Original Article

Face Biometric Prediction and cyber-attacks experienced Using Deep Learning Model

Emperor Journal of Applied Scientific Research
ISSN No. 2581-964X(O)
Vol. 4 Issue–03 March 2022

http://ejasr.mayas.info
http://dx.doi.org/10.35338/EJASR.2022.4301

K. Manikandan
Assistant Professor
Department of ECE
Government College of Engineering, Sengipatti
Email : kmanikandan028@gmail.com

Abstract
Identify the Face biometric prediction by using digital image processing techniques as well as deep learning model. So we introduce image processing and deep learning technique to determine face at initial stage. Initially, the source images are collected from by using the U-Net based technique. And also extract the features from input image. Finally, classify the images as diseases affected or healthy as classify by using Deep Convolution Generative Adversarial Network (DCGAN). In this proposed model, experimentation is conducted using the python OpenCV model, and the performance is evaluated using different performance measures, which is designated in the result section. During the feature extraction process, the threshold values are also dynamically modified. The CNN's advantage is clear because of the uncertainty caused by noise. In the proposed method, 97.94 percent of the data was correctly classified.

Keywords— Adversarial Network , U-Net based technique

I. INTRODUCTION

Currently, spoofing attacks can fool the facial biometric. Fake faces using masks, printed images, films, and so on are all examples of spoofing assaults that can be used as examples. These include [1], Face unlock, Veriface, Visidon, Facelock, Luxand Blinkand, Facelock pro, and Fast Access. With no trouble whatsoever, these systems may be readily tricked, and all that is required is an image of the person being spoofed. Some people can't access the system if they forget their password or someone attempts to hack the password, although this isn't always the case. The fact that most biometric systems used for security purposes are 'uni-modal' should be taken into consideration. The uni-modal biometric system, on the other hand, uses only one source of information for authentication.

As a result of these shortcomings, researchers are now developing a system that combines numerous biometric parameters in order to improve the identification process. To improve recognition accuracy, a multi-featured biometric system combines data from numerous qualities [2]. Because of the inclusion of numerous distinct biometric features inside a single system, these unimodal biometric systems are extremely adaptable. The difficulty of selecting feature extraction algorithms, SIFT (scale invariant feature transforms), transformation methods, normalisation processes, and the high dimensionality problem [3] is still unresolved, though [3]. The biometric system's "feature level fusion" is therefore less targeted by various researchers than the uni-modal biometric system due to the existence of such open issues in the biometric system. In most cases, the only way to choose valuable features from a merged feature space is through optimization. [4] Oppositional Gray Wolf Optimization technique is used to recognise fraudulent faces from genuine faces.

There are no unified taxonomies for spoofing detection approaches. Because of this, we'll break down face spoofing identification systems into three subcategories here. Face anti-spoofing techniques can be divided into three categories: hardware-dependent, challenge-dependent, and software-dependent. Each of these categories has its own set of advantages and disadvantages. It's still possible to access photographs of the target person from any of the social networks. Nonetheless "Crude" photo attacks refer to facial recognition systems that can be fooled by photographs. Different non-intrusive software dependant ways were thus suggested to overcome the difficulties of spoofing attacks [5]. Spoofing attacks can be detected using a variety of visual indicators, including scene context and motion, and a technique that can work just on single photographs of the face regions becomes a competing challenge to be completed. Because the information used to identify a person's face may also be used to detect spoofing, this is a positive task [7]. When it comes to single photographs of the facial areas, strategies that function by exploiting the fact that the images of fake faces taken via masks, video displays, and printed photos can have a broad range in

texture and image quality exploit this. It is the movement or position of the facial muscles beneath the skin that constitutes one or more facial expressions. Emotional states can be conveyed through these motions, according to some dubious hypotheses [8]. Nonverbal communication includes, for example, the way people express themselves through their facial expressions.

Literature survey

There are many different types of spoofing, and Chingovska [9] provides a brief glimpse into the detection and defence of these attacks. IP spoofing attacks and URI spoofing attacks are both feasible. Attacking IP spoofing is a form of forging IP source addresses in order to appear to be a trusted user. IP spoofing detection methods were proposed by Feng [10]. Hosting-based OS fingerprinting uses idle mode methods to verify arriving packets' operating systems to its database, which is a powerful tool for filtering IP spoofing. The ANTID (Anti-Dos) figure printing method is an effective way of identifying and filtering attack faked packets. During DDoS attacks, the TTL value of the source packet header was employed to filter out flooding traffic.

A score-level late fusion approach was developed by Liang Zheng et al. [11]. The sorted score curve was used to determine the feature's efficacy in this manner. There are two advantages to the author's score-level fusion technique that he suggests. Using an unsupervised, query-adaptive approach, the first method predicts the usefulness of each feature that will be fused together. Because ineffectual characteristics are unlikely to have an adverse effect on the overall accuracy, "safe" fusion is possible. Our method's offline phases are not dependent on the test database, which is a significant benefit. Fusion is now compatible with dynamic databases because of this.

The multiple descriptor fusion described by Arashloo et al. [12] concerning the Dynamic texture descriptor integrating blur tolerant descriptor with local phase quantization is more effective for face spoof detection than previous approaches. Anti-spoofing tactics are improved and systems are more secure as a result of the numerous data patterns representations and grid and layered representation of information that is digitalized. It has progressed from face detection to spoof detection in biometric systems to meet the current needs.

The effectiveness of Boulkenafet et al. [13]'s 'colour texture analysis' technique is entirely dependent on the variety of training data. Color texture analysis techniques performed better after training using the CASIA Face Anti-spoofing database, which contains images of varying imaging qualities, and then testing against the Reply attack database, which is extremely limited. However, it should be highlighted that when trained on limited data and subsequently tested on a more diversified dataset such as the CASIA Face Anti-spoofing database, the technique performed less well than it did on the Replay Attack database. In order to explain this, it is owing to the fact that only fundamental LBP was taken into account while looking at facial appearance (Local Binary Patterns).

Problem Definition

Facial recognition frameworks are extremely prone to spoofing attacks, which creates a significant security risk in the biometrics field. In addition, several of the earlier presented methodologies have shown promising results when it comes to detecting face spoofing attacks through intra-test evaluation. As a result, in inter test evaluation, the majority of these techniques produce inaccurate decisions on the recognition of authentic faces with unseen attacks. In the biometric anti-spoofing research field, however, this influence is viewed as a major challenge. Extracting features from a user's input image is done using a biometric recognition system, which is utilised to identify legitimate entries. The extracted feature set is compared to a database set of feature sets to determine the person's identification. Biometric recognition has been investigated on a variety of distinct and specified behavioural and physiological features. The face from the user input image is used for spoof detection in order to distinguish real user input images from counterfeit ones.

Proposed technique

This section introduces the generalised texture representation paradigm known as the convolution neural neteork (CNN). By incorporating the new model's noise-adjustment capabilities, the LBP can better handle minor changes in pixel intensities. Images with a high level of noise can be better represented using a CNN model. The CNN with dynamically shifting threshold is introduced first, followed by a discussion of CNN.

NUAA Dataset

The NUAA Photograph Imposter Database makes both real client access and picture attacks available to the public. Each of the 15 subjects has 500 photos of 640 x 480 quality in the collection. The photographs were taken with a standard webcam. The facial photographs are acquired over a 14-day period and in three separate sessions, each

with a different lighting and ambient setting. In both the testing and training sessions, the participants were not the same.

Classifiers

There is a database of authorised individuals in any authentication system that has been collected during the enrolling process. The system compares the input image's feature vectors to those in the database to verify the image taken by sensors. The input is either acknowledged as real or rejected as a hoax by this system. In its simplest form, the system determines whether an image is real or fake based on its input, hence its response is binary (1 or 0). For face detection, distance measures, CNN systems such as Neural network and Fuzzy systems are widely employed. One of the most often used algorithms for face classification is the CNN classifier, which has been observed to be one of the most popular approaches in the literature.

For classification, we'll use a Convolutional Neural Network (CNN) (CNN). The outputs of CNN classification are stored in picture format and fed into CNN as an input for this application.
Multiple layers of neural networks, such as pooling, recurrent learning units (ReLUs), and fully connected nodes (FCNs), make up a CNN. In this case, CNN is utilised mostly to recognise picture features, such as the image's edges and form..

A. Convolutional Layer

In CNN architecture, the first-come, first-served approach is usually complicated. CNN typically accepts input levels of MxNx1. Here are the 2D image sizes for various MxN values. As the input image has the same depth as the output image, CNN applies filters with specific parameters that are then integrated into the output image. Input images are only allowed to follow a certain curve or shape, which is indicated by the filter. Filter-induced contrast in the input image increases as the curved shape's contrast value increases. An equation can be used to represent the convection process. (1).

$$s(t) = (x^{*}w)(t) \quad (1)$$

B. Pooling layer

The purpose of this layer was to reduce the data's overall size. Multiplying data into parts and replacing each section with one value reduces the overall amount of the metric data. These features include max and average pools, which modify the arrays in a bucket to their highest or most common values.

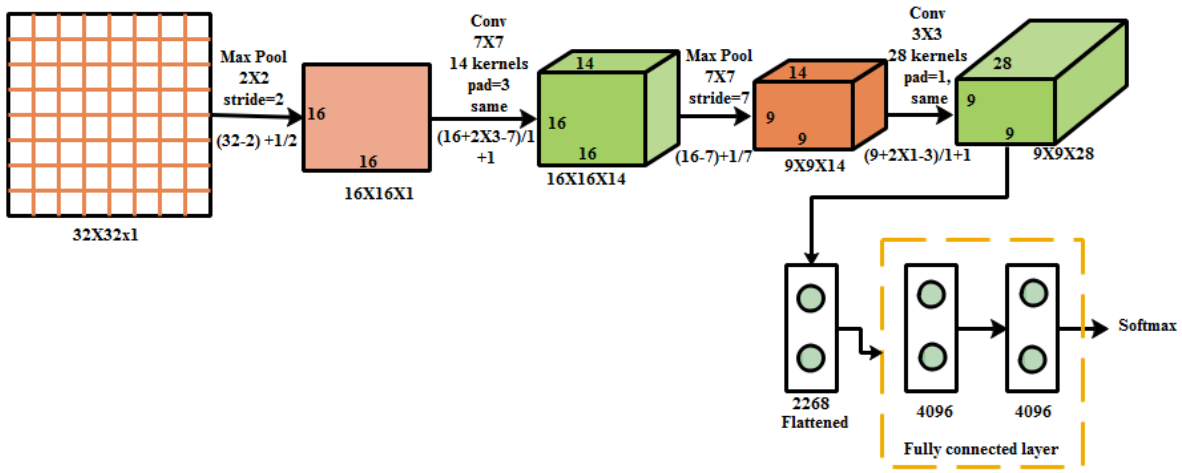

Figure.1. Architecture of the pre-trained deep CNN systems

C. Fully Connected layer

These layers are restructured to fit the network's architecture. All of the input and output parameters of an operation are connected to one another in a completely connected layer. All of the activity from the previous layer is passed via this layer, just like a standard artificial neural network.

D. Soft-max layer

The softmax function uses the inputs from the previous levels to calculate the probabilities for each class. A lot of what gets produced depends on this level, since it's the anticipated output class with the highest likelihood for a given set of data. Images may be classified using a variety of deep neural networks. Transfer learning is necessary to improve our classification problem, even though these networks have already been trained on other images. We have the ability to tailor them to your specifications.

All target networks' hyper training criteria remained constant. The dates have been separated into multiple eras, with a maximum of 25 possible. When updating internal model factors, the size of a mini-batch indicates how many samples are needed. Mini-batch size was 7 and the training rate was 0.0001 for each session in our experimentation.

Table 1
Principal Parameters of convolution layer

	Output Shape	**ernel Size**	**Numbers of kernel**	**tride**	**adding**
Max pooling1-1	16X16X1		--		-
Convolution1-1	16X16X14		14	ame	
Max pooling1-2	X9X14		--		-
Convolution1-2	X9X28		28	ame	
Flattened	X9X28	-	--	-	-
Fully connected layer (2)	096	-	--	-	-
Output (softmax)	2	-	--	-	-

Performance Measures

There are four parametric measures used to evaluate the proposed model performance, which are labelled as follows as,

Sensitivity: It defines the proportion of positives measured as such is defined by using the Equation (1);

$$Sensitivity = \frac{TP}{TP+FN} \quad (2)$$

Specificity: It defines the proportion of real negatives that are correctly identified by using the Equation (2);

$$Specificity = \frac{TN}{TN+FP} \quad (3)$$

Accuracy: It is the proportion of true outcomes (both TP and TN) in the population is defined by using the Equation (7);

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

F-score: When calculating the model's sensitivity and specificity, you'll use the F-score, which is also known as the harmonic mean of those two values.

$$F-score = 2 \cdot \frac{Sensitivity \cdot Specificity}{Sensitivity+Specificity} \quad (5)$$

Table 2
Performance analysis of the proposed scheme under different training sizes and diverse measures

Test and Training Size	Accuracy (%)	Sensitivity (%)	Specificity (%)	F-score (%)
10%-20%	81.54	78.51	85.72	72.12
60%-40%	86.24	83.96	86.32	72.64
40%-60%	89.99	87.56	88.55	84.25
80%-20%	92.95	90.01	91.20	89.47
Average	87.71	85.01	88.25	79.62

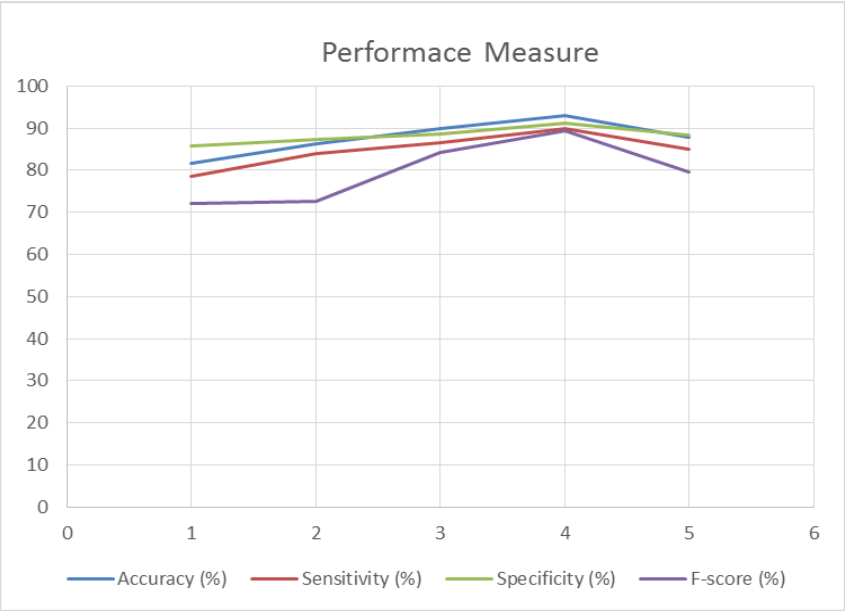

Figure 2: Graphical representation of performance measure

In figure 2 represent that the performance of CNN model performance

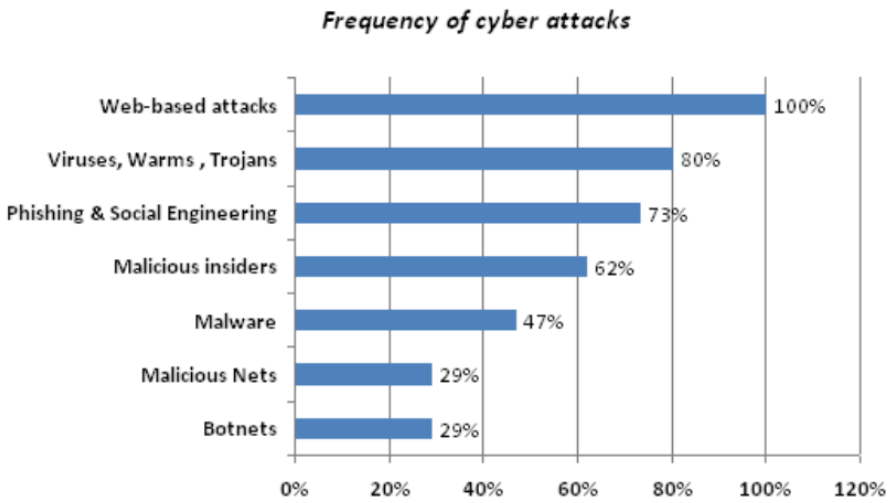

Figure 3: cyber-attacks experienced by benchmark example

There are an average of 50 cyber-attacks each week in the benchmark sample of 45 firms, which means that each company encounters more than one successful attack every week.

II. CONCLUSION

A multimodal biometric framework for the detection of face spoofing was suggested in this study. Our suggested approach relies on the extraction of image features from 'colour spaces,' which is a key component of our work to date. Using the CNN model helps enhance the system's performance, especially when dealing with noisy pictures. This study used FLTP, a CNN extension, to identify people by the expressions on their faces. During the feature extraction process, the threshold values are also dynamically modified. The CNN's advantage is clear because of the uncertainty caused by noise. When fuzzy concepts were incorporated into LTP, the results showed better gains in accuracy. When working with noisy photos, t can boost the system's performance.

III. REFERENCE

1. Hernandez-Ortega J, Fierrez J, Morales A, Galbally J. Introduction to face presentation attack detection. InHandbook of Biometric Anti-Spoofing 2019 (pp. 187-206). Springer, Cham.
2. Daniel N, Anitha A. Texture and quality analysis for face spoofing detection. Computers & Electrical Engineering. 2021 Sep 1;94:107293.
3. Rabie A, Handmann U. Multi-modal biometrics for real-life person-specific emotional human-robot-interaction. In2014 IEEE International Conference on Robotics and Biomimetics (ROBIO 2014) 2014 Dec 5 (pp. 344-349). IEEE.
4. Kavitha P, Vijaya K. Optimal feature-level fusion and layered k-support vector machine for spoofing face detection. Multimedia Tools and Applications. 2018 Oct;77(20):26509-43.
5. Leitch R. Creatively researching children's narratives through images and drawings. InDoing visual research with children and young people 2009 May 7 (pp. 59-80). Routledge.
6. Komulainen J, Hadid A, Pietikäinen M. Context based face anti-spoofing. In2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS) 2013 Sep 29 (pp. 1-8). IEEE.
7. Tan X, Chen S, Zhou ZH, Zhang F. Face recognition from a single image per person: A survey. Pattern recognition. 2006 Sep 1;39(9):1725-45.
8. Yuan X, Park IK. Face de-occlusion using 3d morphable model and generative adversarial network. InProceedings of the IEEE/CVF International Conference on Computer Vision 2019 (pp. 10062-10071).
9. Chingovska, I, Nesli, E, André, A & Sébastien, M 2016, 'Face Recognition Systems under Spoofing Attacks', In Face Recognition across the Imaging Spectrum; Bourlai, T., Ed.; Springer: Berlin/Heidelberg, Germany, pp. 165-194
10. Feng, Litong, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan Terence Chun-Ho Cheung & Kwok-Wai Cheung 2016, 'Integration of image quality and motion cues for face anti-spoofing: A neural network approach', Journal of Visual Communication and Image Representation, vol. 38 pp. 451-460.
11. Mei, L, Yang, D, Feng, Z & Lai, J 2015, 'WLD-TOP Based algorithm against face spoofing attacks. In Biometric Recognition, Proceedings of the 10th Chinese Conference on Biometric Recognition.
12. Arashloo, SR, Kittler, J & Christmas, W 2015, 'Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features', IEEE Trans. Inf. Forensics Secur, vol. 10, pp. 2396-2407.
13. Boulkenafet, Z, Komulainen, J & Hadid, A 2015, 'Face anti-spoofing based on color texture analysis', in IEEE International Conference on Image Processing (ICIP2015)