A New GAN-Based Anomaly Detection (GBAD) Approach for Multi-Threat Object Classification on Large-Scale X-Ray Security Images

Article *in* IEICE Transactions on Information and Systems · February 2020

DOI: 10.1587/transinf.2019EDL8154

CITATIONS
9

READS
530

3 authors, including:

Joanna Kazzandra Dumagpi
Kwangwoon University
4 PUBLICATIONS **16** CITATIONS

SEE PROFILE

IEICE TRANS. INF. & SYST., VOL.E103–D, NO.2 FEBRUARY 2020

LETTER

A New GAN-Based Anomaly Detection (GBAD) Approach for Multi-Threat Object Classification on Large-Scale X-Ray Security Images

Joanna Kazzandra DUMAGPI[†a)], ***Member***, **Woo-Young JUNG**[†], ***and*** **Yong-Jin JEONG**[†], ***Nonmembers***

SUMMARY Threat object recognition in x-ray security images is one of the important practical applications of computer vision. However, research in this field has been limited by the lack of available dataset that would mirror the practical setting for such applications. In this paper, we present a novel GAN-based anomaly detection (GBAD) approach as a solution to the extreme class-imbalance problem in multi-label classification. This method helps in suppressing the surge in false positives induced by training a CNN on a non-practical dataset. We evaluate our method on a large-scale x-ray image database to closely emulate practical scenarios in port security inspection systems. Experiments demonstrate improvement against the existing algorithm.

key words: *anomaly detection, generative adversarial networks, x-ray baggage security, convolutional neural networks, threat classification*

1. Introduction

X-ray imaging is one of the widely known methods in non-destructive evaluation with notable application in security systems [1]. Automatic object recognition is certainly one of the most important developments in computer vision that is valuable mainly in security systems, in which Convolutional Neural Networks (CNNs) are the current state-of-the-art solution. Recent CNN architectures have become deeper and wider to attain higher accuracies [2]–[4]. Even though CNNs were extensively used for photographic images, [5] demonstrates the effectiveness of CNNs as feature extractors for threat object recognition on single-energy x-ray images. Furthermore, an empirical study conducted in [6] shows that using end-to-end CNNs for the similar task works as well on multi-energy x-ray images.

However, the above-mentioned performance of CNNs were from evaluations on datasets that may not be reflective of practical conditions, especially in the context of security systems. For instance, in baggage screening, threat objects typically do not occur nearly as often as normal objects making them underrepresented during the learning process. This is known as the class imbalance problem and is formally defined as a significant skewness in the class distribution of a dataset, wherein some classes severely out represent the others [7]. Such a case is a problem for most of the standard learning algorithms, which assumes a balanced distribution between classes or equal misclassification costs. Both datasets used in [5] and [6] are not only relatively balanced but are severely smaller in size compared to photographic image datasets. Performance on such small datasets may not accurately represent performance in the real-world scenario. Consequently, Miao et al. [8] recently published the largest database on x-ray baggage security images in which they demonstrated the effect of class imbalance in image recognition. They proposed a class-imbalance hierarchal refinement (CHR) approach to classify x-ray images with multiple target threat objects while under varying cases of class imbalance.

Anomaly detection is listed in [7] as an emerging approach to the class imbalance problem. This method aims to detect outliers within a given data distribution based on some measure of normality. As a solution to class imbalance problem, the characteristics of the majority class becomes the basis for normality, making the minority class the target anomalies. Latest research explores the use of Generative Adversarial Networks (GANs) [9] in anomaly detection. The first GAN-based approach to anomaly detection was proposed in [10], however, this approach was impractical in real-time applications due to the need for repeated backpropagation to recover the latent representation. This work was extended in [11] where instead of just plain GAN, the authors used Bi-GAN [12] to speed up inference by up to 800 times.

While anomaly detection is commonly seen as a separate mode of operation in security inspection [13], in this paper we propose to use a novel approach to classify multiple threat objects in an x-ray image under different cases of class imbalance, in which we utilize a GAN-based anomaly detector coupled with a CNN and an SVM classifier. Inspired by the work in [11], we also adapt a Bi-GAN in our anomaly detector, but we extend it to work on higher dimensional data, i.e. x-ray images, by attaching a CNN in the prior stage, which also reduces the dimensionality of the input to the Bi-GAN. Moreover, aside from the usual adversarial loss, we also impose an additional training objective to the Bi-GAN. Finally, we used two criteria for anomaly detection, which are then used to train an SVM classifier to provide a more robust decision. Experiment results show that this particular ensemble of discriminative and generative models produced significant improvement over baseline

Manuscript received August 17, 2019.
Manuscript revised October 7, 2019.
Manuscript publicized October 23, 2019.
[†]The authors are with the Dept. of Electronics and Communications Engineering, Kwangwoon University, Seoul, South Korea.
a) E-mail: jkmdumagpi@kw.ac.kr (Corresponding author)
DOI: 10.1587/transinf.2019EDL8154

approaches.

2. Proposed Method

In the context of this study, we define a taxonomy of datasets as the following:

- *Practical Dataset* – a dataset that mirrors the same distribution between classes that is to be expected in practice or deployment
- *Ideal Dataset* – a dataset that is used to get the maximum ideal performance of the learning algorithm, which may not be reflective of the distribution that is to be expected in practice or deployment

As described in Fig. 1, our classification network is comprised of a backbone CNN subnetwork, which acts as a classifier and a feature extractor, and an anomaly detector subnetwork that is further composed of a Bi-GAN and an SVM classifier.

In practice or during testing phase, all networks are connected, and they all work together. The extracted features and the output prediction of the CNN will be concatenated and fed into the anomaly detector. If the input is deemed to be non-anomalous, the initial output prediction of the CNN will be suppressed by multiplying it with a small positive number. On the other hand, once determined to be an anomaly, it will be multiplied with 1 to retain its initial values.

During training, the same subnetworks described above are optimized separately by dividing the training into three phases. Figure 2 shows the first phase of training. We attach a Feature Pyramid Network (FPN) to the CNN, which has been proven to increase the accuracy of the network for varying object scales [14]. *L1*, *L2*, *L3*, and *L4* are the convolution layers of FPN. *FC1*, *FC2*, *FC3*, and *FC4* are the fully connected layers of features pooled from each convolution layer of the FPN. *FC5* is the n-dimensional vector representing the classification label predicted by the model. Σ is an average operator, and Y corresponds to the target labels. This discriminative model is only trained on all positive samples, or training images with at least one threat, as well as a random sample of negative samples, or training images without threats. The sample size of the negative samples is set to be the same as the size of the available positive samples. This is the ideal training set for this subnetwork. With this dataset, we eliminate the class imbalance problem and prevent the CNN classifier from being distracted by what would have been a larger number of negative samples. The training objective is the binary cross-entropy loss defined by Eq. (1), where p is the predicted output, y_i is the label for class i, and N is the number of classes.

$$L(p, y) = -\frac{1}{N}\sum_{i=0}^{N} y_i \cdot \log(p(y_i)) + (1 - y_i)\log(1 - p(y_i)) \quad (1)$$

Figure 3 shows the second phase of training, wherein we train a Bi-GAN only on features extracted from negative samples. This is the ideal training set for this subnetwork. With this dataset, the network will only learn to model the characteristics of normal x-ray security images. z is an n-dimensional random noise latent vector where the G samples from to produce new data. x is the input feature vector and + is a concatenation operator. To make the training more efficient, we only use randomly sampled negative images from the training set. The sample size must be large enough to represent the entire negative samples, but not too much at the expense of efficiency. We set this size to 50 000 images. This generative model is trained with the adversarial objective as in [11] defined in Eq. (2), but we add another objective defined in Eq. (3), called reconstruction loss, only to network G to encourage generation of similar features. This will also be used later to determine anomalies along with the feature matching loss defined in Eq. (4).

$$\min_{G,E}\max_{D} V(D, E, G) = \mathbb{E}_{x\sim p_X}\left[\mathbb{E}_{z\sim p_E(\cdot|x)}\left[\log D(x, z)\right]\right] + \mathbb{E}_{z\sim p_z}\left[E_{x\sim p_G(\cdot|z)}\left[1 - \log D(x, z)\right]\right] \quad (2)$$

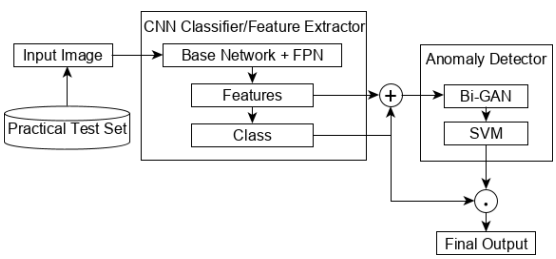

Fig. 1 Classification network

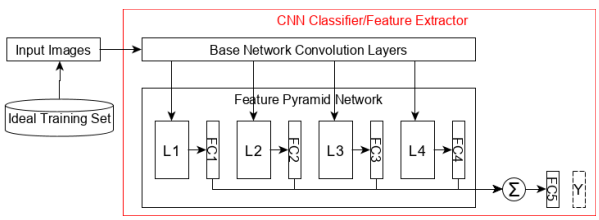

Fig. 2 Training phase 1

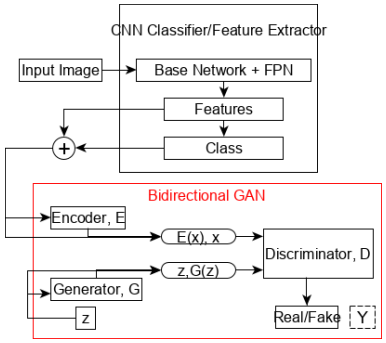

Fig. 3 Training phase 2

$$R_{loss} = \|x - G(E(x))\|_1 \quad (3)$$

$$FM_{loss} = \|f_D(x, E(x)) - f_D(G(E(x)), E(x))\|_2 \quad (4)$$

where f_D are the features extracted from the penultimate fully connected layer of network D.

In theory, GANs should not be able to produce new data that do not belong to the distribution of the input data. Accordingly, our Bi-GAN should not be able to reproduce the input data that contains features of threat objects. Thus, anomalies would result in higher reconstruction and feature matching losses.

Figure 4 shows the final training phase. In here, we propose to train an SVM [15] as a robust alternative to hard thresholding. The input features used to train the SVM are the reconstruction and features matching losses from all the positive training samples and the 50 000 random negative training samples that were used in the previous phase.

It is essential that we divide the training into three phases because the performance of each network depends on how well the preceding network has been trained. Therefore, the training of the backbone CNN ultimately determines the overall performance of the entire classification network. This is the reason that it is important to only train the CNN on an ideal training set. In this manner, the CNN will be focused on learning strong representations of the target threat objects, thereby accurately discriminating between features of positive and negative samples. As a consequence, the CNN has also gained an assumption that the there is an equal distribution of positive and negative samples. This will cause for an increase in false positives during classification. As a countermeasure, we used an anomaly detector composed of a Bi-GAN and an SVM classifier. We trained our Bi-GAN on the strong features, learned by the pre-trained CNN, to model the manifold of the features describing negative samples even when they had been wrongly classified as positive samples. Now, it is apparent that the training of the SVM is highly dependent on the success of the previous two networks. As the backbone CNN learns strong representations of the target threat objects and the Bi-GAN learns the underlying distribution of the negative samples, the SVM will then be optimized to find the best separation of anomalous and non-anomalous inputs. Output predictions on non-anomalous inputs can then be suppressed, thereby evading the increase of false positives.

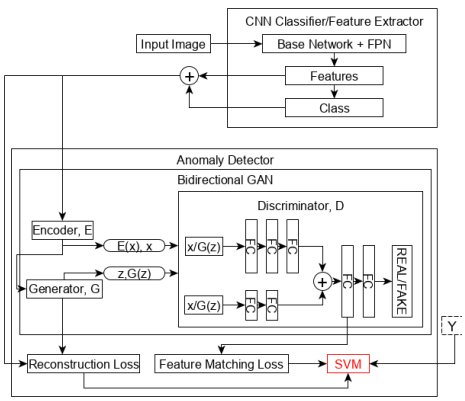

Fig. 4 Training phase 3

3. Experiment Results

We evaluate our network on SIXray – the largest public benchmark dataset on x-ray security images [8]. This dataset is divided into three subsets defined as the following:

- *SIXray10* – 10% of the dataset are positive samples
- *SIXray100* – 1% of the dataset are positive samples
- *SIXray1000* – 0.1% of the dataset are positive samples

We adapt the evaluation metric used in the PascalVOC image classification task [16], wherein the average precision for each class is calculated by ranking all the test data by the confidence of containing a particular threat and taking the mean (mAP) to assess the effectiveness of the model as a whole. We implement our approach using Pytorch [17] (v1.1.0 with Python 3.6.8) on a single machine with Intel Xeon processor and NVIDIA Tesla T4 GPU.

Table 1 shows the classification mAP of the networks on the SIXray10 subset. Our approach shows significant improvement over both unmodified CNN and CHR [8]. The same outcome can be observed in Table 2 showing results on the SIXray100 subset. This subset is the one with the closest distribution to the real-world scenario. In this subset, we obtain significant enhancement over both baselines in all

Table 1 Classification mAP (%) on SIXray10 subset

Method	Gun	Knife	Wrench	Pliers	Scissors	mean
ResNet34 [2]	89.71	85.46	62.48	83.5	52.99	74.83
ResNet34+CHR [8]	87.16	87.17	64.31	85.79	61.58	77.20
(Ours) ResNet34+GBAD	92.88	87.25	78.95	85.62	65.48	**82.04**
ResNet50 [2]	90.64	87.82	63.62	84.8	57.35	76.85
ResNet50+CHR [8]	87.55	86.38	69.12	85.72	60.91	77.94
(Ours) ResNet50+GBAD	92.3	84.76	75.48	84.22	65.18	**80.39**
ResNet101 [2]	87.65	84.26	69.33	85.29	60.39	77.38
ResNet101+CHR [8]	85.45	87.21	71.23	88.28	64.68	79.37
(Ours) ResNet101+GBAD	93.76	89.74	77.08	85.21	65.56	**82.27**
InceptionV3 [3]	90.05	83.8	68.11	84.45	58.66	77.01
InceptionV3+CHR [8]	88.9	87.23	69.47	86.37	65.5	79.49
(Ours) InceptionV3+GBAD	90.51	78.77	78.46	82.61	67.41	**79.55**
DenseNet [4]	87.36	87.71	64.15	87.63	59.95	77.36
DenseNet+CHR [8]	87.05	85.89	70.47	88.34	66.07	79.56
(Ours) DenseNet+GBAD	92.09	91.36	76.65	89.26	67.28	**83.33**

Table 2 Classification mAP (%) on SIXray100 subset

Method	Gun	Knife	Wrench	Pliers	Scissors	mean
ResNet34 [2]	83.06	78.75	30.49	55.24	16.14	52.74
ResNet34+CHR [8]	81.96	77.7	36.85	64.56	14.49	55.11
(Ours) ResNet34+GBAD	86.13	80.31	43.57	48.95	32.99	**58.39**
ResNet50 [2]	84.75	77.92	28.49	50.53	19.39	52.22
ResNet50+CHR [8]	82.64	79.6	41.19	58.02	27.89	57.87
(Ours) ResNet50+ GBAD	82.85	77.66	46.05	52.94	33.21	**58.54**
ResNet101 [2]	82.83	76.16	35.59	54.82	20.63	54.01
ResNet101+CHR [8]	83.25	77.53	42.02	68.01	32.33	60.63
(Ours) ResNet101+GBAD	84.06	84.35	49.86	50.08	39.14	**61.50**
InceptionV3 [3]	81.18	77.28	32.47	66.89	22.63	56.09
InceptionV3+CHR [8]	79.22	73.48	37.2	69.01	31.81	58.14
(Ours) InceptionV3+GBAD	79.94	81.66	43.3	52.18	38.65	**59.15**
DenseNet [4]	83.23	77.24	37.72	62.69	24.89	57.15
DenseNet+CHR [8]	82.06	78.75	43.22	66.75	28.8	59.92
(Ours) DenseNet+GBAD	81.2	85.08	45.09	56.2	44.43	**62.40**

Table 3 Classification mAP (%) on SIXray1000 subset

Method	Gun	Knife	Wrench	Pliers	Scissors	mean
ResNet34 [2]	72.05	56.42	16.47	14.24	7.12	33.26
ResNet34+CHR [8]	73.35	60.46	23.72	17.98	18.19	38.74
(Ours) ResNet34+GBAD	76.64	66.26	13.67	18.63	19.97	**39.03**
ResNet50 [2]	74.19	59.82	16.03	16.59	2.87	33.90
ResNet50+CHR [8]	73.43	61.32	18.88	12.32	19.03	37.00
(Ours) ResNet50+ GBAD	72.59	70.02	18.45	20.82	21.01	**40.58**
ResNet101 [2]	76.04	63.53	13.65	15.57	11.28	36.01
ResNet101+CHR [8]	75.38	64.8	15.27	19.02	16.21	38.14
(Ours) ResNet101+GBAD	74.54	67.66	16.27	21.57	23.94	**40.80**
InceptionV3 [3]	75.52	56.33	24.01	16.75	20.72	38.67
InceptionV3+CHR [8]	76.91	61.29	29.6	19.11	47.56	**46.89**
(Ours) InceptionV3+GBAD	76.19	54.6	25.54	23.91	21.29	40.31
DenseNet [4]	75	65.55	23.57	18.09	14.18	39.28
DenseNet+CHR [8]	74.87	71.23	29.79	21.57	44.27	**48.35**
(Ours) DenseNet+GBAD	71.31	66.15	24.91	19.57	23.6	41.11

cases, which validates our aim to develop an algorithm that can be useful in a practical setting.

Compared to plain CNNs [2]–[4], our approach works significantly better due to the elimination of class imbalance during the training of the classifier supported by suppression of false positives using the anomaly detector. Furthermore, we achieve substantial improvement because our generative model receives stronger direct supervision during training, whereas the supervision signals of the generative models in [8] are weakened by their indirect hierarchical approach. Finally, overall evaluations for the SIXray1000 subset, shown in Table 3, demonstrate the effectiveness of our network even under extreme class imbalance.

To our knowledge, this is the first time that a GAN-based anomaly detection algorithm coupled with classification learning algorithms were used to solve extreme class imbalance problem. Moreover, GAN-based anomaly detection has been recently used high dimensional x-ray images. In [18], Ackay et al. showed that anomaly detection could be done on x-ray images using a combination of subnetworks that are trained in an adversarial manner. In their recent work in [19], they improve the performance of their model by employing skip connections that directly transfer the information between the layers of the subnetworks. Figure 5 and Fig. 6 shows the comparison between the existing GAN-based anomaly detection algorithms using different metrics.

We used the SIXRay100 subset and divided it into positive and negative samples as previously defined. The task of the model is to determine if an image contains at least one of any type of threat described in Tables 1, 2 and 3. Although both graphs show that our approach outperforms previous methods, a significant gap in performance can be observed when using the area under the PR curve. This is because a PR curve can provide a more informative assessment compared to the ROC curve especially when the dataset is highly imbalanced [7]. Furthermore, we calculate the precision, recall and F1 score by taking the unweighted average of the positive and negative class for each of these metrics. Table 4 shows that our approach has a better balance between precision and recall, thus achieving the best F1 score against the previous methods.

Table 5 shows the multi-label confidence output of our model for the corresponding sample images shown in Fig. 7.

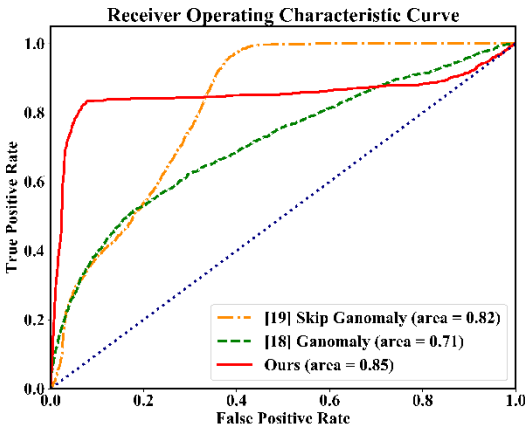

Fig. 5 Comparison of GAN-based anomaly detection algorithms using the area under the Receiver Operating Characteristic (ROC) curve

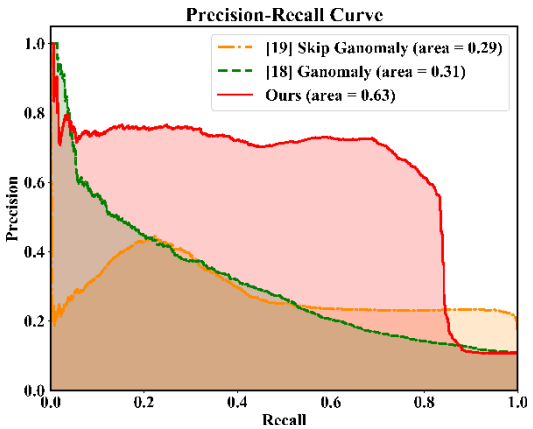

Fig. 6 Comparison of GAN-based anomaly detection algorithms using the area under the Precision-Recall (PR) curve

Table 4 Comparison of GAN-based anomaly detection algorithms on SIXRay100 subset

Method	Precision	Recall	F1 Score
Skip Ganomaly [19]	63.88	55.19	56.51
Ganomaly [18]	**90.48**	51.10	49.41
(Ours) ResNet34+GBAD	81.22	**86.05**	**83.39**

Table 5 Multi-label confidence scores for example images in Fig. 7

Image	Gun	Knife	Wrench	Pliers	Scissors
A	7.4487e-04	3.0811e-08	4.6111e-04	**1.0000e+00**	1.5124e-07
B	**1.0000e+00**	2.9331e-06	9.2091e-07	1.0342e-05	3.4970e-07
C	2.6836e-06	3.1150e-07	**9.6420e-02**	**6.5551e-02**	5.1200e-06
D	2.2917e-09	2.6501e-10	7.0631e-18	3.2918e-12	9.6866e-22
E	2.3883e-08	2.3716e-05	1.9670e-09	7.1067e-07	9.3649e-07
F	1.2351e-09	4.2260e-08	1.6501e-11	2.9173e-05	2.0720e-08

Images A, B, and C are sampled from the positive samples, whereas D, E, and F are sampled from the negative samples. A confidence score of 1 conveys that the model is certain that a particular threat is detected, while a confidence score of 0 conveys that the model is certain that there is not a single threat in the image. Our model gives very low confidence scores to the images D, E, and F, as should be expected. Correspondingly, our model is certain that a particular threat is present in images A and B. However, our model

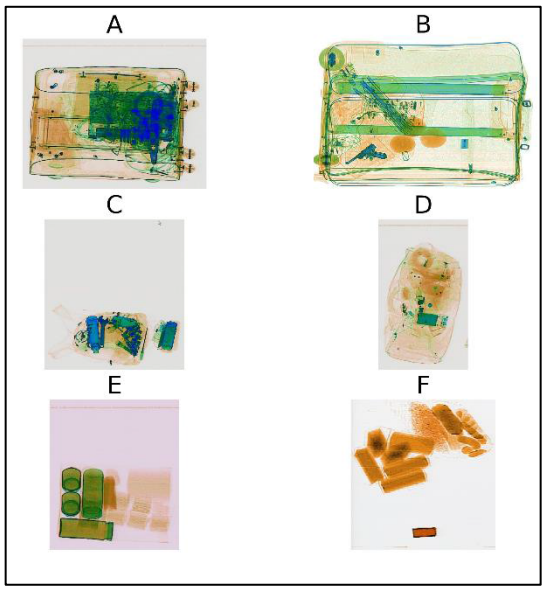

Fig. 7 Example images from the SIXRay dataset

exhibits uncertainty on image C. A possible reason for this behavior is that the area of interest in image C is relatively small compared to the area of the whole image. During the pre-processing stage, where the image undergoes transformations to be suitable as input to the network, much of the necessary information may be lost. This, in turn, opens another possibility for the further improvement of the algorithm.

4. Conclusion

In this study, we presented a novel method for multiple threat object classification, which employs a GAN-based anomaly detection approach together with a CNN classifier, to alleviate the class imbalance problem. We train our network in three phases. In phase 1, we maximize the true positive rate of the classifier by training on the ideal train set. In phase 2, we train a Bi-GAN to learn the distribution of negative samples. In phase 3, we train an SVM on the reconstruction and feature matching losses as a robust alternative to hard thresholding. Initial classification results on detected normal images are suppressed to reduce false positives when evaluating the practical test set. We evaluated on a dataset that closely mirrors the real-world scenario and empirical results show that our approach enhances classification under varying cases of class imbalance. Further research includes improving the overall performance of our current model and extending this method to analyze even higher dimensional data such as video, for applications such as surveillance systems.

Acknowledgments

This work was supported by Kwangwoon University and by the MISP Korea, under the National Program for Excellence in SW (2017-0-00096) supervised by IITP.

References

[1] G. Zentai, "X-ray imaging for homeland security," Proc. IEEE Int. Workshop Imaging Syst. Tech. (IST), Chania, Greece, pp.1–6, 2008.
[2] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, pp.770–778, 2016.
[3] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the Inception Architecture for Computer Vision," Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, pp.2818–2826, 2016.
[4] G. Huang, Z. Liu, L.V.D. Maaten, and K.Q. Weinberger, "Densely Connected Convolutional Networks," Proc. IEEE Conf. Comput. Vis. Pattern Recognit (CVPR), Honolulu, HI, pp.2261–2269, 2017.
[5] D. Mery, E. Svec, M. Arias, V. Riffo, J.M. Saavedra, and S. Banarjee, "Modern Computer Vision Techniques for X-Ray Testing in Baggage Inspection," IEEE Trans. Syst., Man, Cybern. Syst., vol.47, no.4, pp.682–692, 2017.
[6] S. Ackay, M.E. Kundegorski, C.G. Willcocks, and T.P. Breckon, "Using Deep Convolutional Neural Network Architectures for Object Classification and Detection within X-Ray Baggage Security Imagery," IEEE Trans. Inf. Forensics Security, vol.13, no.9, pp.2203–2215, 2018.
[7] H. He and E.A. Garcia, "Learning from Imbalanced Data," IEEE Trans. Knowl. Data Eng., vol.21, no.9, pp.1263–1284, 2009.
[8] C. Miao, L. Xie, F. Wan, C. Su, H. Liu, J. Jiao, and Q. Ye, "SIXray: A large-scale security inspection x-ray benchmark for prohibited item discovery in overlapping images," Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Long Beach, CA, 2019.
[9] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," Advances in Neural Information Processing, pp.2672–2680, 2014.
[10] T. Schlegl, P. Seeböck, S.M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery," Information Processing in Medical Imaging, 2017.
[11] H. Zenati, C.-S. Foo, B. Lecouat, G. Manek, and V. Chandrasekhar, "Efficient GAN-based anomaly detection," Int. Conf. Learning Representations (ICLR), 2018.
[12] J. Donahue, P. Krahenbuhl, and T. Darrel, "Adversarial feature learning," Int. Conf. Learning Representations (ICLR), 2017.
[13] L.D. Griffin, M. Caldwell, J.T.A. Andrews, and H. Bohler, ""Unexpected Item in the Bagging Area": Anomaly Detection in X-Ray Security Images," IEEE Trans. Inf. Forensics Security, vol.14, no.6, pp.1539–1553, 2019.
[14] T. Lin, P. Dollár, R. Girshick, K. He, B. Hariharan, and S. Belongie, "Feature Pyramid Networks for Object Detection," Proc. IEEE Conf. Comput. Vis. Pattern Recognit (CVPR), Honolulu, HI, pp.936–944, 2017.
[15] B.E. Boser, I.M. Guyon, and V.N. Vapnik, "A training algorithm for optimal margin classifiers," Proc. 5th Annual Workshop Computational Learning Theory, pp.144–152, 1992.
[16] M. Everingham, L.V. Gool, C.K.I. Williams, J. Winn, and A. Zisserman, "The PASCAL Visual Object Classification (VOC) Challenge," Int. J. Comput. Vis., vol.88, no.2, pp.303–338, 2010.
[17] A. Paszke, S. Gross, S. Chintala, G. Chanan, E. Yang, Z. DeVito, Z. Lin, A. Desmaison, L. Antiga, and A. Lerer, "Automatic differentiation in pytorch," NIPS Autodiff Workshop, 2017.
[18] S. Ackay, A. Atapour-Abarghouei, and T.P. Breckon, "Ganomaly: Semi-supervised anomaly detection via adversarial training," in Asian Conf. Computer Vision (ACCV), pp.622–637, 2018.
[19] S. Ackay, A. Atapour-Abarghouei, and T.P. Breckon, "Skip-GANomaly: Skip Connected and Adversarially Trained Encoder-Decoder Anomaly Detection," in Int. Joint Conf. Neural Networks (IJCNN), 2019.