electronics

MDPI

Article

A Detection Method for Social Network Images with Spam, Based on Deep Neural Network and Frequency Domain Pre-Processing

Hua Shen [1,2,3], Xinyue Liu [2] and Xianchao Zhang [2,*]

[1] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China; huashen.cn@gmail.com
[2] School of Software, Dalian University of Technology, Dalian 116620, China; xyliu@dlut.edu.cn
[3] College of Mathematics and Information Science, Anshan Normal University, Anshan 114007, China
* Correspondence: xczhang@dlut.edu.cn

Abstract: As a result of the rapid development of internet technology, images are widely used on various social networks, such as WeChat, Twitter or Facebook. It follows that images with spam can also be freely transmitted on social networks. Most of the traditional methods can only detect spam in the form of links and texts; there are few studies on detecting images with spam. To this end, a novel detection method for identifying social images with spam, based on deep neural network and frequency domain pre-processing, is proposed in this paper. Firstly, we collected several images with embedded spam and combined the DIV2K2017 dataset to build an image dataset for training the proposed detection model. Then, the specific components of the spam in the images were determined through experiments and the pre-processing module was specially designed. Low-frequency domain regions with less spam are discarded through *Haar* wavelet transform analysis. In addition, a feature extraction module with special convolutional layers was designed, and an appropriate number of modules was selected to maximize the extraction of three different high-frequency feature regions. Finally, the different high-frequency features are spliced along the channel dimension to obtain the final classification result. Our extensive experimental results indicate that the spam element mainly exists in the images as high-frequency information components; they also prove that the proposed model is superior to the state-of-the-art detection models in terms of detection accuracy and detection efficiency.

Keywords: social networks; images with spam; *Haar* wavelet transform; feature extraction module

Citation: Shen, H.; Liu, X.; Zhang, X. A Detection Method for Social Network Images with Spam, Based on Deep Neural Network and Frequency Domain Pre-Processing. *Electronics* **2022**, *11*, 1081. https://doi.org/10.3390/electronics11071081

Academic Editors: Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag

Received: 7 March 2022
Accepted: 28 March 2022
Published: 29 March 2022

1. Introduction

Digital images are widely utilized in various social networks such as WeChat or Facebook, due to their convenience, fast acquisition, and abundance of redundant information [1–6]. While digital images bring convenience to people's lives, some security risks also follow. To receive free advertising and for other more harmful purposes, some criminals paste links, text, and additional pictures on images that seriously disrupt the order and security of social networks. Therefore, finding ways to accurately and quickly detect images containing spam is a huge challenge for researchers [7–10]. This research field is also of great significance for purifying social networks and improving the security of the social network environment.

In the past few decades, most research has focused on how to detect target objects, such as links, emails, texts, etc., and research on detecting images that include spam is still very rare. Zhu et al. [11] proposed a supervised matrix factorization method with social regularization (SMFSR) for spammer detection in social networks. Their method realized the detection task by combining the user's social behavior and social relationships, detecting some data from Renren.com and obtaining relatively good detection results. Hu

et al. [12] focused on studying how to use network and content information together in Weibo to perform effective social spam detection. In addition, an optimization formula is designed to combine social network and content information for optimizing the model. The experimental results also show that their model can achieve good detection results on Twitter. Wu et al. [13] proposed a unified detection method for the collaborative combination of social spammers and spam messages on Weibo. Their approach combines social spam detection with spam detection exploiting the publishing relationship between the users and the message. Furthermore, an optimization schedule is introduced to improve the capability of their model, and an acceleration strategy is also proposed to improve the detection efficiency of the model. Chen et al. [14] analyzed the vulnerabilities of current detection methods from the perspective of three aspects: data, features, and models. Traditional machine learning technology is introduced to extract features for accomplishing binary classification tasks. In addition, the detection performance of the proposed method was evaluated in terms of the different aspects of the factors. Masood et al. [15] proposed a detection classification method for Twitter spam. The proposed method compared techniques based on several features, such as user characteristics, content characteristics, graphic characteristics, structural characteristics, temporal characteristics, etc. In addition, this paper also expounded on the future development direction of this field and offered solutions for some of the issues. Ahmed et al. [16] analyzed the advantages and challenges of machine learning in the field of spam detection and performed detailed comparative experiments to illustrate the scalability of machine learning in this field. In the same year, Sokhangoee et al. [17] proposed a new method for spam detection based on association-rule mining and genetic algorithm theory. The premise of this method effectively improved the detection accuracy for spam because more refined features can be extracted by combining a genetic algorithm and association rules. According to the above research, it can be seen that the current detection methods for links and text content are very mature; however, the detection methods for images that include spam are rarely studied, which shows that this field regarding images with spam is still in the initial stages.

In recent years, with the rapid development of computer hardware and network bandwidth, the field of artificial intelligence and deep learning has attracted extensive interest from researchers. So far, deep learning and CNN (convolutional neural networks) have provided many good solutions in various fields, such as image recognition [18,19], speech recognition, and natural language processing [20]. Therefore, in this era of deep learning, CNN provides an opportunity for the detection of images with spam. Xie et al. [21] proposed a detection method for pornographic images based on global classification and local sensitive information classification. CNN was introduced to extract image features such as color and texture, and an attention mechanism was utilized as the backbone of the network. Finally, discriminant results were obtained via the Softmax activation function. The experimental results show that their method can detect pornographic images efficiently from a specific dataset. Zhang et al. [22] proposed an image classification method for bad images, based on deep learning model integration, which achieved semantic complementarity by utilizing the image representation capabilities of multiple different deep networks and fused all the obtained features to improve the classification performance of the proposed model. Compared with traditional classification methods, their model has greatly improved upon previous accuracy rates. Cai et al. [23] proposed a method for detecting spam on the Internet, based on the BERT (Bidirectional Encoder Representation from Transformers) model, where the processing object comprises text information. Firstly, a bidirectional transformer structure was used to extract the contextual relationship information of the text content, then the trained BERT model was directly used to encode the sentences of the new task. Then, sentences of any length were encoded into fixed-length vectors to detect and analyze spam websites. From research in recent years, it can be seen that deep learning has made some progress in the field of spam detection, but most of the models focus on the detection of target objects, such as links and text, and research on spam detection in the context of images is still sparse.

To tackle the existing problems of detecting images containing spam, this paper proposes a detection method for social network images with spam based on deep neural network and frequency domain pre-processing. For this paper, first, we collected some images that included spam and combined the DIV2K2017 dataset to build a dataset for training the detection model. (Please note: the DIV2K dataset is a popular single-image super-resolution dataset that contains 1000 images of different scenes. In addition, this dataset contains low-resolution images with different types of degradations, which conform to all kinds of images that are common in everyday life; therefore, the dataset was suitable for training the proposed model). In the pre-processing stage, *Haar* wavelet transform analysis was utilized to extract different frequency domain information from the input image. Meanwhile, the low-frequency information of the image was discarded and the high-frequency information of three different frequency components was used as the input of the feature extraction stage, to improve the efficiency of the model. In the feature extraction stage, a feature extraction module with the designated convolution layers was designed, and an appropriate number of modules was selected through experiments to extract the vertical, horizontal, and diagonal high-frequency features of the input image, so as to maximize the extraction of the defective image characteristics of the information. The obtained different frequency domain features were subjected to the concat operation to obtain the final target feature, then the classification result was obtained. In addition, it has been verified through experiments that most spam exists in the image as high-frequency components, which provides a theoretical and experimental basis for the frame design of the model. The detection model also verified that it is completely feasible to apply deep learning to the field of spam detection.

Section 1 of this paper summarizes the background and research development of the social spam research field. Section 2 presents the proposed model framework in detail. Section 3 analyzes and summarizes the experimental results. Finally, a preliminary discussion is presented on the research significance of this paper and future research directions that are worthy of attention.

2. The Proposed Methods

According to the component of the spam existing in the image (please note: the experiments in Section 3.2 have verified that spam mainly exists in the image with high-frequency components, so the proposed detection model was designed based on experimental validation), the special detection model was designed to improve detection accuracy. The detection model can be divided into three stages to accomplish the detection task, which can be described as the pre-processing stage, the feature extraction stage, and the classification prediction stage. In the pre-processing stage, the input image is first decomposed by *Haar* wavelet analysis to obtain the low-frequency information, horizontal high-frequency information, vertical high-frequency information, and diagonal high-frequency information of the image. The experimental results show that most of the spam existed in the image as high-frequency information (see Section 4 for the experimental analysis). Therefore, in the feature extraction stage, a special feature extraction module and an appropriate number of modules are selected to extract the frequency feature. In the classification prediction stage, the obtained frequency domain features are subjected to the concat operation to obtain the final target feature, then the classification result is obtained. The overall architecture of the detection model is shown in Figure 1.

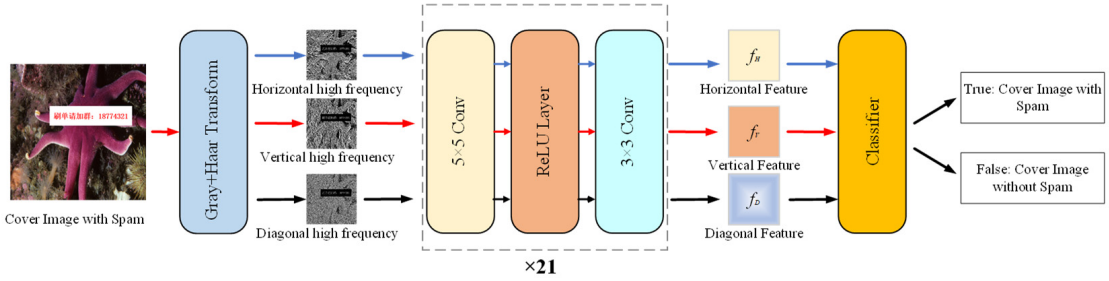

Figure 1. Visualization of the architecture for our proposed detection model.

2.1. The Stage of Pre-Processing

The primary focus of this paper was to verify that the spam mainly existed in the image in the form of high-frequency components, which also indicated that the low-frequency features of the input image have little effect on improving the accuracy of the detection model. To this end, in the pre-processing stage, the input image I_C was first subjected to wavelet transform analysis to obtain the corresponding low-frequency and high-frequency information; the operation is calculated as follows:

$$I_L, (I_H, I_V, I_D) = Haar(I_C) \tag{1}$$

where *Haar* represents the *Haar* wavelet transform, I_L is the corresponding low-frequency image after wavelet transform, I_H, I_V and I_D represent the horizontal high-frequency image, vertical high-frequency image, and diagonal high-frequency image after wavelet decomposition. At this stage, the low-frequency image containing few instances of spam information was discarded, and the three types of high-frequency images were reserved as the input information for the next stage.

2.2. The Stage of Feature Extraction

The task of the feature extraction stage is to extract representative features to determine whether the input image carries spam. The input of this stage is the horizontal high-frequency image I_H, the vertical high-frequency image I_V and the diagonal high-frequency image I_D after wavelet decomposition. The three high-frequency images enter the feature extraction block F with a fixed number of blocks with the same convolutional layer. The corresponding target feature can be obtained as follows:

$$f_H = nF(I_H) \tag{2}$$

$$f_V = nF(I_V) \tag{3}$$

$$f_D = nF(I_D) \tag{4}$$

where n represents the number of feature extraction blocks, F represents the feature extraction block with the designed convolutional layers, and the relationship between n and F is not a product operation. I_H, I_V and I_D are used as the input of F to get the feature vectors f_H, f_V and f_D, which represent the high-frequency features obtained in the feature extraction stage, respectively. During this stage, f_H, f_V and f_D represent the feature vectors for different high-frequency components. By selecting an appropriate number of feature extraction blocks, feature information that has spam in the images can be further extracted from high-frequency images, thereby improving the detection efficiency of the proposed model.

2.3. The Stage of Classification Prediction

In our model, unlike other current detection models, three feature components are obtained in the classification prediction stage, namely, the horizontal high-frequency fea-

ture, vertical high-frequency feature, and diagonal high-frequency feature, respectively. Therefore, the obtained high-frequency features are first concatenated by dimension; that is:

$$f = concat(f_H, f_V, f_D) \tag{5}$$

The final target feature f is obtained by splicing the high-frequency features, which contains most of the spam in the images, then the target features are operated as follows:

$$Result_{prediction} = Sigmoid(FC(f)) \tag{6}$$

As shown in Equation (6), the final target feature f is first sent to the fully connected layers, *FC*. Fully connected layers are able to map the learned distributed feature representation f to the sample label space. In this paper, FC layers consist of the input layer, hidden layer, and ReLU non-linear layer. The final target f is utilized as the input of the input layer. The ReLU layer is also used to enhance the nonlinear fitting ability of the model. The output of the FC layer is used as the input of the *Sigmoid* function. Finally, a prediction result is obtained through the *Sigmoid* function.

3. Experimental Results and Analysis

3.1. Dataset and Setup

In the process of our experiments, a PC with a GPU NVIDIA GeForce Tesla V100 16G was used, and the experimental environments Pytorch 1.1 and Python 3.7 were adopted. We built up our dataset to train the model proposed in this paper. To observe the detection effect of the proposed model, we collected some images with spam and combined the DIV2K2017 dataset to build a dataset for training the detection model (please note: the created dataset contained normal images without spam); some of the training images can be seen in Figure 2. The number of training images was 4000 and the size of the training images was cropped to 256 × 256; the number of test images for the test subset was set to 500. The image data in the training subset did not appear in the test subset. In addition, the architecture of the proposed detection model borrows from the idea of the VGG16 network; many experiments have been carried out on the setting of hyper-parameters, and the optimal parameter combination was selected. (In the training process, the batch size for the image dataset is set to 4, the number of training epochs was set to 350, and the learning rate was set to 0.005.)

Figure 2. Example training images from the collected and created image dataset.

3.2. The Elements of Spam in the Images

The specific components of the spam in the image determine the structural design of the proposed detection model. If the spam exists in the image in the form of high-frequency components, the feature extraction module of the proposed detection model can use the deep architecture to extract the high-frequency information of the image, to better detect the image with spam. Similarly, if the spam in the image comprises low-frequency

components, the architecture of the detection model can appropriately reduce the number of network layers. Therefore, the components of the spam are first analyzed, and *Haar* wavelet transform analysis is utilized to decompose the image with the spam in the first-order frequency domain. The low-frequency information and the horizontal, vertical, and diagonal high-frequency information for images that include spam are obtained, respectively, as shown in Figure 3.

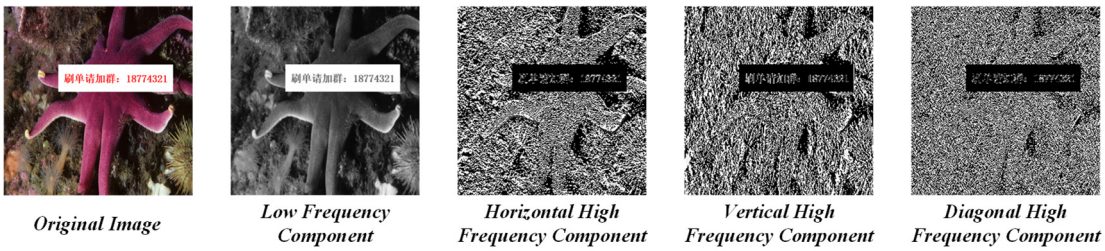

Figure 3. The corresponding frequency domain images after *Haar* wavelet decomposition of an image with spam.

From the experimental results in Figure 3, it is clear that spam mainly exists in the image in the form of high-frequency information, while the background occupies most of the low-frequency region of the image. In order to further verify that the spam exists in a specific region of the image, we also performed a *Haar* wavelet transform analysis on the original image without spam to obtain images corresponding to the different frequency domains. Then, we replaced the corresponding frequency domain of the image containing spam with the frequency domain of the original image for inverse *Haar* wavelet transform analysis. The reconstructed experimental results are shown in Figure 4.

Figure 4. Reconstructed images lacking different frequency domain information.

From the analysis of the experimental results in Figure 4, when only the low-frequency components of spam are replaced, there is less loss of spam in the reconstructed image, and only the background of the image is not perfectly reconstructed; when the high-frequency components are replaced, it is clear that the reconstruction effect of spam is very poor and only the reconstructed background information is more prominent. When the image is reconstructed using only the low-frequency components, we can see that the background of the image is almost the only part to be reconstructed. Therefore, we can conclude that the spam mainly exists in the high-frequency components in the image; that is to say, as long as the detection model can extract most of the high-frequency features of the image containing spam, the detection accuracy for the model can be improved. From the analysis of the experimental results in Table 1, when the inputs of the model are only the low-frequency components, the detection accuracy can only reach 36.5%; when the inputs of the model are the high-frequency components, the detection accuracy can is as high as 86%; when the input of the model is the whole image, the detection accuracy drops to only 74.5%. The experimental results in Table 1 also indicate that the spam mainly exists in the high-frequency components in the image.

Table 1. The influence of the detection model under a combination of different frequency domain components.

	Detection Accuracy
Only low-frequency components	36.5%
Only high-frequency components	86%
Low-frequency components + high-frequency components	74.5%

3.3. The Architecture Depth of the Proposed Model

In order to verify the influence of the network architecture depth on the detection model in terms of its detection ability, we conducted an experimental comparison with different numbers used for the feature extraction block; that is, feature extraction blocks with different numbers (3, 7, 11, 15, 21, 25), and 400 images including spam (not included in the model training dataset) were randomly selected for testing. The experimental results are shown in Table 2.

Table 2. The influence on the detection ability of the detection model under different numbers of feature extraction blocks.

Number of the Feature Extraction Block	**3**	**7**	**11**	**15**	**21**	**25**
Detection accuracy	15%	36.5%	56.5%	82%	91%	84.5%

It can be seen from the experimental results in Table 2 that when the feature extraction block was set at 3, the model could only obtain a detection accuracy of 15%. As the number of the feature extraction block increased, its detection capability increased accordingly; when the feature extraction block number increased from 21 to 25, the detection accuracy dropped by 6.5%, which indicates that when the network architecture of the model reaches a certain level, its feature extraction ability will be affected. From the whole of the experimental results, the detection ability of the detection model with shallow layers is low; conversely, the detection ability of the model based on a deep architecture is stronger, which also verifies the conclusion drawn in Section 2.1: the spam mainly exists in the high-frequency components in the image.

3.4. The Influence of Pre-Processing Module

The main task of the proposed model was to detect the spam contained in the image. We know that most of the spam information existed in the image as high-frequency information. In order to improve the detection accuracy of the proposed model, an image pre-processing module was designed. Firstly, the input image was decomposed using *Haar* wavelet analysis to obtain low-frequency information and horizontal, vertical, and diagonal high-frequency information. Then the low-frequency information was discarded, and the horizontal, vertical, and diagonal high-frequency information was used as the input of the model. Finally, a classification result was obtained. In the experiment, we used the same image dataset to train the detection model with and without the image pre-processing module and randomly selected 200 images (not present in the training dataset) to test the trained detection model. Table 3 shows the experimental comparison results obtained by the models trained with and without the image pre-processing module.

Table 3. The comparison results obtained by the models trained with and without the image pre-processing module.

	Detection Accuracy	**Training Time (min)**
With Pre-processing Module	84.5%	657.3
Without Pre-processing Module	77%	771.4

From the experimental results in Table 3, it can be seen that the image pre-processing module is equivalent to performing a feature extraction operation on the image in advance; it takes less time to train this model than the model without an image pre-processing module. At the same time, the input of the model with the image pre-processing module comprises high-frequency information that focuses on the region where the spam exists and achieves a better detection accuracy. Compared to the model without the image pre-processing module, the detection accuracy was improved by nearly 8%.

3.5. Comparison with State-of-the-Arts

Table 3 compares the detection results between the proposed model and the current popular detection models. These comparison detection models include AlexNet [24], VGG13 [25], VGG16, VGG19, GoogleNet [26], and ResNet50 [18]. The same image dataset and hyper-parameters (learning rate, number of iterations, etc.) were used to train different detection models and 200 test images were randomly selected for testing. Regarding the other detection models, since the detection task was not aimed at detecting spam in the images, during the training process the input and output of other detection models were adjusted to suit the comparison task in this paper. In order to observe the performance of different detection models more intuitively, we compared the detection accuracy and training time, respectively. The detection accuracy can provide a visual indication of the performance of the new detection model, while the length of training time can indicate the ability of the model to extract features. The comparison results obtained are shown in Table 4.

Table 4. The comparison results between the proposed model and the current popular detection models.

	Detection Accuracy	**Training Time (min)**
AlexNet	32.5%	1412.5
VGG13	35.5%	1355
VGG16	44%	1156.3
VGG19	54%	968.5
GoogleNet	66.5%	1045.4
ResNet50	77%	825
The Proposed Method	91%	657.3

From the experimental results in Table 4, compared with the current popular detection models, the proposed method is superior in terms of detection accuracy (please note: the input and output of other detection models have been modified to meet the requirements of the detection task). In addition, from the perspective of the detection accuracy of VGG13, VGG16, and VGG19, VGG19 shows the best performance in terms of detection accuracy, because VGG19 has the deepest network architecture for extracting the detailed information (high-frequency information) in the input image. This also shows that the spam mainly exists in the high-frequency components in the image. In addition, from the perspective of training time, the proposed method can achieve a balanced state with the shortest time and number of iterations, which indicates that the proposed algorithm is superior to the other current detection models in terms of computational cost. From another point of view, the shorter the training time of the detection model, the stronger its ability to extract features. Therefore, it can be seen from the experimental results in Table 3 that the proposed model also has advantages in terms of feature extraction.

4. Conclusions

In this paper, a detection method is proposed for identifying social media images containing spam, based on a deep neural network and frequency domain pre-processing. Our research contributions can be summarized as follows:

(1) An image dataset including spam was collected and created; to the best of our knowledge, in the field of social network spam detection, this is the first time that an image-level training dataset has been proposed.
(2) It has been verified that the spam mainly existed in the high-frequency components in the images. On this basis, *Haar* wavelet transform analysis was introduced as the pre-processing module of the model, and the high-frequency information of the image is extracted as the input of the feature extraction module.
(3) In the feature extraction stage, a special feature extraction block is designed and an appropriate number is selected, according to our experiment and the spam component, which improves the accuracy and efficiency of the detection model.

Unlike the current detection models, this paper first verifies the specific components of spam in the image and then designs a more targeted detection framework, which can enhance the detection efficiency and accuracy of the proposed model. In future work, we will further expand the created image dataset and improve the recognition ability and efficiency of the proposed model. In addition, although the proposed model demonstrates good detection performance on fixed image datasets, it lacks breadth, which will be addressed. Improving the applicability of the model is another future research focus.

Author Contributions: H.S.: conceptualization, methodology, data preprocessing; data analysis, writing-original draft preparation; X.L.: data collection, writing-review and editing, visualization; X.Z.: conceptualization, supervision, project administration. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (61272374, 61300190), the Key Project of the Chinese Ministry of Education (313011), and the Foundation of the Department of Education of Liaoning Province (L2015001).

Acknowledgments: We thank the anonymous reviewers for their careful reading of our manuscript and their many insightful comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, H.; He, X.; Qing, L.; Wu, Y.; Ren, C.; Sheriff, R.E.; Zhu, C. Real-world single image super-resolution: A brief review. *Inf. Fusion* **2022**, *79*, 124–145. [CrossRef]
2. Javed, I.T.; Toumi, K.; Alharbi, F.; Margaria, T.; Crespi, N. Detecting nuisance calls over internet telephony using caller reputation. *Electronics* **2021**, *10*, 353. [CrossRef]
3. Li, Q.; Wang, X.; Ma, B.; Wang, X.; Wang, C.; Gao, S.; Shi, Y. Concealed Attack for Robust Watermarking Based on Generative Model and Perceptual Loss. *IEEE Trans. Circuits Syst. Video Technol.* **2021**. [CrossRef]
4. Wang, Y.; Bashir, S.M.A.; Khan, M.; Ullah, Q.; Wang, R.; Song, Y.; Guo, Z.; Niu, Y. Remote sensing image super-resolution and object detection: Benchmark and state of the art. *Expert Syst. Appl.* **2022**, *197*, 116793. [CrossRef]
5. Minaee, S.; Boykov, Y.Y.; Porikli, F.; Plaza, A.J.; Kehtarnavaz, N.; Terzopoulos, D. Image segmentation using deep learning: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2021**. [CrossRef]
6. Tov, O.; Alaluf, Y.; Nitzan, Y.; Patashnik, O.; Cohen-Or, D. Designing an encoder for stylegan image manipulation. *ACM Trans. Graph.* **2021**, *40*, 1–14. [CrossRef]
7. Zhang, Z.; Hou, R.; Yang, J. Detection of social network spam based on improved extreme learning machine. *IEEE Access* **2020**, *8*, 112003–112014. [CrossRef]
8. Yang, C.; Harkreader, R.; Gu, G. Empirical evaluation and new design for fighting evolving twitter spammers. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1280–1293. [CrossRef]
9. Jiang, M.; Cui, P.; Faloutsos, C. Suspicious behavior detection: Current trends and future directions. *IEEE Intell. Syst.* **2016**, *31*, 31–39. [CrossRef]
10. Rao, S.; Verma, A.K.; Bhatia, T. A review on social spam detection: Challenges, open issues, and future directions. *Expert Syst. Appl.* **2021**, *186*, 115742. [CrossRef]
11. Zhu, Y.; Wang, X.; Zhong, E.; Liu, N.; Li, H.; Yang, Q. Discovering spammers in social networks. In Proceedings of the AAAI Conference on Artificial Intelligence, Toronto, ON, Canada, 22–26 July 2012; Volume 26, pp. 171–177.
12. Hu, X.; Tang, J.; Zhang, Y.; Liu, H. Social spammer detection in microblogging. In Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence, Beijing, China, 3–9 August 2013.
13. Wu, F.; Shu, J.; Huang, Y.; Yuan, Z. Co-detecting social spammers and spam messages in microblogging via exploiting social contexts. *Neurocomputing* **2016**, *201*, 51–65. [CrossRef]

14. Chen, C.; Zhang, J.; Xie, Y.; Xiang, Y.; Zhou, W.; Hassan, M.M.; AlElaiwi, A.; Alrubaian, M. A performance evaluation of machine learning-based streaming spam tweets detection. *IEEE Trans. Comput. Soc. Syst.* **2015**, *2*, 65–76. [CrossRef]
15. Masood, F.; Almogren, A.; Abbas, A.; Khattak, H.A.; Din, I.U.; Guizani, M.; Zuair, M. Spammer detection and fake user identification on social networks. *IEEE Access* **2019**, *7*, 68140–68152. [CrossRef]
16. Ahmed, N.; Amin, R.; Aldabbas, H.; Koundal, D.; Alouffi, B.; Shah, T. Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges. *Secur. Commun. Netw.* **2022**, *2022*, 1862888. [CrossRef]
17. Sokhangoee, Z.F.; Rezapour, A. A novel approach for spam detection based on association rule mining and genetic algorithm. *Comput. Electr. Eng.* **2022**, *97*, 107655. [CrossRef]
18. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.
19. Ma, W.; Tu, X.; Luo, B.; Wang, G. Semantic clustering based deduction learning for image recognition and classification. *Pattern Recognit.* **2022**, *124*, 108440. [CrossRef]
20. Kormilitzin, A.; Vaci, N.; Liu, Q.; Nevado-Holgado, A. Med7: A transferable clinical natural language processing model for electronic health records. *Artif. Intell. Med.* **2021**, *118*, 102086. [CrossRef]
21. Xie, X.; Niu, W.; Zhang, X.; Ren, Z.; Luo, Y.; Li, J. Co-Clustering Host-Domain Graphs to Discover Malware Infection. In Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing, Dublin, Ireland, 17–19 October 2019; pp. 1–6.
22. Zhang, C.; Du, G.; Du, X. Illegal Image Classification Based on Ensemble Deep Model. *J. Beijing Jiaotong Univ.* **2017**, *41*, 21–26.
23. Cai, X. Internet bad information detection based on Bert model. *Telecommun. Sci.* **2020**, *36*, 121–126.
24. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. Imagenet classification with deep convolutional neural networks. *Adv. Neural Inf. Processing Syst.* **2012**, *25*, 226–237. [CrossRef]
25. Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition. *arXiv* **2014**, arXiv:1409.1556.
26. Szegedy, C.; Liu, W.; Jia, Y.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. Going deeper with convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 7–12 June 2015; pp. 1–9.