International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Sep-Oct-2022 Volume 9, Issue-5
Email: editor@ijermt.org www.ijermt.org

THE CLASSIFICATION SCHEME IN IMAGE PROCESSING USING SUPPORT VECTOR MACHINE FOR FACE SPOOF DETECTION IN CNN

Dr. Vikas Jain,

Assistant Professor, SCRIET-DCA,

Ch. Charan Singh University, Meerut, Uttar Pradesh, India

ABSTRACT

The use of biometric systems has significantly increased in recent years, and they are presently being utilized widely for the purpose of identifying and verifying individuals. These biometrics are very important when it comes to the safety of the country, the area, and the whole world. The major objective of this piece is to provide a justification for the use of biometric technologies. Currently, there are a wide variety of biometric technologies that are being used. There are several different types of biometric technology, such as iris scanning, palm vein biometrics, voice recognition, and facial recognition. When it comes to these biometric devices, spoofing is the most significant risk. At the present time, the biometric technology that is used the most often is fingerprint recognition. Face-spoofing may be accomplished in a variety of ways, including attacks that include the use of masks, attacks that use images and videos, and This article discusses a number of different approaches for identifying face spoofing. Face has recently garnered greater interest in a number of different sectors due to the fact that it is both secure and easy to use. Applications that depend on the recognition of human faces for daily identification as well as the storage of sensitive data often utilize face detection that is based on biometric systems for authentication purposes. In spite of this, face recognition systems are still susceptible to assaults that have the capability of using face spoofing. Despite the fact that other researchers have proposed and shown effective methods of detecting face spoofing, our goal is to offer a solution for face spoofing that makes use of machine learning techniques.

Keywords: - *face recognition, spoofing, Artificial Neural Network, classification.*

INTRODUCTION

Biometric-based access control systems are becoming more popular as a result of the ease and simplicity with which they may be used by a growing number of individuals. An increase in the efficiency of automated processing and a reduction in the amount of human labor necessary for identity verification are both outcomes of this. The face is one of the most significant sources of visual biometric data, and it may be readily collected in an uncontrolled setting without the user having to be involved. A strong focus should be placed on the precise detection of simulated faces in order to reinforce face-based identification and access control systems against the possibility of assaults. An approach to deep learning that was developed not too long ago and is based on convolutional neural networks (CNNs) turns out to be a very efficient way to interact with visual input. The CNN is provided with the data, and it automatically acquires knowledge of the intermediate-level hierarchical characteristic. Several CNN-based approaches, such as ResNet and Inception, demonstrated exceptional performance when they were put through the difficulty of picture categorization. One of the

primary objectives of this study is to investigate the effectiveness of CNNs in combating face spoofing. Be prepared. Over the last several years, ant spoofing has emerged as a topic of intense interest in both the academic and professional areas simultaneously. It was discovered that CNNs that were based on multi-modal methods (RGB, depth, and IR) performed better than single-modal classifiers when a variety of CNN-based solutions were used. On the other hand, there is an urgent need for simpler solutions that are not only more effective but also less complex. As a result, we present a streaming-modulated extreme light network design known as FeatherNet A/B. This architecture is able to overcome the limitations of Global Average Pooling while simultaneously reducing the overall number of parameters. Our one and only FeatherNet, which has been trained only on depth photos, provides a superior baseline with 0.00168 ACER, 0.35M parameters, and 83M FLOPS when compared to other networks.

Although it has been some time since then, deep convolutional neural networks have shown that they have the potential to be useful in a variety of computer vision applications. Deep learning has been used by a number of academics as a means of combating face spoofing in order to ensure that it is not successful. The majority of techniques, on the other hand, only make use of the last layer that is completely integrated in order to differentiate between actual and phony photographs. We train a convolutional neural network (CNN) to identify fraudulent faces by extracting deep partial features. This is accomplished by drawing inspiration from the concept that each convolutional kernel functions similarly to a partial filter. Using CNN's fine-tuning on face spoofing datasets to eventually apply it to other datasets is the technique that we have advised. Reducing the dimensionality of features by the use of the block principle component analysis (PCA) method is the next stage in the process of avoiding overfitting. In the end, the support vector machine (SVM) is used to differentiate between genuine and fabricated facial expressions. Some examples of biometric identification technologies that have experienced remarkable breakthroughs and increasing usage over the last few decades include fingerprinting, iris scanning, and finger vein analysis. These are just a few examples. Because of advancements in graphics processing unit (GPU) acceleration technologies and the influence of deep neural networks, face recognition systems have reached a higher level of popularity and accuracy. However, despite the fact that facial recognition technology makes it simpler to identify individuals, it also presents a new problem. Face spoofing and presentation assaults are on the increase. Attacks that utilize face spoofing, which might include the use of static photos, moving images, or even 3D masks, can damage the functionality of a face recognition system as well as its security.

OBJECTIVE

1. In visual processing, to the research categorization strategy for detecting face spoofs
2. It is important that the system can withstand several types of spoofing assaults, such as those using photos, video replays, and 3D masks.

METHODOLOGY

The objective of facial anti-spoofing is to distinguish between real and fake faces in order to find a solution to a problem involving binary classification. The stages of conventional presentation assault detection that use a natural approach involve the capture of the facial region and the extraction of characteristic features. In spite of the remarkable accomplishments of the conventional Facebook detection algorithm that is based on CNN, it is important for practical applications to have a model that combines face recognition with face spoofing. One interpretation of face spoofing detection is that it is an effort at three-way classification for both the

background fake face and the real face. This interpretation is possible when these two phases are combined. Our face spoofing detection model was constructed on top of our improved Faster R-CNN framework, which has shown exceptional performance not only with regard to face identification jobs but also with regard to object recognition procedures.

A. The first approach uses support vector machines and pre-trained convolutional neural networks for data categorization.

B.

Fig. 1. Suggested Approach Visual representation

The first is an SVM-pretrained CNN AlexNet.

The extraction of significant properties from pictures has been accomplished via the use of CNNs in order to get them ready for categorization. When it came to face classification, the use of several CNN models was necessary. AlexNet and ResNet-50 were the two convolutional neural network (CNN) models that we first used. Both of these models had already undergone training. Immediately after the feature extraction process, a support vector machine (SVM) was used for the classification process. Transfer learning was also used in the classification task, and the pre-trained AlexNet CNN was utilized for this purpose. For the purpose of carrying out the investigations, a number of different datasets appeared. In order to determine the effectiveness of each technique, a comparison of the obtained results was carried out. Specifically, we examined the results of support vector machines (SVM) and transfer learning that were performed using the pre-trained AlexNet model.

SVM and pre-trained CNN is method two.

The second step comprises the extraction of features and the classification of data by using the transfer learning capabilities of the AlexNet computer model. In the course of carrying out this study, we followed the

process that is outlined below. During the first stage, which is referred to as pre-processing, each of the images was reduced in size to a grayscale resolution, and the CNN model was transformed into an RGB image format. Two distinct types of CNNs that had been pre-trained were used in the second stage of face representation. In this particular instance, the problem was with ResNet50 and AlexNet. Following the retrieval of the relevant visual properties by CNN networks, the subsequent classification phase will make use of those qualities. In conclusion, a variety of convolutional neural networks were used in order to do face categorization. To begin, we extracted features by using two kinds of pre-trained convolutional neural networks (CNNs): ResNet 50 and Alex Net. These characteristics were then merged with support vector machine classification. Following that, we used transfer learning strategies from CNN and Alex nets that had been pre-trained for the classification tasks of the project.

For the testing, a number of different datasets were used. In the next step, we compared the outcomes obtained via the use of support vector machines and transfer learning from AlexNet that had been trained in the past. Additionally, we examined the various outcomes and evaluated the performance of each approach. For the purpose of our research, we classified faces using support vector machines (SVM) since it provides an observable classification result on nonlinear data. With the use of support vector machines (SVMs), it is possible to efficiently work through issues pertaining to machine learning and pattern recognition. Some examples of these issues are function overfitting and FR.

The supervised form of binary classification is used when the support vector machine (SVM) is employed for classification. This indicates that the training set and procedure are used in order to generate a hyperplane that maximizes the margin that exists between the two individual input classes. Within the context of the example, two distinct categories are taken into consideration for data that may be separated in a linear method. In order to differentiate between the different classes, the classification system makes use of a wide variety of hyper planes. When compared to all of the other hyperplanes, the best ones have a significant gap between them. For the purpose of improving the margin, it is vital to locate the ideal collection of black and white features. It has been recommended that a non-linear support vector machine (SVM) classifier be used since real-time data is not linear and hence cannot be recognized using a linear classifier. The kernel approach is included in the package for support vector machines (SVMs) that are not linear. The kernel technique is an approach that is both very fascinating and quite helpful. The selection of the most suitable kernel for a particular application continues to be a difficult task when using a features set. For the purpose of this investigation, the kernel function that was chosen is the one that does not use any optimization techniques. This means that it does not have any parameters that are capable of being tailored to achieve optimal performance.

All of the testing was done on the Windows platform, which was accompanied by an Intel Core i7 processor operating at 2.7 GHz, 16 gigabytes of random access memory (RAM), and an NVIDIA GeForce 1050TI graphics card. Tests of the methodology were carried out using MATLAB 2018a, and the task of feature selection and classification was successfully completed. We demonstrated that pre-processing is necessary before commencing training using convolutional neural network topologies. This is prior to the training process. For each dataset, the photos in ResNet-50 are shrunk to include 224 224 pixels, while the images in AlexNet are resized to contain 227 227 pixels. The performance of the CNN system that has been pre-trained is evaluated based on the recognition accuracy quality measure. The percentage of labels that were correctly predicted is something that demonstrates the accuracy of the prediction.

RESULTS AND DISCUSSION

Using a deep convolutional neural network (CNN) with a support vector machine (SVM) classifier for image detection ResNet 50 and Alex net, as well as AlexNet-based transfer learning approaches, we describe the experimental results for face recognition. These findings were obtained by using a specified data set. The primary purpose of the three main trials that were conducted for the research was to evaluate it in comparison to the CNN architecture that had been pre-trained. There is a percentage of accuracy shown in both Table 1 and Figure 2..

Table 1. Machine learning's accuracy rate in detecting face spoofs

Machine	ORL	FEL	CLAS'	LE%
Learning		Face	Face	
Principles				
Transfer	9920%	9K.st%	100%	95.7%
Leann pa				
AlexNet -	9920%	97.6%	99.6%	94's
SVM				

The graphic illustrates the competitive performance of an artificial neural network (ANN) that has been pre-trained to recognize face spoofing by comparing false and genuine photographs and generating findings with a high degree of accuracy.

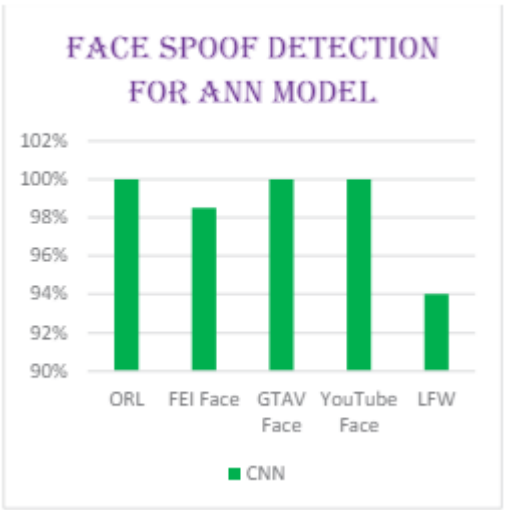

Fig. 2. Analyzing how well different face spoof recognition methods perform

At the outset, we constructed an SVM classifier by employing a CNN that had been pre-trained and given the name AlexNet. Subsequently, we evaluated its performance on picture characteristics. After that, we used an SVM classifier in order to retrieve the image features that ResNet-50 had instructed us to learn. Following the implementation of AlexNet network transfer learning, the next step was to assess the performance of the classification endeavour. The precision of performance recognition served as the foundation upon which everything that came before it was constructed.

In this work, a support vector machine (SVM) was trained by extracting picture characteristics from a CNN AlexNet that had already been trained. As was discussed before, we need to convert any grayscale photographs to RGB and resize all of the photographs to a height and width of 227 227 pixels for AlexNet. In order to minimize any chance of bias in the results, our implementation used a random split of the data, with eighty percent of the data being allocated to the training set and twenty percent being allocated to the test set. It is important to bear in mind that while AlexNet has a large number of layers, not all of them are required for the process of feature extraction.

A number of characteristics, including blobs and edges, are extracted by the first layer of the classification system. This is the reason why utilizing deep layers results in the appearance of more identifiable features. a collection of characteristics that were obtained from the 'fc7' layer. Following the extraction of the feature of the layers that were entirely connected, we examined the performance using a variety of characteristics. This was followed by the application of SVM to the classification problem. Following the extraction of features from the "fc8" layer, a vector of 4096 dimensions was produced.

A linear kernel function was used for the support vector machine (SVM), and the optimization of this function was not performed. Vector data is sent to the kernel function, which then returns the data in its most optimum form. Only twenty pieces were included in the "MiniBatchSize" set. With the help of SGD, also known as stochastic gradient descent, we trained. Every single one of the datasets that were provided was used in order to conduct the evaluation of the approach's outcomes. the 'fc6', 'fc7', and 'fc8' layers were responsible for retrieving the characteristics being discussed. The best feasible level of identification accuracy was achieved by the use of attributes derived from the "fc7" layer.

With this outcome, it is shown without any shadow of a doubt that "fc7" is capable of providing an outstanding feature. It has been shown that the "fc7" layer has made great progress in terms of its capacity to differentiate between classes. Based on the results of the experiment, it was determined that the network performed much better on YouTube face datasets (100 percent accuracy) as compared to ORL (99.20 percent accuracy) and GTAV (99.6 percent accuracy). The process of visualizing the findings via the use of transfer learning, AlexNet, and FDM is the first step toward getting ideal outcomes (up to one hundred percent accuracy). Additionally, the accuracy of the pre-trained CNN that used SVM and AlexNet was one hundred percent when applied to the YouTube face dataset, the ORL dataset, and the GTAV dataset simultaneously. Within the YouTube dataset as well as the GTAV dataset, the AlexNet model is able to obtain a higher level of accuracy of one hundred percent by utilizing transfer learning methods. In addition, we examined the outcomes of testing the models on the DB Collection dataset, which is comprised of photos from all of the previous datasets combined. When the AlexNet + SVM model was used, the results were as follows: 97% accuracy, 90.20% accuracy, 97.50% accuracy, and 94.60% performance, respectively. Based on the datasets that have been provided, we are able to see the accuracy value of precision for SVM and Alex net, which falls within the range of 92% to 99%. Through the use of the ResNet-50 + SVM technique, a range of 92.22% to 100% was accomplished.

CONCLUSION

Face spoof detection is a challenging topic that we tackle in this study. Additionally, it is particularly relevant in the context of cross-database applications. We recommend employing Image Distortion Analysis (IDA) for face spoof identification rather to the bulk of the current approaches, which depend on motion or texture-

based features (IDA). This way, we can identify fake faces more accurately. Specular reflection, blurriness, color moments, and color diversity are the four kinds of IDA features that were developed for the spoof face photographs. These features were created in order to take into account the image distortion that was caused by specular reflection. Through the process of combining the four individual features together, an IDA feature vector of 121 dimensions may be generated. When deciding whether to employ genuine or false faces, an ensemble classifier is used. This classifier is made up of two support vector machine classifiers that have been trained for various types of spoof assaults. According to the findings, ABANN is able to maintain a processing time and estimated detection rate that are comparable to those of the AdaBoost detector, while simultaneously achieving a significant reduction in the number of false positives.

REFERENCE

1. Nagpal, C., & Dubey, S. R. (2019, July). A performance evaluation of convolutional neural networks for face anti spoofing. In 2019 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.
2. Zhang, P., Zou, F., Wu, Z., Dai, N., Mark, S., Fu, M., ... & Li, K. (2019). Feathernets: convolutional neural networks as light as feather for face antispoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 0-0).
3. Li, L., Feng, X., Boulkenafet, Z., Xia, Z., Li, M., & Hadid, A. (2016, December). An original face anti-spoofing approach using partial convolutional neural network. In 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-6). IEEE.
4. Lin, H. Y. S., & Su, Y. W. (2019, November). Convolutional neural networks for face antispoofing and liveness detection. In 2019 6th International Conference on Systems and Informatics (ICSAI) (pp. 1233-1237). IEEE.
5. Lucena, O., Junior, A., Moia, V., Souza, R., Valle, E., & Lotufo, R. (2017, July). Transfer learning using convolutional neural networks for face anti-spoofing. In International conference image analysis and recognition (pp. 27-34). Springer, Cham.
6. George, A., & Marcel, S. (2020). Learning one class representations for face presentation attack detection using multi-channel convolutional neural networks. IEEE Transactions on Information Forensics and Security, 16, 361-375.
7. Ma, Y., Wu, L., & Li, Z. (2020). A novel face presentation attack detection scheme based on multi-regional convolutional neural networks. Pattern Recognition Letters, 131, 261-267.
8. Rehman, Y. A. U., Po, L. M., & Liu, M. (2020). SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network. Expert Systems with Applications, 142, 113002.
9. Shahverdy, M., Fathy, M., Berangi, R., & Sabokrou, M. (2020). Driver behavior detection and classification using deep convolutional neural networks. Expert Systems with Applications, 149, 113240.
10. Yu, Z., Zhao, C., Wang, Z., Qin, Y., Su, Z., Li, X., ... & Zhao, G. (2020). Searching central difference convolutional networks for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5295-5305).
11. Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761.

12. Zhang, Y., Yin, Z., Li, Y., Yin, G., Yan, J., Shao, J., & Liu, Z. (2020, August). Celeba-spoof: Largescale face anti-spoofing dataset with rich annotations. In European Conference on Computer Vision (pp. 70-85). Springer, Cham.
13. Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on face and palmprint biometrics. Signal, Image and Video Processing, 11(7), 1253- 1260.
14. Chinchu, S., Mohammed, A., & Mahesh, B. S. (2017, July). A novel method for real time face spoof recognition for single and multiple user authentication. In 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (pp. 376-380). IEEE.
15. Liang, Y., Hong, C., & Zhuang, W. (2021). Face Spoof Attack Detection with Hypergraph Capsule Convolutional Neural Networks. International Journal of Computational Intelligence Systems, 14(1), 1396-1402.
16. Nixon, K. A., Aimale, V., & Rowe, R. K. (2008). Spoof detection schemes. In Handbook of biometrics (pp. 403-423). Springer, Boston, MA.
17. Nasiri-Avanaki, M. R., Meadway, A., Bradu, A., Khoshki, R. M., Hojjatoleslami, A., & Podoleanu, A. G. (2011). Anti-spoof reliable biometry of fingerprints using en-face optical coherence tomography. Optics and Photonics Journal, 1(03), 91-96.
18. Eskandari, M., & Toygar, Ö. (2015). Selection of optimized features and weights on face-iris fusion using distance images. Computer Vision and Image Understanding, 137, 63-75.
19. Patel, K., Han, H., & Jain, A. K. (2016). Secure face unlock: Spoof detection on smartphones. IEEE transactions on information forensics and security, 11(10), 2268-2283.
20. Patil, P. R., & Kulkarni, S. S. (2021). Survey of non-intrusive face spoof detection methods. Multimedia Tools and Applications, 80(10), 14693-14721.