Encyclopedia of Digital Transformation
Vol. 2; No. 3; PP. 46 - 59
Fall 2021
DOI: 10.22034/dtj.2023.326988.1045

Institute of Higher Education
Mehr Alborz

Modeling Steganography and Steganalysis Strategies in Digital Images using Game Theory

Mohammad Ali Shamalizade Baei [1], Alireza Shabani [2]

Abstract

Steganography is the science and art of hiding a message in images to secure the business or military information, sent from one source to another.steganographer and steganalyst are also two opposing people, each with a strategy that takes into account the strategies of the other. This is especially evident in adaptive steganography. This paper models and analysis the strategies of two players from the point of view of game theory, considering a two-player zero-sum game between a steganographer and steganalyzer In this game, Alice (the steganographer) wants to hide a secret message of length k in a binary sequence (cover image) and Eve (steganalyzer) wants to find out, Is there a secret message in the images being transmitted on the intended communication channel? In this model, without considering the limit for Eve's detection power, each player's Min-Max strategies are presented, along with the necessary structural constraints to compute game's equilibrium, and at the end, it is shown that, the optimal strategy for Alice, while hiding message, is random adaptive.

Keywords: *Steganography, Steganalysis, Modeling, Game Theory, Optimal Strategies.*

1. Assistant Professor, Faculty of Engineering, Imam Hossein University of Officer Training and Guard Training (AS)
2. Assistant Professor of Mathematics, Imam Khomeini University of Marine Sciences

Submitted: 31-01-2022
Accepted: 09-08-2022
Corresponding Author: Mohammad Ali Shamalizade Baei
Email: ma.shamalizade@ihu.ac.ir

دانشنامهٔ تحول دیجیتال

مؤسسه آموزش عالی مهرالبرز

دورهٔ ۲، شمارهٔ ۳

پاییز ۱۴۰۰

صص. ۴۶ - ۵۹

Encyclopedia of Digital Transformation

DOI: 10.22034/dtj.2023.326988.1045

مدل‌بندی راهبردهای نهان‌نگاری و نهان‌کاوی اطلاعات در تصاویر دیجیتال با استفاده از نظریه‌ی بازی‌ها

محمدعلی شمع علیزاده بایی[۱]، علیرضا شعبانی[۲]

چکیده

نهان‌نگاری، علم و هنر مخفی سازی پیام در تصاویر، جهت حفظ امنیت اطلاعات تجاری یا نظامی ارسالی، از یک مبدأ به یک مقصد است. روش‌های نهان‌نگاری تطبیقی برای مخفی سازی پیام به متن پوشانه‌های تصویری توجه ویژه‌ای دارند و با در نظر گرفتن شرایطی در متن تصویر نهانه به مخفی سازی پیام می‌پردازند. نهان‌نگار و نهان‌کاو دو فرد معارض هم هستند که راهبرد هر یک با در نظر گرفتن راهبردهای طرف مقابل تعیین می‌شود. این موضوع بخصوص در نهان‌نگاری تطبیقی آشکارتر است. این مقاله، با در نظر گرفتن یک بازی دونفره با مجموع صفر بین یک نهان‌نگار و نهان‌کاو، به مدل‌بندی و تجزیه‌وتحلیل راهبردهای دو بازیکن از دیدگاه نظریه‌ی بازی می‌پردازد. در این بازی آلیس (نهان‌نگار) می‌خواهد یک پیام محرمانه به طول k را در یک دنباله دودویی (پوشانه تصویری) مخفی کند و ایو (نهان‌کاو) می‌خواهد تشخیص دهد که آیا پیام محرمانه‌ای در تصاویر در حال انتقال در کانال ارتباطی موردنظر وجود دارد؟ در این مدل بدون در نظر گرفتن محدودیتی برای قدرت تشخیص ایو، راهبردهای مین ماکس هر بازیکن، همراه با محدودیت‌های ساختاری لازم برای موازنه بازی ارائه‌شده و در پایان نشان داده می‌شود که راهبرد بهینه برای آلیس راهبرد تطبیقی تصادفی حین مخفی سازی پیام است.

کلمات کلیدی: *نهان‌نگاری، نهان‌کاوی، مدل‌بندی، نظریه‌ی بازی‌ها، راهبردهای بهینه.*

---

۱. استادیار دانشکده مهندسی دانشگاه افسری و تربیت پاسداری امام حسین (ع).

۲. استادیار گروه ریاضی دانشگاه علوم دریایی امام خمینی (ره).

تاریخ دریافت مقاله: ۱۴۰۰/۱۱/۱۱

تاریخ پذیرش نهایی مقاله: ۱۴۰۱/۰۵/۱۸

نویسندهٔ مسئول مقاله: محمدعلی شمع علیزاده بایی

Email: ma.shamalizade@ihu.ac.ir

مقدمه

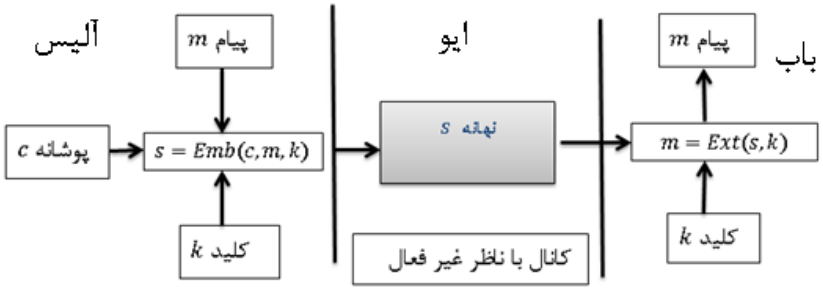
نهان‌نگاری[1] علم و هنر ارتباطات مخفی است؛ برعکس رمزنگاری که هدف از آن ارتباطات امن در مقابل استراق سمع است، روش‌های نهان‌نگاری سعی دارند که تا حد امکان پیام ارسالی را از بیننده مخفی سازند.

یک دستگاه نهان‌نگاری عبارت است از ۵ تایی (X, K, M, Emb, Ext) که در آن:

$$Emb = X \times M \times K \rightarrow X \quad (۱)$$

$$Ext = X \times K \rightarrow M \quad (۲)$$

X مجموعه‌ای از اشیاء تصویری ممکن، معروف به پوشانه[2](تصاویر اصلی) و نهانه[3](تصاویر حاوی پیام مخفی)، K مجموعه‌ی فضای کلید، M مجموعه پیام‌های ممکن m است که می‌توان در پوشانه‌های متفاوت مخفی سازی کرد و $|M|$تعداد این پیام‌های ممکن است (کاکس و همکاران،[4] ۲۰۰۷). همچنین Emb الگوریتم مخفی‌سازی پیام در یک پوشانه و Ext الگوریتم استخراج پیام مخفی‌سازی شده از یک نهانه است. شکل ۱ یک دستگاه نهان‌نگاری با یک ناظر غیرفعال را نشان می‌دهد. ناظر غیرفعال، ناظری است که فقط مشغول نظارت بر ارسال اطلاعات در کانال ارتباطی است و قابلیت تغییر در آن‌ها را ندارد.



شکل ۱: نمودار بلوکی از یک سیستم ارتباطی نهان‌نگاری

همان‌طوری که در شکل ۱ ملاحظه می‌شود، آلیس[5](فرستنده‌ی پیام) با استفاده از یک تابع مخفی سازی Emb پیام m، کلید kو پوشانه تصویری c را دریافت کرده، نهانه s را تولید می‌کند و از طریق یک کانال ناامن برای باب[6](گیرنده‌ی پیام) ارسال می‌کند. باب در مقصد با در دست داشتن همان کلید k و الگوریتم استخراج پیام Ext، پیام پنهان را آشکار می‌کند. یو[7] که نقش یک دشمن غیرفعال[8]را دارد، همواره ناظر بر این کانال ارتباطی بین آلیس و باب است.

یک مدل‌سازی کلی برای نهان‌نگاری مدرن معمولاً برحسب مسئله زندانی بیان می‌شود که در آن آلیس و باب دو زندانی هستند که می‌خواهند با هم ارتباط برقرار کرده تا نقشه فرار را طرح‌ریزی کنند. بااین‌حال، تمامی ارتباطات بین این دو نفر توسط رئیس زندان، یعنی ایو مورد کنترل قرار می‌گیرد و در صورت کوچک‌ترین شک و تردیدی در مورد ارتباط پنهان‌بین این دو، آن‌ها را در سلول‌های انفرادی حبس خواهند کرد و ارتباطشان قطع خواهد شد. به‌طور خاص، در مدل کلی نهان‌نگاری که در شکل ۱ نشان داده شد، آلیس را داریم که می‌خواهد پیام محرمانه m را برای باب ارسال کند. به‌منظور انجام این کار، آلیس پیام m

1. Steganography
2. Cover Image or Original Image
3. Stego Image
4. Cox et al.
5. Alice
6. Bob
7. Eve
8. Pssive

را در یک رسانه پوششی مانند یک تصویر c پنهان می‌کند و یک نهانه چون s به‌دست می‌آورد؛ سپس این نهانه از طریق کانال عمومی برای باب ارسال می‌شود (کاکس و همکاران، ۲۰۰۷)، (بمه[1] ۲۰۲۰) و (کایر و باس[2] ۲۰۰۸).

در چهارچوب نهان‌نگاری، روش مخفی‌سازی پیام برای ایو ناشناخته است و به‌عنوان یک پیام محرمانه مشترک بین آلیس و باب است. بااین‌حال، معمولاً این‌طور فرض می‌شود که الگوریتم مورد استفاده، محرمانه نیست و تنها کلید مورد استفاده توسط این الگوریتم بین دو طرف محرمانه است. این فرضیه همچنین در رمزنگاری به‌عنوان اصل کهرشف[3] معروف است (کایر و باس، ۲۰۰۸). مثلاً کلید محرمانه می‌تواند به عنوان رمز عبوری باشد که در تولید اعداد شبه تصادفی مورد استفاده قرار می‌گیرد تا محل پیکسل‌ها را در تصویر پوشانه برای مخفی‌سازی پیام محرمانه، انتخاب کند.

ایو یا رئیس زندان هیچ اطلاعی از کلید محرمانه که آلیس و باب در آن سهیم هستند، ندارد؛ ولی از الگوریتمی که ممکن است برای مخفی‌سازی پیام‌ها مورد استفاده قرار دهند، مطلع است. رئیس زندان که در امتحان همه پیام‌های تبادل شده بین آلیس و باب آزاد است، می‌تواند یک ناظر فعال یا غیرفعال باشد. یک رئیس زندان فعال به سادگی به بررسی پیام می‌پردازد و سعی می‌کند بفهمد که این شیء رسانه، حامل پیام مخفی است یا خیر؟ اگر معلوم شود که شیء رسانه موردنظر حامل پیام مخفی است، آن را توقیف می‌کند یا دست به اقدام مناسب می‌زند و یا بدون هرگونه اقدامی اجازه مبادله‌ی پیام را می‌دهد. در این مقاله فرض را بر آن قرار می‌دهیم که ناظر یا ایو غیرفعال است و نهانه را هیچ‌گونه تغییری نمی‌دهد (کایر و باس، ۲۰۰۸).

نهان‌کاوی به مجموعه‌ای از فنون اشاره دارد که به ایو در تشخیص اشیاء پوشانه از نهانه کمک می‌کند. لازم به ذکر است که ایو باید این تمایز و تشخیص را بدون اطلاع از کلید محرمانه‌ای که آلیس و باب باهم مشترک هستند، انجام دهد و گاهی اوقات او باید بدون اطلاع از الگوریتم خاصی که آن‌ها برای مخفی‌سازی پیام محرمانه، استفاده می‌کنند، این کار را انجام دهد. با این‌وجود باز هم باید یادآوری کنیم که لازم نیست ایو چیزی از محتوای پیام محرمانه m جمع‌آوری کند؛ بلکه تنها تشخیص وجود پیام مخفی برای او کافی است.

توسعه فنون نهان‌نگاری و در دسترس بودن گسترده ابزار لازم برای این کار منجر به علاقه فراوان در طراحی الگوریتم‌های نهان‌نگاری پیشرفته شده است. مثلاً در سال‌های اخیر شاهد بسیاری از فنون نهان‌کاوی جدید و پرقدرت هستیم که در مقالات مختلف گزارش‌شده‌اند. بسیاری از این فنون، مخصوص روش‌های مختلف مخفی‌سازی پیام هستند و در واقع نشان داده‌اند که در این زمینه کاملاً مؤثر هستند.

به‌طورکلی روش‌های نهان‌نگاری در یک دسته‌بندی عبارت‌اند از ترتیبی[4] تصادفی[5] و تطبیقی.[6] در روش ترتیبی معمولاً از گوشه چپ بالای پوشانه شروع به مخفی‌سازی پیام می‌شود و ادامه پیدا می‌کند. در روش تصادفی، با استفاده از یک مولد اعداد شبه تصادفی و یک کلید، مکان‌های مخفی‌سازی انتخاب می‌شود و در روش تطبیقی، مکان‌های مخفی‌سازی پیام با دقت و توجه به محتوای متن پوشانه، مثلاً مکان‌های پر اعوجاج و لبه که از تغییر شدت روشنایی بالاتری برخوردار هستند، انجام می‌شود. لازم به یادآوری است که نهان‌نگاری تطبیقی هم در حوزه‌ی مکان و هم در حوزه‌ی تبدیل مطرح است. از آنجایی که محور اصلی این تحقیق، نهان‌نگاری تطبیقی است، در ادامه، سیر تکاملی روش‌های نهان‌نگاری تطبیقی و تحقیقات مرتبط مورد بررسی قرار می‌گیرد.

در مقابل مخفی‌سازی یکنواخت تصادفی که در آن نهان‌نگار مکان‌های مخفی‌سازی پیام خود را به صورت شبه تصادفی انتخاب می‌کند، نهان‌نگاری تطبیقی وجود دارد. نهان‌نگاری تطبیقی این حقیقت را برمی‌انگیزد که قسمت‌های مختلف پوشانه ممکن است که دارای سطوح مختلف پیش‌بینی باشند. همه طرح‌های مخفی سازی تطبیقی دارای موارد مشترکی هستند که همه آن‌ها در تلاش‌اند که مکان‌های مخفی‌سازی با احتمال پیش‌بینی کمتر را شناسایی کنند. این طرح‌ها ممکن است دو معیار

1. Bhme
2. Cayre and Bas
3. Kerchoff
4. Sequential
5. Random
6. Adaptive

پیچیده‌گی محلی و به حداقل رسانی تخریب را مدنظر قرار دهند. برای مثال، تصاویر دیجیتالی اغلب دارای مناطقی هستند که دارای رنگ همگن هستند که هرگونه اصلاح اندک در آن‌ها مورد توجه قرار می‌گیرد، درحالی‌که مناطق دیگر دارای رنگ ناهمگن هستند، به‌طوری‌که تغییرات دقیق در حد چند پیکسل هم طبیعی به نظر می‌رسد. نتیجه این می‌شود که اگر یک نهان‌نگار بخواهد پیکسل‌های تصویر را اصلاح کند تا پیامی را مبادله کند، او باید ترجیح دهد که در این مناطق ناهمگن مخفی‌سازی کند (عبدالرئوف[1] ۲۰۲۱)، (بائی و همکاران[2] ۲۰۱۸)، (بائی، ۲۰۲۰)، (فردریچ و گلیجان[3] ۲۰۰۴) و (دوان و گوپتا[4] ۲۰۲۱).

در مدل رقابتی بین نهان‌نگار و نهان‌کاو در این مقاله، یک متغیر تصادفی برای دنباله‌های دودویی متناظر پوشانه و نهانه در نظر گرفته و مفهوم تطبیقی را در آن خلاصه می‌کنیم، در این صورت هر موقعیت در این دنباله دارای سطح متفاوتی از قابلیت پیش‌بینی است. قابلیت پیش‌بینی هر موقعیت، هم توسط آلیس به‌عنوان یک نهان‌نگار تطبیقی و هم توسط ایو به‌عنوان یک نهان‌کاو نامحدود، قابل محاسبه است. در ادامه تجزیه‌وتحلیل مبتنی بر نظریه بازی‌ها برای تعیین راهبردهای بهینه هر بازیکن، به ترتیب برای مخفی‌سازی پیام در پوشانه و تشخیص وجود پیام در نهانه، انجام و نشان داده می‌شود که اگر آلیس دقیقاً k بیت از دنباله پوشانه دودویی را تغییر دهد، در این صورت بهترین راهبرد پاسخ ایو را می‌توان به صورت یک عبارت چندجمله‌ای از درجه k برحسب متغیرهای موقعیت در دنباله بیان کرد. در حالت خاص، وقتی $k=1$ باشد، این عبارت چندجمله‌ای، یک فرمول خطی شبیه آنجایی است که عموماً در تحلیل نهان‌کاوی عملی مورد استفاده قرار می‌گیرد. در مقابل، در نظر گرفتن هر راهبرد ایو برای تشخیص نهانه از پوشانه، آلیس دارای بهترین راهبرد پاسخ است که جمع‌بندی مربوط به انتخاب راهبرد ایو را به حداقل می‌رساند (بارنی و تندی[5] ۲۰۱۳)، (گروسکلاگس[6] ۲۰۰۸) و (شاتل و بومه[7] ۲۰۱۲) .

در این مقاله فرمول‌هایی برای راهبردهای مین‌ماکس[8] هر دو بازیکن ارائه می‌شود و بیان می‌شود که چرا راه‌حل برنامه‌ریزی خطی مستقیم برای محاسبه این راهبردها، در حل مسائل واقعی به‌طور مؤثر قابل‌اجرا نیست. همچنین موازنه‌ی از راهبرد بازیکنان با محدودیت‌های ساختاری ارائه می‌شود و در مواردی که در آن تنها دو موقعیت مخفی‌سازی وجود دارد، همه موازنه‌ها دسته‌بندی‌شده و سؤال باقی‌مانده طبق منبع (شاتل و بومه، ۲۰۱۲) حل می‌شود.

پیشینه پژوهش

نظریه بازی‌ها یک چهارچوب ریاضی است که رقابت بین بازیگران راهبردی با اهداف متضاد را مورد تحقیق و بررسی قرار می‌دهد (بارنی و تندی، ۲۰۱۳)، (گروسکلاگس، ۲۰۰۸) و (جانسون و همکاران[9] ۲۰۱۱). نظریه بازی‌ها، به‌ویژه در همه زمینه‌های مرتبط به امنیت، شامل همه مدل‌های انتزاعی امنیتی در تصمیمات سرمایه‌گذاری، هر روز اهمیت بیشتر و بیشتری پیدا می‌کند. این اهمیت در همه سناریوهای گوناگون کاربردی از قبیل برنامه‌ریزی برای گشت در فرودگاه‌ها مدل سازی برای راهبردهای فیشینگ، شبکه‌های دفاعی و تشکیل گروه‌های دفاعی، در صورت مواجهه با تهدیدات داخلی، نمود دارد (چیا و چانگ،[10] ۲۰۱۱)، (لازکا و همکاران،[11] ۲۰۱۳) و (مایلی و همکاران،[12] ۲۰۱۱).

---

1. AbdelRaouf
2. Baei et al.
3. Fridrich, and Goljan
4. Dhawan and Gupta
5. Barni and Tondi
6. Grossklags
7. Schöttle and Böhme
8. Min-Max
9. Johnson
10. Chia & Chuang
11. Laszka et al
12. Maillé et al

به‌کارگیری نظریه بازی‌ها در شاخه‌های مختلف پنهان‌سازی اطلاعات شامل تحقیق در کانال‌های پنهان، نشان‌گذاری و البته نهان‌نگاری، مورد توجه قرار گرفته است. به‌طور مشابه، روش‌های نظریه بازی را می‌توان در حوزه چندرسانه‌ای پزشکی قانونی هم یافت (الوت و همکاران،[1] ۲۰۰۵)، (مولن و ایوانوویچ،[2] ۲۰۰۳) و (استام و همکاران،[3] ۲۰۱۲)

در این مقاله با در نظر گرفتن نهان‌نگاری تطبیقی که در آن آلیس مکان‌هایی را برای مخفی‌سازی بیت‌های پیام انتخاب می‌کند و ایو تلاش می‌کند که این مکان‌ها را پیش‌بینی کرده تا وجود پیام مخفی را تشخیص دهد، این فرایند به‌طور طبیعی با استفاده از نظریه‌ی بازی مدل‌سازی می‌شود.

از طرف دیگر، طرح‌های عملی نهان‌نگاری تطبیقی معمولاً در مرحله‌ی نخست بر مفهوم غیرقابل تشخیص بودن متکی هستند تا امنیت پیام‌های مخفی‌شده را افزایش دهند. در واقع، طرح‌های اولیه تطبیقی نه تنها مناطق کمتر قابل تشخیص تصاویر را ترجیح می‌دهند؛ بلکه همه تغییرات مخفی‌سازی را به مناطقی که کمترین احتمال پیش‌بینی و تشخیص در آن‌ها وجود داشت محدود می‌کردند (فرنز،[4] ۲۰۰۲). آثار قبلی که کارهای مربوط به مخفی‌سازی تطبیقی را موردبررسی قرار می‌دادند، این راهبرد را مخفی سازی تطبیقی ساده نامیدند و نشان دادند که این راهبرد یک راهبرد مناسبی نیست. در منبع (بومه و وست فلد،[5] ۲۰۰۴) نشان داده شد که نهان‌کاو می‌تواند دانش خود درباره الگوریتم خاص مخفی‌سازی تطبیقی را از منبع (فرنز، ۲۰۰۲) به دست آورد تا با دقت بیشتری آن را، حتی نسبت به مخفی‌سازی یکنواخت تصادفی، تشخیص دهد. در منبع (شاتل و بومه، ۲۰۱۲) برای اولین بار نشان داده شد که اگر نهان‌کاو راهبردی باشد، هیچ‌وقت برای نهان‌نگار مطلوب نخواهد بود که به‌طور قطعی در مواضعی که کمترین قابلیت پیش‌بینی را دارند، مخفی‌سازی کند. تجزیه‌وتحلیل مبتنی بر نظریه بازی منبع (شاتل و بومه، ۲۰۱۲) به یک مدل با دو موضع مخفی‌سازی، محدود می‌شد که در آن ایو تنها به یک موضع می‌توانست نگاه کند. توسعه بعدی این مدل، (جانسون، ۲۰۱۲)، این امکان را به نهان‌نگار داد تا بیت‌های متعددی را در دنباله پوشانه به‌اندازه دلخواه تغییر دهد؛ اما محدودیت‌های کمی را در مورد قدرت نهان‌کاو حفظ کرد، به طوریکه او تنها می‌توانست برای یک موقعیت تصمیم‌گیری کند. توسعه دیگری که باعث تعمیم این مدل شد، معرفی یک تحلیل نهان‌کاوی دیگر با روش غیریکنواخت است که مدل‌بندی آن به‌صورت یک بازی با مجموع صفر در منبع (وو و ژانگ،[6] ۲۰۲۱)، (دنمارک و فردریچ،[7] ۲۰۱۴) و (لازکا و همکاران، ۲۰۱۳) انجام گرفت.

توسعه بعدی این تحقیق که قدرت ایو را گسترش داد ولی آلیس نیاز داشت که در هر موقعیت به‌طور مستقل مخفی‌سازی کند، در منبع (لازکا و همکاران، ۲۰۱۳) صورت گرفت. در سال ۱۹۹۸، اتینگر[8] یک بازی دو نفره با مجموع صفر بین یک نهان‌نگار و یک نهان‌کاو فعال را پیشنهاد کرد که هدف نهان‌کاو ایجاد اختلال در ارتباطات مبتنی بر نهان‌نگاری بود (اتینگر، ۱۹۹۸). کر[9] از نظریه‌ی بازی برای یافتن راهبردهایی در مورد خاص نهان‌نگاری دسته‌ای استفاده می‌کند که در آن بار مفید می‌تواند در بسیاری از اشیاء پوشانه گسترش پیدا کند (کر، ۲۰۰۷). نهان‌کاو این را دنبال و سعی می‌کند تا وجود هرگونه پیام محرمانه را کشف کند. اورس دیمر[10] و همکارانش قاعده رقابت بین نهان‌نگار و نهان‌کاو را با استفاده از نظریه مجموعه‌ها بنا نهادند (اورس دیمر، ۲۰۰۸). در این مدل نهان‌نگار این امکان را دارد که یا از راهبرد ساده و یا از راهبرد پیچیده استفاده کند که در راهبرد

1. Hélouët et al.
2. Moulin and Ivanovic
3. Stamm
4. Franz
5. Bohme and Westfeld
6. Wu and Zhang
7. Denemark and Fridrich
8. Ettinger
9. Ker
1 . Orsdemir 0

پیچیده او محدودیت‌های تشخیص‌ناپذیری آماری را با هم ترکیب می‌کند. با این کار آن‌ها یک متل- بازی طراحی کردند (شاتل و بومه، ۲۰۱۸)، (جانسون و همکاران، ۲۰۱۲، (لازکا و همکاران، ۲۰۱۳) و (مکالا و ماهندران[1] ۲۰۱۸).

روش پژوهش

مدل مبتنی بر نظریه‌ی بازی

برای شرح این مدل، مجموعه‌ای از بازیکنان، مجموعه‌ای از حالت‌هایی که جهان می‌تواند در آن حالت‌ها باشد، مجموعه‌ای از گزینه‌هایی که می‌تواند در دسترس بازیکنان باشد و مجموعه‌ای از نتایج نهایی که در پیامد این انتخاب‌ها هستند را مشخص می‌کنیم. چون بازی ما یک گسترش تصادفی از یک بازی قطعی است، ابتدا ساختار این بازی قطعی را مشخص و به دنبال آن جزئیات مربوط به تصادفی کردن را بیان می‌کنیم.

بازیکنان

بازیکنان این بازی عبارت‌اند از آلیس به‌عنوان یک نهان‌نگار و ایو به‌عنوان یک نهان‌کاو. آلیس می‌خواهد پیامی را از طریق یک کانال ارتباطی و توسط یک پوشانه تصویری برای باب ارسال کند و ایو که ناظر بر این کانال است، می‌خواهد تشخیص دهد که آیا هر رسانه‌ی تصویری موجود در این کانال حاوی یک پیام است یا خیر. گاهی اوقات مناسب است که به طبیعت به‌عنوان نیرویی که باعث می‌شود متغیرهای تصادفی تحقق پیدا کنند و باب به‌عنوان گیرنده پیام هم اشاره‌ای داشته باشیم. هرچند که باب و طبیعت، به دلیل راهبردی نبودن، در مفهوم نظریه‌ی بازی در زمره بازیکنان نیستند.

رویدادها (مراحل بازی)

فضای رویدادهای ممکن این بازی به‌صورت مجموعه $\Omega = \{0,1\}^N \times \{C,S\}$ تعریف می‌شود. هر رویداد شامل دو قسمت، یکی دنباله دودویی $x \in \{0,1\}^N$ و دیگری یک وضعیت نهان‌نگاری $y \in \{C,S\}$ است که در آن C نشان‌دهنده یک تصویر پوشانه و S نشان‌دهنده‌ی تصویر نهانه است. دنباله دودویی نمایانگر آن است که ایو تصویری را در کانال ارتباطی مشاهده می‌کند. وضعیت نهان‌نگاری به ما نشان می‌دهد که آیا پیامی در این دنباله دودویی (تصویر ارسالی) مخفی‌شده است یا خیر. در یک بازی تصادفی، هیچ‌یک از این دو حالت برای بازیکنان معلوم نیست تا اینکه آن‌ها انتخاب خود را انجام دهند. برای تعریف بازی محدود و جهت سادگی فرض می‌کنیم که بعضی از رویدادها توسط طبیعت انتخاب‌شده‌اند به طوریکه جهان در یک حالت ثابت (x,y) قرار دارد.

گزینه‌های بازیکنان

گزینه آلیس (راهبرد خالص) این است که یک زیرمجموعه I از $\{0,...,N-1\}$ با اندازه k را انتخاب کند که نشان‌دهنده‌ی مکان‌هایی است که در آن می‌تواند بیت‌های پیام را مخفی کند.

گزینه ایو (راهبرد خالص) این است که یک زیرمجموعه E_S از $\{0,1\}^N$ را انتخاب کند که نشان‌دهنده مجموعه‌ای از دنباله‌ها است که او آن‌ها را به‌عنوان تصاویر نهانه دسته‌بندی می‌کند. در نتیجه تصاویر موجود در $E_C = \{0,1\}^N \setminus E_S$ به‌عنوان تصاویر پوشانه دسته‌بندی می‌شوند.

نتایج بازی

فرض کنید که آلیس راهبرد خالص $I \subseteq \{0,...,N-1\}$ را انتخاب می‌کند و ایو هم راهبرد خالص $E_S \subseteq \{0,1\}^N$ را انتخاب می‌کند و طبیعت هم دنباله دودویی x و حالت نهان‌نگاری y را انتخاب می‌کند. در این صورت اگر ایو x را درست دسته‌بندی کند، برنده ۱ خواهد بود و اگر غلط دسته‌بندی کرده باشد، ۱ را می‌بازد. از آنجایی این بازی به‌صورت مجموع صفر است؛ لذا،

1. Mekala and Mahendran

نتیجه راهبر آلیس قرینه نتیجه راهبرد ایو است. جدول ۱ نتایج ممکن این بازی را به‌صورت ماتریس بازده با حاصل جمع صفر نشان می‌دهد.

جدول ۱: نتایج حاصله برای ایو و آلیس

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

توصیف تصادفی بودن بازی

برای توصیف ماهیت تصادفی بودن بازی با تعریف دو متغیر تصادفی در فضای رویدادهایمان، یعنی Ω، کار را شروع می‌کنیم. لذا فرض $X:\Omega\to\{0,1\}^N$ متغیری تصادفی باشد که هر رویداد را به فضای دنباله‌های دودویی نسبت می‌دهد. همچنین فرض کنید $Y:\Omega\to\{C,S\}$ متغیر تصادفی دیگری باشد که هر رویداد را به یک حالت نهان‌نگاری می‌برد. در ادامه این بخش ابتدا با توصیف ساختار توزیع فوق روی Ω و سپس توصیف راهبردهای ترکیبی ممکن دو بازیکن و سرانجام با ارائه نتیجه‌ی بازی دو بازیکن به‌عنوان دستاورد راهبردهای ترکیبی آن‌ها، بقیه کار را دنبال می‌کنیم.

حالت‌های نهان‌نگاری: حالت $Y=S$ موقعیت اتفاق می‌افتد که طبیعت حالت نهان‌نگاری را نهانه انتخاب کند و این حالت با احتمال P_S اتفاق می‌افتد. در این صورت $\Pr_\Omega[Y=C]:=P_C=1-P_S$ خواهد بود. از دیدگاه ایو، P_S احتمال اولیه است که او یک دنباله دودویی نهانه را در کانال ارتباطی مشاهده می‌کند. یکی از پروتکل‌های مشترک در نهان‌نگاری، این است که دو احتمال اولیه P_C و P_S مربوط به دو حالت نهان‌نگاری را برابر بدانیم، به‌طوری‌که ایو یک دنباله نهانه را دقیقاً با ۵۰٪ احتمال مشاهده می‌کند. نتایج کار ما که موازنه را برای این مدل توصیف می‌کند، آن‌ها با احتمالات اولیه دلخواه انجام می‌دهد؛ بنابراین، ما دو نماد P_C و P_S را در چندین فرمول متعاقب آن حفظ می‌کنیم. هرچند که باید توجه داشت بازی با احتمالات اولیه و اختلاف خیلی زیاد، می‌تواند بی‌اهمیت باشد؛ زیرا احتمالات اولیه می‌توانند انگیزه‌های دیگر را تحت تأثیر خود قرار دهند، به این دلیل، برای حفظ برخی قضیه‌های ساختاری به احتمالات اولیه مساوی نیازمندیم.

دنباله‌های دودویی: توزیع دنباله‌های دودویی به مقدار حالت نهان‌نگاری بستگی دارد. اگر $Y=C$ باشد، در این صورت حالت نهان‌نگاری پوشانه است و X بر طبق توزیع پوشانه C توزیع می‌شود. اگر $Y=S$ باشد، در این صورت حالت نهان‌نگاری نهانه است و X بر طبق توزیع پوشانه S توزیع می‌شود؛ بنابراین با در دست داشتن این نمادها، برای هر رویداد $(X=x,Y=y)$ تعریف می‌کنیم:

$$\Pr_\Omega\big[(x,y)\big]=\Pr_\Omega[Y=y]\cdot\Pr_\Omega[X=x\mid Y=y]$$
$$=\begin{cases} pc\cdot\Pr_C[X=x] & if \quad y=C \\ ps\cdot\Pr_S[X=x] & if \quad y=S. \end{cases} \qquad (۳)$$

پس از توصیف راهبرد ترکیبی بازیکنان، توزیع C و S را تعریف می‌کنیم.

راهبردهای ترکیبی بازیکنان: به خاطر داشته باشید که راهبرد ترکیبی همان توزیع احتمال در راهبردهای خالص است. در راهبرد ترکیبی، آلیس می‌تواند با یک احتمالی، در هر زیرمجموعه از موقعیت‌های I با اندازه k، از $\{0,...,N-1\}$، با انتخاب توزیع یک توزیع احتمال به مخفی سازی پیام بپردازد. برای توصیف راهبرد ترکیبی، برای هر $I\subseteq\{0,...,N-1\}$، فرض a_I نشان‌دهنده احتمال این باشد که آلیس در هر یک از موقعیت‌های I مخفی سازی پیام را انجام دهد.

به‌طور مشابه راهبرد ترکیبی ایو عبارت است از توزیع احتمالی از زیرمجموعه‌های $\{۰,۱\}^N$؛ بنابراین، راهبرد ترکیبی ایو احتمال eS را به هر یک از زیرمجموعه‌های $S\subseteq\{۰,۱\}^N$ اختصاص دهد. در نتیجه با در نظر گرفتن یک نماد دیگر $e:\{۰,۱\}^N\to[۰,۱]$، خواهیم داشت:

$$e(x)=\sum_{S\subseteq\{۰,۱\}^N:x\in S}e_S \qquad (۴)$$

$e(x)$ کل احتمال این است که ایو تصویر x را به‌عنوان یک نهانه دسته‌بندی می‌کند. توجه داشته باشید که این نمایش طرح‌ریزی‌شده از راهبرد ترکیبی ایو که در رابطه (۴) داده شد، نیازمند تعیین ۲^N عدد حقیقی است، درحالی‌که نمایش استاندارد راهبرد ترکیبی ایو که از نماد e_S استفاده می‌کند، نیازمند تعیین $۲^{۲^N}$ عدد حقیقی است؛ بنابراین، ترجیح می‌دهیم که از یک نمایش طرح‌ریزی‌شده استفاده کنیم. خوشبختانه، یک نمایش طرح‌ریزی‌شده، دارای اطلاعات کافی برای تعیین نتیجه‌ی بازی برای هر دو بازیکن است، لذا توان محاسبه میزان موفقیت هر بازیکن را دارد.

نمایش ساده‌شده راهبرد ترکیبی ایو: در زیر نشان می‌دهیم که نگاشت نمایش استاندارد راهبرد ترکیبی ایو نسبت به نمایش طرح‌ریزی‌شده، پوشا هست؛ بنابراین می‌توانیم نتایج را با استفاده از نمایش ساده‌تر و بدون از دست دادن کلیات بیان کنیم. برای هر تابع $e:\{۰,۱\}^N\to[۰,۱]$، یک توزیع $S\subseteq\{۰,۱\}^N$، e_S وجود دارد که در رابطه‌ی (۴) صدق می‌کند.

برای نشان دادن این مطلب، الگوریتمی را فراهم می‌کنیم که می‌تواند با استفاده از توزیع مناسبی از $S\subseteq\{۰,۱\}^N$، e_S را از تابع اختیاری $e:\{۰,۱\}^N\to[۰,۱]$ محاسبه کند؛ بنابراین ابتدا دنباله‌ها را طبق مقادیر $e(x)$ و به صورت نزولی مرتب می‌کنیم و آن‌ها را به صورت $x^۱,x^۲,...,x^{۲^N}$ نشان می‌دهیم (یعنی بدون از دست دادن کلیت فرض کنید $(e(x^۱)\ge e(x^۲)\ge...\ge e(x^{۲^N}))$). سپس احتمالات را به هر زیرمجموعه از دنباله‌ها به‌صورت زیر اختصاص دهید. فرض کنید اولین زیرمجموعه دنباله‌ها $S^۰=\{\}\ S^۰=\{\}$ باشد، سپس فرض کنید که احتمال آن‌هم $e(s^۰)=۱-e(x^۱)$ باشد. همچنین فرض کنید که دومین زیرمجموعه $S^۱=\{x^۱\}$ باشد و فرض کنید که احتمال آن‌هم $e_{S^۱}=e(x^۱)-e(x^۲)$ باشد. به‌طور مشابه، فرض کنید $(k+۱)$ زیرمجموعه $S^k=\{x^۱,x^۲,...,x^k\}$ باشد و فرض کنید احتمال آن $e_{S^k}=e(x^k)-e(x^{k-۱})$ باشد و سرانجام اگر آخرین زیرمجموعه $S^{۲^N}=\{x^۱,x^۲,...,x^{۲^N}\}$باشد، احتمال آن را $e_{S^{۲^N}}=e(x^{۲^N})$ قرار می‌دهیم.

حال نشان می‌دهیم که خروجی الگوریتم **اولاً**: یک توزیع احتمال است (یعنی مجموع احتمالات برابر با ۱ است) و **ثانیاً**: در رابطه‌ی (۴) صدق می‌کند.

اولاً، مجموع احتمالات حاصله عبارت است از:

$$e_{S^۰}+e_{S^۱}+e_{S^۲}+....+e_{S^{۲^N}} \qquad (۵)$$

$$=۱-e(x^۱)+e(x^۱)-e(x^۲)+e(x^۲)-e(x^۳)+...+e(x^{۲^N}) \qquad (۶)$$

$$=۱ \qquad (۷)$$

ثانیاً، برای یک دنباله اختیاری x^k داریم:

$$\sum_{S\subseteq\{۰,۱\}^N:x^k\in S}e_S=\sum_{l=k}^{۲^N}e_{S^l} \qquad (۸)$$

$$=e(x^k)-e(x^{k+۱})+e(x^{k+۱})-e(x^{k+۲})+...+e(x^{۲^N}) \qquad (۹)$$

$$=e(x^k). \qquad (۱۰)$$

بنابراین، توزیع حاصل، نیازهای رابطه (۴) را برآورده می‌کند. توجه داشته باشید که توزیع حاصل نسبتاً ساده است؛ چرا که به یک احتمال غیر صفر و حداکثر به $N^۲+۱$ زیرمجموعه اعمال می‌شود (و حتی کمتر، اگر بعضی از زیرمجموعه‌ها دارای مقادیر $e(x)$ باشند). به‌آسانی می‌توان دید که کاری بهتر از این کلیات نمی‌توانیم انجام دهیم، به این معنی که تعداد بی‌شماری از توابع e وجود دارند که برای هر یک هیچ توزیعی با کمترین حمایت نمی‌تواند وجود داشته باشد.

توزیع پوشانه: در توزیع پوشانه C، مختصات X به‌طور مستقل توزیع می‌شود، بنابراین:

$$\Pr_C[X = x] = \prod_{i=0}^{N-1} \Pr_C[X_i = x_i]. \quad (۱۱)$$

هرچند که بیت‌ها به‌طور یکسان توزیع نمی‌شوند. برای هر یک از i ها داریم:

$$\Pr_C[X_i = 1] = f_i, \quad (۱۲)$$

که در آن $\langle f_i \rangle_{i=0}^{N-1}$ یک دنباله یکنواخت افزایشی در بازه‌ی $(\frac{1}{2},1)$ است. توجه داشته باشید که این فرض بدون از دست دادن کلیات است؛ زیرا در به‌کارگیری کانال ارتباطی در یک دنباله، ما همیشه می‌توانیم صفرها و یک‌ها را جابه‌جا کنیم تا یک‌ها خیلی به این احتمال نزدیک باشند. همچنین می‌توانیم موقعیت‌ها را از کمترین حالت پیش‌بینی به بیشترین حالت پیش‌بینی مرتب کنیم. برای سادگی تعریف می‌کنیم:

$$\tilde{f}_i = 2f_i - 1. \quad (۱۳)$$

حال $\tilde{f}_i$ را به‌عنوان مقیاس اریبی قابلیت پیش‌بینی در موقعیت i تفسیر می‌کنیم. اگر این اریبی در برخی از موقعیت‌ها نزدیک صفر باشد، در این صورت مقدار آن موقعیت خیلی قابل پیش‌بینی نیست، درحالی‌که اگر این تمایل به‌طرف ۱ باشد، مقدار آن موقعیت قابل پیش‌بینی است. با قرار دادن همه این موارد در کنار هم توزیع پوشانه به‌صورت زیر تعریف می‌شود:

$$\begin{aligned}\Pr_C[X = x] &= \prod_{x_i=1} f_i \cdot \prod_{x_i=0} (1 - f_i) \\ &= \prod_{i=0}^{N-1} (1 - f_i + x_i \tilde{f}_i)\end{aligned} \quad (۱۴)$$

توزیع نهانه: توزیع نهانه S به انتخاب آلیس در راهبرد مخفی‌سازی بستگی دارد. لذا، فرض کنید که $I \subseteq \{0,1,\ldots,N-1\}$ باشد و برای هر $x \in \{0,1\}^N$، فرض کنید x_I نشان‌دهنده‌ی دنباله دودویی باشد که با جایگزینی بیت‌ها در همه موقعیت‌های I از x به‌دست‌آمده باشد. به‌طور خیلی رسمی، فرض کنید که آلیس در هر یک از زیرمجموعه $I \subseteq \{0,\ldots,N-1\}$ جاسازی را با احتمال a_I انجام می‌دهد. در این صورت داریم:

$$\begin{aligned}\Pr_S[X = x] &= \sum_I a_I \cdot \Pr_C[X = x_I] \\ &= \sum_I a_I \cdot \prod_{i \notin I} \Pr_C[X_i = x_i] \cdot \prod_{i \in I} \Pr_C[X_i = 1 - x_i] \\ &= \sum_I a_I \cdot \prod_{i \notin I} (1 - f_i + x_i \tilde{f}_i) \cdot \prod_{i \in I} (f_i - x_i \tilde{f}_i).\end{aligned} \quad (۱۵)$$

نتایج نهایی بازیکن:

$$\begin{aligned}u(Eve) = {} & \Pr_\Omega[X \in E_C \text{ and } Y = S] && \text{مثبت درست} \\ & + \Pr_\Omega[X \in E_C \text{ and } Y = C] && \text{منفی درست} \\ & - \Pr_\Omega[X \in E_S \text{ and } Y = C] && \text{مثبت کاذب} \\ & - \Pr_\Omega[X \in E_C \text{ and } Y = S] && \text{منفی کاذب}\end{aligned}$$

و این را می‌توان به‌صورت زیر محاسبه کرد:

$$\begin{aligned}u(Eve) &= ps\, Pr_S[X \in E_S] + pc \Pr_C[X \in E_C] - pc \Pr_C[X \in E_S] - ps \Pr_S[X \in E_C] \\ &= \sum_{x \in \{0,1\}^N} \Big[e(x)\, ps \Pr_{S(a)}[X = x] + (1 - e(x))\, pc \Pr_C[X = x] \\ &\quad - (1 - e(x))\, ps \Pr_{S(a)}[X = x] - e(x)\, pc \Pr_C[X = x] \Big] \\ &= \sum_{x \in \{0,1\}^N} (2e(x) - 1)\big(ps\, Pr_{S(a)}[X = x] - pc \Pr_C[X = x] \big).\end{aligned} \quad (۱۶)$$

عبارت‌های $Prs(a)[X=x]$ و $Prc[X=x]$ به ترتیب در معادلات (۱۴) و (۱۵) تعریف می‌شوند. توجه داشته باشید که می‌توانیم بنویسیم S = S(a) تا تصریح کنیم که توزیع S به راهبرد ترکیبی آلیس a بستگی دارد. به‌طور خلاصه، نتیجه نهایی راهبرد

آلیس این احتمال است که دسته‌بندی او صحیح است منهای احتمال اینکه این دسته‌بندی نادرست است. از طرفی از آنجایی‌که این بازی با مجموع صفر است، نتیجه نهایی راهبرد آلیس دقیقاً عکس نتیجه نهایی راهبرد ایو است.

تجزیه‌وتحلیل یافته‌ها

در این بخش، نتایج مربوط به تجزیه‌وتحلیل خود را ارائه می‌دهیم؛ بنابراین، کار را با شرح بهترین راهبردهای پاسخ هر بازیکن شروع می‌کنیم. سپس، راهبردهای مین‌ماکس را در نماد رسمی برای هر بازیکن شرح می‌دهیم.

بهترین پاسخ‌ها

برای محاسبه بهترین پاسخ آلیس و ایو، فرض می‌کنیم که بازیکن دیگر یک راهبرد ثابت را بازی می‌کند. راهبردی برای آلیس (یا ایو) به‌طور مناسب تعیین می‌شود که نتیجه نهایی را در معادله (۱۶) به حداقل (یا حداکثر) می‌رساند.

بهترین پاسخ آلیس: با فرض راهبرد e برای ایو، هدف آلیس این است که نتیجه نهایی را در معادله (۱۶) به حداقل برساند. اگرچه، ازآنجایی‌که او کنترلی بر توزیع پوشانه C ندارد، این هدف می‌تواند به‌اندازه به حداقل رسانی ساده شود:

$$\sum_{x\in\{۰,۱\}} \left(۲e(x)-۱\right).ps\ \Pr_{S(a)}\left[X=x\right]$$
$$= ps \sum_{x\in\{۰,۱\}^N} \left(۲e(x)-۱\right). \sum_{I\subseteq\{۰,\ldots,N-۱\}} a_I \Pr_C\left[X=x_I\right]$$
$$= ps \sum_{I\subseteq\{۰,\ldots,N-۱\}} a_I \sum_{x\in\{۰,۱\}^N} \left(۲e(x)-۱\right).\Pr_C\left[X=x_I\right].$$

این فرمول در متغیر انتخاب آلیس خطی است؛ بنابراین او می‌تواند با قرار دادن همه احتمالاتش در حداقل عناصر مجموع، مقدار آن را به حداقل برساند. بهترین پاسخ برای آلیس این است که یک راهبرد خالص I را بازی کند که رابطه زیر را به حداقل می‌رساند:

$$\sum_{x\in\{۰,۱\}^N} \left(۲e(x)-۱\right).\Pr_C\left[X=x_I\right]. \qquad (۱۷)$$

البته چندین I مختلف هم ممکن است که هم‌زمان این مجموع را به حداقل برسانند. در این مورد، بهترین فضای راهبرد پاسخ آلیس نیز ممکن است شامل یک راهبرد ترکیبی باشد که احتمالات مخفی‌سازی او را به‌صورت تصادفی در بین چنین I توزیع می‌کند.

بهترین پاسخ ایو: با فرض یک راهبرد ثابت برای آلیس، هدف ایو این است که نتیجه نهایی خود را، طبق رابطه (۱۶)، به حداکثر برساند؛ بنابراین، برای هر x، او باید e(x) را انتخاب کند تا عبارت مجموع را که معادل x است، به حداکثر برساند. در حالت خاص، اگر

$$p_S \Pr_{S(a)}\left[X=x\right]-P_C\Pr_C\left[X=x\right]>۰,$$

در این صورت بهترین انتخاب عبارت از $e(x)=۱$ است و اگر نامساوی اکید، معکوس شود، در این صورت بهترین انتخاب $e(x)=۰$ است. اگر به جای این نامساوی، مساوی قرار گیرد، در این صورت ایو می‌تواند هر مقداری را برای $e(x)\in[۰,۱]$ انتخاب کند و بهترین پاسخ را اجرا کند. به‌طور رسمی‌تر، قانون تصمیم بهینه ایو عبارت است از:

$$e(x)=\begin{cases} ۱ & \text{if} \quad \dfrac{\Pr_{\Omega}\left[Y=S\mid X=x\right]}{\Pr_{\Omega}\left[Y=C\mid X=x\right]}>۱, \\ ۰ & \text{if} \quad \dfrac{\Pr_{\Omega}\left[Y=S\mid X=x\right]}{\Pr_{\Omega}\left[Y=C\mid X=x\right]}<۱, \\ \text{any} \quad p\in[۰,۱] & \text{if} \quad \dfrac{\Pr_{\Omega}\left[Y=S\mid X=x\right]}{\Pr_{\Omega}\left[Y=C\mid X=x\right]}=۱. \end{cases} \qquad (۱۸)$$

برای یک دنباله ثابت x، شرایط برای دسته‌بندی x به‌عنوان نهانه می‌تواند به‌صورت زیر نوشته شود:

$$
\begin{aligned}
&1 < \frac{\Pr_{\Omega}\left[Y=S \mid X=x\right]}{\Pr_{\Omega}\left[Y=C \mid X=x\right]} \\
&= \frac{\Pr_{\Omega}\left[X=x\right]}{\Pr_{\Omega}\left[X=x\right]} \cdot \frac{\Pr_{\Omega}\left[Y=S \mid X=x\right]}{\Pr_{\Omega}\left[Y=C \mid X=x\right]} \\
&= \frac{\Pr_{\Omega}\left[Y=S\right]}{\Pr_{\Omega}\left[Y=C\right]} \cdot \frac{\Pr_{\Omega}\left[X=x \mid Y=S\right]}{\Pr_{\Omega}\left[X=x \mid Y=C\right]} \\
&= \frac{ps}{pc} \frac{\Pr_{S}\left[X=x\right]}{\Pr_{C}\left[X=x\right]} \\
&= \frac{\mathrm{ps}}{\mathrm{pc}} \frac{\sum_{\mathrm{I}} \mathrm{a}_{\mathrm{I}} . \Pi_{\mathrm{i} \notin \mathrm{I}} (1-\mathrm{f}_{\mathrm{i}}+\mathrm{x}_{\mathrm{i}} \tilde{\mathrm{f}}_{\mathrm{i}}) . \Pi_{\mathrm{i} \in \mathrm{I}} (\mathrm{f}_{\mathrm{i}}-\mathrm{x}_{\mathrm{i}} \tilde{\mathrm{f}}_{\mathrm{i}})}{\prod_{\mathrm{i}=0}^{\mathrm{N}-1} (1-\mathrm{f}_{\mathrm{i}}+\mathrm{x}_{\mathrm{i}} \tilde{\mathrm{f}}_{\mathrm{i}})} \\
&= \frac{\mathrm{ps}}{\mathrm{pc}} \sum_{\mathrm{I}} \mathrm{a}_{\mathrm{I}} \prod_{\mathrm{i} \in \mathrm{I}} \left(\frac{\mathrm{f}_{\mathrm{i}}-\mathrm{x}_{\mathrm{i}} \tilde{\mathrm{f}}_{\mathrm{i}}}{1-\mathrm{f}_{\mathrm{i}}+\mathrm{x}_{\mathrm{i}} \tilde{\mathrm{f}}_{\mathrm{i}}} \right) \\
&= \frac{\mathrm{ps}}{\mathrm{pc}} \sum_{\mathrm{I}} \mathrm{a}_{\mathrm{I}} \prod_{\mathrm{i} \in \mathrm{I}} \left(\frac{\mathrm{f}_{\mathrm{i}}}{1-\mathrm{f}_{\mathrm{i}}} - \mathrm{x}_{\mathrm{i}} \frac{\tilde{\mathrm{f}}_{\mathrm{i}}}{\mathrm{f}_{\mathrm{i}}(1-\mathrm{f}_{\mathrm{i}})} \right)
\end{aligned}
\qquad (۱۹)
$$

توجه کنید که قانون تصمیم‌گیری ایو به‌صورت یک معادله چندجمله‌ای از درجه حداکثر k و در دنباله دودویی x نوشته می‌شود و اینکه تعداد عبارت‌ها در فرمول $\binom{N}{K}$ هست. وقتی k نسبت به N مقدار ثابت است (همانطوریکه در کاربرد عملی هم نوعاً این‌گونه است)، در این صورت $\binom{N}{K}$ در N چندجمله‌ای است و قانون تصمیم‌گیری بهینه ایو می‌تواند به‌نوبه‌ی خود برای هر دنباله دودویی به‌کاربرده شود که خود در طول دنباله، چندجمله‌ای است.

راهبردهای مین ماکس

راهبرد مین‌ماکس در یک بازی دو نفره عبارت از یک راهبرد ترکیبی از یک بازیکن است که با فرض اینکه بازیکن دیگر با راهبرد خالص بهینه پاسخ خواهد داد، راندمان و نتیجه نهایی بازی خود را به حداکثر می‌رساند. راهبرد ماکس‌مین[1] ایو توسط رابطه زیر به دست می‌آید:

$$
\underset{e}{\mathrm{Arg.max}} \left(\min_{I} \left(\sum_{x \in \{0,1\}^N} \left(2e(x)-1\right)\left(p_S \Pr_C\left[X=x_I\right] - p_C \Pr_C\left[X=x\right]\right) \right) \right); \qquad (۲۰)
$$

درحالی‌که راهبرد مین‌ماکس آلیس توسط رابطه زیر به دست می‌آید:

$$
\underset{a}{\mathrm{Arg.min}} \left(\max_{E_S} \left(\sum_{x \in E_S} (p_S \Pr_{S(a)}\left[X=x\right] - p_C \Pr_C\left[X=x\right]) + \sum_{x \in E_C} (p_C \Pr_C\left[X=x\right] - p_S \Pr_{S(a)}\left[X=x\right]) \right) \right). \qquad (۲۱)
$$

هر راهبرد مین‌ماکس می‌تواند (به‌طور بازگشتی) به‌عنوان راه‌حل یک مسئله خطی که در بردارنده ماتریس نتیجه نهایی راهبردهای خالص ایو و آلیس تعیین شود. متأسفانه فضای راهبرد خالص ایو دارای اندازه‌ی 2^N است؛ بنابراین از لحاظ محاسباتی یافتن راهبردهای مین‌ماکس با استفاده از این روش حتی برای $N=5$ هم به‌سختی امکان‌پذیر است.

1. Max min

موازنه‌ی نش

برای این کار، یک محدودیت ساختاری برای موازنه نش در نظر می‌گیریم (وو و ژانگ، ۲۰۲۱)؛ که تحت آن شرط، دسته‌بندی ایو باید با توجه ترتیب جزئی متعارف در دنباله دودویی صورت گیرد. این مسئله نشان می‌دهد که این دسته‌بندی ضرورتاً باید مجموعه همه دنباله‌های دودویی را به دنباله‌هایی با طول کم و زیاد تقسیم کند که دنباله‌های با طول زیاد به‌عنوان پوشانه و دنباله‌های با طول کم به‌عنوان نهانه دسته‌بندی شوند. سپس، محدودیت‌های معینی را در مورد اولویت‌های توزیع متناسب با تمایل به یک موقعیت ارائه شود که تعیین می‌کند که آیا این بازی ناچیز بودن موازنه را تائید می‌کند یا خیر (که در آن دسته‌بندی ایو برای همه دنباله‌های دودویی ثابت است). اگر هر یک از اولویت‌ها نامتوازن باشند و تمایل یا کشش به سمت یک موقعیت، خیلی کم باشد، در این صورت بازی ناچیز بودن توازن را تائید خواهد کرد. اگرچه در بیشتر نواحی، پارامترهای نمونه اولیه بازی چنین چیزی را تائید نمی‌کند. وقتی دسته‌بندی ایو غیر بدیهی باشد، آلیس می‌تواند با تغییر احتمال مخفی‌سازی خود برای یک موقعیت در دنباله، بر تشخیص و آشکارسازی ایو و ازاین‌رو، بر نتیجه نهایی خود تأثیر بگذارد.

نتیجه‌گیری

در این مقاله یک بازی دو نفره بین آلیس به‌عنوان یک نهان‌نگار تطبیقی و ایو به عنوان نهان‌کاو با امکانات نامحدود مورد بررسی و تجزیه‌وتحلیل قرار گرفت. با در نظر گرفتن کاربرد دقیق اصل کهرشف در نهان‌نگاری، به ایو اجازه داده شد تا به راهبرد مخفی‌سازی آلیس، منبع توزیع پوشانه و قدرت نامحدود محاسباتی دسترسی داشته باشد. تحت این فرضیات، فرآیندهایی را برای ایجاد راهبرد مخفی‌سازی تطبیقی مطلوب با فرض دسته‌بندی مطلوب و ایجاد یک آشکارساز بهینه مدل‌بندی شد. این مدل روی دنباله‌های پوشانه با اندازه‌های دلخواه اعمال می‌شود، اگرچه اجرای این برنامه برای پوشانه‌های بزرگ، به‌عنوان یک چالش محاسباتی بزرگ باقی می‌ماند. برای نهان‌کاوی عملی، نتایج، ما را به سمت آشکارسازی بهینه مخفی‌سازی راهبردی و برای مخفی‌سازی مطلوب در برابر آشکارساز راهبردی، هدایت می‌کند. به‌طور خاص، دسته‌بندی بهینه ایو باید در اندازه قابلیت پیش‌بینی پوشانه، یکنواخت باشد و راهبرد مخفی‌سازی تطبیقی مطلوب آلیس حتی نباید از کمترین کشش یا تمایل به موقعیت‌هایی خاص در هنگام مخفی‌سازی پیام استفاده کند؛ یعنی راهبرد بهینه آلیس، راهبرد تطبیقی تصادفی است.

منابع

AbdelRaouf, A. (2021). A new data hiding approach for image steganography based on visual color sensitivity. Multimedia Tools and Applications, 1-25.

Baei, M. S, Norozi, Z, Sabzinezhad, M, & Karami, M. (2018). Designing an Image Steganography Algorithm Based on Entropy and ELSB2. Advanced Defence Sci. & Tech, 2, 39-50.

Baei, S. (2020). Designing a combinatorial Image Steganography algorithm based on game theory. Electronic and Cyber Defense, 8(1), 133-145.

Barni, M, & Tondi, B. (2013). The source identification game: An information-theoretic perspective. IEEE Transactions on Information Forensics and Security, 8(3), 450-463.

Bohme, R, & Westfeld, A. (2004). Exploiting preserved statistics for steganalysis. LNCS: Proceedings of the 6th International Workshop on Information Hiding,

Cayre, F, & Bas, P. (2008). Kerckhoffs-based embedding security classes for woa data hiding. IEEE Transactions on Information Forensics and Security, 3(1), 1-15.

Chia, P. H, & Chuang, J. (2011). Colonel Blotto in the phishing war. International Conference on Decision and Game Theory for Security,

Cox, I, Miller, M, Bloom, J, Fridrich, J, & Kalker, T. (2007). Digital watermarking and steganography. Morgan kaufmann.

Denemark, T, & Fridrich, J. (2014). Detection of content adaptive LSB matching: A game theory approach. Media Watermarking, Security, and Forensics 2014,

Dhawan, S, & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2), 63-87.

Ettinger, J. M. (1998). Steganalysis and game equilibria. International Workshop on Information Hiding,
Franz, E. (2002). Steganography preserving statistical properties. International Workshop on Information Hiding,
Fridrich, J, & Goljan, M. (2004). On estimation of secret message length in LSB steganography in spatial domain. Security, steganography, and watermarking of multimedia contents VI,
Grossklags, J, Christin, N, & Chuang, J. (2008). Secure or insure? A game-theoretic analysis of information security games. Proceedings of the 17th international conference on World Wide Web,
Hélouët, L, Zeitoun, M, & Degorre, A. (2005). Scenarios and Covert channels: another game. Electronic Notes in Theoretical Computer Science, 119(1), 93-116.
Johnson, B, Böhme, R, & Grossklags, J. (2011). Security games with market insurance. International Conference on Decision and Game Theory for Security,
Johnson, B, Schöttle, P, & Böhme, R. (2012). Where to hide the bits? International Conference on Decision and Game Theory for Security,
Ker, A. D. (2007). Batch steganography and the threshold game. Security, Steganography, and Watermarking of Multimedia Contents IX,
Laszka, A. (2013). Modeling content-adaptive steganography with detection costs as a quasi-zero-sum game. Infocommunications Journal,
Laszka, A, Johnson, B, Schöttle, P, Grossklags, J, & Böhme, R. (2013). Managing the weakest link. European Symposium on Research in Computer Security,
Maillé, P, Reichl, P, & Tuffin, B. (2011). Interplay between security providers, consumers, and attackers: a weighted congestion game approach. International Conference on Decision and Game Theory for Security,
Mekala, T, & Mahendran, N. (2018). Improved Security in Adaptive Steganography Using Game Theory. vol, 118, 111-116.
Moulin, P, & Ivanovic, A. (2003). The zero-rate spread-spectrum watermarking game. IEEE Transactions on Signal Processing, 51(4), 1098-1117.
Orsdemir, A, Altun, H. O, Sharma, G, & Bocko, M. F. (2008). Steganalysis-aware steganography: Statistical indistinguishability despite high distortion. Security, Forensics, Steganography, and Watermarking of Multimedia Contents X,
Schöttle, P, & Böhme, R. (2012). A game-theoretic approach to content-adaptive steganography. International Workshop on Information Hiding,
Stamm, M. C, Lin, W. S, & Liu, K. R. (2012). Forensics vs. anti-forensics: A decision and game theoretic framework. 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),
Wu, H, & Zhang, X. (2021). Game-theoretic analysis to parameterized reversible watermarking. IETE Technical Review, 38(1), 26-35.