MaxPix: detecting GAN-generated images by emphasizing local maxima

Abstract: The realistic images generated by GANs(Generative Adversarial Networks) enrich people's lives, but they also pose serious threats to personal privacy and society, and it has become essential to study algorithms that can accurately detect GAN-generated images. Existing studies use artifacts to detect GAN-generated images, but the artifacts present in different GAN-generated images vary widely, and thus the cross-model generalization performance of such algorithms is weak. In this thesis, we propose the MaxPix, a new algorithm based on the combination of statistical features and deep learning techniques, for generating image detection. MaxPix firstly obtains the filter map of the image by designing MaxSel filtering algorithm, and then designs MA Block embedded in ResNet (Residual Network) to obtain MResNet. MaxPix finally utilizes MResNet to extract features from the filter map to detect GAN-generated images. Experimental results on publicly available datasets such as Wang and Faces-HQ show that the detection accuracy of MaxPix reaches 85.9% and 99.6% on average, which improves 7.6% and 10.2% relative to state-of-the-art algorithms such as NAFID and GocNet, and has strong cross-model generalization performance.

Keywords: gan; generative images; artifacts; cross-model generalization

0 Introduction

Digital images have become one of the main carriers for transmitting network information due to the advantages of diverse contents and convenient storage, and have been widely used in the fields of news, information, medical diagnosis, and identification, etc. GANs[1] (Generative Adversarial Networks) is a generative model based on deep learning technology, which was proposed by Ian Goodfellow et al. GAN consists of a generator and a discriminator, in which the generator can generate samples similar to real data. Until now, more than a hundred different GANs capable of generating images have been produced, and these generated images have enriched people's lives. However, some people maliciously use GANs to forge images and abuse them in politics and pornography, posing a serious threat to personal privacy and society. Since digital images are widely used in various fields, their authenticity is very important. In order to prevent GAN-generated images from being abused and bringing harm to the society, effective detection algorithms are needed to detect whether images are generated by GAN or not, so as to help people correctly distinguish real images from generated images. Currently, researchers have proposed a large number of detection algorithms to detect GAN-generated images. These algorithms are mainly categorized into detection algorithms based on traditional digital image forensic methods and detection algorithms based on deep learning techniques.

In the detection algorithms based on traditional digital image forensics, researchers mainly design detection algorithms to detect generated images based on the properties of digital images such as illumination inconsistency, statistical properties in the spatial domain and frequency domain. McCloskey[3]. analyzed the process of color formation in images and argued that the normalization process present in GAN restricts the range of pixels in the generated image, making the exposure of the generated image different from that of a real image differently. They proposed to use the measured frequency of overexposure and underexposure of the image as a feature to detect the generated image. However, the algorithm only achieves an AUC (Area Under Curve) value of 0.7. Durall[4] found that the high-frequency components of the generated images are distorted and proposed to use the azimuthal integral of the image as a feature to detect the generated images through the support vector machine, which achieves 100% accuracy. However, the algorithm lacks cross-model generalization performance. Guo[5] believed that the eye pupils in real face images are elliptical, while the eye pupils in generated face images are irregular. They proposed an algorithm to determine whether an image belongs to a generated image or not by calculating the IoU[6] values of the pupil region and the elliptical mask and judgied whether the image belongs to a generated image by the IoU value. This algorithm has strict requirements on the quality and angle of the image, and if there are defects in the human physiology, it will make the algorithm misjudged. Liu[7] used the Sobel operator to get the gradient of the image in HSV (Hue, Saturation, Value) space and count histograms of the gradient distribution as a feature to detect the generated images. Algorithm achieved 99.4% accuracy when detecting the images generated by PGGAN[8], but cross-model generalization performance was not investigated.

Detection algorithms based on traditional image forensics have theoretical and experimental foundations. However, such algorithms are highly susceptible to overfitting statistical features that exist only in the trainset, while different GAN-generated images have different statistical features and thus tend to have lower accuracy in detecting unknown GAN-generated images. In addition, These algorithms require the images to conform to a specific angle and quality, which also limits the application of the algorithms.

Detection algorithms based on deep learning techniques utilize neural networks to construct algorithmic models and learn general features from massive data to detect the generated images. Since neural networks have strong representational ability, these algorithms generalizes well and attracts many scholars to study. The up-sampling process is almost common to GANs. Zhang[9] designed AutoGAN containing an up-sampling process to generate a large number of images that simulate a variety of generated images and used such images to train the algorithm. However, the detection accuracy of the algorithm will be severely degraded if the up-sampling method used by the GAN is significantly different from that used by AutoGAN. Liu[10] found that the phase spectrum of the image retains rich frequency components and proposed to combine the image spatial domain features and the phase features to detect the generated images. The algorithm detects the two Deepfake datasets[11,12] obtaining an accuracy rate of 91.5% and 76.88%. Jeong[13] proposed an algorithm that uses a high-pass filter to remove irrelevant features in the spatial domain and frequency domain for highlighting the important features to detect the generated image, which obtains more than 72% cross-model detection accuracy and average precision. Tian[14] divided the image frequency components into low, medium, and high components, and then aggregated the features with the original image. They utilized the aggregated features to detect the generated image and obtains an accuracy of 97.74%. Wang[15] used wavelet transform to transform the image in the spatial domain to the frequency domain, then extracted the high frequency components in the image and fused the features with the original image. Algorithms detected the generated image by Xception[16] and achieved more than 98% accuracy, but the accuracy of detecting the low-quality image is lower. Miao[17] designed the Center Differential Attention Transformer to make the algorithm learn global high frequency information and local fine-grained features and designed a high frequency wavelet sampler to make the algorithm extract multi-channel high frequency features. The proposed algorithm aggregated the two features to detect the generated image, but the accuracy of detecting the compressed processed image is low.

Algorithms based on deep learning techniques generally need to utilize the artifacts which brought by the imperfect design of the GAN to detect the generated images. However, with the improvement of the GAN structure, the obvious artifacts in the generated images have been effectively hidden. In addition, the artifacts generated by different GANs vary, which limits the generalization performance of artifact-dependent detection algorithms, resulting in low accuracy when detecting unknown GAN-generated images and a lack of generality of the algorithms.

In view of this, this thesis proposes to investigate detection algorithms that do not need to utilize artifacts to detect the generated images. In this thesis, the pixel value distribution of the GAN-generated images that generated by GAN such as StarGAN[18], StyleGAN2[19], and real images in the datasets such as FFHQ[20] , CelebA are counted, and it is observed that the generated images cannot reproduce the pixel distribution of the real images, and there are more points with larger pixel values in the real images than in the generated images. Therefore, this thesis proposes MaxPix detection algorithm based on statistical features. Firstly, this thesis proposes MaxSel algorithm for performing filtering on the image, and then designs MA Block embedded in ResNet to form MResNet, which is used to extract features from the filtered image to detect the generated image. Numerous experiments show the effectiveness of MaxPix for detecting generated images. The contribution of this thesis is as follows:

Based on the characteristic that GAN-generated images cannot reproduce the pixel value distribution condition of real images, MaxPix detection algorithm is proposed to detect GAN generated images and MaxSel is proposed for filtering images.

MaxPix detects the Wang[21] dataset and the Faces-HQ[4] dataset with an average accuracy of 85.9% and 99.6%, which is an improvement of 7.6% and 10.2% compared to current state-of-the-art detection algorithms. Thus the MaxPix has strong cross-model generalization performance.

1. Algorithm description

Durall[4] found that GAN-generated images cannot reproduce the spectral distribution of real images. He[22] found that the generated images have stronger nonlocal similarity than real images, which inspired this thesis to explore whether there is any difference in the pixel distribution between the generated and real images.

For this purpose, the frequency of image pixel values in each pixel value range is counted and displayed using histograms in this thesis.

In the experiment, the range of pixel values was divided into 60 groups. The experiments counted a total of 34k images including images generated by BigGAN[23], StarGAN and StyleGAN2, and real images samplied from ImageNet[24], CelebA and FFHQ datasets, which are from Wang dataset[21] and Faces-HQ[4]. As shown in Fig.1, although the above mentioned GANs are trained with a large number of real images, it is still difficult to mimic the distribution of pixel values of real images. Obviously, there are more points in the larger pixel value range in the real image than in the generated image. Therefore, this thesis proposes the MaxPix detection algorithm, which detects the generated image by emphasizing the local maxima of the image and using the maxima features.

2. Algorithmic framework

As show in Fig.2, the MaxPix structure consisting of a filtering module (or feature select module), a feature extraction network MResNet, and a classifier C. The filtering module is a feature extraction network. The filtering module uses the MaxSel filtering algorithm proposed in this thesis to perform filtering on the image, making it easy for MResNet to learn distinguishable features to detect GAN-generated images.

2.1 MaxSel Filter

MaxPix uses the convolution kernel as in equation (1) as a filter kernel to perform convolution operation with the image to obtain the filtered image. First, MaxPix splits the image channel-by-channel and performs the convolution operation using four convolution kernels to obtain the convolution values *X*(*c,i,j*) (*α1, α2 ,α3 ,α4* ) in four directions for each point of the three channels. Then, MaxSel compares the convolutional values of the 4 directions at the corresponding location within the group and takes the largest convolutional value among them as the filter value. For *X*(*c,i,j*)(*α1, α2 ,α3 ,α4* ), the maximum value is selected from *α1, α2 ,α3* and *α4* .

As shown in Equation(2), where *X*(*c,i,j*) denotes the filter value at the position (*i,j*) of the image *c* channel. The filter value of each point constitutes the filter map of that channel. MaxSel splices the filter maps of the three channels to form the filter map *Fin*∈*R*3×*H*×*W* .

As shown in Fig.3, the first column is the real image from the Wang[21] dataset; the second column is the filter map obtained by using the Prewitt operator as the convolution kernel; the third column is the filter map obtained by taking the Laplacian operator as the convolution kernel and the fourth column is the filter map obtained by using MaxSel. Obviously, the filter map obtained by MaxSel is delicate and complete in details, which is favorable for the algorithm to learn more complete features from it.

2.2 MResNet feature extraction network

As shown in Fig.4, MResNet is improved from ResNet and has five more MA blocks, which consists of a maximum pooling filter layer, a mean filter layer and a residual layer, than ResNet. MResNet changes the mean pooling of the final output to maximum pooling, which is used for selecting the maximum features for detecting the generated image.

MA block is used to emphasize the local maxima in the feature map as shown in equation (3), where λ is an updatable parameter. *Fin* denotes the input features. *MP* denotes maximum pooling. *AP* denotes mean filtering. *Abs* denotes taking absolute values.

2.3 Classifiers and Loss Functions

The classifier C consists of two fully connected layers. MaxPix spreads the 8192 features output from MResNet and then transforms them into predicted values using the fully connected layers. As shown in Equation(4), where C is the classifier, *y* denotes the true label of the images, and *Fd* are the input features.

3 Experimental

This thesis demonstrates the improvement of MaxPix in cross-model generalization performance by comparing the accuracy and average precision of current representative detection algorithms for detecting different datasets. The role of MaxPix modules is verified through ablation experiments.

3.1 Datasets

In order to avoid misunderstanding in expression, this thesis uses the lowercase English name of the generative model to denote the dataset composed of the corresponding generated image and the real image, e.g., the image generated by StyleGAN and the real image used for training the generative model are called the stylegan dataset.

The Wang dataset: Wang[21] published a publicly available but unnamed dataset, referred to as the Wang dataset in this thesis, which is divided into a trainset, an evaluation set, and a testset and contains real images and generated images. The real images were samplied from the LSUN[25] , ImageNet dataset and other datasets that are commonly used to train GANs. The generated images including 20 scenarios images were generated by GANs such as PGGAN, StyleGAN2 and samplied from the fake face dataset FaceForensics++ (deepfake)[26] . This dataset has been widely used by related researchers[13,21,27-30] to train and evaluate detection algorithms since its release.

The Faces-HQ: Durall[4] released the Faces-HQ dataset. Each image in the Faces-HQ dataset has a resolution of 1024×1024, which is much better than that of the Wang dataset. Faces-HQ contains 20k real face images which sample from CelebA-HQ[8] and FFHQ, and contains 20k generated images which sample from the 100K Faces project[31] and www.thispersondoesnotexist.com. The generated images are generated by StyleGAN and StyleGAN2. CelebA-HQ and FFHQ are often used to train GANs, which are recognized datasets for training and testing detection algorithms.

In this thesis, the person subset of the Wang trainset is used to train PixMSE and the biggan, gaugan, stargan subsets of the the Wang testset and the Faces-HQ total more than 102k images are used as testsets.

3.2 Experimental environment

In this thesis, the algorithm code is written with python 3.7 and PyTorch 1.9.0, the GPU used is RTX 3090 and the system used is Ubuntu. MaxPix performs resize as well as random cuts on the trainset and resize as well as center cuts on the testset, which changes the input image into *X*∈*R*3×299×299.

The training algorithm is set up with the epoch of 36, the batch-size of 4. The optimizer is Adam. The learning rate is 0.00005. The learning decay rate is 0.96 and the loss function is CrossEntropyLoss.

3.3 Comparative Experiments

In this thesis, we select research works that have achieved high accuracy in the task of detecting GAN-generated images in recent years for comparison, including Wang[21], Frank[32], Durall[4], Jeong[13,27], He[22], Deng[33] and Guo[34]. These algorithms have achieved better performance in their respective thesis and can achieve more than 90% accuracy in detecting the same type of GAN-generated images, while maintaining a strong cross-model generalization performance.

Except for the algorithm of Jeong[13,27] , the rest of the algorithms in this thesis were retrained and tested using the Wang dataset. Since the algorithm of Jeong[13,27] uses the Wang dataset and the code implementation details are not available, the experimental data in the table are quoted from the literature[27].

As shown in table1, MaxPix achieves high accuracy for detecting biggan, cyclegan, stargan, and stylegan datasets, which are higher than the highest values achieved among the compared algorithms. In particular, Comparing to compared algorithms, MaxPix achieves an accuracy improvement of 6.1% for detecting biggan and 11.6% for detecting stylegan. MaxPix, like most of the compared algorithms, achieves a lower accuracy of 63% for detecting the gaugan dataset. In terms of average precision performance, MaxPix detects gaugan with an average precision of 75.5%, which is lower than the best of the compared algorithms at 97.6%. However, MaxPix detects the remaining seven datasets all get highest average precision, equaling or exceeding the best of the compared algorithms. It can be seen that the detection performance of MaxPix is better than the current mainstream detection algorithms in terms of accuracy and average precision.

As shown in table2, the average precision and accuracy of the algorithms for detecting the Faces-HQ dataset varies significantly. Since the implementation details of the Jepong [13,27] algorithm are not available, these two algorithms are not involved in the table2. Despite the fact that the training and testing are from two different datasets with a huge difference in image resolution and the algorithms are not retrained in this thesis, MaxPix still performs well, obtaining 99.9% and 99.3% detection accuracy and 100% and 99.9% average precision, respectively, which are better than the comparison algorithms. This indicates that MaxPix detection accuracy and average precision are less affected by image size.

In addition, in Fig.5, the images in the Wang dataset have obvious artifacts, while the images in Faces-HQ have no obvious artifacts. This also indicates that the detection accuracy of MaxPix is less affected by artifacts. Comparison experiments show that the accuracy and average precision of MaxPix detection algorithms can match or exceed current state-of-the-art detection algorithms, with strong cross-model generalization performance.

3.4 Ablation experiments

This thesis explores the role of MaxSel filtering and MA Block through ablation experiments. The modular ablation experiments use ResNet as a benchmark for comparison. ‘ResNet’ takes the unfiltered image as the input to ResNet. ‘MResNet’ takes the unfiltered image as the input to MResNet , which explores the role of MaxSel. ‘MSel’ filters the image through MaxSel and uses it as input to ResNet to explore the role of MA Block.

3.4.1 Module ablation experiments

As shown in table3, ResNet only detects stylegan2 and progan with more than 80% accuracy and more than 90% average precision. MResNet does not improve the accuracy and average precision of detecting the generated images despite the addition of MA Block, meaning MA Block alone does not improve the algorithm's performance. Due to the adoption of MaxSel for filtering the image, which makes it easy for the algorithm to learn distinguishable features from the filtered images, thus the detection accuracy and average precision of MSel are comprehensively improved, especially for detecting deepfake, which improves the accuracy by 40.5% and the average precision by 47.9%. MaxPix introduces MA Block on the basis of Msel to detect progan, biggan, cyclegan, gaugan and stylegan2 with 0.1%, 2.8%, 16.5%, 8.3%, and 0.1% accuracy improvements, respectively. There is a slight decrease in the average precision of MaxPix in detecting deepfake. It can be seen that Maxsel used with MA Block effectively improves the accuracy and average precision of the detection algorithm in detecting the generated images and it is the Maxsel filter that plays the biggest role.

3.4.2 Network structure ablation experiments

In this ablation experiment, filtered images obtained by different filtering algorithms,such as Laplacian, Sobel, Prewitt and Scharr, are used as inputs for MResNet and ResNet to further explore the need for the proposed MaxSel filtering algorithm.

As shown in tables4 and table5, the detection algorithm uses Maxsel to filter the images and achieves the highest accuracy and average precision on multiple datasets regardless of whether MResNet or ResNet is used as the network architecture. Especially for the detection of stargan, which algorithm consistently achieves 100% accuracy and average precision. The accuracy for the detection of gaugan is consistently lower, at 63% and 54.7%, and the average precision were only obtained as 75.5% and 63.5%. However, even when the image is filtered using other operators, the detection algorithm has a low accuracy and average precision for detecting gaugan with maximum accuracy of 70.3% and average precision of only 80%. This indicates that by filtering the image, it is less helpful to improve the accuracy and average precision of algorithm when detecting gaugan.

Overall, the two ablation experiments show that Maxsel and MA Block are more helpful in improving the accuracy and average precision of the algorithms to detect the GAN-generated images, especially Maxsel filtering can efficiently improve the generalization performance of the detection algorithms.

4 Conclusion

This thesis propose MaxPix for detecting GAN-generated images, an algorithm that produces features for detecting generated images by emphasizing the maximum value in the local range of the image. The main contribution of this thesis is to propose MaxSel filtering algorithm and MaxPix detection algorithm. Comparison experiments on Wang and Faces-HQ datasets show that MaxPix outperforms the state-of-the-art algorithms such as Deng[33] and Guo[34] in terms of generalization performance, and ablation experiments validate the importance of MaxSel and MA Block in improving the detection accuracy and average precision of the detection algorithms. The research in this thesis provides reference for the detection of GAN-generated images.