



دو فصلنامه علمی پژوهش‌های سایبرالکترونیک

شماره ۲

بهار و تابستان ۱۴۰۲

صاحب امتیاز: دانشکده علوم و مهندسی دفاعی دانشگاه افسری و تربیت پاسداری امام حسین (ع)

مدیر مسئول: دکتر محمد کاظم بصیرتی

سر دبیر: دکتر محمد علی شمع‌علیزاده بایی

مدیر اجرایی: دکتر جلوانی

مدیر داخلی: دکتر حسینی

دستیاران مدیر اجرایی: مهندس برجعلی و مهندس یزدان‌پناه

اعضای هیأت تحریریه

دکتر رضا جلوانی مدرس دانشگاه

دکتر حسین صابری استادیار دانشگاه

مهندس علیرضا صفایی مدرس دانشگاه

مهندس حامد شیروی مدرس دانشگاه

مهندس علی غلام‌نتاج مدرس دانشگاه

مهندس محسن احترام مدرس دانشگاه

دکتر محمد کاظم بصیرتی استادیار دانشگاه

دکتر حمیدرضا لشکریان استادیار دانشگاه

دکتر حمید باباخانیان مدرس دانشگاه

دکتر ساسان چمنی مدرس دانشگاه

دکتر محمد علی شمع‌علیزاده استادیار دانشگاه



همکاران علمی و داوران این شماره

دکتر رضا جلایی، دکتر محمد مقصودی، مهندس ابوالحسن رضاپور کورنده، دکتر فاطمه زارع

دکتر مهدی علی‌نژاد، مهندس حامد شیروی، مهندس مرتضی یزدان‌پناه، مهندس یوسف برجعلی

مهندس پیمان فتواتی، مهندس مجید حاج‌جوادی، مهندس علی جعفری‌منش، مهندس علی غلام‌نتاج،

مهندس حمید یاری، مهندس محمدطاهر گرجیان

مدیر اجرایی: دکتر رضا جلوانی

ویراستار ادبی: مهندس ابوالحسن رضاپور کورنده

ویراستار انگلیسی و مترجم:

حروفچین و صفحه‌آرا:

طراح جلد: مجتبی مجتبی

شمارگان: ۱۰۰ (نسخه چاپی) ۲۰۰ (نسخه الکترونیکی) قیمت نسخه چاپی:

نشانی: تهران، بزرگراه شهید بابایی، بعد از پل لشکرک، دانشگاه افسری و تربیت پاسداری امام حسین (ع)، دانشکده علوم و مهندسی دفاعی، تلفن: ۷۷۱۰۳۰۵۰ داخلی ۱۰۹

Web Site: www.Jce.ihuo.ac.ir

E-mail: Jce@ihuo.ac.ir

تمام حقوق مادی و معنوی برای دانشکده علوم و مهندسی دفاعی محفوظ است.

اهداف و چشم انداز نشریه

هدف این نشریه، فراهم آوردن بستری مناسب برای تبادل اطلاعات و انتشار نتایج مطالعات و پژوهش‌های علمی، فنی و تخصصی دانشمندان، استادان، پژوهشگران و دانشجویان حوزه‌های مرتبط با فناوری اطلاعات، مخابرات، سایبرالکترونیک، رایانه و ...، جهت اعتلای سطح دانش نظری و علمی مجموعه دانشگاه و محققین سپاه و نیروهای مسلح و نیز تهیه‌ی مجموعه‌ای مفید است.

این نشریه به سردبیری دکتر محمدعلی شمع‌علیزاده بایی (استادیار و مدیر گروه رایانه و دفاع سایبری دانشگاه افسری و تربیت پاسداری امام حسین(ع)) و مدیریت اجرایی مهندس رضا جلوانی (مدیر گروه مخابرات و جنگال) از سال ۱۴۰۱ فعالیت خود را آغاز کرده است.

این نشریه با رعایت نکات بخش راهنمای نویسندگان، در حوزه‌های زیر به صورت رایگان مقاله می‌پذیرد:

- ۱- حفاظت از زیرساخت‌ها و داده‌ها در مقابل حملات سایبری
- ۲- دفاع سایبری (امنیت داده، تهدیدات نرم‌افزار، سیستم عامل، سخت‌افزار و ...)
- ۳- هوش مصنوعی (و فناوری‌های نوین سایبرالکترونیک و سایبرنتیک و علوم شناختی مرتبط)
- ۴- مهندسی دفاعی در حوزه فناوری اطلاعات و ارتباطات شامل: الف- امنیت اطلاعات، رمزنگاری، پنهان‌نگاری، پروتکل‌ها و استانداردها، ب- آسیب‌پذیری‌ها و تهدیدات فضای سایبری، ج- اخلاص و فریب (مخابراتی، راداری، کنترل، مراقبت و ناوبری)، د- ردیابی، مکان‌یابی، آشکارسازی و شنود سیگنال.
- ۵- تهدیدات نوپدید الکترونیک، سایبری، دفاع و پدافند مرتبط با آن‌ها
- ۶- مخابرات دفاعی و ارتباطات سیار
- ۷- الکترونیک رزمی (لیزری، الکترواپتیکی، آکوستیکی) و پدافندهای مرتبط
- ۸- فناوری اطلاعات و حوزه‌های مرتبط
- ۹- مدل‌سازی و شبیه‌سازی فناوری اطلاعات، ارتباطات، الکترونیک، دفاع الکترونیک و سایبری
- ۱۰- فرماندهی و کنترل در پدافند الکترونیک و سایبری

شرایط پذیرش و راهنمای تدوین مقاله

۱. مقاله باید پژوهشی و حاصل تحقیق نویسنده در یکی از حوزه‌های بیان‌شده در قسمت اهداف و چشم انداز نشریه باشد.
۲. مقاله‌های ارسالی به نشریه، نباید در هیچ یک از نشریه‌های داخلی یا خارجی چاپ شده باشد.
۳. مقاله‌ها پس از پذیرش اولیه در هیأت تحریریه، به‌منظور ارزیابی برای دو نفر از داوران صاحب‌نظر و کارشناس فرستاده خواهد شد و پذیرش نهایی بر اساس نظر داوران و موافقت هیئت تحریریه خواهد بود.
۴. مسئولیت علمی مقاله بر عهده‌ی نویسنده است و دیدگاه‌های نویسندگان مقالات، لزوماً دیدگاه نشریه نیست.
۵. مقاله باید حداکثر در ۱۲ صفحه A4 (حدود ۲۲ صفحه قطع نشریه) و در قالب Word و با قلم B Nazanin و سایز ۱۲ تایپ شود و در وبگاه نشریه (<http://ihuo.ac.ir>) بارگذاری کرده یا به آدرس پست الکترونیک (Jce@ihuo.ac.ir) ارسال شود.
۶. نشریه از مقاله‌های تحقیقی و تحلیلی اصیل استقبال می‌کند که در آن مطلب یا نظریه‌ای تخصصی دارای نوآوری، نکات علمی نوین و غیر اکتباسی ارائه، و به‌ویژه از مقاله‌های برگرفته از پایان‌نامه‌ها که طی آن نظری بدیع مطرح شده باشد، مجله از چاپ مقاله‌های مبنی بر گردآوری یا ترجمه معذور است.
۷. **برگه رویه (عنوان):** که در آن فقط اطلاعات شناسنامه‌ای تحقیق از جمله، عنوان، نام نویسنده یا نویسندگان، عنوان شغلی یا علمی، زمان نگارش، نشانی کامل فرد یا مؤسسه یا مؤسسات متبوع، پست الکترونیکی (ایمیل) و شماره تلفن درج می‌شود.
۸. **چکیده:** خلاصه‌ای دقیق از مقاله است که در یک صفحه جدا و در قالب و قلم متفاوت از متن نوشته می‌شود و در آن باید درستی و دقت، استقلال، ایجاز و صراحت، غیر قضاوتی بودن و روانی و انسجام رعایت شود.
۹. **مقدمه:** بخش اصلی مقاله با مقدمه آغاز می‌شود که در ضمن آن، مسأله تحقیق (سؤال‌ها، فرضیه‌ها، اهداف) و پیشینه علمی پژوهش بیان می‌شود.
۱۰. **روش تحقیق:** پس از مقدمه می‌آید و محقق جزئیات شیوه اجرای پژوهش را توصیف می‌کند. در این بخش، همکاران پژوهش و مراحل پژوهش (جامعه آماری، نمونه‌گیری، حجم نمونه و ...) بیان می‌شود.
۱۱. **بدنه نوشتار (بحث و تحلیل):** این بخش، بدنه اصلی و ستون فقرات نوشتار را تشکیل می‌دهد. داده‌ها و تحلیل‌ها باید بر اساس نظم و در چارچوب روشی منظم و بر اساس طرح کلی مقاله پیش برود.
۱۲. **نتیجه‌گیری و پیشنهاد:** نویسنده در بخش پایانی مقاله باید نتایج را بیان، و مطالب را چنان جمع‌بندی کند که خواننده احساس کند به پایان مقاله رسیده و از بحث و بررسی‌ها به نتیجه‌ای دست‌یافته است؛ هم‌چنین، پیشنهادهای بعدی و چشم‌انداز آینده و مسائل باقیمانده درباره موضوع در بخش نتیجه‌گیری مطرح می‌شود. این بخش یک پاراگراف تا یک صفحه باشد.

- ❖ سخن سردبیر ۱۱
- ❖ راهکارهای شناسایی حمله به شبکه‌های اینترنت اشیاء با روش‌های مبتنی بر ناهنجاری و هوش مصنوعی ۱۳
- ❖ سیدرضا راعی مقدم ۲۶
- ❖ تعیین ابعاد عملیات سایبری در نیروهای نظامی، دسته‌بندی تهدیدات و حوزه‌های کاربری ۲۶
- ❖ فرهاد فرنیا ۴۴
- ❖ مزایای عملیاتی استفاده از جنگ الکترونیک سایبری (CEW) در میدان نبرد ۴۴
- ❖ حامد شیروی ۵۸
- ❖ طراحی الگوریتم شناسایی تصاویر جعلی با استفاده از شبکه عصبی پیچشی ۵۸
- ❖ فاطمه زارع مهرجردی ۷۲
- ❖ شناسایی تهدیدات در شبکه‌های رایانه‌ای با الگوریتم شاهین هریس ۷۲
- ❖ هادی نیک‌منش

به نام آن که جان را فکرت آموخت چراغ دل به نور جان برافروخت
ز فضلش هر دو عالم گشت روشن ز فیضش خاک آدم گشت گلشن

با یاد و نام خدا و سلام به ارواح شهدا، امام شهدا، شهدای صدر اسلام، شهدای انقلاب اسلامی، شهدای جبهه مقاومت و بنیان‌گذار انقلاب اسلامی و ادامه‌دهنده راه‌شان رهبر معظم انقلاب اسلامی. شماره‌ی دوم فصل‌نامه‌ی پژوهش‌های سایبرالکترونیک، به کوشش همکاران ارجمند دو گروه علمی دفاع سایبری و مخابرات دانشکده فنی مهندسی، تقدیم کلیه‌ی محققان و پژوهش‌گران حوزه سایبرالکترونیک می‌شود. در سال‌های اخیر، تحقیقات در حوزه‌ی علوم سایبرالکترونیک و راهای مقابله با تهدیدات در این حوزه، اهمیت زیادی پیدا کرده است. لذا، انتشار تحقیقات و یافته‌های محققان در این زمینه از اهمیت ویژه‌ای برخوردار است. در این راستا، دانشکده فنی مهندسی دانشگاه افسری و تربیت پاسداری امام حسین(ع) بر آن شد تا یافته‌های علمی محققین در این حوزه را در این نشریه انتشار دهد. با آماده شدن دومین شماره نشریه، جا دارد از مدیر مسؤول محترم جناب دکتر بصیرتی بابت تذکرها و حمایت‌های به‌جایشان، اعضای محترم هیات تحریریه، مسئولین و محققان محترم رده کاربر این دو گروه علمی، اعم از معاونت فاوا و سایبرالکترونیک سپاه که با نظرهای سازنده‌ی‌شان ما را در بهبود هر چه بیشتر این شماره کمک کرده‌اند، تشکر و قدردانی نماییم.

امید است که در دو فصل‌نامه شماره ۳ که در پاییز و زمستان ۱۴۰۲ تقدیم حضور می‌شود، مقالات مفیدتری را تقدیم خوانندگان عزیز نماییم.

محمدعلی شمع‌علیزاده بایی

شناسایی تهدیدات شبکه‌های اینترنت اشیاء با روش‌های مبتنی بر ناهنجاری و هوش

مصنوعی

سیدرضا راعی مقدم^{*۱} - سیدرضا کامل طبابخ فریضنی^۲

۱- دانشجوی مقطع کارشناسی ارشد رشته شبکه‌های کامپیوتری، دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد مشهد،

S.Reza.Raei.M@gmail.com

۲- ^۱استاد، گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد، RezaKamel@yahoo.com

چکیده:

اینترنت اشیاء شبکه‌ای متشکل از دستگاه‌های مختلف با منابع محدود است؛ از این رو تأمین امنیت داده‌ها و حفظ محرمانگی آن پیچیدگی خود را دارد. سیستم‌های تشخیص نفوذ باید متناسب با حال اینترنت اشیاء طراحی شود تا بیش‌ترین دقت را داشته باشد. در این مقاله، با مقایسه انواع سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری نشان داده می‌شود که بهره‌برداری از روش ترکیبی، موجب افزایش دقت تشخیص نفوذها می‌گردد. همچنین، به تحلیل و ارزیابی ویژگی‌های مهم و ابزارهای مفید در این خصوص پرداخته می‌شود.

کلیدواژه‌ها: اینترنت اشیاء، سیستم‌های تشخیص نفوذ، مبتنی بر ناهنجاری، روش‌های ترکیبی، یادگیری عمیق، شبکه های عصبی.

Identification of threats to Internet of Things networks based on anomaly and artificial intelligence

Seyyed reza raei moghaddam^{*1} – Seyed Reza Kamel Tabbakh Farizani²

1*-Department of computer engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran , S.Reza.Raei.M@gmail.com

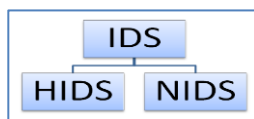
2-Assistant Prof, Department of computer engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran , RezaKamel@yahoo.com

Abstract

The Internet of Things (IoT) is a network consisting of various devices with limited resources, in this sense, providing data security and maintaining its confidentiality has its own complexity. Intrusion detection systems (IDS) should be designed according to the IoT to be most accurate. In this article, by comparing different types of anomaly-based IDSs, we represent that the use of the combined method increases the accuracy of intrusion detection. It also analyzes and evaluates important features and useful tools in this regard.

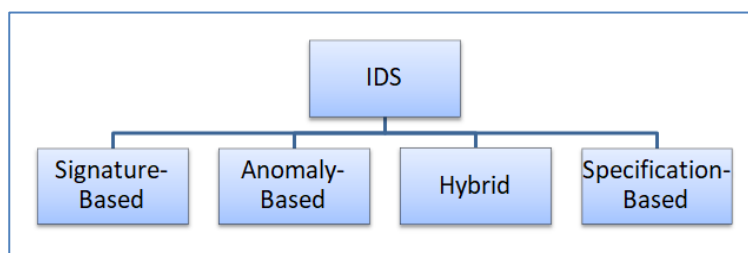
Keywords: Internet of Things , Intrusion Detection Systems , Combined Method , Deep Learning , Neural Networks

سیستم‌های تشخیص نفوذ به سیستم‌هایی که با روش‌های مختلف قابلیت تشخیص نفوذ را دارند، گفته می‌شود. طبق شکل ۱، IDS از منظر محل استقرار به دو دسته تحت شبکه (NIDS) و مبتنی بر میزبان (HIDS) تقسیم می‌شوند.



شکل (۱): تقسیم‌بندی سیستم‌های تشخیص نفوذ به لحاظ استقرار

سیستم‌های تشخیص نفوذ مبتنی بر شبکه، در لبه شبکه نصب می‌شوند و سیستم‌های تشخیص نفوذ مبتنی بر میزبان بر روی یک میزبان نصب می‌شوند و بهره‌برداران متناسب با شرایط خود از آنها استفاده می‌کنند. در یک تقسیم بندی دیگر، سیستم‌های تشخیص نفوذ بر اساس شیوه‌های تشخیص نفوذ طبق شکل ۲ به چهار دسته‌ی تشخیص بر اساس امضاء، تشخیص بر اساس ناهنجاری، تشخیص بر اساس مشخصه و یا ترکیبی تقسیم می‌شوند.



شکل (۲): تقسیم بندی سیستم های تشخیص نفوذ بر اساس رویکرد تشخیص

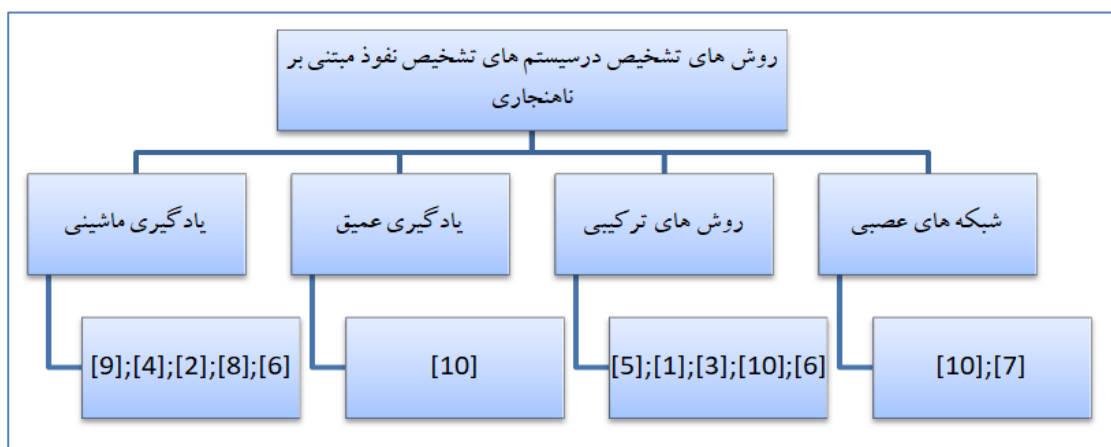
در روش مبتنی بر امضاء، الگوهای حمله که از قبل شناسایی شده، در یک پایگاه داده ذخیره شده است که به آنها امضاء می‌گویند. از این‌رو، قابلیت شناخت حملات قبلی بر اساس نام و ارائه راهکار وجود دارد؛ اما قابلیت تشخیص حملات جدید را ندارد. لذا، سیستم‌های تشخیص نفوذ با استفاده از روش‌های مبتنی بر ناهنجاری این ضعف را برطرف می‌کند.

مسئله و چالش اصلی در سیستم‌های تشخیص نفوذ اینترنت اشیا این است که با توجه به پایین بودن قدرت و منابع سخت‌افزاری این دستگاه‌ها، چگونه بتوانیم با استفاده از روش مبتنی بر ناهنجاری که عموماً از روش‌ها و الگوریتم های هوش مصنوعی، یادگیری ماشینی و یادگیری عمیق هستند و نیاز به منابع بیشتری دارند، قدرت و دقت تشخیص نفوذ را افزایش دهیم.

در این مقاله، تکنیک‌های افزایش قدرت و دقت تشخیص در سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری، تحلیل و ارزیابی می‌گردد. در ادامه، در بخش ۲ به مرور روش‌های تشخیص نفوذ بر اساس ناهنجاری و کاربردهای آن در مقالات پرداخته، سپس، در بخش ۳ به تحلیل الگوریتم‌ها، ابزارها و داده‌های استفاده‌شده در مقالات می‌پردازیم و در بخش ۴، نتیجه‌ای از مقالات و کارهای آینده بیان می‌شود.

۲- مرور بر روش‌های تشخیص نفوذ بر اساس ناهنجاری

همان‌طور که مطرح شد، حفظ امنیت داده‌ها و حریم خصوصی از مهم‌ترین دغدغه‌های سیستم‌های متصل به اینترنت است. از طرفی، با توجه به محدودیت شدید منابع دستگاه‌های اینترنت اشیا، باید از شیوه‌های کمتر وابسته به منابع و به عبارتی سبک‌وزن استفاده شود تا در حد امکان ضمن افزایش قدرت تشخیص نفوذ، حداقل بهره‌کشی از منابع را داشته باشیم. در شکل ۳ روش‌های مختلف، ارائه شده در مقالات برای تشخیص نفوذ در دستگاه‌های اینترنت اشیا بر اساس ناهنجاری دسته‌بندی شده است.



شکل (۳): تفکیک روش‌های تشخیص نفوذ بر اساس ناهنجاری در اینترنت اشیا.

۲-۱- یادگیری ماشین

به عنوان زیرمجموعه‌ای از هوش مصنوعی، الگوریتم‌های یادگیری ماشین یک مدل ریاضی بر اساس داده‌های نمونه یا داده‌های آموزش به‌منظور پیش‌بینی یا تصمیم‌گیری بدون برنامه‌ریزی آشکار، ایجاد می‌کنند و در طول زمان و تکرارهای مستمر پایگاه داده قوی‌تری می‌سازند و با توجه به الگوهای قبلی حالت‌های ناهنجار از هنجار را شناسایی و تشخیص می‌دهند. مزیت این روش در تشخیص حملات ناشناخته است.

حامد حدادپژوه و همکارانش، در تحقیقی [۹] معماری نوین دولایه با استفاده از شیوه‌های طبقه‌بندی ارائه داده و ادعا کرده‌اند که با استفاده از این روش، می‌توان قابلیت تشخیص را افزایش داد و از طرفی متناسب با منابع محدود دستگاه‌های اینترنت اشیا است. آنها با استفاده از روش‌های طبقه‌بندی چندلایه مدل جدیدی به نام TDTC را ارائه نمودند. همچنین، مجتبی اسکندری و همکارانش، در تحقیقی دیگر [۴] یک سامانه با عنوان پاسبان طراحی نموده‌اند.

تا قابلیت تشخیص نفوذهای ناشناخته را افزایش دهند و این سامانه را در برابر حملات چهارگانه به طور واقعی اجرا کردند که طبق نتایج حاصله، عملکرد قابل قبولی را ثبت کردند. در مقاله دیگری [۲] نویسندگان باز هم با استفاده از شیوه‌های یادگیری ماشینی و روش‌های تجزیه و تحلیل هسته، روشی پیشنهاد کردند تا موجب بهبود عملکرد سیستم در تشخیص نفوذهای جدید گردد. نویسندگان مقاله [۸] نیز با یک روش ابداعی طبقه‌بندی دوسطحی مبتنی بر یادگیری ماشینی ادعا نمودند که نرخ تشخیص را افزایش داده‌اند. در مقاله دیگری [۶] که در سال ۲۰۱۹م منتشر شده است، نویسندگان برای حفظ امنیت از الگوریتم‌های یادگیری ماشینی مانند جنگل تصادفی، K-نزدیک‌ترین همسایه و درخت تصمیم استفاده نمودند.

۲-۲- یادگیری عمیق

یادگیری ژرف یا ژرف‌آموزی بر مبنای مجموعه‌ای از الگوریتم‌ها است که یادگیرنده در تلاش است مفاهیم انتزاعی سطح بالا را در دادگان مدل نماید. این فرآیند را با استفاده از یک گراف عمیق که دارای چندین لایه پردازشی متشکل از چندین لایه تبدیلات خطی و غیرخطی هستند، مدل می‌کنند. در تحقیقی [۱۰] در سال ۲۰۲۲م، تانزیلا صباح با همکاری، یک مدل بر اساس یادگیری عمیق با استفاده از راهکارهای شبکه‌های عصبی پیچشی ارائه دادند و مدعی شدند که علاوه بر مراعات محدودیت‌های دستگاه‌های اینترنت اشیاء، قابلیت تشخیص نفوذهای ناشناخته را افزایش می‌دهد. سایرین [۱۱] و [۱۴] نیز از همین شیوه استفاده کرده‌اند.

۲-۳- روش ترکیبی

در این شیوه، با ترکیب روش‌های متداول به یک رویکرد جدید می‌رسند. در یک تحقیق [۵] کومار و همکارانش، با ترکیب الگوریتم‌های بهینه‌سازی گرگ خاکستری و ازدحام ذرات راهکار جدیدی ارائه نموده تا قدرت تشخیص حملات را افزایش دهند. همچنین، در سال ۲۰۲۲م در مقاله‌ای [۱] با استفاده از روش بهینه‌سازی یادگیری گروهی و روش یادگیری ماشینی یک مدل ارائه شده تا موجب افزایش دقت نرخ مثبت حقیقی گردد. در مقاله دیگری [۳] نویسنده با ترکیب قابلیت‌های سیستم‌های نفوذ مبتنی بر ناهنجاری و سیستم‌های نفوذ مبتنی بر مشخصه روشی ارائه می‌نماید و مدعی شده است که این روش موجب افزایش دقت تشخیص حمله فروچاله می‌گردد. در مقاله [۱۳] نیز با روش‌های ترکیبی به نتایج مناسبی دست یافته است.

۲-۴- شبکه‌های عصبی

در این روش، با الگوبرداری از سیستم مغز انسان یک شبکه عصبی مصنوعی جهت تولید الگوریتم آموزشی تولید می‌شود. در مقاله‌های [۷] و [۱۵] استفاده از روش‌های شبکه‌های عصبی سبک وزن، یک مدل جدید جهت افزایش قدرت تشخیص حملات ارائه می‌کند. در ادامه به تحلیل و ارزیابی الگوریتم‌ها، داده‌ها، ویژگی‌های مهم و ابزارهای مورد استفاده، پرداخته می‌شود.

۳- مجموعه داده

طراحی یک مجموعه داده پهباد مستلزم تفکر دقیق در مورد استراتژی جمع‌آوری داده، پروتکل پرواز پهباد و انتخاب کلاس شیء برای حاشیه‌نویسی است. کل فرآیند با در نظر گرفتن سودمندی و اثربخشی برای تحقیق تقسیم‌بندی معنایی پهباد طراحی شده است که ما از آن استفاده می‌کنیم. در این بخش، نحوه ایجاد مجموعه داده از تصاویر گرفته‌شده توسط پهباد نشان داده شده است. بخش ۳-۱ راهبرد کسب داده را نشان می‌دهد. بخش ۳-۳ و ۳-۴ به ترتیب کلاس‌های کار و روش‌های حاشیه‌نویسی را شرح می‌دهد. بخش ۳-۵ تقسیم‌بندی داده‌ها را برای وظیفه تقسیم‌بندی معنایی نشان می‌دهد.

۳-۱- مشخصات داده‌ها

روش کسب داده و حاشیه‌نویسی برای تقسیم‌بندی معنایی پهباد در صحنه‌های شهری پیچیده طراحی شده است که دارای قابلیت تشخیص شیء ثابت و متحرک است. ویژگی‌های زیر برای مجموعه داده‌ها در نظر گرفته شده است که به شرح زیر است:

نمای مایل: برای پلتفرم پهباد، ضبط تصاویر یا ویدئوها در یک نمای مایل یا در نمای نادر طبیعی است. نماهای نادر تصاویر ماهواره‌ای رایج است؛ زیرا فاصله بین دوربین تا زمین زیاد است. نماهای نادر برای نمایش اشیاء، در تصویر تغییرناپذیری ایجاد می‌کند، زیرا فقط قسمت بالای اشیاء را می‌توان مشاهده کرد. با این حال، نمایش محدود هم‌چنین، باعث سردرگمی در تشخیص شیء در بیناشیای مختلف می‌شود. در مقابل، یک نمای مایل نمایش متنوعی از اشیاء با زمینه صحنه غنی را ارائه می‌دهد که می‌تواند برای تشخیص شیء مفید باشد. هنگامی که پهباد در فاصله‌ی نزدیک‌تر به زمین پرواز می‌کند، می‌توان ناحیه بزرگ‌تری با جزئیات بیشتر مشاهده کرد که باعث ایجاد تنوع در مقیاس بزرگ در یک تصویر می‌شود. برای مشاهده در نمای مایل، زاویه دوربین در حدود ۶۵ درجه نسبت به جهت عمودی تنظیم می‌شود.

و ضوح بالا: حالت ضبط ویدئو با وضوح K4 را با ارتفاع پرواز ایمن در حدود ۵۰ متر اتخاذ شده است. توجه داشته باشید قالب تصاویر ضبط شده در ارتفاع ۳۰ متری از سطح زمین است. وضوح تصویر ۴۰۹۶×۲۱۶۰ یا ۶۰۰۰×۴۰۰۰ است. در این تنظیمات که از نظر بصری تصویر به اندازه کافی واضح است برای متمایز کردن بیشتر اشیاء، اجسامی که به صورت افقی دور هستند، نیز قابل شناسایی هستند. علاوه بر این، حتی می‌توان انسان‌هایی را که در نزدیکی پهباد قرار دارند، شناسایی کرد.

برچسب زدن متوالی: مجموعه داده‌های موجود، برای وظیفه تقسیم‌بندی معنایی طراحی شده است که ترجیح می‌دهیم تصاویر را در یک دنباله برچسب‌گذاری کنیم؛ جایی که بتوان ثبات پیش‌بینی را ارزیابی کرد. از آن جایی که برچسب‌گذاری متراکم در فضای زمانی بسیار پرهزینه است، روش ارائه‌شده توسط ما به این صورت است که ۱۰ تصویر را با فاصله ۵ ثانیه در هر دنباله برچسب‌گذاری می‌کنیم.

صحنه‌های پیچیده و پویا با اشیاء متنوع: مجموعه داده مورد استفاده ما با هدف دستیابی به پیچیدگی صحنه در دنیای واقعی طراحی شده است. به طور مثال، صحنه‌های نزدیک خیابان‌ها برای مجموعه داده‌های شناسه پهباد انتخاب

شده‌اند؛ زیرا به اندازه کافی پیچیده هستند و فعالیت‌های انسانی پویاتری دارند. اشیاء مختلفی در صحنه ظاهر می‌شوند؛ مانند اتومبیل‌ها، عابران پیاده، ساختمان‌ها، جاده‌ها، پوشش گیاهی و غیره.

تنوع داده‌ها: در مجموع، ۳۰ توالی ویدئویی کوچک پهپاد در ۲۰ مکان مختلف گرفته شده است. جمع‌آوری داده‌ها در شرایط آب‌وهوایی خوب با روشنایی کافی انجام شد. داده‌های به‌دست‌آمده در محیط‌های تاریک یا سایر شرایط آب‌وهوایی مانند بارش برف یا باران به تکنیک‌های پردازش خاصی نیاز دارند که مجموعه داده‌های فعلی ما بر این مورد تمرکز ندارد.

DJI Phantom 3 Pro و DJI Phantom 4 پهپادهای سبک‌وزن مدرنی هستند که برای جمع‌آوری داده‌ها مورد نیاز ما استفاده می‌شود. پهپادها به طور پیوسته با حداکثر سرعت پرواز ۱۰ متر بر ثانیه پرواز می‌کنند. دوربین‌های پیش‌فرض نصب‌شده بر روی پهپادها برای دریافت ویدئو فقط با کانال‌های RGB استفاده می‌شوند.

۳-۲- اندازه‌ی مجموعه داده

شنا سه مجموعه داده‌های پهپاد ما دارای ۴۰۰ تصویر و هر کدام به اندازه ۴۰۹۶×۲۱۶۰ یا ۶۰۰۰×۴۰۰۰ است. برای مقایسه‌ی اندازه‌ی مجموعه داده‌های مختلف برای تقسیم‌بندی معنایی، نه تنها تعداد تصاویر، بلکه اندازه‌ی هر تصویر را باید در نظر بگیریم. یک معیار اصولی‌تر، مقایسه تعداد پیکسل‌های برچسب‌گذاری شده در کل داده‌ها است که ما چندین مجموعه داده‌ی تقسیم‌بندی معنایی شناخته‌شده را برای مقایسه انتخاب می‌کنیم. مجموعه داده [۳] CamVid دارای ۷۰۱ تصویر با اندازه ۹۶۰×۷۲۰ است که تنها یک پنجم مجموعه داده‌های ما از نظر تعداد پیکسل‌های برچسب‌گذاری شده است. مجموعه داده گول‌پیکر Cityscapes [۱] دارای ۵۰۰۰ تصویر با اندازه ۲۰۴۸×۱۰۲۴ است که ۴ برابر بزرگ‌تر از مجموعه داده‌های پهپاد ما هست. با این حال، بسیاری از اشیاء در تصاویر ما کوچک‌تر از آنها هستند، واریانس بیشتر، شیء در همان تعداد پیکسل را در تشخیص شیء در یک درجه بیشتر جبران می‌کند. در بخش ۶ نشان داده است که روش‌های یادگیری عمیق می‌توانند به نتایج کمی و کیفی رضایت‌بخشی برای اهداف تجربی دست یابند که قابلیت استفاده از شناسه مجموعه داده‌های پهپاد ما را بیشتر اثبات می‌کند.

۳-۳- تعریف کلاس و تجزیه و تحلیل آماری

برچسب زدن کامل انواع اشیاء در صحنه خیابان در یک تصویر پهپاد $k4$ به‌سیار پرهزینه است. در نتیجه، فقط رایج‌ترین و معروف‌ترین نوع اشیاء برای مجموعه داده فعلی ما برچسب‌گذاری می‌شوند. در مجموع، ۸ کلاس کلی برای تقسیم‌بندی معنایی انتخاب شده است؛ یعنی ساختمان (دیوار و پنجره و ...)، جاده، درخت، پوشش گیاهی کوتاه، ماشین ساکن، ماشین متحرک، انسان، نمونه‌هایی از کلاس‌های مختلف هستند.

۳-۴- روش حاشیه‌نویسی

برای تصاویر پهپاد با وضوح بالا حاشیه‌نویسی‌های دقیق با برچسب‌گذاری متراکم، ارائه داده‌ایم که همه برچسب‌ها، با ابزار برچسب‌زنی ما به‌دست می‌آیند. تقریباً ۱۲۰ دقیقه طول می‌کشد تا همه پیکسل‌ها در یک تصویر برچسب‌گذاری شوند. روش‌های حاشیه‌نویسی سطح پیکسل، سطح سوپر پیکسل و سطح چندضلعی برای حاشیه‌نویس‌ها، همان‌طور که در شکل ۱ نشان داده شده است. برای حاشیه‌نویسی سطح سوپر پیکسل، در روش ما از یک استراتژی مشابه به

عنوان مجموعه داده COCO-Stuff [۷] استفاده می‌شود. ابتدا از روش SLIC [۸] برای تقسیم کردن تصویر به سوپرپیکسل‌ها استفاده می‌کنیم که هر کدام گروهی از پیکسل‌ها هستند و از نظر فضایی به هم متصل هستند و ویژگی‌های مشابه مانند رنگ و بافت دارند. از آن جایی که ممکن است اشیاء هم‌پوشانی داشته باشند، پیکسل‌های هم‌پوشانی را به عنوان کلاسی که به دوربین نزدیک‌تر است، برچسب‌گذاری می‌کنیم.



شکل (۴): روش‌های حاشیه‌نویسی سمت چپ حاشیه‌نویسی سطح پیکسل، وسط حاشیه‌نویسی سطح فوق پیکسل، و سمت راست حاشیه‌نویسی سطح چندضلعی را نشان می‌دهد.

۳-۵- تقسیم مجموعه داده‌ها

کل ۳۰ دنباله ویدئویی با برچسب متراکم به بخش‌های آموزشی، اعتبارسنجی و تقسیم‌بندی آزمایشی تقسیم می‌شوند. ما داده‌ها را کاملاً تصادفی تقسیم نمی‌کنیم، بلکه هر تقسیم‌بندی به اندازه کافی برای تنوع صحنه‌های مختلف، نماینده‌ی داده‌ها است. هر سه تقسیم باید شامل همه کلاس‌ها باشد. داده‌های ما در سطح سکانس تقسیم می‌شوند و هر سکانس از محل صحنه متفاوتی می‌آید. با پیروی از این طرح، ما به ترتیب ۱۵ دنباله آموزشی (۱۵۰ تصویر برچسب‌گذاری شده) و ۵ دنباله اعتبارسنجی (۵۰ تصویر برچسب‌گذاری شده) برای تقسیم‌های آموزشی و اعتبارسنجی دریافت می‌کنیم. تقسیم آزمایشی شامل ۲۰ دنباله سمت چپ (۲۰۰ تصویر برچسب‌دار) است. نسبت اندازه بین آموزش، اعتبارسنجی و تقسیم آزمون ۴:۱:۳ است.

۴- وظیفه برچسب‌گذاری معنایی

در این بخش، وظیفه برچسب‌گذاری معنایی برای مجموعه داده ما تشریح می‌شود. بخش ۴-۲- شبکه‌های عصبی عمیق را در روش‌های پایه معرفی می‌کنند، بخش ۴-۳- منظم‌سازی مکانی و زمانی را معرفی می‌کنند که عملکرد را برای همه روش‌های پایه افزایش می‌دهد.

۴-۱- وظیفه و متریک

وظیفه تعریف‌شده در شناسه مجموعه داده‌های پهباد، پیش‌بینی برچسب‌گذاری معنایی سطح پیکسل برای تصاویر پهباد است. عملکرد برچسب‌گذاری معنایی بر اساس معیار استاندارد IOU [۹] ارزیابی می‌شود. هدف این کار دستیابی به بالاترین میانگین امتیاز IOU تا حد امکان است. برای شناسه مجموعه داده‌های پهباد، کلاس Clutter تعداد

پیکسل نسبتاً زیادی دارد و از اشیاء معنادار تشکیل شده است که به جای نادیده گرفته شدن، به عنوان یک کلاس برای آموزش و ارزیابی در نظر گرفته می‌شود.

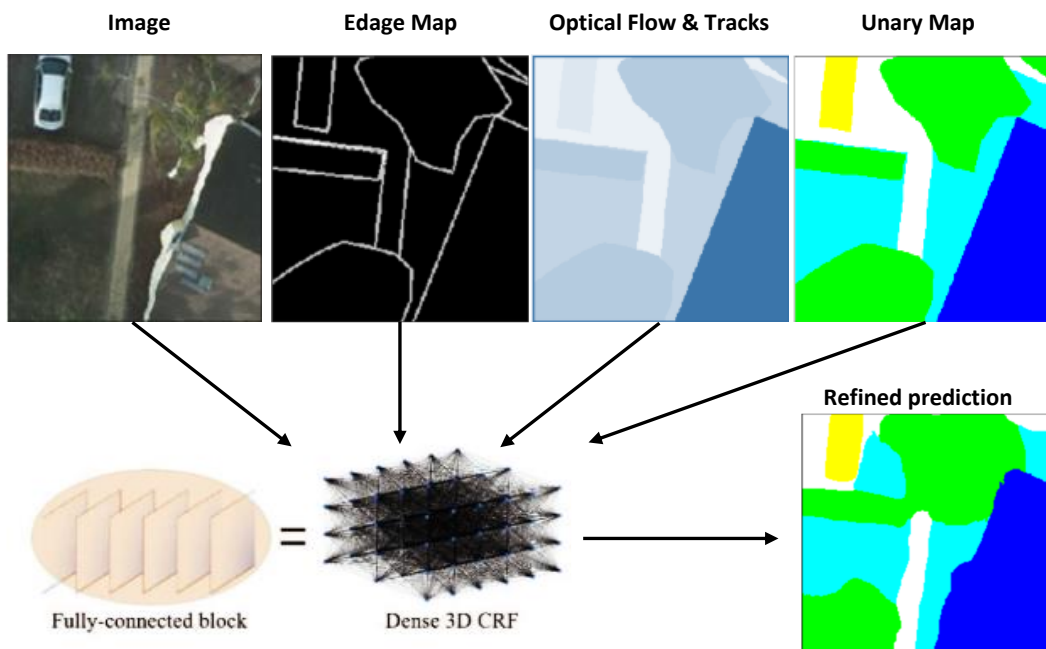
۲-۴- شبکه‌های عصبی عمیق برای خطوط پایه

به منظور ارائه مراجع عملکرد و آزمایش قابلیت استفاده از شناسه مجموعه داده‌های پهباد ما برای کار برچسب گذاری معنایی، چندین مدل یادگیری عمیق را برای پیش‌بینی تصویر واحد آزمایش کرده‌ایم. اگرچه ماشین‌های ساکن و ماشین‌های متحرک را نمی‌توان از نظر ظاهری تنها از یک تصویر متمایز کرد، اما هنوز هم می‌توان بر اساس زمینه آنها استنباط کرد. ما با سه شبکه عصبی کاملاً پیچیده عمیق و پُر کاربرد شروع می‌کنیم. آنها FCN-8s [۴]، شبکه Dilution [۵] و U-Net [۶] هستند. FCN-8s اغلب یک نامزد پایه خوب برای تقسیم‌بندی معنایی بوده است. این یک مدل عظیم با قابلیت استخراج ویژگی‌های قوی و مؤثر است، در عین حال، ساختار ساده‌ای دارد. U-Net یک شبکه رمزگذار-رمزگشا متقارن معمولی است که در اصل برای تقسیم‌بندی در تصاویر پزشکی طراحی شده است. U-Net نیز از نظر ساختار ساده است؛ اما در حفظ مرزهای اشیاء خوب است.

Multi-Scale-Dilation برای یک تصویر با وضوح بالا است که توسط یک پهباد در یک نمای مایل گرفته می‌شود که به طور چشم‌گیری اندازه اشیاء در فواصل مختلف می‌تواند متفاوت باشد. در مجموع سه جریان برای سه مقیاس ایجاد می‌شود که برای هر جریان، یک FCN-8s اصلاح شده به عنوان ساختار اصلی استفاده می‌شود که در آن عمق برای هر بلوک کانولوشن به دلیل محدودیت حافظه کاهش می‌یابد. در اینجا، عمق فیلتر، قربانی مقیاس‌های بیش‌تر می‌شود. به منظور کاهش از دست دادن جزئیات در استخراج ویژگی، لایه ادغام در بلوک کانولوشن پنجم حذف می‌شود تا یک میدان پذیرنده کوچک‌تر حفظ شود. در عوض، ویژگی‌هایی با میدان‌های دریافتی بزرگ‌تر از جریان‌های دیگر از طریق اتصال پرش در لایه‌های conv7 به ویژگی‌های وضوح بالاتر الحاق می‌شوند. به این ترتیب، هر جریانی استخراج ویژگی را در مقیاس خاص خود انجام می‌دهد و ویژگی‌های مقیاس‌های بزرگ‌تر برای تقویت پیش‌بینی برای جریان‌های با وضوح بالاتر تجمیع می‌شوند. مقیاس‌های چندگانه نیز ممکن است با نمونه‌برداری مستقیم تصاویر به دست آیند. با این حال، سه مزیت برای پردازش چند مقیاسی ما وجود دارد. ابتدا، هر پیکسل به یک دسته در فضای به عملیات دسته‌ای اختصاص داده می‌شود و تمام پیکسل‌های برچسب گذاری شده باید برای هر مقیاس بدون ضایعات استفاده شوند. دوم، تراز دقیقی بین جفت‌های برچسب تصویر در هر مقیاس وجود دارد، زیرا هیچ ترکیبی از پیکسل‌های تصویر و یا ترکیبی از پیکسل‌های برچسب وجود ندارد. و سوم اینکه، ویژگی‌های الحاقی در لایه Conv7 نیز کاملاً در یک راستا قرار دارند. برای هر مقیاس، برچسب‌های حقیقت زمینی متناظر نیز می‌توانند از طریق عملیات فضایی به دسته‌ای به همان شیوه تولید تصاویر ورودی در جریان‌های مختلف تولید شوند. با برچسب‌های حقیقت زمینی برای هر مقیاس، آموزش عمیقاً نظارت‌شده می‌تواند انجام شود. تلفات در هر سه مقیاس باعث دست‌دادن آنتروپی متقاطع می‌شود.

۴-۳- منظم‌سازی مکانی - زمانی

برای برچسب‌گذاری معنایی، بیشتر این موضوع بررسی می‌شود که چگونه یک نظم مکانی - زمانی می‌تواند پیش‌بینی را بهبود بخشد. استفاده از اطلاعات زمانی برای پیش‌بینی برچسب برای داده‌های توالی ارزشمند است. به طور معمول، شبکه‌های عصبی عمیقاً آموزش داده شده بر روی تصاویر منفرد نمی‌توانند پیش‌بینی‌های کاملاً منسجمی را در چندین فریم ارائه دهند. با این حال، فریم‌های مختلف مشاهداتی را از موقعیت‌های مختلف مشاهده ارائه می‌دهند که از طریق آنها می‌توان سرنخ‌های متعددی برای پیش‌بینی اشیاء جمع‌آوری کرد. برای استفاده از اطلاعات زمانی در شناسه مجموعه داده‌های پهباد، از روش بهینه‌سازی فضای ویژگی (FSO) [۱۱] برای پیش‌بینی داده‌های توالی استفاده می‌کنیم. این پیش‌بینی برچسب نهایی را برای کل دنباله با اعمال CRF سه‌بعدی که هر دو حوزه مکانی و زمانی را پوشش می‌دهد، صاف می‌کند. این روش از جریان نوری و ردیابی برای پیوند دادن پیکسل‌ها در حوزه زمانی بهره می‌برد. کل پس‌پردازش به ورودی‌های داده‌های متعددی نیاز دارد، از جمله تصویر، نقشه یکپارچه از شبکه‌های عصبی عمیق، نقشه لبه، جریان نوری، و مسیرهایی که در شکل ۵ نشان داده شده است.



شکل (۵): ورودی‌های داده برای روش پس‌پردازش FSO [۱۱]. تصویر، نقشه لبه، نقشه یکپارچه، جریان نوری و مسیره‌ها برای روش موردنیاز هستند. نقشه لبه احتمال یال بودن هر پیکسل را نشان می‌دهد. نقاط آبی در تصویر (دومی از سمت راست) جریان نوری و مسیره‌ها، نقاط ردیابی شده را مشخص می‌کنند. نقشه واحد، احتمالات کلاس برای هر پیکسل است که توسط شبکه‌های عصبی عمیق پیش‌بینی می‌شود.

۵- آزمایش

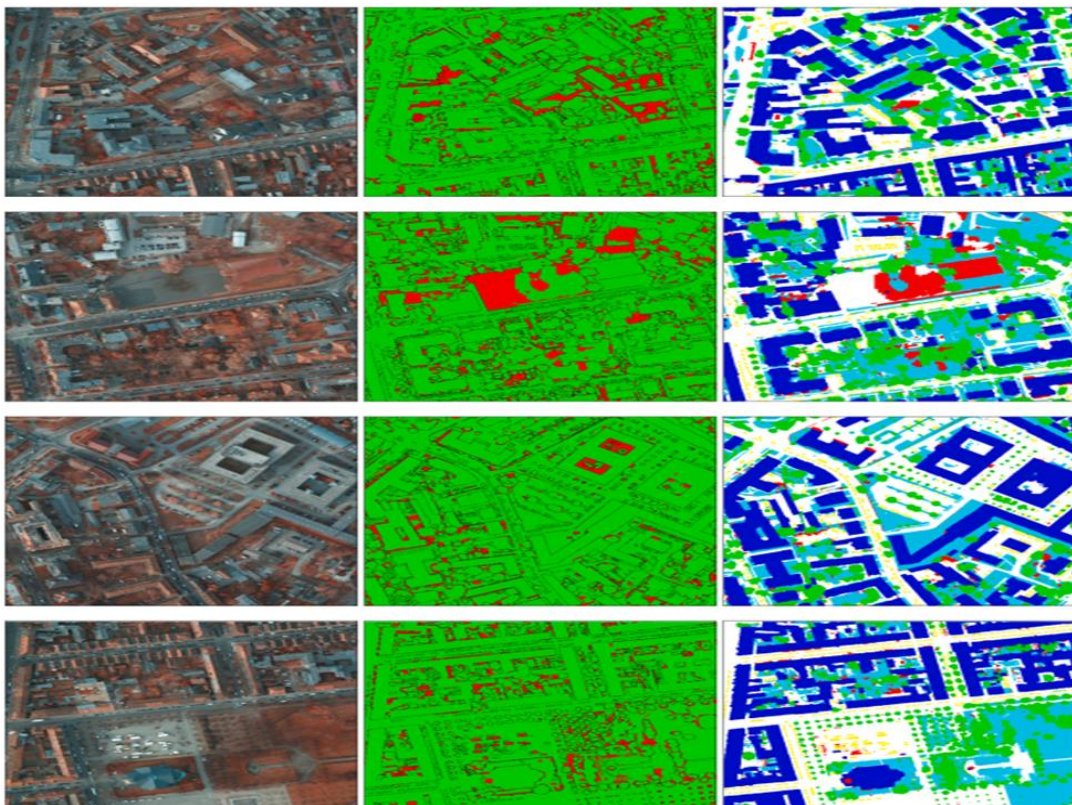
آزمایش‌های ما به سه قسمت تقسیم شده است. ابتدا، ما نتایج تقسیم‌بندی معنایی را با آموزش شبکه‌های عصبی عمیق از ابتدا مقایسه می‌کنیم. در مرحله دوم، ما تجزیه و تحلیل می‌کنیم که چگونه مدل‌های از پیش آموزش‌دیده می‌توانند برای کار برچسب زدن معنایی شناسه پهیاد مفید باشند. در نهایت، تأثیر تنظیم مکانی - زمانی با استفاده از روش FSO برای بخش‌بندی ویدئوی معنایی بررسی می‌شود. اندازه تصاویر پهیاد ما بسیار بزرگ است. در نتیجه، هر تصویر پهیاد را به ۹ تصویر کوچک‌تر با توزیع یکنواخت برش می‌دهیم که کل تصویر را برای آموزش پوشش می‌دهند. هر تصویر برش‌خورده در اندازه 1024×2048 است.

۵-۱- از ابتدا آموزش می‌دهیم

برای مقایسه منصفانه بین شبکه‌های مختلف، همه شبکه‌ها را با Tensorflow [۱۰] دوباره پیاده‌سازی می‌کنیم و همه شبکه‌ها با یک GPU Nvidia TitanX آموزش داده می‌شوند. به منظور قرار دادن شبکه‌ها در حافظه GPU 12G، عمق برخی از لایه‌ها در شبکه U-Net، Dilatation و MSDilationnet کاهش می‌یابد تا حداکثر در حافظه جا شود. همه مدل‌ها با بهینه‌ساز Adam برای ۲۷K تکرار (۲۰ دوره) آموزش‌دیده‌اند. نرخ یادگیری پایه روی ۴-۱۰ تنظیم شده است که به صورت تصاعدی به ۷-۱۰ کاهش می‌یابد. کاهش وزن برای همه وزن‌ها در هسته‌های کانولوشن روی ۵-۱۰ تنظیم شده است. همه شبکه‌ها به صورت سرتا سر آموزش داده می‌شوند و میانگین نمرات IOU به دست آمده به درصد گزارش می‌شود. برای هر چهار شبکه، آنها در تمایز طبقات ساختمان، جاده و درختان بهتر عمل می‌کنند و به امتیازات IOU بالاتر از ۵۰ درصد می‌رسند.

۵-۲- تنظیم دقیق مدل‌های از پیش آموزش‌دیده

برای تنظیم دقیق، همه شبکه‌ها با مجموعه داده‌های منظر شهری [۱] از قبل آموزش‌داده شده‌اند. داده‌های حاشیه‌نویسی دقیق از تقسیم‌بندی آموزشی و اعتبارسنجی استفاده می‌شود که در مجموع شامل ۳۴۵۰ تصویر با برچسب متراکم است. در مرحله بعد، تمام شبکه‌ها با داده‌های شناسه مجموعه داده‌های پهیاد به خوبی تنظیم می‌شوند. نرخ یادگیری روی ۵-۱۰ تنظیم شده است که به صورت تصاعدی به ۷-۱۰ برای FCN-8 کاهش می‌یابد، و ۴-۱۰ به طور نمایی به ۷-۱۰ برای ۳ شبکه دیگر کاهش می‌یابد، زیرا آنها به راحتی در حداقل محلی با نرخ یادگیری اولیه گیر می‌کنند. ۷-۱۰ در طول تمرین. جدا کردن فیلترها با مقیاس‌های مختلف زمانی می‌تواند مفید باشد که اشیاء در مقیاس بزرگ ظاهر شوند. به منظور مشاهده اثر پردازش در مقیاس چندگانه، مقایسه عملکرد کیفی بین FCN-8، شبکه U-Net، Dilatation و MS-Dilation Net در شکل ۶ ارائه شده است.



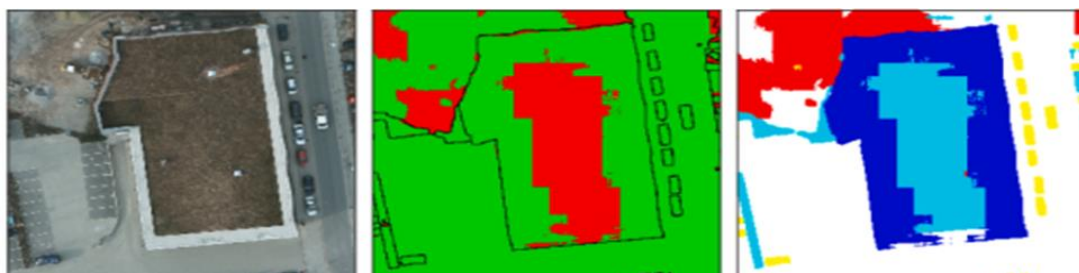
شکل (۶): نمونه پیش‌بینی FCN8s (ردیف اول)، شبکه Dilation (ردیف دوم)، U-Net (ردیف سوم) و MS-Dilation Net (ردیف چهارم).

۵-۳- منظم‌سازی مکانی - زمانی برای تقسیم‌بندی معنایی

برای منظم‌سازی مکانی و زمانی، از روش‌های مورد استفاده در بهینه‌سازی فضای ویژگی (FSO) استفاده می‌کنیم [۱۱]. همان‌طور که FSO یک بلوک از تصاویر را به‌طور همزمان پردازش می‌کند، یک بلوک از ۵ فریم متوالی با فاصله ۱۰ فریم از فایل‌های ویدیویی ارائه شده استخراج می‌شود و تصویر آزمایشی در مرکز هر بلوک قرار می‌گیرد. شکاف بین فریم‌های متوالی خیلی زیاد نیست تا بتوان جریان مناسب را استخراج کرد. امتیاز IoU برای پردازش پس از FSO با Unary map از شبکه‌های مختلف تنظیم شده در جدول ۱ گزارش شده است. برای هر مدل، حدود ۱٪ بهبود امتیاز IOU برای هر کلاس جداگانه وجود دارد، به جز برای کلاس‌های انسان و ماشین‌های متحرک. FSO بیشتر برای کلاسی که نمونه آن پیکسل‌های تصویر بیشتری را پوشش می‌دهد. امتیاز IOU کلاس انسانی برای شبکه MS-Dilation با حاشیه زیادی، نزدیک به ۴٪ کاهش می‌یابد. نمونه‌ای از پالایش در شکل ۷ نشان داده شده است.

جدول (۱): IOU برای استراتژی‌های آموزشی مختلف امتیاز می‌گیرد. نمرات IOU به‌صورت درصد گزارش شده و بهترین نتایج به صورت پُررنگ نشان داده شده است. w مخفف with و w/o مخفف without است.

Model	Buliding	Tree	Clutter	Rroad	Low Vegetation	Static Car	Moving Car	Human	Mean IOH
Fine-Tune W/O AuXiliary Loss	97.5	94.2	94	95.3	91.5	95.4	92.5	91.2	93.75
Fine-Tune W AuXiliary Loss	98.2	94.5	94.8	96.6	92.3	95	93.8	93.4	94.82
Fine-Tune W+W/O AuXiliary Loss	98.4	95.1	93.7	97.7	93.3	98.3	95.8	96.3	96.75



شکل (۷): نمونه‌هایی از منظم‌سازی مکانی و زمانی برای تقسیم‌بندی معنایی شناسه تصویر پهپاد (تصویر سمت چپ تصویر اصلی ما است تصویر وسط پیش‌بینی را بدون اصلاح FSO به‌علاوه DCRF^۳ نشان می‌دهد. ستون سمت راست پیش‌بینی تصفیه‌شده مربوطه را با پالایش FSO به‌علاوه DCRF^۳ نشان می‌دهد).

۶- مقایسه و ارزیابی نتایج

در بحث مقایسه با دیگر کارهای انجام شده در تقسیم‌بندی معنایی تصاویر پهپاد در مقاله تجزیه و تحلیل عملکرد الگوریتم‌های تقسیم‌بندی معنایی برای مجموعه داده‌های ویدئویی هوایی پهپاد جدید با حاشیه‌نویسی دقیق (ManipalUAVid) برای تقسیم‌بندی معنایی با دقت پیکسل (0.90, FCN)، (0.93, CRF)، (0.92, U-Net) و (0.91, DeepLabV3C) دست یافته‌اند. هم‌چنین، در مقاله تقسیم‌بندی معنایی پیشرفته ویدئوهای هوایی پهپاد با جاسازی اطلاعات زمانی برای تقسیم‌بندی معنایی با استفاده از مدل پیشنهادی معماری CNN مبتنی بر رمزگذار-رمزگشا به دقت ۰/۷۹ در صد دست یافته‌اند که مدل ترکیبی پیشنهادی ما از نظر دقت نسبت به کار دیگران میانگین ۹۶/۷۵ داشته است که خروجی هر کلاس در جدول ۱ منتشر شده است.

۷- نتیجه‌گیری

در این مقاله، ما یک شناسه‌ی مجموعه‌ی داده‌های پهپاد جدید برای پیشبرد توسعه بخش‌بندی معنایی در صحنه‌های خیابان شهری از تصاویر پهپاد ارائه کرده‌ایم. مجموعه‌ی داده‌ی ما چندین چالش را برای کار تقسیم‌بندی معنایی به همراه داشته است، از جمله، تنوع در مقیاس بزرگ برای اشیاء مختلف، تشخیص شیء متحرک در صحنه‌های خیابان، و سازگاری زمانی در فریم‌های متعدد. هشت کلاس برای وظیفه برچسب‌گذاری معنایی تعریف و برچسب‌گذاری شده است. قابلیت استفاده از شناسه مجموعه داده‌های پهپاد ما نیز با چندین شبکه عصبی کانولوشنال عمیق ثابت شده است. در میان آنها شبکه اتساع چند مقیاسی پیشنهادی بهترین عملکرد را از طریق استخراج ویژگی

چند مقیاسی دارد. همچنین، نشان داده شده است که پیش آموزش شبکه و اعمال منظم سازی مکانی - زمانی برای کار برچسب گذاری معنایی شناسه پهناد مفید است. اگرچه شناسه ی مجموعه ی داده های پهناد دارای محدودیت هایی در اندازه و تعداد کلاس ها در مقایسه با بزرگ ترین مجموعه ی داده در جامعه بینایی کامپیوتر است، مجموعه داده شناسه UAV در حال حاضر می تواند برای مقاصد معیار استفاده شود. در آینده، می خواهیم مجموعه داده ها را از نظر اندازه و تعداد دسته ها بیشتر گسترش دهیم تا برای پیشبرد تحقیقات تقسیم بندی معنایی برای تصاویر پهناد چالش برانگیز تر و مفید تر شود.

منابع:

- [1] Cordts, M., Omran, M., Ramos, S., Rehfeld, T., Enzweiler, M., Benenson, R., Franke, U., Roth, S., and Schiele, B., "The cityscapes dataset for semantic urban scene understanding," In CVPR, 2016.
- [2] Rottensteiner, F., Sohn, G., Gerke, M., Wegner, J. D., Breitkopf, U., and Jung, J., "Results of the isprs benchmark on urban object detection and 3d building reconstruction," ISPRS journal of photogrammetry and remote sensing, Vol. 93, pp. 256–271, 2014.
- [3] Brostow, G. J., Shotton, J., Fauqueur, J., and Cipolla, R., "Segmentation and recognition using structure from motion point clouds. In ECCV, pp. 44–57, 2008.
- [4] Long, J., Shelhamer, E., and Darrell, T., "Fully convolutional networks for semantic segmentation," In CVPR, June 2015.
- [5] Yu, F., and Koltun, V., "Multi-scale context aggregation by dilated convolutions," In ICLR, 2016.
- [6] Ronneberger, O., Fischer, P., and Brox, T., "U-net: Convolutional networks for biomedical image segmentation," In MICCAI, pp 234–241, 2015.
- [7] Caesar, H., Uijlings, J., and Ferrari, V., "Cocostuff: Thing and stuff classes in context," In CVPR, June 2018.
- [8] Achanta, R., Shaji, A., Smith, K., Lucchi, A., Fua, P., Susstrunk, S., et al, "Slic superpix- els compared to state-of-the-art superpixel methods," PAMI, Vol. 34, No. 11, pp 2274–2282, 2012.
- [9] Everingham, V., Eslami, S. M. A., Van Gool, L., Williams, C. K. I., Winn, J., and Zisserman, A., "The pascal visual object classes challenge: A retrospective," IJCV, Vol. 111, No. 1, pp 98–136, Jan. 2015.
- [10] Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., et al, "Tensorflow: a system for large-scale machine learning," In OSDI, Vol. 16, pp 265–283, 2016.
- [11] Kundu, A., Vineet, V., and Koltun, V., "Feature space optimization for semantic video segmentation," In CVPR, pp 3168–3175, 2016.

تعیین ابعاد عملیات سایبری در نیروهای نظامی، دسته‌بندی تهدیدات و حوزه‌های کاربری آنها

فرهاد فرنی^۱، مهرداد نجفی نوکاشتی^۲، تورج قهرمانی^۳

۱- دانشجوی دکترا، ۲- دانشجوی دکترا و عضو هیات علمی دانشگاه افسری و تربیت پاسداری امام حسین(ع)، ۳- دانشجوی دکترا

چکیده:

با ورود سایبر به عملیات نظامی و تشکیل عرصه پنجم صحنه نبرد، تعاریف و حوزه‌های رزم منحصر به فردی را ایجاد کرده است. یکی از تعاریف مهم ایجاد شده، سایبرالکترومغناطیس نظامی است که در کنار عملیات سایبر و عملیات جنگ الکترونیک مورد استفاده قرار می‌گیرد. در این تحقیق، پس از بررسی علمی و دقیق ابعاد سایبر در حوزه نظامی و بیان قابلیت‌ها و تفاوت‌های یاد شده، متناسب با مراجع و گزارش‌های منتشر شده، نمونه‌ای از کاربردهای آنها در عملیات نظامی مورد توجه قرار گرفته است. این تحقیق از نظر هدف، کاربردی-توسعه‌ای و از نظر شیوه‌ی گردآوری داده‌ها، توصیفی-موردی است. به منظور گردآوری داده‌ها، از منابع کتابخانه‌ای، اسناد و گزارشات علمی داخلی و خارجی استفاده شده و رویکرد مورد استفاده برای تجزیه و تحلیل داده‌ها نیز از نوع کیفی است. نتایج حاصل از این تحقیق نشان می‌دهد، عملیات سایبرالکترومغناطیس به عنوان یک بُعد، جدای از عملیات سایبر و عملیات جنگ الکترومغناطیس در نظر گرفته می‌شود؛ برای مقابله با تهدیدات منشعب شده از این بُعد، باید تفاوت‌ها و اشتراک‌های مابین بُعد سایبرالکترومغناطیس را با دو بُعد دیگر شناخت و مرز شفاف‌تری را برای این سه بُعد و اشتراکات آنها ترسیم کرد.

کلید واژه‌ها: سایبرالکترومغناطیس، عملیات سایبری، عملیات جنگ الکترومغناطیس.

Determining the dimensions of cyber operations in military forces, categorizing threats and their areas of use

¹Farhad farnia*, ²Mehrdad Najafi Nokashti, ³Toraj Ghahramani,

1- Ph.D Student in Cyber Defense, 2- Ph.D Student in Cyber Defense, 3- M.S in management

Abstract

With the introduction of cyber into military operations and the formation of the fifth battlefield, it has created unique definitions and areas of combat. One of the important definitions created is military cyber-electromagnetism, which is used alongside cyber operations and electronic warfare operations. In this research, after the scientific and detailed examination of cyber dimensions in the military field and the expression of the capabilities and differences of the mentioned dimensions in accordance with the published references and reports, an example of their applications in military operations has been considered. This research is applied-developmental in terms of purpose and descriptive-case in terms of data collection method. In order to collect data, internal and external library sources, documents and scientific reports were

* نویسنده مسئول: نویسنده اول

used, and the approach used for data analysis was qualitative and in-depth interviews with 12 specialists and university professors in the field of cyberelectromagnetism. The results of this research show that cyber-electromagnetic operations are considered as a separate dimension from cyber operations and electromagnetic warfare operations and have common limits with the two mentioned dimensions; The differences and commonalities between the cyberelectromagnetic dimension and the other two dimensions have been explained and the border between the cyberelectromagnetic dimension and other dimensions has been clearly defined.

Keywords: Cyber-electromagnetic, cyber operation, electromagnetic warfare operation

۱- مقدمه

با پیشرفت فناوری و ورود تعاریف فضای سایبری به حوزه‌ی نظامی، علاوه بر در نظر گرفتن حوزه‌ی سایبری به عنوان عرصه‌ی پنجم صحنه‌ی نبرد، عامل توانمندسازی سایر عرصه‌های زمینی، هوایی، دریایی و فضایی نیز شناخته شد [۱]. در سال‌های اخیر تلاش‌های زیادی برای ایجاد یک تعریف مشخص و مأموریت خاص نظامی به‌ویژه در ترکیب با سایر حوزه‌های عملیاتی صورت گرفت و به تبع آن به دنبال توسعه این مفهوم، واژه‌ها و تعاریف جدیدی ایجاد گردید. یکی از پُرکاربردترین و در عین حال پُرچالش‌ترین واژه‌های ایجادشده، واژه سایبرالکترومغناطیس است که اولین بار توسط وزارت دفاع آمریکا در سال ۲۰۱۴م تحت عنوان اقدامات سایبرالکترومغناطیس (CEMA)^۱ مورد بررسی و تعریف قرار گرفت [۲]. پیرو تعریف CEMA، ساختار سازمانی و یگان‌های عملیات سایبری تحت عنوان فرماندهی سایبری (CYBERCOM) در وزارت دفاع و نیروهای رزمی آمریکا تشکیل و دستورالعمل‌های مربوطه تنظیم و به کار گرفته شد. ادعای وجود تهدیداتی همانند پروژه سوتر^۲ و یا هک سیستم‌های پدافند هوایی در سوریه و همچنین، اقداماتی مانند در اختیاریت تجهیزات نظامی در حوزه رادار، هواپیما، ریزپرنده و ... بر اهمیت شناخت دقیق بُعد سایبرالکترومغناطیس نظامی می‌افزاید. زیرا، می‌توان با تعیین حدود و مشخصات این نوع ویژه از عملیات، صحت ادعاهای مطرح‌شده را آزمود و در صورت تأیید، اقدامات تقابلی مربوطه را در عملیات مدنظر قرار داد.

بر اساس اسناد منتشرشده، CEMA حدّ مشترک بین عملیات فضای سایبر، عملیات جنگ الکترونیک و مدیریت طیف الکترومغناطیس تعیین گردیده است [۳]؛ لذا، با توجه به نوع، محیط و مشخصات خاص هر عملیات می‌توان بُعد سایبرالکترومغناطیس را تعریف کرد. سؤالی که در اینجا مطرح می‌شود این است که آیا اساساً، اشتراکی بین بُعدهای عملیات فضای سایبر، جنگ الکترونیک و مدیریت طیف الکترومغناطیس به معنای بیان شده در اسناد منتشره وجود دارد؟ در صورت وجود، ارتباط آنها چگونه است؟ و در غیر این صورت، بُعد سایبرالکترومغناطیس نظامی چیست و چه ابعادی را شامل می‌شود؟ برای پاسخ‌گویی به سؤالات مطرح‌شده، ابتدا تعاریف موجود در بُعد عملیات سایبری و عملیات جنگ الکترونیک را مورد مطالعه و بررسی قرار می‌دهیم؛ سپس، با توجه به تعاریف و مصادیق، بُعد سایبرالکترومغناطیس را تعریف و در نهایت، شباهت‌ها، تفاوت‌ها و محدوده‌های اشتراکی بین این بُعدها را تعریف و تشریح خواهیم کرد.

¹ Cyber Electromagnetic Activity

² SUTER

۲-۱-۱- مفهوم سایبر و عملیات سایبری

مفهوم عملیات سایبر، اولین بار توسط نویسنده آمریکایی ویلیام فورد^۱ در رمان علمی-تخیلی نئورومانسر^۲ در سال ۱۹۸۴م آورده شده است [۴]. تاکنون تعاریف متعددی توسط مراکز علمی، پژوهشی و نظامی در بُعد فضای سایبر صورت گرفته است. اما، با توجه به رویکرد نظامی مدنظر این پژوهش، تعاریف مورد استفاده توسط اسناد دفاعی آمریکا و ناتو را مورد توجه قرار می‌دهیم. مهم‌ترین اسناد وزارت دفاع آمریکا که به تعریف فضای سایبر و عملیات فضای سایبر پرداخته‌اند عبارتند از: JP 1-02، JP 3-0، FM 3-38 و FM 3-12.

تعریف وزارت دفاع آمریکا از فضای سایبر: «فضای سایبر یک بُعد جهانی محیط اطلاعاتی است که متشکل از شبکه مستقل زیرساخت فناوری اطلاعات و اطلاعات موجود در این شبکه بوده و شامل اینترنت، شبکه‌های ارتباطی، سیستم‌های رایانه‌ای و کنترل‌گرها و پردازنده‌های تعبیه شده در آنها است» [۵]. این تعریف به تجهیزات الکترونیکی پردازش اطلاعات و نرم‌افزار رایانه‌ای نصب شده روی این تجهیزات اشاره می‌کند.

تعریف ناتو از محیط اطلاعاتی: «فضای فیزیکی و مجازی است که در آن اطلاعات دریافت، پردازش و انتقال می‌یابند. این محیط شامل اطلاعات و سیستم‌های اطلاعاتی است». در این تعریف، «فضای فیزیکی» به معنی تجهیزات الکترونیکی (رایانه‌ها) بوده و «فضای مجازی» به معنی محیط نرم‌افزاری است. همکاری هر دو محیط می‌تواند منجر به دریافت، پردازش و انتقال اطلاعات گردد [۶].

تعریف عملیات فضای سایبر: به کارگیری قابلیت‌های فضای سایبر در جایی که هدف اولیه‌ی آن دستیابی به اهداف دریا از طریق فضای سایبری باشد [۳].

آنچه در تعاریف فوق مشترک است، محیط اطلاعاتی است که از محدوده الکترونیکی (جایی که اطلاعات به صورت فیزیکی توسط رایانه پردازش می‌شوند) و فضای مجازی (جایی که اطلاعات توسط نرم‌افزار پردازش می‌شوند) تشکیل شده است. در واقع، باید به این مهم توجه کرد که تمام عملیات‌ها تنها در محیط اطلاعاتی انجام می‌گیرند. بنابراین، عملیات در فضای سایبر، به سه بخش عمده‌ی زیر تقسیم می‌شود:

۱- دزدی اطلاعات (نشت اطلاعات) توسط نرم‌افزار ویژه

۲- ایجاد خطای عمدی روی تجهیزات توسط نرم‌افزار ویژه

۳- ایجاد داده خطا توسط سیستم فریب (مانند فیشینگ و ...) توسط نرم‌افزار ویژه

در این تقسیم‌بندی عملیات سایبری بر اساس روش (تکنیک) مشترک استفاده از نرم‌افزار ویژه، رایانه پردازش اطلاعات را انجام می‌دهد که می‌توان تمام روش‌های یادشده را تحت عنوان «فعالیت سایبری» در نظر گرفت [۷]. این نوع عملیات تنها منوط به کاربرد نظامی نبوده و در حوزه‌های غیرنظامی توسط انواع افراد، گروه‌ها، شرکت‌ها و حتی دولت‌ها اقداماتی در راستای ارتقای امنیت و یا آسیب‌رسانی بر امنیت سایبری با انواع انگیزه‌ها و اهداف غیرنظامی نیز

¹ William ford

² Neuromancer

انجام می‌شود و مقالات متعددی در این حوزه منتشر گردیده است [۸]. برای انجام عملیات فضای سایبری در بُعد نظامی از سلاح سایبری استفاده می‌شود که برابر تعریف فرهنگ لغت نظامی وزارت دفاع ایالات متحده آمریکا، سلاح سایبری «سلاحی است که به طور ویژه، به گونه‌ای طراحی می‌شود که پرسنل یا مواد (تأسیسات، تجهیزات و ...) را از کار بیندازد و در عین حال، تلفات، صدمات دائمی به پرسنل و آسیب‌های نامطلوب را به اموال و محیط‌زیست به حداقل برساند» [۹]. انواع ویروس‌ها، کرم‌ها، بدافزارها، باج افزارها و ... را می‌توان به عنوان سلاح سایبری^۱ در نظر گرفت.

برای مقابله با عملیات فضای سایبری دشمن، از تجهیزات و نرم‌افزارهایی همانند آنتی‌ویروس، فایروال‌ها^۲، سیستم‌های شناسایی نفوذ (IDS) و رمزگذاری داده استفاده می‌شود. این تجهیزات حیاتی که اقدامات مقابله‌ای را انجام می‌دهند، از این پس آن را «پدافند سایبری»^۳ می‌نامیم، شامل معیارهایی به شرح زیر است [۱۰]:

- ۱- معیار فنی، که بر پایه زیرساخت و دوره پاسخ به حوادث طراحی می‌شود.
 - ۲- امنیت بازگشت سرمایه (ROI)، که به محاسبه هزینه-فایده برای به کارگیری سیاست یا فناوری جدید می‌پردازد.
 - ۳- حالت خطر، که به تحلیل رخداد یک رویداد سایبری نسبت به سرمایه‌گذاری و عملیات انجام شده می‌پردازد.
- با توجه به مطالب بیان شده به منظور دسته‌بندی اجزای عملیات فضای سایبری متناسب با نوع اقدام (تهاجم، پدافند، بهره‌برداری) می‌توان حوزه‌های اختلال و فریب را در بخش تهاجم سایبری^۴ و تحت عنوان رزم سایبری در نظر گرفت. بخش‌های عمده سایبری در جدول (۱) آورده شده است. لازم به یادآوری است واژه‌ی دفاع سایبری در زبان فارسی دارای دو معنی آفند سایبری و پدافند سایبری است و در سند سازمان پدافند غیرعامل کشور، پدافند سایبری را به صورت «بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به موقع، مقابله‌ی مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری، توسط متخصصین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به نحوی که امکان تهاجم سایبری را از کلیه متخصصین سلب نماید»، آورده شده است.

¹ Cyber weapon

² Firewall

³ Cyber defense

⁴ Cyber attack

جدول (۱): بخش‌های عمده عملیات فضای سایبری.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	اطلاعات سایبری	دزدی اطلاعات (نشت اطلاعات) توسط نرم‌افزار ویژه	بهره‌برداری
۲	رزم سایبری	ایجاد خطای عمدی روی تجهیزات توسط نرم‌افزار ویژه	اختلال در عملکرد
۳	رزم سایبری	ایجاد داده خطا توسط سیستم فریب توسط نرم‌افزار ویژه	فریب
۴	پدافند سایبری	مقابله با عملیات سایبری دشمن	پدافند

۳- مفهوم جنگ الکترونیک و جنگ الکترومغناطیس

در اسناد وزارت دفاع آمریکا، تا سال ۲۰۲۱م از واژه جنگ الکترونیک^۱ استفاده شده، ولی از سال ۲۰۲۱م این واژه به جنگ الکترومغناطیس^۲ تغییر نموده است؛ تمام تعاریف و زیربخش‌های دو تعریف مذکور یکسان بوده و فقط کلمه الکترومغناطیس جایگزین الکترونیک گردیده است. به عنوان مثال، حمله‌ی الکترونیک با همان تعریف قبلی به حمله‌ی الکترومغناطیس تغییر کرده است.

تعریف واژه جنگ الکترومغناطیس: «اقدام نظامی شامل استفاده از الکترومغناطیس و انرژی هدایت شده برای کنترل طیف الکترومغناطیس یا حمله به دشمن است» [۳].

عملیات جنگ الکترومغناطیس را می‌توان به بخش‌های زیر تقسیم کرد [۷]:

۱- ایجاد خطای عمدی روی تجهیزات دشمن از طریق تشعشع مستقیم و پُر قدرت موج الکترومغناطیس.

۲- ایجاد داده‌ی خطا توسط تولید میدان الکترومغناطیس پُر توان بُرد بلند که سیستم ناوبری و تشخیص الکترونیکی را فریب می‌دهد.

۳- آسیب فیزیکی و قابل توجه روی تجهیزات الکترونیکی و الکترومغناطیسی توسط گسیل انرژی مستقیم (مانند HEMP).

علاوه بر بخش‌های یاد شده، می‌توان شنود سیگنالی (اعم از ارتباطی و راداری) را نیز به صورت در لحظه (سامانه های ESM^۳) و راهبردی (سامانه‌های ELINT^۴ و COMINT^۵) به عنوان بهره‌بردای اطلاعات سیگنال الکترونیکی در نظر گرفت. همچنین، استفاده از تکنیک های ECCM^۶ را به عنوان روش مقابله‌ای با اقدامات تهاجمی جنگ الکترومغناطیس در نظر گرفت [۱۱]. بخش‌های عمده‌ی عملیات جنگ الکترومغناطیس در جدول (۲) نشان داده شده است. لازم به ذکر است که سلاح جنگ الکترومغناطیس، شامل سامانه‌های اخلاگر و فریب سیگنالی است.

¹ Electronic warfare

² Electromagnetic warfare

³ Electronic Support measurements

⁴ Electronics Intelligence

⁵ Communication Intelligence

⁶ Electronics Counter Counter- Measurements

در سال ۲۰۰۷م، آژانس امنیت ملی آمریکا سند یک فناوری که با نام گذشته TEMPEST شناسایی می‌شود و در سال ۱۹۶۰م منتشر گردیده را از طبقه‌بندی خارج نمود [۱۰]. در سند مذکور به نشت اطلاعات از طریق تشعشع ناخواسته الکترومغناطیس اشاره می‌کند که امکان بازبازی اطلاعات مذکور توسط یک آنتن در فاصله‌ای قابل توجه از محل انتشار وجود دارد. این پدیده در سند با نام کد TEMPEST شناخته می‌شود.

جدول (۲): بخش‌های عمده عملیات جنگ الکترومغناطیس.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	پشتیبانی جنگ الکترومغناطیس	شنود اطلاعات سیگنالی (راداری و ارتباطی)	بهره‌برداری
۲	حمله الکترومغناطیس	ایجاد خطای عمدی روی تجهیزات توسط تشعشع الکترومغناطیس	اختلال در عملکرد
۳	حمله الکترومغناطیس	ایجاد داده خطا توسط سیگنال الکترومغناطیس	فریب
۴	مصون سازی الکترومغناطیس ^۱	استفاده از تکنیک‌های ضد جنگ الکترومغناطیس	پدافند

TEMPEST چیست؟

یک اسم رمز آژانس امنیت ملی آمریکا (NSA)^۲ و ناتو است [۱۲]، که مرتبط با جاسوسی از سیستم‌های اطلاعاتی از طریق نشت سیگنال‌ها، شامل سیگنال‌های رادیویی ناخواسته یا سیگنال‌های الکتریکی، صوتی و ارتعاشات می‌شود. در واقع این اسم رمز هم به روش‌های جاسوسی و هم راهکارهای محافظت از تجهیزات در مقابل این روش‌ها را پوشش می‌دهد [۱۳]. تعاریف متفاوتی برای این اسم رمز آورده شده است که هیچ یک تاکنون به طور رسمی توسط آژانس امنیت ملی آمریکا تأیید نشده است. از مهم‌ترین این تعاریف می‌توان به موارد زیر اشاره کرد^۳:

- مواد الکترونیکی ارتباطات از راه دور محافظت شده از انتقالات جعلی^۴
- تابش‌گذاری محافظت شده از انتقالات جعلی^۵
- استاندارد انتشار پالس الکترومغناطیس گذرا^۶
- استاندارد امنیت انتشار ارتباطات راه دور^۷

^۱ مصون‌سازی الکترومغناطیس که ترجمه واژه Electromagnetics protection می‌باشد، در بعضی از منابع فارسی تحت عنوان حفاظت الکترومغناطیس یا دفاع الکترومغناطیس آورده شده است که به لحاظ لغوی مصون‌سازی ترجمه صحیح‌تری می‌باشد (توضیح مؤلف).

^۲ National Security Agency

^۳ <https://www.learnsecurityonline.com>

^۴ Telecommunications Electronics Material Protected from Emanating Spurious Transmissions

^۵ Transient Emanation Protected from Emanating Spurious Transmissions

^۶ Transient Electromagnetic Pulse Emanation Standard

^۷ Telecommunications Emission Security Standards

روش‌های حفاظت در برابر آن نیز به عنوان امنیّت انتشار (EMSEC)^۱ شناخته می‌شوند که زیرمجموعه‌ای از امنیّت ارتباطات (COMSEC)^۲ می‌باشند. تعریف دیگر از آن عبارت است از: تجهیزات پردازش اطلاعات الکترونیکی و الکترومکانیکی می‌توانند انتشارات ناخواسته اطلاعاتی را ایجاد کنند که معمولاً به عنوان TEMPEST شناخته می‌شود. در صورت رهگیری و تجزیه و تحلیل این انتشارات، ممکن است اطلاعات منتقل شده، دریافت، پردازش یا پردازش شده توسط تجهیزات را فاش کنند.

با وجود آنکه TEMPEST بیشتر برای نشت امواج الکترومغناطیس است، امواج صوتی و لرزش‌های مکانیکی را نیز در بر می‌گیرد. برای مثال، ممکن است به منظور به دست آوردن کلمه‌ی عبور یک کاربر از سنسور حرکت داخل گوشی هوشمند او استفاده کنند [۱۴]. سیگنال‌های حامل اطلاعات غیرعمدی که در صورت قطع و تجزیه و تحلیل (حمله کانال جانبی)، ممکن است انتقال، دریافت و به‌کارگیری اطلاعات به‌دست آمده و یا پردازش توسط هر سامانه پردازشگر اطلاعات را فاش نماید، به خطر افتادن از طریق انتشار تعریف می‌شود [۱۳].

۴- پیشینه

شنود اطلاعات از سیگنال به جنگ جهانی دوم باز می‌گردد. در طول جنگ جهانی دوم، شرکت تلفن بل^۳، یک دستگاه میکسر^۴ با نام B2-131 را در اختیار ارتش آمریکا قرار داد تا سیگنال‌های تله چاپگر را با استفاده از XOR نمودن با مواد کلیدی از نوارهای یکبار مصرف (سیستم SIGTOT) و یا پیش از آن توسط یک ژنراتور کلیدی مبتنی بر روتور، رمزگذاری می‌کرد که SIGCUM نامیده می‌شد. در این زمان، بل اعلام نمود که با استفاده از میخ‌های الکترومغناطیسی در فواصل مشخصی از میکسر می‌توانند متن ساده را بازیابی نمایند. در سال ۱۹۵۶م، آزمایشگاه نیروی دریایی آمریکا، میکسر بهتری را توسعه داد که در ولتاژ و جریان کمتری کار می‌کرد. بنابراین، امکان استخراج داده از تشعشعات آن کمتر بود. این طراحی در سیستم‌های جدید رمزنگاری NSA مورد استفاده قرار گرفت. در سال ۱۹۵۸م، NSA استانداردهای تشعشع NAG-1 را برای تجهیزات و تأسیسات بر اساس محدودیت ۵۰ فوت (معادل ۱۵ متر) برای کنترل تعیین کرد و در این استاندارد، سطوح طبقه‌بندی جنبه‌های مختلف TEMPEST را مشخص نمود. با گذشت زمان و اهمیت موضوع، استانداردهای TEMPEST در دهه ۱۹۷۰م و بعد از آن با انجام آزمایش‌های جدیدتر و دستورالعمل‌های دقیق‌تر که خطرات را در مکان‌ها و موقعیت‌های خاص در نظر می‌گرفت، به تکامل خود ادامه دادند [۱۵].

روش‌های مختلفی برای ارزیابی و تنظیم تشعشعات ناخواسته امواج الکترومغناطیس (CE)^۵ وجود دارد که یکی از اولین روش‌ها، بر مفهوم قرمز/سیاه مبتنی است. این مفهوم تفکیک سیگنال‌هایی که محرمانگی اطلاعات را حفظ می‌کند (سیگنال قرمز) و سیگنال‌هایی که حاوی اطلاعات غیرطبقه‌بندی شده و غیر رمز هستند (سیگنال‌های سیاه) را توصیف می‌کند. این تفکیک غالباً توسط طبقه‌بندی فایروال‌ها یا درگاه‌های بدون جهت، تشخیص داده می‌شود. در جدول (۳) سطوح ایزولاسیون الکتریکی مطابق با دستورالعمل نصب RED/BLACK فاقد طبقه‌بندی نشان داده شده

^۱ Emission Security

^۲ Communication Security

^۳ Bell Telephone

^۴ Mixer

^۵ Compromising Emanation (CE)

است. برنامه مراقبتی ECHELON که به طور رسمی در سال ۱۹۷۱م ایجاد و توسط آمریکا، استرالیا، کانادا، نیوزلند و انگلستان به کار گرفته شد، معروف به پنج چشم^۱ است که هدف آن کنترل اتحاد جماهیر شوروی بود. اما بعدها دامنه‌ی جستجوی آن گسترش یافت و به برنامه مراقبت جهانی که وظیفه آن علاوه بر مانیتور اهداف نظامی، مانیتور ارتباطات تجاری و خصوصی هم بود، تغییر یافت [۱۶].

جدول (۳): سطح ایزولاسیون الکتریکی برای جلوگیری از تشعشعات نخواستہ در اسناد استاندارد سازی آمریکا [۱۵].

نوع سیگنال قرمز	سطح ایزولایون	محدوده فرکانسی
صوتی آنالوگ	۱۰۰dB	۱۰۰ تا ۵۰۰۰ هرتز
سیگنال‌های آنالوگ شامل ویدئوی آنالوگ	۸۰dB	کمترین نرخ سیگنال دهی به بیشینه‌ی نرخ سیگنال دهی
سیگنال‌های دیجیتال	۶۰dB	کمترین نرخ سیگنال دهی به ۱۰ برابر بیشترین نرخ سیگنال دهی

برنامه TEMPEST بخشی از برنامه‌های بالادستی را شکل می‌دهد که همانند برنامه ECHELON مراقبت و جاسوسی سیگنالی را پوشش می‌دهند [۱۷]. به دنبال آن، سایر کشورها نیز برنامه‌هایی مشابه آن را در سرویس‌های اطلاعاتی خود ایجاد کرده‌اند که می‌توان به SORM^۲ روسی^۳ [۱۸]، برنامه مراقبتی فرانسسه "L infrastructure demutualisation (IM)" که به Ferrenchelon معروف است [۱۹]، برنامه Projekt 6 آلمان و برنامه Onyx سوئیس اشاره کرد.

آخرین سند غیرمحرمانه منتشر شده درباره TEMPEST مربوط به سال ۲۰۰۲م است که استاندارد ارزیابی NSA TEMPEST 01-02 NONSTOP نام دارد [۲۰]. در این سند، بخش‌های کوچکی از تکنیک‌های مراقبتی NONSTOP آورده شده است. مطابق با مفاد این سند، مشخص می‌شود که تکنیک‌های NONSTOP بسیار شبیه به تکنیک‌های TEMPEST است [۲۱]. حملات اشاره شده در این سند از نوع غیرفعال^۴ هستند که با بهره‌برداری^۵ از نشت غیر عمدی امواج الکترومغناطیس، موجب کشف اطلاعات آن شده، به دست می‌آید. گروه اقدام آادی اطلاعات (FOIA)^۶ که اقدام به افشای اطلاعات مرتبط با اسناد TEMPEST کرده است، نشان می‌دهد که NSA هم‌چنین، بر روی روش‌های ایجاد تشعشعات الکترومغناطیس عمدی روی سیستم‌های امنیتی با استفاده از بدافزار سرمایه‌گذاری نموده است. اسم رمز TEAPOT که برای این نوع از اقدامات استفاده می‌شود اشاره دارد به «سرمایه‌گذاری، مطالعه، و

^۱ Five eyes

^۲ System for Operation Investigative Activities

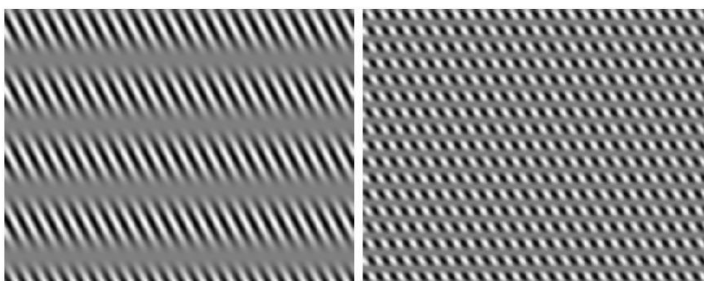
^۳ Russian SORM

^۴ Passive

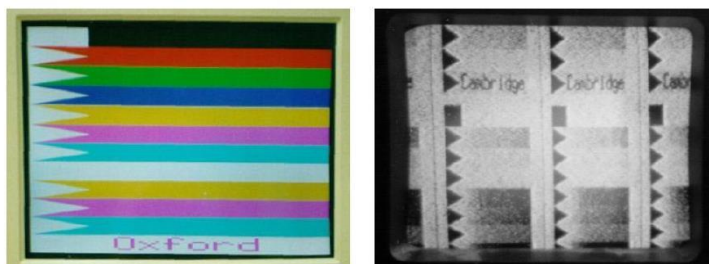
^۵ exploit

^۶ Freedom-Of-Information-Act

کنترل تشعشعات الکترومغناطیس عمدی» [۲۱ و ۲۲]. این بدافزار می‌تواند داده‌های ویدئویی را در درجات کوچک غیرقابل تشخیص برای کاربرد، به گونه‌ای دست‌کاری نماید که به ایجاد نشت الکترومغناطیس قوی‌تر در سیستم به واسطه‌ی جا دادن یک فرکانس خاص در تولید سیگنال ویدئویی مدوله‌شده روی فرکانس رادیویی حامل گردد، بیانجامد. این امر به تبدیل شدن سیستم به یک فرستنده‌ی سرتاسری رادیویی می‌انجامد که می‌تواند یک کانال رادیویی را پوشش دهد. یک مثال از این در شکل (۱) نشان داده شده است. این حمله به‌ویژه برای سیستم‌های امن شده با شکاف هوایی^۱ بسیار خطرناک است. یک روش مناسب‌تر تغییر ارزش بایت^۲ در ارزش پیکسل^۳ است که منجر به انحراف کوچک در رنگ می‌شود، اما در میدان دور^۴ ناشستی الکترومغناطیس قوی‌تری ایجاد خواهد کرد [۲۳ و ۲۴]. مثال این نوع حمله در شکل (۲) نشان داده شده است.



شکل (۱): مثالی از مانیتور CRT (لوله اشعه کاتودی) با انتشار ۳۰۰ مگاهرتز (تصویر سمت چپ) و ۱۲۰۰ مگاهرتز (تصویر سمت راست)، تنظیم‌شده برای فرکانس حامل مدوله‌شده دامنه ۲ مگاهرتز [۲۳].



شکل (۲): تصویر نمایش داده شده روی مانیتور CRT (سمت چپ). تصویر ویدئویی بازبازی شده (سمت راست) نشان می‌دهد که پیام مخفی شده قابل مشاهده وی تصویر ویدئو اصلی نیست [۲۳].

۵- تحقیقات منتشر شده

^۱ Air-gapped secured system

^۲ Byte

^۳ Pixel

^۴ Far-field

با ظهور این تهدید خاص، توجه محققین به‌ویژه در ۳۵ سال اخیر به این بُعد جلب شده است. در سال ۱۹۸۵م، دلیو وان اک^۱ تحقیقاتش را درباره نشت ناخواسته الکترومغناطیس صفحات CRT منتشر کرد که در آن موفق به بازسازی تصویر نمایش داده شده در CRT با استفاده از یک آنتن، گیرنده مدولاسیون دامنه (AM) و تولیدکننده سیگنال شده بود [۲۵]. در واقع اثبات کرد که نه تنها امکان استراق سمع VDUها^۲ وجود دارد، بلکه می‌توان این کار را با تجهیزات فاقد سکوی تجاری (COTS)^۳ نیز انجام داد. تحقیقات مشابه توسط پی. اسمولدرس^۴ روی کابل‌های RS-232 و ام.جی. کوهن^۵ روی صفحات نمایش تخت^۶ انجام شد [۲۴]. کوهن اثبات کرد که سیگنال‌های ویدئو دیجیتال روی کابل LVDS^۷ یا لینک FPD^۸ هم قابل استراق سمع هستند.

سایر محققین بررسی‌های خود را درباره خطرات استراق سمع در این بُعد توسعه دادند [۲۴، ۲۶، ۲۷ و ۲۹]. این تحقیقات ثابت می‌کند که VDUها در حالت کلی و کابل‌های سیگنال‌دهی دیتا مانند VGA^۹، DVI^{۱۰}، HDMI^{۱۱} و LVDS دارای نشت الکترومغناطیس ناخواسته هستند. تاناکا و همکاران^{۱۲} پژوهش کوهن را روی نمایشگرهای کریستال مایع (LCD^{۱۳}) توسعه دادند. در این تحقیق، تشعشعات LCD در میدان دور و نزدیک و همچنین، اثر کوپلینگ LCD^{۱۴} روی کابل‌های برق مورد بررسی قرار گرفت. تاناکا توانست تصویر را در فاصله ۶ متری بازیابی کند. هایشی و همکاران^{۱۵} در سال ۲۰۱۷م [۳۰] ولی و همکاران^{۱۶} در سال ۲۰۱۸م [۳۱]، به دنبال روشی برای بازیابی اطلاعات ویدئویی نشت یافته از فاصله ۱۰ متری همراه با روش شناسایی هم‌زمانی بودند. باید توجه کرد که به‌دلیل نوع خاص این تهدید، هنوز مستندات حاصل از تحقیقات علمی به اندازه کافی حاصل نشده و یا به دلایل امنیتی در دسترس عموم قرار نگرفته است.

۵-۱- TEMPEST نرم^{۱۷}

همان‌گونه که پیش‌تر بیان گردید، حملات TEMPEST، بر استفاده از تشعشعات الکترومغناطیس ناخواسته در انواع سناریوهای موجود دلالت دارد؛ اما نوع دیگری از حملات وجود دارد که در آن حمله‌کننده از نشت سیگنال الکترومغناطیس برای ایجاد یک کانال ارتباطی پوششی غیرمستقیم برای عدم پالایش و فیلترینگ داده استفاده می‌کند. این مدل از حملات را TEMPEST نرم می‌نامند. در این حالت مهاجم از نشت سیگنال الکترومغناطیس به‌منظور ایجاد

^۱ W. van Eck

^۲ Video Display Unit

^۳ Commercial off-the-shelf

^۴ P. Smulders

^۵ M. G. Kuhn

^۶ Flat panel display

^۷ Low-Voltage differential signaling

^۸ Front panel display

^۹ Video graphics array

^{۱۰} Digital Visual Interface

^{۱۱} High-Definition Multimedia Interface

^{۱۲} Tanaka et al.

^{۱۳} liquid crystal displays

^{۱۴} Coupling effect

^{۱۵} Hayashi et al

^{۱۶} Lee et al

^{۱۷} Soft TEMPEST

یک کانال مخفی یک طرفه برای استخراج و بهره‌برداری داده استفاده می‌کند؛ این بهره‌برداری ممکن است فعال کردن یک نرم‌افزار مخرب به صورت عمدی با اهداف مختلف از جمله مدوله کردن^۱ یک تشعشع الکترومغناطیس جعلی استفاده کند [۲۳]. چنین کانال‌های مخفی فیزیکی معمولاً به عنوان کانال‌های مخفی شکاف‌هوایی^۲ نامیده می‌شود و مطالعات متعددی در حوزه طراحی و تجزیه و تحلیل حملات TEMPEST نرم شامل سیگنال‌های ویدیویی [۳۲]، ارتباطات CPURAM [۳۳]، دسترسی به هارد دیسک^۳ [۳۴] و ارتباطات USB [۳۵] انجام شده است. یک مثال معروف از چنین حملاتی، اثبات مفهوم "TEMPESTforElisa" است که در آن یک جریان ویدئویی در هنگام نمایش نسخه مدوله شده از آهنگ Für Elise اثر بتهوون را منتشر می‌کند [۳۲].

۲-۵- TEMPEST نرم مرتبه دوم^۴

حالت دیگری از حملات TEMPEST است. TEMPEST نرم مرتبه دوم امکان بهره‌برداری آبشاری از اثرات متقابل تشعشعات الکترومغناطیس زیاد و کم در دستگاه هدف به منظور ایجاد یک کانال مخفی دور برد تعریف می‌شود. در واقع حمله TEMPEST نرم مرتبه دوم به حمله TEMPEST نرم دو مرحله‌ای اشاره دارد که فرآیند مخرب در آن داده‌های درگیر در انتشارات الکترومغناطیس که می‌تواند مستقیماً توسط مهاجم دریافت شود را کنترل نمی‌کند. در عوض، انتشارات کنترل شده یک مؤلفه داخلی را به خطر می‌اندازد که به نوبه‌ی خود داده‌ها را به سمت گیرنده مهاجم منتشر می‌کند [۳۶]. در این نوع حملات فرآیند اصلی به صورت زیر است:

- یک عملیات عمدی (خرابکارانه) انجام می‌شود.
- این عملیات به طور خاص تقابل داخلی تشعشعات الکترومغناطیس را ایجاد می‌کند.
- اثر این اثرات متقابل بین اجزای دارای انتشار کم و انتشار بالای الکترومغناطیس است.
- موجب یک حمله n مرحله‌ای TEMPEST نرم می‌شود

در جدول (۴)، مقایسه سه نوع حمله TEMPEST آورده شده است.

جدول ۴: مقایسه حملات TEMPEST، TEPEST، TEMPEST نرم و TEMPEST نرم مرتبه دوم [۳۶].

عملیات	TEMPEST	TEMPEST نرم	TEMPEST مرتبه دوم
قانونی	ایجاد شده برای اهداف مخرب	ایجاد شده برای اهداف مخرب	

^۱ Modulation

^۲ Air-gap covert channel

^۳ Hard disk

^۴ Second order soft TEMPEST

تشعشع الکترومغناطیس	غیر عمدی	عمدی	عمدی
اثر متقابل نرم افزار موج الکترومغناطیس	مستقیم	مستقیم	غیر مستقیم
اثر حمله	بازیابی اطلاعات	ایجاد کانال مخفی	ایجاد کانال مخفی

۶- روش شناسی

در این تحقیق به مفهوم سازی و توصیف ابعاد عملیات سایبری نظامی مشتمل بر عملیات سایبر، جنگ الکترومغناطیس و عملیات سایبر الکترومغناطیس و کاربردهای آنها به همراه اشتراکات و افتراق های آنها پرداخته شده است. بنابراین، این تحقیق از نوع کاربردی- توسعه ای است. این تحقیق از نظر ماهیت و روش گردآوری داده ها از نوع توصیفی موردی است. در تحقیقات توصیفی موردی، محقق به دنبال مطالعه ی عمیق در چپستی و چگونگی یک موضوع و توصیف ویژگی ها و تجزیه و تحلیل یک پدیده است. به منظور گردآوری داده ها، از منابع کتابخانه ای، سایت های معتبر علمی، اسناد و گزارش های داخلی و خارجی استفاده شده است. این تحقیق از نظر رویکرد مورد استفاده برای تجزیه و تحلیل داده ها از نوع کیفی است. روایی و پایایی تحقیق بر مبنای معیارهای کرسول محقق شده است [۳۷]. در این روش، معیارهای روایی و پایایی شامل تماس طولانی با فضای پژوهش، مشاهده مستمر، بررسی از زوایای مختلف، گردآوری از منابع اطلاعاتی متنوع و تبادل نظر با همتایان است.

۷- تجزیه و تحلیل داده ها

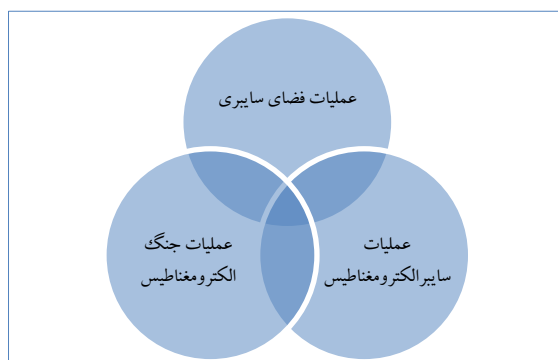
۷-۱- تعریف سایبر الکترومغناطیس نظامی

TEMPEST شامل حمله TEMPEST، TEMPEST و TEMPEST نرم مرتبه دوم را به عنوان زیرگروه جدید از تهدیدات که در آن ابزار داده بوده و محیط اثر طیف الکترومغناطیس می باشد، در نظر گرفت. بخش های عمده عملیات سایبر الکترومغناطیس در جدول ۵ نشان داده شده است. این مجموعه دارای تفاوت هایی با عملیات سایبری و عملیات جنگ الکترومغناطیس است و در عین حال دارای اشتراکات جزئی در بعضی حوزه ها است؛ این اشتراکات را به عنوان سایبر الکترومغناطیس نظامی تعریف می کنیم. جنگ الکترومغناطیس و سایبر الکترومغناطیس هردو به طیف الکترومغناطیس وابسته هستند. در جدول ۶ مقایسه بین EMP^۱ به عنوان یکی از زیربخش های جنگ الکترومغناطیس با حملات TEMPEST به عنوان یکی از زیر بخش های سایبر الکترومغناطیس نظامی آورده شده است. بدیهی است ابزاری که برای اثرگذاری بر داده ها و از طریق امواج الکترومغناطیس به کار گرفته می شود را می توان به عنوان سلاح سایبر الکترومغناطیس در نظر گرفت.

¹ High Electromagnetic Puls

۲-۷- حدود اشتراک سه بُعد عملیات

ساختار نهایی عملیات‌های فضای سایبری، سایبرالکترومغناطیس و جنگ الکترومغناطیس برابر شکل (۳) هست، می‌باشد. در ادامه، به بررسی تفاوت این سه بُعد به صورت دو به دو خواهیم پرداخت.



شکل (۳): ابعاد عملیات فضای سایبر، جنگ الکترومغناطیس و عملیات سایبرالکترومغناطیس

جدول (۵): بخش‌های عمده عملیات سایبر الکترومغناطیس.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	TEMPE SR	استراق سمع داده‌های محرمانه	بهره‌برداری
۲	TEMPE ST نرم و EMI ۱	ایجاد کانال مخفی یک‌طرفه جهت اختلال در عملکرد	اختلال در عملکرد
۳	TEMPE ST نرم مرتبه دوم	ایجاد کانال مخفی برد بلند به منظور انجام کنترل در عملکرد	فریب
۴	EMC ^۲	استفاده از فیلترها و محدودسازهای تشعشع ناخواسته الکترومغناطیس	پدافند

جدول (۶): مقایسه HEMP و TEMPE ST [۶].

TEMPE ST	HEMP	
میکرو و ولت، میکرووات	کیلو ولت، مگاهرتز	توان سیگنال
تا ۱۰۰ گیگاهرتز	تا ۱۰۰ مگاهرتز	محدوده فرکانسی
فیلترهای ضد تداخل الکترومغناطیسی	موانع ولتاژی	اقدامات حفاظتی

^۱ Electromagnetic Interference

^۲ Electromagnetic Compatibility

اثرات مخرب	تخریب فیزیکی زیرساخت‌ها	دسترسی غیرمجاز به اطلاعات طبقه‌بندی شده
تجهیزات و روش‌های تست	تجهیزات بسیار بزرگ ولتاژ با توان بسیار بالا	تجهیزات الکترونیکی با حساسیت بسیار بالا

۷-۳- اشتراک عملیات فضای سایبری و عملیات جنگ الکترومغناطیس

همان‌گونه که پیش‌تر بیان شد، این دو بُعد از لحاظ ابزار و محیط اثر کاملاً متفاوت هستند. اما اثر هر یک از عملیات های یادشده را می‌توان در خروجی پردازنده‌ی سامانه‌ی هدف مدنظر قرار داد. در عملیات فضای سایبری، سیگنال ورودی به پردازنده، سیگنال سالم و بدون خطا است ولی به واسطه‌ی عملیات فضای سایبر، کد مخرب موجب خطا در نرم‌افزار پردازنده شده و سیگنال خروجی دارای خطا خواهد بود که می‌تواند منجر به اختلال در عملکرد و یا فریب گردد. اما، در عملیات جنگ الکترومغناطیس، سیگنال ورودی به پردازنده، سیگنالی خطا یا فریب است که با عملکرد صحیح پردازنده نیز خروجی از صحت و دقت لازم برخوردار نبوده و نتیجه همان اختلال در عملکرد و فریب خواهد بود. در واقع اثر مخرب در ایجاد سیگنال خروجی پردازش شده خطا را می‌توان به عنوان حوزه‌ی مشترک کاربری این دو عملیات درنظر گرفت. مثال دیگر از این نوع عملیات، در روش‌هایی از رمزگشایی است که در آنها با ارسال سیگنال نویز، لینک داده را کشف و نسبت به رمزگشایی اقدام می‌گردد.

۷-۴- اشتراک عملیات فضای سایبری و عملیات سایبرالکترومغناطیس

هک و نفوذ به Wi-Fi و یا در اختیارگیری^۱ ریزپرنده^۲ یا پهپاد و امثال این نوع عملیات‌ها، حدمشترک عملیات فضای سایبری و عملیات سایبرالکترومغناطیس خواهد بود. به عنوان مثال، در عملیات در اختیارگیری ریزپرنده، سیگنال تبادل داده بین ریزپرنده و ایستگاه کنترل زمینی توسط یک گیرنده کشف و سپس، پروتکل استخراج و رمزگشایی می‌شود. در مرحله‌ی بعد با تغییر پارامترها در پروتکل ارتباطی مذکور، و ارسال آن به ریزپرنده، ضمن تغییر در مشخصات کنترلی، امکان در اختیارگیری هدایت و کنترل کامل ریزپرنده وجود خواهد داشت [۳۸ و ۳۹]. در این عملیات، هم از عملیات فضای سایبر (کشف پروتکل، رمزگشایی و تغییر) و هم عملیات سایبرالکترومغناطیس (ارسال داده خطا برای ریزپرنده از طریق موج الکترومغناطیس و در اختیارگیری هدایت آن) استفاده می‌شود.

۸- اشتراک عملیات سایبرالکترومغناطیس و عملیات جنگ الکترومغناطیس

تغییر نرخ نمونه‌برداری از سیگنال در یک پردازنده‌ی مخابراتی با استفاده از سر ریز شدن بافر، می‌تواند به ایجاد خطا در خروجی انجامد؛ این نوع از عملیات با حالت یاد شده در اشتراک عملیات فضای سایبر و جنگ الکترومغناطیس متفاوت است زیرا در آن سیگنال ورودی به پردازنده سالم بوده و پردازنده نیز به صورت درست در حال انجام عملیات

^۱ - Hijacking

^۲ - Drone

پردازش است. اما به دلیل تغییر در نوع ارسال سیگنال به عنوان مثال ارسال سیگنال پُر توان در بازه‌هایی از باند گیرنده می‌تواند موجب سرریز شدن بافر، تغییر در نرخ نمونه‌برداری سیگنال، ایجاد خطا در پردازش و در نتیجه تولید سیگنال خطا خواهد شد [۴۰]. این حالت را که می‌توان به عنوان اشتراک عملیات سایبرالکترومغناطیس با عملیات جنگ الکترومغناطیس در نظر گرفت. در جدول ۷، مثال سیگنال ورودی و پردازنده برای سه بُعد عملیاتی آورده شده است.

جدول (۷): مقایسه عملکرد پردازنده مخابراتی در سه بُعد عملیاتی.

بُعد عملیات	سیگنال ورودی	عملکرد پردازنده	سیگنال خروجی
عملیات فضای سایبری	صحیح	خطا	خطا
عملیات جنگ الکترومغناطیس	خطا	صحیح	خطا
عملیات سایبرالکترومغناطیس	صحیح	صحیح	خطا

۹- نتیجه‌گیری و پیشنهاد

عملیات‌های وابسته به سیگنال و نرم‌افزار که موجب ایجاد اختلال در عملکرد سامانه‌های وابسته به رایانه می‌شوند، به واسطه ویژگی‌های سایبر و جنگ الکترونیک، دارای حدود فاصل نبوده و به واسطه اشتراکات همواره مشکلاتی را در تعریف و به‌کارگیری ایجاد کرده‌اند. با تعریف عملیات سایبر و عملیات جنگ الکترومغناطیس، تفاوت در عامل تأثیرگذاری و محیط اثر این مهم را نشان می‌دهد که این دو بُعد هیچ اشتراکی با هم نداشته و نمی‌توان سایبرالکترومغناطیس را به عنوان اشتراک آنها تعریف کرد. از طرفی با بررسی اسناد منتشرشده، می‌توان دریافت حالتی وجود دارد که به واسطه نشت الکترومغناطیس در بین اجزای الکترونیکی مانند پردازنده، صفحه نمایش و ...، می‌توان اطلاعات تبادل شده را به طور غیرمجاز استراق سمع کرد. این حالت که با کدرمز TEMPEST شناخته می‌شود دارای حملات در اشکال TEMPEST نرم و TEMPEST نرم مرتبه‌دوم نیز هست که با ایجاد کانال‌های مخفی می‌توانند در عملکرد اختلال، و یا تغییر در داده ایجاد کند. بُعد مذکور که از طریق موج الکترومغناطیس به صورت مستقیم از داده بهره‌برداری کنند و یا بر داده اثر گذارند را می‌توان به عنوان بُعد سایبرالکترومغناطیس در نظر گرفت. در جدول ۸ سه بُعد عملیاتی از لحاظ ابزار و محیط اثر نشان داده شده‌اند.

جدول (۸): مقایسه عملیات سایبری، جنگ الکترومغناطیس و سایبرالکترومغناطیس از منظر ابزار و محیط.

بُعد عملیات	اثرگذاری بر	محیط
عملیات سایبری	داده	نرم افزار
عملیات جنگ الکترومغناطیس	موج الکترومغناطیس	طیف الکترومغناطیس
عملیات سایبرالکترومغناطیس	داده	طیف الکترومغناطیس

با تعریف چهار عمل اصلی در عملیات شامل اختلال در عملکرد، ایجاد فریب، بهره‌برداری سایبرالکترومغناطیس، می‌توان تفکیک بین این بُعدهای رزمی را در نظر گرفت. و عملیات دفاعی بین بُعدهای عملیات سایبری، عملیات جنگ الکترومغناطیس و عملیات جدول ۹ این دسته بندی را نشان می‌دهد.

جدول (۹): مقایسه سه بُعد عملیات از نظر بخش های عمده عملیاتی.

بخش‌های عمده عملیات	عملیات سایبری	عملیات جنگ الکترومغناطیس	عملیات سایبرالکترومغناطیس
بهره برداری	اطلاعات سایبری	پشتیبانی جنگ الکترومغناطیس	TEMPESTR
اختلال در عملکرد	رزم سایبری	حمله الکترومغناطیس(*)	TEMPESTR نرم و EMI(*)
فریب	رزم سایبری	حمله الکترومغناطیس(*)	TEMPESTR نرم مرتبه دوم(*)
دفاع	پدافند سایبری	دفاع الکترومغناطیس	EMC

*: این موارد را می‌توان به عنوان حوزه سایبر در رزم لحاظ کرد

لازم به ذکر است که این عملیات سه‌گانه، علی‌رغم تفاوت‌های آشکار و حدود فاصل، دارای اشتراکاتی هستند که به صورت دوگانه با هم در ارتباط بوده و یک عملیات پیچیده را تشکیل می‌دهند. استفاده‌ی مؤثر، به‌موقع و همزمان از هر سه بُعد عملیات در صورتی که با ملاحظات کامل به‌ویژه در تخصیص فرکانس صحنه نبرد همراه باشد می‌تواند برتری در صحنه نبرد را تضمین کند و توازن قوا در میدان نبرد را به شکل قابل توجهی تغییر دهد.

منابع:

- [1] McGuffin, C., and Mitchell, P., "On domains: Cyber and the practice of warfare," International Journal, Vol. 3, No. 69, pp 394-412, 2014.
- [2] FM 3-38 Cyber Electromagnetic Activities. United States Army, 2014.
- [3] FM 3-12: Cyberspace Operations and Electromagnetic Warfare. United State Army, 2021.
- [4] Gibson, W., Neuromancer. Ace, 1984.
- [5] JP 1-02. US Department of Defense, 2010.
- [6] AJP-3.10., "Allied joint Doctrine for Information Operation," NATO, 2009.
- [7] Gurevich, V., "Cybernetic and Electromagnetic Impacts on Electronic Equipment: Do they have Anything in Common?," International Journal Of Research Studies in Electronics Engineering (IJRSEEE), Vol. 5, No. 3, pp 36-40, 2019.
- [8] Moghaddasi, A., and Bagheri, M., "Automatic XSS Exploit Generation Using Grammatical Evolution," Journal of Electronical and Cyber Defense, Vol. 9, No. 2, pp 101-119, 2021.
- [9] Mallick, M. G., Cyber Weapons: a weapon of war?. New Dehli: Vivekananda International Foundation, 2021.
- [10] Winterfeld, S., and Andress, J., The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress, 2021.
- [11] JP 3-13: Electronic Warfare. US Department of Defense, 2007.

- [12] TEMPEST Equipment Selection Process. NATO, 1981.
- [13] NACSIM 5000: TEMPEST Fundamentals. National Security Agency of United State, 2015.
- [14] Goodman, C., An Introduction to TEMPEST. SANS Technology Institute, 2001.
- [15] Boak, D. G., A History of U.S. Communications Security, National Security Agency of United States, 1973.
- [16] Nabbali, T., and Perry , M., "Going for the throat: Carnivore in an ECHELON world," Computer Law & Security Review, Vol. 2, No. 20, pp 84-97, 2004.
- [17] O'Neill, J., ECHELON: Somebody's Listening. Word Association, 2005.
- [18] Maréchal, N., "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," Media and Communication, Vol. 1, No. 5, pp 29-41, 2017.
- [19] Follorou, J., and Johannes, F., Révélations sur le Big Brother français. Le Monde, 2013.
- [20] Committee in National Security Systems Advisory Memorandum TEMPEST 01-02 Nonstop Evaluation Standard. National Security Agency of United States, 2002.
- [21] NSA/CSS Regulation 90-6: Technical Security program. National Security Agency Of United States, 1999.
- [22] Anderson, J. R., Security Engineering: A Guide to Building Dependable Distribute Systems. Wiley, 2008.
- [23] Kuhn, G. M., and Anderson, J. R., "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," International Workshop on Information Hiding. Berlin, 1998.
- [24] Kuhn, G. M., Compromising emanations: Eavesdropping Risks of Computer Displays. Cambridge: University of Cambridge, 2003.
- [25] Eck, v. W., "Electromagnetic radiation from video display units: An eavesdropping risk?," Computer & Security, Vol. 4, No. 4, pp269-286, 1985.
- [26] Sekiguchi, H., and Seto, S., "Proposal of an Information Signal Measurment method in Display Image Contained in Electromagnetiv Noise Emanated from a Personal Computer," 2008 IEEE Instrumentation and Measurement Technology Conference, Victoria, BC, Canada, pp. 1859-1863, 2008.
- [27] Kuhn, M. G., "Compromising Emanations of LCD TV sets," IEEE Transactions on Electromagnetic Compatibility, Vol. 3, No. 55, pp 564-570, 2013.
- [28] Hayashi, Y.-i., Homma, N., Toriumi, Y., Takaya, K., and Aoki, T., "Remote Visualization of Screen Image Using a Pseudo-Antenna That Blends into Mobile Enviroment," IEEE Transactions on Electromagnetic Compatibility, Vol. 59, No. 1, pp 24-33, 2017.
- [29] Hidema, T., Takizawa, O., and Yamamura, A., "A Trial of the Intercaption of Display Image Using Emanation of Electromagnetic Wave," the institue of image Electronics Engineering of Japan, Vol. 25, No. 1/2, pp 213-223, 2005.
- [30] Hayashi, Y., Homma, N., Miura, M., Aoki, T., and Sone, H., "A threat for Tablet PCs in Public Space: Remote Visualization of Screen Image Using EM Emanation," Computer and Communication Security, 2014.
- [31] Lee, S. H., Choi, D. H., Sim, K., and Yook, J. G., "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Enviroment," IEEE Transactions on Electromagnetic Compatibility, Vol. 61, No. 4, pp 1098-1106,

- 2019.
- [32] Thiele, E., Tempest for Eliza. the Guardian News, 2001.
 - [33] Guri, M., Kedma, G., Kachlon, A., and Elvoici, Y., "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequency," 9th International Conference on Malicious and Unwanted Software, 2014.
 - [34] Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., and Elovici, Y., "GSMem: Data Exfiltration from Air-Gapped Computers Over GSM Frequencies," 24th USENIX Security Symposium, Washington D.C., 2015.
 - [35] Guri, M., Monitz, M., and Elovici, Y., "USBee: Air-gap Covert-channel via Electromagnetic Emission from USB," 14th Annual Conference on Privacy, Security and Trust (PST), 2016.
 - [36] Cottais, E., Esteves, J. L., and Kasmi, C., "Second order soft-tempest in rf front-ends: Design and detection of polyglot modulations. Second order soft-tempest in rf front-ends," Desig International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018.
 - [37] Creswell, J. W., Qualitative inquiry and research design: Choosing among five approaches (4th ed.). thaousand Oaks, CA: Sage, 2014.
 - [38] Zheng, X. C., and Sun, H. M., "Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defende radio," Sensors and Mterials, Vol. 38, No. 8, pp. 2729-2743, 2020.
 - [39] Giray, S. M., "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," 6th International Conference on Recent Advances in Space Technology (RAST), 2013.
 - [40] Kim, A., Wampler, B., Goppert, J. M., Hwang, I., and Aldeidge, H., "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," Infotech@Aerospace. California, 2012.

مزایای عملیاتی استفاده از جنگ الکترونیک سایبری (CEW)^۱ در میدان نبرد

حامد شیروی^{۱*}

۱- مربی دانشکده فنی مهندسی، دانشگاه افسری و تربیت پاسداری امام حسین(ع) - hshiravi@ihu.ac.ir

چکیده:

در حالی که فضای سایبری به عنوان یک میدان نبرد جدید در حال ظهور است، روش‌ها و کاربردهای جنگ الکترونیک متعارف احتمالاً تغییر خواهد کرد. مفهوم جنگ الکترونیک سایبری که قابلیت‌های فضای سایبری را با روش‌های سنتی EW^۲ ادغام می‌کند، شکل جدید و پیشرفته‌ای از حمله الکترونیکی است. در این مقاله بر حوزه فضای سایبری میدان نبرد تأکید شده و امکان ادغام مفهوم CW^۳ در اقدامات EW مورد بررسی قرار گرفته است. از روش تحلیل SWOT^۴ (نقاط قوت، ضعف، فرصت‌ها و تهدیدها) برای بیان مزایای عملیاتی استفاده از مفهوم CEW در میدان جنگ استفاده می‌شود. مزایای عملیاتی CEW با استفاده از اثرات آن بر سیستم‌های دفاع هوایی دشمن، شبکه‌های ارتباطی و سیستم‌های اطلاعاتی مورد تحلیل قرار می‌گیرد. در نهایت، مقایسه مفهوم CEW و کاربردهای EW، به این موضوع می‌انجامد که استفاده از مفهوم CEW در میدان جنگ امکان‌پذیر است و ممکن است مزایای عملیاتی مهمی را به همراه داشته باشد. اگرچه رایانه‌های سیستم‌های نظامی توسعه‌یافته پیچیده‌تر از رایانه‌های معمولی هستند، اما از آن جایی که سیستم‌های بسته هستند، در معرض تهدیدات سایبری قرار نمی‌گیرند. این مفهوم قصد دارد نشان دهد که این سیستم‌های بسته در برابر تهدیدات سایبری نیز باز هستند. در نتیجه، تجزیه و تحلیل SWOT، مفهوم CEW نیروی هوایی را برای استفاده مؤثر در عملیات سایبری فراهم می‌کند. از سوی دیگر، از آن جا که معیارهای خسارت وثیقه آن (CDC)^۵ کم است، به نظر می‌رسد استفاده از سیستم‌های حمله الکترونیکی سایبری رو به افزایش است.

کلید واژه‌ها: جنگ سایبری، جنگ الکترونیک، جنگ الکترونیک سایبری، فضای مجازی.

Operational Advantages Of Using Cyber Electronic Warfare (CEW) In The Battlefield

*Hamed Shiravi

¹ Cyber Electronic Warfare

² Electronic Warfare

³ Cyber Warfare

⁴ Strengths, Weaknesses, Opportunities and Threats

⁵ Collateral Damage Criteria

Abstract

While cyberspace is emerging as a new battlefield, conventional Electronic Warfare (EW) methods and applications are likely to change. Cyber Electronic Warfare (CEW) concept which merges cyberspace capabilities with traditional EW methods, is a new and enhanced form of the electronic attack. In this study, cyberspace domain of the battlefield is emphasized and the feasibility of integrating Cyber Warfare (CW) concept into EW measures is researched. The SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis method is used to state the operational advantages of using CEW concept in the battlefield. The operational advantages of CEW are assessed by means of its effects on adversary air defense systems, communication networks and information systems. Outstanding technological and operational difficulties are pointed out as well. As a result, a comparison of CEW concept and conventional EW applications is presented. It is concluded that, utilization of CEW concept is feasible at the battlefield and it may yield important operational advantages. Even though the computers of developed military systems are less complex than normal computers, they are not subjected to cyber threats since they are closed systems. This concept intends to show that these closed systems are also open to the cyber threats. As a result of the SWOT analysis, CEW concept provides Air Forces to be used in cyber operations effectively. On the other hand, since its Collateral Damage Criteria (CDC) is low, the usage of cyber electronic attack systems seems to grow up.

Keywords: Cyber war, electronic war, cyber electronic war, virtual space.

۱- مقدمه

پس از عملیات طوفان صحرا (۱۹۹۱م) با کمک اینترنت، که در آن برای اولین بار سیستم‌های ارتباطی ملی در برنامه‌های عملیاتی هدف قرار می‌گرفت، اینترنت، بسیار سریع گسترش یافت. جنگ سایبری به عنوان یک مفهوم جدید شروع به ظهور کرده است. از سوی دیگر، در جنگ دوم خلیج فارس، مزایای استفاده از فناوری در منطقه عملیاتی به وضوح دیده شد و تکنیک‌های جدید مرتبط با جنگ سایبری شروع به توسعه کردند.

در سال ۲۰۰۷م، استونی، یکی از کشورهای پیشرو اروپا که دولت الکترونیک را در اروپا اعمال کرد، در معرض اولین حمله سایبری سیستماتیک توسط روسیه قرار گرفت [۱]. حمله سایبری روسیه به گرجستان در طول جنگ اوستیای جنوبی در سال ۲۰۰۸م را می‌توان به عنوان حمله سایبری جنبشی توصیف کرد؛ زیرا این حمله در یک جنگ متعارف رخ داده است. استاکسنت، حمله دیگری است که در سال ۲۰۱۰م علیه نیروگاه‌های هسته‌ای ایران رخ داد، حادثه مهمی بود که آشکارا تأثیر سلاح سایبری توسعه‌یافته را برای یک هدف خاص نشان می‌داد [۲].

علاوه بر این، لاکهید مارتین، یک شرکت پیشرو در ارائه‌ی تسلیحات، اعلام کرد که در معرض حمله سایبری قرار گرفتند و در سال ۲۰۱۱م با انجام اقدامات احتیاطی از سیستم خود با موفقیت دفاع کردند. این حمله شبکه قابلیت‌های CW [۳] را برجسته می‌کند. می‌توان گفت که حملات سایبری اخیر متوجه شرکت‌های دفاعی بوده است. با توجه به اینکه این حملات برای دستیابی به اطلاعات سیستم تسلیحاتی است، می‌توان آنها را به عنوان حملات

سایبری غیرمستقیم به سیستم‌های نظامی توصیف کرد. در نتیجه، به تدریج CW خود را به یک راه بی‌خون اما مؤثر برای جنگ به‌ویژه علیه کشورهای توسعه‌یافته که هدف سایر کشورها در مورد حمله سایبری هستند، تبدیل کرد. جنگ الکترونیک با استفاده از سیستم‌های راداری به عنوان دفاع هوایی در جنگ جهانی دوم پدیدار شد. هنگامی که موشک‌های هدایت‌شونده به کمک رادار باعث تلفات هواپیماهای زیادی در ویتنام شد، EW به تدریج در جنگ‌های بعدی مانند جنگ خلیج فارس، جنگ کوزوو، کارایی خود را افزایش داد و همچنان به یکی از مهم‌ترین عوامل در میدان جنگ تبدیل شد.

به عنوان سیستم‌های تسلیحاتی مورد استفاده در میدان عملیات، می‌توان در نظر گرفت که جنگ الکترونیک علاوه بر باندهای فرکانس رادیویی و راداری، باندهای مادون قرمز، مرئی و فرابنفش را در طیف الکترومغناطیسی نیز پوشش می‌دهد. بنابراین، می‌توان نتیجه گرفت که EW بر روی مبارزه در تمام مراحل تأثیر می‌گذارد [۴].

رابطه بین CW و EW را می‌توان به عنوان رابطه بین جنگ نامتقارن و متقارن در نظر گرفت. برخلاف CW، هدف EW جلوگیری از انتقال اطلاعات با اقدام تقریباً بدون در نظر گرفتن اهداف خاص است. CW به عملیاتی می‌پردازد که شامل اهداف خاص تر و اطلاعات دیجیتالی می‌شود [۵]. در حالی که فضای سایبری به عنوان جنگ نامتقارن در حال ظهور است، روش‌ها و کاربردهای رایج EW قدیمی و کافی نیستند. بنابراین، علاوه بر استفاده از طیف الکترومغناطیسی، باید تکنیک‌های جدیدی برای حمله و دفاع از شبکه‌ها، سیستم‌های ارتباطی و سیستم‌های الکترونیکی ایجاد شود.

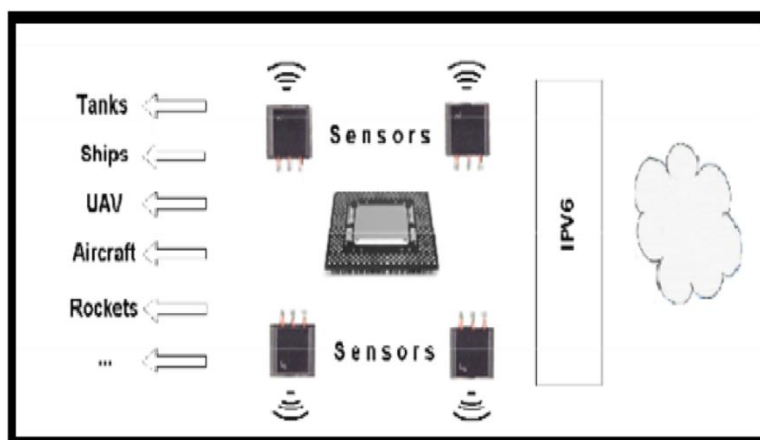
با توجه به دلایل یادشده در بالا، برنامه‌ریزان عملیات آینده، بر استفاده از CW و EW با هم تأکید دارند. در نتیجه، این مطالعه به بررسی جنگ الکترونیک سایبری می‌پردازد. در جنگ سایبری از روش‌ها و برنامه‌های کاربردی CW و EW با هم و متفاوت از هر یک از آنها، از نظر استفاده از اهداف حمله بهره می‌برند. در این مرحله می‌توان ادعا کرد که مفهوم CEW شکل جدید و پیشرفته‌ای از حمله الکترونیکی و حاوی عناصر جنگ سایبری است. در واقع، این دگرگونی حمله الکترونیکی به دلیل وابستگی روزافزون به شبکه‌ها، اینترنت و سیستم‌های ارتباطی تقریباً اجتناب‌ناپذیر است.

۲- دامنه فضای مجازی در منطقه نظامی

قبل از صحبت در مورد مفهوم CEW، لازم است حوزه فضای سایبری را بررسی کنیم تا به عمق فضای سایبری و تأثیرات جنگ سایبری در میدان نبرد پی ببریم و خطرات آن را بهتر تحلیل کنیم. با توجه به این هدف، یکی از بهترین توصیف‌های فارنکروگ این است که: «طیف وسیعی از افکار در مورد وسعت فضای مجازی یا آنچه باید در CW گنجانده شود، وجود دارد. یک پاسخ معمولی به فضای سایبری چیست؟ معمولاً شامل توصیفی از شبکه‌های رایانه‌ای یا اینترنت است. با این حال، تعریف ارتش از فضای سایبری، اذعان دارد که فضای سایبری چیزی بیش از این شبکه‌های رایانه‌ای است. مهم‌تر از آن، از آنجایی که سیستم‌های شبکه‌ای از طریق استفاده از انرژی الکترومغناطیسی ایجاد می‌شوند، جنگ در فضای سایبری لزوماً شامل قابلیت‌هایی است که در حال حاضر جنگ الکترونیک محسوب می‌شود. حتی شبکه‌هایی که مستقیماً به اینترنت متصل نیستند، ممکن است با استفاده از انرژی الکترومغناطیسی برای بازجویی یا اختلال در اجزای الکترونیکی شبکه مورد حمله قرار گیرند. این یک تمایز مهم برای ارتش است» [۶].

در این بخش، سعی می‌شود این تمایز مهم برای نظامیان مشخص شود. از این رو، می‌توان گفت که حوزه‌ی فضای سایبری شامل سیستم‌های EW است که از طیف الکترومغناطیسی، سیستم‌های الکترونیکی و زیرساخت‌های فیزیکی در سیستم‌های نظامی استفاده می‌کند. این رابطه توسط AFDD 2-11 حاوی تعامل بین حوزه فیزیکی و فضای مجازی به شرح زیر توضیح داده شده است: «فضای مجازی، داده‌ها را ذخیره، اصلاح و مبادله می‌کند. از الکترونیک و انرژی الکترومغناطیسی به منظور انجام این تغییر و تبادل استفاده می‌شود که اتصال شبکه‌ای را ایجاد و داده‌ها را مبادله می‌کند. این همه توسط زیرساخت فیزیکی فعال می‌شود که شامل تجهیزاتی مانند آنتن‌ها، روترها، سوئیچ‌ها، خطوط انتقال و کابل‌های فیبر نوری است. حوزه‌ی فضای سایبری از طیف الکترومغناطیسی (EMS) برای ذخیره، انتقال و اصلاح داده‌ها در زیرساخت‌های مناسب استفاده می‌کند» [۷].

فعالیت‌هایی مانند ذخیره سازی داده‌ها، اصلاح و تبادل با ایجاد شبکه بیناین سیستم‌ها ممکن است برنامه‌هایی باشد که در CW از آنها استفاده می‌شود. بنابراین، دارایی‌هایی که از فناوری و سیستم‌های رایانه‌ای در سطوح استراتژیک، عملیاتی و تاکتیکی استفاده می‌کنند، به‌ویژه در مراکز فرماندهی و کنترل، نیروی هوایی ارتش و نیروی دریایی مورد استفاده در میدان نبرد می‌توانند در معرض خطر حملات سایبری قرار گیرند. ادغام سیستم‌های نظامی می‌تواند خطرات سایبری بیشتری در میدان نبرد داشته باشد. در حقیقت، بسیاری از شبکه‌های فرماندهی و کنترل نظامی و سامانه‌های پدافند هوایی، شبکه‌های ایزوله یا بسته هستند که مستقیماً قابل دسترسی نیستند. اما، تمام سیستم‌های نظامی با اطلاعات فشرده، همان‌طور که در شکل ۱ ارائه شده است، به قابلیت‌های پردازش اطلاعات، ارتباطات و حس‌گر در میدان نبرد مجهز خواهند شد [۸]. با توجه به این موضوع، ما باید تهدیدات سایبری برای ارتش یا در میدان جنگ را نه تنها با شبکه‌ها، بلکه با شبکه‌های بسته و انرژی الکترومغناطیسی مورد انتقاد قرار دهیم.



شکل (۱): سیستم‌های نظامی با اطلاعات فشرده در معرض تهدید [۸].

تعریف نظامی CW، ترکیبی از حمله شبکه کامپیوتری و دفاع شبکه کامپیوتری و احتمالاً عملیات اطلاعاتی ویژه است [۹]. به منظور درک CW، تفاوت بین جنگ متعارف و CW در جدول ۱ ارائه شده است.

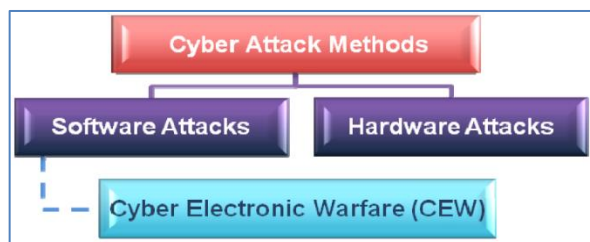
جدول (۱): تفاوت بین جنگ متعارف و جنگ سایبری [۱۰].

شاخص	جنگ متعارف	جنگ سایبری
منبع حمله	به راحتی می توان منبع را پیدا کرد	یافتن منبع بسیار دشوار است
سرعت	سرعت هواپیما، تانک یا سیستم تسلیحاتی هم همین طور	با سرعت نور
اثر	در ناحیه فیزیکی مؤثر است	بیشتر در مورد سیستم های اطلاعات و ارتباطات (ICS)، اما همچنین اثرات جانبی در حوزه فیزیکی
طرفین	بین دو یا چند نیروی مسلح	یک فرد، یک گروه، یک سازمان یا یک کشور
هزینه	بستگی به هزینه سیستم های تسلیحاتی دارد	بسیار ارزان، حتی یک کامپیوتر نیز می تواند کافی باشد
سلاح ها	سلاح های متعارف	تراشه ها و سایر سخت افزارها و نرم افزارهای مورد استفاده در سیستم های کامپیوتری
الزامات فناوری	به تکنولوژی پیشرفته نیاز دارد	فناوری پیشرفته مورد نیاز نیست، اما فناوری پیشرفته می تواند اثربخشی را افزایش دهد
نشانه های حمله	امکان تشخیص	عمدتاً تشخیص آن سخت است
تشخیص آسیب	تشخیص آسان آسیب با توجه به اثر فیزیکی جنگ	تشخیص نتایج حمله تقریباً غیرممکن است

به موازات آن، تفاوت معیارهای CW ارائه شده در جدول را می توان به عنوان ویژگی های نامتقارن CW ارزیابی کرد. همان طور که در جدول ۱ ارائه شده است، استفاده از روش های CW مؤثرتر از استفاده از روش های جنگ متعارف خواهد بود، زیرا سلاح های سایبری ارزان تر، نامرئی و غیرقابل شناسایی هستند. بنابراین، کشورهایی که در حال توسعه سلاح های سایبری هستند ممکن است فقط از روش های CW استفاده کنند یا از تلاش های جنگ متعارف از طریق سلاح های سایبری در میدان نبرد حمایت کنند. خصوصاً داشتن قابلیت حمله سایبری در میدان نبرد، در کنار روش های جنگی متعارف، می تواند اقتصاد نیرو را فراهم کند.

۳ - روش‌های حمله سایبری در میدان نبرد

روش‌های حمله سایبری قابل استفاده در میدان نبرد را می‌توان در دو گروه «حملات نرم‌افزاری» و «حملات سخت‌افزاری» بررسی کرد. همه‌ی حملات سایبری چه نرم‌افزاری و چه سخت‌افزاری، سعی می‌کنند با استفاده از شبکه‌های سیمی یا بی‌سیم، سیستم هدف را کاملاً دست‌کاری یا نابود کنند.



شکل (۲): روش‌های حمله سایبری در میدان نبرد.

همان‌طور که در شکل ۲ ارائه شده است، مفهوم CEW ممکن است به عنوان روشی برای حملات نرم‌افزاری تعیین شود. همه روش‌های حمله سایبری از سلاح‌های سایبری متغیر استفاده می‌کنند. بر این اساس، تهدیدات سایبری احتمالی برای میدان نبرد تعیین شده و سلاح‌های سایبری در جدول ۲ نشان داده شده است.

جدول (۲): تهدیدات سایبری احتمالی در میدان نبرد.

سلاح‌های سایبری	روش‌های حمله سایبری
بدافزار	حملات نرم‌افزاری
نرم‌افزارهای جاسوسی	
بمب ساعتی سایبری	
سیستم حمله جنگ الکترونیک سایبری	
ریزتراشه‌ها	حملات سخت‌افزاری
سلاح‌های میکروویو با قدرت بالا	
طوفان	
نانو مکانیک	

همان‌طور که در جدول ۲ ارائه شده است، CW نوع جدیدی از سلاح با اثرات مختلف آن بر روی یک هدف است. علاوه بر سلاح‌هایی که به عنوان یک سلاح سایبری ساخته شده‌اند، برخی از سلاح‌های دیگر که برای توسعه به عنوان یک سلاح سایبری در نظر گرفته نشده بودند، کاندیدای حضور در زرادخانه هستند. به عنوان مثال، اگرچه آنها هنوز در دوره ارتقا هستند، سلاح‌های حمله سخت‌افزاری را می‌توان سلاح‌های سایبری آینده در نظر گرفت. این سلاح‌ها:

ریز تراشه‌ها (CTB برای سخت‌افزار)، HPMW (بمب‌های پالس الکترومغناطیسی: بمب‌های الکترونیکی)، TEMPEST (سلاح‌های جاسوسی سایبری برای حملات سخت‌افزاری) و نانومکانیک (قطعات مکانیکی بسیار کوچک که به راحتی می‌توانند به سیستم‌های الکترونیکی تزریق شوند) هستند.

بدافزارها (ویروس‌های کامپیوتری، کرم‌ها، تروجان‌ها)، جاسوس افزارها، CTBها (بمب منطقی و دروازه‌های تله) و سیستم حمله CEW سلاح‌های سایبری هستند که نرم‌افزار را هدف قرار می‌دهند. در حال حاضر، بیشتر حملات نرم‌افزاری بر سیستم‌های غیرنظامی و نظامی تأثیر می‌گذارد. با این حال، آگاهی از این حملات بسیار دشوار است زیرا سلاح‌های سایبری آنها پس از داشتن مکان‌هایشان در سیستم‌ها قابل شناسایی نیستند. حملات اخیر با هدف قرار دادن رایانه‌های مأموریت تسلیحات نیروی هوایی نشان می‌دهد که اهداف این حملات نه تنها سرقت اطلاعات بلکه تأثیرگذاری بر سیستم در حال اجراست. برای تأثیرگذاری بر سیستم در حال اجرا، CTBها نیز به راحتی قابل استفاده هستند. آنها را می‌توان در مناطق آسیب‌پذیر شناسایی شده در زمان صلح قرار داده و در زمان جنگ فعال کرد. در این بخش، جایگاه سیستم CEW در روش‌های حمله سایبری به اختصار نشان داده شده است. از آنجایی که سیستم حمله CEW استفاده از نیروی هوایی در جنگ سایبری را برجسته می‌کند، مفهوم حمله CEW در بخش دیگری به تفصیل توضیح داده شده است.

۴- نیروی هوایی در جنگ سایبری

با بررسی حملات سایبری که قبلاً ذکر شد، بدیهی است که هیچ یک از آنها به طور مستقیم بر زندگی خصوصی ما تأثیر نمی‌گذارند، اما با توجه به حملات سایبری احتمالی در آینده، ممکن است به دلیل افزایش تعداد رایانه‌ها و نیاز به سیستم‌های کنترل رایانه، به شدت گسترش یابد؛ مانند بسیاری از فعالیت‌ها و سیستم‌های دولتی، سیستم‌های نظامی به طور فزاینده‌ای به فناوری و فضای سایبری وابسته هستند. در میان سیستم‌های نظامی، سیستم‌های مربوط به نیروی هوایی بیش‌ترین درصد پلت‌فرم‌های مبتنی بر فناوری را دارند.

سیستم‌های تسلیحات هوایی نیز به طور فزاینده‌ای به نرم‌افزار، سخت‌افزار رایانه و شبکه‌های میدان نبرد وابسته هستند و بنابراین، می‌توانند از طریق سیستم‌های سایبری مورد هدف قرار گیرند. در حالی که امنیت این سیستم‌های تسلیحاتی همگام با توسعه و پیاده‌سازی فناوری سایبری پیشرفت می‌کند، می‌توانند به طور فزاینده‌ای تحت تأثیر حملات سایبری قرار گیرند (جدول ۳) [۱۱].

جدول (۳): وابستگی‌های نرم‌افزاری سکوها هوایی [۱۱].

هواپیما	سال	درصد توابع نرم‌افزار
F-4	۱۹۶۰	۸
A-7	۱۹۶۴	۱۰
F-111	۱۹۷۰	۲۰
F-15	۱۹۷۵	۳۵

۴۵	۱۹۸۲	F-16
۶۵	۱۹۹۰	B-2
۸۰	۲۰۰۰	F-22

همان طور که در جدول ۳ ارائه شده، مشخص شده است که نیروهای نظامی به‌ویژه واحدهای نیروی هوایی از این حملات احتمالی تحت تأثیر سکوهاى هوایی شامل شبکه‌ها، سیستم‌های دیجیتال، زیرساخت‌ها و هر عنصر دیگری که به عنوان اطلاعات، ارتباط و یا عمل می‌کند، متأثر خواهند شد. سیستم‌های کنترل. مثلاً؛ جنگنده‌های فرانسوی رافال در ژانویه ۲۰۰۹م به دلیل یک کرم ویندوز مایکروسافت که برخی از نرم افزارهای سیستم‌های پشتیبانی زمینی را آلوده کرده بود، زمین گیر شدند [۱۲]. در این مثال، عفونت کرم کاملاً تصادفی است. در صورت عمدی بودن و در حین آماده سازی مأموریت عملیاتی مهم، کارآیی هواپیما کاهش می‌یابد. در چنین مواردی، مأموریت‌های پروازی برنامه‌ریزی شده را نمی‌توان لزوماً در میدان جنگ انجام داد. مثال مهم دیگر، در مورد ماهواره‌ها است. بر اساس پیش‌نویس گزارش کمیسیون بازبینی اقتصادی و امنیتی ایالات متحده و چین، ماهواره Terra EOS AM-1 ناسا که برای مطالعه تغییرات آب و هوایی و محیطی استفاده می‌شد، در اکتبر ۲۰۰۸م، ۹ دقیقه یا بیشتر تداخل را تجربه کرد که توسط دیفنس نیوز به دست آمد [۱۳]. اگر یک مهاجم سایبری ماهواره‌ای را به عنوان هدف انتخاب کند، می‌تواند زیرساخت‌ها و سیستم های حیاتی در میدان نبرد را نیز به عنوان هدف انتخاب کند. به همین ترتیب، سیستم‌های هواپیمای بدون سرنشین (UAS) نیز می‌توانند از طریق جنگ سایبری مورد هدف دشمنان قرار گیرند. مثلاً؛ یک UAS حواصیل که ۸۰-۹۹ درصد وابستگی به نرم‌افزار دارد، مأموریت SAR خود را (شامل برخاستن/ فرود) تنها با فشار دادن دو دکمه در اتاق کنترل انجام می‌دهد.

جدول (۴): زیرساخت‌ها و سیستم‌های حیاتی برای نیروی هوایی.

ردیف	سیستم‌ها
۱	سیستم‌های C4ISR
۲	سیستم‌های پیوند داده
۳	سیستم‌های دفاع هوایی
۴	هواپیما
۵	UASها
۶	سیستم‌های تسلیحاتی
۷	امکانات فرودگاه
۸	سیستم‌های الکتریکی

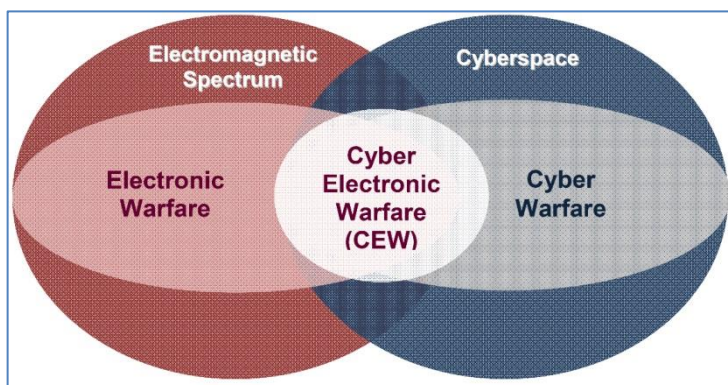
سیستم‌های جدول ۴ به عنوان برخی از زیرساخت‌ها و سیستم‌های حیاتی برای نیروی هوایی تعیین شده‌اند. همان‌گونه که مشاهده می‌شود، اکثر سیستم‌های نیروی هوایی به نرم‌افزار وابسته هستند. بنابراین، دفاع از این سیستم‌ها با روش‌های متعارف کافی نیست. از این‌رو، به‌دست آوردن قابلیت حمله سایبری در کنار دفاع سایبری برای بقای دارایی‌های نیروی هوایی بسیار مهم است. در این زمینه، این مطالعه CEW را به عنوان یک روش حمله سایبری پیشنهاد می‌کند که از دامنه سایبری به منظور تولید شکل پیشرفته‌تری از حمله الکترونیکی استفاده می‌کند.

۵- مفهوم جنگ الکترونیک سایبری

CW و EW ابتدا با هم در جنگ بین روسیه و گرجستان در سال ۲۰۰۸ مورد استفاده قرار گرفتند. قبل از عملیات، برخی از مهاجمان سایبری روسی (یا هکرها) CW را علیه گرجستان از جمله سیستم‌های غیرنظامی با مسدود کردن بسیاری از وب‌سایت‌ها و تغییر زمینه آنها آغاز کردند. پس از این اقدامات، عملیات نظامی آغاز شد [۱۴]. اگرچه این اقدامات بین روسیه و گرجستان CW نامیده می‌شود، یک CW واقعی هنوز اتفاق نیفتاده است. شکل CW آینده‌نگر مشخص نیست، اما تصور می‌شود که سلاح‌های سایبری فعلی، سلاح‌های سایبری احتمالی و حتی سلاح‌های سایبری شدید در اولین CW آینده استفاده خواهند شد.

مطالعات نشان می‌دهد که اگرچه اثرات حملات سایبری در استفاده غیرنظامی شدید است، اما نتایج آن کشنده نیست. گام بعدی CEW با پشتیبانی از تسلیحات متعارف است. قرار است از طیف الکترومغناطیسی و فناوری اطلاعات در جنگ‌ها استفاده شود و کسی که این قدرت را داشته باشد اثرات دلخواه را ایجاد می‌کند. از آن جایی که مطالعات در این زمینه بسیار محرمانه است، جزئیات آن فاش نمی‌شود. با این وجود، مشخص است که کشورهای توسعه یافته در این زمینه کار می‌کنند.

تحلیل‌گران از ایالات متحده تأکید می‌کنند که مبارزه با چریک‌های سایبری غیرنظامی بسیار دشوار است. صاحب‌نظران بر این نظرند که دستگاه‌های جنگ الکترونیکی می‌تواند سیستم‌های SAM معمولی را به راحتی کنترل کند، اما نکته چالش برانگیز شناسایی تروریست‌ها و تحت تأثیر قرار گرفتن واحدهای کنترل است. به دلیل ضعف امنیتی ناشی از شبکه‌های بی‌سیم، اطلاعات در معرض پارگی هستند. حتی اگر سیستم‌های نظامی نرم‌افزار رمزنگاری بسیار قابل اعتمادی دارند، می‌توان این سیستم‌ها را مسدود کرد.



شکل (۳): مفهوم CEW.

همان طور که در شکل ۳ ارائه شده است، در حالی که جنگ الکترونیک از طیف الکترومغناطیسی استفاده می کند و CW از عناصر فضای سایبری استفاده می کند، جنگ الکترونیک سایبری استفاده یکپارچه از همه ی این عناصر را پیشنهاد می کند.

مطالعات درباره سیستم های حمله CEW هنوز در مراحل اولیه خود هستند، اما برخی از آنها در حال توسعه هستند. به عنوان مثال، نیروی دریایی ایالات متحده سلاحی به نام مختل کننده نسل بعدی تولید کردند. برخلاف سیستم های نسل قدیم EW، این سلاح سایبری اطلاعات را توسط دستگاهی مانند رادار تولید می کند و به روشی الگوریتمی انتقال می دهد [۱۵]. رویه های حمله الکترونیک سایبری که در سکوها ی هوایی مورد استفاده قرار می گیرد را می توان به طور خلاصه و به شرح زیر فهرست کرد:

- ترسیم نقشه شبکه دشمن توسط حس گر
- تشخیص دقیق محل آنتن شبکه
- تولید بسته اطلاعاتی شامل الگوریتم با استفاده از آرایه اسکن الکترونیکی
- نفوذ به شبکه هدف با دسترسی به آنتن مناسب

با استفاده از این مراحل می توان به آنتن هدف نفوذ کرد. این روش های حمله ی سایبری می توانند سیستم ارتباطی دشمن را به روش های مختلفی تحت تأثیر قرار دهند: گوش دادن، تغییر ارتباطات آنها یا از بین بردن کامل سیستم آنها [۱۴].

برای بیان شفاف این موضوع باید حمله الکترونیکی که رُکن EW است با حمله الکترونیک سایبری مقایسه شود. در حمله الکترونیکی، رادار هدف گیر می کند و سیگنال پارازیت می تواند به طور مداوم ارسال شود. از طرفی در حمله الکترونیکی سایبری می توان پردازنده ی مرکزی سیستم الکترونیکی را به عنوان هدف انتخاب کرد. هدف اصلی ارسال جریان داده به پردازنده سیستم هدف است. برای موفقیت در این فرآیند زمانی که با حمله الکترونیکی متفاوت است، کافی است. نکته دیگر این است که حمله الکترونیکی را می توان شناسایی کرد و دشمنان می توانند اقدامات احتیاطی

مختلفی را انجام دهند در حالی که تشخیص حمله الکترونیکی سایبری تقریباً غیرممکن است. حتی اگر حمله الکترونیکی سایبری شناسایی شود، ممکن است برای انجام اقدامات احتیاطی در برابر آن دیر باشد.

جدول (۵): مقایسه EW معمولی و CEW.

EW متعارف	CEW
مداوم	ممکن است یک حمله کافی باشد
قابل تشخیص	تشخیص مشکل است
تا حدی مؤثر است	کاملاً مؤثر
نیاز به هوش در مورد هدف	به اطلاعات دقیق در مورد هدف نیاز دارد
بخشی از یک سیستم را هدف قرار می‌دهد	سیستم عصبی مرکزی را هدف قرار می‌دهد
از طیف الکترومغناطیسی استفاده می‌کند	از فضای مجازی از طریق طیف الکترومغناطیسی استفاده می‌کند
جلوه محدودی ایجاد می‌کند	تمام جلوه‌های مورد نظر را ایجاد می‌کند
قادر به نفوذ به هدف	برای نفوذ به هدف باید بر چالش‌های امنیتی غلبه کرد

نرم‌افزار CEW بر منطق سیستم عامل تجهیزات دفاع هوایی دشمن تأثیر می‌گذارد. یک حمله موفقیت‌آمیز CEW ممکن است باعث شود که سیستم عامل خود را چیز دیگری احساس کند. به منظور واقع بینانه‌تر، می‌توان ادعا کرد که نرم‌افزاری که به سیستم عامل هدف تزریق می‌شود، می‌تواند چیزی را ایجاد کند که بدیهی است دشمن انتظارش را ندارد. در واقع، سیستم‌های نظامی توسعه یافته طوری طراحی شده‌اند که بسیار ساده و سریع عمل کنند. حتی اگر رایانه‌های سیستمی آنها نسبت به رایانه‌های معمولی کارایی کمتری دارند، اما از آنجایی که سیستم‌های بسته هستند، در معرض تهدید قرار نمی‌گیرند. این مفهوم قصد دارد چنین سیستم‌های بسته‌ای را در برابر تهدیدات آسیب‌پذیر کند. در حالی که مفهوم CEW در حال پیشرفت است، نرم‌افزار جدید برای برنامه‌های کاربردی CEW در حال ایجاد است. برنامه کامپیوتری Suter، یک سیستم حمله شبکه هابرد، می‌تواند به عنوان مثال برای این مورد ذکر شود. Suter یک برنامه کامپیوتری نظامی است که توسط BAE Systems (شرکت هوافضا و دفاع بریتانیا) توسعه یافته و به شبکه‌های کامپیوتری و سیستم‌های ارتباطی متعلق به دشمن حمله می‌کند. این متخصص برای تداخل با رایانه‌های سیستم‌های یکپارچه دفاع هوایی است. سه نسل از Suter توسعه یافته است. Suter-1 به اپراتورهای خود اجازه می‌دهد تا آنچه را که اپراتورهای رادار دشمن می‌توانند ببینند، نظارت کنند. Suter-2 به آنها اجازه می‌دهد کنترل شبکه های دشمن را در دست بگیرند و حسگرهای آنها را هدایت کنند. Suter-3 که در تابستان ۲۰۰۶ آزمایش شد، امکان

تهاجم به اهداف حساس زمانی مانند پرتابگرهای موشک بالستیک میدان نبرد یا پرتابگرهای متحرک موشک زمین به هوا را فراهم می‌کند. این برنامه با هواپیماهایی مانند EC-130، RC-135 و F-16CJ آزمایش شده است [۱۶].

۶- تجزیه و تحلیل SWOT مفهوم CEW

علاوه بر مزایای عملیاتی CEW در میدان نبرد، می‌توان از آن به عنوان تابعی از نیروی هوایی در آینده نیز استفاده کرد. بنابراین، نیروی هوایی برای CW بسیار مهم و مؤثر خواهد بود. در این تحقیق از روش تحلیل SWOT برای بیان نقاط قوت، ضعف، فرصت‌ها و تهدیدات CEW در میدان نبرد استفاده شده است.

جدول (۶): تجزیه و تحلیل SWOT مفهوم CEW.

نقاط قوت	نقاط ضعف
➤ بسیار سریع زیرا از طیف EM استفاده می‌کند ➤ موجود در هزینه‌های کم ➤ قابل استقرار در سیستم عامل‌های مختلف با توجه به سطح اثر مورد نظر ➤ تحت تاثیر شرایط آب و هوایی قرار نمی‌گیرد ➤ تولید آسان، نیازی به کارخانه‌های جامع ندارد ➤ تشخیص سخت است.	➤ به اطلاعات عمیق و بیش‌تری نیاز دارد ➤ نیاز به غلبه بر برخی موانع برای نفوذ به سیستم‌های دشمن ➤ به گیرنده‌های قدرتمندی برای تشخیص نقاط ضعف سیستم دشمن نیاز دارد
فرصت‌ها	تهدیدها
۱. اثرات مطلوب زمانی به دست می‌آید که کنترل سیستم هدف قرار گیرد ۲. غیرکشنده‌گی را فراهم می‌کند ۳. معیار CDC کم است ۴. می‌تواند بازدارنده باشد ۵. منطق سیستم هدف را می‌توان فریب داد ۶. شبکه‌های بسته را در معرض تهدیدات سایبری قرار می‌دهد ۷. نیروهای هوایی را برای استفاده مؤثر در عملیات سایبری فراهم می‌کند. نیروی هوایی می‌تواند در عملیات سایبری به طور مؤثر diyelim استفاده شود. ۸. حمله استراتژیک علیه مرکز ثقل دشمن را بهبود می‌بخشد	۱. می‌تواند در برابر فریب آسیب‌پذیر باشد ۲. ارزیابی خسارت سخت است

	۹. می‌تواند به دفاع سایبری دشمن حمله کند ۱۰. مقابله با حملات سایبری را فراهم می‌کند ۱۱. می‌تواند با حمله معمولی به طور هم‌زمان اعمال شود ۱۲. اقتصاد نیرو را فراهم می‌کند
خلاصه تحلیل SWOT	
در نتیجه تجزیه و تحلیل، نیروهای هوایی می‌توانند و ممکن است به طور مؤثر در CW مورد استفاده قرار گیرند. با توجه به حملات سایبری علیه سیستم‌های کنترل‌شده رایانه‌ای و روش‌های حمله الکترونیک سایبری برای سیستم‌های دفاع هوایی، نیروی هوایی می‌تواند بیشتر در معرض تهدیدات سایبری قرار گیرد، بنابراین، مهارت‌های حمله سایبری باید به شدت بهبود یابد. به علاوه، تحت تأثیر قرار دادن سیستم‌های رایانه‌ای که نمی‌توانند شبکه‌های بهره‌برداری را تحت تأثیر قرار دهند، توسط CEW می‌تواند آسان باشد. از طرفی، چون CDC آن کم است، استفاده از سیستم‌های حمله الکترونیکی سایبری می‌تواند رشد کند.	

۶- نتیجه‌گیری

در این تحقیق، بر اهمیت فضای سایبری در منطقه رزمی تأکید شده است. روش‌های حمله سایبری با توجه به پیشرفت‌های فناوری اخیر در دو گروه حملات نرم‌افزاری و سخت‌افزاری مورد بررسی قرار می‌گیرند. نوآوری در فناوری، مفاهیم عملیات را تغییر داده و CEW به عنوان یک مفهوم جدید نظامی ظاهر شده است. استفاده یکپارچه از CW و EW می‌تواند از ابتدای جنگ به مناطق عملیاتی گسترده‌ای برسد. ضرورت وجود سلاح سایبری امری اجتناب‌ناپذیر شده است و برای رفع این ضرورت مطالعات خاصی انجام شده و برخی هنوز در حال انجام است. سیستم‌های حمله CEW می‌توانند بر سیستم‌های کامپیوتری و شبکه‌های ارتباطی در میدان نبرد تأثیر بگذارند. سیستم‌های بسته دشمن را می‌توان با تزریق نرم‌افزار مناسبی که در سیگنال‌های هدایت شده به آنها تعبیه شده است، به سیستم‌های باز تبدیل کرد. اگرچه استفاده از مفهوم CEW در یک حمله از نظر فناوری امکان‌پذیر است، اما موانعی مانند پیچیدگی سیستم تهدید، نیاز به هوشمندی، انواع مختلف فایروال‌ها و رمزهای عبور وجود دارد. مفهوم CEW از نظر استفاده از نیروی هوایی در عملیات سایبری نقش مهمی دارد. با توجه به حل مشکلات فوق، مفهوم CEW با استفاده از C4ISR، جنگ الکترونیک و جنگ سایبری در میدان نبرد، باعث پیشرفت‌های زیادی می‌شود.

منابع:

- [1] Cavelty, M. D., "Cyber-Allies," Strengths and Weaknesses of NATO's Cyberdefense Posture. IP Journal, 2011. <https://ip-journal.dgap.org/en/ip-journal/topics/cyber-allies>.
- [2] All About Stuxnet, 2010, Retrieved on 2010-11-06. <http://www.stuxnet.net/>
- [3] Rash, W., "Lockheed Martin Network Attack Highlights Dangers of 'Cyber-Cold War'," Lockheed-Martin Network Attack Highlights Dangers of CyberCold War-190580/, 2011. <http://www.eweek.com/c/a/Security/>
- [4] Electronic Warfare, Joint Publication 3-13.1., 2007.

- [5] Cay, O., “Bilgi Harbi ve Turkiye (Information Warfare and Turkey),” 2009. <http://savunmahaber.wordpress.com/>
- [6] Fahrenkrug, D. T., “Cyberspace Defined,” National Military Strategy for Cyberspace Operations, 2007. http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm
- [7] Cyberspace, Air Force Doctrine Document 2-11, United States Air Force, 2008.
- [8] Koprulu, T., “Ag Destekli Yetenek Kapsamında Siber Savas Konsepti (Scope of Network Enabled Capability Concept Cyber War),” Ankara, 2010.
- [9] Cyber Operations and Cyber Terrorism, DCSINT Handbook No. 1.02, 2005.
- [10] Cifci, H., “Bilgi Harbinden Siber Savaşlara Dogru (From Information Warfare to Cyber Warfares),” Ankara, Unpublished, 2012.
- [11] Alford, L.D., “Cyber Warfare: To Threat to Weapon Systems,” Cyber Warfare: Understanding The Threat To Weapon Systems, WSTIAC (Weapon Systems Technology Information Analysis Center), Quarterly Vol. 9, No. 4, 2009. <http://wstiac.alionscience.com/quarterly>
- [12] Keggler, J. and Mahon, T., “Preparing for Cybergeddon,” Armada International, April-May, 2009, http://findarticles.com/p/articles/mi_hb3031/is_2_33/ai_n31641640/
- [13] Johnson, N. B., “Report: Cyber Attacks Targeted U.S. Satellites,” Defense News, 2011. <http://www.defensenews.com/article/20111028/DEFSECT01/110280301/Report-Cyber-Attacks-Targeted-U-S-Satellites>
- [14] Fulghum, D., “Army Embraces Airborne Electronic and Cyber-warfare,” Aviation Week and Space Technology, 2010.
- [15] Armed Forces Int. Technology Analyst, “Raytheon's Next Generation Jammer Power System Passes Technology Readiness Tests,” 2010. <http://www.armedforces-int.com/news-releases/raytheon-s-next-generation-jammer-power-system-passes-technology-readiness-tests.html>
- [16] Fulghum, D. , Dornheim, M. A. and Scott, W. B., “Black Surprises,” Aviation Week and Space Tech.

طراحی الگوریتم شناسایی تصاویر جعلی با استفاده از شبکه عصبی پیچشی

فاطمه زارع مهرجردی^{۱*}، علی محمد لطیف^۲، محسن سرداری زارچی^۳

۱- دکتری هوش مصنوعی و رباتیک، دانشگاه یزد- zarefateme41@yahoo.com

۲- دانشیار مهندسی کامپیوتر، دانشگاه یزد- alatif@yazd.ac.ir

۳- دانشیار مهندسی کامپیوتر، دانشگاه میبد- sardari@meybod.ac.ir

چکیده:

شناسایی تصاویر جعل یکی از موضوعهای چالش برانگیز در زمینه‌ی بینایی کامپیوتر است. تصاویر منبعی از اطلاعات هستند و در برخی از کاربردها به عنوان سند و شاهد مورد استفاده قرار می‌گیرند، از این رو اعتبار و صحت تصاویر مهم است. امروزه عمل جعل یا دست‌کاری تصویر با استفاده از ابزارهای ویرایش تصویر به راحتی انجام می‌شود. در دست‌کاری تصویر هدف، تغییر دادن مفهوم تصویر و در عین حال حفظ حداکثری یکپارچگی بافت و ساختار تصویر است. یکی از ساده‌ترین روش‌های دست‌کاری تصویر روش جعل کپی- انتقال است. در این روش بخشی از تصویر کپی و در مکان دیگری در همان تصویر منتقل می‌شود. این عمل با هدف پنهان سازی جزئیات خاصی از تصویر یا تکثیر جلوه‌های ویژه در تصویر صورت می‌گیرد. در این پژوهش، هدف طراحی شبکه یادگیری عمیق جهت شناسایی تصاویر جعلی از تصاویر سالم است و برای این منظور دو روش ارائه شده است. در روش اول یک شبکه با سه انشعاب مختلف متشکل از لایه‌های کانولوشن با ساین فیلترهای متفاوت طراحی شده است. این شبکه با تصاویر رنگی و تصاویر حاصل از تجزیه و تحلیل خطا، آموزش و مورد ارزیابی قرار گرفته است. در روش دوم یک شبکه با دو انشعاب متشکل از لایه‌های کانولوشن کاملاً مشابه اما با دو ورودی متفاوت، تصاویر رنگی و تصاویر حاصل از تجزیه و تحلیل خطا طراحی شده است. در هر دو روش انشعاب‌ها با هم ادغام شده و تصاویر به دو گروه جعل و سالم طبقه‌بندی می‌شوند. روش‌های

پیشنهادی با استفاده از پایگاه داده MICC مورد ارزیابی قرار گرفته است و نتایج ارزیابی‌ها عملکرد رضایت‌بخش روش‌های پیشنهادی را نشان می‌دهد.

کلید واژه‌ها: یادگیری عمیق، جعل کپی - انتقال، تجزیه و تحلیل خطا، شبکه عصبی کانولوشنی.

Designing model to identify forgery images using convolutional neural network

Fatemeh Zare Mehrjardi¹, Ali Mohammad Latif², Mohsen Sardari Zarchi³

1- PhD in artificial intelligence and robotics, Yazd University - zarefateme41@yahoo.com

2- Associate Professor of Computer Engineering, Yazd University – alatif@yazd.ac.ir

3- Associate Professor of Computer Engineering, Meybod University – sardari@meybod.ac.ir

Abstract

Detecting forgery images is one of the most challenging topics in computer vision. Images are a source of information and are used as documents and evidence in various applications, so the validity and accuracy of images are crucial. Today, it is easy to manipulate an image using image editing tools. In image manipulation, the goal is to change the concept of the image while maintaining the maximum integrity of its texture and structure. Copy-move forgery is one of the simplest image manipulation methods. In this method, a part of the image is copied and pasted to another place in the same image with the purpose of hiding certain details of the image or adding special effects. The purpose of this research is to design a deep learning network that can identify forgery images from healthy ones. Two methods are presented for this purpose. In the first method, a network with three different branches consisting of convolution layers with different filter sizes is designed. This network has been trained and evaluated using color images and error level analysis images. In the second method, a network with two branches consisting of completely similar convolution layers but with two different inputs, color images and error level analysis images, is designed. In both methods, the branches are merged, and the images are classified into forgery and healthy groups. The proposed methods have been evaluated using the MICC dataset, and the evaluation results show the satisfactory performance of the proposed methods.

Keywords: Deep Learning, Copy-move forgery, Error Analysis, Convolutional Neural Network.

۱- مقدمه

تصویر به عنوان یکی از ابزارهای ارتباطی قوی و مهم بین انسان‌ها شناخته شده است. این یک حقیقت است که ارزش یک تصویر بیشتر از هزار کلمه است. با توسعه و گسترش دستگاه‌های دیجیتالی مانند دوربین و موبایل در هر لحظه از زمان و مکان تصویربرداری به راحتی امکان‌پذیر است. در بعضی از کاربردها تصاویر دیجیتال می‌توانند به عنوان سند مورد استفاده قرار گیرند. بنابراین، صحت و اعتبار تصویر اهمیت دارد. جعل تصویر به معنای دست‌کاری در تصویر دیجیتال است. امروزه با استفاده روزافزون از نرم افزارهای مدرن ویرایش تصویر مانند فتوشاپ دست‌کاری تصاویر دیجیتال به راحتی انجام می‌شود.

هدف دست‌کاری، پنهان کردن برخی از اطلاعات مفید یا اضافه کردن اطلاعات غلط یا اضافی به تصویر است. با جعل تصویر یکپارچگی و اصالت تصویر در ساختار و بافت تصویر دست‌کاری می‌شود. اگر تصویر مورد استفاده به عنوان

سند دست‌کاری شود دیگر قابل اعتماد نخواهد بود. تصاویر دیجیتال به کمک روش‌های مختلفی جعل می‌شوند. رویکردهای موجود برای تشخیص جعل تصاویر دیجیتال را می‌توان به طور کلی به دو دسته‌ی عمده رویکرد فعال و رویکرد غیرفعال طبقه‌بندی کرد [۱].

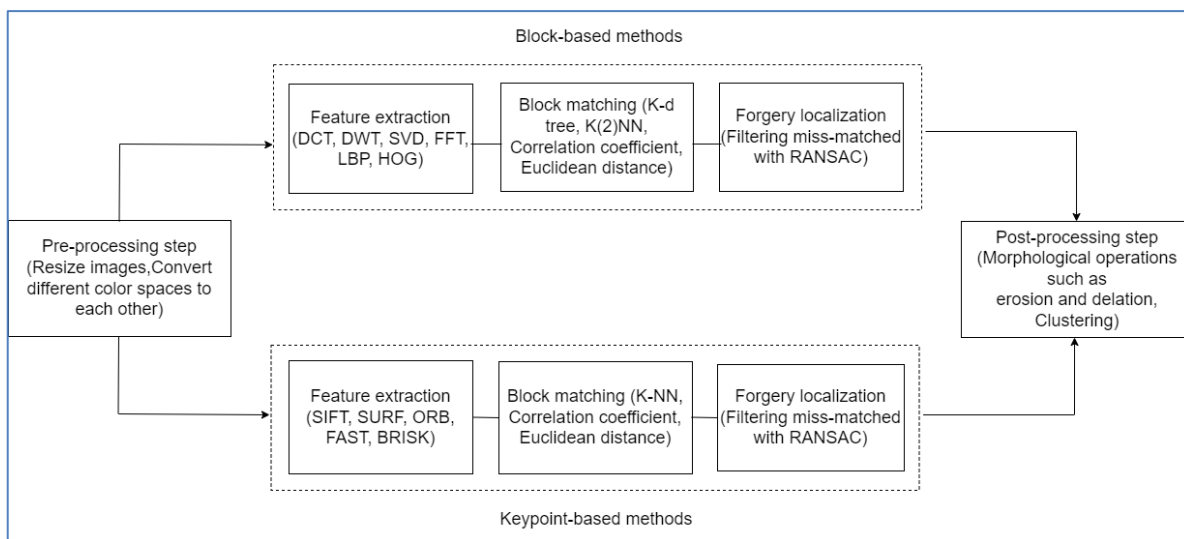
در رویکرد فعال، ابتدا بر روی تصاویر پیش پردازش اعمال شده، سپس، با تعبیه کردن اطلاعات درون تصاویر اصلی عمل دست‌کاری انجام می‌شود. امضای دیجیتال و واترمارکینگ را می‌توان به عنوان مثال‌هایی از رویکرد فعال نام برد. در رویکرد غیرفعال که به عنوان رویکرد کور شناخته می‌شود، نیازی به پیش پردازش تصویر نیست. رویکرد غیرفعال با تحلیل محتوا و ساختار تصویر، جعلی بودن یا نبودن تصویر را تشخیص می‌دهد و ناسازگاری‌ها را کشف می‌کند. جعل کپی - انتقال^۱، اتصال تصویر^۲، روتوش تصویر^۳ و حذف شی^۴ از جمله مثال‌های رویکرد غیرفعال است [۲].

روش کپی - انتقال یکی از ساده‌ترین و رایج‌ترین روش‌های دست‌کاری تصاویر است. این روش بخشی از تصویر را کپی و در محل دیگر از همان تصویر انتقال می‌دهد. انگیزه‌ی چنین جعلی، پنهان کردن بخشی از تصویر، تأکید بر بخشی از تصویر و درج اطلاعات غلط در تصویر است. از آن جایی که بخش کپی شده متعلق به همان تصویر است، از لحاظ پویایی و رنگ با بقیه تصویر سازگاری دارد. همراه با عمل کپی و انتقال تبدیل‌های هندسی مانند چرخش^۵ و مقیاس‌بندی^۶ و عملیات پس پردازش مانند محو کردن، تغییر روشنایی، فشرده‌سازی و افزودن نویز به تصویر نیز انجام می‌شود تا ناحیه دست‌کاری شده برای چشم انسان به راحتی قابل تشخیص نباشد [۱ و ۲]. شکل ۱ مثالی از جعل کپی - انتقال را نشان می‌دهد.



شکل (۱): تعدادی از تصاویر موجود در پایگاه داده MICC (سطر اول تصاویر سالم و سطر دوم تصاویر جعلی با روش کپی - انتقال) [۳].

با توجه به مطالعه‌های انجام شده، الگوریتم‌های تشخیص جعل کپی - انتقال را می‌توان به دو گروه اصلی سنتی و مبتنی بر یادگیری عمیق تقسیم‌بندی کرد. الگوریتم‌های تشخیص سنتی خود به دو روش بر پایه‌ی بلوک‌بندی^[۳] و یافتن نقاط کلیدی^[۴] در تصویر تقسیم می‌شوند. شکل ۲ مراحل الگوریتم‌های تشخیص سنتی را نشان می‌دهد.



شکل (۲): مراحل تشخیص جعل به روش سنتی[۲].

در روش بر پایه‌ی بلوک‌بندی ابتدا تصویر به نواحی مستطیل یا دایره‌ای شکل هم‌پوشان و غیرهم‌پوشان تقسیم شده و برای هر کدام از این نواحی یک بردار ویژگی محاسبه می‌شود. در مرحله بعد بردارهای ویژگی مشابه با هم انطباق می‌یابند و حمله کپی - انتقال تشخیص داده می‌شود. عیب این روش پیچیدگی محاسباتی بالا و عملکرد ضعیف در برابر تغییرات هندسی و عملیات پس‌پردازش است[۴].

در روش‌های مبتنی بر نقاط کلیدی ابتدا ویژگی‌های نواحی با آنروپی بالا به‌دست می‌آیند و سپس، ویژگی‌های مشابه تطبیق می‌یابند. در روش مبتنی بر نقاط کلیدی، ویژگی با استفاده از روش‌های مختلف مانند SIFT, SURF بدون تقسیم‌بندی تصویر استخراج می‌شود. نقاط ویژگی با استفاده از رویکردهای مختلف مانند خوشه‌بندی، فاصله اقلیدسی با یکدیگر تطابق داده شده و جعل مشخص می‌شود. این روش دارای محاسبات کم و مقاومت مناسب در برابر تبدیل‌های هندسی است[۵].

روش یادگیری عمیق امروزه در بیشتر مسائل وارد شده است و نتایج خوبی را به دست آورده است. الگوریتم‌های یادگیری عمیق زیرمجموعه‌ای از الگوریتم‌های یادگیری ماشین هستند که هدف آنها کشف چندین سطح از بازنمودهای (نمایش‌های) توزیع شده از داده ورودی است. برخلاف دو روش بر پایه بلوک‌بندی و نقاط کلیدی، روش یادگیری عمیق تمام مراحل را به صورت خودکار انجام می‌دهد و ویژگی‌های سطح بالا را از روی داده‌ها استخراج می‌کند و از استخراج ویژگی به صورت دستی جلوگیری می‌کند. یکی از چالش‌های روش یادگیری عمیق نیاز به داده زیاد برای آموزش است. استفاده از شبکه‌های از پیش آموزش داده شده با پایگاه داده‌های بزرگ از جمله ImageNet.

روش انتقال دانش و روش‌های تقویت داده برای افزایش تعداد داده‌ها برای حل مشکل کمبود داده ارائه شده‌اند [۱] و [۲].

۲- مروری بر کارهای گذشته

در سال‌های اخیر مطالعه‌های زیادی برای تشخیص جعل کپی - انتقال با استفاده از سه رویکرد براساس بلوک‌بندی، مُبَتَنی بر نقاط کلیدی و یادگیری عمیق انجام شده است. خلاصه‌ای از برخی از این مطالعه‌ها در این بخش آورده شده است. برای مثال، یک روش مُبَتَنی بر بلوک‌بندی با استفاده از ترکیب دو الگوریتم DCT و PCA در سال ۲۰۱۶م ارائه شده است. برای این منظور ابتدا در مرحله پیش‌پردازش، تصاویر رنگی به تصاویر سطح خاکستری تبدیل شده است. سپس، تصاویر به بلوک‌های مربعی شکل و به صورت هم‌پوشان تقسیم‌بندی شده‌اند و از هر بلوک با استفاده از الگوریتم DCT یک بردار ویژگی استخراج شده است. بردارهای ویژگی استخراج شده دارای ابعاد فضای ویژگی بالایی هستند، جهت کاهش ابعاد فضای ویژگی از الگوریتم PCA استفاده شده است. در نهایت برای تشخیص جفت بلوک مشابه و تشخیص ناحیه جعل، از مقایسه فاصله اقلیدسی بین تمام جفت بلوک‌ها استفاده شده است [۶].

در مطالعه‌ای دیگر جهت تشخیص جعل کپی - انتقال از روش مُبَتَنی بر بلوک‌بندی و ترکیب دو الگوریتم DCT و SVD استفاده شده است. ابتدا در مرحله پیش‌پردازش تصاویر رنگی به تصاویر خاکستری تبدیل شده و تصاویر به بلوک‌های هم‌پوشان تقسیم‌بندی شده‌اند. در مرحله استخراج ویژگی از ترکیب دو الگوریتم DCT و SVD جهت به دست آوردن بردارهای ویژگی کوچک و منحصر به فرد استفاده شده است. سپس، در مرحله تطابق ویژگی و یافتن جفت بلوک مشابه از مقایسه جفت بلوک‌ها با استفاده از روش فاصله اقلیدسی استفاده شده است [۷].

در روش مُبَتَنی بر نقاط کلیدی، بر خلاف روش مُبَتَنی بر بلوک‌بندی نیازی به تقسیم‌بندی تصاویر نیست و با استخراج نقاط کلیدی از نواحی با آنتروپی بالا، عمل تشخیص جعل انجام می‌شود، از این رو نسبت به روش بلوک‌بندی سریع‌تر است. برای مثال یک روش تشخیص جعل با نقاط کلیدی و با استفاده از الگوریتم استخراج‌کننده نقاط کلیدی به نام SIFT توسط Alberry و همکاران ارائه شده است. از این‌رو در مرحله استخراج ویژگی، بدون تقسیم‌بندی تصویر و با استفاده از الگوریتم SIFT نقاط کلیدی تصاویر کشف شده است. سپس، در مرحله تطابق ویژگی از الگوریتم خوشه‌بندی C-means جهت شناسایی نقاط کلیدی مشابه استفاده شده است [۸].

یکی از مشکلات روش نقاط کلیدی عملکرد ضعیف این روش در تشخیص جعل نواحی هموار و کوچک به‌خاطر کمبود نقاط کلیدی کافی است. برای حل این مشکل محققان معمولاً از ترکیب تعدادی الگوریتم استخراج‌کننده نقاط کلیدی استفاده می‌کنند. برای مثال یک روش تشخیص جعل مُبَتَنی بر نقاط کلیدی با استفاده از ترکیب دو الگوریتم استخراج‌کننده نقاط کلیدی SURF و A-KAZE ارائه شده است. بعد از استخراج نقاط کلیدی با استفاده از الگوریتم فاصله اقلیدسی، شباهت جفت نقاط کلیدی محاسبه و مرتب شده است. سپس، با استفاده از الگوریتم دو نزدیک‌ترین همسایگی نقاط کلیدی مشابه کشف شده است [۹].

برخی محققان از ترکیب دو روش نقاط کلیدی و روش بلوک‌بندی جهت تشخیص جعل استفاده می‌کنند. یک نمونه از روش ترکیبی توسط Narayanan و همکاران ارائه شده است. بدین‌ترتیب ابتدا تصاویر به بلوک‌های مستطیل شکل و

همپوشان تقسیم‌بندی شده و نقاط کلیدی هر بلوک با استفاده از الگوریتم استخراج‌کننده نقاط کلیدی SIFT کشف شده است. در مرحله تطابق ویژگی از الگوریتم فاصله اقلیدسی جهت یافتن نقاط کلیدی مشابه هر بلوک استفاده شده است. در پایان اگر تعداد نقاط کلیدی تطابق‌یافته از سطح آستانه بیشتر باشد، جفت بلوک مشابه شنا سایی شده است [۱۰].

بر خلاف دو روش نقاط کلیدی و مبتنی بر بلوک‌بندی که شامل مراحل برای استخراج ویژگی و تطابق ویژگی جهت تشخیص جعل هستند، روش یادگیری عمیق تمام مراحل این فرآیند را به صورت یکجا و به صورت خودکار انجام می‌دهد، اما جهت آموزش شبکه‌های یادگیری عمیق، داده زیادی مورد نیاز است. برای مثال یک روش مبتنی بر یادگیری عمیق جهت شناسایی تصاویر جعلی توسط Elaskily و همکاران ارائه شده است. در این روش به دلیل کمبود داده در حوزه جعل از شبکه‌های از پیش آموزش دیده شده با پایگاه داده بزرگ imagenet و مفهوم یادگیری انتقالی^[۱۱] استفاده شده و پارامترهای شبکه با داده‌های کم موجود تنظیم شده است. در نهایت تصاویر در دو دسته تصاویر اصلی و تصاویر جعل طبقه‌بندی شده‌اند [۱۱].

در مطالعه‌ای دیگر از شبکه یادگیری عمیق از پیش آموزش داده شده AlexNet جهت تشخیص جعل استفاده شده است. در این روش از شبکه از پیش آموزش داده شده AlexNet به عنوان یک واحد استخراج‌کننده ویژگی^{۱۲} استفاده شده است و از تمام تصاویر سالم و جعل یک بردار ویژگی استخراج شده است. در نهایت این بردارهای ویژگی به طبقه‌بند ماشین بردار پشتیبان^{۱۳} داده شده و تصاویر در دو دسته سالم و جعل دسته‌بندی شده‌اند [۱۲].

در این پژوهش هدف تشخیص تصاویر جعل با استفاده از روش یادگیری عمیق است. برای این منظور شبکه‌ای عصبی کانولوشن با بیش از یک انشعاب، با لایه‌ها و ورودی‌های مختلف و با استفاده از مفهوم API عملکردی طراحی شده است که در ادامه آورده شده است.

۳- مفاهیم پایه

۳-۱- شبکه عصبی کانولوشن

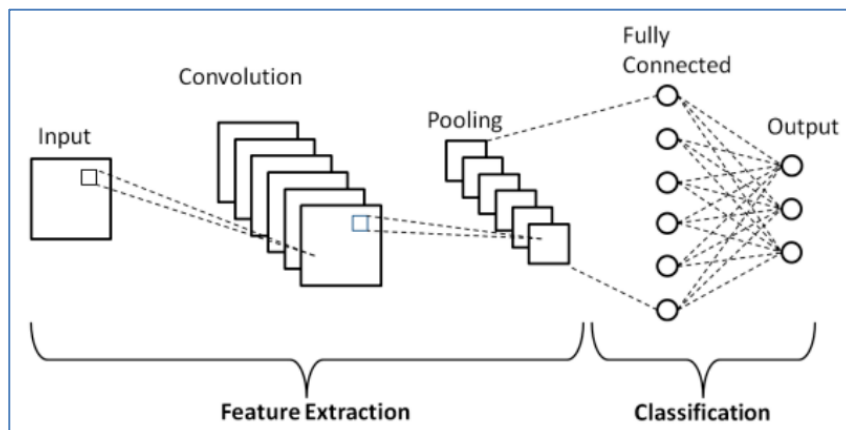
شبکه‌های عصبی کانولوشن یکی از مهم‌ترین روش‌های یادگیری عمیق در کاربردهای مختلف بینایی کامپیوتر هستند. شبکه عصبی کانولوشن نوعی شبکه عصبی مصنوعی است که از پرسپترون چندگانه استفاده می‌کند. یکی از مزایای استفاده از شبکه عصبی کانولوشن، استفاده از انسجام مکانی محلی در تصاویر ورودی است که به آنها اجازه می‌دهد تا با به اشتراک گذاشتن برخی پارامترها، وزن کمتری داشته باشند. این فرآیند از نظر حافظه و پیچیدگی کارآمد است. به طور کلی، یک شبکه عصبی کانولوشن از سه لایه اصلی لایه کانولوشن^{۱۴}، لایه پولینگ^{۱۵} و لایه کاملاً متصل^{۱۶} تشکیل می‌شود و هر لایه وظیفه خاصی را بر عهده دارند [۱۳].

لایه کانولوشن به عنوان اصلی‌ترین لایه در این دسته از شبکه‌های عصبی محسوب می‌شود به همین دلیل، آنها را به عنوان شبکه‌های عصبی کانولوشن می‌شناسند. وظیفه این لایه استخراج ویژگی‌ها است. لایه‌های اول معمولاً ویژگی‌های سطح پایین (مانند لبه‌ها، خط‌ها و گوشه‌ها) و لایه‌های بالاتر ویژگی‌های سطح بالا (مانند قواعد و شکل‌ها) را استخراج می‌کنند. این لایه عملیات کانولوشن را بر روی داده ورودی اعمال می‌کند و خروجی‌هایی به نام نقشه ویژگی^{۱۷} از این لایه به دست می‌آید. در نتیجه، تمامی نرون‌ها در یک نقشه ویژگی، مجموعه‌ای از وزن‌ها و بایاس‌های

مشابه و مشترکی دارند. این اشتراک وزن‌ها باعث کاهش تعداد پارامترهای مورد نیاز برای آموزش می‌گردد. در شبکه‌های کانولوشن با استفاده از فیلتر، اتصالات به صورت نواحی کوچک و محلی صورت می‌گیرد. به بیان دیگر هر نرون در نخستین لایه مخفی به ناحیه کوچکی از نرون‌های ورودی متصل است. بر روی هر تصویر می‌توان چندین نوع فیلتر اعمال کرد که در نتیجه به تعداد فیلترها، همان تعداد عمق ایجاد می‌شود. رایج‌ترین شکل استفاده از این لایه به صورت لایه‌ای با فیلترهایی به اندازه سائز 3×3 و اندازه گام 1×1 با مقدار ۱ است.

در یک شبکه عصبی کانولوشن به طور معمول پس از هر لایه کانولوشن یک لایه پولینگ قرار می‌گیرد. این لایه از آن جهت اهمیت دارد که باعث کاهش تعداد پارامترها می‌شود. این لایه بر روی هر برش از لایه‌های عمق ورودی اعمال می‌شود و اندازه‌ی آن را تغییر می‌دهد. دو تابع عملکردی معروف این لایه، پولینگ بیشینه و میانگین‌اندازند. طریقه عمل پولینگ بیشینه بدین صورت است که در هر پنجره، بزرگ‌ترین پیکسل را به خروجی می‌فرستد. به دلیل اعمال عملیات بر روی تمامی برش‌ها، عمق خروجی همان عمق ورودی به لایه پولینگ است و تغییری نمی‌کند. به علت برش‌ها، عمق خروجی همان عمق ورودی به لایه پولینگ است و تغییری نمی‌کند. رایج‌ترین شکل استفاده از این لایه به صورت لایه‌ای با فیلترهایی به اندازه سائز 2×2 و اندازه گام با مقدار ۲ است.

در انتهای یک شبکه عصبی کانولوشن، خروجی آخرین لایه پولینگ به عنوان ورودی به لایه کاملاً متصل عمل می‌کند. یک یا چند مورد از این لایه‌ها وجود دارد. لایه کاملاً متصل به این معنی است که هر گره در لایه اول به هر گره در لایه دوم وصل می‌شود. در واقع این لایه به عنوان لایه پایانی و لایه امتیازدهی برای خروجی سیستم در نظر گرفته می‌شود [۱۳]. شکل ۳ ساختار شبکه عصبی کانولوشن را نشان می‌دهد.

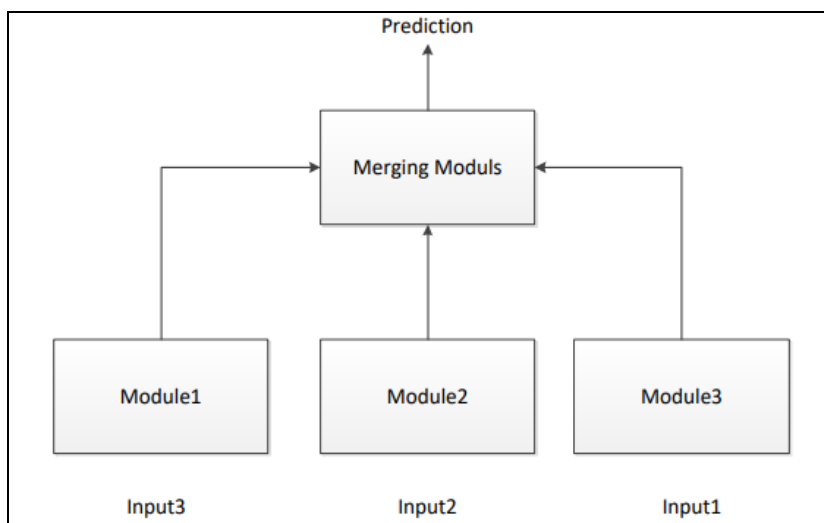


شکل (۳): ساختار شبکه عصبی کانولوشن [۱۳].

۲-۳- مفهوم API عملکردی

معمولاً معماری‌های یادگیری عمیق با استفاده از روش مدل ترتیبی ساخته می‌شوند. به این معنی که لایه‌ها همانند یک پشته خطی در کنار هم قرار دارند و هر لایه یک ورودی و یک خروجی دارد. گاهی در مسائل مختلف شبکه، ممکن است به تعدادی ورودی مستقل نیاز داشته باشد، برخی از شبکه‌ها باید بیش از یک خروجی داشته باشند و یا دارای

انشعابات داخلی در بین لایه‌ها باشند، این موارد با مفهوم API شناخته می‌شوند [۱۴]. شکل ۴ طرز کار مفهوم API عملکردی را نمایش می‌دهد.



شکل (۴): طرز کار مفهوم API عملکردی.

۳-۳- تجزیه و تحلیل سطح خطا

تجزیه و تحلیل سطح خطا امکان شناسایی مناطقی در یک تصویر که در سطوح مختلف فشرده‌سازی هستند، را نشان می‌دهد. در یک تصویر JPEG، کل تصویر باید در یک سطح از فشرده‌سازی باشد. اگر بخشی از تصویر دارای تفاوت قابل توجهی باشد، نشان‌دهنده یک تغییر دیجیتال است [۱۵]. ELA تفاوت در نرخ فشرده‌سازی JPEG را برجسته می‌کند. مناطق با رنگ‌بندی یکنواخت، مانند آسمان آبی یا دیوار سفید نسبت به لبه‌های با کنتراست بالا نتیجه ELA کمی خواهند داشت. بنابراین، اگر در یک تصویر جعل رخ داده باشد، نرخ فشرده‌سازی ناحیه جعل متفاوت خواهد بود، بنابراین، از ELA برای تشخیص جعل می‌توان استفاده کرد.

۳-۴- پایگاه داده MICC

پایگاه داده MICC یکی از معروف‌ترین و قدیمی‌ترین پایگاه داده‌های موجود در زمینه تشخیص جعل است. این پایگاه داده دارای چهار زیرمجموعه با نام‌های MICC-F220، MICC-F600، MICC-F2000 و MICC-F8multi است. تصاویر موجود در این پایگاه داده با روش جعل کپی-انتقال به وجود آمده است. همراه با عمل جعل برخی از تبدیل‌های هندسی از جمله چرخش و مقیاس‌بندی بر روی ناحیه جعل اعمال شده است. پایگاه داده MICC دارای معیایی نیز هست که در ادامه آورده شده است [۳]:

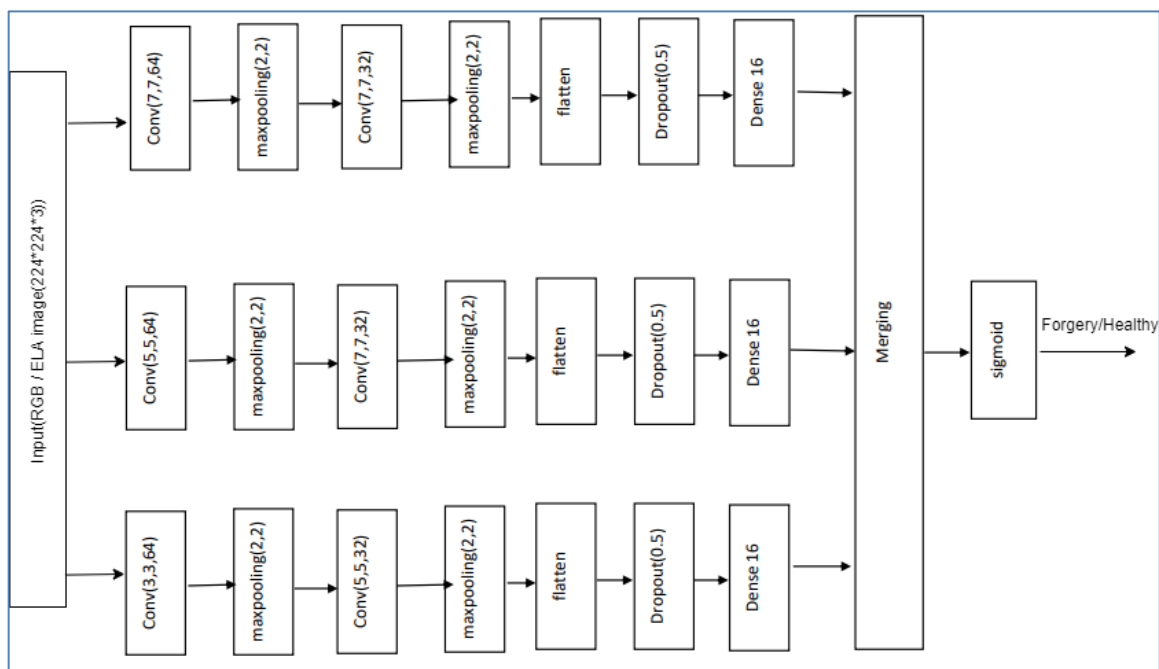
۱- در این پایگاه داده تصاویر جعلی هیچ عملیات پس‌پردازشی ندارند.

- ۲- تصاویر جعلی موجود در سه زیرمجموعه MICC-F220، MICC-F2000 و MICC-F8multi بدون ماسک حقیقی است که نشان‌دهنده ناحیه جعل است.
- ۳- اندازه‌ی تصاویر در این پایگاه داده بزرگ است و برای الگوریتم‌های مبتنی بر بلوک‌بندی زمان‌بر است، این پایگاه داده برای الگوریتم‌های نقاز کلیدی مناسب است
- ۴- تصاویر سالم و جعل در این پایگاه داده محدود و نامتعادل است و تعداد تصاویر جعل کمتر است [۳].

۴- روش پیشنهادی

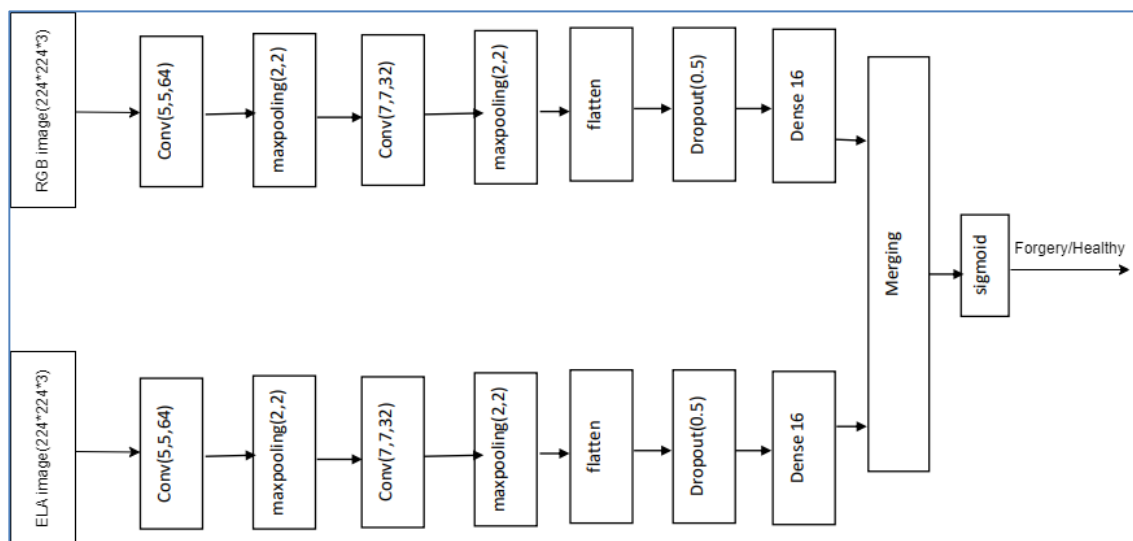
در این پژوهش با استفاده از مطالب مطرح شده در قسمت مفاهیم پایه دو روش متفاوت بررسی شده است.

روش اول: در این حالت از مفهوم API عملکردی استفاده شده و یک معماری کم عمق طراحی شده است که دارای سه انشعاب با تعداد لایه‌های یکسان، دو لایه کانولوشن، دو لایه پولینگ بیشینه و دو لایه کاملاً متصل است. از آنجا که اطلاعات مفید برای تشخیص جعل در لایه‌های ابتدایی شبکه موجود است از طراحی شبکه با تعداد لایه‌های بیشتر خودداری شده است. هر سه انشعاب از لحاظ تعداد لایه‌ها و تعداد فیلترها برابر هستند، ولی اندازه فیلترها متفاوت انتخاب شده است. در برخی از تصاویر، عمل جعل همراه با عملیات مقیاس انجام می‌شود انتخاب اندازه فیلترها با مقادیر ۳، ۵ و ۷ در سه انشعاب می‌تواند در تشخیص جعل همراه با عملیات مقیاس نقش مهمی رداشته باشد. در ادامه خروجی سه انشعاب با هم ادغام شده و پیش‌بینی نهایی با لایه امتیازدهی با یک نرون و تابع سیگموید انجام می‌شود. شبکه طراحی شده طی ۲۵ تکرار هم با تصاویر رنگی و هم با تصاویر حاصل از ELA آموزش داده می‌شود. شکل ۵ روندنمای رویکرد اول را نشان می‌دهد.



شکل (۵): روندنمای روش پیشنهادی اول.

روش دوم: در این حالت یک معماری دارای دو انشعاب با تعداد لایه‌ها، تعداد فیلترها و اندازه فیلتر یکسان، ولی با ورودی‌های متفاوت طراحی شده است. مانند رویکرد اول نقشه‌های ویژگی دو انشعاب با هم ادغام شده و با تابع سیگموید پیش‌بینی نهایی انجام می‌شود. شبکه طراحی شده طی ۲۵ بار تکرار با ورودی‌های متفاوت تصاویر رنگی و تصاویر حاصل از ELA آموزش داده می‌شود. شکل ۶ روند رویکرد دوم را نشان می‌دهد.



شکل (۶): روندنمای روش پیشنهادی دوم.

۵- ارزیابی نتایج

برای ارزیابی روش پیشنهادی از تصاویر سالم و جعل سه زیر مجموعه MICC-F220، MICC-F600 و MICC-F2000 استفاده شده است. از آن جا که مجموع تصاویر سالم با مجموع تصاویر جعل برابر نیست و در فرآیند آموزش احتمال سوگیری وجود دارد، به تعداد مساوی از هر کدام از مجموعه تصاویر جعل و سالم تصویر انتخاب شده است. برای افزایش تعداد تصاویر برای آموزش شبکه از روش تقویت داده استفاده شده است. در این روش با انجام عملیات انتقالی متفاوت مانند چرخش، برش دادن و بزرگ‌نمایی بر روی تصاویر موجود در پایگاه داده، تعداد تصاویر را افزایش می‌دهند.

برای ارزیابی روش اول یک‌بار تصاویر رنگی و بار دیگر تصاویر حاصل از ELA به شبکه که دارای سه انشعاب متفاوت است داده می‌شود. تعداد لایه‌ها و فیلترهای هر انشعاب برابر، ولی در اندازه فیلترها متفاوت هستند. در ادامه خروجی سه انشعاب با هم ادغام شده و در نهایت تصویر در یکی از دو دسته جعل و سالم قرار داده می‌شود. فرآیند آموزش شبکه پیشنهادی ۲۵ تکرار می‌شود. جدول ۱ میزان دقت و تابع زیان نتایج روش اول را نشان می‌دهد.

جدول (۱): نتایج ارزیابی روش پیشنهادی اول.

نوع تصاویر	معیار	Acc	Loss
رنگی	Train	۹۵/۳۱	۰/۱۴۵۲

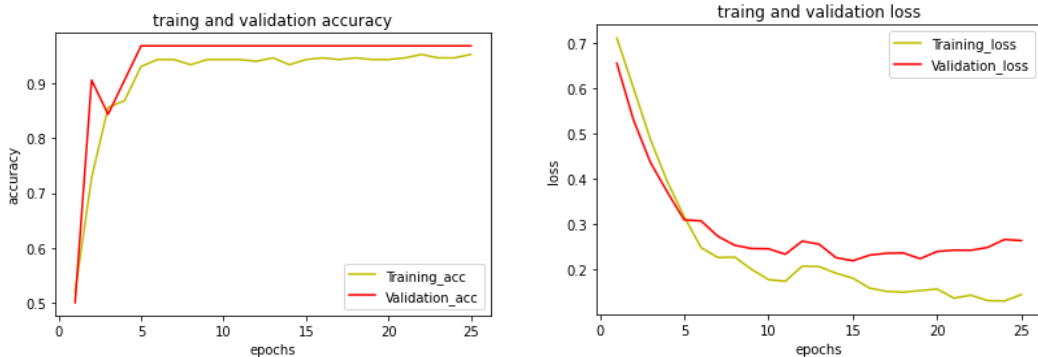
	Test	۹۶/۸۸	۰/۲۱۹۷
ELA	Train	۹۵/۸۷	۰/۱۸۵۳
	Test	۹۶/۳۹	۰/۲۱۹۲

در روش دوم شبکه طراحی شده دارای دو انشعاب مشابه است و تعداد لایه‌ها، تعداد فیلترها و اندازه‌ی آنها مشابه در نظر گرفته شده است. برای ارزیابی این رویکرد دو ورودی متفاوت تصاویر رنگی و تصاویر حاصل از ELA به شبکه داده می‌شود. نقشه‌های ویژگی دو انشعاب با هم ادغام شده و با تابع سیگموئید تصاویر طبقه‌بندی می‌شوند. شبکه طی ۲۵ تکرار آموزش داده می‌شود. جدول ۲ میزان دقت و تابع زیان این رویکرد را نشان می‌دهد.

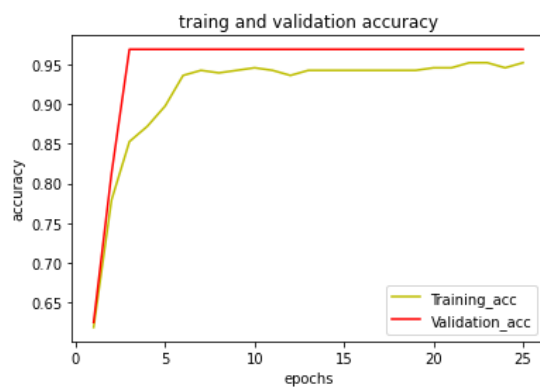
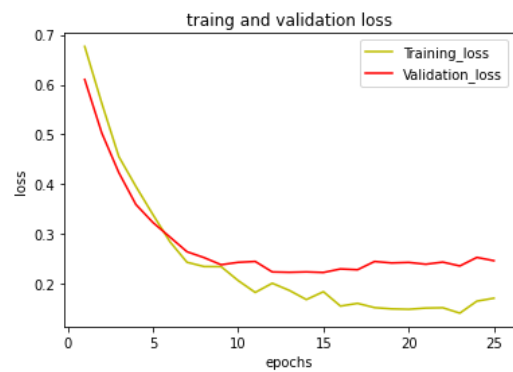
جدول (۲): نتایج ارزیابی روش پیشنهادی دوم.

	Acc	Loss
Train	۹۵/۳۰	۰/۱۴۲۲
Test	۹۶/۹۱	۰/۲۱۴۵

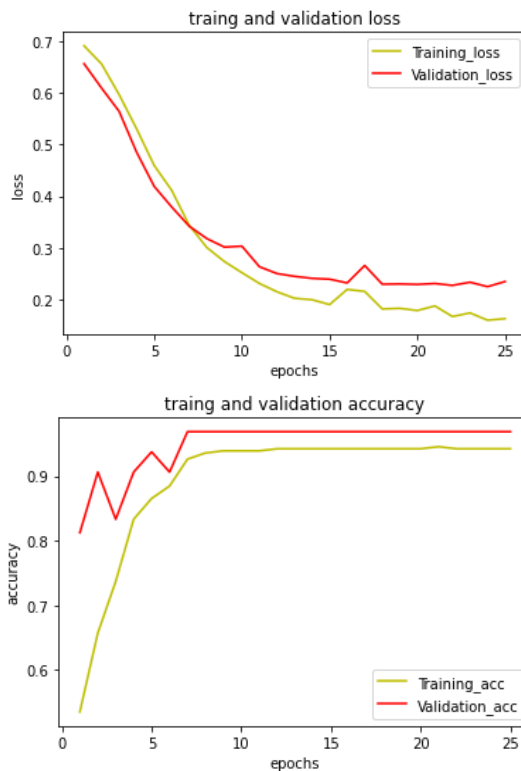
لازم به ذکر است برای هر دو روش پیشنهادی از بهینه‌ساز Adam با نرخ یادگیری ۰,۰۰۰۱ استفاده شده است. نمودار دقت و تابع زیان این دو روش بر روی تصاویر رنگی و تصاویر ELA در شکل ۷ آورده شده است.



روش اول (تصاویر رنگی)



روش اول (تصاویر ELA)



روش دوم

شکل (۷): نمودار دقت و تابع زیان دو روش پیشنهادی بر روی تصاویر رنگی و ELA.

برای مقایسه‌ی روش‌های پیشنهادی با روش‌های دیگران دو روش دیگر بررسی شده است. در مقاله [۱۲] از شبکه از پیش‌آموزش دیده‌شده AlexNet به عنوان استخراج‌کننده‌ی ویژگی استفاده شده است. از هر تصویر یک بردار ویژگی استخراج شده و سپس، با استفاده از الگوریتم ماشین بردار پشتیبان تصاویر در دو دسته سالم و جعل طبقه‌بندی شدند. در مقاله دیگر [۱۶] از شبکه از پیش‌آموزش داده شده MobileNetV2 و مفهوم انتقال دانش برای این منظور استفاده شده است. نتایج مقایسه در جدول ۳ آورده شده است.

جدول (۳): مقایسه روش پیشنهادی با کارهای دیگران.

روش	Accuracy
مقاله [۱۲]	۹۴/۴۶
مقاله [۱۶]	۹۳/۳۸
روش اول (تصاویر ELA)	۹۶/۳۹
روش اول (تصاویر رنگی)	۹۶/۸۸
روش دوم	۹۶/۹۱

۶- نتیجه‌گیری

تصاویر در زندگی امروزی انسان‌ها نقش مهمی دارد و از آن در برخی کاربردها به عنوان سند استفاده می‌شود. تصاویر با روش‌ها و ابزارهای مختلف و به سادگی می‌توانند دست‌کاری شوند، و اعتبار خود را از دست دهند. بنابراین، تشخیص تصویر جعل یک موضوع مهم در دنیای امروز به حساب می‌آید تا بتوان از حوادث ناگوار بعدی جلوگیری کرد. روش‌های سنتی موجود از قبیل روش بلوک‌بندی و نقاط کلیدی برای تشخیص جعل، دارای مشکلاتی است. هر دو روش تنها قادر به تشخیص تصاویر جعل از نوع کپی-انتقال هستند. روش بلوک‌بندی دارای محاسبات زیاد و ناکارآمدی در برابر تبدیلات هندسی است. روش نقاط کلیدی اگر چه در برابر تبدیلات هندسی مقاوم است، ولی وابستگی به نقاط کلیدی یکی از ضعف‌های این روش است. در سال‌های اخیر از روش‌های یادگیری عمیق در همه‌ی زمینه‌ها از جمله تشخیص جعل استفاده می‌شود. در این پژوهش از شبکه عصبی کانولوشن و مفهوم API عملکردی و تصاویر ELA استفاده شده و شبکه‌هایی با دو و سه انشعاب با ورودی‌های متفاوت و سائز فیلترهای متفاوت برای غلبه بر تبدیل‌های هندسی و عملیات پس‌پردازش ارائه شده است. نتیجه‌ی ارزیابی‌ها و مقایسه با کارهای دیگران از عملکرد رضایت‌بخش، روش پیشنهادی است.

منابع:

- [1] Mehrjardi, F. Z., Latif, A. M., and Zarchi, M. S., "Copy-move forgery detection and localization using deep-learning," *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 37, No. 9, pp. 1-21, 2023.
- [2] Mehrjardi, F. Z., Latif, A. M., Zarchi, M. S., and Sheikhpour, R., "A survey on deep learning-based image forgery detection," *Pattern Recognition*, Vol. 144, pp. 1-31, 2023.
- [3] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., and Serra, G., "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," *Signal Processing: Image Communication*, Vol. 28, No. 6, pp. 659-669, 2013.
- [4] Mohamadian, Z., and Pouyan, A. A., "Detection of duplication forgery in digital images in uniform and non-uniform regions," In *15th International Conference on Computer Modelling and Simulation*, IEEE pp. 455-460, 2013.
- [5] Mahmood, T., Nawaz, T., Ashraf, R., Shah, M., Khan, Z., Irtaza, A., and Mehmood, Z., "A survey on block-based copy move image forgery detection techniques," In *International Conference on Emerging Technologies (ICET)*, IEEE, pp. 1-6, 2015.
- [6] Mahmood, T., Nawaz, T., Irtaza, A., Ashraf, R., Shah, M., and Mahmood, M. T., "Copy-move forgery detection technique for forensic analysis in digital images," *Mathematical Problems in Engineering*, 2016.
- [7] Kumar, S., Mukherjee, S., and Pal, A. K., "An improved reduced feature-based copy-move forgery detection technique," *Multimedia Tools and Applications*, Vol. 82, No. 1, pp. 1431-1456, 2023.

- [8] Alberry, H. A., Hegazy, A. A., and Salama, G. I., "A fast SIFT based method for copy move forgery detection," *Future Computing and Informatics Journal*, Vol. 3, No. 2, pp. 159-165, 2018.
- [9] Wang, C., Zhang, Z., and Zhou, X., "An image copy-move forgery detection scheme based on A-KAZE and SURF features," *Symmetry*, Vol. 10, No. 12, 2018.
- [10] Narayanan, S. S., and Gopakumar, G., "Recursive block based keypoint matching for copy move image forgery detection," In *11th International conference on computing, communication and networking technologies (ICCCNT)*, pp. 1-6, 2020.
- [11] Elaskily, M.A., Elnemr, H.A., Sedik, A., Dessouky, M.M., Banby, G.M.E., Elshakankiry, O.A., and El-Samie, F.E.A., "A novel deep learning framework for copy-move forgery detection in images," *Multimedia Tools and Applications*, Vol. 79, No. 27, pp. 19167–19192, 2020.
- [12] Doegar, A., Dutta, M., and Gaurav, K., "Cnn based image forgery detection using pre-trained alexnet model," *International Journal of Computational Intelligence & IoT*, Vol. 2, No. 1, 2019.
- [13] Albelwi, S., and Mahmood, A., "A framework for designing the architectures of deep convolutional neural networks," *Entropy*, Vol. 19, No. 6, 2017.
- [14] Chollet, F., "Deep learning with python," Simon and Schuster, 2021.
- [15] Ramadhani, E., "Photo splicing detection using error level analysis and laplacian-edge detection plugin on GIMP," In *Journal of Physics: Conference Series*, Vol. 1193, No. 1, 2019.

شناسایی تهدیدات در شبکه‌های رایانه‌ای با الگوریتم شاهین هریس

هادی نیک‌منش^{۱*}

۱- کارشناس ارشد شبکه‌های کامپیوتری، مؤسسه غیرانتفاعی اقبال لاهوری مشهد hadiynikmanesh@gmail.com

چکیده:

در مقابله با حملات و نفوذ در شبکه‌های رایانه‌ای و اینترنت اشیاء از ابزارهای متعددی استفاده می‌شود که یکی از آنها سیستم تشخیص نفوذ است. این سیستم از چندین روش برای تشخیص نفوذ استفاده می‌کند که یکی از مهم‌ترین آنها روش تشخیص ناهنجاری است که امروزه بسیار مورد توجه قرار گرفته است. مشکل اساسی روش تشخیص ناهنجاری، نرخ هشدار غلط بالای آن است. تاکنون روش‌های مختلفی به منظور کاهش نرخ هشدار غلط و افزایش دقت و نرخ تشخیص صحیح، در تشخیص نفوذ مورد استفاده و آزمایش قرار گرفته است؛ اما هیچ یک نتوانسته‌اند به موفقیت کامل دست یابند. در این پژوهش، یک سیستم تشخیص ناهنجاری در شبکه‌های رایانه‌ای و اینترنت اشیاء با استفاده از الگوریتم بهینه‌سازی شاهین هریس ارائه شده است. مجموعه ویژگی انتخاب شده توسط الگوریتم پیشنهادی، بیش‌ترین تأثیر را در تشخیص ناهنجاری تراکنش‌ها دارد. استفاده از الگوریتم شاهین هریس به همراه طبقه‌بندی درخت تصمیم، میزان دقت را به ۹۹٫۸۳۳ درصد افزایش داده است و در مقایسه با الگوریتم‌های مشابه نشان از بهبود آن دارد.

کلید واژه‌ها: اینترنت اشیاء، تشخیص ناهنجاری، الگوریتم درخت تصمیم.

Identification of computer network threats with Shahin Harris algorithm

Hadi Nik Manesh^{*1}

1-Senior expert in computer networks, Iqbal Lahori non-profit Institute, Mashhad,
hadiynikmanesh@gmail.com

Abstract:

In dealing with attacks and intrusions in computer networks and Internet of Things, several tools are used, one of which is the intrusion detection system. This system uses several methods for intrusion detection, one of the most important of which is the anomaly detection method, which is of great interest today. The main problem of the anomaly detection method is its high false alarm rate. So far, various methods have been used and tested in intrusion detection in order to reduce the false alarm rate and increase the accuracy and correct detection rate; but none of them have been able to achieve complete success. In this research, an anomaly detection system in computer networks and Internet of Things is presented using Shahin Harris optimization algorithm. The set of features selected by the proposed algorithm has the greatest effect in identifying the abnormality of transactions. The use of Shahin Harris algorithm along with the decision tree classifier increased the accuracy to 99.833% and shows an improvement compared to similar algorithms.

Keyword: Internet of things, anomaly detection, decision tree algorithm.

۱- مقدمه

مفهوم اینترنت اشیا^۱ یا IoT در سال ۱۹۹۹م [۱] بعد از ورود دستگاه‌های بی‌سیم به بازار و معرفی فناوری‌های RFID^۲ و شبکه‌های سنسور بی‌سیم^۳ [۲] معرفی شد. اینترنت اشیا یکی از رایج‌ترین فناوری‌هایی است که امکان اتصال داخلی بین دستگاه‌ها یا اشیای انبوه را از طریق اینترنت یا اینترنت اشیاء فراهم می‌سازد و این امکان را به اشیاء می‌دهد تا با یکدیگر ارتباط برقرار سازند [۳].

سیستم‌های تشخیص نفوذ، یک زمینه تحقیقاتی مهم در زمینه امنیت شبکه‌های اینترنت اشیا است. سیستم تشخیص نفوذ، سخت‌افزار و یا نرم‌افزاری است که کار نظارت بر شبکه‌های کامپیوتری را در مورد فعالیت‌های مخرب و یا نقض سیاست‌های مدیریتی و امنیتی انجام می‌دهد و گزارش‌های حاصله را به بخش مدیریت شبکه ارائه می‌دهد [۴]. از زمان ارائه سیستم‌های تشخیص نفوذ تا به امروز، این سیستم‌ها با مشکلات بسیاری روبرو بوده‌اند که با تحقیقات انجام شده و بهبودهای صورت گرفته در جهت رفع مشکلات آن‌ها، روزبه‌روز به سمت تکامل خود پیش می‌روند. یکی از مشکلات اساسی که سیستم‌های تشخیص نفوذ با آن مواجه هستند، تعداد زیاد هشدارها و بالا بودن نرخ تشخیص نادرست در بین هشدارها است.

در سال‌های اخیر از الگوریتم‌ها و روش‌های هوش مصنوعی مختلفی در طراحی سیستم‌های تشخیص نفوذ استفاده شده است. چالش‌هایی که هم‌چنان در استفاده از این الگوریتم‌ها وجود دارد، انتخاب بهترین مجموعه از ویژگی‌ها برای داده‌های مورد استفاده و انتخاب بهترین پارامترها برای روش‌های طبقه‌بندی است. برای رفع این مشکل، الگوریتم‌های فراابتکاری پنجره جدیدی به روی محققان گشوده است. در مطالعات پیشین از روش‌های تکاملی با اهداف مختلفی بهره گرفته شده است. به طور مثال، رایس و همکاران، از روش الگوریتم مورچگان (ACO) به منظور انتخاب بهترین ویژگی‌ها در حل مسئله تشخیص نفوذ به شبکه بهره گرفته شده است [۵]. علی و همکاران از الگوریتم ازدحام ذرات (PSO) به منظور انتخاب وزن‌های بهینه در شبکه‌های یادگیری سریع (FLN) در کاربرد IDS استفاده کرده‌اند [۶]. یانگ و همکاران از الگوریتم کلونی زنبورها (ABC) با هدف بهینه کردن پارامترهای طبقه‌بندی شبکه‌های بیزین بهره گرفتند و از آن در تشخیص نفوذ به شبکه استفاده کرده‌اند [۷]. با مروری بر سایر پژوهش‌های انجام شده می‌توان نتیجه گرفت که الگوریتم‌های فراابتکاری به صورت گسترده‌ای در حل مسائل تشخیص نفوذ به شبکه و در یکی از دو کاربرد انتخاب پارامترهای بهینه روش‌های طبقه‌بندی و یا انتخاب ویژگی‌های بهینه به کار گرفته شده‌اند.

از آن جایی که سرعت و دقت در طراحی سیستم‌های تشخیص نفوذ از اهمیت بالایی برخوردار است، الگوریتم بهینه‌سازی شاهین هریس، به عنوان یک الگوریتم فراابتکاری که از قدرت همگرایی بالا و سرعت زیادی برخوردار است، گزینه مناسبی به نظر می‌رسد. در این مقاله، برای تشخیص ناهنجاری در شبکه از روش‌های مبتنی بر دسته‌بندی (درخت تصمیم و دسته‌بندی بیزین) و مبتنی بر خوشه‌بندی (روش نزدیک‌ترین هم‌سایه) و برای انتخاب ویژگی‌ها از الگوریتم شاهین هریس استفاده می‌شود.

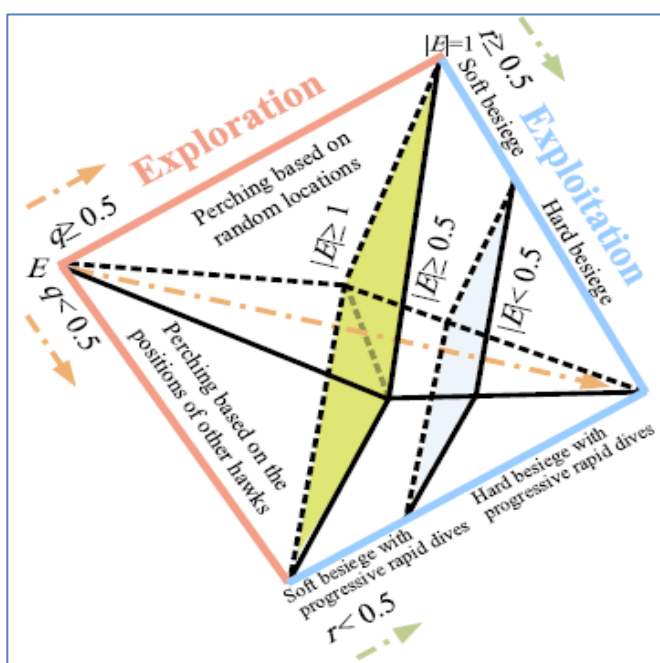
¹ Internet of Thing

² Radio-frequency identification

³ Wireless Sensor Networks (WSN)

۲- الگوریتم شاهین هریس

در این پژوهش، الگوی بهینه‌سازی مبتنی بر جمعیت و الهام از طبیعت، ارائه شده است که به آن بهینه‌ساز هریس هاوکس (HHO) یا شاهین هریس گفته می‌شود. الگوریتم HHO از رفتار مشارکتی و سبک تعقیب طعمه توسط گروه شاهین هریس در طبیعت با روش گشت‌وگذار غافل‌گیرانه استنباط شده است. در این استراتژی هو شمنند، چندین شاهین با حمله از جهات مختلف، تلاش دارند طعمه (خرگوش) را غافلگیر کنند. هر الگوریتم تکاملی جدیدی که معرفی می‌شود برای اثبات قدرت خود در بهینه‌سازی باید بر روی دو فاز مهم یعنی اکتشاف (Exploration) و بهره‌برداری (Exploitation) تمرکز داشته باشد و بتواند تعادل خوبی بین این دو فاز ایجاد کند. در فاز اکتشاف، الگوریتم به دنبال کشف فضای جستجو است؛ و به‌روزرسانی موقعیت شاهین‌ها، بر اساس عملگر تصادفی و یا بر اساس موقعیت سایر شاهین‌ها صورت می‌گیرد و در فاز بهره‌برداری، الگوریتم به دنبال بهبود جواب‌های پیدا شده است و از عملگرهای محاصره سخت و محاصره نرم استفاده می‌کند. در شکل ۱ فازهای مختلف الگوریتم دیده می‌شود [۸].



شکل (۱): فازهای مختلف الگوریتم شاهین [۸].

۲-۱- فاز اکتشاف

در HHO، شاهین‌های هریس به طور تصادفی در موقعیت‌های مختلفی (مکان‌های بلند) قرار می‌گیرند و منتظر می‌مانند تا طعمه‌ای را بر اساس دو استراتژی شناسایی کنند. اگر شانس q را برای هر استراتژی قرارگیری در نظر بگیریم و شاهین‌ها با توجه به موقعیت دیگر اعضای خانواده خود (تا هنگام حمله به اندازه‌ی کافی نزدیک به آنها

با شند) و موقعیت طعمه یا خرگوش قرار بگیرند، موقعیت آنها با معادله ۱ و شرط $q < 0.5$ مدل می شوند و اگر روی درختان بلند به طور تصادفی (در محدوده‌ی خانه‌ی گروه) قرار بگیرند، با شرط $q \geq 0.5$ مدل می‌شوند [۸].

$$X(t+1) = \begin{cases} X_{\text{rand}}(t) - r_1 |X_{\text{rand}}(t) - 2r_2 X(t)| & q \geq 0.5 \\ (X_{\text{rabbit}}(t) - X_m(t)) - r_3 (LB + r_4 (UB - LB)) & q < 0.5 \end{cases} \quad (۱)$$

در این معادله، $X(t+1)$ بردار موقعیت شاهین‌ها در تکرار بعدی t ، $X_{\text{rabbit}}(t)$ موقعیت خرگوش، $X(t)$ بردار موقعیت فعلی شاهین‌ها، r_1, r_2, r_3, r_4 اعداد تصادفی بین صفر و یک هستند که در هر تکرار به‌روز می‌شوند، LB و UB مرزهای بالا و پایین متغیرها (محدوده خانه گروه) را نشان می‌دهد، $X_{\text{rand}}(t)$ موقعیت تصادفی یک شاهین انتخاب شده از جمعیت فعلی است و X_m موقعیت متوسط جمعیت فعلی شاهین‌ها است که از رابطه‌ی زیر به دست می‌آید:

$$X_m(t) = \frac{1}{N} \sum_{i=1}^N X_i(t) \quad (۲)$$

که در آن $X_i(t)$ موقعیت هر شاهین را در تکرار t و N تعداد کل شاهین‌ها را نشان می‌دهد [۸].

۲-۲- فاز بهره‌برداری

با توجه به رفتارهای گریز طعمه و راهبردهای تعقیب و گریز شاهین هریس، چهار مدل استراتژی احتمالی در HHO برای مدل‌سازی مرحله حمله پیشنهاد شده است.

فرض کنید که r شانس طعمه در فرار موفق ($r < 0.5$) یا فرار ناموفق ($r \geq 0.5$) قبل از گشت‌وگذار غافل‌گیرانه است. شاهین‌ها بسته به انرژی احتمالی طعمه، طعمه را از جهات مختلف محاصره می‌کنند. در شرایط واقعی، شاهین‌ها به طعمه موردنظر نزدیک‌تر و نزدیک‌تر می‌شوند تا با انجام گشت‌وگذار غافل‌گیرانه، شانس خود را در گرفتن طعمه افزایش دهند. پس از چند دقیقه که طعمه انرژی بیشتری را از دست می‌دهد، شاهین‌ها روند محاصره را تشدید می‌کنند تا طعمه گیج شده را گرفتار کنند. برای مدل‌سازی این استراتژی، از پارامتر E استفاده می‌شود. در این رابطه، هنگامی که $|E| \geq 0.5$ ، محاصره نرم اتفاق می‌افتد، و زمانی که $|E| < 0.5$ ، محاصره سخت رخ می‌دهد [۸].

۲-۲-۱- محاصره نرم

هنگامی که $r \geq 0.5$ و $|E| \geq 0.5$ ، طعمه هنوز هم به اندازه‌ی کافی انرژی دارد و سعی در فرار با برخی جهش‌های گمراه‌کننده تصادفی دارد، اما در نهایت نمی‌تواند فرار کند. در طی این تلاش‌ها، شاهین‌های هریس آن را محاصره می‌کنند تا خرگوش را خسته‌تر کنند. این رفتار طبق معادلات زیر انجام می‌شود:

$$X(t+1) = \Delta X(t) - E |X_{\text{rabbit}}(t) - X(t)| \quad (۳)$$

$$\Delta X(t) = X_{\text{rabbit}}(t) - X(t) \quad (۴)$$

در جایی که $\Delta X(t)$ تفاوت بین بردار موقعیت خرگوش و موقعیت فعلی شاهین در تکرار t است، r_5 یک عدد تصادفی بین صفر و یک و $J = 2(1 - r_5)$ نشان‌دهنده قدرت پرش تصادفی خرگوش هنگام فرار است. مقدار J به طور تصادفی در هر تکرار تغییر می‌کند تا ماهیت حرکات خرگوش را شبیه‌سازی کند [۸].

۲-۲-۲- محاصره سخت

هنگامی که $r \geq 0.5$ و $|E| < 0.5$ ، طعمه بسیار خسته است و انرژی فرار کمی دارد. علاوه بر این، شاهین‌های هریس به سختی طعمه موردنظر را محاصره می‌کنند تا در نهایت گشت‌وگذار غافل‌گیرانه را انجام دهند. در این شرایط موقعیت‌های فعلی با استفاده از معادله زیر به‌روز می‌شوند:

$$X(t+1) = X_{\text{rabbit}}(t) - E|\Delta X(t)| \quad (5)$$

۲-۲-۳- محاصره نرم با شیرجه‌های سریع مترقی

هنگامی که $r < 0.5$ و $|E| \geq 0.5$ ، خرگوش دارای انرژی کافی برای فرار موفق است و هنوز هم محاصره نرم قبل از گشت‌وگذار غافل‌گیرانه انجام می‌شود. این رویه نسبت به مورد قبلی هوشمندانه‌تر است. برای مدل‌سازی ریاضی الگوهای فرار طعمه و حرکات جهشی، از مفهوم LF^1 در الگوریتم HHO استفاده می‌شود. LF برای تقلید از حرکات فریبنده زیگزآگی طعمه در مرحله فرار و شیرجه‌های نامنظم، ناگهانی و سریع شاهین در اطراف طعمه استفاده می‌شود. در واقع، شاهین‌ها چندین شیرجه سریع تیمی را در اطراف خرگوش انجام می‌دهند و سعی می‌کنند با توجه به حرکات فریبنده‌ی طعمه، مکان و مسیرهای خود را به تدریج تصحیح کنند. با الهام از رفتارهای واقعی شاهین‌ها، فرض شده است که برای قرار دادن طعمه در موقعیت‌های رقابتی، شاهین‌ها می‌توانند بهترین شیرجه را به سمت طعمه انتخاب کنند. بنابراین، برای انجام یک محاصره نرم، فرض می‌شود که شاهین‌ها می‌توانند حرکت بعدی خود را بر اساس معادله زیر ارزیابی کنند:

$$Y = X_{\text{rabbit}}(t) - E|JX_{\text{rabbit}}(t) - X(t)| \quad (6)$$

سپس، آن‌ها نتیجه‌ی احتمالی چنین حرکتی را با شیرجه‌ی قبلی مقایسه می‌کنند تا دریابند که این یک شیرجه‌ی خوب خواهد بود یا نه. اگر بینند طعمه حرکات فریبنده‌تر را انجام می‌دهد، شروع به انجام شیرجه‌های نامنظم، ناگهانی و سریع می‌کنند. ما تصور می‌کنیم که آنها با استفاده از معادله زیر بر اساس الگوهای LF شیرجه بزنند:

$$Z = Y + S \times LF(D) \quad (7)$$

جایی که D ابعاد مسئله است و S یک بردار تصادفی با ابعاد $1 \times D$ و LF تابعی است که با استفاده از معادله زیر محاسبه می‌شود:

$$LF(x) = 0.01 \times \frac{u \times \sigma}{|v|^{\frac{1}{\beta}}}, \sigma = \left(\frac{L(1+\beta) \times \sin \frac{\pi\beta}{2}}{L(\frac{1+\beta}{2}) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}} \right) \quad (8)$$

در جایی که u ، v مقادیر تصادفی بین صفر و یک هستند، β یک مقدار ثابت پیش‌فرض برابر ۱٫۵ است. از این رو، استراتژی نهایی برای به‌روزرسانی موقعیت شاهین‌ها در فاز محاصره نرم توسط معادله زیر قابل اجرا است:

$$X(t+1) = \begin{cases} Y & \text{if } F(Y) < F(X(t)) \\ Z & \text{if } F(Z) < F(X(t)) \end{cases} \quad (9)$$

جایی که Y و Z با استفاده از معادلات ۶ و ۷ به دست می‌آیند.

¹levy flight

۴-۲-۲- محاصره سخت با شیرجه‌های سریع مترقی

وقتی $r < 0.5$ و $|E| < 0.5$ ، خرگوش انرژی کافی برای فرار ندارد و محاصره سخت قبل از گشت‌وگذار غافل‌گیرانه برای گرفتن و کشتن طعمه شکل می‌گیرد. وضعیت این مرحله در سمت طعمه شبیه به شرایط موجود در محاصره نرم است، اما این بار شاهین‌ها سعی می‌کنند متوسط فاصله خود را با طعمه کاهش دهند. بنابراین، قانون زیر در شرایط محاصره سخت انجام می‌شود:

$$X(t+1) = \begin{cases} Y & \text{if } F(Y) < F(X(t)) \\ Z & \text{if } F(Z) < F(X(t)) \end{cases} \quad (10)$$

جایی که Y و Z با استفاده از قوانین جدید در معادلات زیر به دست می‌آیند.

$$Y = X_{\text{rabbit}}(t) - E|X_{\text{rabbit}}(t) - X_m(t)| \quad (11)$$

$$Z = Y + S \times LF(D) \quad (12)$$

جایی که $X_m(t)$ با استفاده از معادله ۲ به دست می‌آید.

شبه‌الگوریتم پیشنهادی HHO در الگوریتم ۱ (شکل ۲) گزارش شده است [۸].

الگوریتم ۱. شبه‌کد الگوریتم شاهین هریس (HHO)
ورودی‌ها: اندازه جمعیت N و حداکثر تعداد تکرار T
خروجی‌ها: موقعیت خرگوش و مقدار شایستگی آن
ساخت جمعیت تصادفی $X_i (i = 1, 2, \dots, N)$
تا زمانی که (شرط توقف برآورده نشده است) مراحل زیر را انجام دهید:
محاسبه مقادیر شایستگی شاهین‌ها
تعیین X_{rabbit} به عنوان موقعیت خرگوش (بهترین جواب)
برای (هر شاهین X_i) مراحل زیر را انجام دهید:
بروز کردن انرژی اولیه E و قدرت پرش J
$J = 2(1 - \text{rand}())$, $E = E - \text{rand}()$
بروز کردن E با استفاده از معادله ۳-۵
اگر $(E \geq 1)$ سپس (مرحله اکتشاف: بروز کردن بردار مکانی با استفاده از معادله ۳-۳)
اگر $(E < 1)$ سپس (مرحله بهره برداری)
اگر $(E \geq 0.5)$ و $ E \geq 0.5$ سپس (محاصره نرم: بروز کردن بردار مکانی با استفاده از معادله ۳-۶)
در غیر این صورت اگر $(E < 0.5)$ و $ E < 0.5$ سپس (محاصره سخت: بروز کردن بردار مکانی با استفاده از معادله ۳-۸)
در غیر این صورت اگر $(E < 0.5)$ و $ E < 0.5$ سپس (محاصره نرم با شیرجه‌های سریع مترقی: بروز کردن بردار مکانی با استفاده از معادله ۳-۱۲)
در غیر این صورت اگر $(E < 0.5)$ و $ E < 0.5$ سپس (محاصره سخت با شیرجه‌های سریع مترقی: بروز کردن بردار مکانی با استفاده از معادله ۳-۱۳)
برگرداندن X_{rabbit}

شکل (۲): شبه‌کد الگوریتم شاهین هریس.

۵- روش پیشنهادی

در الگوریتم پیشنهاد شده، تا نمونه‌ای تصادفی و بدون جای‌گذاری به اندازه‌ی ۱۰۰۰۰ را از مجموعه‌ی داده Kddcup99 انتخاب شود و با استفاده از الگوریتم شاهین هریس با تعداد جمعیت ۳۰ و با ماکزیمم تکرار ۲۰ به انتخاب ویژگی پرداخته و این الگوریتم را با الگوریتم ژنتیک و گرگ خاکستری مقایسه کرده‌ایم. سپس، از الگوریتم درخت تصمیم جهت طبقه‌بندی داده‌های آموزش انتخاب ویژگی شده استفاده شده است. جهت ارزیابی، روش پیشنهادی خود را با روش‌های Navie Bayes و K-Nearest Neighbor مقایسه کرده و از لحاظ دقت به ترتیب الگوریتم پیشنهادی در جایگاه نخست و سپس، الگوریتم نزدیک‌ترین همسایه و در مرتبه بعد، الگوریتم بیزین بهترین نتایج را به دست آورده‌اند. نتایج در قالب نمودارهایی در ادامه نشان داده شده است. در الگوریتم K-Nearest Neighbor مقدار k را برابر ۵ در نظر گرفته شده است. همان‌طور که در جدول ۱ مشاهده می‌کنید استفاده از الگوریتم شاهین نسبت به گرگ خاکستری و ژنتیک از دقت و نرخ تشخیص بالاتری برخوردار است.

جدول (۱): نمایش پارامترهای مختلف ارزیابی با استفاده از روش‌های مختلف انتخاب ویژگی.

پارامتر ارزیابی	HHO+DT	GWO+DT	GA+DT
Accuracy (دقت)	۹۹,۸۳۳	۹۹,۶۶۷	۹۹,۵۸
DR (نرخ تشخیص)	۱۰۰	۱۰۰	۹۶,۱۱
FPR (نرخ مثبت کاذب)	۰,۰۰۰۶۷۰۰۲	۰,۰۰۰۳۳۵۰۱	۰,۷

بعد از انتخاب ۱۰ ویژگی توسط الگوریتم شاهین هریس، از دسته‌بندی‌های مختلف نزدیک‌ترین همسایه، درخت تصمیم CART و دسته‌بندی بیزین، برای یافتن بهترین دسته‌بندی استفاده شده است. همان‌گونه که در جدول ۲ مشاهده می‌شود روش پیشنهادی (استفاده از الگوریتم CART) از نرخ هشدار کاذب قابل قبولی برخوردار است.

جدول (۲): مقایسه نتایج روش‌ها.

پارامتر ارزیابی	HHO+CART*	HHO+KNN	HHO+NB
Accuracy (دقت)	۹۹,۸۳۳	۹۹,۷	۹۸,۱۳۳
Precision (صحت)	۸۸,۲۳۵	۱۰۰	۱۰۰
DR (نرخ تشخیص)	۱۰۰	۱۰۰	۸۸,۸۸۹
FPR (نرخ مثبت کاذب)	۰,۰۰۰۶۷۰۰۲	۰	۰
Specificity (خاصیت)	۹۹,۹۳۳	۱۰۰	۱۰۰

۶- نتیجه‌گیری و جمع‌بندی

در این پژوهش، شناسایی و انتخاب ویژگی‌های تأثیرگذار در تعیین وضعیت نرمال یا ناهنجاری تراکنش‌ها مورد ارزیابی قرار گرفته است. کاهش ویژگی‌ها، برای بهبود عملکرد در زمان یادگیری، دقت دسته‌بندی و به دست آوردن قوانین قابل فهم، ضروری می‌باشد؛ البته کاهش ویژگی‌ها نباید موجب کاهش نرخ تشخیص و افزایش نرخ تشخیص کاذب شود. بنابراین، نیاز به الگوریتمی داریم که زیرمجموعه قدرتمندی از ویژگی‌ها را برای ما به ارمغان داشته باشد، در این زمینه از الگوریتم شاهین استفاده کردیم و نشان دادیم که استفاده از این الگوریتم نسبت به گرگ خاکستری و ژنتیک از دقت و نرخ تشخیص بالاتری برخوردار است. نتایج حاکی از آن بود که بهترین ویژگی‌ها در مجموعه داده نمونه تشخیص نفوذ، تعداد ۱۰ ویژگی بود. این مجموعه ویژگی، بیش‌ترین تأثیر را در تعیین نرمال بودن یا ناهنجار بودن تراکنش‌ها دارا بودند.

روش پیشنهادی در این پایان‌نامه دارای نرخ تشخیص بسیار مطلوب و نرخ هشدار غلط پایین است. نرخ هشدار غلط بالا سبب می‌شود که بار محاسباتی زیادی به سیستم تحمیل شده و سبب کند و ناکارآمدی آن در تشخیص نفوذها و حملات گردد. موارد فوق حاکی از آن است که می‌توان از مدل طبقه‌بندی پیشنهادی برای سایر مجموعه داده‌های تشخیص نفوذ به منظور یافتن الگوی مناسب طبقه‌بندی تراکنش‌ها به دو طبقه نرمال و ناهنجاری استفاده نمود.

منابع:

- [1] Gubbi, J. Buyya, R. Marusic, S. and Palaniswami, M., "Internet of things (IoTs): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, Vol. 29, No. 7, pp. 1645–1660, 2013.
- [2] Riahi Sfar, A. Natalizio, E. Challal, Y. and Chtourou, Z., "a roadmap for security challenges in the Internet of Things," *Digital Communications and Networks* 4, pp. 118–137, 2018.
- [3] Deepa V. Jose, Vijyalakshmi A., "an Overview of Security in Internet of Things," *Procedia Computer Science*, 143, pp. 744–748, 2018.
- [4] Alampalayam Kumar, S. Vealey, T. and Srivastava, H., "Security in Internet of Things: Challenges, Solutions and Future Directions," *IEEE Computer Society* 16, pp. 1530–1605, 2016.
- [5] Rais, H. M. and Mehmood, T., "Dynamic Ant Colony System with Three Level Update Feature Selection for Intrusion Detection," *IJ Network Security*, 20, pp. 184–192, 2018.
- [6] Ali, M., Al Mohammed, B. A. D., Ismail, A. and Zolkipli, M. F., "A new intrusion detection system based on fast learning network and particle swarm optimization," *IEEE Access*, 6, pp. 20255–20261, 2018.
- [7] Yang, J. Ye, Z. Yan, L. Gu, W. and Wang, R., "Modified Naive Bayes Algorithm for Network Intrusion Detection based on Artificial Bee Colony Algorithm," *International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, pp. 35–40, 2018.
- [8] Heidari, A. A. et al., "Harris hawks optimization: Algorithm and applications," *Future Generation Computer Systems*, pp. 849–872, 2019.

پاورقی ها:
