异常检测，GAN如何gan？

原创 bryant8 机器学习与生成对抗网络 2019-12-15

欢迎点击上方蓝字，关注啦 ~

相关阅读：

【1】GAN在医学图像上的生成，今如何？

虚拟换衣！速览这几篇最新论文咋做的！

脸部妆容迁移！速览几篇用GAN来做的论文

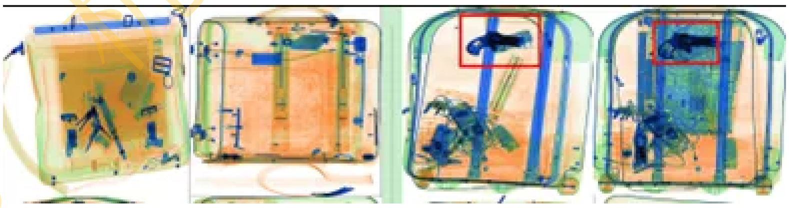
GAN整整6年了！是时候要来捋捋了！

01-GAN公式简明原理之铁甲小宝篇

今天记录一下、一些用**GAN**来做**异常检测**的论文！

异常检测(Anomaly detection)，一个很常见的问题。

在图像方面，比如每天出入地铁安检，常常看到小姐姐小哥哥们坐在那盯着你的行李过检图像，类似如下（图来自GANomaly论文）：



又比如在一些医学图像分析上，源自健康人的影像也许是比较容易获取的，并且图像的“模式”往往固定或者不多变的，而病变的图像数量是很少、很难获取，或者病变区域多变、甚至未知的，此时异常检测就面临着正样本/异常图像很少，而相对地，正常图像更容易获得的情况。这种情况其实在很多场景下有所体现，比如工业视觉检测等等。

对于已知类别、数量较多情况下，不管异常与否，我们也许可以通过训练一个分类模型就能解决。但面对也许未知、多变的情况，要想用一个多分类模型分辨出来似乎很难。如果是想仅仅分辨出是不是异常，那也许可以做一个单分类器即可。

我们尽可能地去让模型充分学习正常数据的分布长什么样子，一旦来了异常图像，它即便不知道这是啥新的分布，但依旧可以自信地告诉你：这玩意儿没见过，此乃异类也！

用GAN一些网络怎么做呢？大体思想是：

在仅有负样本（正常数据）或者少量正样本情况下：

训练阶段：

可以通过网络仅仅学习负样本（正常数据）的数据分布，得到的模型G只能生成或者重建正常数据。

测试阶段：

使用测试样本输入训练好的模型G，如果G经过重建后输出和输入一样或者接近，表明测试的是正常数据，否则是异常数据。

模型G的选择：

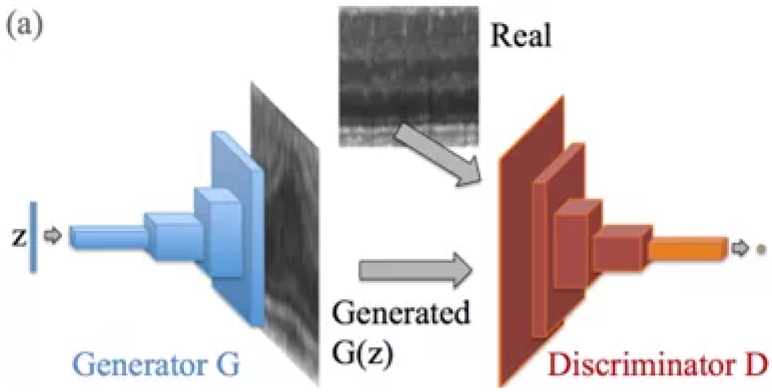
一个重建能力或者学习数据分布能力较好的**生成模型**，例如GAN或者VAE，甚至encoder-decoder。

下面速览几篇论文、看看GAN是如何做异常检测的（数据主要为图像形式）：

---

1. IPMI 2017 AnoGAN (Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery)

思路：通过一个GAN的生成器G来学习正常数据的分布，测试时图像通过学习到的G找到它应该的正常图的样子，再通过对比来找到异常与否的情况。



如上图所示，AnoGAN论文中采用的是DCGAN，一种较简单的GAN架构。

训练阶段：

对抗训练，从一个噪声向量Z通过几层反卷积搭建的生成器G学习生成正常数据图像。

测试阶段：

随机采样一个高斯噪声向量z，想要通过已经训练好的G生成一幅和测试图像x对应的正常图像G(z)。G的参数是固定的，它只能生成落在正常数据分布的图像。但此时仍需进行训练，把z看成待更新的参数，通过比较G(z)和x的差异去更新，从而生成一个与x尽可能相似、理想对应的正常图像。

如果x是正常的图像，那么x和G(z)应该是一样的。

如果x异常，通过更新z，可以认为重建出了异常区域的理想的正常情况，这样两图一对比不仅仅可以认定异常情况，同时还可以找到异常区域。

为了比较G(z)和x差异去更新z：

一是通过计算G(z)和x的图像层面的L1 loss：

Residual Loss The *residual loss* measures the visual dissimilarity between query image $\mathbf{x}$ and generated image $G(\mathbf{z})$ in the image space and is defined by

$$\mathcal{L}_R(\mathbf{z}) = \sum |\mathbf{x} - G(\mathbf{z})|. \qquad (3)$$

Under the assumption of a perfect generator G and a perfect mapping to latent space, for an ideal normal query case, images $\mathbf{x}$ and $G(\mathbf{z})$ are identical. In this case, the *residual loss* is zero.

二是利用到训练好的判别器D，取G(z)和x在判别器D的中间层的特征层面的loss：

a richer intermediate feature representation of the discriminator and define the *discrimination loss* as follows:

$$\mathcal{L}_D(\mathbf{z}\ ) = \sum |\mathbf{f}(\mathbf{x}) - \mathbf{f}(G(\mathbf{z}\ ))|, \tag{4}$$

where the output of an intermediate layer $f(\cdot)$ of the discriminator is used to specify the statistics of an input image. Based on this new loss term, the adaptation of the coordinates of $\mathbf{z}$ does not only rely on a hard decision of the trained discriminator, whether or not a generated image $G(\mathbf{z}\ )$ fits the learned distribution of normal images, but instead takes the rich information of the feature representation, which is learned by the discriminator during adversarial training, into account. In this sense, our approach utilizes the trained discriminator not as classifier but as a feature extractor.

两者综合：

For the mapping to the latent space, we define the overall loss as weighted sum of both components:

$$\mathcal{L}(\mathbf{z}_\gamma) = (1-\lambda) \cdot \mathcal{L}_R(\mathbf{z}_\gamma) + \lambda \cdot \mathcal{L}_D(\mathbf{z}_\gamma). \tag{5}$$

Only the coefficients of $\mathbf{z}$ are adapted via backpropagation. The trained parameters of the generator and discriminator are kept fixed.

另外，异常分数计算方法：

2.3 Detection of Anomalies

During anomaly identification in new data we evaluate the new query image $\mathbf{x}$ as being a normal or anomalous image. Our loss function (Eq. (5)), used for mapping to the latent space, evaluates in every update iteration γ the compatibility of generated images $G(\mathbf{z}_\gamma)$ with images, seen during adversarial training. Thus, an *anomaly score*, which expresses the fit of a query image $\mathbf{x}$ to the model of normal images, can be directly derived from the mapping loss function (Eq. (5)):

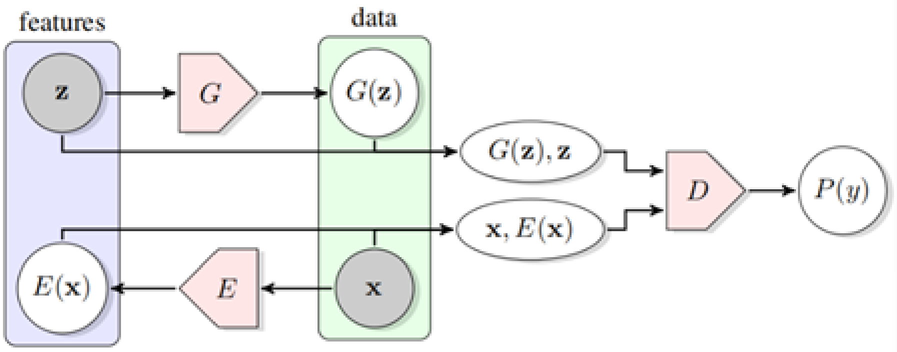
$$A(\mathbf{x}) = (1-\lambda) \cdot R(\mathbf{x}) + \lambda \cdot D(\mathbf{x}), \tag{6}$$

where the *residual score* $R(x)$ and the *discrimination score* $D(x)$ are defined by the *residual loss* $\mathcal{L}_R(\mathbf{z}_\Gamma)$ and the *discrimination loss* $\mathcal{L}_D(\mathbf{z}_\Gamma)$ at the last (Γ^{th}) update iteration of the mapping procedure to the latent space, respectively. The model yields a large *anomaly score* $A(\mathbf{x})$ for anomalous images, whereas a small *anomaly score* means that a very similar image was already seen during training. We use the *anomaly score* $A(\mathbf{x})$ for image based anomaly detection. Additionally, the residual image $\mathbf{x}_R = |\mathbf{x} - G(\mathbf{z}_\Gamma)|$ is used for the identification of anomalous regions within an image. For purposes of comparison, we additionally define a *reference anomaly score* $\hat{A}(\mathbf{x}) = (1-\lambda) \cdot R(\mathbf{x}) + \lambda \cdot \hat{D}(\mathbf{x})$, where $\hat{D}(\mathbf{x}) = \mathcal{L}_{\hat{D}}(\mathbf{z}_\Gamma)$ is the *reference discrimination score* used by Yeh et al. [13].

2. 2018-02 EFFICIENT GAN-BASED ANOMALY DETECTION

针对AnoGAN测试阶段仍然需要更新参数的缺陷，此方法提出一种基于BiGAN可快百倍的方法。

训练时，同时学习将输入样本x映射到潜在表示z的编码器E，以及生成器G和判别器D：



$\min_{G,E} \max_D V(D,E,G)$, with $V(D,E,G)$ defined as

$$V(D,E,G) = \mathbb{E}_{x\sim p_X}\left[\mathbb{E}_{z\sim p_E(\cdot|x)}\left[\log D(x,z)\right]\right] + \mathbb{E}_{z\sim p_Z}\left[\mathbb{E}_{x\sim p_G(\cdot|z)}\left[1-\log D(x,z)\right]\right].$$

Here, $p_X(x)$ is the distribution over the data, $p_Z(z)$ the distribution over the latent representation, and $p_E(z|x)$ and $p_G(x|z)$ the distributions induced by the encoder and generator respectively.

如此可避免测试仍需要“找到z”那个耗时的步骤。与常规GAN中的D仅考虑输入（实际的或生成的）图像不同，而还考虑了潜在表示z(作为输入)。

测试时，判断图像的异常与否的分值计算方法，可选择可AnoGAN基本一样的方法。

Having trained a model on the normal data to yield G, D and E, we then define a score function $A(x)$ (as in Schlegl et al. (2017)) that measures how anomalous an example x is, based on a convex combination of a reconstruction loss L_G and a discriminator-based loss L_D:

$$A(x) = \alpha L_G(x) + (1-\alpha)L_D(x)$$

where $L_G(x) = ||x - G(E(x))||_1$ and $L_D(x)$ can be defined in two ways. First, using the cross-entropy loss σ from the discriminator of x being a real example (class 1): $L_D(x) = \sigma(D(x,E(x)),1)$, which captures the discriminator's confidence that a sample is derived from the real data distribution. A second way of defining the L_D is with a “feature-matching loss”$L_D(x) = ||f_D(x,E(x)) - f_D(G(E(x)),E(x))||_1$, with f_D returning the layer preceding the logits for the given inputs in the discriminator. This evaluates if the reconstructed data has similar features in the discriminator as the true sample. Samples with larger values of $A(x)$ are deemed more likely to be anomalous.

3. 2018-12 Adversarially Learned Anomaly Detection

第二种方法的加强版，也是基于BiGAN,并且在稳定训练上做了些功夫。如下所示，（乖乖，搞了三个判别器 =_=

$\min_{G,E} \max_{D_{xz},D_{xx},D_{zz}} V(D_{xz}, D_{xx}, D_{zz}, E, G)$, with $V(D_{xz}, D_{xx}, D_{zz}, E, G)$ defined as

$$V(D_{xz}, D_{xx}, D_{zz}, E, G) = V(D_{xz}, E, G) + V(D_{xx}, E, G) + V(D_{zz}, E, G).$$

A schematic of this final GAN model is shown in Figure 1.

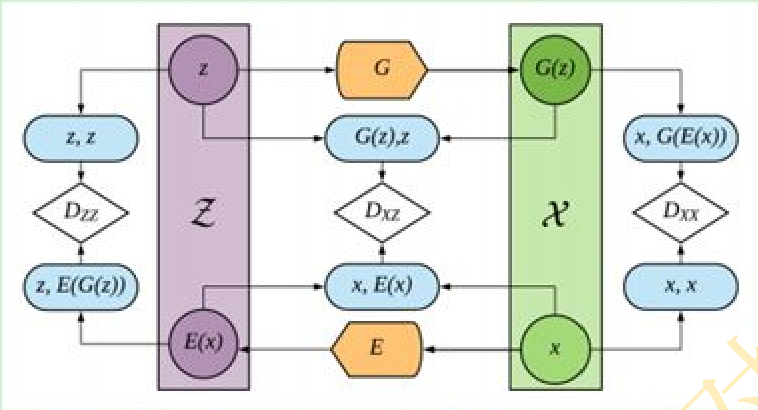


Figure 1. The GAN used in Adversarially Learned Anomaly Detection. D_{zz}, D_{xz} and D_{xx} denote discriminators (white), G the generator (orange), and E the encoder (orange); these networks are simultaneously learned during training.

检测时的计算方法：

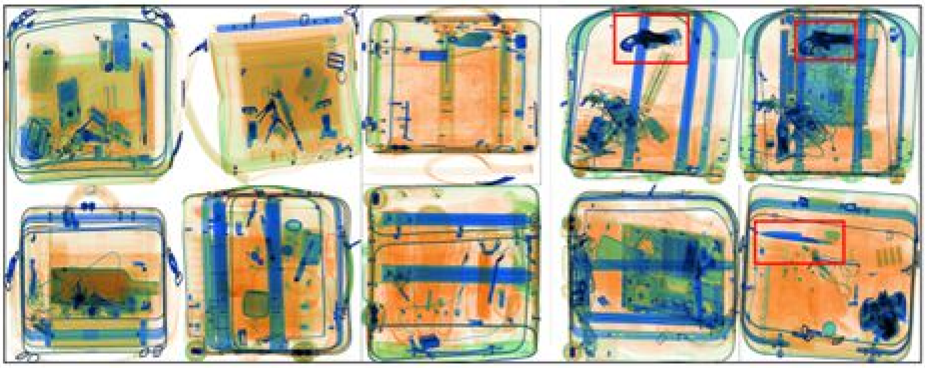
Algorithm 1 Adversarially Learned Anomaly Detection

Input $\boldsymbol{x}, \sim p_{X_{Test}}(x), E, G, f_{xx}$ where f_{xx} is the feature layer of D_{xx}

Output $A(\boldsymbol{x})$, where A is the anomaly score

```
procedure INFERENCE
    z̃ ← E(x)                          ▷ Encode samples
    x̂ ← G(z̃),                         ▷ Reconstruct samples
    f_δ ← f_xx(x, x̂)
    f_α ← f_xx(x, x)
    return ||f_δ − f_α||_1
end procedure
```

4. 2018-11-13 GANomaly: Semi-Supervised Anomaly Detection via Adversarial Training



(a) Normal Data (X-ray Scans) (b) Normal + Abnormal Data (X-ray Scans)

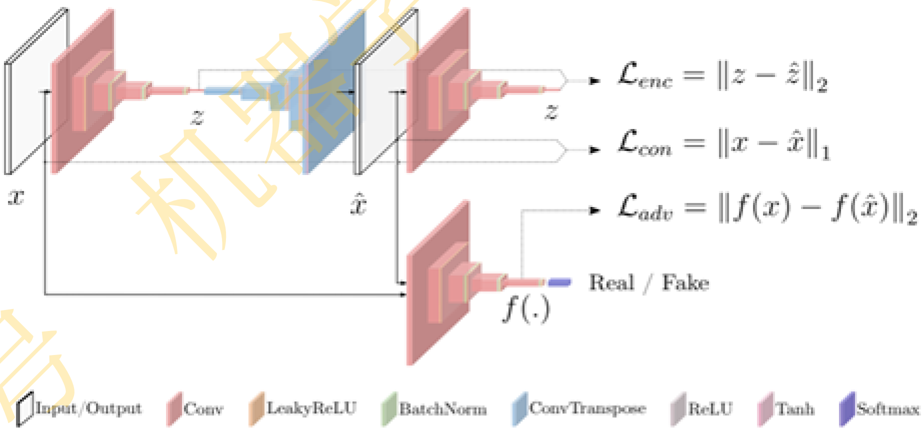
Fig. 1. Overview of our anomaly detection approach within the context of an X-ray security screening problem. Our model is trained on normal samples (a), and tested on normal and abnormal samples (b). Anomalies are detected when the output of the model is greater than a certain threshold $\mathcal{A}(x) > \phi$.

原理：

训练时，约束正常的数据编码得到潜在空间表示z1，和对z1解码、再编码得到的z2，差距不会特别大，理想应该是一样的。

所以训练好后，用正常样本训练好的 G只能重建正常数据分布，一旦用于从未见过的异常样本编码、解码、再经历编码得到的潜在空间Z差距是大的。

当两次编码得到的潜在空间差距大于一定阈值的时候，就判定样本是异常样本。



5. 2019-01-25 Skip-GANomaly: Skip Connected and Adversarially Trained Encoder-Decoder Anomaly Detection

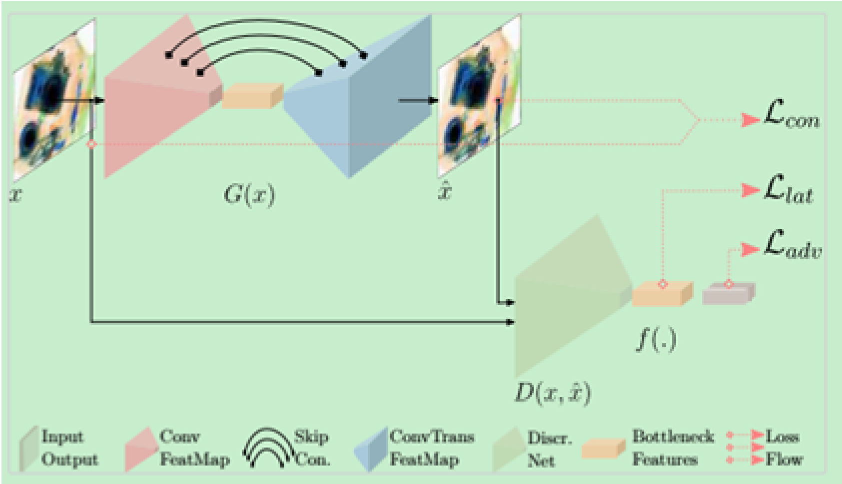
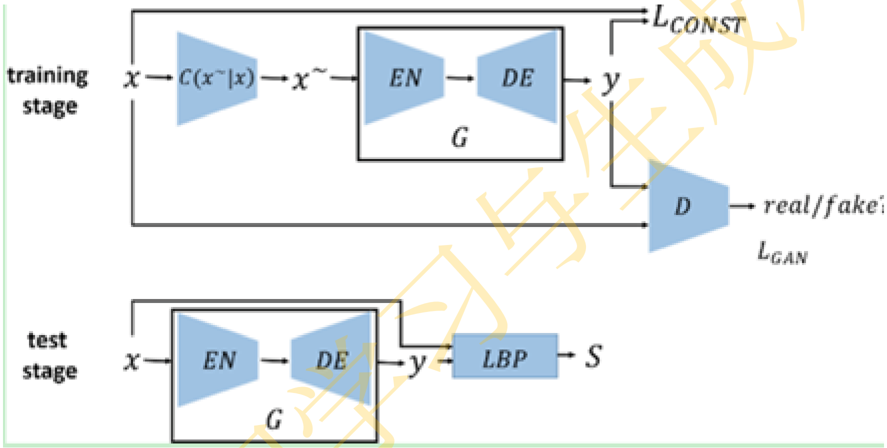


Fig. 2: Overview of the proposed adversarial training procedure.

6. PRICAI 2018 A Surface Defect Detection Method Based on Positive Samples



原理：

C（x~|x）是人工缺陷制造模块。X~是模拟缺陷的样本，经过EN-DE编码解码器后重建正常样本Y。

测试阶段，X输入EN-DE后得到理想正常样本y，使用LBP对Y和X逐像素特征比较，相差大则有缺陷。

7. MIDL 2018 Unsupervised Detection of Lesions in Brain MRI using constrained adversarial auto-encoders

使用的是AAE来学习建模正常数据分布。有时，对于在正常分布的的两个数据之间的距离，比一个正常和一个异常之间的距离还大，所以提出在隐空间也加一个约束。

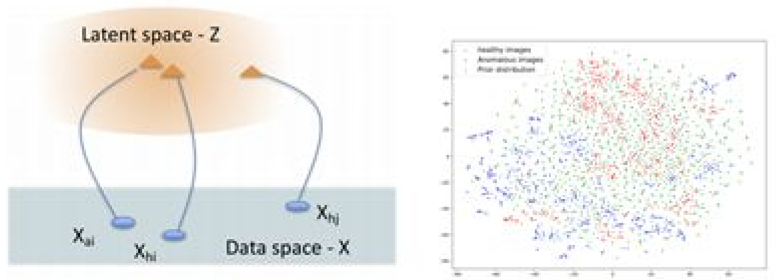
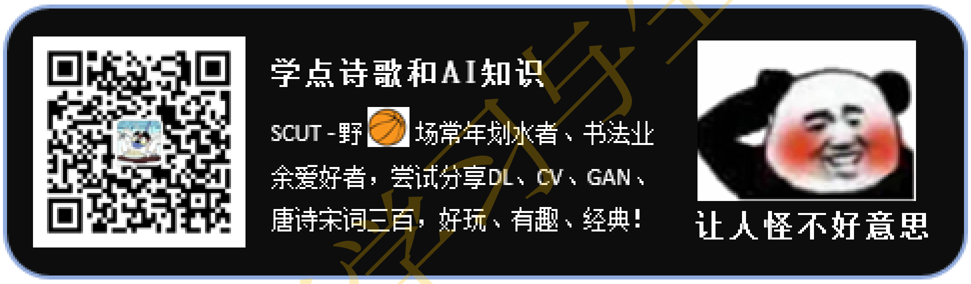


Figure 1: Encoding input data into latent representation. Left: Illustration shows the encoding of VAE/AAE model. Data samples (blue circles) are encoded into latent representation (orange triangles). Difference between two 'healthy' images X_{hi} and X_{hj} might be larger than the distance between an image with an abnormal lesion X_{ai} and its 'healthy' version X_{hi}. Latent representation of these images may also satisfy the same relationship. As a result, images with abnormalities may not lie separate than normal images. Right: Image shows TSNE embeddings of healthy images (red) and lesion images (blue) from the BRATS dataset. We also show samples from the prior distribution in green. Healthy images and abnormal images can be mapped close in the latent space, the latent representations of the abnormal images also lie in the prior distribution together with the representations of healthy images, making them indistinguishable in the latent space.

暂时先写到这吧。

最后，欢迎关注公众号啦~



最后的最后，再来发一波、到**目前为止**、**部分**、用 **GAN** 做**异常检测**的基本相关（**直接用“adversarial anomaly detection”在arxiv上爬下来的，不一定相关！2333**）论文供参考！！！

---

001 (2019-12-10) Event Detection in Micro-PMU Data A Generative Adversarial Network ScoringMethod
https://arxiv.xilesou.top/pdf/1912.05103.pdf

002 (2019-12-10) Outage Detection in Partially Observable DistributionSystems using Smart Meters and Generative Adversarial Networks
https://arxiv.xilesou.top/pdf/1912.04992.pdf

003 (2019-12-9) Oversampling Log Messages Using a Sequence GenerativeAdversarial Network for Anomaly Detection and Classification

https://arxiv.xilesou.top/pdf/1912.04747.pdf

004 (2019-12-2) Anomaly Detection in Particulate Matter Sensor usingHypothesis Pruning Generative Adversarial Network

https://arxiv.xilesou.top/pdf/1912.00583.pdf

005 (2019-11-27) Sparse-GAN Sparsity-constrained Generative Adversarial Network for AnomalyDetection in Retinal OCT Image

https://arxiv.xilesou.top/pdf/1911.12527.pdf

006 (2019-11-21) EvAn NeuromorphicEvent-based Anomaly Detection

https://arxiv.xilesou.top/pdf/1911.09722.pdf

007 (2019-11-19) Attention Guided Anomaly Detection and Localization in Images

https://arxiv.xilesou.top/pdf/1911.08616.pdf

008 (2019-11-17) Deep Verifier Networks Verification of Deep Discriminative Models with Deep Generative Models

https://arxiv.xilesou.top/pdf/1911.07421.pdf

009 (2019-11-16) RSM-GAN A ConvolutionalRecurrent GAN for Anomaly Detection in Contaminated Seasonal Multivariate TimeSeries

https://arxiv.xilesou.top/pdf/1911.07104.pdf

010 (2019-10-30) Robust and Computationally-Efficient Anomaly Detectionusing Powers-of-Two Networks

https://arxiv.xilesou.top/pdf/1910.14096.pdf

011 (2019-10-29) Small-GAN SpeedingUp GAN Training Using Core-sets

https://arxiv.xilesou.top/pdf/1910.13540.pdf

012 (2019-10-23) Photoshopping Colonoscopy Video Frames

https://arxiv.xilesou.top/pdf/1910.10345.pdf

013 (2019-10-21) GraphSAC Detectinganomalies in large-scale graphs

https://arxiv.xilesou.top/pdf/1910.09589.pdf

014 (2019-10-21) Adversarial Anomaly Detection for Marked Spatio-TemporalStreaming Data

https://arxiv.xilesou.top/pdf/1910.09161.pdf

015 (2019-10-10) Misbehaviour Prediction for Autonomous Driving Systems

https://arxiv.xilesou.top/pdf/1910.04443.pdf

016 (2019-10-9) Adversarial Learning of Deepfakes in Accounting

https://arxiv.xilesou.top/pdf/1910.03810.pdf

017 (2019-09-12) Perceptual Image Anomaly Detection

https://arxiv.xilesou.top/pdf/1909.05904.pdf

018 (2019-08-27) Self-Supervised Representation Learning viaNeighborhood-Relational Encoding

https://arxiv.xilesou.top/pdf/1908.10455.pdf

019 (2019-08-10) Transcriptional Response of SK-N-AS Cells to Methamidophos

https://arxiv.xilesou.top/pdf/1908.03841.pdf

020 (2019-09-3) Februus InputPurification Defence Against Trojan Attacks on Deep Neural Network Systems

https://arxiv.xilesou.top/pdf/1908.03369.pdf

021 (2019-08-8) What goes around comes around Cycle-Consistency-based Short-Term MotionPrediction for Anomaly Detection using Generative Adversarial Networks

https://arxiv.xilesou.top/pdf/1908.03055.pdf

022 (2019-08-2) Detection of Accounting Anomalies in the Latent Space usingAdversarial Autoencoder Neural Networks

https://arxiv.xilesou.top/pdf/1908.00734.pdf

023 (2019-09-3) Q-MIND DefeatingStealthy DoS Attacks in SDN with a Machine-learning based Defense Framework

https://arxiv.xilesou.top/pdf/1907.11887.pdf

024 (2019-10-8) Real-time Evasion Attacks with Physical Constraints on DeepLearning-based Anomaly Detectors in Industrial Control Systems

https://arxiv.xilesou.top/pdf/1907.07487.pdf

025 (2019-07-12) AMAD AdversarialMultiscale Anomaly Detection on High-Dimensional and Time-Evolving CategoricalData

https://arxiv.xilesou.top/pdf/1907.06582.pdf

026 (2019-06-27) A Survey on GANs for Anomaly Detection

https://arxiv.xilesou.top/pdf/1906.11632.pdf

027 (2019-06-15) Physical Integrity Attack Detection of Surveillance Camerawith Deep Learning Based Video Frame Interpolation

https://arxiv.xilesou.top/pdf/1906.06475.pdf

028 (2019-07-8) GAN-based Multiple Adjacent Brain MRI Slice Reconstructionfor Unsupervised Alzheimer's Disease Diagnosis

https://arxiv.xilesou.top/pdf/1906.06114.pdf

029 (2019-06-3) Generative Adversarial Networks for Distributed IntrusionDetection in the Internet of Things

https://arxiv.xilesou.top/pdf/1906.00567.pdf

030 (2019-11-20) Unsupervised Learning of Anomaly Detection fromContaminated Image Data using Simultaneous Encoder Training

https://arxiv.xilesou.top/pdf/1905.11034.pdf

031 (2019-10-18) Adversarially-trained autoencoders for robust unsupervisednew physics searches

https://arxiv.xilesou.top/pdf/1905.10384.pdf

032 (2019-05-19) Spatio-Temporal Adversarial Learning for Detecting UnseenFalls

https://arxiv.xilesou.top/pdf/1905.07817.pdf

033 (2019-05-20) Finding Rats in Cats Detecting Stealthy Attacks using Group Anomaly Detection

https://arxiv.xilesou.top/pdf/1905.07273.pdf

034 (2019-04-25) End-to-End Adversarial Learning for Intrusion Detection inComputer Networks

https://arxiv.xilesou.top/pdf/1904.11577.pdf

035 (2019-04-24) GAN Augmented Text Anomaly Detection with Sequences of DeepStatistics

https://arxiv.xilesou.top/pdf/1904.11094.pdf

036 (2019-04-23) A Comparison Study of Credit Card Fraud Detection Supervised versus Unsupervised

https://arxiv.xilesou.top/pdf/1904.10604.pdf

037 (2019-09-24) Trick or Heat Manipulating Critical Temperature-Based Control Systems UsingRectification Attacks

https://arxiv.xilesou.top/pdf/1904.07110.pdf

038 (2019-12-2) Adversarial Learning in Statistical Classification A Comprehensive Review of Defenses AgainstAttacks

https://arxiv.xilesou.top/pdf/1904.06292.pdf

039 (2019-04-11) (Martingale) Optimal Transport And Anomaly Detection WithNeural Networks A Primal-dual Algorithm

https://arxiv.xilesou.top/pdf/1904.04546.pdf

040 (2019-07-24) Efficient GAN-based method for cyber-intrusion detection

https://arxiv.xilesou.top/pdf/1904.02426.pdf

041 (2019-04-2) Fence GAN TowardsBetter Anomaly Detection

https://arxiv.xilesou.top/pdf/1904.01209.pdf

042 (2019-03-27) Fundamental Limits of Covert Packet Insertion

https://arxiv.xilesou.top/pdf/1903.11640.pdf

043 (2019-05-20) Deep Generative Design Integration of Topology Optimization and Generative Models

https://arxiv.xilesou.top/pdf/1903.01548.pdf

044 (2019-11-14) adVAE Aself-adversarial variational autoencoder with Gaussian anomaly prior knowledgefor anomaly detection

https://arxiv.xilesou.top/pdf/1903.00904.pdf

045 (2019-07-14) Secure Distributed Dynamic State Estimation in Wide-AreaSmart Grids

https://arxiv.xilesou.top/pdf/1902.07288.pdf

046 (2019-02-19) Anomaly Detection with Adversarial Dual Autoencoders

https://arxiv.xilesou.top/pdf/1902.06924.pdf

047 (2019-05-9) The Odds are Odd AStatistical Test for Detecting Adversarial Examples

https://arxiv.xilesou.top/pdf/1902.04818.pdf

048 (2019-11-6) BIVA A Very DeepHierarchy of Latent Variables for Generative Modeling

https://arxiv.xilesou.top/pdf/1902.02102.pdf

049 (2019-01-28) Heartbeat Anomaly Detection using Adversarial Oversampling

https://arxiv.xilesou.top/pdf/1901.09972.pdf

050 (2019-01-25) Skip-GANomaly SkipConnected and Adversarially Trained Encoder-Decoder Anomaly Detection

https://arxiv.xilesou.top/pdf/1901.08954.pdf

051 (2019-05-27) Maximum Entropy Generators for Energy-Based Models

https://arxiv.xilesou.top/pdf/1901.08508.pdf

052 (2019-01-10) Adversarial Pseudo Healthy Synthesis Needs PathologyFactorization

https://arxiv.xilesou.top/pdf/1901.07295.pdf

053 (2019-01-18) Robust Anomaly Detection in Images using AdversarialAutoencoders

https://arxiv.xilesou.top/pdf/1901.06355.pdf

054 (2019-01-15) MAD-GAN MultivariateAnomaly Detection for Time Series Data with Generative Adversarial Networks

https://arxiv.xilesou.top/pdf/1901.04997.pdf

055 (2019-12-4) Event Generation and Statistical Sampling for Physics withDeep Generative Models and a Density Information Buffer

https://arxiv.xilesou.top/pdf/1901.00875.pdf

056 (2018-12-11) Anomaly Generation using Generative Adversarial Networks inHost Based Intrusion Detection

https://arxiv.xilesou.top/pdf/1812.04697.pdf

057 (2018-12-11) Anomaly detection with Wasserstein GAN

https://arxiv.xilesou.top/pdf/1812.02463.pdf

058 (2018-12-5) Adversarially Learned Anomaly Detection

https://arxiv.xilesou.top/pdf/1812.02288.pdf

059 (2018-11-11) Adversarial Learning-Based On-Line Anomaly Monitoring forAssured Autonomy

https://arxiv.xilesou.top/pdf/1811.04539.pdf

060 (2018-10-19) Subset Scanning Over Neural Network Activations

https://arxiv.xilesou.top/pdf/1810.08676.pdf

061 (2018-10-11) MDGAN BoostingAnomaly Detection Using \\Multi-Discriminator Generative Adversarial Networks

https://arxiv.xilesou.top/pdf/1810.05221.pdf

062 (2019-04-30) Prospect Theoretic Approach for Data Integrity in IoTNetworks under Manipulation Attacks

https://arxiv.xilesou.top/pdf/1809.07928.pdf

063 (2019-01-15) Anomaly Detection with Generative Adversarial Networks forMultivariate Time Series

https://arxiv.xilesou.top/pdf/1809.04758.pdf

064 (2018-09-28) Layerwise Perturbation-Based Adversarial Training for HardDrive Health Degree Prediction

https://arxiv.xilesou.top/pdf/1809.04188.pdf

065 (2018-09-7) Coupled IGMM-GANs for deep multimodal anomaly detection inhuman mobility data

https://arxiv.xilesou.top/pdf/1809.02728.pdf

066 (2019-08-2) Detection and Mitigation of Attacks on TransportationNetworks as a Multi-Stage Security Game

https://arxiv.xilesou.top/pdf/1808.08349.pdf

067 (2018-08-23) DOPING GenerativeData Augmentation for Unsupervised Anomaly Detection with GAN

https://arxiv.xilesou.top/pdf/1808.07632.pdf

068 (2018-08-1) Anomaly Detection via Minimum Likelihood GenerativeAdversarial Networks

https://arxiv.xilesou.top/pdf/1808.00200.pdf

069 (2018-07-22) SAIFE UnsupervisedWireless Spectrum Anomaly Detection with Interpretable Features

https://arxiv.xilesou.top/pdf/1807.08316.pdf

070 (2018-06-27) Adversarial Distillation of Bayesian Neural NetworkPosteriors

https://arxiv.xilesou.top/pdf/1806.10317.pdf

071 (2019-03-25) Learning Neural Random Fields with Inclusive AuxiliaryGenerators

https://arxiv.xilesou.top/pdf/1806.00271.pdf

072 (2018-07-17) AVID AdversarialVisual Irregularity Detection

https://arxiv.xilesou.top/pdf/1805.09521.pdf

073 (2018-11-13) GANomaly Semi-Supervised Anomaly Detection via Adversarial Training

https://arxiv.xilesou.top/pdf/1805.06725.pdf

074 (2018-05-5) Population Anomaly Detection through Deep Gaussianization

https://arxiv.xilesou.top/pdf/1805.02123.pdf

075 (2018-04-13) Group Anomaly Detection using Deep Generative Models

https://arxiv.xilesou.top/pdf/1804.04876.pdf

076 (2018-04-13) Adversarial Clustering A Grid Based Clustering Algorithm Against Active Adversaries

https://arxiv.xilesou.top/pdf/1804.04780.pdf

077 (2018-04-12) Deep Autoencoding Models for Unsupervised AnomalySegmentation in Brain MR Images

https://arxiv.xilesou.top/pdf/1804.04488.pdf

078 (2018-04-3) Correlated discrete data generation using adversarialtraining

https://arxiv.xilesou.top/pdf/1804.00925.pdf

079 (2018-03-17) A Multi-perspective Approach To Anomaly Detection ForSelf-aware Embodied Agents

https://arxiv.xilesou.top/pdf/1803.06579.pdf

080 (2018-04-9) CIoTA CollaborativeIoT Anomaly Detection via Blockchain

https://arxiv.xilesou.top/pdf/1803.03807.pdf

081 (2018-05-24) Adversarially Learned One-Class Classifier for NoveltyDetection

https://arxiv.xilesou.top/pdf/1802.09088.pdf

082 (2019-05-1) Efficient GAN-Based Anomaly Detection

https://arxiv.xilesou.top/pdf/1802.06222.pdf

083 (2018-02-13) Satellite Image Forgery Detection and Localization UsingGAN and One-Class Classifier

https://arxiv.xilesou.top/pdf/1802.04881.pdf

084 (2018-02-8) Detection of Adversarial Training Examples in PoisoningAttacks through Anomaly Detection

https://arxiv.xilesou.top/pdf/1802.03041.pdf

085 (2018-01-5) Shielding Google's language toxicity model againstadversarial attacks

https://arxiv.xilesou.top/pdf/1801.01828.pdf

086 (2018-06-27) When Not to Classify Anomaly Detection of Attacks (ADA) on DNN Classifiers at Test Time

https://arxiv.xilesou.top/pdf/1712.06646.pdf

087 (2018-04-24) Bayesian Hypernetworks

https://arxiv.xilesou.top/pdf/1710.04759.pdf

088 (2017-09-15) To Go or Not To Go ANear Unsupervised Learning Approach For Robot Navigation

https://arxiv.xilesou.top/pdf/1709.05439.pdf

089 (2017-04-5) Counter-RAPTOR Safeguarding Tor Against Active Routing Attacks

https://arxiv.xilesou.top/pdf/1704.00843.pdf

090 (2017-03-17) Unsupervised Anomaly Detection with Generative AdversarialNetworks to Guide Marker Discovery

https://arxiv.xilesou.top/pdf/1703.05921.pdf