

دانشگاه صنعتي امیرکبیر  
(پلی تکنیک تهران)

دانشكده مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه کارشناسی ارشد

تشخیص ناهنجاری با استفاده از شبکه‌های مولد تخاصمی

دانشجو

زهرا دهقانیان

اساتید راهنما

دکتر محمد رحمتی

دکتر مریم امیرمزلقانی

بهار 1401



|  |  |  |
| --- | --- | --- |
| Untitled | **به نام خدا** |  |
| **تعهدنامه اصالت اثر** | **تاريخ:** |
|  |

صفحه فرم ارزیابی و تصویب پایان نامه- فرم تأیید اعضاء كميته دفاع

در این صفحه (هر سه مقطع تحصيلي) بايد فرم ارزيابي یا تایید و تصویب پایان­نامه/رساله موسوم به فرم کمیته دفاع براي ارشد و دكترا و فرم تصويب براي كارشناسي، موجود در پرونده آموزشی را قرار دهند.

اينجانب زهرا دهقانیان متعهد مي‌شوم كه مطالب مندرج در اين پايان نامه حاصل كار پژوهشي اينجانب تحت نظارت و راهنمايي اساتيد دانشگاه صنعتي اميركبير بوده و به دستاوردهاي ديگران كه در اين پژوهش از آنها استفاده شده است مطابق مقررات و روال متعارف ارجاع و در فهرست منابع و مآخذ ذكر گرديده است. اين پایان نامه قبلاً براي احراز هيچ مدرك هم‌سطح يا بالاتر ارائه نگرديده است.

در صورت اثبات تخلف در هر زمان، مدرك تحصيلي صادر شده توسط دانشگاه از درجه اعتبار ساقط بوده و دانشگاه حق پيگيري قانوني خواهد داشت.

كليه نتايج و حقوق حاصل از اين پایان نامه متعلق به دانشگاه صنعتي اميركبير مي‌باشد. هرگونه استفاده از نتايج علمي و عملي، واگذاري اطلاعات به ديگران يا چاپ و تكثير، نسخه‌برداري، ترجمه و اقتباس از اين پایان نامه بدون موافقت كتبي دانشگاه صنعتي اميركبير ممنوع است.   
نقل مطالب با ذكر مآخذ بلامانع است.

در صفحه تعهدنامه اصالت اثر، در قسمت بالا سمت چپ، تاریخ دفاع خود را جایگزین تاریخ نوشته شده کنید.

همچنین در صفحه تعهدنامه اصالت اثر، در خط اول، نام و نام خانوادگی خود را به صورت کامل با نام و نام خانوادگی نمونه، جایگزین کنید. در انتهای متن تعهد، در قسمت امضا نیز باید نام و نام خانوادگی کامل خود را وارد نماید.

تقدیم

به...تشکر

چكيده

یکی از مهم‌ترین فعالیت‌های حوزه تحلیل داده تشخیص ناهنجاری می‌باشد که در طیف وسیعی از کاربرد‌ها همچون تشخیص جعل، کاربردهای پزشکی و سیستم‌های امنیتی به کار گرفته می‌شود. علی‌رغم وجود روش‌های آماری و مبتنی بر یادگیری ماشین طراحی مدل‌های موثر در تشخیص ناهنجاری در فضای داده پیچیده با ابعاد بالا همچنان به عنوان یک چالش اساسی باقی‌ مانده است. شبکه‌های مولد تخاصمی[[1]](#footnote-1) قادرند تا بر چالش مورد نظر فائق آمده و توزیع داده‌های دنیای واقعی که دارای پیچیدگی و ابعاد بالا هستند را مدل کنند و همین امر سبب می‌شود تا عملکرد امیدوارکننده‌ای در زمینه تشخیص ناهنجاری از خود نشان دهند. در این کار چارچوب تخاصمی RCALAD[[2]](#footnote-2) با هدف تشخیص ناهنجاری ارائه شده است. اساس کار مدل پیشنهادی بازسازی داده ورودی با استفاده از شبکه مولد و در ادامه محاسبه میزان اختلاف داده اصلی و بازسازی آن به منظور شناسایی نمونه‌های ناهنجار است. لازمه شناسایی موثر نمونه‌های ناهنجار بازسازی ضعیف داده‌های ناهنجار است. در چارچوب پیشنهاد شده در این کار بازسازی ضعیف نمونه‌های ناهنجار تضمین و همچنین از بیشینه اطلاعات موجود در شبکه به صورت توامان برای آموزش مدل استفاده می‌شود. تشخیص ناهنجاری با استفاده از خطای بازسازی نیازمند تعریف امتیاز ناهنجاری مناسب است، بنابراین علاوه بر معماری پیشنهادی دو امتیاز ناهنجاری جدید نیز در این کار ارائه شده است. نتایج تجربی بیانگر برتری مدل RCALAD در مقایسه با سایر مدل‌های مطرح در زمینه تشخیص ناهنجاری بوده است.

واژگان کلیدی:

تشخیص ناهنجاری، یادگیری ماشین، شبکه مولد تخاصمی، خطای بازسازی، امتیاز ناهنجاری.

|  |  |
| --- | --- |
| فهرست مطالب | صفحه |

[فصل اول 1](#_Toc103904951)

[1-1- ساختار گزارش 4](#_Toc103904952)

[فصل دوم 5](#_Toc103904953)

[1-2- طبقه‌بندی روش‌های تشخیص ناهنجاری از دیدگاه در دسترس بودن برچسب داده 6](#_Toc103904954)

[1-1-2- تشخیص ناهنجاری با نظارت 7](#_Toc103904955)

[2-1-2- تشخیص ناهنجاری نیمه‌نظارتی 7](#_Toc103904956)

[3-1-2- تشخیص ناهنجاری بدون نظارت 7](#_Toc103904957)

[2-2- طبقه‌بندی روش‌های تشخیص ناهنجاری از نظر رویکرد حل مسئله 8](#_Toc103904958)

[1-2-2- روش‌های آماری 9](#_Toc103904959)

[1-1-2-2- روش‌های پارامتری 9](#_Toc103904960)

[2-1-2-2- روش‌های غیرپارامتری 10](#_Toc103904961)

[2-2-2- روش‌های یادگیری ماشین 10](#_Toc103904962)

[1-2-2-2- دسته‌بندی 11](#_Toc103904963)

[2-2-2-2- نزدیک‌ترین همسایه 12](#_Toc103904964)

[3-2-2-2- خوشه‌بندی 12](#_Toc103904965)

[3-2- دسته‌بندی بر اساس نحوه تشخیص ناهنجاری 13](#_Toc103904966)

[1-3-2- بر اساس فاصله 13](#_Toc103904967)

[2-3-2- دسته‌بندی تک‌کلاسی 13](#_Toc103904968)

[3-3-2- بر اساس بازسازی 14](#_Toc103904969)

[4-2- معیار‌های ارزیابی روش‌های تشخیص ناهنجاری 14](#_Toc103904970)

[1-4-2- صحت 15](#_Toc103904971)

[2-4-2- بازیابی 15](#_Toc103904972)

[3-4-2- F1-score 16](#_Toc103904973)

[4-4-2- مساحت زیر نمودار مشخصه عملکرد 16](#_Toc103904974)

[5-2- شبکه‌های مولد تخاصمی و تشخیص ناهنجاری 16](#_Toc103904975)

[1-5-2- شبکه‌های مولد تخاصمی 17](#_Toc103904976)

[1-1-5-2- تحلیل نظری شبکه مولد تخاصمی 21](#_Toc103904977)

[2-1-5-2- مزایا و معایب 22](#_Toc103904978)

[2-5-2- مدل ANOGAN 23](#_Toc103904979)

[1-2-5-2- یادگیری بدون نظارت تنوع آناتومیکی طبیعی 24](#_Toc103904980)

[2-2-5-2- نگاشت تصاویر جدید به فضای نهفته 25](#_Toc103904981)

[3-2-5-2- تشخیص ناهنجاری 26](#_Toc103904982)

[4-2-5-2- مزایا و معایب 27](#_Toc103904983)

[3-5-2- مدل f-AnoGan 27](#_Toc103904984)

[1-3-5-2- GAN یادگیری بدون نظارت تنوع آناتومیکی طبیعی 28](#_Toc103904985)

[2-3-5-2- یادگیری نگاشت سریع از فضای تصویر به فضای نهفته 29](#_Toc103904986)

[3-3-5-2- شناسایی ناهنجاری 32](#_Toc103904987)

[4-3-5-2- مزایا و معایب 33](#_Toc103904988)

[4-5-2- مدل ALI 33](#_Toc103904989)

[1-4-5-2- مقایسه مدل‌های ALI و GAN 36](#_Toc103904990)

[2-4-5-2- رویکرد‌های جایگزین برای استنتاج در GAN 37](#_Toc103904991)

[3-4-5-2- مزایا و معایب 37](#_Toc103904992)

[5-5-2- مدل EGBAD 38](#_Toc103904993)

[1-5-5-2- مزایا و معایب 39](#_Toc103904994)

[6-5-2- مدل ALICE 40](#_Toc103904995)

[1-6-5-2- یادگیری تخاصمی با اندازه‌گیری اطلاعات 40](#_Toc103904996)

[2-6-5-2- آنتروپی شرطی 41](#_Toc103904997)

[3-6-5-2- فرایند یادگیری 42](#_Toc103904998)

[4-6-5-2- مزایا و معایب 42](#_Toc103904999)

[6-2- جمع‌بندی 43](#_Toc103905000)

[فصل سوم 44](#_Toc103905001)

[1-3- مدل ALAD 46](#_Toc103905002)

[1-1-3- تثبیت آموزش GAN بر پایه ALICE 48](#_Toc103905003)

[2-1-3- تشخیص ناهنجاری 49](#_Toc103905004)

[2-3- مدل RCGAN 52](#_Toc103905005)

[1-2-3- شناسایی نمونه‌های تخاصمی از دیدگاه آماری 52](#_Toc103905006)

[2-2-3- GAN 52](#_Toc103905007)

[3-2-3- منظم‌سازی شبکه مولد و تمایزگر 53](#_Toc103905008)

[4-2-3- پایداری چرخه 55](#_Toc103905009)

[3-3- مدل RCALAD 56](#_Toc103905010)

[1-3-3- معماری شبکه 58](#_Toc103905011)

[2-3-3- روال آموزش 62](#_Toc103905012)

[3-3-3- تشخیص ناهنجاری 66](#_Toc103905013)

[4-3-3- جمع‌بندی 69](#_Toc103905014)

[فصل چهارم 70](#_Toc103905015)

[1-4- دادگان و پیش‌پردازش 71](#_Toc103905016)

[1-1-4- مجموعه داده KDDCup99 71](#_Toc103905017)

[2-1-4- مجموعه داده Arrhytthmia 72](#_Toc103905018)

[3-1-4- مجموعه داده Thyroid 72](#_Toc103905019)

[4-1-4- مجموعه داده Musk 72](#_Toc103905020)

[5-1-4- مجموعه داده CIFAR-10 73](#_Toc103905021)

[6-1-4- مجموعه داده SVHN 73](#_Toc103905022)

[2-4- تنظیمات مدل 73](#_Toc103905023)

[3-4- مدل‌های پایه 74](#_Toc103905024)

[1-3-4- روش OC-SVM 74](#_Toc103905025)

[2-3-4- روش IF 74](#_Toc103905026)

[3-3-4- روش DSEBM 75](#_Toc103905027)

[4-3-4- روشDAGMM 75](#_Toc103905028)

[5-3-4-مدل AnoGan 75](#_Toc103905029)

[4-4- نتایج 76](#_Toc103905030)

[1-4-4- دادگان جدولی 76](#_Toc103905031)

[1-4-4- دادگان تصویری 77](#_Toc103905032)

[5-4- بحث 81](#_Toc103905033)

[1-5-4- مطالعه فرسایشی 81](#_Toc103905034)

[2-5-4- انتخاب تابع توزیع جریمه 83](#_Toc103905035)

[3-5-4- ارزیابی کارایی امتیاز‌های ناهنجاری 84](#_Toc103905036)

[6-4- جمع‌بندی 85](#_Toc103905037)

[فصل پنجم 86](#_Toc103905038)

[منابع و مراجع 93](#_Toc103905039)

|  |  |
| --- | --- |
| فهرست شکل­ها | صفحه |

[شکل 2-1: دسته­بندی روش­های تشخیص ناهنجاری 8](#_Toc103959327)

[شکل 2-2: رویکرد کلی شبکه­های مولد تخاصمی [28]. 19](#_Toc103959328)

[شکل 2-3: شمای کلی روند آموزش کدگذار 30](#_Toc103959329)

[شکل 2-4: معماری شبکه ALI 34](#_Toc103959330)

[شکل 3-1: شمای کلی شبکه­ ALAD 49](#_Toc103959331)

[شکل 3-2: نمونه­ای از خروجی شبکه ALAD به همراه داده­های ناهنجار 50](#_Toc103959332)

[شکل 3-3: نحوه­ی عملکرد توزیع *t(x)* 54](#_Toc103959333)

[شکل 3-4: معماری شبکه تمایزگر *Dxxzz* 60](file:///C:\Users\Fateme%20Ghasemi\Downloads\Telegram%20Desktop\final%20(AutoRecovered).docx#_Toc103959334)

[شکل 3-5: معماری RCALAD 61](#_Toc103959335)

[شکل 3-6: تاثیر حضور توزیع t(x) در روند آموزش مدل 62](file:///C:\Users\Fateme%20Ghasemi\Downloads\Telegram%20Desktop\final%20(AutoRecovered).docx#_Toc103959336)

[شکل 4-1: عملکرد مدل RCALAD روی کلاس عدد سه 79](#_Toc103959337)

[شکل 4-2: تاثیر توزیع *t(x)* بر بازسازی نمونه­های ناهنجار 82](#_Toc103959338)

[شکل 5-1: معماری اولیه شبکه مولد تخاصمی 86](#_Toc103959339)

[شکل 5-2: معماری مدل ALI 87](#_Toc103959340)

[شکل 5-3: معماری شبکه ALICE 88](#_Toc103959341)

[شکل 5-4: معماری شبکه ALAD 88](#_Toc103959342)

[شکل 5-5: معماری شبکه RCALAD 89](#_Toc103959343)

|  |  |
| --- | --- |
| فهرست جدول­ها | صفحه |

[جدول 4-1: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه بر روی مجموعه داده­های جدولی 76](#_Toc103959475)

[جدول 4-2: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه برروی مجموعه داده­ی CIFAR10 77](#_Toc103959476)

[جدول 4-3: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه بر روی مجموعه داده­ی SVHN 78](#_Toc103959477)

[جدول 4-4: میانگین معیار AUROC بر روی تمامی کلاس­های داده 79](#_Toc103959478)

[جدول 4-5: تاثیر بخش­های مختلف پیشنهادی در بهبود نتایج دادگان جدولی 80](#_Toc103959479)

[جدول 4-6: تاثیر بخش‌های مختلف پیشنهادی در بهبود نتایج دادگان تصویری 81](#_Toc103959480)

[جدول 4-7: تاثیر ‌های مختلف بر عملکرد مدل RCALAD 82](#_Toc103959481)

[جدول 4-8: مقایسه عملکرد امتیاز‌های ناهنجاری پیشنهادی با سایر امتیاز‌های ناهنجاری 83](#_Toc103959482)

[جدول 4-9: روند تکامل توابع بهینه‌سازی شبکه‌های مولد تخاصمی 90](#_Toc103959483)

|  |  |
| --- | --- |
| فهرست الگوریتم­ها | صفحه |

[الگوریتم 2-1: آموزش گرادیان نزولی کوچک دسته­ای شبکه­های مولد تخاصمی 20](#_Toc103959115)

[الگوریتم 2-2: رویه آموزش یادگیری خصمانه استنتاج 36](#_Toc103959116)

[الگوریتم 3-1: شبه کد الگوریتم ALAD 51](#_Toc103959117)

[الگوریتم 3-2: روند محاسبه­ی امتیاز ناهنجاری 67](#_Toc103959118)

# فصل اول

**مقدمه**هنگام تجزیه و تحلیل دادگان موجود در دنیای واقعی، شناسایی نمونه‌های غیرمشابه با سایر نمونه‌ها امری ضروری به نظر می‌رسد. چنین نمونه‌هایی با عنوان ناهنجاری شناخته می‌شوند و از عملیات شناسایی چنین نمونه‌هایی با عنوان مسئله تشخیص ناهنجاری یاد می‌شود. این مسئله یک بخش حائز اهمیت از زمینه تحقیقاتی داده‌کاوی است چرا که شامل کشف الگو‌های جذاب و نادر در داده‌هاست]1[. این مسئله به طور گسترده در آمار و یادگیری ماشین مورد مطالعه قرار گرفته است و با مترادف‌هایی مانند تشخیص داده پرت، شناسایی نوآوری، تشخیص انحراف و استخراج استثنا نیز یاد می‌شود. تعریف رسمی و مورد قبول این مسئله به صورت زیر است:

"یك ناهنجاری مشاهده‌ای است که به ميزاني از سایر مشاهدات منحرف  
مي‌شود که ظن‌هایي را برای این که توسط مكانيسم متفاوتي توليد شده باشد، ایجاد مي‌کند."

ناهنجاری‌ها جزو پارامترهای مهم هر مجموعه داده‌ای‌ در نظر گرفته مي‌شوند و در دامنه وسیعی از کاربردها تاثیرگذار هستند. به عنوان مثال، الگوی غير معمول ترافيك در یك شبكه کامپیوتری ميتواند به معنای هك شدن رایانه و انتقال داده‌ها به مقصدهای غيرمجاز باشد. رفتار غير عادی در معاملاتی که توسط کارت‌های اعتباری انجام می‌شوند مي‌تواند نشانگر فعاليت‌های اقتصادی با هدف کلاهبرداری باشد]2[، و یا یك ناهنجاری در تصویر MRI ممكن است وجود تومور بدخيم را نشان دهد]3.[ تشخيص ناهنجاری به طور گسترده در زمینه‌های کاربردی گوناگونی مانند: پزشكي، بهداشت عمومي، تشخيص کلاهبرداری، سنجش از دور[[3]](#footnote-3)، تشخيص نفوذ، پردازش تصویر، آسيب‌های صنعتي، شبكه‌های حسگر]4[، رفتار روبات‌ها و داده‌های نجومي بكار گرفته شده است]1،2[.

با هدف تشخیص نمونه‌های ناهنجار موجود در دادگان دنیای واقعی، تاکنون روش‌های متنوعی مورد استفاده قرار گرفته‌اند. به طور کلی تشخیص ناهنجاری بر دو اصل استوار است، شناسایی و مدل کردن رفتار داده هنجار و میزان انحراف از رفتار داده هنجار]7[. به طور کلی می‌توان روش‌های تشخیص ناهنجاری را به دوسته روش‌های آماری و روش‌های مبتنی بر یادگیری ماشین اشاره کرد. روش‌های آماری اگرچه در برخی از موارد کارایی مناسبی دارند اما عملکرد صحیح و مناسب آن‌ها در گرو صحت پیش‌فرض‌های استفاده شده در همین روش‌هاست و در صورتی که پیش‌فرض‌های اولیه در مورد توزیع داده اشتباه باشد نتایج نهایی ناامید کننده خواهد بود]8[. مزیت اصلی روش‌های مبتنی بر یادگیری ماشین استفاده از تجربه‌های گذشته به منظور انجام پیش‌بینی‌های صحیح در آینده است. این روش‌ها تنها با مشاهده نمونه‌های گذشته به طراحی مدل می‌پردازند و پیش‌فرض خاصی نسبت به توزیع داده ندارند. این دسته از الگوریتم‌ها نیازمند تعداد مناسبی از داده‌ها هستند تا بتوانند مدل پیشنهادی خود را آموزش دهند. از جمله مهم‌ترین مدل‌های موجود در این دسته می‌توان به شبکه‌های عصبی اشاره کرد که سابقه طولانی در زمینه تشخیص ناهنجاری دارد. به عنوان مثال شبکه‌های عصبی رمزگذار[[4]](#footnote-4) و خودرمزگذار[[5]](#footnote-5) مدلی برای بازسازی داده‌های عادی آموزشی آموزش داده می‌شود و نمونه‌های با خطای بازسازی بالا به عنوان نمونه ناهنجار در نظر گرفته می‌شوند]9[.

در سال 2017 از شبکه‌های عصبی مولد تخاصمی برای تشخیص ناهنجاری در زمینه تصاویر پزشکی (تصاویر شبکیه) و در مقایسه با سایر روش‌ها به موفقیت قابل توجهی دست یافت]10[. نتایج درخشان شبکه‌های مولد تخاصمی در عرصه پردازش تصویر و استخراج ویژگی سبب محبوبیت آن در زمینه‌های کاربردی مختلف شده است. به طور خاص این دسته از شبکه‌ها به عنوان یک چهارچوب قدرتمند برای مدل‌سازی مجموعه داده‌های پیچیده با ابعاد بالا شناخته می‌شوند. یک از اصلی‌ترین چالش‌های موجود در استفاده از شبکه‌های مولد تخاصمی مقابله با پیچیدگی‌های استنتاج است]11[. در سال‌های اخیر تلاش‌های گسترده‌ای انجام شده است تا با استفاده از شبکه‌های عصبی خود رمزگذار در ساختار شبکه‌های عصبی مولد تخاصمی از پیچیدگی‌های استنتاج کاسته شده و بر چالش‌های موجود غلبه کنند. علیرغم این تلاش‌ها همچنان ضعف‌هایی در روند یادگیری بلوک‌های موجود در ساختار شبکه‌های مولد تخاصمی موجود است و از تمامی ظرفیت موجود به منظور دریافت اطلاعات و آموزش هر چه بهتر مدل استفاده نمی‌شود.

## 1-1- ساختار گزارش

در فصل بعدی ابتدا به دسته‌بندی روش‌های تشخیص ناهنجاری از دیدگاه‌های مختلف می‌پردازیم، معیار‌های ارزیابی مدل‌های تشخیص ناهنجاری را معرفی می‌کنیم و در قسمت انتهایی فصل روش‌های تشخیص ناهنجاری مبتنی بر شبکه‌های مولد تخاصمی را بررسی و مرور می‌کنیم. در این قسمت سعی می‌شود تا ضمن دسته‌بندی روش‌‌های تشخیص ناهنجاری، مروری گذرا بر روش‌های به نسبت قدیمی‌تر نیز انجام شود. در ادامه به طور دقیق‌تر زنجیره‌ای از کارها مورد بحث قرار خواهد گرفت که در طول این زنجیره نقاط ضعف و کمبود‌های مدل پیشنهادی بر طرف می‌شود. فصل سوم به معرفی مدل ‌پیشنهادی و روش نوین تشخیص ناهنجاری اختصاص خواهد داشت. در این فصل الگوریتم پیشنهادی، که بر اساس حل یک مسئله بهینه‌سازی با در نظر گرفتن توزیع توام[[6]](#footnote-6) پارامترهای موجود در ساختار شبکه‌ عصبی مولد تخاصمی طراحی شده است، به شناسایی نمونه‌های ناهنجار در فضای نهفته[[7]](#footnote-7) و فضای ورودی می‌پردازد. در فصل چهارم عملکرد مدل روی دادگان‌های مختلف آزمایش می‌شود. در این فصل با دو نوع مختلف از دادگان روبرو خواهیم بود، دادگانی جدولی[[8]](#footnote-8) که شامل دادگان KDD و ARRHYTHMIA و دادگان تصاویر که شامل CIFAR-10 و SVHN[[9]](#footnote-9) است. در فصل پنجم و نهایی این گزارش پیشنهاد‌های موثر به منظور اصلاح و بهبود احتمالی روند آموزش شبکه‌ مولد تخاصمی ارائه می‌شود و در گام آخر جمع‌بندی مطالب ارائه شده و نتیجه‌گیری نهایی صورت خواهد پذیرفت.

# فصل دوم

**مروری بر کارهای پیشین**

در این فصل ابتدا به دسته‌بندی روش‌های مختلف تشخیص ناهنجاری و مرور روش‌های شاخص هر دسته پرداخته خواهد شد. در گام بعدی معیار‌های ارزیابی مدل‌های تشخیص ناهنجاری معرفی می‌شوند. در ادامه بر روی کارهایی که تاکنون در زمینه تشخیص ناهنجاری با استفاده از شبکه‌های مولد تخاصمی انجام گرفته‌اند مروری خواهیم داشت. در گام اول این قسمت، مقاله پایه با عنوان شبکه‌های مولد تخاصمی مورد بررسی قرار خواهد گرفت در ادامه، کار تشخیص ناهنجاری بدون نظارت با شبکه‌های عصبی تخاصمی به منظور راهنمایی عملیات اکتشاف نشانگر[[10]](#footnote-10) به اختصار AnoGan شرح داده خواهد شد و پس از آن f-AnoGan[[11]](#footnote-11) که در ادامه کار قبلی و توسط همان نویسندگان انجام شده است بررسی خواهد شد. با توجه به ضعف‌های موجود در ساختار f-AnoGan مقاله مکمل این مدل با نام استنتاج یادگرفته شده به روش تخاصمی[[12]](#footnote-12) به اختصار ALI مرور خواهد شد. . در گام بعدی مدل EGBAD[[13]](#footnote-13) که جزو اولین کار‌ها در زمینه تشخیص ناهنجاری که با الهام از مدل ALI خلق شده است مرور می‌شود. در مرحله بعدی با توجه تضمین نشدن شرط سازگاری حلقه[[14]](#footnote-14) در ALI مقاله آلیس[[15]](#footnote-15) مورد اشاره قرار می‌گیرد و در انتها تشخیص ناهنجاری یادگرفته شده به روش تخاصمی[[16]](#footnote-16) که در ادامه کارهای پیشین و همچنین مقاله پایه در این پروژه است به طور دقیق بررسی خواهد شد.

## 1-2- طبقه‌بندی روش‌های تشخیص ناهنجاری از دیدگاه در دسترس بودن برچسب داده

بیشتر روش‌های تشخیص ناهنجاری در مرحله آموزش خود نیاز دارند تا برچسب نمونه‌های مختلف در دسترس آن‌ها باشد تا بتوانند در خصوص طبیعی یا ناهنجار بودن یک نمونه در مرحله آزمایش تصمیم‌گیری کنند]12[. فرایند تهیه و دستیابی به داده‌های دارای برچسب دقیق شامل طیف گسترده‌ای از عملیات‌های بسیار هزینه‌بر و دشوار است، از این‌رو تکنیک‌های تشخیص ناهنجاری را بر اساس میزان در دسترس بودن برچسب‌ها می‌توان به سه دسته: تشخیص ناهنجاری با نظارت، تشخیص ناهنجاری نیمه نظارتی و تشخیص ناهنجاری بدون نظارت تقسیم کرد]13[.

### 1-1-2- تشخیص ناهنجاری با نظارت

در این دسته از روش‌ها هر دو الگوری رفتاری غیرطبیعی و طبیعی مدل ‌می‌شوند. در این مدل‌ها به داده‌های غیر طبیعی برچسب ناهنجاری و به داده‌های طبیعی برچسب عادی می‌زنند. در این رویکرد، برخی از مدل‌ها نمونه‌های ورودی را با نمونه‌های غیرعادی مقایسه می‌کنند و برخی دیگر نمونه‌ها را با نمونه‌های برچسب عادی مقایسه می‌کنند تا بر اساس آن در مورد ماهیت نمونه ورودی تصمیم‌گیری کنند]14[.

### 2-1-2- تشخیص ناهنجاری نیمه‌نظارتی

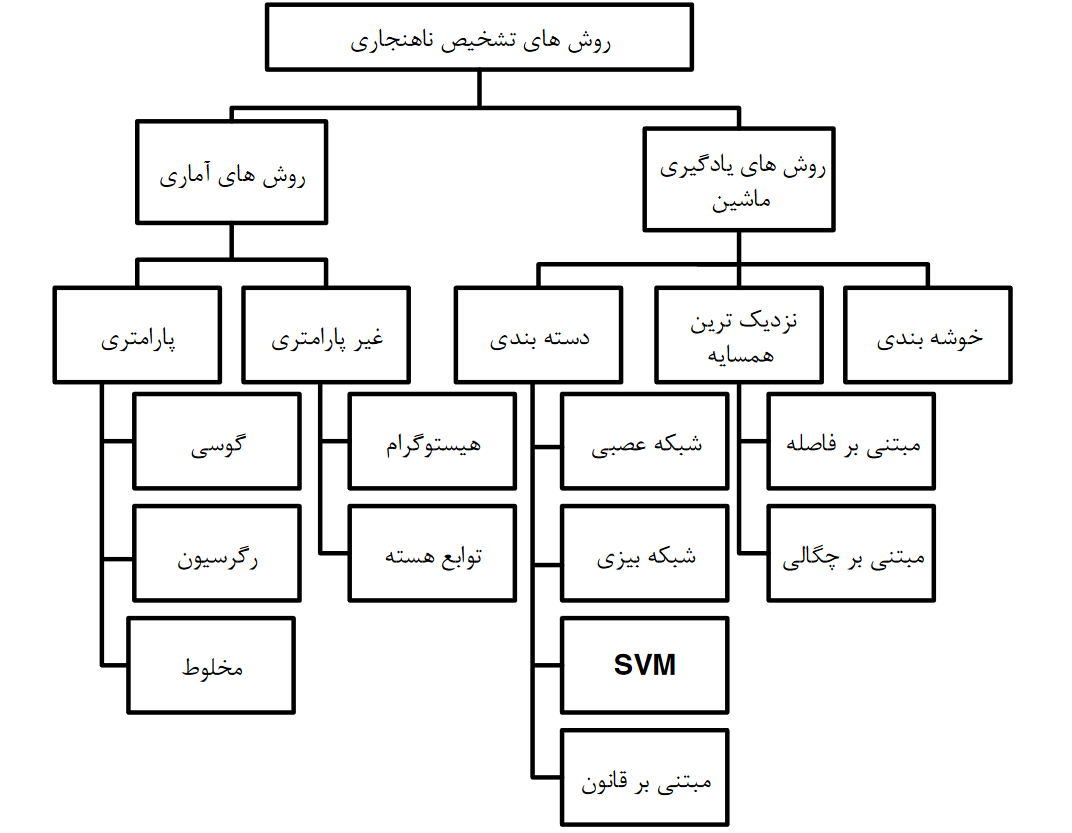
در تشخیص ناهنجاری نیمه‌نظارتی تنها الگوی رفتار طبیعی داده مدل می‌شود و به بیان دیگر تنها به برچسب‌های کلاس عادی نیاز داریم. از نظر کمی این دسته از روش‌ها کاربرد بیشتری نسبت به روش‌های تشخیص ناهنجاری نظارتی دارند]15[.

### 3-1-2- تشخیص ناهنجاری بدون نظارت

اساس کار این دسته از روش‌ها همانند روش‌های خوشه‌بندی[[17]](#footnote-17) است و مدل کلاس داده‌های ناهنجاری را به صورت خودکار از سایر کلاس‌ها تمیز می‌دهد]16[. این روش خوشه‌ای از داده‌ها با رفتار نزدیک به هم پیدا می‌کند و بدین ترتیب عملیات شناسایی ناهنجاری صورت می‌گیرد. اینگونه از مدل‌ها در بسیاری از تشخیص‌ها دچار مشکل می‌شوند چراکه ممکن است نمونه‌های ناهنجار خود باعث ایجاد خوشه‌هایی با الگوی مشابه داده‌های عادی شوند، به همین دلیل تکنیک‌های بدون نظارت در تولید نتایج دقیق کارآمد نیستند و اغلب دارای نرخ مثبت کاذب[[18]](#footnote-18) هستند]17 [.

## 2-2- طبقه‌بندی روش‌های تشخیص ناهنجاری از نظر رویکرد حل مسئله

روش‌های تشخیص ناهنجاری به طور کلی به دو دسته روش‌های آماری و روش‌های مبتنی بر یادگیری ماشین تقسیم می‌شوند. روش‌های آماری خود شامل دو دسته پارامتری و غیرپارامتری هستند و روش‌های یادگیری ماشین شامل خوشه‌بندی، نزدیک‌ترین همسایه و دسته‌بندی است. در شکل 2-1 دسته‌بندی این روش‌ها به طور دقیق‌تر به تصویر کشیده شده است. در ادامه هر یک از این روش‌ها بررسی و مرور خواهد شد.



شکل 2-1: دسته­بندی روش­های تشخیص ناهنجاری

### 1-2-2- روش‌های آماری

تشخیص ناهنجاری با روش‌های آماری به ترتیب بر اساس آمارگان‌های آماری مانند میانگین و انحراف از معیار، توزیع داده‌ها و توابع احتمال (برای ساختن نمایه‌های رفتاری) انجام می‌شود]18 [. در اینگونه از روش‌ها بر اساس آزمون‌های آماری هر نوع انحراف از رفتار عادی داده‌ها تشخیص داده می‌شود و داده مورد نظر به عنوان ناهنجاری در نظر گرفته می‌شود. به منظور توسعه مدل‌های اماری در تشخیص ناهنجاری از دو نوع تکنیک پارامتری و غیرپارامتری استفاده می‌شود]19 [. تکنیک‌های غیرپارامتری از اطلاعات زمینه‌ای داده‌ها استفاده نمی‌کنند، به بیان دیگر اطلاعی از توزیع داده ورودی ندارند در حالی که روش‌های پارامتری با استفاده از همین اطلاعات مدل را طراحی می‌کنند.

#### 1-1-2-2- روش‌های پارامتری

در روش‌های آماری فرض می‌شود داده‌های واقعی بر اساس پارامتر‌های مشخص از یک توزیع یا تابع خاص تولید می‌شوند، این دسته از روش‌ها خود به سه دسته کلی مدل رگرسیونی، مدل گاوسی و مدل مخلوط تقسیم می‌شوند.

در مدل رگرسیونی داده‌ها بر یک مدل رگرسیونی منطبق می‌شوند و باقی مانده[[19]](#footnote-19) هر داده که بر مدل منطبق نیست به عنوان معیار جهت تشخیص ناهنجاری به کار برده می‌شود.

در مدل گاوسی، فرض بر این است که داده‌ها به توزیع گاوسی تعلق دارند و پارامترهای مدل با استفاده از

استفاده از تخمین بیشینه درستنمایی[[20]](#footnote-20) تعیین می‌شوند. در این مدل‌ها از آزمون‌هایی نظیر آزمون کای-دو[[21]](#footnote-21) جهت شناسایی نمونه ناهنجار استفاده می‌شود]20 [.

مدل‌های مخلوط خود ترکیبی از سایر مدل‌های پارامتری هستند. چنین مدل‌هایی در برخی از کاربردها عملکرد بسیار موفقی از خود نشان داده‌اند. به عنوان مثال با به کارگیری یک مدل مخلوط از روش‌های پارامتری برای تشخیص ناهنجاری‌های شبکه، توانسته‌اند در طی زمان بسیار کوتاهی تمام ناهنجاری‌‌های موجود در شبکه که توسط سناریوهای مختلف ایجاد شده بودند را شناسایی کنند]8[.

#### 2-1-2-2- روش‌های غیرپارامتری

در این روش از نمونه‌های عادی برای تولید مدل استفاده می‌شود و انحراف نمونه از مدل به عنوان امتیاز ناهنجاری در نظر گرفته می‌شود. این روش را می‌توان به دو دسته مدل‌های مبتنی بر هیستوگرام و مدل‌های مبتنی بر هسته تقسیم کرد.

در مدل‌های مبتنی بر هیستوگرام، هیستوگرام بر اساس تقریب از داده‌های عادی تولید می‌شود و برای اگر نمونه ورودی در محدوده‌های خاصی از هیستوگرام قرار گیرد به عنوان ناهنجاری شناخته می‌شود]21[.

روش مدل‌سازی مبتنی بر هسته[[22]](#footnote-22) یک تابع تشابه بر اساس نمونه‌های موجود از داده استنباط می‌شود]22[. در اینگونه از مدل‌ها در دسترس بودن نمونه‌های کافی به منظور بازنمایی کامل رفتار مجموعه داده ضروریست چراکه در غیر این صورت دقت مدل کاهش می‌یابد.

### 2-2-2- روش‌های یادگیری ماشین

روش‌های مبتنی بر یادگیری ماشین بر اساس تجربه حاصل از مشاهده نمونه‌های قدیمی و به کار گیری آن، ظرفیت تمایز میان رفتار‌های غیر­طبیعی و طبیعی داده تا حد مناسبی بهبود می‌بخشند]23 [. این طبقه از روش‌ها خود به سه گروه دسته‌بندی، نزدیک‌ترین همسایه و خوشه‌بندی تقسیم می‌شوند]24[، در ادامه به بررسی هر یک از این دسته‌ها می‌پردازیم.

#### 1-2-2-2- دسته‌بندی

هدف اصلی از روش‌های مبتنی بر دسته‌بندی، اختصاص هر نمونه از داده به یکی از کلاس‌های از پیش‌ تعیین شده بر اساس ویژگی‌های آن نمونه است. از مزیت‌های این دسته از روش‌ها می‌توان به توانایی بالای آن‌ها در تمایز میان کلاس‌های مختلف داده در زمان آزمایش اشاره کرد. از روش‌های متداول که در این دسته جای دارند می‌توان به شبکه‌های بیزی، ماشین بردار پشتیبان[[23]](#footnote-23) ، برخی روش‌های مبتنی بر قانون و شبکه‌های عصبی اشاره کرد.

شبکه­های بیزی در واقع مدل‌های گرافیکی هستند که اتصالات میان نمونه­های مختلف را بر اساس محاسبه احتمال پیشین[[24]](#footnote-24) یک نمونه از داده به همراه دسته‌ای از پیش‌شروط مورد بررسی و ترجمه قرار می‌دهند. اساس کار این دسته از روش‌ها استفاده از یادگیری با نظارت است.

ماشین‌های بردار پشتیبان از دسته الگوریتم‌های یادگیری با نظارت هستند که در صورت استفاده از هسته نمونه‌ها را فضای با ابعاد بالاتر می‌برند و در فضای جدید نمونه‌ها را به دو کلاس تقسیم می‌کنند. استفاده از هسته زمانی توجیه پذیر است که نمونه‌ها در فضای با ابعاد پایین جداپذیر نباشند. این مدل به دلیل استفاده از یک مرز خطی به منظور جداسازی نمونه‌های غیرطبیعی و عادی به عنوان دسته‌بندی خطی شناخته می‌شود]25[.

روش‌های مبتنی بر قانون بر اساس یک سری از قواعد رفتار و عملکرد نمونه‌های عادی را می‌آموزد، بنابراین اگر یک نمونه نتواند از این مجموعه قوانین پیروی کند به عنوان نمونه ناهنجار شناخته خواهد شد. از مطرح‌ترین روش‌هایی که در این دسته می‌گنجند می‌توان به درخت تصمیم[[25]](#footnote-25) اشاره کرد]26[.

شبکه‌های عصبی رفتار سیستم عصبی انسان را تقلید می‌کنند و شامل مجموعه‌ای از فرایندهای بهم پیوسته هستند که به طور همزمان روی داده‌ عمل می‌کنند. در این دسته از روش‌ها از نمونه‌های عادی برای آموزش شبکه عصبی استفاده می‌شود. از نظر دسترسی به برچسب نمونه‌ها شبکه‌های عصبی را می‌توان مشترک بین دسته‌های یادگیری با نظارت و بدون نظارت در نظر گرفت]27[. یکی از انواع این شبکه‌ها که در سال‌های اخیر به موفقیت چشم‌گیری دست یافته است، شبکه‌های مولد تخاصمی[[26]](#footnote-26) هستند. این دسته از شبکه‌ها با موفقیت بر روی داده‌های دنیای واقعی که دارای ابعاد بالا هستند اعمال شده‌اند و چهارچوب یادگیری خصمانه آن‌ها عملکرد مناسبی از خود بر جای گذاشته است. قابلیت این شبکه‌ها نشان‌دهنده ظرفیت آن‌ها برای استفاده در مسئله تشخیص ناهنجاری می‌باشد و به همین جهت به کارگیری شبکه‌های مولد تخاصمی در حوزه تشخیص ناهنجاری اخیرا مورد توجه و کاوش قرار گرفته است]28[. در تشخیص ناهنجاری به کمک شبکه‌های مولد تخاصمی با استفاده از فرایند آموزش تخاصمی رفتار عادی داده مدل می‌شود سپس با اندازه‌گیری امتیاز ناهنجاری روی نمونه‌های مختلف عمل شناسایی نمونه ناهنجار صورت می‌پذیرد. شبکه‌های مولد تخاصمی با کمک آموزش و نمونه‌گیری از مدل‌های مولد به نتایجی بسیار مناسبی در مقایسه با دیگر روش‌ها دست می‌یابند همچنین این مدل‌ها امکان آموزش داده‌های از دست رفته به کمک الگوریتم‌های یادگیری تقویتی[[27]](#footnote-27) را می‌دهد. بیان جزئیات بیشتر در خصوص این دسته از شبکه‌ها را به به بخش‌هایی که در آینده خواهیم داشت موکول می‌کنیم.

#### 2-2-2-2- نزدیک‌ترین همسایه

روش نزدیک‌ترین همسایه مبتنی بر سنجش فاصله یا تراکم میان داده‌هاست به بیان دیگر امتیاز ناهنجاری مقدار همین فاصله است و بسته به مسئله و میزان در دسترس بودن برچسب‌ها این روش می‌تواند به عنوان روش یادگیری بدون نظارت و یا با نظارت به کار گرفته شود]8[.

#### 3-2-2-2- خوشه‌بندی

روش مبتنی بر خوشه‌بندی از دسته روش‌های یادگیری بدون نظارت است که برای شناسایی مجموعه نمونه‌های شبیه به هم به کار برده می‌شود. ناهنجاری‌ها ممکن است تشکیل یک خوشه کوچک بدهند یا در هیچ خوشه‌ای جای نگیرند. این روش در مقایسه با روش‌های مبتنی بر فاصله از پیچیدگی محاسباتی کمتری برخوردار است و در عین حال نقطه ضعف این روش عملکرد نامناسب روی دادگان کوچک است چرا که مدل بینش مناسبی نسبت به داده ندارد و به عنوان مثال برای قسمتی از فضا که برای آن نمونه آموزشی نداریم همواره برچسب ناهنجاری در نظر می‌گیرد در صورتی که ممکن است در حضور تعداد داده کافی برچسب آن نمونه خاص برچسب عادی باشد]8[.

## 3-2- دسته‌بندی بر اساس نحوه تشخیص ناهنجاری

در این قسمت بر اساس نحوه تشخیص ناهنجاری روش‌های موجود را به دسته بر اساس فاصله، دسته‌بندی تک‌کلاسی و بر اساس بازسازی[[28]](#footnote-28) تقسیم می‌کنیم]29[.

### 1-3-2- بر اساس فاصله

از روش‌های مبتنی بر فاصله می‌توان به عنوان یکی از کلاس‌های اصلی روش‌های تشخیص ناهنجاری یاد کرد. در این روش‌ها با استفاده از محاسبه فاصله یک نمونه‌ خاص با نزدیک‌ترین همسایه‌ها و یا نزدیک‌ترین کلاستر، نمونه ناهنجار شناسایی می‌شود. بدیهی‌ست به کار بردن چنین روش‌هایی نیازمند طراحی یا انتخاب معیار فاصله مناسب است]29[.

### 2-3-2- دسته‌بندی تک‌کلاسی

در رویکرد دسته‌بندی تک‌کلاسی تنها نمونه‌های عادی به یک دسته‌بند نظیر SVM آموزش داده می‌شوند]30[، در واقع این مدل‌ها یک مرز تصمیم حول نمونه‌های عادی یاد می‌گیرند، در صورتی که نمونه ورودی داخل این مرز قرار گیرد به عنوان نمونه عادی و در غیر اینصورت به عنوان نمونه ناهنجار شناخته می‌شود.

### 3-3-2- بر اساس بازسازی

این دسته از الگوریتم‌ها بر اساس میزان خطای بازسازی به شناسایی نمونه‌های ناهنجار می‌پردازند. PCA[[29]](#footnote-29) و الگوریتم‌های مشتق از آن جزو همین دسته روش‌ها هستند. اخیرا اساس کار بیشتر کارهای پژوهشی و کاربردی در زمینه تشخیص ناهنجاری شبکه‌های عصبی هستند و به نظر می‌رسد این شبکه‌‌ها دارای سابقه طولانی در این زمینه هستند]29 [. به عنوان مثال رویکردهای مبتنی بر خودکدگذار‌ و خودکدگذار متغیر[[30]](#footnote-30) روند بازسازی نمونه‌های عادی را فرامی‌گیرند و نمونه‌های با خطاری بازسازی زیاد را به عنوان ناهنجاری در نظر می‌گیرند. مدل‌های مبتنی بر انرژی و مدل‌های ترکیبی گوسی با خود رمزگذار عمیق[[31]](#footnote-31) به طور خاص در زمینه تشخیص ناهنجاری مورد تحقیق و پژوهش قرار گرفته‌اند. چنین روش‌هایی توزیع داده را با استفاده از خودرمزگذار یا روش‌های مشابه مدل می‌کنند و سپس بر اساس انرژی و یا ترکیب گوسی‌ها یک معیار آماری تشخیص ناهنجاری پدید می‌آورند. در سال‌های اخیر از شبکه‌های مولد تخاصمی به منظور تشخیص ناهنجاری استفاده شده است. در این مدل‌ها به هنگام آزمایش برای هر نمونه ورودی عمل استنتاج انجام می‌شود و با استفاده از انتشار خطای گرادیان نزولی[[32]](#footnote-32) در شبکه مولد، پارامترهای فضای نهفته بازیابی می‌شوند و با استفاده از این پارامترها می‌توان به شناسایی نمونه‌های ناهنجار پرداخت.

## 4-2- معیار‌های ارزیابی روش‌های تشخیص ناهنجاری

صرف نظر از رویکرد به کار گرفته شده، تشخیص ناهنجاری از مرحله یادگیری که در آن با استفاده از نمونه‌های آموزشی مدل آموزش داده می‌شود، آغاز می‌شود. پس از اتمام مرحله یادگیری، مدل دسته‌بندی نمونه‌هایی که تاکنون آن‌ها را مشاهده نکرده است را بر اساس معیارهای مورد نظر انجام می‌دهد. . نتیجه ارزیابی در میزان تشخیص ناهنجاری‌ها می‌تواند در چهار دسته مختلف گزارش شود که عبارتند از مثبت صحیح[[33]](#footnote-33) به اختصار TP، منفی صحیح[[34]](#footnote-34) به اختصارTN ، مثبت کاذب یا FP و منفی کاذب یا [[35]](#footnote-35) FN. در حوزه تشخیص ناهنجاری از معیارهای­ معمول و استانداردی نظیر صحت[[36]](#footnote-36) ، بازیابی[[37]](#footnote-37)، F1-score و مساحت زیر نمودار مشخصه عملکرد[[38]](#footnote-38) و یا به اختصار AUROC که در ادامه به بررسی جزئیات ریاضی هر یک خواهیم پرداخت.

### 1-4-2- صحت

معیار صحت یکی از معیارهای پایه در تمامی مسائل مربوط به دسته­بندی علی الخصوص تشخیص ناهنجاری می­باشد. این معیار بیانگر این است که چه مقدار از داده­هایی که به عنوان ناهنجاری تشخیص داده شده­اند، واقعا ناهنجار هستند. بیان ریاضی این معیار مطابق معادله 2-1 می­باشد.

|  |  |
| --- | --- |
| (1-2) |  |

### 2-4-2- بازیابی

این معیار در کنار معیار صحت دید نسبتا خوبی از وضعیت کلی عملکرد مدل نمایان می­کند. این معیار بیان می­کند که چه بخشی از داده­های ناهنجار کشف شده و مدل توانسته چه نسبتی از این دسته را بازیابی کند. معادله 2-2 نحوه محاسبه این معیار را نمایش می­دهد.

|  |  |
| --- | --- |
| (2-2) |  |

### 3-4-2- F1-score

در حالت کلی، یک مدل خوب باید هر دو معیار صحت و بازیابی بالایی داشته باشد و به هنگام مقایسه مدل­ها، در صورتی که هر دو معیار یادشده یک مدل از دیگری بیشتر باشد، مشخصا آن مدل عملکرد بهتری داشته است. اما اگر هر دو به صورت همزمان به سمت یک مقدار مناسب همگرا نباشند، انتخاب مدل بهتر با مشکل روبرو می­شود و نیاز به یک معیار با دید کلی­تر می­باشد. معیار F1-score به طور همزمان هر دو جنبه مورد سنجش را ارزیابی می­کند و معیار جامع­تری برای مقایسه می­باشد. بیان ریاضی این معیار مطابق معادله 2-3 می­باشد.

|  |  |
| --- | --- |
| (3-2) |  |

### 4-4-2- مساحت زیر نمودار مشخصه عملکرد

این معیار به منظور تعیین میزان توانایی مدل در تشخیص ناهنجاری به هنگام افزایش اندازه مجموعه داده تعریف شده است. این معیار با هدف ایجاد اطمینان از توانایی مدل درکنترل تغییرات سریع حجم داده ایجاد شده است و برای محاسبه آن با توجه به جنس مجموعه داده مورد آزمایش روش‌های متفاوتی ارائه شده است]8[.

## 5-2- شبکه‌های مولد تخاصمی و تشخیص ناهنجاری

هدف از مدل‌های یادگیری عمیق، کشف مدل‌های سلسله‌مراتبی قوی است. این مدل‌ها نشان‌دهنده توزیع احتمال انواع داده‌هایی است که در کاربردهای هوش مصنوعی نظیر تصاویر طبیعی، شکل موج صوتی حاوی گفتار به کار می‌رود. برجسته‌ترین موفقیت یادگیری عمیق در طراحی مدل‌های تمایزگر[[39]](#footnote-39) بوده است. این مدل‌ها قادرند تا ورودی با ابعاد بالا را دریافت کنند و کلاس هر یک از نمونه‌ها را با قدرت تشخیص خود با دقت بالا مشخص کنند. استفاده از الگوریتم‌های پس‌انتشار[[40]](#footnote-40) ، حذف تصادفی[[41]](#footnote-41) و واحدهای خطی تکه‌ای[[42]](#footnote-42) که دارای گرادیان با رفتار مناسب هستند عامل موفقیت چشم‌گیر یادگیری عمیق است.

استفاده کاربردی از الگوریتم‌هایی نظیر تخمین بیشینه درستنمایی و الگوریتم‌های مرتبط با آن همراه با چالش‌ها و دشواری‌های زیادی نظیر محاسبات احتمالاتی زیاد و خارج از کنترل است، وجود این چالش و همچنین سختی‌های موجود در استفاده از واحد‌های خطی تکه‌ای در حوزه مدل‌های مولد سبب شده است تا مدل‌های مولد عمیق کمتر مورد توجه قرار گیرند. شبکه‌های مولد تخاصمی بر این دست از چالش‌ها و دشواری‌ها فائق آمده و نقش مدل‌های مولد عمیق را پررنگ‌تر ساخته است.

### 1-5-2- شبکه‌های مولد تخاصمی

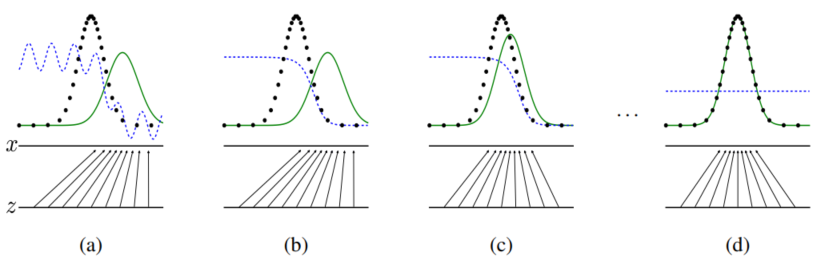
در شبكه‌های مولد تخاصمی، یک مدل مولد در برابر یك مدل تمایزگر قرار مي‌گير، مدل تمایزگر سعی می‌کند میان داده‌های واقعی و داده‌های تولیدی توسط شبکه مولد تمایز ایجاد کند. مدل مولد را مي‌توان مانند تيمي فرض کرد که سعي در توليد ارز جعلي با میزان شباهت بسیار بالا به ارز واقعی دارد و در طرف مقابل مدل تمایزگر مشابه پليس است که سعي در کشف ارز تقلبي دارد. رقابت در این بازی، هر دو تيم را به سمت بهبود روش های خود سوق مي‌دهد تا اینکه ارز تقلبي از ارز اصلي غيرقابل تشخيص باشد. این چارچوب مي‌تواند الگوریتم‌های آموزشي خاصي را برای انواع مختلف از مسائل و مدل‌ها بهينه‌سازی کند. بخش مولد با دریافت نویز تصادفي، از طریق پرسپترون چند لایه نمونه‌هایی با توزیع مشابه داده اصلی توليد مي‌کند و مدل تمایزگر با استفاده از مدل پرسپترونی چند لایه تلاش می‌کند تا میان نمونه‌‌های مختلف تمایز ایجاد کند. در این نوع از تعریف شبكه مي‌توان هر دو مدل را با استفاده از الگوریتم‌های پس‌انتشار و حذف تصادفي ایجاد کرد و برای نمونه‌گيری از مدل مولد تنها از الگوریتم انتشار رو به جلو[[43]](#footnote-43) استفاده کرد و در نتيجه به كارگيری هيچ الگوریتمی نظیر استنتاج تقریبي و یا زنجيره مارکوف ضروری نيست.

در شبكه مولد تخاصمی به طور همزمان دو مدل مولد و تمایزگر آموزش داده مي‌شود. مدل مولد توزیع داده را ضبط مي‌کند و مدل تمایزگر که احتمال این که نمونه از داده‌های توليد شده توسط باشد را تخمين مي‌زند. تابع هدف برای شبكه مولد به حداکثر رساندن احتمال اشتباه شبكه *D* است. این بستر منجر به یك بازی دو نفره مانند بازی‌های بیشینه-کمینه[[44]](#footnote-44) مي­شود. در فضای توابع دلخواه و یك راه حل منحصر به فرد وجود دارد و در این راه حل شبكه مولد توزیع داده‌های آموزشي را یاد گرفته است و شبكه تمایزگر احتمال را در همه جا برابر مقدار 2/1 نشان می‌دهد، به بیان دیگر میان داده‌های واقعی و داده تولید شده توسط شبکه مولد نمی‌تواند تمیز دهد.

مدل­سازی چارچوب تخاصمی به وسیله ایجاد یک مدل چند لایه پرسپترونی برای هر دو مدل مولد و تمایزگر انجام می‌شود. برای یادگيری توزیع مولد روی داده ، یك تابع نویز خالص را به عنوان ورودی تعریف مي­کنيم، سپس یك نگاشت از فضای نهفته به فضای داده را به عنوان نشان مي‌دهيم، در اینجا یك تابع مشتق‌پذیر است که توسط یك پرسپترون چند لایه با پارامترهای نمایش داده مي­شود. همچنين برای شبكه تمایزگر یك پرسپترون چند لایه لایه با یك خروجي اسكالر[[45]](#footnote-45) تعریف مي­کنيم. بيانگر احتمال این است که از داده‌های اصلي به جای توزیع ناشی شده باشد. در این میان به شبكه آموزش داده مي‌شود تا احتمال تخصيص برچسب صحيح را به داده‌های واقعی و نمونه‌های توليدی از را به حداکثر برساند. به طور همزمان به شبكه آموزش داده مي‌شود تا تابع هدف را به حداقل برساند. به عبارت دیگر، شبكه‌های و بازی کمینه-بیشینه دو نفره زیر با تابع مطابق معادله 2-4 انجام می‌دهند.

|  |  |
| --- | --- |
| (4-2) |  |

با تحليل نظری صورت گرفته بر روی شبكه‌های مولد تخاصمی، نشان داده شده است که این شبكه‌ها پتانسيل کافي برای بازیابي توزیع داده‌های اصلي را در قالب شبكه مولد دارند. در عمل معادله 2-1 ممکن است گرادیان کافی برای آموزش شبکه را فراهم نکند. در اوایل یادگیری، هنگامی که شبکه مولد ضعیف است، شبکه تمایزگر می‌تواند با اطمینان بالا نمونه‌های غیرواقعی را شناسایی کند چرا که نمونه‌های تولیدی با نمونه‌های آموزشی کاملا متفاوت هستند. در این حالت شباع می‌شود. در این حالت می‌توان به جای آموزش برای به حداقل رساندن تابع می‌توانیم را برای به حداکثر رساندن آموزش دهیم. این تابع در همان نقطه ثابت و قرار دارد اما گرادیان قوی‌تری در یادگیری فراهم می‌کند. رویكرد کلي شبکه‌های مولد تخاصمی در شكل 2-2 نشان داده شده است.



شکل 2-2: رویکرد کلی شبکه­های مولد تخاصمی [28].

همانطور که در شكل 2-2 مشاهده‌ می‌کنید توزیع تمایزگر (خط آبي شكسته) به‌روز‌رسانی می‌شود تا بتواند نمونه‌های توزیع داده‌های اصلي (خط مشكي نقطه‌چي) از داده‌های توليدشده توسط توزیع مولد )خط سبز پيوسته) تمیز دهد. خط افقي پایين بیانگر فضای نهفته است که متغیر z با توزیع یکنواخت از آن نمونه‌برداری شده است. خط افقی بالا بخشی از فضای داده واقعی x است. فلش‌های رو به بالا نشان می‌دهد که چگونه تابع ، z را به طور غیریکنواخت به x نگاشت می‌کند. به مرور زمان در مناطق چگال‌تر منقبض می‌شود و در مناطق با چگالی کمتر باز می‌شود. در قسمت (a) شکل 2-2 دو بلوک تخاصمی نزدیک همگرایی هستند،یعنی به نزدیک شده است و همچنین دسته‌بند تا حدی دقیق می‌باشد. در قسمت (b) در حلقه داخلی الگوریتم، آموزش می‌بیند تا بتواند نمونه‌های غیرواقعی را تشخیص دهد و به  همگرا شود. در (c) پس از به روزرسانی گرادیان ناشی از ، را به گونه‌ای هدایت می‌کند که به سمت مناطقی مایل شود که به توزیع داده واقعی نزدیک‌تر شود. در قسمت آخر (d) پس از انجام چند مرحله از آموزش اگر و ظرفیت کافی را داشته‌ باشند به نقطه تعادلی می‌رسند که در آن . و تمایزگر دیگر قادر نیست میان توزیع داده‌های واقعی و غیرواقعی تفاوتی قائل شود.

به منظور پیاده‌سازی این شبکه‌ها از روش عددی مبتنی بر تکرار استفاده می‌شود. تکمیل بهینه‌سازی شبکه در حلقه داخلی مرحله آموزش همراه با چالش‌هایی نظیر هزینه محاسباتی زیاد است و همچنین روی دادگان کوچک منجر به بیش‌برازش[[46]](#footnote-46) است. حال به جای اینکه در هر تکرار هر دو شبکه و بهینه شوند، به ازای k مرحله بهینه کردن یک مرحله بهینه می‌شود. با این کار تا زمانی که به اندازه کافی آهسته تغییر کند در نزدیکی نقطه بهینه باقی خواهد ماند. شبه کد الگوریتم شبکه‌های مولد تخاصمی در الگوریتم 2-1 آورده شده است.

|  |
| --- |
| k تعداد مراحل اعمال شده تمایزگر ( برای کاهش هزینه محاسبات اینجا عدد یک فرض می­شود) و n تعداد تکرار آموزش |
| for k steps do  for n steps do   * نمونه­برداری کوچک­دسته­ای[[47]](#footnote-47) mتایی نویز از نمونه­های نویز. * نمونه­برداری کوچک­دسته­ای mتایی نویز از داده­های تولید توزیع. * بروزرسانی صعودی تمایزگر به وسیله گرادیان تصادفی.   end for   * نمونه­برداری کوچک­دسته­ای mتایی نویز از نمونه­های نویز. * بروزرسانی صعودی مولد به وسیله گرادیان تصادفی.   end for |

الگوریتم 2-1: آموزش گرادیان نزولی کوچک دسته­ای شبکه­های مولد تخاصمی

#### 1-1-5-2- تحلیل نظری شبکه مولد تخاصمی

شبکه مولد به طور ضمنی یک تابع توزیع احتمال را به عنوان توزیع نمونه‌های تعریف کرده است(توجه داشته باشید z). در صورتی که ظرفیت مناسب و زمان کافی برای آموزش در اختیار الگوریتم 2-1 قرار گیرد در نهایت این الگوریتم توزیع داده ورودی را خواهد یافت. نتایج حاصل از شبکه‌های عصبی مولد تخاصمی بر اساس تنظیمات غیرپارامتری به دست آمده است. در این بخش نشان می‌دهیم که در بازی کمینه-بیشینه بین دو شبکه یک بهینه عمومی است. برای این منظور ابتدا تمایزگر بهینه را برای هر مولد در می‌گیریم.

**قضیه 2-1-** برای هر تابع مولد ثابت، تابع تمایزگر بهینه عبارت است از:

|  |  |
| --- | --- |
| (5-2) |  |

**اثبات:** معیار آموزش برای تمایزگر، با توجه به هر مولد ، به حداکثر رساندن مقدار می­باشد، پس داریم:

|  |  |
| --- | --- |
| (6-2) |  |

از طرفی می­دانیم برای هر،تابع دربازه در بیشینه است. هم­چنین می­دانیم تمایزگر نیاز به تعریف بیرون از مرز ندارد، پس در نتیجه نقطه بهینه برای به حداکثر رساندن می­باشد.

می­توان هدف از آموزش شبکه را به حداکثر رساندن لگاریتم درست­نمایی[[48]](#footnote-48) احتمال تعبیر کرد، که بیانگر آن است که هرجا از توزیع باشد و هر جا از توزیع باشد است. با این تعریف بازی کمینه-بیشینه در معادله 2-4 را می­توان به­صورت زیر، بازنویسی کرد:

|  |  |
| --- | --- |
| (7-2) |  |

**قضیه 2-2-** کمینه سراسری تنها در حالتی قابل محاسبه است که اگر و تنها اگر و مقدار برابر با باشد.

**اثبات:** طبق قضیه 2-1، می­دانیم هنگامی­که باشد ، می­شود. در ادامه نشان دادیم که حال برای اثبات این­که بهترین مقدار این مقدار است، این عبارت را از تعریف کم می­کنیم. طبق همگرایی جنسن-شانون[[49]](#footnote-49) داریم:

|  |  |
| --- | --- |
| (8-2) |  |

می­دانیم تابع همگرایی جنسن-شانون بین دو توزیع همواره نامنفی است و صفر است اگر و تنها اگر دو توزیع برابر باشند. پس ما نشان دادیم مقدار بهینه برابر با است و نقطه بهینه هنگام برابری دو توزیع رخ می­دهد. بدین ترتیب اثبات این قضیه نیز به پایان رسید.

#### 2-1-5-2- مزایا و معایب

شبکه­های مولد تخاصمی نسبت به مدل­های قبلی دارای مزایا و معایبی می­باشد. این معایب در درجه اول این است که نمایش صریح وجود ندارد و باید در حین آموزش به خوبی با هماهنگ شود به طور خاص، نباید بدون به‌روزرسانی خیلی زیاد آموزش داده شود که در آن مقدار مقادیر زیادی z به همان مقدار x بدست می آید تا از تنوع کافی برای مدل سازی برخوردار باشد، در هنگام یادگیری نیازی به استنباط نیست و می توان طیف گسترده­ای از توابع را در مدل گنجانید. مزایای ذکر شده در بالا در درجه اول محاسباتی است. مدل­های تخاصمی همچنین ممکن است برخی از مزیت­های آماری را از شبکه مولد به دست آورند که مستقیماً با نمونه داده‌ها به روز نمی­شوند، اما فقط با گرادیان­هایی که از طریق تمایزگر جریان می­یابند، بروزرسانی می­شود.

این بدان معنی است که اجزای ورودی مستقیماً در پارامترهای مولد کپی نمی­شوند. یکی دیگر از مزیت­های شبکه‌های تخاصمی این است که آنها می­توانند توزیع­های بسیار تیز و حتی تخریب کننده را نشان دهند، در حالی که روش­های مبتنی بر زنجیره‌های مارکوف نیاز دارند که توزیع تا حدی مبهم باشد تا زنجیرها بتوانند میان حالت­ها مخلوط شوند.

### 2-5-2- مدل ANOGAN

مدل ANOGAN به منظور مدل‌سازی در زمینه پزشکی و به طور خاص مدل‌سازی وضعیت سلامت موضعی آناتومی طراحی شده است. این مدل از دسته الگوریتم‌های مولد و بدون‌نظارت است. با به وجود آمدن این مدل توانایی شبکه‌های مولد تخاصمی در ایجاد یک مدل با قدرت بازنمایی بالا در تشریح وضعیت آناتومی ثابت شد. لازم به ذکر است مدل پیشنهادی شبکه تمایزگر و شبکه مولد را به طور همزمان آموزش می‌دهد و با استفاده از هر دو شبکه مشخص می‌کند داده ورودی از جنس داده‌های آموزشی است و یا باید به عنوان ناهنجاری دسته‌بندی شود.

به منظور تشخیص ناهنجاری مدل مورد نظر بازنمایی نمونه‌های متنوع آناتومیکی طبیعی را می‌آموزد. در این کار به جای استفاده از بهینه­سازی تابع هزینه واحد، از تعادل نش[[50]](#footnote-50) میان هزینه‌ها استفاده شده است که سبب افزایش قدرت بازنمایی و رشد نرخ منفی صحیح[[51]](#footnote-51) به اختصار TNR مدل تولیدی، بهبود روند نگاشت ویژگی[[52]](#footnote-52) و همچنین دستیابی به دقت بالا در طبقه­بندی داده­های واقعی از داده­های غیرواقعی می­شود. در ادامه چگونگی طراحی مدل و نحوه شناسایی وضعیت و ظواهری که در داده‌های آموزش دیده نشده‌اند شرح داده خواهد شد.

#### 1-2-5-2- یادگیری بدون نظارت تنوع آناتومیکی طبیعی

مجموعه­ای از تصاویر پزشکی است که هر نمونه آن نمایانگر نمونه‌هایی از آناتومی‌های سالم است و با نمایش داده می­شود که ، در اینجا است یعنی اندازه یک تصویر برابر است. از هر تصویر ، تکه­ تصویر دو بعدی ، با ابعاد بطور تصادفی از موقعیت­های مختلف نمونه­گیری می­کنیم که منجر به داده­های ، می شود. در طول آموزش، فقط را در اختیار داریم و برای یادگیری توزیع حاشیه­ای، که نشان دهنده تنوع تصاویر آموزش است، از یک روش بدون نظارت استفاده می­شود. برای آزمایش، داریم ، که تصاویر مشاهد نشده با ابعاد استخراج شده از داده است و آرایه­ای از برچسب­های حقیقی مبتنی بر تصویر باینری با است. این برچسب­ها فقط در طول آزمایش استفاده می­شوند، تا کارایی روش تشخیص ناهنجاری ارزیابی شود.

شبکه مولد توزیع را روی داده از طریق نگاشت نمونه‌های z توسط تابع آموزش می­بیند؛ در واقع بردارهای تک بعدی با توزیع یکنواخت از فضای نهفته نمونه­برداری می­‌شوند و به فضای دو بعدی تصویر که در آن تصاویر آناتومی سالم وجود دارند نگاشت می‌شوند. در این تنظیمات، معماری شبکه مولد معادل یک رمزگذار پیچشی[[53]](#footnote-53) که از پشته­های پیچشی استفاده می­کند، در نظر گرفته می­شود. تمایزگر یک CNN استاندارد است که یک تصویر دو بعدی را به یک مقدار نگاشت می­کند. مقدار خروجی تمایزگر بیانگر احتمال این است که ورودی تمایزگر، از فضای تصاویر واقعی یعنی فضای نمونه‌های آموزشی نمونه­برداری شده باشد و یا توسط شبکه مولد تولید شده باشد. و به طور همزمان از طریق بازی کمینه-بیشینه با تابع و معادله 2-9 بهینه­سازی می­شوند]10[.

|  |  |
| --- | --- |
| (9-2) |  |

در این بازی شبکه تمایزگر آموزش می­بیند که احتمال اختصاص نمونه­های واقعی را بیشینه و نمونه­های تولیدی از با برچسب جعلی را کمینه کند. هم­چنین شبکه مولد آموزش می­بیند همزمان با حداقل کردن که معادل با حداکثرکردن است، شبکه تمایزگر را فریب دهد. به طور کلی در طول آموزش تخاصمی، مولد در تولید تصاویر واقع بینانه و تمایزگر در شناسایی صحیح تصاویر واقعی و تولید شده بهبود می­یابد.

#### 2-2-5-2- نگاشت تصاویر جدید به فضای نهفته

وقتی آموزش تخاصمی به پایان رسید، شبکه مولد یاد می­گیرد که را از فضای نهفته با نمایش z به تصویر واقعی (عادی) xنگاشت کند. شبکه­های GAN­ به­طور خودکار نگاشت معکوس را انجام نمی­دهد. فضای نهفته دارای گذار خطی است، بنابراین نمونه­گیری از دو نقطه نزدیک بهم در فضای نهفته، دو تصویر مشابه بصری نیز ایجاد می­کند.

با فرض اینکه تصویر را برای بررسی داریم، هدف این است که یک نقطه را در فضای پنهان پیدا کنیم که مطابق با تصویر باشد و از نظر بصری در آن نقطه شبیه به تصویر باشد و در توزیع حاشیه­ای قرار داشته باشد. میزان شباهت و بستگی به این دارد که چه تصویری از توزیع داده برای آموزش مولد استفاده می‌شود. برای پیدا کردن بهترین ، با نمونه­گیری تصادفی از توزیع فضای نهفته شروع می‌کنیم و آن را به شبکه مولد آموزش دیده، برای تولید تصویر اعمال می­کنیم. سپس بر اساس تصویر ایجاد شده یک تابع اتلاف تعریف می­کنیم، که گرادیان به روزرسانی ضرایب را فراهم می­کند و در نتیجه یک موقعیت بروز شده در فضای نهفته بدست می­آید. به عبارتی برای پیدا کردن شبیه­ترین تصویر ، نقطه در فضای نهفته در یک فرآیند تکراری از طریق با مراحل پس­انتشار بهینه می­شود.

تعریف تابع اتلاف برای نگاشت از تصاویر فضای نهفته شامل دو بخش است]31[، باقی­مانده اتلاف[[54]](#footnote-54) و باقی­مانده تمایز[[55]](#footnote-55). باقی­مانده اتلاف شباهت بصری بین تصویر تولید شده و تصویر مورد بررسی را تقویت می­کند. باقی­مانده تمایز، تصویر تولید شده را در حاشیه توزیع آموزش دیده قرار می­دهد. بنابراین، هر دو مؤلفه GAN آموزش دیده، تمایزگر و مولد ، برای یافتن ضرایب از طریق پس­انتشار مورد استفاده قرار می­گیرند.

باقی‌مانده اتلاف معیار عدم شباهت بصری بین تصویر مورد بررسی و تصویر تولید شده در فضای تصویر اندازه­گیری می­کند و به­صورت معادله 2-10 تعریف می­شود.

|  |  |
| --- | --- |
|  | (10-2) |

با فرض یک مولد کامل و یک نگاشت کامل فضای نهفته، برای یک مورد بررسی ایده­آل، تصاویر و یکسان هستند. در این حالت باقی­مانده تلفات برابر با صفر است.

باقی‌مانده تمایز برای تأمین تصویر، باقی­مانده تمایز را بر اساس خروجی تمایزگر با اعمال تصویر تولید شده در تمایزگر محاسبه می­کنیم، در این­ رابطه آنتروپی متقاطع سیگموئید[[56]](#footnote-56)، که از تمایز اتلاف تصاویر واقعی حین آموزش متخاصم، با تابع لاجیت[[57]](#footnote-57) و تعریف می­شود.

#### 3-2-5-2- تشخیص ناهنجاری­

در طی شناسایی ناهنجاری­ها در داده­ی جدید، ابتدا نمونه مورد بررسی جدید را به عنوان یک تصویر طبیعی یا غیر عادی ارزیابی می­کنیم. تابع اتلافی که برای نگاشت به فضای نهفته مورد استفاده قرار می­گیرد، در هر تکرار بروزرسانی می­شود و سازگاری تصاویر تولید شده با تصاویر را که در طول آموزش متخاصم مشاهده می­شود ارزیابی می­کنیم. بنابراین، یک نمره ناهنجاری که تناسب تصویر مورد جستجو را با مدل تصاویر عادی بیان می­کند، این معیار می­تواند مستقیماً از تابع اتلاف 2-11 بدست آید.

|  |  |
| --- | --- |
|  | (11-2) |

که در آن به ترتیب امتیاز باقی­مانده و امتیاز تمایزگر است که توسط باقی­مانده اتلاف و باقی­مانده تمایز در فضای نهفته تعریف می­شود. این مدل، نمره ناهنجاری بزرگی برای تصاویر غیر عادی بدست می آورد و یک نمره ناهنجاری کوچک بدین معنی است که این تصویر بسیار مشابه تصاویر قبلاً در طول آموزش دیده شده، می­باشد. برای تشخیص ناهنجاری مبتنی بر تصویر، از نمره ناهنجاری استفاده می­شود. علاوه بر این، از تصویر باقی­مانده برای شناسایی مناطق غیر عادی در یک تصویر استفاده می‌شود. برای مقایسه، علاوه بر این امتیاز ناهنجاری را مطابق معادله 2-12 تعریف می­شود، در اینجا همان امتیاز تمایزگر و امتیاز باقی­مانده می­باشد.

|  |  |
| --- | --- |
|  | (12-2) |

#### 4-2-5-2- مزایا و معایب­

علیرغم نتایج قابل قبول این مدل در تشخیص ناهنجاری در تصاویر پزشکی، همانطور که مشاهده کردیم، برای بررسی تصویر ، باید نقطه متناظر با آن در فضای نهفته پیدا شود به طوری که در آن نقطه از نظر بصری بیشتر شبیه به تصویر باشد. برای پیدا کردن بهترین ، باید با نمونه­گیری تصادفی از توزیع فضای نهفته شروع کنیم و آن را به شبکه مولد آموزش بدهیم و برای تولید تصویر اعمال می­کنیم. سپس بر اساس تصویر ایجاد شده می‌بایست یک تابع اتلاف تعریف کنیم، که گرادیان به روزرسانی ضرایب را فراهم کند و در نتیجه یک موقعیت بروز شده در فضای نهفته بدست آورد. به عبارتی برای پیدا کردن شبیه­ترین تصویر ، نقطه در فضای نهفته در یک فرآیند تکراری از طریق با مراحل پس­انتشار بهینه و پیدا می‌شود. این فرایند تکراری مبتنی بر تصادف است و هزینه و پیچیدگی محاسباتی زیادی به مدل تحمیل می‌کند. با توجه به وجود این مشکل می‌توان مکانیزمی طراحی کرد که مدل پیشنهادی فرایند نگاشت معکوس تصاویر در حین آموزش مدل فرابگیرد.

### 3-5-2- مدل f-AnoGan

مدل f-AnoGan در ادامه کار قبلی و توسط همان نویسندگان در سال 2019 ارائه شد. در مدلAnoGan از شبکه‌های عصبی عمیق کانولوشنی مولد تخاصمی[[58]](#footnote-58) به اختصار DCGAN برای آموزش بدون نظارت شبکه مولد و تمایزگر استفاده شده است. در مدل قبلی برای شناسایی نقطه متناسب با تصویر ورودی بر اساس الگوریتم پس‌انتشار از یک فرایند مبتنی بر تکرار استفاده می‌شد. به هنگام شناسایی ناهنجاری در کاربردهای دنیای واقعی این فرایند مبتنی بر تکرار از نظر پیچیدگی زمانی مشکلاتی را از نظر زمان ایجاد می‌کند.f-AnoGan فرایند مبتنی بر تکرار مورد نظر را با یادگیری یک نگاشت از فضای اصلی به فضای نهفته جایگزین می‌کند. علاوه بر این در ساختار مدل جدید از WGAN[[59]](#footnote-59) به جای DCGAN استفاده شده است.

چهارچوب ارائه شده در این کار شامل دو گام آموزشی روی تصاویر عادی است، در گام اول شبکه مولد تخاصمی آموزش می‌بیند و در گام بعدی بر اساس شبکه مولد آموزش دیده شده کدگذار آموزش می‌بیند. پس از آموزش قسمت‌های مختلف مدل بر اساس استنتاج برای هر تصویر یک امتیاز ناهنجاری محاسبه می‌شود. همانند کار قبلی شبکه مولد روی تصاویر عادی آموزش داده می‌شود و بازنمایی‌های تنوع آناتومی‌های سالم در فضای نهفته به دست می‌آید. علاوه بر این کدگذار نیز نگاشت تصاویر به فضای نهفته را آموزش می‌بیند. در ادامه در سه بخش به بررسی شبکه‌های تمایزگر و مولد، کدگذار و نحوه امتیاز‌دهی به داده‌ها به منظور تشخیص داده‌های ناهنجار می‌پردازیم.

#### 1-3-5-2- GAN یادگیری بدون نظارت تنوع آناتومیکی طبیعی

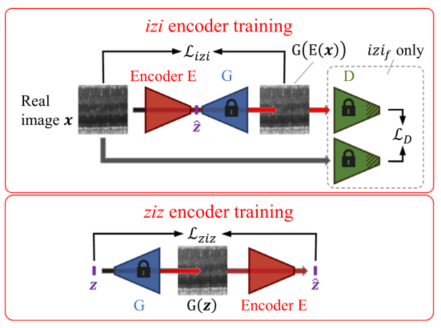
داده‌های آموزشی در این مدل به شکل نمایش داده می‌شود. در این نوع از نمایش و است. به بیان دیگر تعداد تصویر پزشکی داریم و از هر تصویر *به صورت تصادفی از مناطق مختلف تصویر تعداد نمونه با ابعاد انتخاب می‌شود. توجه شود*  *و*  و *.* برای ارزیابی مدل از داده تصویر با ابعاد  که از میان دادگان آزمایش انتخاب شده است، حاشیه نویسی پیکسل مربوطه به صورتو برچسب مربوطه استفاده می‌شود. این مجموعه داده آزمایش به صورت است و به طور همزمان شامل داده عادی و ناهنجار است.

برای یادگیری تنوع آناتومی موجود در تصاویر از WGAN استفاده می‌شود. این شبکه نگاشت غیرخطی از فضای نهفته *به فضای ورودی را یاد می‌گیرد. مانند مدل‌های دیگر در این مدل نیز شبکه مولد و تمایزگر به طور همزمان بهینه می‌شوند. در ابتدا از فضای با ابعاد d نمونه نویز انتخاب می‌کنیم. در طول فرایند آموزش شبکه مولد تلاش می‌کند تا توزیع شبکه مولد یعنی را تا حد امکان به توزیع داده ورودی یعنی نزدیک کند و در نتیجه بتواند شبکه تمایزگر را به گونه‌ای فریب دهد که نتواند تشخیص دهد از توزیع داده واقعی است و یا توسط شبکه مولد ایجاد شده است. در پایان فرایند آموزش شبکه مولد توزیع داده‌های آموزشی را یاد گرفته است و شبکه تمایزگر می‌تواند تخمین بزند داده تولیدی توسط مولد تا چه اندازه به توزیع داده واقعی نزدیک است.*

#### 2-3-5-2- یادگیری نگاشت سریع از فضای تصویر به فضای نهفته

شبکه مولد GAN را می‌توان به صورت *نمایش داد. این نمایش به توانایی نگاشت شبکه مولد از فضای نهفته به فضای داده ورودی اشاره دارد. در روند آموزشی* GAN *هیچ نگاشتی از فضای داده ورودی به فضای نهفته آموزش داده نمی‌شود. در مدل پیشنهادی این مقاله نگاشت معکوس به صورت* نمایش داده می‌شود و این نگاشت توسط یک کدگذار آموزش دیده می‌شود. آموزش این کدگذار با دو معماری مختلف قابل پیاده‌سازی است، روش اول z-image-z و روش دوم image-z-image نام دارد. روش اول که به صورت خلاصه ziz و روش دوم به طور خلاصه izi نامیده می‌شود. در هر دو معماری از خودکدگذار‌های کانولوشنی استفاده می‌شود. از کدگذار *E* برای نگاشت معکوس استفاده می‌شود و از شبکه مولد که در واقع یک WGAN با اوزان یادگرفته‌شده ثابت است به عنوان کدگشا استفاده می‌شود. تفاوت دو روش فوق در ترتیب استفاده از کدگذار و کدگشاست.

هنگام آموزش کدگذار تنها پارامترهای کدگذار بهینه می‌شوند و پارامترهای شبکه مولد ثابت هستند. معماری‌های مختلف جهت آموزش کدگذار در شکل 2-3 قابل مشاهد است.



شکل 2-3: شمای کلی روند آموزش کدگذار

درآموزش کدگذار به روش izi خطای *بر اساس باقی‌مانده[[60]](#footnote-60)* *از تفاوت تصاویر ورودی واقعی و تصویر بازسازی شده بهینه می‌شوند کد گذار آموزش می‌بیند. آموزش کدگذار به روش به صورت توام خطای*  که همان خطای باقی‌مانده میان تصویر ورودی واقعی و تصویر بازسازی شده است به همراه خطای *بر اساس خطای باقی‌مانده روی ویژگی‌های شبکه تمایزگر است بهینه می‌شود. در آموزش کدگذار به روش*  خطای باقی‌مانده میان نمونه‌های تصادفی و موقعیت‌های موجود در فضای نهفته بهینه می‌شود.

الگوریتم ziz با معکوس کردن ترتیب کدگذار و کدگشا در ساختار معمول یک خودکدگذار به وجود می‌آید. در هنگام آموزش یک نمونه از فضای نهفته انتخاب می‌شود و با استفاده از شبکه مولد که وزن‌های آن ثابت نگاه داشته شده است به فضای داده واقعی نگاشت می‌شود و کدگذار تلاش می‌کند تا معکوس این نگاشت به فضای نهفته را یاد بگیرد، بنابراین در این روش به هیچ تصویر واقعی یا به بیان دیگر به هیچ نمونه‌ای از فضای داده واقعی نیاز نیست. در واقع در معماری ziz ساختار یک کدگذار از فضای نهفته به فضای نهفته است و در همین حال نگاشت مورد نیاز از فضای نهفته به فضای واقعی داده ورودی ثابت در نظر گرفته شده است. تابع هدف این آموزش به صورت خطای MSE[[61]](#footnote-61) روی نمونه اولیه z و مقدار بازسازی شده آن توسط کدگذار تعریف شده است. تابع هدف این معماری را در زیر مشاهده می‌کنید:

|  |  |
| --- | --- |
| (13-2) |  |

d در معادله بیانگر ابعاد نمونه‌ها در فضای نهفته است. در این روش کدگذار بر خلاف روش izi هیچ نمونه‌ای از فضای تصاویر واقعی نمی‌بیند و این مسئله می‌تواند بر آموزش صحیح کدگذار تاثیر منفی بگذارد.

در آموزش کدگشا به روش izi از ساختار کدگذار استاندارد استفاده می‌شود، بدین صورت که در ادامه کدگذار کدگشا (شبکه مولد) قرار خواهد گرفت. در فرایند آموزش ابتدا نگاشت معکوس از فضای داده واقعی به فضای نهفته توسط کدگذار انجام می‌شود و در ادامه نگاشت از فضای نهفته به فضای داده واقعی توسط کدگشا با ضرایب ثابت صورت می‌پذیرد. ساختار این روش به صورت از فضای واقعی به فضای واقعی است. تابع هدف این روش با استفاده از خطای MSE بدین شکل پیاده‌سازی می‌شود که خطای باقی‌مانده میان تصویر واقعی و تصویر خروجی مولد کمینه می‌شود، تابع هدف مورد نظر در ادامه آمده است:

|  |  |
| --- | --- |
| (14-2) |  |

در معادله 2-14 بیانگر جمع مربعات خطا در سطح پیکسل میان دو تصویر است. داده‌های آموزشی این روش داده‌های آموزش همان WGAN یعنی داده‌های عادی است. در این روش نمی‌توان به طور مستقیم میزان دقت کدگذار را در فضای نهفته اندازه گرفت و تنها می‌توان به صورت غیرمستقیم نگاشت مربوط به فضای نهفته را به فضای داده واقعی انتقال داده و در این فضا میزان دقت را اندازه گرفت به بیان دیگر میزان دقت به صورت تصویر-تصویر محاسبه می‌شود.

در روش دیگر به نام izifاز تمایزگر نیز استفاده می‌شود. در روش izi تابع هدف میزان شباهت در فضای تصویر را تحمیل می‌کند. هنگام نگاشت تصاویر جدید ممکن است با نمونه‌هایی روبرو شویم که در مرحله آموزش به صورت تنک از فضای نهفته متناظر آن‌ها نمونه گرفته باشیم وقتی نقطه متناظر را به فضای تصویر(فضای داده ورودی) می‌بریم با تصاویر تولیدی دیگر نمی‌توان تمایزگر را متقاعد کرد. در نتیجه این اتفاق تنها کمینه کردن تفاوت تصاویر در سطح پیکسل گاهی اوقات منجر به تولید تصاویر عادی می‌شوند که واقعی به نظر نمی‌رسند ولی هنوز خطای باقی‌مانده کمی حتی برای نمونه‌های ناهنجار دارند و این مورد سبب می‌شود تا دیگر خطای باقی مانده (خطای بازسازی) در فضای داده ورودی دیگر به عنوان معیار مناسب تشخیص ناهنجاری در نظر گرفته نشود.

نویسندگان مقاله دریافتند که باقی‌مانده که خود معیار مورد نظر ما برای تشخیص ناهنجاری است در فضای ویژگی توسط تمایزگر انباشته می‌شود و این عبارت حتما باید در تابع هدف مربوط به آموزش کدگذار گنجانده شود. بنابر این آمارگان تصاویر ورودی و تصاویر خروجی محاسبه می‌شود تا با استفاده از آن‌ها تصاویر خروجی شبکه مولد شبیه تصاویر ورودی بشود و بدین ترتیب روش izif پدید آید. تابع هدف این روش به شکل زیر است:

|  |  |
| --- | --- |
| (15-2) |  |

در معادله 2-15 ویژگی‌های شبکه تمایزگر که در واقع بردار ویژگی لایه‌های میانی این شبکه است با *و* *ابعاد این ویژگی با نماد نمایش داده می‌شود، همچنین* عامل وزن است. اوزان شبکه تمایزگر همان اوزانی است که در آموزش WGAN یاد گرفته شده‌اند و هنگام آموزش کدگشا ثابت در نظر گرفته شده‌اند. این مدل سبب می‌شود تا هم در فضای تصویر و هم در فضای نهفته کدگذار به جهت مناسبی حرکت کند.

#### 3-3-5-2- شناسایی ناهنجاری

در مرحله آزمایش میزان انحراف تصویر اصلی از تصویر بازسازی شده به منظور تشخیص ناهنجاری اندازه‌گیری می‌شود. تمامی موارد مورد نیاز برای بازسازی تصویر و تشخیص ناهنجاری در هنگام آموزش WGAN و کدگذار یادگرفته می‌شود. برای محاسبه امتیاز ناهنجاری مستقیما از تعریف خطای استفاده شده در آموزش کدگذار استفاده می‌شود. امتیاز نهایی که برای تشخیص ناهنجاری در مدل f-AnoGan استفاده می‌شود به صورت زیر است.

|  |  |
| --- | --- |
| (16-2) |  |

در اینجا و ، همچنین *عامل وزن است. عبارت مورد نظر برای نمونه‌های عادی دارای خطای کمی است و برای نمونه‌های ناهنجار دارای مقدار بزرگی است. از آنجایی که مدل تنها روی نمونه‌های عادی آموزش دیده است نمونه‌های بازسازی شده از نظر بصری شبیه تصویر ورودی هستند. توانایی بازسازی تصویر به طوری که شبیه تصویر ورودی باشد رابطه عکس دارد با درجه یا میزان تمایز ناهنجاری دارد. تصاویر عادی میزان انحراف کمی دارند در حالی‌که تصاویر ناهنجار که به بازسازی خود نگاشت می‌شوند میزان انحراف زیادی دارند. قدر مطلق خطای باقی‌مانده در سطح پیکسل به صورت زیر تعریف می‌شود.*

|  |  |
| --- | --- |
| (17-2) |  |

#### 4-3-5-2- مزایا و معایب

f-AnoGan مشکلات مدل قبلی (AnoGan) نظیر پیچیدگی زمانی بالا در هنگام اجرا رفع کرد. همچنین از شبکه مولد تخاصمی قوی‌تری در ساختار مدل خود استفاده کرد و به نتایج قبابل قبولی نیز دست یافت. در مدل قبلی از یک فرایند تصادفی و مبتنی بر تکرار برای نگاشت معکوس از فضای داده واقعی به فضای نهفته استفاده می‌شد که از نظر زمانی هزینه گزافی را به هنگام اجرا به مدل تحمیل می‌کرد. در مدل جدید f-AnoGan با استفاده از یک کدگشا پارامترهای نگاشت معکوس مورد نظر فراگرفته می‌شود. علی‌رغم این موفقیت این مدل همچنان از مشکلاتی نظیر عدم استفاده توام از هر دو فضای تصویر و نهفته برای آموزش کدگشا رنج می‌برد.

### 4-5-2- مدل ALI

این شبکه در سال 2017 در کنفرانس ICLR معرفی شد]11[. این شبکه­ها با هدف یادگیری نگاشت معکوس از دامنه ورودی­ها به دامنه توزیع تعریف شد. در این شبکه، علاوه بر شبکه مولد که در معماری اصلی نیز تعریف شده بود، یک رمزگذار[[62]](#footnote-62) E نیز وجود دارد که از دامنه داده­های ورودی به دامنه ویژگی­ها می­برد. بدین ترتیب خروجی بخش مولد یک دوتایی[[63]](#footnote-63) است؛ که یکی از دامنه ویژگی­ها و دیگری از دامنه داده­های ورودی است. این مدل به طور همزمان شبکه مولد و شبکه استنتاج را با استفاده از یک فرآیند تخاصمی به کار می­برند. شبکه مولد، نمونه­ها را از یک فضای نهفته آماری به فضای داده­ها نگاشت می­کند و شبکه استنتاج نمونه­های آموزش را از فضای داده به فضای متغیرهای نهفته نگاشت می­کند. به این صورت یک بازی خصمانه بین دو شبکه انجام می­شود. در این جا شبکه متمایزگر باید یاد بگیرد تا تفاوت بین جفت ورودی فضای نهفته و فضای داده را تشخیص دهد. شبکه تمایزگر در این­جا علاوه بر تفکیک در فضای داده، در فضای ویژگی نیز تفکیک می­کند. به این معنا که تشخیص می­دهد دوتایی وارد­شده، داده واقعی است با ویژگی تولیدشده توسط و یا داده جعلی است که توسط و با ویژگی­های درست شده­است. در تصویر زیر چارچوب کلی این الگوریتم، به نمایش درآمده است:



شکل 2-4: معماری شبکه ALI

**دو تابع توزیع احتمال روی و در نظر بگیرید:**

* **تابع توزیع تعریف شده برای رمزگذار**  *E*
* **تابع توزیع تعریف شده برای رمزگشا**

**این دو توزیع، توابع توزیع حاشیه­ای دارند که برای ما آشناست: توزیع حاشیه­ای رمزگذار تابع توزیع داده­های اصلی است و توزیع حاشیه­ای رمزگشا معمولا به عنوان یک تابع توزیع ساده مانند تابع توزیع استاندارد در نظر بگیریم. بدین ترتیب روند تولید معکوس می­باشد.**

**هدف اصلی شبکه** ALI **مطابقت این دو توزیع است. اگر این شرط محقق شود، ما اطمینان حاصل می­کنیم که تمام توزیع­های حاشیه­ای و توزیع­های شرطی مطابقت دارد. برای دستیابی به این توابع توزیع، یک بازی تخاصمی صورت می‌گیرد. جفت از دو توزیع در نظر گرفته می‌شود و یک شبکه تمایزگر می‌آموزد تا بین این دو خروجی، تمایز قائل شود؛ در حالی که دو شبکه رمزگشا و رمزگذار می­آموزند تا این شبکه را فریب دهند. در نهایت تابع هدفی که این بازی بر اساس آن صورت می­گیرد به صورت زیر است:**

|  |  |
| --- | --- |
| (18-2) |  |

**ویژگی جالب رویکردهای خصمانه این است که آنها نیازی به محاسبه تابع چگالی شرطی ندارند. آنها فقط نیاز دارند که به نحوی نمونه برداری شوند که این امکان را به وجود آورد که بتواند از پس انتشار گرادیان استفاده کند. در مورد شبکه** ALI **، این بدان معنی است که گرادیان ها باید از شبکه تمایزگر به شبکه­های رمزگذار و رمزگذار انتشار یابند.**

**به طور دقیق­تر شبکه تمایزگر آموزش می بیند که بین نمونه­هایی که از رمزگذار و نمونه هایی که از رمزگشا تولید می­شود، تمایز بگذارد. شبکه مولد و شبکه رمزگذار نیز می­آموزند که شبکه تمایزگر را فریب دهند؛ یعنی جفت تولید کنند که غیر قابل تشخیص باشد.**

**در الگوریتم 2-2 شبکه** ALI **توصیف شده است. اثبات می­شود که با فرض یک تمایزگر بهینه، شبکه مولد، واگرایی جنسن-شانون را بین به حداقل می‌رساند.**

روش استفاده شده در مدل ALI تنها راه استنتاج در شبکه‌های عصبی مولد تخاصمی نیست. راه دیگر برای انجام این کار استفاده از شبکه استنتاج جلورو[[64]](#footnote-64) در ساختارGAN است. در مدل InfoGAN[[65]](#footnote-65) ]32[ با کمینه کردن اطلاعات متقابل[[66]](#footnote-66) میان مجموعه **از فضای نهفته و**  **به وسیله توزیع کمکی**  نگاشت معکوس را یاد می‌گیرد. InfoGan نیاز دارد تا تابع احتمال پسین[[67]](#footnote-67) قابل تخمین و ارزیابی باشد. در مدل ALI تنها نیاز است که بتوان از شبکه استنتاج نمونه گرفت تا بدین وسیله تابع پیچیده توزیع پسین را بازنمایی کرد. عمل انجام شده در این کار مشابه این است که یک کدگذار برای بازسازی آموزش دهیم. به عنوان مثال پیدا کردن کدگذار به طوری که . نمونه که در جمله قبل بدان اشاره شد از نظر رویه‌ای شبیه به InfoGAN اما در این روش از یک شبکه مولد با ضرایب ثابت و همچنین تابع توزیع پسین گوسی با واریانس قطری ثابت استفاده شده است.

روند آموزش را می‌توان به دو فاز تقسیم کرد. در فاز اول شبکه مولد تخاصمی به صورت معمول آموزش می‌بیند. در فاز دوم کدگشا ثابت در نظر گرفته می‌شود و کدگذار به روش مدل ALI آموزش داده می‌شود. در این روش کدگذار و کدگشا در هنگام آموزش هیچ تعاملی با هم ندارند و در واقع کدگذار بر اساس هر چه کدگشا آموخته است آموزش می‌بیند. مشخص است اگر کدگذار و کدگشا با هم تعامل داشته باشند روند مدل‌سازی داده بهبود خواهد یافت.

|  |
| --- |
| رویه آموزش یادگیری خصمانه استنتاج |
| Repeat  M نمونه برداری اولیه از مجموعه داده  انتخاب شرطی  محاسبه پیش­بینی تمایزگر  محاسبه تلفات تمایزگر  محاسبه تلفات مولد  بروزرسانی گرادیان تمایزگرشبکه  بروزرسانی گرادیان مولد شبکه  Until |

الگوریتم 2-2: رویه آموزش یادگیری خصمانه استنتاج

#### 1-4-5-2- مقایسه مدل‌های ALI و GAN­

شبکه ALI شباهت زیادی به شبکه GAN دارد ، اما دو تفاوت اساسی با آن دارد:

1- بخش مولد دارای دو مؤلفه است: بخش رمزگذار، که نمونه­های داده را به فضای z نگاشت می­کند و بخش رمزگشایی که نمونه­ها را از (منبع منبع نویز) به فضای ورودی نگاشت می­کند.

2- بخش تمایزگر به منظور تمایز بین جفت ، آموزش دیده می­شود.

#### 2-4-5-2- رویکرد‌های جایگزین برای استنتاج در GAN

**روش استفاده شده در مدل** ALI **تنها راه استنتاج در شبکه‌های عصبی مولد تخاصمی نیست. راه دیگر برای انجام این کار استفاده از شبکه استنتاج جلورو[[68]](#footnote-68) در ساختار**GAN **است. در مدل** InfoGAN[[69]](#footnote-69) ]**32**[ **با کمینه کردن اطلاعات متقابل[[70]](#footnote-70) میان مجموعه**  **از فضای نهفته و به وسیله توزیع کمکی نگاشت معکوس را یاد می‌گیرد.** InfoGan **نیاز دارد تا تابع احتمال پسین[[71]](#footnote-71) قابل تخمین و ارزیابی باشد. در مدل** ALI **تنها نیاز است که بتوان از شبکه استنتاج نمونه گرفت تا بدین وسیله تابع پیچیده توزیع پسین را بازنمایی کرد. عمل انجام شده در این کار مشابه این است که یک کدگذار برای بازسازی آموزش دهیم. به عنوان مثال پیدا کردن کدگذار به طوری که . نمونه که در جمله قبل بدان اشاره شد از نظر رویه‌ای شبیه به** InfoGAN **اما در این روش از یک شبکه مولد با ضرایب ثابت و همچنین تابع توزیع پسین گوسی با واریانس قطری ثابت استفاده شده است.**

**روند آموزش را می‌توان به دو فاز تقسیم کرد. در فاز اول شبکه مولد تخاصمی به صورت معمول آموزش می‌بیند. در فاز دوم کدگشا ثابت در نظر گرفته می‌شود و کدگذار به روش مدل** ALI **آموزش داده می‌شود. در این روش کدگذار و کدگشا در هنگام آموزش هیچ تعاملی با هم ندارند و در واقع کدگذار بر اساس هر چه کدگشا آموخته است آموزش می‌بیند. مشخص است اگر کدگذار و کدگشا با هم تعامل داشته باشند روند مدل‌سازی داده بهبود خواهد یافت.**

#### 3-4-5-2- مزایا و معایب

**اگرچه وجود مکانیزم مناسب جهت نگاشت معکوس از فضای داده واقعی به فضای نهفته سبب موفقیت و عملکرد قابل قبول مدل** ALI **شده است اما در این مدل هیچ سازوکاری جهت کنترل میزان شباهت تصویر اصلی و تصویر بازسازی سده در آن تعبیه نشده است و به همین جهت در برخی موارد هیچ شباهتی میان داده اصلی و داده بازسازی شده وجود ندارد. به بیان دیگر پس از یافتن نقطه متناسب با داده مورد نظر در فضای داده واقعی در فضای نهفته، نقطه مورد نظر را به شبکه مولد می‌دهیم و خروجی حاصل را با ورودی ابتدایی مقایسه می‌کنیم. انتظار می‌رود داده ورودی و خروجی در این چرخه شباهت زیادی داشته باشند ولی همانطور که گفته شد در برخی از نمونه‌ها شباهتی میان این دو تصویر وجود ندارد.**

### 5-5-2- مدل EGBAD

همانطور که گفته شد شبکه‌های عصبی تخاصمی قادرند توزیع‌‌های پیچیده دنیای واقعی با ابعاد بالا را مدل کنند و همین امر سبب می‌شود تا بتوان از این شبکه‌ها در زمینه تشخیص ناهنجاری نیز کرد. با توجه به تعداد کارهای انگشت شمار در این زمینه، مدل EGBAD را می‌توان از اولین کارها در تشخیص ناهنجاری با استفاده از شبکه‌های عصبی تخاصمی به شمار آورد.

مدل ارائه شده بر اساس شبکه عصبی تخاصمی دوطرفه به اختصار BiGAN[[72]](#footnote-72) بنا نهاده شده است. وظیفه نگاشت معکوس از فضای داده ورودی به فضای نهفته نیز بر عهده کدگذار است. کدگذار، شبکه مولد و تمایزگر در اینجا به طور همزمان آموزش می‌بینند و وجود بلوک کدگذار سبب کاهش هزینه‌های محاسباتی در گام آزمایش می‌شود. بر خلاف ساختار استاندارد GAN که در آن تمایزگر تنها تصویر واقعی و تصویر تولیدی شبکه مولد را ورودی می‌گیرد، بازنمایی این تصاویر در فضای نهفته هم به عنوان ورودی به شبکه تمایزگر داده می‌شود.

استراتژی مورد استفاده در گام آموزش مدل مشابه کار ]11[ است. همانطور که در قسمت قبل بررسی شد در این استراتژی آموزشی تاکید بر آن است که شبکه مولد و کدگذار به طور توامان آموزش داده شوند. در هنگام آموزش معادله زیر بهینه می‌شود.

|  |  |
| --- | --- |
| (19-2) |  |

**در معادله 2-19**  بیانگر تابع توزیع داده ورودی است، بیانگر توزیع نمونه‌ها در فضای نهفته است، و به ترتیب بیانگر تابع توزیع کدگذار و کدگشا هستند.

پس از آموزش مدل نوبت به تعریف معیاری می‌رسد که به وسیله آن بتوان نمونه‌های ناهنجار را تشخیص داد. بیان ریاضی این معیار در ادامه آمده است.

|  |  |
| --- | --- |
| (20-2) |  |

**در معادله 2-20**  و را می‌توان به دو روش تعریف کرد. در روش اول تابع خطای آنتروپی[[73]](#footnote-73) متقابل استفاده می‌شود. ورودی این تابع در واقع خروجی تمایزگر است و خود شامل خروجی کدگذار و نمونه متناظر با آن است و به صورت تعریف می‌شود. در اینجا خروجی تمایزگر میزان اطمینان آن در قبال واقعی بودن نمونه ورودی است. در روش دوم تعریف از خطای تطبیق ویژگی[[74]](#footnote-74) استفاده می‌شود. تابع امتیاز این روش به صورت تعریف می‌شود. در واقع لاجیت‌های تمایزگر است و بیان می‌کند ویژگی‌های تصویر بازسازی شده تا چه اندازه شبیه ویژگی‌های تصویر واقعی هستند. توجه شود هر چه مقدار امتیاز محاسبه شده بالاتر باشد نمونه مورد نظر با احتمال بیشتری نمونه ناهنجار است.

#### 1-5-5-2- مزایا و معایب

***مدل مورد بحث در این قسمت ثابت کرد می‌توان با تعریف تابع امتیاز مناسب و استفاده از ساختارهای تخاصمی به روز ناهنجاری را داده‌های دنیای واقعی شناسایی کرد. در این مدل هیچ نظارتی بر میزان تشابه داده ورودی و داده بازسازی وجود ندارد در حالی که انتظار می‌رود داده ورودی و داده بازسازی شده توسط شبکه مولد برای نمونه‌های هنجار یکسان باشد. در ادامه به بررسی این مشکل و روش ارائه شده برای حل آن پرداخته می‌شود.***

### 6-5-2- مدل ALICE

در حالت استاندارد شبکه GAN تنها نگاشت یک طرفه از فضای نهفته به فضای داده بدست می­آورد، یعنی فاقد مکانیسم معکوس (از فضای داده به فضای نهفته) است و این امر مانع می­شود که این شبکه ها قادر به استنباط باشند. توانایی محاسبه تابع توزیع متغیر نهفته شرطی ممکن است برای تفسیر داده­ها و برای برنامه­های پایین دستی (به عنوان مثال، طبقه­بندی متغیر نهفته) مهم باشد.

تلاش­های زیادی برای یادگیری همزمان یک مدل دو طرفه کارآمد برای تولید نمونه­هایی با کیفیت بالا برای هر دو فضای نهفته و داده صورت گرفته است. در میان این طرح­ها، یکی از طرح­ها که به موفقیت چشم­گیری دست یافته است، شبکه یادگیر استنباط خصمانه ALI است]11[. دراین مدل در یک چارچوب شبکه مولد متخاصم، شبکه تمایزگر می­آموزد تا تفاوت بین دو توزیع توام را تشخیص دهد.

با این که شبکه ALI یک رویکرد جالب و خلاقانه است، اما یک ایراد اساسی دارد؛ این که بازسازی­های صورت گرفته از داده­ها در بعضی موارد حتی به داده های اصلی شبیه هم نیستند. دلیل این امر این است که شبکه ALI تنها به دنبال مطابقت دو توزیع توامان است، اما همبستگی بین دو متغیر تصادفی شرطی در هر یک از این توابع مشخص و اعمال نمی­شود. در نتیجه حاصل، راه­حل­هایی می­شود که هدف ALI را برآورده سازند اما در بازسازی داده­های مشاهده شده با مشکل روبرو هستند. این شبکه هم­چنین مشکلاتی در کشف رابطه صحیح جفت­ها در زمان تغییر دامنه دارد.

#### 1-6-5-2- یادگیری تخاصمی با اندازه‌گیری اطلاعات

به یاد داریم که تابع هدف در شبکه ALI به صورت معادله 2-20 بود:

|  |  |
| --- | --- |
| (20-2) |  |

نقطه تعادل این معادله هنگامی است که  **باشد. ارتباط بین متغیرهای تصادفی توسط** ALI **محدود و مقید نشده است. در نتیجه، این امکان وجود دارد که توزیع همسان**  **برای یک کاربرد خاص نامطلوب باشد. در واقع بسیاری از کاربردها به ثبات چرخه و وجود یک نگاشت معنی­دار دو طرفه بین دامنه ها احتیاج دارند.**

**جهت مقابله با مشکل توزیع­های نامطلوب اما برابر، بر روی راه­حل­های شبکه** ALI **باید محدویتی بر روی توزیع های و اعمال شود. این کار با کنترل "عدم قطعیت" بین جفت متغیرهای تصادفی، یعنی با استفاده از آنتروپی­های شرطی انجام می­شود.**

#### 2-6-5-2- آنتروپی شرطی[[75]](#footnote-75)

**آنتروپی شرطی یک معیار نظریه اطلاعاتی است که عدم قطعیت متغیر تصادفی را هنگام مقید شدن بر روی با کمک توزیع توامان تعیین می­کند:**

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | (21-2) |  | |  |

**عدم قطعیت متغیر مقید بر روی متغیر با مرتبط است. در حقیقت، اگر**  **باشد در این صورت به طور قطعی به** Z **وابسته می­باشد. به کمک کنترل میزان عدم قطعیت**  *و***، می توان راه حل های** ALI **را در توزیع های توامانی که نگاشت آن ها منجر به نتایج بهتری می شود، محدود کرد. در نهایت با افزودن یک عامل تنظیم کننده آنتروپی شرطی، به تابع هدف زیر دست می یابیم:**

|  |  |
| --- | --- |
| **(2 -22)** |  |

وابسته به متغیرهای تصادفی توزیع های توامان است. در حالت ایده آل، پس از شناسایی تمام نقاط تعادل تابع هدف ALI، می­توان با محاسبه آنتروپی شرطی آن­ها، راه­حل مطلوب را انتخاب کنیم. با این حال، در عمل این راه غیرقابل استفاده است، زیرا ما از قبل به نقاط تعادل دسترسی نداریم. در ادامه یک راه­حل برای محاسبه آنتروپی شرطی ارائه می­شود.

#### 3-6-5-2- فرایند یادگیری

در نبود تابع توزیع احتمال صریح که برای محاسبه آنتروپی شرطی مورد نیاز است، می­توان حدود آنتروپی شرطی را با استفاده از معیار ثبات چرخه[[76]](#footnote-76) محدود کرد. در این­جا برای بازسازی به طریق زیر عمل می شود:

|  |  |
| --- | --- |
| **(2 -23)** |  |

به کمک روال تولید بالا، تلاش می شود تا با احتمال بالایی شبیه اصلی باشد. اثبات می­شود که به کمک این روال تولید ها، حد بالای آنتروپی شرطی می­باشد.

نکته حائز اهمیت این است که می­توان عامل تنظیم آنتروپی را به تابع هدف شبکه ALI، بدون اعمال تغییرات اضافی دیگری، در روال آموزش این شبکه اضافه کرد. بدین ترتیب تابع بهینه­سازی برای شبکه ALICE به­صورت 2-24 خواهد بود.

|  |  |
| --- | --- |
| **(2 -24)** |  |

ویژگی پایداری چرخش در مقالات پیش از نیز وجود داشته است این ویژگی در این مقالات به کمک نرم درجه[[77]](#footnote-77) یک و دو و داده­های­ واقعی مانند تصاویر محاسبه ­شده ­است. وجود تابع اتلاف بر اساس نرم درجه 2 مبتنی بر پیکسل، سبب می­شود که نمونه­های خروجی این شبکه­ها تصاویر تاری باشند. به همین علت در این شبکه از یک شبکه تمایزگر که اختلاف بین ها و های بازسازی­شده را اندازه­گیری می­کند، استفاده­ شده ­است.

#### 4-6-5-2- مزایا و معایب

همانطور که بررسی شد در این کار با استفاده از کدگذار تلاش شد تا شرط پایداری در شبکه‌های عصبی مولد برقرار شود به بیان دیگر اگر تصویر ورودی را به کدگذار بدهیم و نقطه متناظر در فضای نهفته را بدست آوریم و سپس آن را به عنوان ورودی به شبکه مولد بدهیم انتظار داریم نتیجه نهایی شبیه به تصویر اولیه باشد. علی‌رغم عملکرد مناسب این مدل هنوز توزیع‌های توامی وجود دارد که از آن‌ها استفاده نشده است و همین امر سبب می‌شود تا از تمامی اطلاعات موجود استفاده نشود.

## 6-2- جمع‌بندی

در این فصل ابتدا به دسته‌بندی روش‌های مختلف تشخیص ناهنجاری پرداختیم، در خلال همین دسته‌بندی ‌ها برخی مدل‌های به نسبت قدیمی‌تر و سنتی بررسی شدند. در ادامه اهمیت جایگاه شبکه‌های عصبی تخاصمی روشن شد. در گام بعدی معیار‌های ارزیابی مدل‌های تشخیص ناهنجاری معرفی شده‌اند. در ادامه پس از بررسی مدل پایه شبکه عصبی تخاصمی زنجیره کارهایی که روی شبکه‌هایی عصبی تخاصمی به منظور بهبود صورت گرفته است بررسی شده است. در ادامه مدل AnoGan شرح داده شد و با توجه به مشکل آن در نگاشت معکوس از فضای داده ورودی به فضای نهفته مدل f-AnoGan که در ادامه کار قبلی است بررسی شد. با توجه به ضعف‌های موجود در ساختار f-AnoGan مقاله مکمل این مدل ALI مرور شد. . در گام بعدی مدل EGBAD که جزو اولین کار‌ها در زمینه تشخیص ناهنجاری که با الهام از مدل ALI خلق شده است مرور می‌شود. در مرحله بعدی با توجه تضمین نشدن شرط سازگاری حلقه در ALI مقاله آلیس بررسی شد.

# فصل سوم روش پیشنهادی

در فصول قبل به بررسی روش­های تشخیص ناهنجاری با رویکردهای مختلف پرداختیم. همان­طور که پیش­تر ذکر شد، با پیشرفت روزافزون زیرساخت­های محاسباتی و افزایش توان پردازشی، علاقه و توجه محققان حوزه هوش مصنوعی به سمت شبکه­های عصبی جلب شد. در میان این انواع شبکه­های عصبی ارائه ­شده در چند سال اخیر، شبکه های مولد تخاصمی به نتایج قابل توجه و درخشانی در کاربرد­های مختلف دست­ یافته­اند. علی­رغم نتایج قابل دفاع این نوع شبکه­ها در زمینه­های پردازش تصویر]10[، پردازش گفتار و پردازش متن]33[ در حوزه تشخیص ناهنجاری آن طور که شایسته است بدان توجه نشده. در زمینه شناسایی نمونه‌های ناهنجار در دادگان دنیای واقعی به ندرت می‌توان الگوریتمی یافت که بر مبنای شبکه‌های مولد تخاصمی طراحی شده باشد؛ در حقیقت بیشتر الگوریتم‌های تخاصمی برای کاردبر‌های دیگر طراحی شده است و صرفا همان ساختار در فضای جدید تشخیص ناهنجاری مورد استفاده قرار گرفته است و با این حال همین مدل‌های عام منظوره توانسته به نتایج نسبتا معقولی دست یابد]29[.

در این بخش روشی مبتنی بر شبکه‌های مولد تخاصمی که به صورت خاص با هدف تشخیص ناهنجاری پیشنهاد شده است. در طراحی این روش تمرکز اصلی بر روی ارائه روشی است که بتواند در کاربردهای دنیای واقعی نظیر تصاویر پزشکی مورد استفاده قرار بگیرد. مانند بسیاری از الگوریتم‌های مبتنی بر یادگیری، در این‌ جا دو مرحله اصلی آموزش و آزمایش وجود دارد. در قسمت آموزش همانند دیگر چهارچوب‌های تخاصمی به نوبت بخش مولد و بخش تمایزگر را آموزش می‌دهیم تا هر دو بخش در عین تناسب به نوبت به‌روزرسانی شود. همچنین یک مرحله پیش‌پردازش شامل نرمال‌سازی تصاویر به منظور افزایش دقت مدل نهایی انجام شده است. در همین مرحله نمونه‌ها ناهنجار را از تصاویر آموزشی حذف می‌کنیم و فقط از آن‌ها در مرحله آزمایش برای ارزیابی مدل پیشنهادی استفاده می‌کنیم. به بیان دیگر مدل تنها توزیع داده‌های عادی را می‌آموزد؛ روند آموزش مدل به حدی قدرتمند است که می‌تواند به خوبی فضای داده‌های ناهنجار را از داده‌های عادی تبیین کند.

در ادامه و در قسمت تشخیص ناهنجاری، یک ورودی بدون برچسب به ساختار شبکه وارد می‌شود و به کمک اختلاف بازسازی ارائه شده توسط شبکه برای آن ورودی در هر دو فضای داده و فضای نهان، امتیاز ناهنجاری برای هر ورودی محاسبه می‌شود. با توجه به این نکته که شبکه بر روی دادگان نرمال آموزش داده می‌شود انتظار می‌رود که برای داده‌های ناهنجار بازسازی ضعیف‌تری داشته باشد و بدین ترتیب این اختلاف بیشتر شود و در نهایت این داده‌ها امتیاز ناهنجار بیشتری بگیرند. بدین ترتیب با انتخاب یک حدآستانه[[78]](#footnote-78) و یا انتخاب یک نسبت معین از میان داده‌های با بیشترین امتیاز، داده‌های که ناهنجار هستند شناسایی می‌شوند.

در قسمت‌های بعد جزئیات دقیق‌تر روش پایه و همچنین جزئیات هر قسمت از الگوریتم پیشنهادی مورد بررسی قرار خواهد گرفت.

## 1-3- مدل ALAD

در این بخش، یک روش تشخیص ناهنجاری مبتنی بر شبکه مولد متخاصم را بررسی می­کنیم که در زمان آزمون بسیار کارآمد است. در این روش به طور هم­زمان یک شبکه رمزگذار را در حین آموزش فرا می­گیرد و بدین ترتیب استنتاج سریع­تر و کارآمدتر را در زمان آزمون امکان­پذیر می­کند. علاوه بر این در شبکه معرفی­شده، تکنیک­هایی که اخیرا برای بهبود بیشتر شبکه رمزگذار و تثبیت آموزش شبکه مولد متخاصم ترکیب­شده و نشان­ داده­ شده که این تکنیک­ها عملکرد و کارایی را در کاربرد تشخیص ناهنجاری بهبود می­بخشند. آزمایشات روی طیف وسیعی از داده­های جدولی و تصویری، کارایی و اثربخشی این رویکرد را در عمل نشان می­دهد[29].

شبکه­های GAN استاندارد از نمونه­گیری کارآمد پشتیبانی می­کنند و روش­های مختلفی وجود دارد که می­تواند آن­ها را برای تشخیص ناهنجاری تطبیق دهد. به عنوان مثال، برای یک نقطه داده ، می­توان از نمونه‌گیری استفاده کرد تا احتمال ناهنجار بودن را تخمین زند. تخمین دقیق احتمال به تعداد زیادی نمونه نیاز دارد و در نتیجه محاسبه احتمال، بار محاسباتی سنگینی دارد.

روش دیگر معکوس کردن[[79]](#footnote-79) شبکه مولد برای یافتن متغیرهای نهفته است که به معنای به حداقل رساندن خطای بازسازی با تابع هدف گرادیان نزولی تصادفی می باشد. این روش هم­چنین از نظر محاسباتی بسیار پرهزینه است زیرا هر محاسبه گرادیان نیاز به یک پس انتشار از طریق شبکه مولد دارد.

به واسطه بهره­وری محاسباتی بالا و قابلیت مدل­سازی داده­های ابعاد بالا، از شبکه­های مولد متخاصمی به همراه یک شبکه رمزگذار (که نمونه­ها را از فضای داده به فضای نهفته نگاشت می­کند) استفاده می­شود. نمایش نهفته هر نمونه از فضای داده در چنین مدل­هایی صرفاً با عبور از شبکه رمزگذار انجام می­شود. هم­چنین این مدل پیشرفت­های اخیر که برای بهبود شبکه رمزگذار صورت گرفته مانند افزودن یک شبکه تمایزگر برای بهبود سازگاری چرخه را شامل می­شود.

شبکه ALI توزیع توامان داده­ها را به همراه یک شبکه رمزگذار مدل می­کند. این مدل یک شبکه تمایزگر دارد که را به عنوان ورودی می­گیرد و بررسی می­کند که این جفت ورودی از کدام منبع – شبکه مولد و یا شبکه رمزگذار – تولید شده است.

|  |  |
| --- | --- |
| **(3 -1)** |  |

با این­که به لحاظ نظری توزیع توامان به یک نقطه میل می­کند، اما در عمل اغلب نتیجه یکسان نیست و لزوما به یک نقطه همگرا نمی­شوند و این پدیده سبب نقض پایداری چرخه می­شود. نبود پایداری چرخه به این معناست که باشد. این مشکل برای روش های تشخیص ناهنجاری مبتنی بر بازسازی چالش­های جدی ایجاد می­کند. برای حل این مشکل، چارچوب ALICE پیشنهاد می­کند که آنتروپی شرطی را به صورت زیر به روش تخاصمی برای سازگاری چرخه تقریب بزنیم.

|  |  |
| --- | --- |
| **(3 -2)** |  |

در این تعریفبه معنای توزیع توامان می­باشد.این مسئله شامل یکپارچه­سازی آنتروپی شرطی در شبکه رمزگذار و شبکه مولد است:

|  |  |
| --- | --- |
| **(3 -3)** |  |

که افزودن این عامل به مسئله معادل افزودن یک شبکه تمایزگر جدید به مسئله می­باشد. با افزودن این عامل، مسئله بهینه­سازی به صورت معادله 3-4 خواهد بود:

|  |  |
| --- | --- |
| **(3 -4)** |  |

### 1-1-3- تثبیت آموزش GAN بر پایه ALICE

برای تثبیت آموزش در مدل پایه ALICE، توزیع­های شرطی را با اضافه­کردن یک قید آنتروپی شرطی دیگر تنظیم می­کنیم و سپس عملیات نرمال­سازی طیفی را انجام می­دهیم.

توضیح دقیق­تر این­که، فضای نهفته شرطیرا با یک شبکه تمایزگر مخالف دیگر با نقطه تعادل مشترک تنظیم می­کنیم.

|  |  |
| --- | --- |
| **(3 -5)** |  |

با کنار هم قرار دادن تمامی این اجزا، شبکه ALAD تلاش می­کند تا نقطه تعادل این مسئله را آموزش ببیند.

|  |  |
| --- | --- |
| **(3 -6)** |  |

در نهایت شماتیک کلی شبکه طراحی­شده به صورت شکل 3-1 خواهد بود.

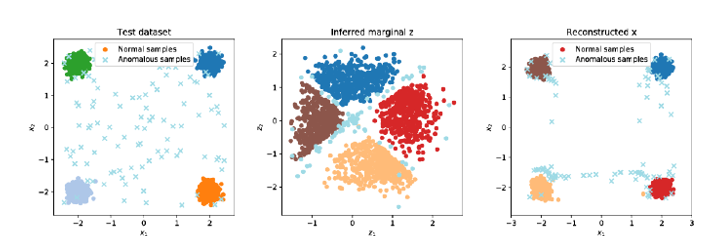


شکل 3-1: شمای کلی شبکه­ ALAD

اضافه کردن مرحله نرمال­سازی طیفی با انگیزه یادشده مقاله ]34[ می­باشد. در این مقاله نشان داده­شده که با افزودن قیود لیپسچیتز[[80]](#footnote-80) به تمایزگر شبکه GAN، فاز آموزش تثبیت خواهد شد. در عمل نشان داده شده که با تنظیم مجدد پارامترهای وزن، بهبود بسیار خوبی روی عملکرد شبکه خواهیم داشت. بدین صورت که بزرگ­ترین مقادیر ویژه ماتریس وزن را در شبکه تمایزگر ثابت نگه داریم. این روش از نظر محاسباتی کارآمد است و هم­چنین آموزش را تثبیت می­کند. با آزمایش­های صورت­گرفته نشان داده شد که افزودن این قیود، نه تنها برای شبکه تمایزگر، بلکه برای شبکه رمزگذار نیز سودمند است. قابل توجه است که مدل ALICE شامل این مرحله نمی باشد.

### 2-1-3- تشخیص ناهنجاری

شبکه ALAD یک روش تشخیص ناهنجاری مبتنی بر بازسازی است و بدین صورت عمل می­کند که فاصله نمونه از بازسازی را توسط شبکه GAN ارزیابی می­کند. نمونه­های عادی باید به طور دقیق بازسازی شوند در حالی که نمونه­های ناهنجار احتمالاً به طور ضعیف­تری بازسازی می­شوند. نحوه تشخیص ناهنجاری در شکل 3-2 نشان شده است.



شکل 3-2: نمونه­ای از خروجی شبکه ALAD به همراه داده­های ناهنجار

در شکل 3-2 ضربدر‌ها نمونه‌های ناهنجار و دایره‌های رنگی نمونه‌های عادی هستند.

به منظور مدل کردن توزیع داده‌ها به طور موثر از شبکه‌های مولد تخاصمی استفاده می‌شود. تابع مولد برای یادگیری توزیع داده­های عادی استفاده می­شود، به طوری که می­باشد. هم­چنین باید توزیع حاشیه­ای داده­ها را بیاموزیم تا بازنمایی­های نهفته منجر به بازسازی صحیح نمونه­های عادی شود. دو عنصر پایداری چرخه شرطی متقارن در این مدل، به اطمینان از این امر کمک می­کند.

مؤلفه کلیدی دیگر ALAD نمره ناهنجاری است که فاصله بین نمونه­های اصلی و بازسازی آن­ها را اندازه­گیری می­کند. انتخاب اولیه­ای که به ذهن می­رسد، فاصله اقلیدسی بین نمونه­های اصلی و بازسازی آن­ها در فضای داده است. اما، این معیار ممکن است معیار مطمئنی برای اندازه­گیری تشابه نباشد. به عنوان مثال، این معیار در مورد تصاویر می­تواند بسیار پرخطا باشد؛ زیرا تصاویر با ویژگی­های تصویری مشابه الزاماً از نظر فاصله اقلیدسی نزدیک به یک­دیگر نیستند. معیار تعریف­شده در این روش از فاصله بین نمونه­ها در فضای ویژگی­های تمایزگر محاسبه می­شود، که توسط لایه قبل از لاجیت تعریف شده است. از این ویژگی­ها هم­چنین به عنوان کدهای CNN یاد می­شود. به­طور دقیق­تر می­توان گفت با آموزش یک مدل برای داده­های عادی و محاسبه*E* ، *G* ، *Dxz* ، *Dxx* و *Dzz* یک تابع نمره­دهی را بر اساس خطای بازسازی نرم1 مطابق معادله 4-9 تعریف می­شود. در این تعریف تابع فعال­ساز[[81]](#footnote-81)های لایه قبل از لاجیت و یا همان کد CNN می­باشد. این نوع تعریف به ما این اطمینان را می­دهد که نمونه به درستی کدگذاری و بازسازی­شده و در نتیجه از توزیع داده واقعی می­باشد.

|  |  |
| --- | --- |
| **(3 -7)** |  |

با این تعریف، نمونه­ها با بیش­تر به احتمال بالاتری داده ناهنجار خواهند بود. در ادامه در الگوریتم 3-1 روال محاسبه ارائه می­شود.

|  |
| --- |
| الگوریتم محاسبه امتیاز ناهنجاری مدل ALAD |
| ورودی  خروجی  انجام روال استنتاج   1. رمزگذاری نمونه 2. ) رمزگشایی نمونه  5. اتمام روال محاسبه نمره ناهنجاری |

الگوریتم 3-1: شبه کد الگوریتم ALAD

معیار استفاده شده در این­جا از ایده تطابق ویژگی­های از دست­رفته الهام گرفته شده است]35[. اما در این­جا به جای استفاده از ویژگی­های محاسبه شده درشبکه تمایزگر GAN استاندارد (که اختلاف را بین نمونه­های تولید شده و داده­های واقعی را محاسبه می­کند)، از ویژگی­های محاسبه­شده در شبکه تمایزگر استفاده می­شود. هم­چنین در این­جا به جای استفاده از این معیار در حین آموزش شبکه GAN، از این معیار در هنگام روال استنتاج بهره می­جوییم.

سوالی که در این­جا مطرح می­شود این است که : چرا نباید از خروجی تمایزگر به عنوان معیار فاصله استفاده کرد. پاسخ این سوال بدین صورت است که هدف از شبکه تمایزگر تمایز بین یک جفت نمونه واقعی و بازسازی آن می­باشد و شبکه رمزگذار و شبکه مولد داده­های واقعی و توزیع متغیر نهفته را کاملاً ضبط خواهند کرد. در این حالت قادر به تفکیک بین نمونه­های واقعی و نمونه­های بازسازی شده نخواهد بود و بدین ترتیب یک پیش بینی تصادفی را تولید می­کند که معیار ناهنجاری مناسبی نخواهد بود.

## 2-3- مدل RCGAN[[82]](#footnote-82)

تمرکز مقاله ]36[ بر ارائه ساختاری مبتنی بر شبکه‌های عصبی تخاصمی به منظور هر چه بهتر کردن تشخیص نمونه‌های ناهنجار به وسیله پوشش تمام فضای نهفته و فضای داده ورودی است. اساس این کار بر پایه تعریف تابع جریمه، بیان جدیدی از تابع هزینه و همچنین استفاده نوآورانه از تمایزگر است. عملکرد مناسب این مدل در خلال بررسی نتایج آن قابل مشاهده است.

### 1-2-3- شناسایی نمونه‌های تخاصمی از دیدگاه آماری

داده‌های هنجار مورد استفاده در مرحله آموزش به عنوان تابع توزیع احتمال با نام تعریف می‌شود. با توجه به این‌که در مرحله آموزش تنها به نمونه‌های تابع توزیع  دسترسی داریم این مدل نیز به عنوان آموزش بی‌نظارت دسته‌بندی می‌شود. هدف در این مدل آموزش تابع است، این تابع در واقع به هر نمونه یک امتیاز ناهنجاری اختصاص می‌دهد به گونه‌ای که برای نمونه‌های ناهنجار مقدار بیشتری اختصاص می‌دهد.

### 2-2-3- GAN

شبکه مولد تخاصمی توزیع داده ورودی را با نمونه گرفتن از توزیع فضای نهفته و با استفاده از تبدیل مدل می‌کند به بیان دیگر  *توزیع احتمال شرطی را تعریف می‌کند. توزیع مولد را می‌توان به صورت زیر تعریف کرد.*

|  |  |
| --- | --- |
| **(3 -8)** |  |

در چارچوب GAN تمایزگر وظیف دارد تا میان داده‌هایی که از توزیع می‌آیند و داده‌های مصنوعی که از توزیع نشئت می‌گیرد تمیز دهد. تمایزگر و مولد به هنگام تطابق () در حالت بهینه قرار دارند. کدگذار مدل ALI تلاش می‌کند تا توزیع توام خود را را با توزیع توام مولد تطابق دهد. تابع ا=هدف مدل ALI نیز با توجه به همین عبارات به صورت زیر تنظیم می‌شود.

|  |  |
| --- | --- |
| **(3 -9)** |  |

در معادله 3-9 بیانگر شبکه مولد است که از هر دو فضای نهفته () و فضای داده واقعی () ورودی می‌گیرد و خروجی آن احتمال تعلق **و**  **به توزیع**  است. همانطور که در فصل گذشته دیدیم به منظور ارضای شرط پایداری حلقه، به ساختار مدل اضافه می‌شود تا میان داده تولیدی شبکه مولد و داده واقعی شباهت ایجاد کند.

بیشتر مدل‌هایی که اخیرا به تشخیص ناهنجاری به وسیله شبکه‌های عصبی تخاصمی پرداخته‌اند مبتنی بر شبکه‌های عصبی دو طرفه هستند، اگرچه این مدل‌ها قادرند تا تصاویر هنجار را با امتیاز پایین ناهنجاری بازسازی کنند اما هیچ ضمانتی در اختصاص نمره بالای ناهنجاری به نمونه‌های ناهنجار وجود ندارد.

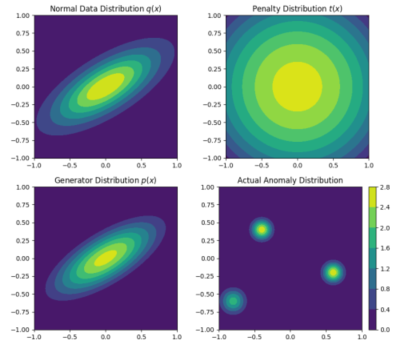
### 3-2-3- منظم‌سازی شبکه مولد و تمایزگر

برای رفع محدودیت‌های ذکر شده و قادر ساختن شبکه‌های عصبی تخاصمی برای تشخیص نمونه‌های ناهنجار از هنجار در این کار توزیع جریمه به گونه‌ای تعریف می‌شود که باشد، نمونه‌های تولیدی از این توزیع باید به عنوان داده تقلبی توسط تمایزگر شناخته شود. تابع هدف مدل پیشنهادی به صورت زیر است.

|  |  |
| --- | --- |
| **(3 -10)** |  |

تابع توزیع یک تابع تصادفی مانند توزیع گوسی انتخاب می‌شود. توزیع گوسی کاربرد‌های زیادی در زمینه‌ آموزش تخاصمی دارد. در انتهای آموزش شبکه‌های مولد و تمایزگر متمایل به توزیع داده‌های هنجار خواهد بود. در مدل پیشنهادی این مقاله نمونه که در آن  **نمونه ناهنجار است، نزدیک به توزیع داده هنجار خواهد، بنابراین بازسازی با خود فاصله خواهد داشت. این فاصله سبب می‌شود تا تشخیص نمونه ناهنجار آسان شود. همانطور که در شکل 3-3 مشخص است، نمونه‌های ناهنجار به گونه‌ای در مدل هدایت می‌شوند که بازسازی آن‌ها به سمت داده هنجار صفر متمایل شود. چنین رویکردی سبب می‌شود تا میان داده‌های ناهنجار و بازسازی آن‌ها تفاوت زیادی حاصل شود و در نتیجه تشخیص نمونه‌های ناهنجار گارانتی شود.**

**فرض کنید دارای پشتیبانی کمتر از مقدار در یک مکعب واحد است به ازای بعد‌های مختلف است، بنابراین داخل این ابعاد بزرگ و خارج از آن‌ها کوچک است. در مقابل دارای توزیع یکنواخت داخل یک کره واحد است. با این تنظیمات هنگامی که بزرگ است**   **کوچک خواهد و هنگامی که بزرگ باشد کوچک خواهد بود و در این حالت پیش‌بینی‌های مدل بهبود خواهند یافت. مثال ساده دو بعدی موجود در شکل 3-3 را مشاهده کنید. در این شکل یک توزیع گوسی باریک است و تابع توزیع یکنواخت در است. توجه کنید از نمونه‌های تخاصمی مستقل است.**



شکل 3-3: نحوه­ی عملکرد توزیع *t(x)*

در شکل 3-3 در این شکل نشان داده شده است که الگوریتم ارائه شده سبب می‌شود تا نقاطی که در آن‌ها کوچک است پوشش داده شود. این تنظیم مستقل از ارتباط میان و توزیع نمونه‌های ناهنجار انجام می‌شود.

### 4-2-3- پایداری چرخه

به منظور ارضای شرط پایداری چرخه تمایزگر به معماری مورد نظر اضافه شده است. تابع هدف چرخه پایداری به صورت زیر است.

|  |  |
| --- | --- |
| **(3 -11)** |  |

در معادله 3-11 بازسازی داده ورودی  **است. تابع هدف کامل ارائه شده در این کار به به شکل زیر است.**

|  |  |
| --- | --- |
| **(3 -12)** |  |

**پس از آموزش مدل نوبت به محاسبه امتیاز ناهنجاری می‌رسد، در مدل پشنهادی این کار تابع امتیاز پیشنهادی مطابق معادله زیر است.**

|  |  |
| --- | --- |
| **(3 -13)** |  |

امتیاز ناهنجاری بیانگر میزان کیفیت بازسازی  **است. الگوریتم ارائه شده در این کار مدل را مجبور به تولید خطای بزرگ برای نمونه‌های ناهنجار می‌کند در حالی که تابع هدف چرخه پایداری مدل مجبور به تولید بازسازی مناسب برای نمونه‌های هنجار می‌کند. این اختلاف امتیاز میان نمونه‌های هنجار و ناهنجار معیار مناسبی برای تشخیص نمونه‌های ناهنجار است.**

## 3-3- مدل RCALAD[[83]](#footnote-83)

بخش فعلی به معرفی مدل پیشنهادی اختصاص داده شده است. روش مورد بحث به منظور تشخیص ناهنجاری به دسته روش‌های مبتنی بر بازسازی تعلق دارد و از نظر دسترسی برچسب داده‌ها همانند سایر مدل‌های مبتنی بر شبکه‌های عصبی تخاصمی بررسی شده جزو دسته الگوریتم‌های بدون نظارت به حساب می‌آید. در این روش شبکه مولد موجود در ساختار GAN نگاشت از فضای نهان به فضای داده ورودی را فرا می‌گیرد، به بیان دیگر در این قسمت از شبکه عصبی تخاصمی توزیع داده هنجار ورودی مدل می‌شود. برای یادگیری نگاشت معکوس از فضای داده ورودی به فضای نهان از ساختار کدگذار-کدگشا استفاده شده است.

با افزودن تمایزگر به ساختار ارائه شده شرط چرخه پایداری در هر دو فضای نهفته و فضای ورودی در مدل پیشنهادی ارضا می‌شود اما تمایزگر مورد استفاده در کارهای قبلی، تنها به توزیع‌های منفرد داده‌ها در هر دو فضای نهفته و داده ورودی توجه می‌کردند و عملا برخی از جریان اطلاعات موجود در شبکه که متعلق به توزیع توامان متغیرهای فضای داده ورودی و نگاشت متناسب آن در فضای نهفته است، بلا استفاده باقی می‌ماند.

قابل توجه است که این روال و اثر بکاگیری این نوع تمایزگر توامان یک مرتبه پیش از این ثابت شده است؛ در واقع برای آموزش به هنگام افزودن شبکه کدگذار به ساختار اولیه GAN در هنگام معرفی مدل ALI، دو راه پیشرو بود. یک راه افزودن یک شبکه تمایزگر در کنار تمایزگر اولیه موجود، برای تمیز بین متغیرهای فضای پنهان بود و یک راه، تقویت شبکه تمایزگر اولیه و آموزش این شبکه به نحویست که توزیع توامان در هردو فضای نهان و واقعی را فرا بگیرند و بتوانند داده­های آموزشی را از داده­های تولیدشده توسط این مدل تشخیص دهد.

در مدل­های پیشین، جریان اطلاعات شامل یک فرایند دو مرحله­ایست، به این ترتیب که ابتدا از روی داده اولیه در فضای واقعی یک نگاشت توسط کدگذار به فضای نهان انجام می­شود و سپس از روی همین داده یک نگاشت معکوس به عنوان بازسازی به فضای داده اولیه توسط شبکه مولد انجام می­شود. سپس بار دیگر همین بازسازی به کدگذار فرستاده شده و در واقع بازسازی متغیر در فضای نهان بدست می­آید. در این مدل­ها متغیرها در هر کدام از فضاها با بازسازی آن­ها به صورت جداگانه مورد بررسی قرار می­گرفتند و تفکیک­شده تمیز داده می­شدند و بدین ترتیب ارتباط موجود بین این دو فضا نادیده گرفته می­شد.

بر مبنای استفاده از همین اطلاعات از دست رفته و سابقه بکارگیری توزیع­های توامان در این زمینه، در این جا مدل RCALAD پیشنهاد شده­است. در این­ ساختار در کنار چهارچوب اولیه شبکه­های مولد تخاصمی، یک شبکه تمایزگر توامان افزوده شده، تا با بکارگیری بیشترین اطلاعات موجود، مدل به جهت بهتری هدایت شده و سازگاری چرخه تا دو مرحله بررسی شود؛ یعنی برای آموزش مدل از اطلاعات هر دوفضا به صورت توامان استفاده شود و در نهایت مدل آموزش بهتری ببیند.

یک پیش­فرض اشتباه نیز در کارهای پیشین وجود داشت؛ این که اگر آموزش و بازسازی برای داده­های هنجار به خوبی انجام بگیرد، برای داده­های ناهنجار باید خراب شود و از داده اولیه ورودی متفاوت باشد. در صورتی که این فرض سهل­انگارانه است و هیچ استلزامی برای این قضیه در هیچ یک از مدل­های پیشین ارائه نشده است. در مدل ارائه شده با افزودن نمونه­گیری از کل فضا، این استلزام برای بازسازی در فضای هنجار ایجاد و مدل را به سمت فضای بازسازی داده­های هنجار متمایل کردیم[[84]](#footnote-84). در بخش­های آتی به بررسی جزئیات دقیق­تر این مدل می­پردازیم.

نتایج آزمایش­ها بر روی هر دو نوع داده تصویر و جدولی بیانگر کارایی و اثربخشی روش پیشنهادی می­باشد و نمایانگر سازگاری نتایج تئوری و عملی بدست­آمده برای این مسئله می­باشد.

### 1-3-3- معماری شبکه

در این ساختار همانند کارهای پیشین با هدف افزایش کارایی محاسباتی، یک کدگذار توام با شبکه مولد در ساختار کلی شبکه عصبی تخاصمی آموزش داده می‌شود. نگاشت معکوس از فضای داده ورودی به فضای نهفته به سادگی با تعبیه کدگذار در معماری پیشنهادی محاسبه می‌شود. این کدگذار تنها از فضای داده ورودی نمونه می‌گیرد و به طور تقریبی بازنمایی متناسب با آن را در فضای نهفته را تولید می‌کند. در اینجا برای آموزش هم‌زمان هر دو شبکه مولد و کدگذار از یک شبکه تمایزگر توامان با نام *Dxz* استفاده شده است. این تمایزگر بررسی می‌کند که جفت متغیر ورودی متعلق به توزیع داده ورودی و نقطه متناظر با آن در فضای نهفته است و یا توسط شبکه مولد و نمونه‌گیری از فضای نهفته z تولید شده است.

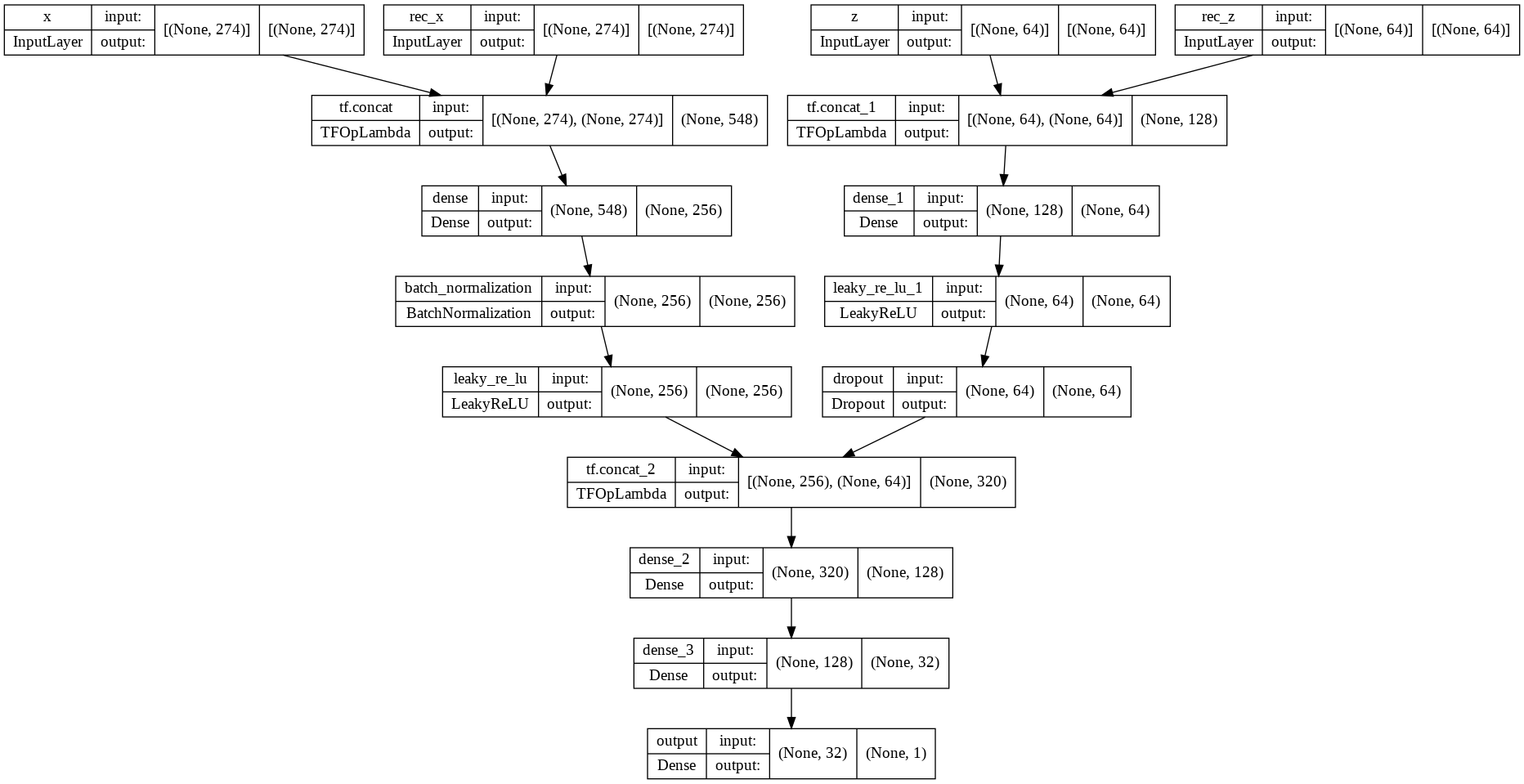
به منظور ارضای شرط پایداری حلقه از تمایزگر *Dxx* افزوده شده است، این تمایزگر به صورت توام نمونه داده ورودی و نمونه بازسازی شده متناظر آن را به عنوان ورودی اول و دوتایی به عنوان ورودی دوم دریافت می‌کند و برای تقویت شرط پایداری حلقه در فضای نهفته تمایزگر *Dzz* به این مجموعه اضافه شده است. این تمایزگر شرط پایداری حلقه را در خلال روند تولید نمونه بازسازی شده چک می‌کند. ورودی این تمایزگر نمونه ورودی شبکه مولد از فضای نهفته و خروجی کدگذار به عنوان ورودی اول و دوتایی است.

در این مدل یک شبکه تمایزگر جامع با نام *Dxxzz*  به ساختار فوق افزوده شده است. در این شبکه تلاش شده تا از تمامی اطلاعات موجود در مدل استفاده شود یعنی در کنار بررسی هر دو متغیر و بازسازی آن‌ها در همان فضا، توزیع توامان چهارتایی آن‌ها ( با بررسی جریان اطلاعات در دو گام ) در روند تشخیص نمونه ناهنجار به کار گرفته شود. این شبکه وظیفه تمییز بین نمونه‌های چهارتایی و را دارد به بیان دیگر تلاش می‌کند تا و بازسازی ارائه شده توسط شبکه و همینطور و بازسازی خروجی شبکه مولد توسط کدگذار تا حد امکان به یکدیگر نزدیک کند. هدف از تعبیه این تمایزگر در این ساختار حل مشکل چرخه پایداری توامان[[85]](#footnote-85) یا به اختصار JCC می‌باشد. تعریف دقیق مسئله JCC در ادامه بررسی می‌شود.

بیان ریاضی مسئله JCC بدین صورت می‌باشد. به ازای هر متغیر از فضای ورودی شبکه ابتدا کدگذار نگاشت معکوس به فضای نهفته را تخمین می‌زند که معادل می‌باشد. در مرحله بعد بازنمایی بدست آمده را به شبکه مولد وارد می‌کنیم تا بازسازی شبکه از متغیر ورودی تولید کند. سپس همین بازسازی را بار دیگر به شبکه کدگذار می‌دهیم تا بازسازی در فضای نهفته را نیز محاسبه شود یعنی . در این جریان، انتظار منطقی از هر شبکه مدعی بازسازی این است که دو متغیر و همچنین دو متغیر تا حد امکان کمترین اختلاف را داشته باشند. جریان اطلاعات در یک چرخه به صورت خلاصه در شکل 3-4 آمده است.

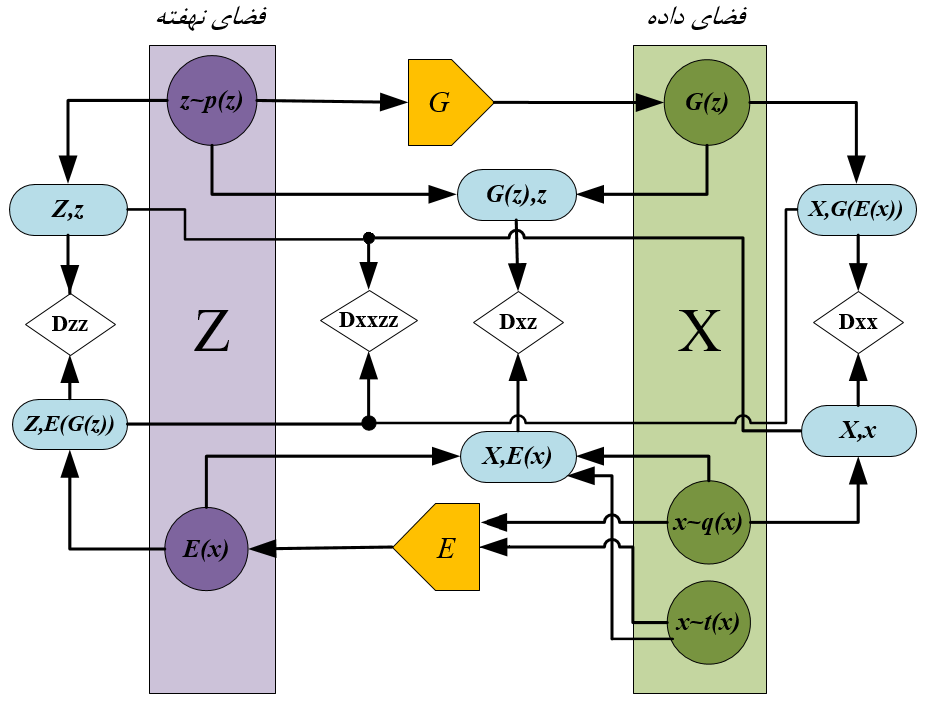
به منظور تقویت قدرت تشخیص تمایزگر اطلاعات حاصل از روند دگردیسی داده ورودی در تمامی مراحل چرخه، باید توسط تمایزگر قابل دسترس باشد. چرخه مورد نظر در این مسئله شامل سه گام متوالی است، در کارهای قبلی از خروجی‌‌های چرخه اطلاعات به طور کامل در شبکه استفاده نمی‌شد و این انتظار در جریان آموزش مدل­های مختلف ارائه شده با فرمولاسین مطرح­شده، مورد بررسی قرار نگرفته است. در حقیقت، مدل­های پیشین ارائه شده به بررسی مستقل این دو جفت متغیر در فضای جداگانه می­پرداخت و تمایزگر دید کاملی از جریان اطلاعات و وضعیت داده در هر دو فضا داده ورودی و نهفته به طور همزمان نداشت. قابل توجه است که این متغیرها پیش از این نیز محاسبه می­شد و این چرخه در مدل­های قبلی وجود داشت، اما مورد استفاده قرار نمی­گرفت. و از نظر بار محاسباتی، هزینه جدیدی به شبکه تحمیل نشده است.

برای حل این مسئله در این­جا شبکه تمایزگر *Dxxzz* پیشنهاد شده است. این شبکه هر چهار متغیر ( را به عنوان ورودی می­گیرد و تلاش می­کند تا از این مجموعه ورودی، ویژگی­های جدید و عمیق­تری ( به نسبت تمایزگرهای تک گامی *Dxx* و *Dzz* ) استخراج کند. این شبکه با در اختیار گرفتن خروجی کل چرخه داده، دید جامعی از وضعیت تمام قسمت‌های شبکه دارد و با استفاده از تمام این خروجی­ها به طور همزمان، به ویژگی­های ترکیبی قوی­تری برای تمیز نمونه‌های ناهنجار از نمونه داده‌های هنجار دست می­یابد. جزئیات معماری این تمایزگر در شکل 3-4 نمایش داده شده است.

این روند آموزش با همه مزیت‌هایی که نسبت به مدل‌های پیشین دارد، اما از یک مشکل اساسی چشم‌پوشی کرده است؛ مشکل استلزام بازسازی ضعیف. تعریف دقیق این مشکل بدین ترتیب می‌باشد: در تمامی روال‌های آموزش مدل‌های تشخیص ناهنجاری بازسازی دقیق نمونه‌های هنجار با کمترین خطا به مدل آموزش داده می‌شود، در مرحله آزمایش نمونه‌های ناهنجار و هنجار به مدل داده می‌شود، و همیشه فرض می­شود که برای نمونه‌های هنجار میزان اختلاف تصویر ورودی با تصویر بازسازی شده کم و برای نمونه‌های ناهنجار این اختلاف زیاد خواهد بود. در برخی موارد فرض فوق صحیح نیست و نمونه بازسازی شده داده ناهنجار، میزان اختلاف کمی با نمونه ورودی دارد و به همین سبب تشخیص آن به عنوان نمونه ناهنجار دشوار خواهد بود. در واقع در مدل‌های ارائه شده پیشین هیچ استلزامی برای بازسازی ضعیف نمونه ناهنجار وجود ندارد. علت وقوع این امر نگاشت تنک از فضای داده ورودی به فضای نهفته است. در حالت عادی آموزش فضای داده ورودی تنها به قسمت فضای کوچکی از نگاشت می‌شود، و در نتیجه نمونه‌گیری از فضای نهفته به منظور نگاشت دوباره به فضای داده ورودی تنک خواهد بود. در زمان مواجهه با نمونه‌های هنجار این امر مشکلی ایجاد نخواهد کر چرا که فضای متناسب زد برای نمونه‌های هنجار به خوبی مدل شده است ولی در نمونه‌های ناهنجار با توجه به اینکه مدل تا به حال چنین داده‌های را ندیده است ممکن است نمونه را به نقطه‌ای ناشناخته از فضای نهفته نگاشت کند و در نتیجه بازسازی نمونه ناهنجار نیز ممکن است به نقطه‌ای دورتر از فضای همیشگی بازسازی نگاشت شود. نگاشت به دست آمده از این فرایند هیچ ضمانتی برای ایجاد بازسازی مورد علاقه از نمونه ناهنجار ارائه نمی‌دهد.

شکل 3-4: معماری شبکه تمایزگر *Dxxzz*

بلوک به منظور پوشش حداکثری فضای نهفته در ساختاری کلی مدل تعبیه شده است. هدف از تعبیه این بلوک تولید نمونه‌های جدید در فضای داده ورودی و سپس نگاشت آن به فضای نهفته است. انتظار می‌رود در این روند فضای نهفته به شکل مناسب‌تری نسبت به کارهای قبلی پوشش داده شود. نتایج عملی نمایانگر صحت تئوری ارائه شده در این قسمت است. در نهایت شمای کلی مدل پیشنهادی RCALAD در شکل 3-5 قابل مشاهده است.



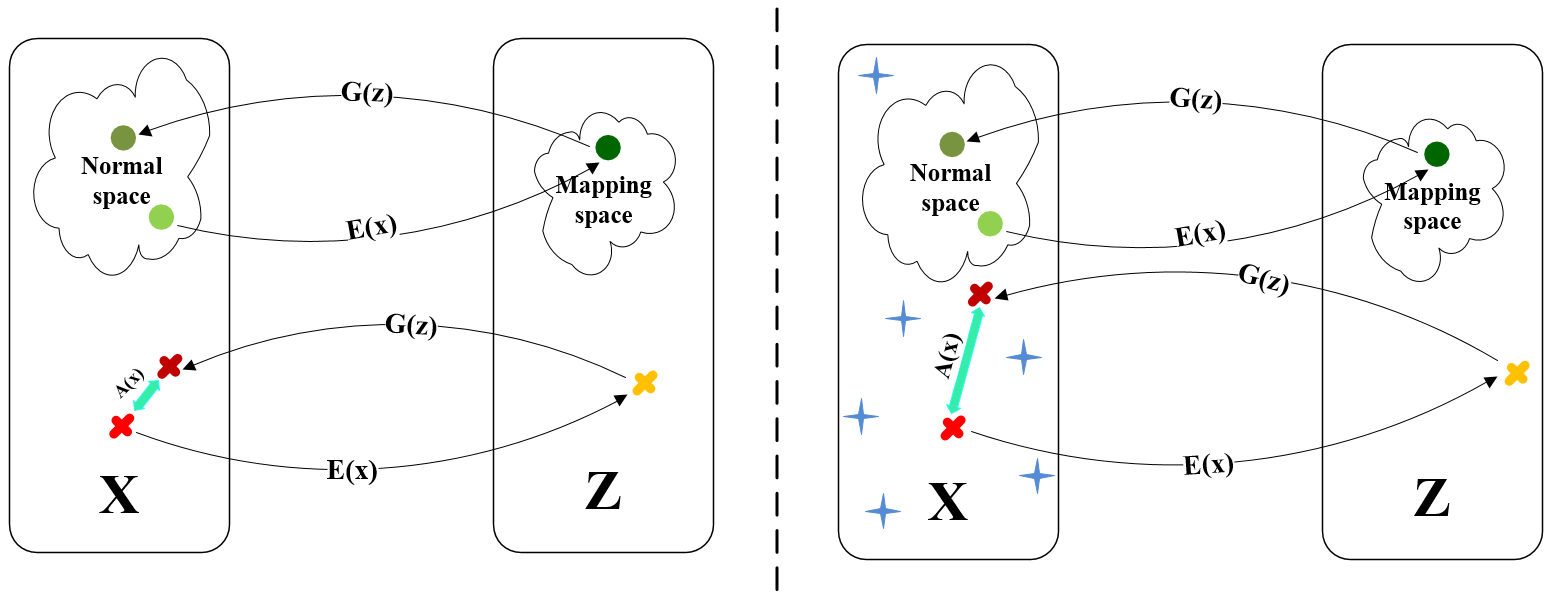
شکل 3-5: معماری RCALAD

در بخش 3-3-2 به توضیح دقیق­تر روال آموزش و بررسی جزئیات بلوک­های موجود در مدل خواهیم پرداخت.

### 2-3-3- روال آموزش

همانند سایر مدل‌های پیشین در روند آموزش مدل پیشنهادی از روال‌های آموزش تخاصمی استفاده می‌شود، بدیت ترتیب که به صورت متوالی بخش مولد و رمزگذار و پس از آن تمایزگر‌ها آموزش داده می‌شوند، یعنی به ترتیب با ثابت نگه داشتن وضعیت بخش مولد و رمزگذار، پارامترهای شبکه‌های تمایزگر را به‌روزرسانی می‌کنیم. سپس آموزش این بخش‌ها را متوقف کرده و با توجه به خروجی بهبود یافته آن‌ها، پارامترهای بخش مولد و رمزگذار به روزرسانی می‌شود و این روال بارها و بارها تکرار شده تا مدل به کیفیت خروجی مطلوب دست یابد.

هدف از آموزش تمامی مدل‌های مبتنی بر بازسازی از جمله مدل RCALAD تولید بازسازی مناسب برای داده‌های هنجار و بازسازی ضعیف برای نمونه داده‌های ناهنجار است. در اینجا برای ضمانت ایجاد بازسازی ضعیف برای داده ناهنجار، تلاش شده است تا تمامی فضای داده ورودی را به کمک نویز پوشش دهیم و مولد شبکه را به سمت بازسازی هر بیشتر نزدیک به توزیع داده هنجار متمایل کنیم. در شکل 3-3 چگونگی عملکرد این قسمت از مدل پیشنهادی و نحوه تاثیر آن در فرایند آموزش به تصویر کشیده شده است.



شکل 3-6: تاثیر حضور توزیع t(x) در روند آموزش مدل

در شکل 3-6 x بیانگر فضای داده ورودی و z بیانگر فضای داده ورودی است. نمونه‌ها توسط مولد از فضای داده ورودی به فضای نهفته نگاشت می‌شوند و وظیفه انجام نگاشت معکوس بر عهده کدگذار است. دایره‌های سبز رنگ نماد نمونه داده‌های هنجار و ضربدر‌های قرمز نماد نمونه‌های ناهنجار هستند. بعلاوه آبی رنگ نشانگر نمونه‌های تولید شده توسط توزیع هستند که در تنها مرحله آموزش مورد استفاده قرار گرفته‌اند. فلش فیروزه‌ای مقدار امتیاز ناهنجاری را نشان می‌دهد . همانطور که در شکل 3-4 مشاهده می‌شود در صورت عدم حضور *t(x)* ( در سمت چپ شکل ) در روند آموزش، امتیاز ناهنجاری برای نمونه­های غیرعادی کمتر از زمانی است که از این توزیع استفاده شده است، در واقع در تصویر سمت راست، توزیع *t(x)* مدل را به سمت بازسازی همه نمونه‌ها اعم از ناهنجار و هنجار به سمت توزیع داده‌‌های هنجار متمایل کرده است.

بیان ریاضی تابع هدف مدل پیشنهادی حاصل از جمع دو بخش کلی و مطابق معادله 3-14 می‌باشد.

|  |  |
| --- | --- |
| **(3 -14)** |  |

در ادامه به بررسی هدف و جزئیات ریاضی هر یک از این دو بخش خواهیم پرداخت.

اولین بخش از این تابع هدف می‌باشد. با هدف حل مسئله استلزام بازسازی (که در بخش قبلی به تعریف دقیق آن پرداختیم) و توانمندسازی شبکه پیشنهادی برای تمایز هر چه بهتر بین داده‌های هنجار و ناهنجار از توزیع جریمه استفاده شده است. ابعاد داده‌های خروجی این توزیع برابر با ابعاد داده ورودی می‌باشد و در حالتی که هیچ اطلاعات اضافه ای از داده نداشته باشیم، با توجه به این که داده­ها در مرحله پیش­پردازش نرمال شده اند، از توزیع گوسی نرمال برای پوشش کلی­تر فضا استفاده می­کنیم. البته اگر اطلاعات اضافه ای به مدل از توزیع داده­های ناهنجار داده شود، می­توان با بکارگیری به جای توزیع اعمال کرد. در حالت کلی بخش اول تابع هدف این مسئله طبق معادله 3-15 تعریف می­شود.

|  |  |
| --- | --- |
| **(3 -15)** |  |

در این معادله، داده‌های هنجار مورد استفاده در مرحله آموزش با تابع توزیع احتمال تعریف می‌شود و به عنوان تابع توزیع ورودی برای شبکه مولد در نظر گرفته شده است. در این معادله از تابع توزیع جریمه برای پوشش بهتر فضای داده ورودی و حل مشکل تنک بودن فضای نهفته استفاده می­شود. در این معادله با داده­های خروجی از توزیع و بازسازی آن­ها به عنوان نمونه­های تخاصمی برخورد می­شود و بدین ترتیب با افزودن عبارت سوم یعنی به تابع هزینه کلی، تلاش می­شود تا تمامی فضای ورودی به زیرفضا متعلق به توزیع داده­های هنجار در فضای نهفته نگاشت شود و با این روش بازسازی­های ارائه شده توسط شبکه به سمت توزیع داده هنجار ورودی متمایل شود. توضیح بیشتر این که ابتدا داده تولیدی از توزیع به شبکه کدگذار وارد می‌شود، در طی فرایند آموزش کدگذار می‌آموزد تمام فضای داده ورودی را به فضای متناسب توزیع داده هنجار در فضای نهفته نگاشت کند، در نتیجه این روند، توزیع داده ورودی شبکه مولد همواره از فضای متناسب با توزیع داده هنجار خواهد بود و خروجی حاصل نیز متعلق به توزیع متناسب با آن در فضای داده ورودی می­شود. از آن جایی که شبکه مولد نگاشت از فضای نهفته متعلق به داده هنجار به فضای داده ورودی متناسب را یاد گرفته است، تمامی فضای ورودی فارغ از هنجار یا ناهنجار بودن به فضای داده هنجار نگاشت می­شود. پس به ازای داده­های ناهنجار اختلاف بازسازی ارائه شده توسط شبکه بیشتر از داده­های هنجار خواهد بود.

**برای اثبات نظری تمایل شبکه‌های مولد و تمایزگر به سمت داده‌های هنجار ابتدا تمایزگر و مولد بهینه را آموزش می‌دهیم. توزیع توام کدگذار روی داده‌های هنجار به صورت**  و توزیع توام کدگذار روی *داده*‌*های ناشی از توزیع جریمه به صورت و است*. نقطه بهینه برای تمایزگر *Dzz* که از معادله 3-15 بدست می­آید مطابق معادله 3-16 می­باشد.

|  |  |
| --- | --- |
| **(3 - 16)** |  |

در معادله 3-16 هر دو توزیع داده ورودی و توزیع داده جریمه در نظر گرفته است. از معادله فوق می‌توان نتیجه گرفت بر خلاق GAN استاندارد که تنها روی نمونه‌های عادی آموزش می‌بیند تمایزگر مدل ارائه شده در این کار احتمال بیشتری به نمونه‌های عادی اختصاص می‌دهد، و با توجه به این که به نمونه‌های ناهنجار با کوچکتر اختصاص می‌یابد، خروجی تمایزگر بهینه برای داده­های ناهنجار کم می­شود. نتایج عملی ارائه شده در فصل چهارم گزاره‌های ارائه شده در این قسمت را پشتیبانی می‌کنند.

بخش دوم تابع هدف مورد استفاده در تابع هزینه این مدل تلاش می­کند تا شباهت میان داده تولیدی و بازسازی آن توسط شبکه مولد برای داده­های هنجار را تضمین کند. در واقع این تابع هدف شرط پایداری چرخه را هم به صورت تک مرحله­ای و هم به صورت دو مرحله ای یعنی چرخه کامل ارضا می‌کند. این بخش مطابق معادله 3-17 فرمول­بندی می­شود.

|  |  |
| --- | --- |
| **(3 -17)** |  |

در معادله 3-17 که متعلق به بخش چرخه پایداری تابع هدف می­باشد، سطر اول مربوط به تمایزگر *Dxx* می­باشد. این تمایزگر تلاش می­کند که شرط چرخه پایداری را به صورت تک گامی با شروع از فضای داده در این مدل ایجاد کند. سطر دوم مربوط به تمایزگر *Dzz* است که با هدف ایجاد چرخه پایداری تک گامی با شروع از فضای نهفته به مدل اضافه شده است. و در نهایت دو عبارت آخر مربوط به تمایزگر جامع*Dxxzz*  است. این تمایزگر در دو گام جریان اطلاعات را دنبال می­کند و خروجی تمامی مراحل را بررسی می­کند و چرخه پایدار را برای همه مراحل نگاشت داده در مدل ایجاد می­نماید. همان­طور که در بخش قبل نیز اشاره شد، هدف از تعبیه این تمایزگر در این ساختار، حل مشکل چرخه پایداری توامان[[86]](#footnote-86) یا JCC می‌باشد که تعریف دقیق این مسئله JCC در بخش 3-3-1 اشاره شد.

### 3-3-3- تشخیص ناهنجاری

همانطور که گفته شد مدل پیشنهادی در این پروژه به منظور تشخیص ناهنجاری بر اساس بازسازی داده ورودی است. داده هنجار به صورت دقیق بازسازی می‌شود در حالی که بازسازی نمونه ناهنجار ضعیف خواهد بود. پس از بازسازی نمونه‌ها، عنصر کلیدی در تشخیص ناهنجاری تعریف امتیاز ناهنجاری با هدف محاسبه فاصله میان نمونه ورودی و خروجی بازسازی شده توسط شبکه است. اولین انتخاب در زمینه محاسبه میزان فاصله این دو داده فاصله اقلیدسی است ولی در فضای داده این معیار ممکن است به اندازه کافی قابل اتکا نباشد]29[. به عنوان مثال در زمینه تشخیص ناهنجاری در تصاویر ممکن است علی‌رغم ویژگی‌های بصری مشابه فاصله اقلیدسی زیادی داشته باشند.

در این کار به جای محاسبه فاصله میان نمونه‌ها در فضای داده ورودی، از فضای ویژگی موجود در تمایزگر استفاده می‌شود. به این منظور خروجی توابع فعالیت[[87]](#footnote-87) لایه یکی مانده به آخر به عنوان ویژگی استفاده می‌شوند. امتیاز ناهنجاری مورد استفاده به صورت زیر و با استفاده از خطای بازسازی نرم یک و مطابق معادله 3-18 تعریف می‌شود.

|  |  |
| --- | --- |
| **(3 -18)** |  |

*در معادله 3-18 بیانگرتابع فعالیت لایه یکی مانده به آخر در ساختار تمایزگر است. میزان اطمینان تمایزگر از کیفیت روند کدگذاری و بازسازی داده توسط مولد است که اگر خوب انجام شده باشد در واقع نمونه متعلق به توزیع داده هنجار است که مدل روی آن آموزش دیده است. بنابر مطالب گفته شده هر چه مقدار این معیار بیشتر باشد احتمال ناهنجاری بودن آن بیشتر است. الگوریتم محاسبه امتیاز ناهنجاری در الگوریتم 3-2 قابل مشاهده است. عملکرد مناسب این معیار در مقایسه با سایر معیارهای تشخیص ناهنجاری در فصل آینده نمایش داده شده است.*

|  |
| --- |
| Algorithm 2 Regularized Comprehensive Adverarially Learned Anomaly Detection |
| Input where is the feature layer of  Output  1: procedure INFERENCE  2: Encode samples, Construct latent Embedding  3: Reconstruct samples  4: Reconstruct latent Embedding  5:  6:  7: return  8: end procedure |

الگوریتم 3-2: روند محاسبه­ی امتیاز ناهنجاری

معیار پیشنهادی در این قسمت بر اساس روش تطبیق ویژگی[[88]](#footnote-88) و یا به اختصار FM، پایه‌گذاری شده است ]35[ ، در ساختار GAN استاندارد برای تطبیق ویژگی از خروجی شبکه مولد استفاده شده است و در مقاله]29[ اگرچه از خروجی تمایزگر استفاده کرده است اما لاجیت‌های تولیدی توسط این شبکه از نظر اطلاعات نسبت به تمایزگر فقیرتر هستند.

در مدل ALAD تنها از خروجی تمایزگر برای شناسایی نمونه‌های ناهنجار استفاده شد و بنابر نتایج به‌دست آمده خروجی این تمایزگر فاقد اطلاعات مفید است و نمی‌توان بر اساس آن نمونه­های ناهنجار را تشخیص داد اما در این کار از جمع خروجی تمایزگر‌های ، و به عنوان معیار تشخیص ناهنجاری استفاده شد. تمام تمایزگر‌های موجود در مدل پیشنهادی تنها روی نمونه‌های هنجار آموزش دیده‌اند پس انتظار می‌رود تصویر بازسازی شده نمونه ناهنجار و همچنین بازنمایی آن در فضای نهفته که توسط کدگذار تولید می‌شود ضعیف باشد، علاوه بر این‌ها خروجی بر اساس ویژگی‌های غنی‌تری تولید می‌شود و طبیعی‌ست که از اهمیت بالایی برخوردار باشد. حال مسئله قابل بررسی این موضوع می‌باشد که آیا معیار حاوی اطلاعات مفید کافی برای تشخیص داده‌های هنجار از ناهنجار می‌باشد یا خیر. پاسخ به این سوال در حالت کلی بله می‌باشد زیرا این تمایزگرها در طی فرایند آموزش یاد می‌گیرند که به اختلاف میان دوتایی و و همچنین دوتایی و توجه کنند یعنی هر چه از و یا از فاصله بگیرد، تشخیص آن برای تمایزگرها ساده­تر می­شود. حال با افزودن توزیع به این مجموعه و تلاش برای متمایل کردن تمامی بازسازی به سمت توزیع داده­های هنجار، اختلاف بازسازی برای داده­های ناهنجار زیادتر شده و عملاً خروجی تمایزگرها یک معیار قابل اتکا برای تشخیص ناهنجاری می­شود. بیان ریاضی این معیار در معادله 3-19 آورده شده است.

|  |  |
| --- | --- |
| **(3 -19)** |  |

در فصل آینده این معیار با سایر معیار‌های تشخیص ناهنجاری مقایسه شده و در عمل کارایی این امتیاز نشان داده می­شود.

### 4-3-3- جمع‌بندی

در این فصل ابتدا مدل‌های پایه مورد بررسی قرار گرفتند. مدل ALAD را می‌توان از اولین مدل‌ها در زمینه تشخیص ناهنجاری به وسیله شبکه‌های عصبی تخاصمی دانست. این مدل به منظور تقویت روند آموزش شبکه و چرخه پایداری تمایزگر را به ساختار تخاصمی پیشین اضافه کرد و با این کار بهبود قابل توجهی در افزایش دقت تشخیص نمونه‌های ناهنجار ایجاد کرد. در ادامه مدل RCGAN بررسی شد. تلاش این مدل بر پوشش هر چه بهتر فضایی ورودی و حل مشکل استلزام بازسازی ضعیف برای نمونه‌های ناهنجار بود. در گام بعدی با الهام از کارهای قبلی چارچوب جدید پیشنهادی با هدف تشخیص داده ناهنار معرفی شد. در مدل پیشنهادی با اضافه کردن تمایزگر از تمامی اطلاعات موجود در شبکه به طور توام استفاده شد و روند آموزش و چرخه پایداری به بیشینه دقت در بین سایر مدل‌های مبتنی بر شبکه‌های مولد تخاصمی رسید. به منظور هدایت کردن مدل به سمت تولید بازسازی ضعیف برای نمونه‌های ناهنجار با الهام از مدل RCGAN توزیع جریمه معرفی و به ساختار معرفی شده اضافه شد. در گام نهایی دو امتیاز ناهنجاری جدید با نام‌های و معرفی شدند، همانطور که مشاهده شد معیار اول مبتنی بر خروجی تمایزگرهای موجود بر شبکه تعریف شد بود و اساس کار معیار دوم بر استفاده از تطبیق ویژگی در لایه‌های تمایزگر بنا نهاده شده بود. در فصل آینده کارایی مدل پیشنهادی روی دادگان مختلف بررسی خواهد شد.

# 

# فصل چهارم آزمایش­ها و نتایج

به منظور بررسی و ارزیابی کارایی الگوریتم پیشنهادی در تشخیص ناهنجاری در این فصل نتایج عملکرد آن طی چندین روال آزمایشی ارائه می‌شود. در ابتدا به معرفی مجموعه داده‌های آزمایشی و تنظیمات متناسب با هر یک از آن‌ها برای مدل پیشنهادی می‌پردازیم. سپس دیگر الگوریتم‌های تشخیص ناهنجاری مطرح پایه را معرفی کوتاهی خواهیم کرد، در گام بعدی به بررسی نتایج بر روی مجموعه داده‌های جدولی[[89]](#footnote-89) و تصویری ارائه شده می‌پردازیم و سپس نتایج به‌دست آمده بررسی، مقایسه و تحلیل می‌شود. درنهایت به بحث بیشتر و موشکافی نحوه عملکرد هر یک از امتیاز­های معرفی شده در بخش 3-3-3 در مجموعه داده­های مختلف اشاره می‌شود.

## 1-4- دادگان و پیش‌پردازش

برای سنجش عملکرد مدل پیشنهادی و بررسی کارایی آن ار جنبه‌های مختلف از مجموعه داده‌هایی با ویژگی متفاوت استفاده می‌شود. در این قسمت مشخصات و ویژگی‌های این مجموعه داده‌ها معرفی خواهد شد.

### 1-1-4- مجموعه داده KDDCup99

مجموعه دادگان KDDCUP یک دادگان جدولی در ارتباط با نفوذ به شبکه‌های کامپیوتری است. این دادگان شامل 494021 نمونه با 34 ویژگی اسمی[[90]](#footnote-90) و هفت ویژگی پیوسته[[91]](#footnote-91) است. در مرحله پیش‌پردازش ویژگی‌های اسمی به روش بازنمایی one-hot کدگذاری می‌شوند و نمونه‌های نهایی هر کدام 121 بعد خواهند داشت. داده‌های با برچسب غیرنفوذ با توجه به اینکه حدود بیست درصد مجموعه داده را شامل می‌شود و در اقلیت است به عنوان ناهنجاری در نظر گرفته می‌شود. در مرحله آزمون بیست درصد از داده‌ها با بیشترین امتیاز ناهنجاری به عنوان داده ناهنجار در نظر گرفته می‌شود. معیار‌های ارزیابی برای سنجش این مجموعه داده شامل صحت، بازیابی و F1-score است. توضیحات این معیارها در بخش 2-4 به تفصیل مورد بررسی قرار گرفته است.

### 2-1-4- مجموعه داده Arrhytthmia

دادگان جدولی آریتمی قلبی شامل 452 نمونه با 274 ویژگی است و هر داده می‌تواند به 16 کلاس مختلف دسته‌بندی شود. کوچکترین کلاس‌ها به ترتیب شامل 3،4،5،7،8،9،14 و 15 نمونه هستند و جمعا 15 درصد از نمونه‌های این دادگان را شامل می‌شوند و همین نمونه‌ها در واقع ناهنجاری هستند. سایر کلاس‌ها به عنوان داده هنجار در نظر گرفته می‌شوند. در اینجا نیز در مرحله آزمایش 15 درصد از دادگان با بیشترین امتیاز به عنوان داده‌های ناهنجار در نظر گرفته می‌شوند. معیار‌های ارزیابی برای سنجش این مجموعه داده شامل صحت، بازیابی و F1-score است.

### 3-1-4- مجموعه داده Thyroid

این دادگان مربوط به بیماری تیرویید و جدولی است و شامل 3772 نمونه در سه کلاس و شامل شش ویژگی پیوسته است. کلاس با برچسب hyperfunction که شامل 2.5 درصد از مجموعه داده است به عنوان داده ناهنجار دسته‌بندی می‌شود، بنابراین در مرحله آزمون 2.5 درصد از نمونه‌ها با امتیاز ناهنجاری بالا به عنوان داده ناهنجار تشخیص داده می‌شود. در این مجموعه داده 50% از نمونه­های موجود به صورت تصادفی به عنوان داده آموزشی انتخاب شده است. توجه شود که نمونه­های ناهنجار در تمامی مراحل آموزش مدل از داده­­های آموزشی حذف می­شود. معیار‌های ارزیابی برای سنجش این مجموعه داده همانند دیگر مجموعه داده­های جدولی شامل صحت، بازیابی و F1-score است.

### 4-1-4- مجموعه داده Musk

دادگان Musk دادگانی جدولی مربوط به دسته‌بندی شش کلاسی روی مشک مولکولی[[92]](#footnote-92) شامل 3062 نمونه با 166 ویژگی است. کلاس‌های موجود در دسته به نام 213 و 211 به عنوان داده ناهنجار در نظر گرفته می‌شوند و شامل 3.2 درصد دادگان است. . معیار‌های ارزیابی برای سنجش این مجموعه داده مانند بخش­های گذشته شامل صحت، بازیابی و F1-score است.

### 5-1-4- مجموعه داده CIFAR-10

این دادگان شامل 6000 تصویر 32\*32 در ده کلاس است. برای آزمایش مدل پیشنهادی روی این دادگان هر بار یک کلاس به عنوان داده هنجار در نظر گرفته می‌شود و نه کلاس دیگر به عنوان داده ناهنجار در نظر گرفته می‌شود. معیار مقایسه مدل پیشنهادی با سایر مدل‌ها در این مجموعه داده AUROC[[93]](#footnote-93) است. 80 درصد داده به عنوان داده آموزشی در نظر گرفته می‌شود و 20 درصد باقی به عنوان داده آزمون و 25 درصد نمونه‌های آزمون به عنوان داده اعتبارسنجی در نظر گرفته می‌شود. توجه شود نمونه‌های ناهنجار از داده آموزشی و اعتبارسنجی حذف می‌شود.

### 6-1-4- مجموعه داده SVHN

دادگان SVHN مربوط به دسته‌بندی اعداد بین صفر تا نه روی پلاک خانه‌هاست. این مجموعه داده شامل 600000 تصویر 32\*32 است. رویکرد آموزش، اعتبار سنجی و آزمون در این دادگان همانند دادگان CIFAR10 است.

## 2-4- تنظیمات مدل

در این قسمت به معرفی و بررسی جزئیات به کارگیری و تنظیمات معماری شبکه عصبی مدل پیشنهادی بر روی مجموعه داده‌های مختلف می‌پردازیم. تمامی نتایج گزارش شده در پایان­نامه با استفاده از چارچوب Tensorflow1 و به زبان پایتون تولید شده است. توان پردازشی مورد نیاز در این کار با استفاده از NVIDIA A100 تامین شده است. تنظیمات آزمون[[94]](#footnote-94) همانند مدل پایه ALAD می­باشد. جزئیات ساختاری و معماری مدل پیشنهادی در بخش 3-2 به تفضیل بررسی شده است. فراپارامتر[[95]](#footnote-95)ها برای بهینه ساز Adam از کتابخانه Tensorflow1 همانند [36] معادل و می­باشد. اندازه هر دسته[[96]](#footnote-96)­ در تمامی آزمایش­ها 32 در نظر گرفته شده است.

## 3-4- مدل‌های پایه

در این قسمت چارچوب پیشنهادی با تعداد زیادی از روش‌های تشخیص ناهنجاری مقایسه می‌شود، در ادامه هر کدام از این روش‌ها به طور مختصر شرح داده می‌شود.

### 1-3-4- روش OC-SVM[[97]](#footnote-97)

این روش یک مرز حول نمونه‌های هنجار یاد می‌گیرد و نمونه‌هایی که خارج از این مرز قرارگیرند به عنوان ناهنجاری در نظر گرفته می‌شوند. این مرز توسط روش ماشین بردار پشتیبان ایجاد می‌شود و هسته[[98]](#footnote-98) مورد استفاده در این روش RBF[[99]](#footnote-99) است. پارامتر برابر نسبت تعداد داده‌های ناهنجار به کل داده‌هاست و برابر 1/m قرار داده می‌شود، m برابر تعداد ویژگی‌های دادگان است.

### 2-3-4- روش IF[[100]](#footnote-100)

این روش از دسته روش‌های کلاسیک یادگیری ماشین است و به جای مدل کردن توزیع داده هنجار داده ناهنجار را از سایر نمونه‌ها جدا می‌کند. ابتدا در این روش ابتدا تعدادی ویژگی انتخاب می‌شود و یک مقدار تصادفی برای هر ویژگی انتخاب می‌شود تا بتوان داده‌ها را جدا کرد. در ادامه میانگین فاصله هر نمونه تا ریشه به عنوان امتیاز ناهنجاری در نظر گرفته می‌شود.

### 3-3-4- روش DSEBM[[101]](#footnote-101)

اساس کار این روش بر استفاده از انرژی لایه‌هایی که در خودگذارهای حذف نویز به کار برده می‌شوند بنا نهاده شده است. از خطای بازسازی و همچنین خود انرژی به عنوان امتیاز ناهنجاری در این مدل استفاده شده است. DSEBM-r بیانگر تشخیص ناهنجاری با خطای بازسازی و DSEBM-e بیانگر تشخیص ناهنجاری با امتیاز انرژی است.

### 4-3-4- روشDAGMM[[102]](#footnote-102)

این مدل بر اساس خودکدگذارهای مورد استفاده در تشخیص ناهنجاری طراحی شده است. در گام اول مدل یک خودکدگذار را برای تولید فضای نهفته معقول و بازسازی ویژگی‌ها آموزش می‌دهد. شبکه تخمین‌گر دیگری نیز در این مدل آموزش داده می‌شود که به عنوان خروجی پارامترهای GMM که فضای نهفته با ابعاد کوچک را مدل‌سازی می‌کند، تولید می‌کند. در مرحله آزمون میزان درستنمایی بازنمایی مدل در فضای نهفته و ویژگی‌های بازسازی شده توسط GMM محاسبه می‌شود و این مقدار به عنوان امتیاز ناهنجاری در نظر گرفته می‌شود.

### 5-3-4-مدل AnoGan

این مدل بر اساس شبکه‌های عصبی مولد تخاصمی ایجاد شده است. در گام اول یک DCGAN آموزش داده می‌شود و با استفاده از یک روش مبتنی بر تکرار بازنمایی نهفته هر نمونه محاسبه می‌شود. امتیاز ناهنجاری در این کار ترکیبی از بازسازی نمونه و استفاده از تمایزگر است. قسمت بازسازی بیانگر میزان کیفیت بازسازی تولیدی توسط شبکه مولد است و امتیاز دیگر با استفاده از شبکه تمایزگر تعریف می‌شود.

## 4-4- نتایج

در این بخش به مقایسه مدل پیشنهادی با مدل­های پایه بخش 4-3 روی مجموعه داده­هایی­که در بخش 1-4 معرفی شد، می­پردازیم. در ادامه مقایسه­ها را در دو بخش دادگان جدولی و تصویری ارائه می­کنیم.

### 1-4-4- دادگان جدولی

مدل پیشنهادی بر روی چهار مجموعه داده جدولی شامل KDDCup99 ، Arrhythmia ، Thyroid و MUSK آزمایش شده است. دادگان Thyroid و MUSK به دلیل نرخ پایین ناهنجاریشان انتخاب شده­اند تا مقاومت[[103]](#footnote-103) مدل در شرایط تفاوت فاحش در میزان نسبت داده­های ناهنجار به هنجار نیز بررسی شود. در جدول 4-1 نتایج حاصل از آزمودن مدل­های پایه و مدل پیشنهادی را با سه معیار استاندارد صحت، بازیابی و F1-score ارزیابی می­شوند. نتایج زیر مقادیر متوسط به ازای 30 اجرا برای هر یک از مدل­ها می­باشد.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model | KDDCUP | | | Arrhythmia | | | Thyroid | | | Musk | | |
| Prec. | Recall | F1 | Prec. | Recall | F1 | Prec. | Recall | F1 | Prec. | Recall | F1 |
| IF |  |  |  |  |  |  |  |  |  |  |  |  |
| OC-SVM |  |  |  |  |  |  |  |  |  |  |  |  |
| DSEBMr |  |  |  |  |  |  |  |  |  |  |  |  |
| DSEBMe |  |  |  |  |  |  |  |  |  |  |  |  |
| ADGAN |  |  |  |  |  |  |  |  |  |  |  |  |
| DAGMM |  |  |  |  |  |  |  |  |  |  |  |  |
| ALAD |  |  |  |  |  |  |  |  |  |  |  |  |
| DSVDD |  |  |  |  |  |  |  |  |  |  |  |  |
| RCALAD |  |  |  |  |  |  |  |  |  |  |  |  |
| error bar |  |  |  |  |  |  |  |  |  |  |  |  |

جدول 4-1: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه بر روی مجموعه داده­های جدولی.

### 1-4-4- دادگان تصویری

در این بخش عملکرد مدل پیشنهادی روی مجموعه داده تصویری شامل SVHN و CIFAR10 آزمایش شده است. نتایج آزمایش به تفکیک برای هر کلاس از داده­ها مطابق جدول 4-2 و 4-3 گزارش می­شود. این نتایج حاصل از میانگین 3 مرتبه اجرای هر یک از مدل­ها می باشد. همچنین میانگین معیار AUROC برای هر مجموعه داده در جدول 4-4 آورده شده است.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Normal | DCAE | DSEBM | DAGMM | IF | ADGAN | ALAD | RCALAD |
| Airplane |  |  |  |  |  |  |  |
| auto. |  |  |  |  |  |  |  |
| Bird |  |  |  |  |  |  |  |
| Cat |  |  |  |  |  |  |  |
| Deer |  |  |  |  |  |  |  |
| Dog |  |  |  |  |  |  |  |
| Frog |  |  |  |  |  |  |  |
| Horse |  |  |  |  |  |  |  |
| Ship |  |  |  |  |  |  |  |
| Truck |  |  |  |  |  |  |  |
| Mean |  |  |  |  |  |  |  |

جدول 4-2: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه برروی مجموعه داده­ CIFAR10.

همان­طور که در جدول 4-2 مشاهده می­شود، مدل پیشنهادی RCALAD می­تواند در نگاه کلی (7 کلاس از 10 کلاس داده را) دیگر مدل­های پایه از جمله ALAD و RCGANرا در مجموعه داده CIFAR10 مغلوب کند و حتی در کلاس­هایی که به بهترین نتیجه دست نیافته است، به نتایج قابل قبولی دست یافته است. در ادامه عملکرد مدل پیشنهادی بر روی مجموعه داده SVHN مورد ارزیابی قرار گرفته است.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Normal | OCSVM | DSEBMr | DSEBMe | IF | ANOGAN | ALAD | RCALAD |
| 0 |  |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |
| Mean |  |  |  |  |  |  |  |

جدول 4-3: نتایج خروجی مدل پیشنهادی در مقایسه با مدل­های پایه بر روی مجموعه داده­ SVHN.

همانطور که از جدول 4-3 مشخص است اگرچه مدل پیشنهادی RCALAD در بیشتر کلاس‌ها عملکرد بهتری نسبت به سایر مدل‌های پایه دارد برای برخی از کلاس‌ها قادر به تشخیص نمونه‌‌های ناهنجار نیست. مقایسه وضعیت کلی هر یک از این مدل­ها بر روی هر دو مجموعه­داده در یک نگاه در سطر آخر جدول 4-3 انجام شده است. همان­طور که می­بینیم عملکرد کلی مدل پیشنهادی RCALAD از دیگر مدل­ها بهتر است.

عملکرد ضعیف مدل پیشنهادی روی عدد سه می‌تواند به دلیل شباهت ظاهری میان عدد سه به عدد پنج و دو در زبان انگلیسی باشد. برای مشاهده نحوه عملکرد مدل روی کلاس عدد سه در شکل 4-4 را مشاهده کنید.



شکل 4-1: عملکرد مدل RCALAD روی کلاس عدد سه.

در شکل 4-1 ردیف اول داده هنجار، ردیف دوم بازسازی داده هنجار، ردیف سوم داده ناهنجار و ردیف چهارم بازسازی داده ناهنجار است.

## 5-4- بحث

در این بخش به بررسی کارایی و تاثیر جز به جز هر یک از عناصر موجود در مدل می­پردازیم. سپس توایع توزیع جریمه مختلف و تاثیر انتخاب هر کدام بحث قرار می­گیرد و نشان داده می­شود که نتایج بدست آمده وابستگی چندانی به یک تابع توزیع جریمه خاص ندارند. در نهایت دو امتیاز ناهنجاری ارائه شده مقایسه و حوزه عملکرد متناسب با هر یک بررسی می­شود.

### 1-5-4- مطالعه فرسایشی[[104]](#footnote-104)

در این قسمت تاثیر جزء به جزء قسمت‌های مختلف مدل را بر دقت نهایی به دست آمده بررسی ‌می‌کنیم. آزمایش‌ها در این‌جا در شرایط حضور و عدم حضور هر جزء تکرار می‌شوند و نتایج حاصل از آن‌ها با هم مقایسه می‌شود تا میزان تاثیر هر قسمت به طور جداگانه مشخص شود. نماد Dxxzz نشان­دهنده افزودن همین تمایزگر به مدل پایه ALAD می­باشد. و همچنین نماد به معنای اضافه شدن توزیع کمکی برای پوشش فضای x می­باشد.

|  |  |  |  |
| --- | --- | --- | --- |
| Model | Precision | Recall | F1 score |
| KDD99 | | | | |
| Baseline (ALAD) |  |  |  |
| Baseline + Dxxzz (CALAD) |  |  |  |
| Baseline + (RALAD) |  |  |  |
| Baseline + Dxxzz + (RCALAD) |  |  |  |
| Arrhythmia | | | | |
| Baseline (ALAD) |  |  |  |
| Baseline + Dxxzz (CALAD) |  |  |  |
| Baseline + (RALAD) |  |  |  |
| Baseline + Dxxzz + (RCALAD) |  |  |  |

جدول 4-4 تاثیر بخش­های مختلف پیشنهادی در بهبود نتایج دادگان جدولی.

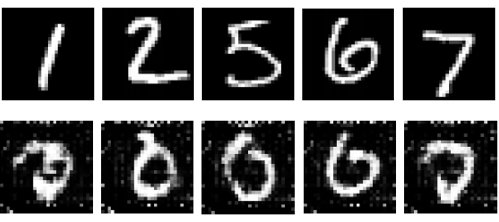
0.617647 0.65625 0.636364

نتایج جدول 4-4 نشان می‌دهد اضافه کردن تمایزگر به طور قابل ملاحظه‌ای کارایی مدل را روی دادگان جدولی افزایش داده است. همچنین این تمایزگر نتایج روی مجموعه داده‌های تصویری CIFAR-10 و SVHN را نیز به شکل مناسبی بهبود داده است. همان­طور که در جدول 4-5 مشاهده می­شود، نتایج مجموعه‌ داده جدولی درخشان­تر از مجموعه داده­های تصویری می­باشد. شایان ذکر است که اگرچه بهبود حاصل­شده در دادگان تصویری کمتر می­باشد، اما در این جنس مجموعه داده­ها حتی بهبودهای جزئی­تر از این هم باارزش بوده و قابل توجه می­باشد.

|  |  |
| --- | --- |
| Model | AUROC |
| SVHN | |
| Baseline |  |
| Baseline + DL |  |
| Baseline + SN |  |
| Baseline + SN + DL |  |
| CIFAR-10 | |
| Baseline |  |
| Baseline + DL |  |
| Baseline + SN |  |
| Baseline + SN + DL |  |

جدول 4-5 تاثیر بخش‌های مختلف پیشنهادی در بهبود نتایج دادگان تصویری.

برای مشاهده هر چه بهتر تاثیر توزیع بر بازسازی نمونه‌های ناهنجار شکل 4-2 آورده شده است. همانطور که در شکل مشخص است این توزیع مدل را متمایل به تولید کلاس هنجار صفر به ازای همه ورودی‌های ناهنجار کرده است.



شکل 4-2: تاثیر توزیع *t(x)* بر بازسازی نمونه­های ناهنجار

### 2-5-4- انتخاب تابع توزیع جریمه

در این زیربخش به آزمایش تابع توزیع‌های مختلف و میزان تاثیر آن‌ها بر نتایج نهایی مدل می‌پردازیم. توزیع‌های مورد استفاده در این‌جا دو توزیع گوسی به صورت ، و یک توزیع یکنواخت به صورت است. با استفاده از هر کدام از توابع توزیع یاد شده در مدل ارائه شده همانطور که در جدول 4-7 مشخص است، بهبود‌های پایداری حاصل شده است. تابع توزیع به منظور تقلید و یا تخمین توزیع داده ناهنجار طراحی نشده است و می‌تواند مستقل از توزیع داده ناهنجار حتی در شزایطی که متفاوت با آن است تاثیر مورد نظر خود را بر مدل بگذارد.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | KDDCUP | | | Thyroid | | |
| Prec. | Recall |  | Prec. | Recall |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

جدول 4-7: تاثیر ‌های مختلف بر عملکرد مدل RCALAD

### 3-5-4- ارزیابی کارایی امتیاز‌های ناهنجاری

در این قسمت امتیاز‌های ناهنجاری پیشنهادی در این پروژه با دیگر معیارهای مبتنی بر بازسازی مقایسه می‌شود. خروجی خام تمایزگرها را در این‌جا لاجیت[[105]](#footnote-105) می‌نامیم و غرض از ویژگی[[106]](#footnote-106)، ویژگی‌های تولیدی تمایزگر در لایه‌های پنهان است. نمونه ورودی و بازسازی تولیدی همان نمونه به وسیله مدل RCALAD است. امتیاز‌های مورد استفاده در این بخش به شرح زیر است.

|  |  |
| --- | --- |
| **(4 -1)** | Logits  Features |

|  |  |  |  |
| --- | --- | --- | --- |
| Model | Precision | Recall | F1 score |
| KDD99 | | | |
|  |  |  |  |
|  |  |  |  |
| Logits |  |  |  |
| Features |  |  |  |
| Arrhythmia | | | |
|  |  |  |  |
|  |  |  |  |
| Logits |  |  |  |
| Features |  |  |  |

جدول 4-8: مقایسه عملکرد امتیاز‌های ناهنجاری پیشنهادی با سایر امتیاز‌های ناهنجاری.

همانطور که در جدول 4-8 مشاهده می‌شود ویژگی‌های یادگرفته شده به روش تخاصمی در تمایزگر امتیاز کارکردی مناسب روی مجموعه داده‌های جدولی و تصویری است.

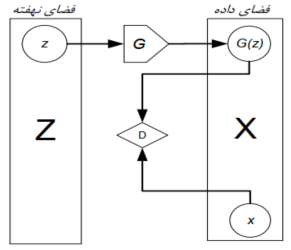
## 6-4- جمع‌بندی

در این فصل ابتدا مجموعه داده‌های استفاده شده در این پروژه معرفی شد. همچنین تنظیمات مورد نیاز برای هر مجموعه داده در تقسیم نمونه‌ها به مجموعه آموزشی و آزمون و چگونگی انتخاب تعداد نمونه‌های ناهنجار در هر دادگان مورد بررسی قرار گرفت. در گام بعدی مدل‌های پایه‌ای که به منظور مقایسه با مدل پیشنهادی به کار برده شده‌اند به طور مختصر بررسی شدند. در قدم بعدی مدل پیشنهادی با سایر مدل‌ها مقایسه و برتری کلی آن ثابت شد سپس میزان مشارکت هر قسمت از مدل پیشنهادی بر بهبود نهایی بررسی شد. در مرحله بعدی توابع مختلف به عنوان توزیع امتحان شدند و ثابت شد بهبود حاصل از این توزیع مستقل از توزیع داده‌های ناهنجار است. در گام آخر امتیازهای ناهنجاری پیشنهادی در مقایسه با سایر امتیاز‌های ناهنجاری مبتنی بر بازسازی آزموده شدند و کارایی آن‌ها تایید شد.

# فصل پنجم جمع‌بندی، نتیجه‌گیری و کارهای آتی

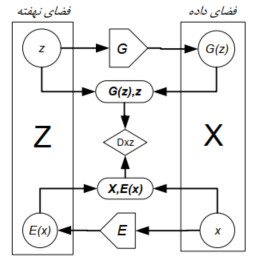
در بخش پایانی به بر مرور و جمع‌بندی هر آنچه در این پروژه گفته شد می‌پردازیم و خط مش کلی کارهای آتی را مشخص می‌کنیم.

در بخش اول به اهمیت مسئله تشخیص ناهنجاری و کاربردهای آن در دنیای واقعی پرداختیم و سپس در همین فصل جایگاه شبکه‌های مولد تخاصمی در زمینه تشخیص ناهنجاری مشخص شد. در فصل دوم به دسته‌بندی روش‌های که تا کنون در تشخیص ناهنجاری به کار برده شده‌اند از دیدگاه‌های مختلف و همچنین معرفی معیارهای پرکاربرد در ارزیابی مدل‌‌های تشخیص ناهنجاری پرداختیم. در خلال بررسی‌ها لزوم وجود روش‌هایی برای مدل‌سازی داده‌هایی پیچیده و با ابعاد بالا احساس و در نتیجه توجه‌ها به سمت شبکه‌های مولد تخاصمی که قادر به انجام این مهم هستند معطوف شد. در ادامه همین فصل به بررسی تعریف و اصول این نوع از شبکه‌ها پرداخته شد و روند تکاملی و محلی‌سازی آن‌ها با هدف تشخیص ناهنجاری مورد اشاره قرار گرفت. همانطور که مشاهده شد شبکه مولد تخاصمی که معماری آن در شکل 5-1 مشخص است در سال 2014 معرفی شد.



شکل 5-1: معماری اولیه شبکه مولد تخاصمی

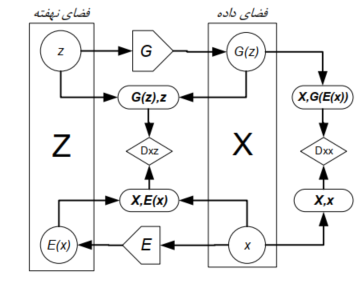
مطابق با آنچه در فصل دو بیان شد با هدف تشخیص ناهنجاری علاوه شبکه مولد که وظیفه نگاشت از فضای نهفته به فضایی داده ورودی را بر عهده دارد نیازمند فرایند استنتاجی برای نگاشت معکوس از فضای داده ورودی به فضای نهفته هستیم. مدل AnoGan با استفاده از یک فرایند مبتنی بر تکرار نقطه متناظر با داده ورودی را در فضای نهفته محاسبه می‌کرد. مشکل مدل مورد بحث پیچیدگی محاسباتی بالا و همچنین تا حد زیادی تصادفی بودن فرایند آن است. مدل‌های ALI و f-anogan و EGBAD با استفاده از یک کدگذار نگاشت معکوس به فضای نهفته آموخته می‌شود. معماری مدل ALI در شکل 5-2 قابل مشاهده است.



شکل 5-2: معماری مدل ALI

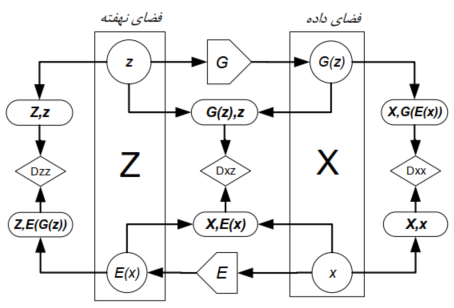
این کارهای اگرچه در جزئیات متفاوتند اما چالش اصلی آن‌ها یکسان است. در ادامه با توجه به اینکه هیچ ساختاری برای کنترل مشابهت میان تصویر ورودی و تصویر بازسازی شده توسط شبکه مولد تا به حال وجود نداشته است مدل ALICE به رفع این نقصان پرداخته است. مدل ALICE با اضافه کردن یک تمایزگر که داده ورودی و بازسازی آن را به عنوان ورودی دریافت می‌کند مشکل مورد نظر را که شرط پایداری حلقه نام داشت برطرف نمود. معماری ALICE د شکل 5-3 آورده شده است.

در فصل سه ابتدا دو مدل پایه مورد استفاده در این شبکه به طور دقیق مورد بررسی قرار گرفت. مدل ALAD بر پایه مدل قبلی بنا نهاده شده است و در معماری خود برای تضمین بیشتر پایداری حلقه تمایزگر دیگری برای فضای نهفته اضافه کرده است و همچنین ورودی‌های تمازگر‌های موجود در شبکه را به صورت توام در نظر گرفته است. معماری پیشنهادی ALAD سبب افزایش بازدهی در زمان آزمایش شده است و همچنین روند آزمایش را تثبیت کرده است. معماری این شبکه نیز در 5-4 نمایش داده شده است.



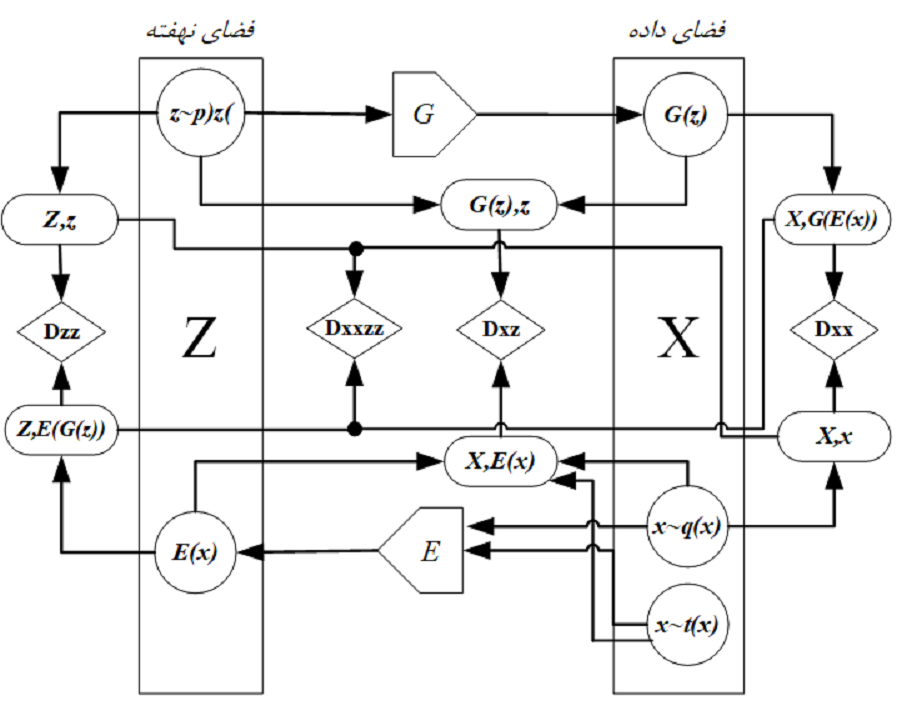
شکل 5-3: معماری شبکه ALICE

مدل پایه دیگر که در این فصل بررسی شده است، مدل RCGAN است. این شبکه با هدف ضمانت بازسازی ضعیف برای نمونه‌های ناهنجار تابع توزیع را به ساختار تخاصمی ALICE اضافه کرد تا مدل را به گونه‌ای متمایل به سمت بازسازی تمامی نمونه‌های ورودی به فضای داده هنجار در فضای داده ورودی کند. با انجام این کار فاصله میان داده ناهنجار و بازسازی آن زیاد خواهد شد و در نتیجه شناسایی نمونه ناهنجار ساده‌تر خواهد بود.



شکل 5-4: معماری شبکه ALAD

پس از این قسمت‌ها نوبت به معرفی مدل پیشنهادی این پروژه می‌رسد. همانطور که در فصل سه گفته شد به منظور تقویت قدرت تشخیص تمایزگر اطلاعات حاصل از روند دگردیسی داده ورودی در تمامی مراحل چرخه، باید توسط تمایزگر قابل دسترس باشد. چرخه مورد نظر در این مسئله شامل سه گام متوالی است، در کارهای قبلی از خروجی‌‌های چرخه اطلاعات به طور کامل در شبکه استفاده نمی‌شد. به منظور پوشش این نقص تمایزگر *Dxxzz* به ساختار‌ تخاصمی قبلی اضافه شد. علاوه بر این تمایزگر توزیع برای ضمانت بازسازی ضعیف داده ناهنجار نیز مورد استفاده قرار گرفت. در گام بعدی امتیازهای ناهنجاری جدید معرفی شدند. ساختار مدل پیشنهادی در شکل 5-5 آورده شده است.



شکل 5-5: معماری شبکه RCALAD

توابع بهینه‌سازی هر یک از شبکه‌های مورد بحث در جدول 5-1 آمده است. همانطور که مشخص است توابع بهینه‌سازی این شبکه‌ها کاملا در امتداد هم و در راستای رفع نقاط ضعف کارهای قبلی هستند.

|  |  |
| --- | --- |
| نام شبکه | تابع بهینه­سازی |
| GAN |  |
| ALI |  |
| ALICE |  |
| ALAD |  |
| RCALAD |  |

جدول 5-1: روند تکامل توابع بهینه‌سازی شبکه‌های مولد تخاصمی

نتایج عملی که در فصل چهارم مشاهده کردیم بیانگر کارایی مدل RCALAD در زمینه تشخیص ناهنجاری است. از مجموع مطالب گفته شده تا اینجا می‌توان چنین برداشت کرد استفاده توام از اطلاعات موجود در ساختارهای تخاصمی سبب بهبود عملکرد آن‌ها می‌شود. علاوه بر این وجود توزیع که مستقل از توزیع داده ناهنجار است سبب می‌شود که مدل به سمت تولید بازسازی‌ها در فضای داده هنجار سوق داده شود.

در کارهای آتی تلاش خواهد شد با روش‌های معرفی شده در ]35 [ آموزش شبکه به شکل هر چه بهتر صورت پذیرد. در این کار با استفاده از تطبیق ویژگی به جای آن‌که شبکه مولد روی تمایزگر آموزش بیش از حد ببیند، تلاش کند تا آمارگان توزیع داده ورودی را آموزش ببیند. علاوه بر این با استفاده از روش تمایز کوچک دسته‌ای[[107]](#footnote-107) مولد را مجبور به تولید خروجی‌‌های متفاوت کنیم تا کار شبکه تمایزگر سخت‌تر و روند آموزش بهبود یابد. میانگین‌گیری تاریخی[[108]](#footnote-108) از دور باطل حول یک نقطه بهینه جلوگیری می‌کند و انتظار می‌رود در صورت استفاده از این روش به بهینه محلی مناسب‌تری دست یابیم. نرمال کردن مجازی دسته[[109]](#footnote-109) سبب می‌شود تا نمونه‌های موجود در یک دسته مستقل از هم شوند و در نتیجه روند بهینه‌سازی شبکه عصبی بهبود یابد. کارایی این روش روی DCGAN ثابت شده است. انتظار می‌رود با پیاده‌سازی روش‌های نام برده شده در این بخش روند تشخیص ناهنجاری به حالت بهینه نزدیک‌تر شود.

# منابع و مراجع

[1] X. Shu, L. Cheng, and S. J. Stolfo, “Anomaly Detection as a Service.”

[2] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, “Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism,” *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3637–3647, 2018, doi: 10.1109/JIOT.2018.2816007.

[3] X. Dai and M. Bikdash, “Distance-based outliers method for detecting disease outbreaks using social media,” *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2016-July, 2016, doi: 10.1109/SECON.2016.7506752.

[4] S. A. Haque, M. Rahman, and S. M. Aziz, “Sensor anomaly detection in wireless sensor networks for healthcare,” *Sensors (Switzerland)*, vol. 15, no. 4, pp. 8764–8786, 2015, doi: 10.3390/s150408764.

[5] S. Matteoli, M. Diani, and J. Theiler, “An overview of background modeling for detection of targets and anomalies in hyperspectral remotely sensed imagery,” *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 7, no. 6, pp. 2317–2336, 2014, doi: 10.1109/JSTARS.2014.2315772.

[6] A. Del Giorno, J. Andrew Bagnell, and M. Hebert, “A discriminative framework for anomaly detection in large videos,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9909 LNCS, pp. 334–349, 2016, doi: 10.1007/978-3-319-46454-1\_21.

[7] F. Sönmez, M. Zontul, O. Kaynar, and H. Tutar, “Anomaly Detection Using Data Mining Methods in IT Systems: A Decision Support Application,” *Sak. Univ. J. Sci.*, vol. 22, no. 4, pp. 1–1, 2018, doi: 10.16984/saufenbilder.365931.

[8] G. Muruti, F. A. Rahim, and Z. A. Bin Ibrahim, “A survey on anomalies detection techniques and measurement methods,” *2018 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2018*, no. 1, pp. 81–86, 2019, doi: 10.1109/IISA.2018.8631436.

[9] M. Ahmed, A. Naser Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2016, doi: 10.1016/j.jnca.2015.11.016.

[10] T. Schlegl, P. Seeb, S. Waldstein, U. Schmidt-Erfurth, and G. Langs, “Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery,” *Int. Confrence Inf. Process. Med. Imaging*, vol. 2, pp. 146–157, 2017, doi: 10.1007/978-3-319-59050-9.

[11] V. Dumoulin *et al.*, “Adversarially learned inference,” *5th Int. Conf. Learn. Represent. ICLR 2017 - Conf. Track Proc.*, pp. 1–18, 2017.

[12] H. Issa and M. A. Vasarhelyi, “Application of Anomaly Detection Techniques to Identify Fraudulent Refunds,” *SSRN Electron. J.*, 2012, doi: 10.2139/ssrn.1910468.

[13] R. Kaur and S. Singh, “A survey of data mining and social network analysis based anomaly detection techniques,” *Egypt. Informatics J.*, vol. 17, no. 2, pp. 199–216, 2016, doi: 10.1016/j.eij.2015.11.004.

[14] N. Görnitz, M. Kloft, K. Rieck, and U. Brefeld, “Toward supervised anomaly detection,” *J. Artif. Intell. Res.*, vol. 46, pp. 235–262, 2013, doi: 10.1613/jair.3623.

[15] R. N. Reza Hassanzadeh, “A Semi­Supervised Graph­Based Algorithm for Detecting Outliers in Online­Social­Networks,” pp. 577–582, 2013.

[16] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, “A survey of deep learning-based network anomaly detection,” *Cluster Comput.*, vol. 22, pp. 949–961, 2019, doi: 10.1007/s10586-017-1117-8.

[17] Z. Zhao, C. K. Mohan, and K. G. Mehrotra, “Adaptive sampling and learning for unsupervised outlier detection,” *Proc. 29th Int. Florida Artif. Intell. Res. Soc. Conf. FLAIRS 2016*, pp. 460–465, 2016.

[18] D. Digitalcommons@uri and Y. Chae, “Representing Statistical Network-Based Anomaly Detection by Representing Statistical Network-Based Anomaly Detection by Using Trust Using Trust,” 2017, [Online]. Available: https://digitalcommons.uri.edu/oa\_diss.

[19] M. A. Rassam, A. Zainal, and M. A. Maarof, “Advancements of data anomaly detection research in Wireless Sensor Networks: A survey and open issues,” *Sensors (Switzerland)*, vol. 13, no. 8, pp. 10087–10122, 2013, doi: 10.3390/s130810087.

[20] G. Thatte, U. Mitra, and J. Heidemann, “Parametric methods for anomaly detection in aggregate traffic,” *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 512–525, 2011, doi: 10.1109/TNET.2010.2070845.

[21] J. Wu, W. Zeng, and F. Yan, “Hierarchical Temporal Memory method for time-series-based anomaly detection,” *Neurocomputing*, vol. 273, pp. 535–546, 2018, doi: 10.1016/j.neucom.2017.08.026.

[22] S. Zou, Y. Liang, H. V. Poor, and X. Shi, “Unsupervised nonparametric anomaly detection: A kernel method,” *2014 52nd Annu. Allert. Conf. Commun. Control. Comput. Allert. 2014*, pp. 836–841, 2014, doi: 10.1109/ALLERTON.2014.7028541.

[23] D. B. Araya, K. Grolinger, H. F. ElYamany, M. A. M. Capretz, and G. Bitsuamlak, “An ensemble learning framework for anomaly detection in building energy consumption,” *Energy Build.*, vol. 144, pp. 191–206, 2017, doi: 10.1016/j.enbuild.2017.02.058.

[24] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network anomaly detection: Methods, systems and tools,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.

[25] M. S. Mohd Pozi, M. N. Sulaiman, N. Mustapha, and T. Perumal, “Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming,” *Neural Process. Lett.*, vol. 44, no. 2, pp. 279–290, 2016, doi: 10.1007/s11063-015-9457-y.

[26] R. Ul Islam, M. S. Hossain, and K. Andersson, “A novel anomaly detection algorithm for sensor data under uncertainty,” *Soft Comput.*, vol. 22, no. 5, pp. 1623–1639, 2018, doi: 10.1007/s00500-016-2425-2.

[27] A. H. Moghaddam, M. H. Moghaddam, and M. Esfandyari, “Stock market index prediction using artificial neural network,” *J. Econ. Financ. Adm. Sci.*, vol. 21, no. 41, pp. 89–93, 2016, doi: 10.1016/j.jefas.2016.07.002.

[28] I. Goodfellow *et al.*, “Generative Adversarial Nets,” in *Advances in Neural Information Processing Systems*, Oct. 2014, pp. 2672–2680, doi: 10.1109/ICCVW.2019.00369.

[29] H. Zenati, M. Romain, C. S. Foo, B. Lecouat, and V. Chandrasekhar, “Adversarially Learned Anomaly Detection,” *Proc. - IEEE Int. Conf. Data Mining, ICDM*, vol. 2018-Novem, pp. 727–736, 2018, doi: 10.1109/ICDM.2018.00088.

[30] B. Schölkopf, R. Williamson, A. Smola, J. Shawe-Taylor, and J. Piatt, “Support vector method for novelty detection,” *Adv. Neural Inf. Process. Syst.*, pp. 582–588, 2000.

[31] R. A. Yeh, C. Chen, T. Yian Lim, A. G. Schwing, M. Hasegawa-Johnson, and M. N. Do, “Semantic image inpainting with deep generative models,” *Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017*, vol. 2017-Janua, pp. 6882–6890, 2017, doi: 10.1109/CVPR.2017.728.

[32] X. Chen, Y. Duan, R. Houthooft, J. Schulman, I. Sutskever, and P. Abbeel, “InfoGAN: Interpretable representation learning by information maximizing generative adversarial nets,” *Adv. Neural Inf. Process. Syst.*, pp. 2180–2188, 2016.

[33] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, “Generative Adversarial Networks: An Overview,” *IEEE Signal Process. Mag.*, vol. 35, no. 1, pp. 53–65, 2018, doi: 10.1109/MSP.2017.2765202.

[34] T. Miyato, T. Kataoka, M. Koyama, and Y. Yoshida, “Spectral normalization for generative adversarial networks,” in *6th International Conference on Learning Representations, ICLR 2018 - Conference Track Proceedings*, 2018.

[35] T. Salimans, I. Goodfellow, V. Cheung, A. Radford, and X. Chen, “Improved Techniques for Training GANs,” pp. 1–10.

[36] Z. Yang, I. S. Bozchalooi, and E. Darve, “Regularized Cycle Consistent Generative Adversarial Network for Anomaly Detection.”

**Abstract**

Anomaly detection is a significant and hence wellstudied problem in field of data analysis which is used in a wide range of applications such as fraud detection, medical application and cyber security systems. Despite the existence of statistical and machine learning-based methods, designing effective models for anomaly detection in complex high-dimensional data space remains a major challenge. As generative adversarial networks are able to handle this challenge and model the complex high-dimensional distribution of real-world data. as a result it can operate promisingly in field of anomaly detection. In this work we propose regularized comprehensive adversarially learned anomaly detection framework to detect anomalies. Our reconstruction based method reconstruct the input data through generative network and compute reconstruction error to find anomalous example. In order to effective anomaly detection it is crucial to reconstruct anomalous example in a poor way. The proposed method guarantees the poor reconstruction of anomalous data and utilize maximum joint information to train the model. Reconstruction anomaly detection requires appropriate anomaly score so as a last contribution two new anomaly score are proposed. Empirical results show that the RCALAD outperforms the current state-of-the-art models.

**Key Words:** anomaly detection, machine learning, generative adversarial networks, reconstruction error, anomaly score



Amirkabir University of Technology   
(Tehran Polytechnic)

Department of Computer Engineering and Information Technology

Master Thesis

Anomaly Detection with Generative Adversarial Network

By

Zahra Dehghanian

May 2022

1. Generative Adversarially Networks [↑](#footnote-ref-1)
2. Regularized Comprehensive Adversarially Learned Anomaly Detection [↑](#footnote-ref-2)
3. Remote sensing [↑](#footnote-ref-3)
4. Encoder [↑](#footnote-ref-4)
5. Autoencoder [↑](#footnote-ref-5)
6. Joint [↑](#footnote-ref-6)
7. Latent [↑](#footnote-ref-7)
8. Tabular [↑](#footnote-ref-8)
9. Street view house number [↑](#footnote-ref-9)
10. Unsupervised anomaly detection with generative adversarial networks to guid marker [↑](#footnote-ref-10)
11. Fast unsupervised anomaly detection with generative adversarial networks [↑](#footnote-ref-11)
12. Adversarially Learned Inference [↑](#footnote-ref-12)
13. Efficient GAN-Based Anomaly Detection [↑](#footnote-ref-13)
14. Cycle consistency [↑](#footnote-ref-14)
15. ALICE [↑](#footnote-ref-15)
16. Adversarially Learned Anomaly Detection [↑](#footnote-ref-16)
17. Clustering [↑](#footnote-ref-17)
18. False positive rate [↑](#footnote-ref-18)
19. Residual [↑](#footnote-ref-19)
20. Maximum likelihood estimation [↑](#footnote-ref-20)
21. Chi-square [↑](#footnote-ref-21)
22. kernel [↑](#footnote-ref-22)
23. Support vector machine [↑](#footnote-ref-23)
24. Posterior [↑](#footnote-ref-24)
25. Decision tree [↑](#footnote-ref-25)
26. Generative Adversarial Networks (GAN) [↑](#footnote-ref-26)
27. Reinforcement learninig [↑](#footnote-ref-27)
28. Reconstruction [↑](#footnote-ref-28)
29. Principal component analysis [↑](#footnote-ref-29)
30. Variational autoencoder [↑](#footnote-ref-30)
31. Deep autoencoding gaussian mixture models [↑](#footnote-ref-31)
32. Gradient descent [↑](#footnote-ref-32)
33. True positive [↑](#footnote-ref-33)
34. True negative [↑](#footnote-ref-34)
35. False negative [↑](#footnote-ref-35)
36. Precision [↑](#footnote-ref-36)
37. Recall [↑](#footnote-ref-37)
38. Area Under Curve Receiver Operating Characteristics [↑](#footnote-ref-38)
39. Discriminator models [↑](#footnote-ref-39)
40. Backpropagation [↑](#footnote-ref-40)
41. Dropout [↑](#footnote-ref-41)
42. Piecewise linear units [↑](#footnote-ref-42)
43. Feed forward [↑](#footnote-ref-43)
44. Minimax [↑](#footnote-ref-44)
45. Scaler [↑](#footnote-ref-45)
46. Overfitting [↑](#footnote-ref-46)
47. Minibatch [↑](#footnote-ref-47)
48. Log-Liklihood [↑](#footnote-ref-48)
49. Jensen-Shanon divergence [↑](#footnote-ref-49)
50. Nash cost [↑](#footnote-ref-50)
51. True Negative Rate [↑](#footnote-ref-51)
52. Feature matching [↑](#footnote-ref-52)
53. Convolutional [↑](#footnote-ref-53)
54. Residual Loss [↑](#footnote-ref-54)
55. Discrimination loss [↑](#footnote-ref-55)
56. Sigmoid cross entropy [↑](#footnote-ref-56)
57. logits [↑](#footnote-ref-57)
58. Deep convolutional generative adversarial network [↑](#footnote-ref-58)
59. Wasserstein GAN [↑](#footnote-ref-59)
60. Residual [↑](#footnote-ref-60)
61. Mean squared error [↑](#footnote-ref-61)
62. Encoder [↑](#footnote-ref-62)
63. Tuple [↑](#footnote-ref-63)
64. Feedforward [↑](#footnote-ref-64)
65. Interpretable Representation Learning by Information Maximizing Generative Adversarial Nets [↑](#footnote-ref-65)
66. Mutual information [↑](#footnote-ref-66)
67. Posterior [↑](#footnote-ref-67)
68. Feedforward [↑](#footnote-ref-68)
69. Interpretable Representation Learning by Information Maximizing Generative Adversarial Nets [↑](#footnote-ref-69)
70. Mutual information [↑](#footnote-ref-70)
71. Posterior [↑](#footnote-ref-71)
72. Bidirectional Generative Adversarial Model [↑](#footnote-ref-72)
73. Cross entropy [↑](#footnote-ref-73)
74. Feature matching loss [↑](#footnote-ref-74)
75. Conditional entropy [↑](#footnote-ref-75)
76. Cycle Consistency [↑](#footnote-ref-76)
77. L-norm [↑](#footnote-ref-77)
78. Threshold [↑](#footnote-ref-78)
79. Invert [↑](#footnote-ref-79)
80. Lipschitz Constraints [↑](#footnote-ref-80)
81. Activation [↑](#footnote-ref-81)
82. Regularized Cycle onsistent Generative Adversarial Network for anomaly detection [↑](#footnote-ref-82)
83. Regularized Comprehensive Adversarialy Learned Anomaly Detection [↑](#footnote-ref-83)
84. Bias [↑](#footnote-ref-84)
85. Joint Cycle Consistency [↑](#footnote-ref-85)
86. Joint Cycle Consistency [↑](#footnote-ref-86)
87. Activation function [↑](#footnote-ref-87)
88. Feature Matching [↑](#footnote-ref-88)
89. Tabular [↑](#footnote-ref-89)
90. categorical [↑](#footnote-ref-90)
91. Continuous [↑](#footnote-ref-91)
92. Musk molecular [↑](#footnote-ref-92)
93. Area Under Receiver Operating Curve [↑](#footnote-ref-93)
94. Experimental Setup [↑](#footnote-ref-94)
95. Hyper Parameter [↑](#footnote-ref-95)
96. Batch [↑](#footnote-ref-96)
97. One Class Support Vector Machines [↑](#footnote-ref-97)
98. Kernel [↑](#footnote-ref-98)
99. Radial Basis Function [↑](#footnote-ref-99)
100. Isolation Forests [↑](#footnote-ref-100)
101. Deep Structures Energy Based Models [↑](#footnote-ref-101)
102. Deep Autoencoding Gaussian Mixture Model [↑](#footnote-ref-102)
103. Robustness [↑](#footnote-ref-103)
104. Ablation studies [↑](#footnote-ref-104)
105. Logit [↑](#footnote-ref-105)
106. Feature [↑](#footnote-ref-106)
107. Minibatch discrimination [↑](#footnote-ref-107)
108. Historical averaging [↑](#footnote-ref-108)
109. Virtual batch normalization [↑](#footnote-ref-109)