International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Security System based on Transfer Learning Model

Dubasi Tejaswini[1], Dr. Uma Rani Vanamala[2]

Master of Technology, Department of Information Technology, JNTUH UCESTH, Kukatpally, Hyderabad, Telangana, India, 500085.
Email: *tejaswini12cp12[at]email.com*

Professor of Computer Science and Engineering, JNTUH UCESTH, Kukatpally, Hyderabad, Telangana, India, 500085.
Email: *umaranivanamala[at]email.com*

Abstract: ***Present days, we have technology that helps us in security in different domains such as data security, personal protection, residential security, internet security, construction security, event management security, etc. Even though we have advanced technologies, still there are loopholes in every system which can be effective or partially defective. Here, taking another step to increase the security system for advanced security system and non-physical interaction purpose by using the Transfer learning model. The Transfer learning model in Keras for security system that helps in organizations or communities to collect insights of the data which can be observed from the model by giving ImageNet data to the model. This model generates accurate results compare to traditional learning models because the transfer learning model will take the data which is already trained on one task, then this data is reassigned as input to another task.***

Keywords: Transfer Learning Model, Deep Learning, VGG 16, Image Classification

1. Introduction

1.1 Safety System

The security gadget is a means or method by way of which something is secured through a device of interworking components and gadgets. Here, the safety gadget is defined as a sensor- primarily based gadgets designed to come across or sign the intrusion on or unauthorized use of equipment, residence, shape, or leasehold. Given are few devices used for protection machine. Burglar alarms, heart alarms, smoke detectors, carbon monoxide detectors, video surveillance, environmental sensors…and many others. In line with a recent survey, 93% of Americans recall expert monitoring to be the most important feature of a home safety system.

Taking a step forward to this safety system to locate the probabilities of automation through surveillance by shooting pictures. For that transfer getting to know is beneficial to categorise the humans into legitimate and invalid users which gives authentication and does not allow trespassers. If the evaluation results properly, with the assistance of an IOT interface prototype, this idea may be designed. The maximum of use this idea will be carried out to groups, non-public organizations, and also collages in a way to lessen biometric structures and avoid bodily interplay for attendance.

1.2 Transfer Learning Mode

Working on a completely large set of statistics or a confined amount of records is tricky. To avoid this trouble, switching the studying version has grown to be a solution. By using a transfer studying model with a small amount of data, high-degree overall performance may be achieved. ImageNet, AlexNet, and Inception are example models that have the idea of switch getting to know.

Switch studying is also carried out in picture processing. Deep neural networks are used to clear up image-related tasks as they could paintings well figuring out complicated functions of the photograph. The dense layer contains the good judgment for detecting the photo consequently, tuning the better layers will not have an effect on the bottom logic. Picture reputation, item detection, noise removal for pixels, and so on. Those are ordinary utility regions of switch learning due to the fact that photograph-associated duties require simple information and pattern detection of acquainted photos.

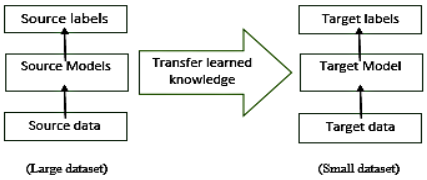


Figure 1: Transfer Learning

1.2.1 Transfer Learning benefits

A. Insufficient schooling and check statistics for constructing a version from scratch.
Transfer mastering does not require lots of data due to the fact the set of rules will not be learned from scratch to build a model. As a substitute a pre-skilled model is used which found out those parameters. Only a small quantity of data is needed to adapt the trained version to the hassle of handling it.

B. No want for labelling statistics to amplify the dataset.
Manually labelling the times is not without difficulty achieved and automated labelling may not be correctly sufficient. Switch studying tackles this problem as it isn't always required to construct a version from scratch and for this reason, no tons of facts are wanted. Just first-class-music the pre-educated version.

C. Imbalanced information distribution.
Just use a few realistic samples to satisfactory-music the model. Extra samples are favoured to do this activity however if there aren't a good deal of samples then shifting the mastering is the preferred alternative as compared to gaining knowledge from scratch.

D. Despite the fact that the education records are enough, educating a model from scratch usually requires excessive processing strength and takes plenty of time.
Transfer studying isn't always just decided on whilst there is some amount of facts but because building a model from scratch requires machines with excessive processing electricity and massive amounts of RAM. That is why switch studying might nonetheless be used although there is an enough amount of data. A sufficient quantity of facts would possibly assist in properly improving the model and adapting it to the hassle being solved. The model is anticipated to be well-known after which the engineer adapts it to the trouble being solved. This is a count of shifting from a well-known case to a more specified case that serves the motive well.

E. Despite the fact that the education time is sufficient the check statistics might not be much like the schooling statistics and a few new instances inside the test statistics are probably to be had that are not covered formerly in the schooling data. Retain new samples to cover such new instances.
Using switch learning, the pre-trained model has already hundreds or thousands and thousands of samples that cover many of the cases that would exist within the take-a-look at facts the opportunity of seeing a strange pattern inside the future drops.

F. Building a version from scratch calls for gaining knowledge of the problem and deep information on how things paint.
With the usage of transfer mastering, the researcher no longer ought to understand everything due to the fact there's no need to build an architecture from scratch.

1.2.2 Conditions to apply switch mastering

a) Facts type consistency
If snapshots are used for constructing a Deep studying model, pictures must additionally be used whilst moving the getting to known of such a model to a new hassle. The functions found out from the pix are exceptional from what has to be found out from speech alerts and vice versa.

b) Similarity in trouble domains
Statistics consistency is a very important thing that ought to be legitimate before learning to switch. Other factors contribute to maximizing the advantage of the use of transfer getting to know.

1.2.3Secureness
Training records will decrease since it takes pre-processed records.
Expanded overall performance.
Offers a greater correct and efficient version.

1.3Feasibility Study

Consistent with the evaluations on the safety device, this method is optimized compared to previous protection mechanisms. By way of the usage of the IOT interface, it could further develop with automated authentication of users to go into and go out simply by spotting their sample.

2. Literature Survey

2.1 Associated Works

a) A comprehensive Survey on switch gaining knowledge of Transfer Learning.
Switch getting to know objectives at improving the performance of target newcomers on course domains by means of shifting the expertise contained in different but associated source domains. In this way, the dependence on a large variety of target-area information can be reduced for constructing goal rookies. Due to the wide application potentialities, transfer mastering has become a popular and promising area in device getting to know. Despite the fact that there are already some valuable and brilliant surveys on transfer getting to know, those surveys introduce processes in a particularly isolated way and absence the recent advances in transfer getting to know. Due to the speedy growth of the switch learning location, it is both important and difficult to comprehensively assessment the applicable studies. This survey tries to attach and systemize the prevailing transfer getting to know research studies, in addition to summarize and interpret the mechanisms and the techniques of transfer learning in a comprehensive manner, which may additionally help readers have a better understanding of the contemporary studies status and thoughts. Not like preceding surveys, this survey article critiques more than forty consultant switch gaining knowledge of procedures, particularly homogeneous switch gaining knowledge of procedures, from the perspective of facts and model. The applications of switch mastering also are in brief delivered. In order to show the performance of various switch studying fashions, over 20 representative transfer getting to know fashions are used for experiments. The fashions are carried out on three distinctive statistics units, this is, Amazon reviews, Reuters-21578, and office-31, and the experimental consequences exhibit the importance of selecting suitable transfer mastering fashions for different packages in exercise [1].

b) Image type the usage of transfer getting to know and deep learning
Deep learning version have tested improved efficacy in photo category since the ImageNet large Scale visible recognition undertaking started out because 2010.

Classification of photos has similarly augmented inside the field of laptop imaginative and prescient with the sunrise of switch learning. To train a model on massive dataset needs huge computational sources and add a whole lot of fee to gaining knowledge of. Transfer getting to know permits to lessen the fee of gaining knowledge of and additionally assist avoid reinventing the wheel. There are several pre-skilled models like VGG16, VGG 19, ResNet50, Inceptionv3, Efficient Net, etc. Which are broadly used.

This paper demonstrates photo type the usage of pre-skilled deep neural network version VGG16 that's skilled on snap shots from ImageNet dataset. After obtaining the convolutional base version, a brand new deep neural community model is built on top of it for picture type based totally on fully connected network. This classifier will use capabilities extracted from the convolutional base model [2].

c) Human action popularity based on switch mastering technique

Human action reputation techniques have received sufficient interest amongst subsequent era technologies due to their precise functions and high capability to inspect video sequences to apprehend human movements. As a end result, many fields have benefited from human movement recognition strategies. Deep learning techniques performed a primary function in lots of approaches to human movement recognition. The new generation of studying is spreading through switch learning. For this reason, this observe's fundamental objective is to propose a framework with 3 most important stages for human action popularity. This framework affords a set of novel techniques which are three-fold as follows, in the pre-schooling phase, a general convolutional neural network is educated on a regular dataset to modify weights. To perform popularity method, this pre-skilled version is then implemented to the goal dataset and the recognition section exploits convolutional neural network and long brief time period reminiscence to use 5 special architectures. Three architectures are stand-by myself and single-circulation, at the same time as the other two are mixtures between the primary three in -move styles. Experimental consequences show that the first three architectures recorded accuracies of 83.24%, ninety.72%, and ninety.85% respectively. The ultimate two architectures achieved accuracies of 93.48% and ($.87% respectively. Moreover, the recorded outcomes outperform other today's models in the identical area [3].

d) Switch studying for Anime character reputation

Lately, the switch getting to know method is proposed for face recognition the usage of CNN. The consequences have established that the given switch learning approach offers higher popularity effects than other techniques. Retaining this in mind, professionals experimented with testing the overall performance of transfer mastering similarly by the usage of three extraordinary anime characters which have many similar capabilities to see how properly transfer studying works in detecting the Anime characters in snap shots.

This task was dependent in diverse steps:

Detecting faces of anime characters from each image the usage of lbpcascade_animeface.

Resize the snap shots to ninety six*96 pixels after which break up the idea to train and test pics.

Capabilities extraction and preprocessing become done earlier than schooling.

Train the model and examine the consequences on check and validation snap shots.

Switch gaining knowledge of lets in the Convolutional Neural network to study features from the VGG-sixteen version pre-trained with big ImageNet weights to teach the snap shots from the face database. Then the extracted capabilities are fed as input to the completely linked layer and softmax activation characteristic for category [4].

3. Design of the System

3.1Framework

One of the maximum straightforward strategies of switch learning is referred to as function switch. The network is made from many layers. These layers are important due to the fact deep getting to know is layered architecture that learns exceptional capabilities of various layers.

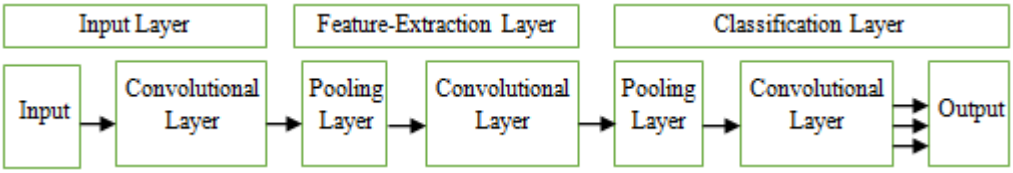


Figure2: Simple layers of Deep studying community

3.1.1 Workflow

The network accepts a three-D photo (width, height, depth for the coloration.) this constitutes the input layer, mapping the input to the subsequent layer. Next is the feature-extraction layer, which could have many internal layer such as convolutions (which map spatially placed neurons from the earlier layer thru a hard and fast of weights to the output) and pooling (which reduce the spatial size of the outputs of the convolutions), similarly to different capabilities. The output of the characteristic extraction layers are "functions"

Which can constitute capabilities from the photo (such as wheel) and can then be used hierarchically to translate to better-stage features. The final class layer pulls together the capabilities determined inside the feature-extraction layer and offers a type.

Category layer is responsible for figuring out the object from the photographs as a characteristic of the detected features. The idea behind feature transfer is then to use the input feature-extraction layers which have been trained with a given statistics set (with their weights and structure frozen) and train a brand new category layer for the related problem area. On this way, a deep getting to know community used to come across cars in an image might be have a newly educated class layer to locate bicycles. This technique is right if the two domains are similar.

3.1.2 Dataset

The dataset includes legitimate users images of a corporation with a specific domain classes. Based totally at the entry the version will compare with the dataset and gives an end as given photo consists in the dataset or now not.

Also includes information of the users in .csv format connected with images names.

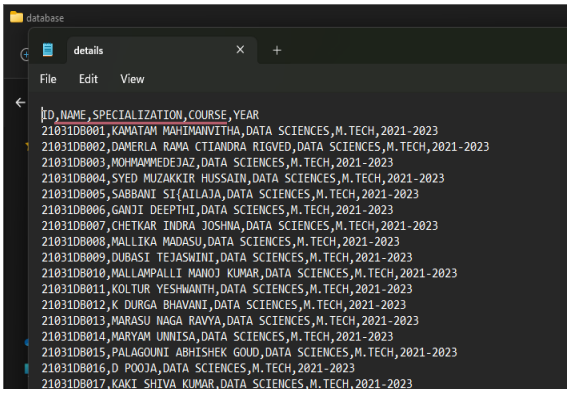


Figure 3: .CSV Data file

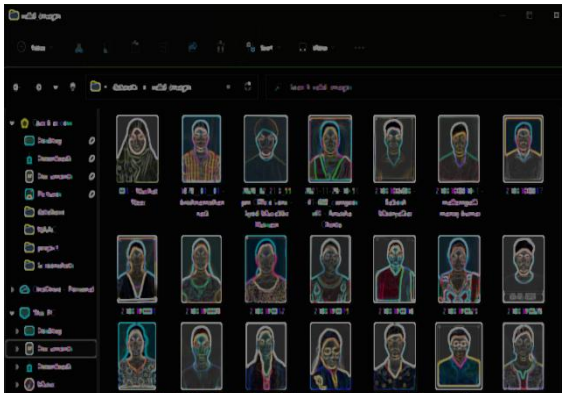


Figure 4: Image data

3.2 Fine-tuning

A simple opportunity is to introduce a brand new classification layer, however then pleasant-music the earlier layers thru additional education the use of the brand new education dataset.

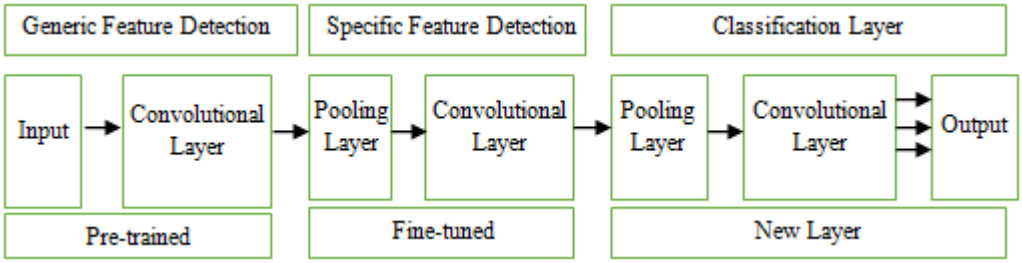


Figure 5: Fine-tuning the precise function extraction layers

This first-rate-tuning ought to suggest that we educate the later layers of the deep mastering network (meaning modify the weights primarily based upon the classification blunders) whilst leaving the earlier layers frozen.

On this way, we first-class-music the layers which are greater unique to capabilities of the type task (in comparison to earlier layers, which are more established). This technique is right whilst the problem domain names have some distance, requiring new functions to be categorised.

3.3Liveliness

The human face is an essential biometric amount which may be used to get entry to a consumer-based totally machine. As human face pixels can effortlessly be received via cell cameras and social networks, user-primarily based get entry to systems ought to be sturdy towards spoof face attacks. In other words, a dependable face-based get right of entry to machine can decide both the identification and the liveness of the enter face. To this give up, numerous characteristic-based totally spoof face detection methods were proposed. These methods usually apply a sequence of tactics towards the enter photo(s) on the way to locate the liveness of the face. On this paper, a deep-gaining knowledge of-based totally spoof face detection is proposed. Two specific deep studying models are used to achieve this, particularly neighbourhood receptive fields (LRF)-ELM and CNN. LRF-ELM is a currently evolved model which includes a convolution and a pooling layer before a fully connected layer that makes the version speedy. CNN, however, incorporates a chain of convolution and pooling layers. Similarly, the CNN version might also have greater fully linked layers. A series of experiments have been conducted on popular spoof face detection databases, namely NUAA and CASIA. The obtained consequences were then in comparison, and the LRF-ELM technique yielded better results in opposition to both databases.

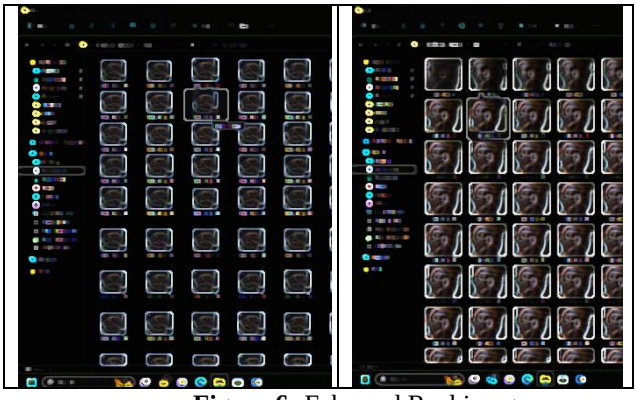


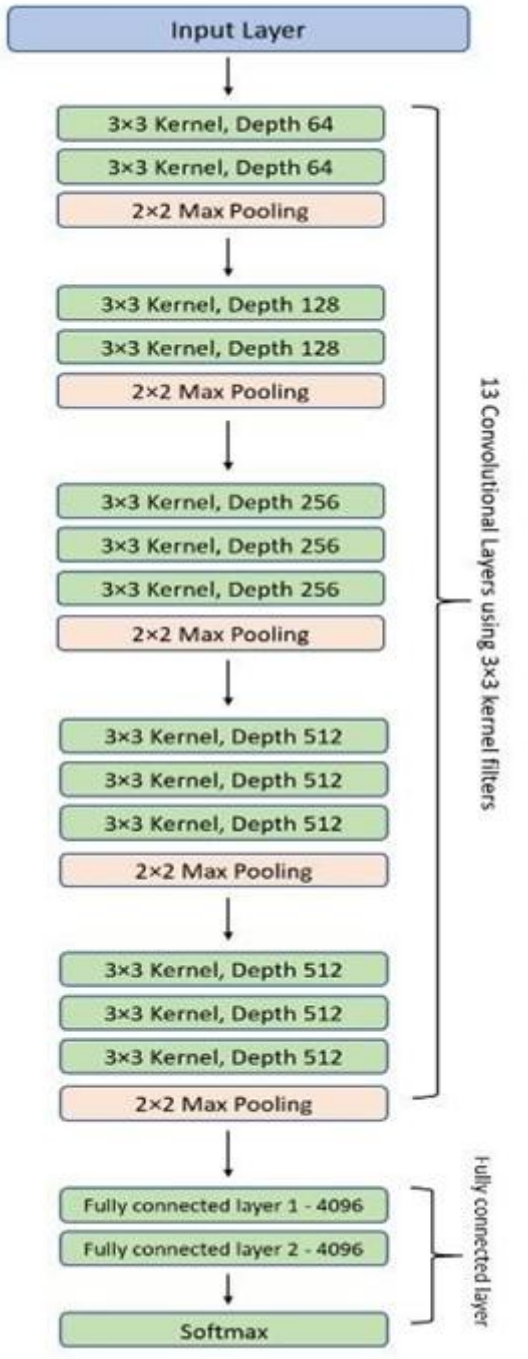
Figure 6: Fake and Real images

4. Implementation

Input: The VGGNet takes in an image input size of 224×224. For the ImageNet competition, the creators of the version

cropped out the center 224×224 patch in each photo to keep the input size of the photograph constant.

Convolutional Layers: VGG's convolutional layers leverage a minimal receptive field, i.e., 3×3, the smallest possible size that still captures up/down and left/proper. Furthermore, there are also 1×1 convolution filters acting as a linear transformation of the enter. That is accompanied by using a ReLU unit, which is a huge innovation from AlexNet that reduces education time. ReLU stands for rectified linear unit activation function; it is a piecewise linear feature a good way to output the input if tremendous; in any other case, the output is 0. The convolution stride is constant at 1 pixel to maintain the spatial resolution preserved after convolution (stride is the variety of pixel shifts over the enter matrix).



Hidden Layers: all of the hidden layers within the VGG community use ReLU. VGG does no longer usually leverage local response Normalization (LRN) as it will increase memory intake and schooling time. Furthermore, it makes no improvements to overall accuracy.

Fully-related Layers: The VGGNet has three fully linked layers. Out of the 3 layers, the first two have 4096 channels each, and the 0.33 has a thousand channels, 1 for eachelegance.

5. Observations

5.1 Working Process Output

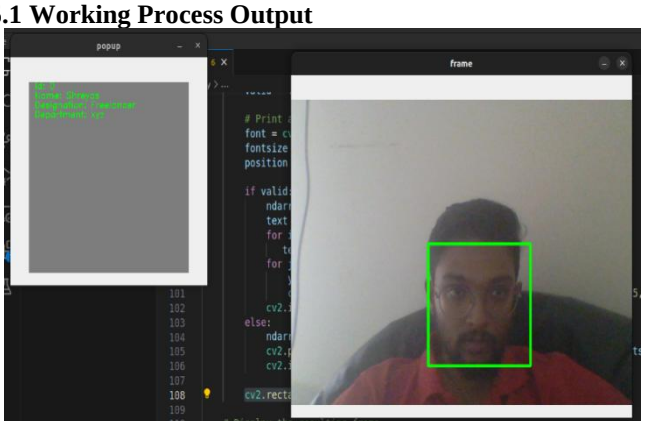


Figure 7: Output of Transfer Learning Model for Valid Image

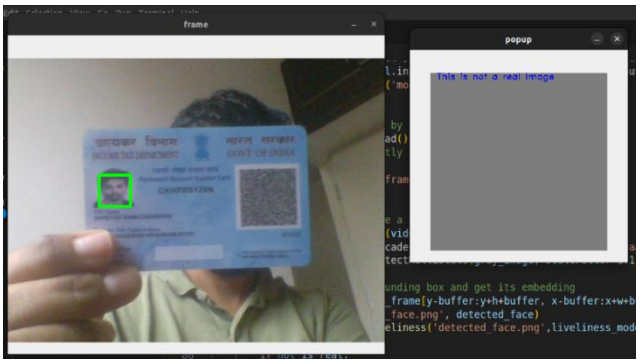


Figure 8: Output of Transfer Learning Model using Liveliness

5.2 Accuracy and Loss

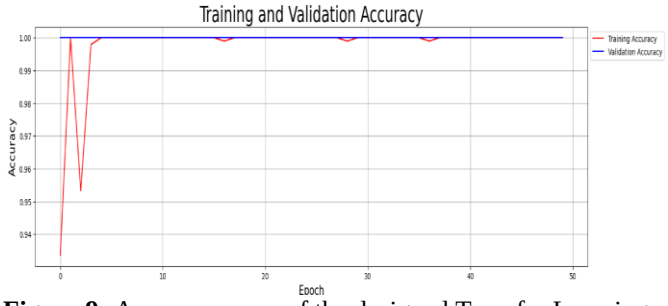


Figure 9: Accuracy score of the designed Transfer Learning Model

Having a low accuracy however a high loss would imply that the model makes large errors in maximum of the information. However, if each loss and accuracy are low, it method the version makes small errors in maximum of the facts. However, in the event that they're each excessive, it makes big errors in a number of the records. Eventually,

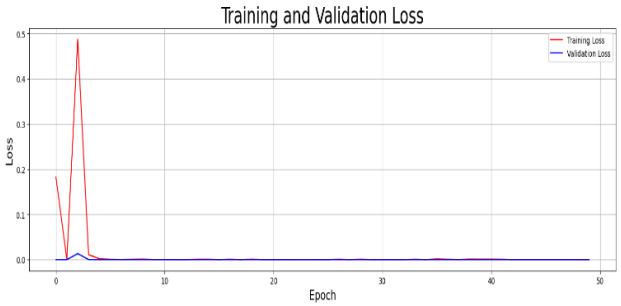


Figure 10: Loss of the designed Transfer Learning Model

6. Summary

Gift days, we've era which enables us in protection in exclusive domains together with records security, non-public safety, residential protection, internet security, production security, occasion management security, and so on.

Despite the fact that we've got superior technologies, still there are loop holes in each gadget which can be effective or partially faulty. Here, taking any other step to increase the safety system for superior security system and non-physical interplay motive through the usage of switch studying version. Switch getting to know model in Keras for protection machine allows in corporations or communities to gather insights of the records which may be discovered from the model through giving ImageNet data to the model. This version generates correct effects compare to traditional getting to know fashions due to the fact transfer mastering model will take the records which is already trained on one challenge, then this information is re-assigned as input to another challenge.

References

[1] A Comprehensive Survey on Transfer Learning | IEEE Journal & Magazine | IEEE Xplore
[2] (PDF) Image Classification Using Transfer Learning and Deep Learning (researchgate.net)
[3] (PDF) Human Action Recognition Based on Transfer Learning Approach (researchgate.net)
[4] Projects · transfer-learning-anime · GitHub
[5] https://pyimagesearch.com/2019/03/11/liveness-detection-with-opencv/
[6] https://pyimagesearch.com/2019/03/11/liveness-detection-with-opencv/

Author Profile

Tejaswini Dubasi, student of JNTUH in Department of Information Technology, specialized in Data Sciences completing Master of Technology by on Deep Learning project called Security System Based on Transfer Learning Model.

Dr. Umarani Vanamala is working professor in Department of Information Technology, JNTUH, and Professor of CSE. Her research interests include data mining.