

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

## Real Or Fake Face Detection

**Mr. CH.Venkatesh<sup>1</sup> M. U. N. J. Bhavani<sup>2</sup>, K. Lalitha<sup>3</sup>, N. Prasanna Kumar<sup>4</sup>,  
M. Prudhvi Raj<sup>5</sup>**

<sup>1</sup> Assistant Professor, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

<sup>2,3,4,5</sup> UG Students, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

### ABSTRACT


Now-a-days biometric systems are useful in recognizing person's identity but criminals change their appearance in behavior and psychological to deceive recognition system. To overcome from this problem we are using new technique called Deep Texture Features extraction from images and then building train machine learning model using CNN (Convolution Neural Networks) algorithm. This technique refers as LBPNet or NLBPNet as this technique heavily dependent on features extraction using LBP (Local Binary Pattern) algorithm.

In this project we are designing LBP Based machine learning Convolution Neural Network called LBPNET to detect fake face images. Here first we will extract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate training model. Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-fake image. Below we can see some details on LBP.

Local binary patterns (LBP) is a type of visual descriptor used for classification in computer vision and is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. Due to its discriminative power and computational simplicity, LBP texture operator has become a popular approach in various applications. It can be seen as a unifying approach to the traditionally divergent statistical and structural models of texture analysis. Perhaps the most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale changes caused, for example, by illumination variations. Another important property is its computational simplicity, which makes it possible to analyze images in challenging real- time settings.

The LBP feature vector, in its simplest form, is created in the following manner: Divide the examined window into cells (e.g. 16x16 pixels for each cell). For each pixel in a cell, compare the pixel to each of its 8 neighbors (on its left-top, left-middle, left- bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise. Where the center pixel's value is greater than the neighbor's value, write "0". Otherwise, write "1". This gives an 8-digit binary number (which is usually converted to decimal for convenience). Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center). This histogram can be seen as a 256-dimensional feature vector.

Optionally normalize the histogram. Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window. The feature vector can now be processed using the Support vector machine,

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023


extreme learning machines, or some other machine learning algorithm to classify images. Such classifiers can be used for face recognition or texture analysis.

## 1. INTRODUCTION

Recently, the generative model based on deep learning such as the generative adversarial net (GAN) is widely used to synthesize the photo-realistic partial or whole content of the image and video. Furthermore, recent research of GANs such as progressive growth of GANs (PGGAN) and BigGAN could be used to synthesize a highly photo-realistic image or video so that the human cannot recognize whether the image is fake or not in the limited time. In general, the generative applications can be used to perform the image translation tasks. However, it may lead to a serious problem once the fake or synthesized image is improperly used on social network or platform. For instance, cycleGAN is used to synthesize the fake face image in a pornography video. Furthermore, GANs may be used to create a speech video with the synthesized facial content of any famous politician, causing severe problems on the society, political, and commercial activities. Therefore, an effective fake face image detection technique is desired. In this paper, we have extended our previous study associated with paper ID #1062 to effectively and efficiently address these issues. In traditional image forgery detection approach, two types of forensics scheme are widely used: active schemes and passive schemes. With the active schemes, the externally additive signal (i.e., watermark) will be embedded in the source image without visual artifacts. In order to identify whether the image has tampered or not, the watermark extraction process will be performed on the target image to restore the watermark. The extracted watermark image can be used to localize or detect the tampered regions in the target image. However, there is no "source image" for the generated images by GANs such that the active image forgery detector cannot be used to extract the watermark image. The second one-passive image forgery detector—uses the statistical information in the source image that will be highly consistency between different images. With this property, the intrinsic statistical information can be used to detect the fake region in the image. However, the passive image forgery detector cannot be used to identify the fake image generated by GANs since they are synthesized from the low-dimensional random vector. Nothing change in the generated image by GANs because the fake image is not modified from its original image

Intuitively, we can adopt the deep neural network to detect the fake image generated by GAN. Recently, there are some studies that investigate a deep learning-based approach for fake image detection in a supervised way. In other words, fake image detection can be treated as a binary classification problem (i.e., fake or real image). For example, the convolution neural network (CNN) Network is used to learn the fake image detector. In the performance of the fake face

image detection can be further improved by adopting the most advanced CNN—Xception network. However, there are many GANs proposed year by year. For example, recently proposed GANs such as can be used to produce the photo-realistic images. It is hard and very time-consuming to collect all training samples of all GANs. In addition, such a supervised learning strategy will tend to learn the discriminative

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

features for a fake image generated by each GANs. In this situation, the learned detector may not be effective for the fake image generated by another newGAN excluded in the training phase.

In order to meet the massive requirement of the fake image detection for GANs-based generator, we propose novel network architecture with a pairwise learning approach, called common fake feature network (CFFN). Based on our previous approach, it is clear that the pairwise learning approach can overcome the shortcomings of the supervised learning-based CNN such as methods in. In this paper, we further introduce a novel network architecture combining with pairwise learning to improve the performance of the fake image detection. To verify the effectiveness of the proposed method, we apply the proposed deep fake detector (DeepFD) to identify both fake face and generic image. The primary contributions of the proposed method are two-fold: We propose a fake face image detector based on the novel CFFN consisting of several dense blocks to improve the representative power of the fake image. The pairwise learning approach is first introduced to improve the generalization property of the proposed DeepFD.


## 2. LITERATURE SURVEY

1. Karras, T.; Aila, T.; Laine, S.; Lehtinen, J. Progressive growing of gans for improved quality, stability, and variation. arXiv Preprint, arXiv:1710.10196 2017. 256

We describe a new training methodology for generative adversarial networks. The key idea is to grow both the generator and discriminator progressively: starting from a low resolution, we add new layers that model increasingly fine details as training progresses. This both speeds the training up and greatly stabilizes it, allowing us to produce images of unprecedented quality, e.g., CelebA images at  $1024^2$ . We also propose a simple way to increase the variation in generated images, and achieve a record inception score of 8.80 in unsupervised CIFAR10. Additionally, we describe several implementation details that are important for discouraging unhealthy competition between the generator and discriminator. Finally, we suggest a new metric for evaluating GAN results, both in terms of image quality and variation. As an additional contribution, we construct a higher-quality version of the CelebA dataset.

2. Brock, A.; Donahue, J.; Simonyan, K. Large scale gan training for high fidelity natural image synthesis. arXiv Preprint, arXiv:1809.11096 2018.

Despite recent progress in generative image modeling, successfully generating high-resolution, diverse samples from complex datasets such as ImageNet remains an elusive goal. To this end, we train Generative Adversarial Networks at the largest scale yet attempted, and study the instabilities specific to such scale. We find that applying orthogonal regularization to the generator renders it amenable to a simple "truncation trick," allowing fine control over the trade-off between sample fidelity and variety by reducing the variance of the Generator's input. Our modifications lead to models which set the new state of the art in class-conditional image synthesis. When trained on ImageNet at  $128 \times 128$  resolution, our models (BigGANs) achieve an Inception Score (IS) of 166.5 and Frechet Inception Distance (FID) of 7.4, improving over the previous best IS of 52.52 and FID of 18.6.

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

3. Zhu, J.Y.; Park, T.; Isola, P.; Efros, A.A. Unpaired image-to-image translation using cycle-consistent adversarial networks. arXiv Preprint, 2017.

Image-to-image translation is a class of vision and graphics problems where the goal is to learn the mapping between an input image and an output image using a training set of aligned image pairs. However, for many tasks, paired training data will not be available. We present an approach for learning to translate an image from a source domain  $X$  to a target domain  $Y$  in the absence of paired examples. Our goal is to learn a mapping  $G: X \rightarrow Y$  such that the distribution of images from  $G(X)$  is indistinguishable from the distribution  $Y$  using an adversarial loss. Because

this mapping is highly under-constrained, we couple it with an inverse mapping  $F: Y \rightarrow X$  and introduce a cycle consistency loss to push  $F(G(X)) \approx X$  (and vice versa). Qualitative results are presented on several tasks where paired training data does not exist, including collection style transfer, object transfiguration, season transfer, photo enhancement, etc. Quantitative comparisons against several prior methods demonstrate the superiority of our approach

4. AI can now create fake porn, making revenge porn even more complicated, <http://theconversation.com/ai-can-now-create-fake-porn-making-revenge-porn-even-more-complicated-92267>, 262 2018.


In January this year, a new app was released that gives users the ability to swap out faces in a video with a different face obtained from another photo or video – similar to Snapchat’s “face swap” feature. It’s an everyday version of the kind of high-tech computer-generated imagery (CGI) we see in the movies.

You might recognise it from the cameo of a young Princess Leia in the 2016 Star Wars film *Rogue One*, which used the body of another actor and footage from the first Star Wars film created 39 years earlier. Now, anyone with a high-powered computer, a graphics processing unit (GPU) and time on their hands can create realistic fake videos – known as “deepfakes” – using artificial intelligence (AI). Sounds fun, right?

The problem is that these same tools are accessible to those who seek to create non-consensual pornography of friends, work colleagues, classmates, ex-partners and complete strangers – and post it online.

5. Hsu, C.; Lee, C.; Zhuang, Y. Learning to detect fake face images in the Wild. 2018 International Symposium 264 on Computer, Consumer and Control (IS3C), 2018, pp. 388–391. doi:10.1109/IS3C.2018.00104.

Although Generative Adversarial Network (GAN) can be used to generate the realistic image, improper use of these technologies brings hidden concerns. For example, GAN can be used to generate a tampered video for specific people and inappropriate events, creating images that are detrimental to a particular person, and may even affect that personal safety. In this paper, we will develop a deep forgery discriminator (DeepFD) to efficiently and effectively detect the computer-generated images. Directly learning a binary classifier is relatively tricky since it is hard to find the common discriminative features for judging the fake images generated from different GANs. To address this shortcoming, we adopt contrastive loss in seeking the typical features of the synthesized images generated by different GANs and follow by concatenating a

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

classifier to detect such computer-generated images. Experimental results demonstrate that the proposed DeepFD successfully detected 94.7% fake images generated by several state-of-the-art GANs.

### **3. EXISTING SYSTEM**

- Now-a-days biometric systems are useful in recognizing person's identity but criminals change their appearance in behaviour and psychological to deceive recognition system.
- To overcome from this problem. We are using new technique called Deep Texture Features extraction from images and then building train machine learning model using CNN (Convolution Neural Networks) algorithm. This technique refers as LBPNet or NLBPNet as this technique heavily dependent on features extraction using LBP (Local Binary Pattern) algorithm.

#### **DISADVANTAGES**


- High complexity.
  - Time-consuming.
  - Non real time detection.
- Poor results for small and dense objects.

### **4. PROPOSED SYSTEM**

In this project we are designing LBP Based machine learning Convolution Neural Network called LBPNET to detect fake face images. Here first we will extract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate training model. Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-fake image. Below we can see some details on LBP.

#### **ADVANTAGES**

- It is faster and more convenient compared to other biometric technologies like fingerprints or retina scans.
  - There are also fewer touch points in facial recognition compared to entering passwords or PINs.
  - It supports multifactor authentication for additional security verification.
  - Detecting local and global matching
- Background analysis

 <p>(Enriching the Research)</p>	Open Access Research Article	
	Volume: 23 Issue: 07	
	July, 2023	

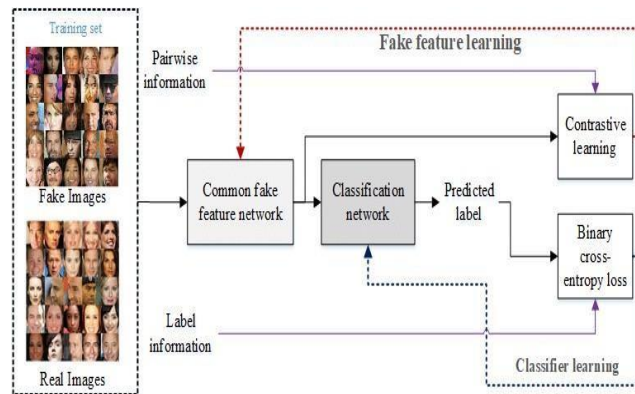


Fig: 1 System Architecture

## 5. RESULTS

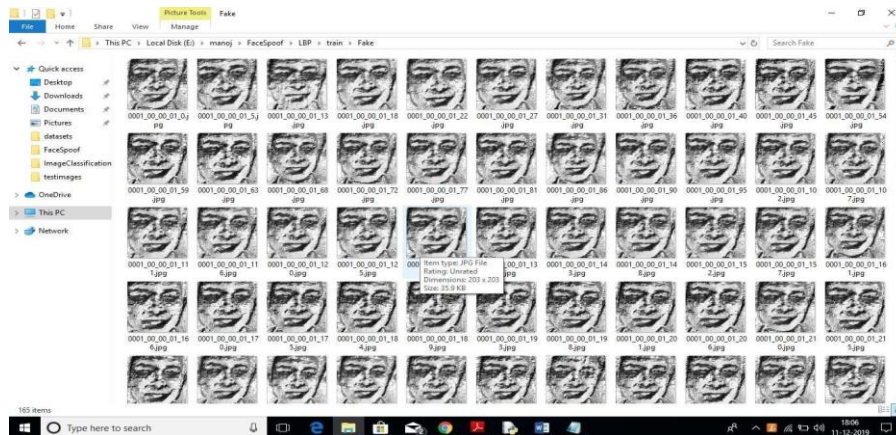



Fig.2 Database



Fig.3: Generate Image Train & Test Model

 (Enriching the Research)	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

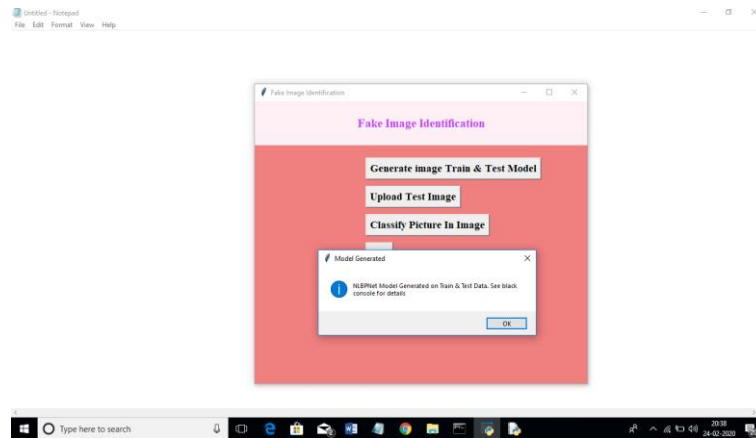


Fig.4: CNN LBPNET model generated

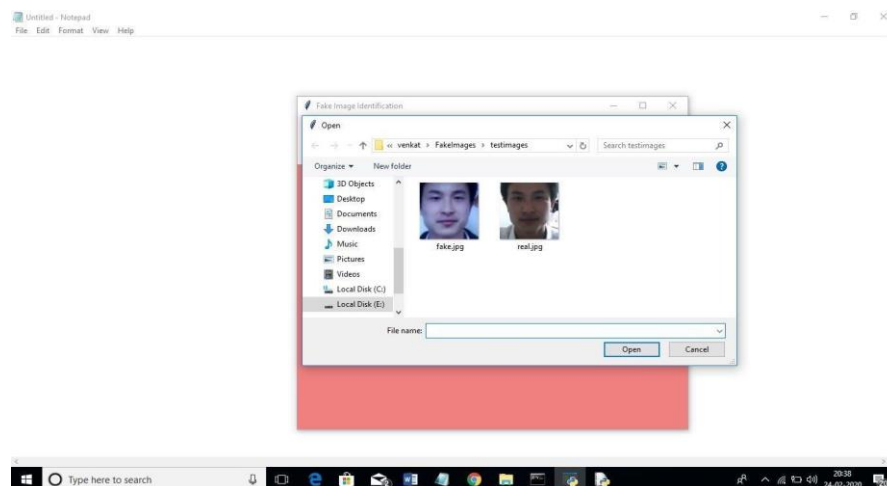



Fig.5: showing differences in face

 (Enriching the Research)	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

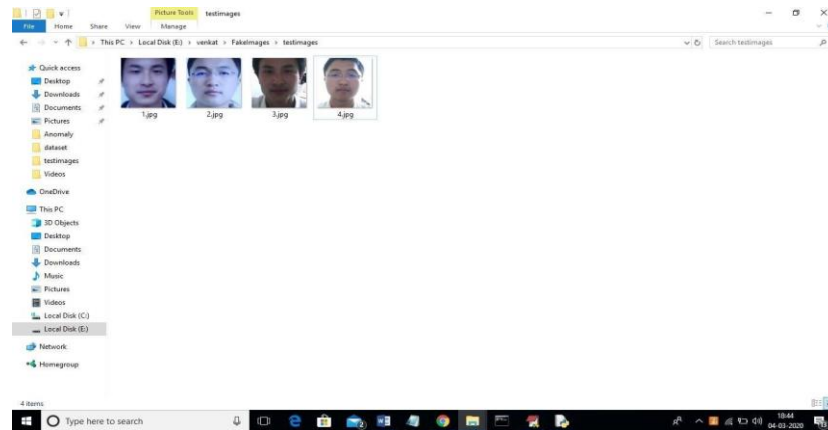


Fig.6: shows original face

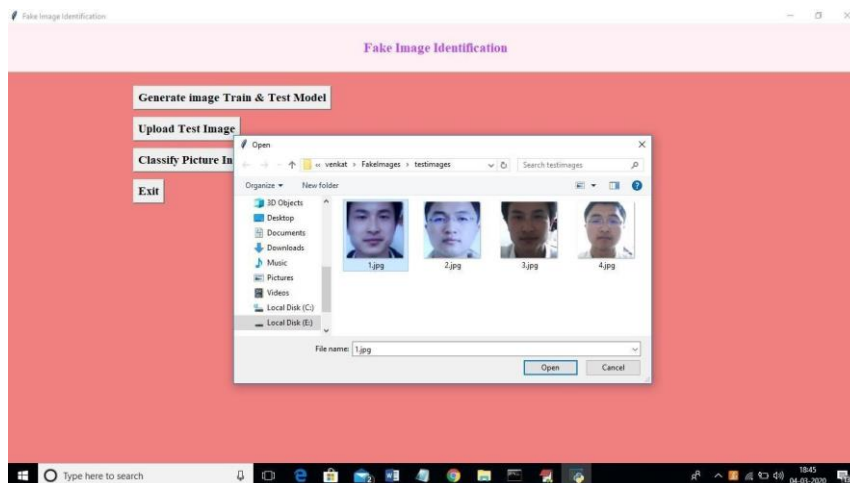
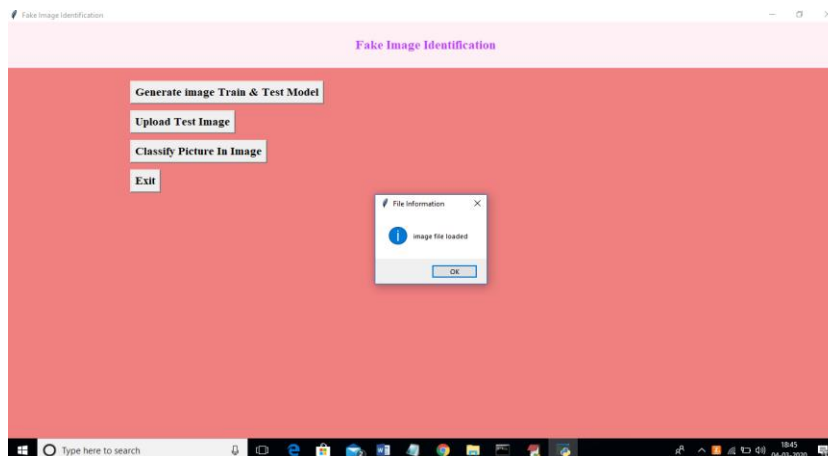

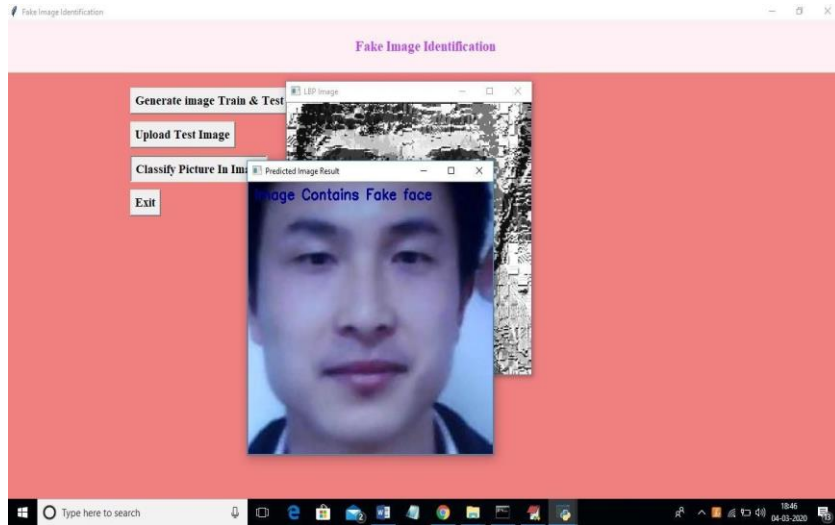


Fig.7: image uploading



 <p>(Enriching the Research)</p>	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

**Fig.8: classify picture**



**Fig.9: Shows real or fake face result**

## 6. CONCLUSION

In this paper, we have proposed a novel common fake feature network based the pair wise learning, to detect the fake face/general images generated by state-of-the-art GANs successfully. The proposed CFFN can be used to learn the middle- and high-level and discriminative fake feature by aggregating the cross-layer feature representations into the last fully connected layers. The proposed pair wise learning can be used to improve the performance of fake image detection further. With the proposed pairwise learning, the proposed fake image detector should be able to have the ability to identify the fake image generated by a new GAN. Our experimental results demonstrated that the proposed method outperforms other state-of-the-art schemes in terms of precision and recall rate.

## REFERENCES

1. Karras, T.; Aila, T.; Laine, S.; Lehtinen, J. Progressive growing of gans for improved quality, stability, and variation. arXiv Preprint, arXiv:1710.10196 2017. 256
2. Brock, A.; Donahue, J.; Simonyan, K. Large scale gan training for high fidelity natural imagesynthesis. arXiv Preprint, arXiv:1809.11096 2018.
3. Zhu, J.Y.; Park, T.; Isola, P.; Efros, A.A. Unpaired image-to-image translation using cycle-consistent 259 adversarial networks. arXiv Preprint, 2017.
4. AI can now create fake porn, making revenge porn even more complicated., <http://theconversation.com/ai-can-now-create-fake-porn-making-revenge-porn-complicated-92267>, 262 2018.

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

5. Hsu, C.; Lee, C.; Zhuang, Y. Learning to detect fake face images in the Wild. 2018 International Symposium 264 on Computer, Consumer and Control (IS3C), 2018, pp. 388–391. doi:10.1109/IS3C.2018.00104.
6. H.T. Chang, C.C. Hsu, C.Y.a.D.S. Image authentication with tampering localization based on watermark 266 embedding in wavelet domain. Optical Engineering 2009, 48, 057002.
7. Hsu, C.C.; Hung, T.Y.; Lin, C.W.; Hsu, C.T. Video forgery detection using correlation of noise residue. Proc. of the IEEE Workshop on Multimedia Signal Processing. IEEE, 2008, pp. 170–174.
8. Farid, H. Image forgery detection. IEEE Signal Processing Magazine 2009, 26, 16–25.
9. Huaxiao Mo, B.C.; Luo, W. Fake Faces Identification via Convolutional Neural Network. Proc. of the ACM Workshop on Information Hiding and Multimedia Security. ACM, 2018, pp. 43–47.
10. Marra, F.; Gragnaniello, D.; Cozzolino, D.; Verdoliva, L. Detection of GAN-Generated Fake Images over Social Networks. Proc. of the IEEE Conference on Multimedia Information Processing and Retrieval, 2018, 274 pp. 384–389. doi:10.1109/MIPR.2018.00084.
11. Chollet, F. Xception: Deep learning with depth wise separable convolutions. Proc. of the IEEE conference on 276 Computer Vision and Pattern Recognition 2017, pp. 1610–02357.