Face Image Manipulation Detection using Deep Learning

Mr. A. Arockia Abins
Assistant Professor,Department of Computer Science And Engineering,Velammal Engineering College.
Gowthaman.R
UG Scholar,Department of Computer Science And Engineering,Velammal Engineering College.
Pughazhenthi.R.R
UG Scholar,Department of Computer Science And Engineering,Velammal Engineering College.

ABSTRACT

Image manipulation detection is drawing prominent attention as there are a lot of editing tools and software which allows to cause manipulation in images. The process of manipulating the image is termed as forgery and the existence of this led to the development of digital forensics. This proposal is a passive image manipulation scheme that is based on supervised learning approach. The digital input image is fed into viola-jones algorithm and the face is detected in the image. Then the detected face images are extorted to feature extraction. The results from the feature extraction is given as input to the SVNN classifier. It then classifies the input to detect the presence of manipulation in the image. The proposed system is reasonably faster and performance is greater than other existing methods.

I. INTRODUCTION

The field of forensics classifies the image manipulation methods such as cloning (copy–paste), splicing, erasing, and retouching. The splicing is the process of transferring a portion of the image into another image that can be done either through cut and paste operation or through the usage of other techniques such that there is a perfect match in the gradients of the target image. The operation copy–paste is same as splicing, but the portion of the image is transferred within the image. The process of retouching is something similar to that of blurring the portion of the image, recolouring, and applying filters. It is possible to generate number of images through copying and pasting the portions of an image on another image. Likewise, the portion of the image could be modified with some other portions of the same image, which is termed as healing, cloning, or retouching. Thus, there are a diverse number of manipulating methods that offer a perfect image without any doubts of manipulation.

Image forgery detection is the process of detecting the presence or the absence of the manipulation in a given image. There are two types of detecting forgeries in the image, one is the active forgery detection and another one is the passive forgery detection.

The active forgery detection is the non-blind approach that detects the information inserted in advance from the digital image. The examples of the active forensics are digital watermarks, signatures and so on, authenticating the images. If the embedded image is found to be different from the original one then, the image is addressed as being tampered and image watermarking is the famous method in the active forensics. In this image watermarking, the hidden message was inserted at the time of recording and it is unsheathed during the verification step. In the passive forgery detection approach, there is no trace of the manipulation of the image and hence, it is a challenge. These manipulations are determined using the alterations present in the statistical patterns obtained from image doctoring. The feature consistency of an image is determined using the watermark or signature by employing the blind methods. Moreover, the image forgery detection techniques are grouped as block-based and keypoint-based techniques. The former one divides the image into square blocks and the features of the square block are extracted following the image comparison so that to ensure the similarity, but the later method extracts the features of the image based on the high entropy followed by the image comparison of the image to identify the region duplication forgery detection.

II. RELATED WORKS

Learning-based techniques: There is aforgery detection method used the inconsistencies in the illumination colour of the images. The forgery detection strategy discussed uses machine learning and it required very less user interaction. The shortcoming is that this technique is suitable for the images with two or three faces, but the advantage is that the method operates without the need of the experts' interaction. The proposed forgerydetection method is suitable for detecting forgery images from number of faces. The benefit was that they were tuned properly for the specific case, but lacked the theoretical structure.

Descriptors-based techniques: There is a generic passive image forgery scheme depending on the spatial rich model along with the local binary pattern (LBP). The method is found to be more accurate and less complex such that only less number of sub-models is employed. Even though the complexity is low, the dimension of the features can be reduced only through developing the better models. In the proposed method, the process of transformation to the code format is simple and easy while consuming less time. An integrated algorithm by utilising the Joint Photographic Experts Group (JPEG) features and local noise discrepancies for detecting the fraud practices, such as copy–move (CM) and splicing forgery in a digital image. This technique was effective on detecting both CM and splicing forgery.

III. PROPOSED SYSTEM

To overcome the challenges in the existing forgery detection techniques, this paper proposes the forgery detection scheme using the support vector neural network (SVNN)-based classifier for classifying the images as manipulated and non-manipulated images. Initially, the images are fed to the texture descriptor and the face is detected using the Viola–Jones algorithm which effectively determines the face in the image. The Viola–Jones algorithm is efficient and fast in detecting the face and the computational speed is reported in milliseconds.

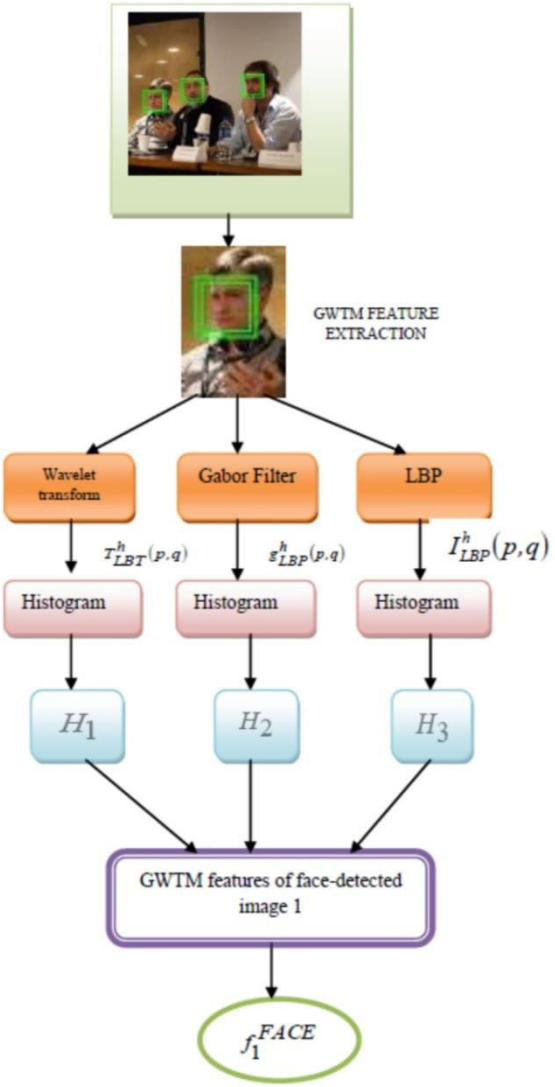

Figure 1: GWTM feature extraction

The face detected images are subjected to the feature extraction using the Gabor filter + wavelet + texture (GWTM) operator and the features are concatenated to present the input to the classifier. The Gabor filters and the wavelet transforms are advantageous in the GWTM operator as they preserve the facial features. Finally, the proposed SVNN classifier classifies the features to detect the presence of the manipulation. The proposed scheme of classification is found to be effective in classifying the images such that if there are manipulations, the classifier reports are forged or otherwise, the image is reported as the original image. The importance of the proposed algorithm is that the computational speed is high and the best solution converges to the global optimal solution. The process of transformation to the code format is simple and easy while consuming less time.

The experimentation of the proposed technique of detecting the forgery is done in the system with 2 GB RAM, Intel core processor,Windows 10 Operating System. The technique is implemented using the editorAnaconda.

IV. IMPLEMENTATION

The proposed system is implemented using opencv which is generated by using the cascade algorithm to get its datasets.Using the datasets the training is given by python cascade algorithm to train the users along with the code.

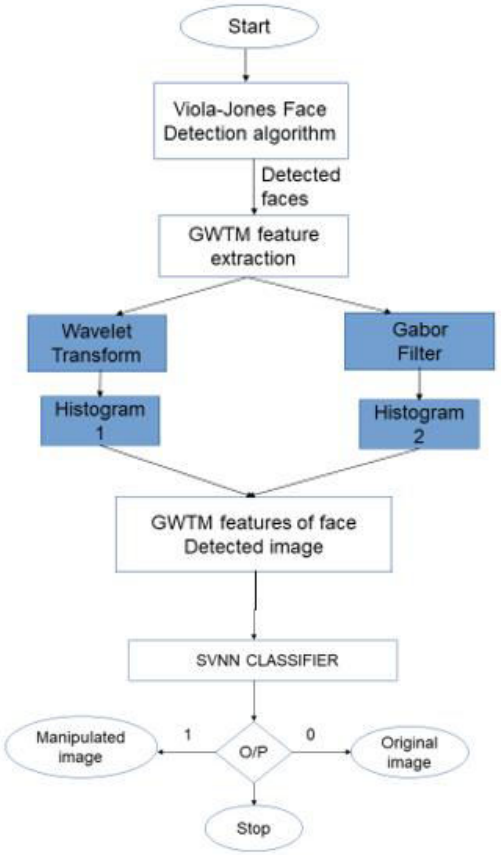

Figure 2: Architecture

The Anaconda editor is used to implement and run the python file since it has its own data and training sets. This training sets are imported in our application to identify the expressionsdetected on the face. The face is identified and recognized using the classifier where it identifies the frames of the face and id makes the face which is identified.

4.1.Face extraction using the Viola–Jones

The importance of using the Viola–Jones algorithm for detecting the face is that the algorithm is efficient and fast in detecting the face and the computational speed is

reported in milliseconds. Initially, the black pixels are marked and subtracted from the white pixels and the results are compared with the threshold value such that the features are identified based on the criterion. The steps in Viola–Jones are given as

Haar-like features: The Haar-like features determine the blackand the white portions of the image that uses a rectangle around the face.

- ***Formation of the integral image:*** The integral image is formedby summing the pixel value of the individual pixels with the pixel values of its neighbours. In other words, the value of the individual pixel is formed by summing the pixel value of the neighbouring four pixels that is accumulated in the rectangle.
- ***Adaboost machine-learning method:*** The Adaboost is themachine-learning method employed for detecting the face and it follows the bagging concept. The importance of the Adaboost algorithm is to choose small features of the face such that the computation becomes easy and fast. The AdaBoost algorithm provides the highly significant features by neglecting the unnecessary background.
- ***Cascade classifier for concatenating the features****:* The cascadeclassifier comprises of a number of the classifiers that allows the selection of the face image. Each of the sub-windows is send to the classifiers such that to determine whether the sub-window possess the face or not.

Thus, the Viola–Jones algorithm to detect the face from the image is performed successfully.

4.2.Feature extraction using GWTM:

The input face-detected images are subjected to the feature extraction using the GWTM operator. The images are fed to the wavelet transform and the Gabor filter, among which the wavelet images are generated using the wavelet transform and features based on the orientation and the frequency are determined using the Gabor filters.

The output from the wavelet and the Gabor filters is fed to the LBP model with the input image. The analysis of the texture is analysed for the input image that transforms the input image into an array. The output from the LBP is subjected to the histogram analysis such that the histogram yields the global appearance of the image.

The Gabor filters and the wavelet transforms are advantageous in the GWTM operator used for the feature extraction as they preserve the facial features. The GWTM considers the approximation coefficient for extracting the features as they possess the tendency to reveal the facial features in a different scale. Moreover, the Gabor filters yield the frequency information and they preserve spatial and frequency information of the image. The Gabor filters possess the phase and the magnitude information and the magnitude of the image gains significance as they preserve the edge information effectively.

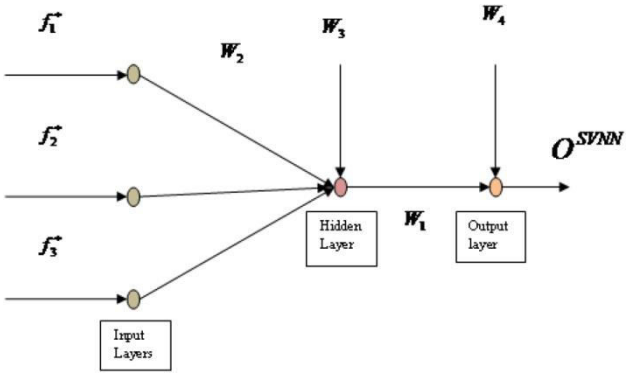

Figure 3: SVNN Architecture

4.3 Architecture of SVNN:

The SVNN comprises of theinput layer, hidden layer, and the output layer, as shown in Fig. 3. SVNN is generated by introducing the eigenvalue decay in the neural networks (NNs) based on the same principles of SVM hence, the classification margin is improved. The use of SVM with non-linear kernels requires a prohibitive computational cost; since its decision function needs a summation of non-linear functions which demands a large amount of time when the number of support vectors is big. Therefore, a maximal margin NN can be a suitable option, since it can offer a fast non-linear classification with good generalisation capacity. The input to the SVNN is the features extracted from the images that are obtained as a result of concatenating the GWTM features. The features fed to the SVNN classifier trains the network such that the forgery detection is made.

4.4.Testing phase:

Whenever the new image arrives at theclassifier for detecting the forged image, the classifier classifies and provides the output. If the output is one then, the image is said to be forged or else, the image is the original image without any manipulation. Fig. 4 shows the testing phase of the proposed classifier.

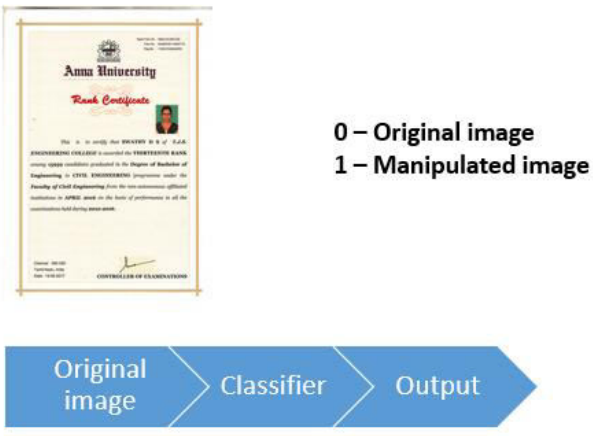

Figure 4: Testing Phase

Figure 5. shows the step-by-step tracing of the proposed technique for a normal image taken from the dataset.

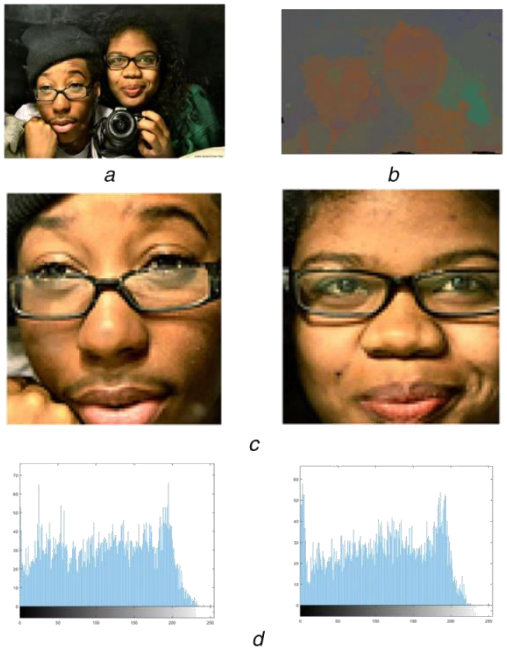

Figure 5: Step-by-step tracing of the proposed technique for a normal imagetaken from the dataset (a)Normal image, **(b)** Illumination map, **(c)** Face detected image. **(d)** GWTM-based feature extraction

V. CONCLUSION

The paper focuses on a scheme for detecting the forgery for which the SVNN-based classifier is employed. The proposed SVNN classifier aims at categorising the images as forged or non-forged images. The images are colour transformed so that to enable the easy feature extraction and the transformed image is applied to theViola–Jones algorithm that effectively finds the face in the image. The face detected image is allowed to the feature extraction using the GWTM and the features are fed to the classifier for classification. The proposed classifier is found to be more robust and effective in identifying the forged images. The classifier is highly effective that offers better classification accuracy and it is not computationally complex. The proposed scheme is highly accurate in detecting the presence of the forgery in the images.

VI. REFERENCE

[1] Robust Real-Time Face Detection- PAUL VIOLA,Microsoft Research, One Microsoft WayRedmond, WA 98052,USA, viola@microsoft.com and MICHAEL J. JONES,Mitsubishi ElectricResearch Laboratory, 201 Broadway Cambridge, MA 02139, USA, mjones@merl.com- Received September 10, 2001; Revised July 10, 2003; Accepted,July11,2003.

[2] Illumination-based texture descriptor and fruitfly support vector neural network for image forgery detection in face images ISSN 1751-9659 Revised 22nd February 2018 Accepted on 16th March 2018 E-First on 30th April 2018 doi: 10.1049/iet-ipr.2017.1120 www.ietdl.org Rajan Cristin1 , John Patrick Ananth2 , Velankanni Cyril Raj

[3] Hayat, K., Qazi, T.: 'Forgery detection in digital images via discrete wavelet and discrete cosine transforms', Comput. Electr. Eng., 2017

[4] Shen, X., Shi, Z., Chen, H.: 'Splicing image forgery detection using textural features based on the grey level co-occurrence matrices', IET Image Process.,2017

[5] Bhartiya, G., Jalal, A.S.: 'Forgery detection using feature-clustering in recompressed JPEG images', Multimedia Tools Appl., 2017.

[6] Farooq, S., Yousaf, M.H., Hussain, F.: 'A generic passive image forgery detection scheme using local binary pattern with rich models', Comput.Electr. Eng., 2017

[7] Zhao, F., Shi, W., Qin, B., et al.: 'Image forgery detection using segmentation and swarm intelligent algorithm', Wuhan Univ. J. Nat. Sci., 2017.