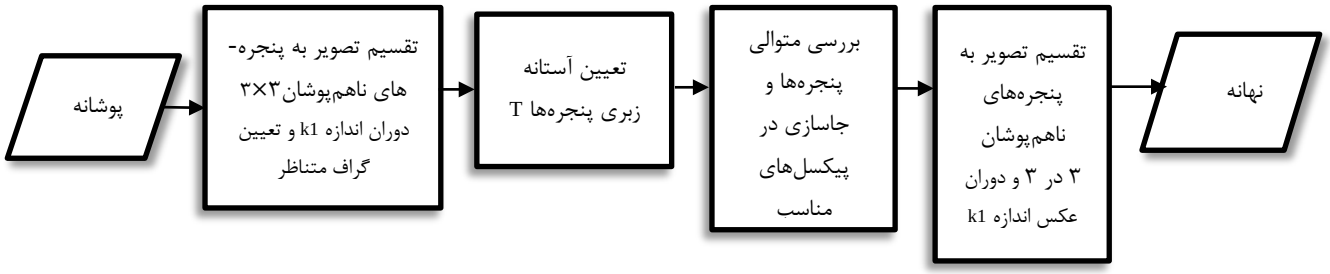
۵. طراحی الگوریتم تطبیقی ترکیبی

منظور از الگوریتم ترکیبی، الگوریتمی تطبیقی همراه با یک روند تصادفی است. لذا در این قسمت با اعمال یک روند تصادفی در الگوریتم تطبیقی محض ارائه‌شده در بخش قبل، به یک الگوریتم نهان‌نگاری تطبیقی تصادفی یا ترکیبی می‌رسیم.

۵-۱. الگوریتم مخفی‌سازی پیام

ورودی‌ها: تصویر پوششی C با ابعاد $h \times w$ و پیام محرمانه M.
خروجی‌ها: تصویر نهانه S با ابعاد $h \times w$ و آستانه استخراج پیام از آن یعنی T.

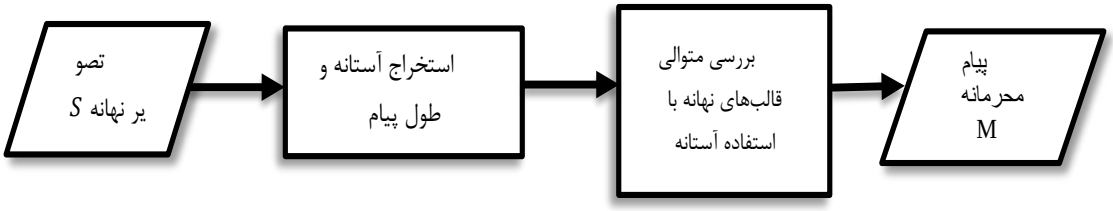
تفاوت این الگوریتم با الگوریتم تطبیقی محض در اعمال تصادفی‌سازی حین مخفی‌سازی پیام و عمل عکس پس از مخفی‌سازی همه بیت‌های پیام است. به این ترتیب که در گام ۱، تصویر را به‌صورت پنجره‌های ناهم‌پوشان ۳×۳ تقسیم کرده، هر پنجره را با کلید محرمانه key1 به یکی از اندازه‌های تصادفی {0، 90، 180، 270} برحسب درجه دوران می‌دهیم و پس از جاسازی پیام، تصویر حاصله را مجدداً به پنجره‌های ناهم‌پوشان ۳×۳ تقسیم کرده و هر یک از آن‌ها را با یک درجه تصادفی {0، 90، 180، 270} بر اساس کلید key1 و در جهت عکس دوران می‌دهیم (شکل ۵).



شکل (۵): فرایند جاسازی پیام طبق الگوریتم نهان‌نگاری ترکیبی

۵- ۲. الگوریتم استخراج پیام

شکل (۶) نشان‌دهنده نمودار عملیاتی فرایند استخراج برای یک نهانه تصویری است، که با بازیابی مقدار آستانه آغاز می‌گردد. پنجره‌های زبر تصویر نهانه با استفاده از آستانه زبری T، بازیابی می‌شوند. در ادامه، ۴ پیکسل گوشه‌ای هر پنجره زبر، که آنتروپی گراف متناظر آن، مطابق شکل (۲) محاسبه می‌شود، انتخاب گردیده و LSB1 آن‌ها را به ترتیب q_1 ، q_2 ، q_3 و q_4 می‌نامیم و عملیات xor طبق (۱۹) جهت بازیابی سه بیت پیام m_1 ، m_2 و m_3 به کار می‌رود.



شکل (۶): فرایند استخراج داده نهان‌نگاری ترکیبی

۶. نتایج تجربی و مقایسه امنیتی دو الگوریتم

برای ارزیابی امنیت پیام جاسازی‌شده توسط الگوریتم‌های نهان‌نگاری از حملات مختلفی استفاده می‌شود. یکی از این روش‌ها، روش استفاده از الگوریتم‌های نهان‌کاوی است. این

الگوریتم‌ها خود به دو دسته معین[1] یا اختصاصی و کور[2] یا جامع تقسیم می‌شوند. دسته اول مختص الگوریتم‌های نهان‌نگاری معین طراحی می‌شوند ولی دسته دوم که معمولاً مبتنی‌بر آماره‌های مراتب بالاتر و استخراج انواع ویژگی‌های آماری هستند. برای تشخیص جاسازی اکثر روش‌های نهان‌نگاری در حوزه مربوطه (مکان یا فرکانس) با الگوریتم نامشخص به‌کار می‌روند. اجرای هر الگوریتم نهان‌کاوی شامل دو مرحله آموزش[3] و آزمون[4] می‌باشد. به این ترتیب که ابتدا بردارهای ویژگی پوشانه‌ها و نهانه‌های موجود توسط یک استخراج‌کننده ویژگی، استخراج‌شده سپس ویژگی‌های استخراج‌شده در مرحله آموزش، به یک طبقه‌بندی‌کننده آموزش داده می‌شود. سرانجام توسط یک طبقه‌بندی‌کننده آموزش‌دیده، در مرحله آزمون به تفکیک پوشانه از نهانه اقدام می‌شود.

برای ارزیابی الگوریتم نهان‌نگاری پیشنهادی، از نرم‌افزار نهان‌کاوی SRM و یک طبقه‌بندی‌کننده[5] استفاده می‌کنیم [۲۰]. چهار رویداد متفاوتی که در هنگام طبقه‌بندی پوشانه‌ها و نهانه‌ها رخ می‌دهند، به یکدیگر وابسته بوده و بر هم تأثیر متقابل دارند. برای فهم بهتر و مقایسه ارزیابی همه‌جانبه عملکرد حمله نهان‌کاوی از یک منحنی مشخصه عملکرد گیرنده[6] معروف به منحنی ROC، که نشان‌دهنده تغییرات نرخ تشخیص مثبت نادرست f_p در مقابل نرخ تشخیص مثبت درست t_p است، استفاده می‌شود [۱ و ۲]. این کار را با استفاده از ۵۰۰۰ تصویر، بر طبق نرخ‌های جاسازی متفاوت، بر اساس سطح زیر منحنی ROC هریک، معروف به AUC در جدول (۴) به نمایش می‌گذاریم. مساحت زیر منحنی ROC یا همان AUC درواقع نشان‌دهنده احتمال تشخیص مثبت درست[7] (P_{detect}) است [۱۱]، که با استفاده از رابطه (۲۵) قابل محاسبه است.

$$p_{detect} = 1 - p_{error} \qquad (۲۰)$$

$$p_{error} = \frac{1}{2} \times P_{FP} + \frac{1}{2} \times p_{FN} \qquad (۲۱)$$

که در آن، P_{FP} و P_{FN} به‌ترتیب برابر احتمال تشخیص مثبت نادرست و احتمال تشخیص منفی نادرست است. مقدار $p_{detect} = 0.5$ نشان می‌دهد که تشخیص طبقه‌بندی‌کننده در شناسایی نهانه از پوشانه معادل یک روند تصادفی است. به عبارتی نشان‌دهنده امنیت کامل الگوریتم نهان‌نگاری است. در مقابل $p_{detect} = 1$ نیز نشان‌دهنده این است که طبقه‌بندی‌کننده دارای دقت کامل است و الگوریتم نهان‌نگاری هیچ‌گونه امنیتی ندارد. احتمال تشخیص درست P_{detect} یا AUC حاصل از ارزیابی الگوریتم پیشنهادی و دو الگوریتم دیگر توسط الگوریتم نهان‌کاوی SRM در جدول (۴) به نمایش گذاشته شده است.

جدول(۴): مقایسه احتمال تشخیص صحت p_{detect} یا AUC

نرخ جاسازی(٪)	EAMR	Edge xor Coding	الگوریتم محض	الگوریتم ترکیبی
۵	۰٫۵۴۲۱	۰٫۵۳۴۴	۰٫۵۲۷۸	۰٫۵۱۰۶
۱۰	۰٫۵۷۶۱	۰٫۵۶۶۲	۰٫۵۵۹۵	۰٫۵۴۱۱
۱۵	۰٫۶۰۳۲	۰٫۵۹۴۶	۰٫۵۸۸۷	۰٫۵۷۰۸
۲۰	۰٫۶۳۲۸	۰٫۶۱۴۴	۰٫۵۹۶۸	۰٫۵۸۱۰
۳۰	۰٫۶۶۲۹	۰٫۶۲۴۰	۰٫۶۲۹۳	۰٫۶۱۰۵

۷. نتیجه‌گیری

در این مقاله، نهان‌نگاری تطبیقی محض و ترکیبی معرفی گردید. سپس با استفاده نظریه بازی‌ها، راهبردهای یک نهان‌نگار تطبیقی و یک نهان‌کاو راهبردی مدل‌بندی گردیده و به‌صورت نظری نشان داده شد که امنیت الگوریتم تطبیقی ترکیبی از الگوریتم تطبیقی محض بیش‌تر است.

همان‌طوری که انتظار می‌رفت، ارزیابی الگوریتم‌های تطبیقی محض و ترکیبی طراحی‌شده برای ۵۰۰۰ تصویر طبیعی، با استفاده از الگوریتم نهان‌نکاوی SRM نشان می‌دهد، در نرخ‌های جاسازی متفاوت از ۵٪ تا ۳۰٪، امنیت روش ترکیبی بین ۱ تا ۲ درصد بالاتر از روش محض است. ضعف عمده روش‌های نهان‌نگاری تطبیقی محض، بنابر اصل کهرشف، در آشکار بودن الگوریتم مخفی‌سازی و تطبیق برای همگان است و برتری روش‌های ترکیبی، به دلیل برخورداری از یک روند شبه‌تصادفی در حین مخفی‌سازی پیام می‌باشد. در مطالعات آینده می‌توان با طراحی الگوریتم‌های نهان‌نگاری تطبیقی ترکیبی با حالت شبه‌تصادفی بیش‌تر در حوزه مکان و فرکانس، امنیت پیام‌های مخفی‌شده در نهان‌نگاری تطبیقی تصویر را افزایش داد.

۸. مراجع

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T.Kalker, “Digital Watermarking and Steganography,” Second edn. Morgan Kaufmann, Burlington, 2007.

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

1 Targeted
2 Blind or Universal
3 Training
4 Test
5 Ensemble Classifier
6 Receiver Operating Characteristic Curve
7 Detection accuracy

[3] F. Cayre,, P. Bas, "Kerckhoffs–based embedding security classes for WOA data hiding", IEEE Transactions on Information Forensics and Security 3, pp. 1–15, 2008.

[4] D.C. Wu, and W.H. Tsai, "A Steganographic Method for Images by Pixelvalue Differencing"; Pattern Recognition Letters, 24, pp. 1613–1626, 2003.

[5] X. Zhang, S. Wang, "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security"; Pattern Recogn. Lett., vol. 25, no. 3, pp. 331–339, 2004.

[6] C-H. Yang, C-Y. Weng, S-J. Wang, and H-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, 2008.

[7] L. Bin, He. Junhui, H. Jiwu, and Q. S. Yun, "A Survey on Image Steganography and Steganalysis," Ubiquitous International Journal of Information Hiding and Multimedia Signal Processing, vol. 2, pp. 2073-4212, 2011.

[8] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

[9] W. Luo, F. Huang, and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 201–214, 2010.

[10] F. Huang, Y. Zhong, and J.Huang, "Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm," Springer-Verlag Berlin Heidelberg, pp. 19–31, 2014.

[11] H. Al-Dmour and A. Al-Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding". Elsevier; Sience direct, vol. 46, pp. 293-306, 2016.

[12] M. Ettinger, "Steganalysis and game equilibria," In Aucsmith, D., ed.: Information Hiding, vol. 1525 of Lecture Notes in Computer Science, pp. 319– 328, 1998.

[13] S. Pascal, L. Aron, J. Benjamin, G. Jens, and B. Rainer, "A game-theoretic analysis of content-adaptive steganography with independent embedding," In EUSIPCO. IEEE, 2013.

[14] S. Pascal and B. Rainer, "A game-theoretic approach to content-adaptive steganography," In: Ghosal, D., Kirchner, M. (eds.) Information Hiding. LNCS, 2012.

[15] J. Benjamin, S. Pascal, and B. Rainer, " Where to hide the bits?," In GameSec, vol. 7638 of LNCS, pp. 1–17, 2012.

[16] T. Mekala and N. Mahendran, "Improved Security in Adaptive Steganography Using Game Theory," vol.118, no. 8, pp. 111-116, 2018.

[17] T. Pun, "A new method for gray-level picture thresholding using the entropy of the histogram," Signal Processing, vol. 2, pp. 223-237, 1980.

[18] GU. Guanghua, Yao Zhao, and Zhu Zhenfeng, "Integrated Image Representation Based Natural Scene Classification," Elsevier, Expert Systems with Applications, vol. 38, pp. 11273–11279, 2011.

[19] M. A. Shamalizadeh Baei, & et.al., "Designing an Image Steganography Algorithm Based on Entropy and ELSB2," Advanced Defence Sci. & Tech., vol. 2, pp. 39-50, 2018. (In Persian)

[20] http://dde.binghamton.edu/download/feature_extractors/

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

Designing a combinatorial Image Steganography Algorithm Based on Game Theory

M. A. Shamalizadeh Baei

* Imam Hossein's Officer University, Imam Khamenei University Complex, Gilan, Iran

(Received: 30/12/2018, Accepted: 18/06/2019)

ABSTRACT

Adaptive steganography methods using an adaptive criterion, sequentially or randomly, hide a message in an image. The aim of security is to reduce the probability of detecting the existence of a message. In this article, first by using game theory it is illustrated that adaptive steganography algorithms with a simulation along with a quasi-random process, named as combinatorial image steganography algorithms have higher security compared to the pure adaptive steganography algorithms. Then, this matter is shown practically by designing patterns based on entropy and the operator for 5000 natural images. The comparison of two designed algorithms, using SRM which is one of the most famous steganography algorithms, shows about 1.5% security superiority of the combinatory method compared to the purely adaptive method.

Keywords: Pure Adaptive steganography, Combinatory steganography, Security, Game Theory

* Corresponding Author Email: ma.shamalizade@gmail.com