PalArch's Journal of Archaeology of Egypt / Egyptology

FACE LIVENESS DETECTION FOR AUTHENTICATION SYSTEMS USING CONVOLUTIONAL NEURAL NETWORKS

M. Kusuma Sri[1], K. Sai Krishna[2]

[1,2] Assistant Professor, Anurag University

Email: [1]kusumasri.personal2@gmail.com, [2]saikrishnaece@cvsr.ac.in

M. Kusuma Sri, K. Sai Krishna. Face Liveness Detection for Authentication Systems Using Convolutional Neural Networks -- Palarch's Journal of Archaeology of Egypt/Egyptology 18(18), 1-11. ISSN 1567-214x

Keywords: Deep Learning, Cnn, Feather-Net Architecture, Fusion Method, Data Augmentation

ABSTRACT:

Face Anti-Spoofing is profoundly fundamental in the two scholastics and modern fields. Un-approved individuals are attempting to get confirmed through face introduction assaults (PAs, for example, a printed face photo, showing recordings on computerized gadgets, or a 3D veil assault). Along these lines, face introduction assault recognition (facial anti- spoofing) is required, which is the errand of forestalling bogus facial check by utilizing a photograph, video, veil, or an alternate substitute for an approved individual's face. The multimodal (RGB, profundity, and IR) technique dependent on CNN is proposed in this work for anti-spoofing of face for validation. The proposed technique demonstrated preferable presentation over the single model classifiers. Even though the multi-model demonstrated improved Performance, Feather-Net will present A/B network to decrease the unpredictability. This design utilized the combination technique in the Face Anti-mocking Attack identification and accomplished preferred outcomes over multi-model ways.

INTRODUCTION

The biometric framework is typically utilized for security capacities in face acknowledgment like unique mark or iris identification and penmanship confirmation. Face location might be an innovation utilized in numerous applications like facial movement catch, Eye flickering, and face acknowledgment to investigate human countenances in computerized pictures [1]. In current and cutting-edge innovations for security purposes, face acknowledgment innovation has grown quickly in a couple of years. Albeit, like other biometric frameworks, face acknowledgment is additionally immediately mock. Picture and video of an individual are frequently effectively open from the web or web-based media stages. Farce techniques are typically delegated evidence given confirmation frameworks like pictures or recordings taken from web-based media or the web [2]. Numerous ways are

accessible for face acknowledgment, yet then again, face acknowledgment strategies are risky and ineffectively unstable and can undoubtedly be tricked. Face liveness discovery is proposed to try not to parody from unstable face acknowledgment. In this submitted work, photographs, veils, and video pictures are frequently effectively perceived relying upon some facial attributes.

At present, face recognition is a basic route for character verification frameworks. Be that as it may, it stands up to the test of face caricaturing assaults, much the same as the 2D/3D Presentation Attack. Thusly, it's basic to furnish the framework with vigorous anti-spoofing calculations. Anti-spoofing is ordinarily considered as a twofold characterization. Nonetheless, these strategies experience helpless speculation's ill effects since they feel data differs from cameras/catch gadgets. Another issue of surface-based methodologies is that the surface data isn't as discriminative based on the profundity data on the 2D introduction assault identification task.

The profundity data is more discriminative since the profundity of the basic face is lopsided, and thusly the profundity pictures of the assaulting front are plane [3]. Top to bottom highlights areas of late separation utilizing profound learning procedures [4], which have semantical data than customary handmade highlights. Consequently, using profound learning for face Presentation Attack Detection (PAD) has been broadly utilized as of late; this necessitates the anti-spoofing face calculations to run with less calculation and capacity costs. Hence, it's important to build up a lightweight profound learning calculation so that ridiculing recognition is frequently utilized. Initially, Feather Nets have a thin CNN stem. Hence, the computational expense is a more modest sum. Furthermore, a substitution engineering (named as Streaming Module) is proposed, which has preferable execution exactness over the overall Average Pooling (GAP) approach.

This paper additionally proposed a substitution combination classifier engineering [5], which gathers and falls a few models gained from multimodal information, i.e., the profundity and IR information, to encourage preferable forecast exactness over single profundity models. Face anti-spoofing is treated as a parallel order issue by customary SVM (Support Vector Machine). The means are beneath: Crafted highlights identification: Various channels were utilized to identify the focuses to introduce the component. As it may highlight, the climate significantly impacts recognition; for instance, the lighting condition [10]. Besides, the element location shows restricted highlights, and hence the element focuses don't give, however much highlights' data that those CNN techniques could carry with the enormous informational indexes.

Utilizing RGB single edge with binary supervision, most methodologies receive the most elevated completely associated layer to separate the fundamental and false faces. To connect the inside and out fractional highlights from CNN and Principle Component Analysis (PCA) to downsize the measurement, and in conclusion, SVM is utilized to separate genuine and phony countenances. Accordingly, the scientists found that this will at present be improved through numerous oversights. Various casings additionally are caught by the move of the camera and structures to anticipate the depth.

There are two primary viewpoints to strengthen for the multimodal technique: (1) The pattern execution of CASIA-SURF actually includes a ton of space to improve; (2) The lightweight detail's selection will benefit more edge side applications. The paper's remainder follows as part 2 is a writing survey; section 3 is the proposed technique; part 4 is results and conversation; lastly, chapter5 is the conclusion.

LITERATURESURVEY:

Depend on methods; liveness detection can be classified mainly as motion- based, frequency-based, or quality-based.

Group Pan et al. [6] proposed a proceeding with liveness revelation strategy so on check photograph spoofing in face affirmation by seeing-eye squinting, which might be a non-intrusive way. This face liveness area method aims to contradict the personifying attack in a non-intrusive way with none outer equipment aside from a nonexclusive camera. The flicker's physiological movement is to close and open eyelids immediately; it helps spread the tears across and eliminates the surface's aggravations. Since a nonexclusive camera can catch over 15 casings for every second, the time term between outlines isn't over 70 milliseconds. At that point, the camera can charge at least two edges at the hour of the face in looking secretly.

Jukka et al. [7] proposed a method of face parody assault discovery utilizing miniature surface investigation. The idea to highlight the distinctions of miniature surface inside the component space. LBP is utilized to depict the surface. The vector in this component is then given to the SVM (uphold vector machine) classifier, which decides if the miniature surface example is phony orlive.

Kollreider et al. [8] present a development-based countermeasure that checks the association between unmistakable pieces of the face using an optical stream field. In this procedure, the information is seen as fake if the visual stream field centers around the front and the ears' bearing presents a comparable heading. The entrance was the chronicles of this subset, and the attacks were made with printed duplicates of the data. Utilizing this information base, which was not accessible, an equivalent blunder rate (EER) of 0.5% was gotten.

Eyeblink lead is executed during a Conditional Random Field framework and combined with a discriminative extent of eye states with the probability of the adaptable boosting figuring, genuine regard oppressive part for the consideration picture, called Eye intently, is described as assessing the degree of Eye's closeness. If the close assessment is higher, around then, the territory of eye closeness is likewise more prominent. The region's decision choice relies upon the most raised and base parts; nearly a face is hair and neck yet not the scene.

Anjos et al. [9] proposed a strategy for checking an individual's liveness utilizing a relationship. This strategy is named development location. To discover connection creator utilizes a fine- grained development course. Optical how is utilized to discover the course of development. This methodology is a clear cycle; however requires numerous edges to see liveness, so the client should be helpful.

Maatta et al. [10] proposed a technique dependent on neighborhood paired example [LBP]. It extricates the miniature surfaces used to try not to parody assault. These strategy investigations the facial picture surfaces to identify whether a live individual or phony picture is in front of the camera. Surfaces of face pictures are removed utilizing LBP, which gives a vigorous technique contrasted with different strategies.

Wang et.al.[11] utilizes Fourier spectra of a solitary picture or grouping of thoughts to search out the face liveness. Structures of the live face and phony faces like pictures or recordings are extraordinary. In this technique, the albedo surface standard is wont to separate fake and live colorings. This gives the distinctive light reflectivity. Fourier spectra of live and false look have such a great deal of contrasts, settling on a choice effectively phony or live.

PROPOSEDMETHOD:

Face recognition requires the anti-spoofing face algorithms to run with less calculation and capacity costs. From this viewpoint, the plan of profound learning-based anti-spoofing calculations turns out to be additionally testing. Along these lines, it is important to build up a lightweight profound learning calculation. To address these issues of computational and capacity costs, we executed a lightweight CNN architecture.

Figure1 and 2 show the flowchart of face liveness identification and order of the face, regardless of whether it is genuine or counterfeit. This paper proposed a light organization design of Convolutional Neural Network is quill net to separate the highlights from the given pictures. The Feather Nets' principle blocks have appeared in Figure 3. Quill Net is incorporates in Block A, and Block C. Plume Net is incorporates in Block A and Block B. (BN: Batch Norm; DW Conv: profundity shrewd convolution; c: number of information channels).

There are Block A/B/C, as appeared in Figure 3, to create Feather Net A/B. Square is the altered lingering block utilized as our essential structure block A, which appeared in Figure 3. Square B is the down-inspecting module of Feather Net B. Normal pooling (AP) has been demonstrated to benefit performance due to its capacity to install multi-scale data and totaling highlights in various responsive fields. Consequently, normal pooling (2x2 piece with step = 2) is presented in Block B. Plus, in Shuffle Net, the down-inspecting module joins a 3x3 halfway pooling layer with stride=2 to acquire magnificent execution. The expanding normal pooling layer functions admirably and impacts the computational cost pretty much nothing. Down-sampling of quill Net An is Block C. It is quick, with less unpredictability contrasted with Block B.

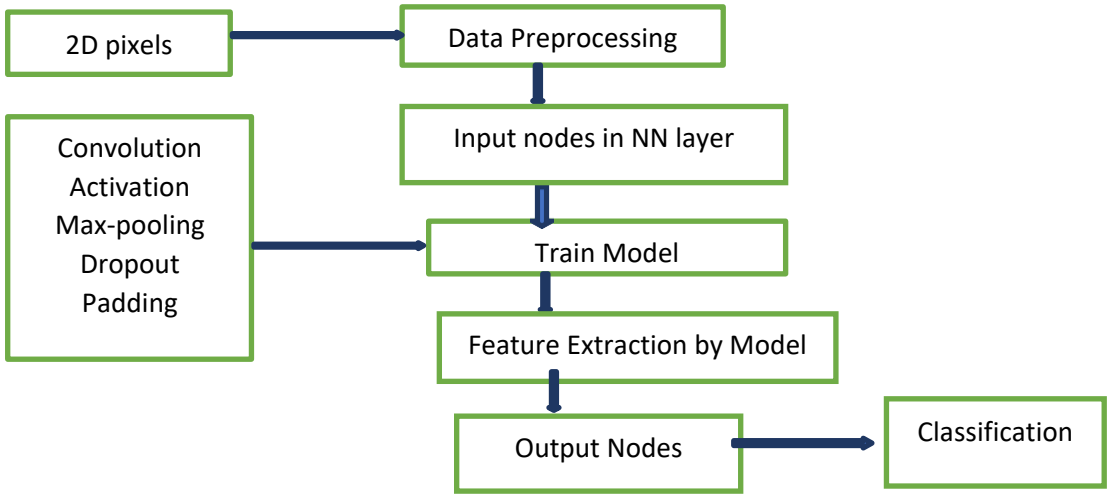

Figure1: Flowchart of face live-ness detection

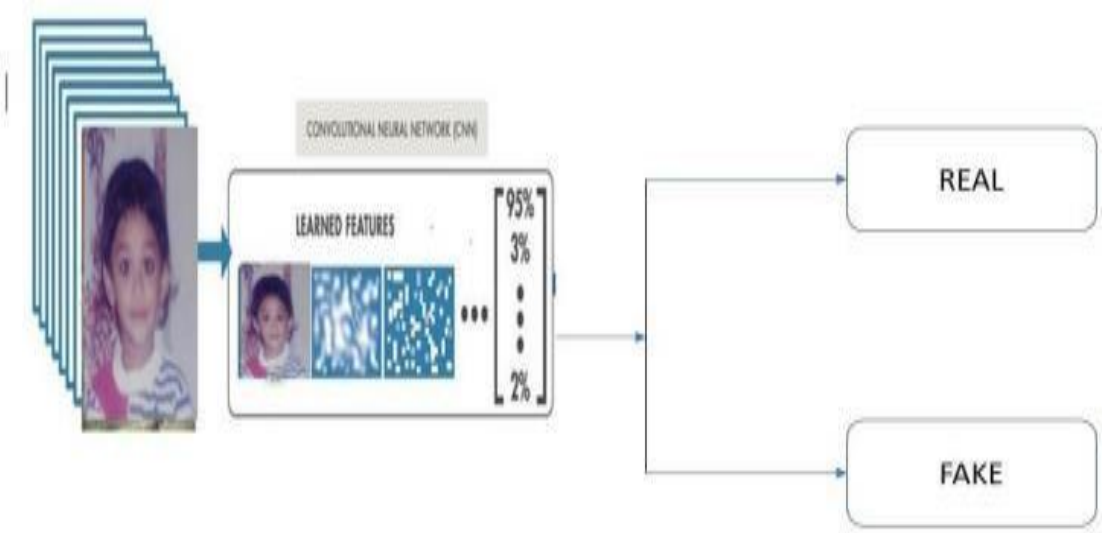

Figure 2: classification of face

Network Architecture: Feather Net B, all spatial convolutions utilize 3x3 portions. After each down sampling phase, SE-module is embedded with diminishing = 8 in both Feather Net A and Feather-Net B. When planning the model, a quick down-testing system is utilized toward the start of our architecture, making the component map size decline quickly and absent a lot of boundaries. Embracing this system can dodge feeble component inserting and high handling time brought about by delayed down-inspecting because of restricted registering financial plan. The essential Feather Net has 0.35M boundaries.

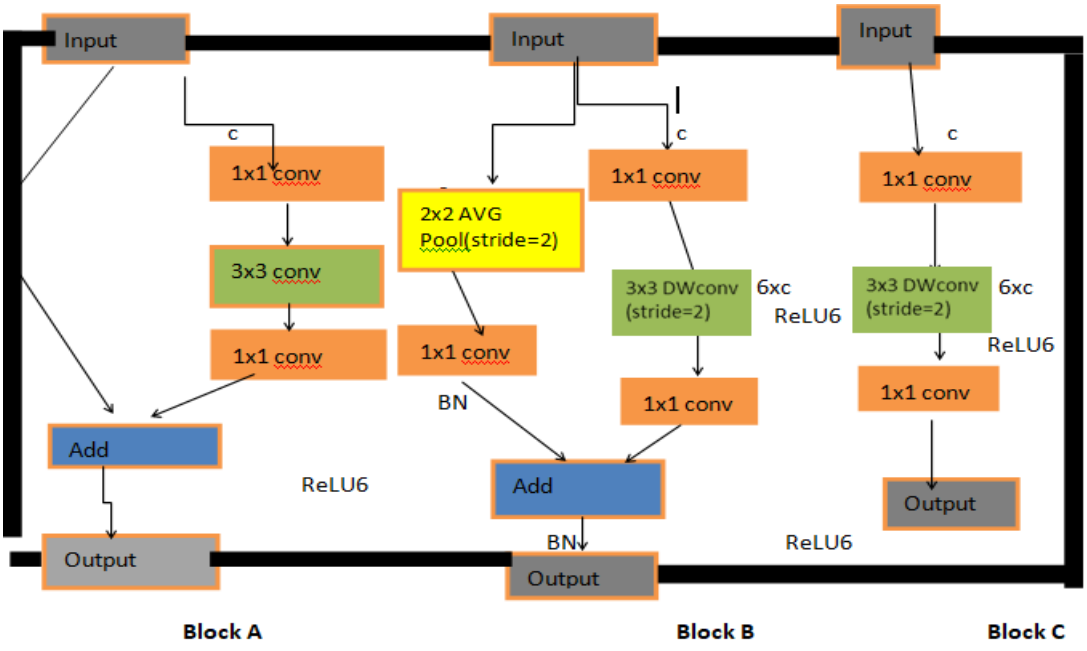

Figure 3: Feathernet architecture

The Feather Net's structure is based on Block A/B/C referenced above aside from the principal layer completely associated. As appeared in Table 1, the size of the information picture is 224x224. Rather than profundity convolutions, a layer with normal convolutions is utilized toward the starting to keep more highlights. Reuse channel pressure to decrease 16 while utilizing upset residuals and direct bottleneck with extension proportion = 6 to limit data misfortune due to down-examining. At last, the Streaming module is utilized without adding a
completely associated layer, straightforwardly straighten the 4x4x64 element map into a single dimensional vector, lessening danger of over-fitting brought about completely associated layer.

The primer work will be presented initially, for example, the assessment measurements, datasets utilized for preparing, the proposed information growth strategy, the preparation settings of the Feather Nets, and the pattern models.

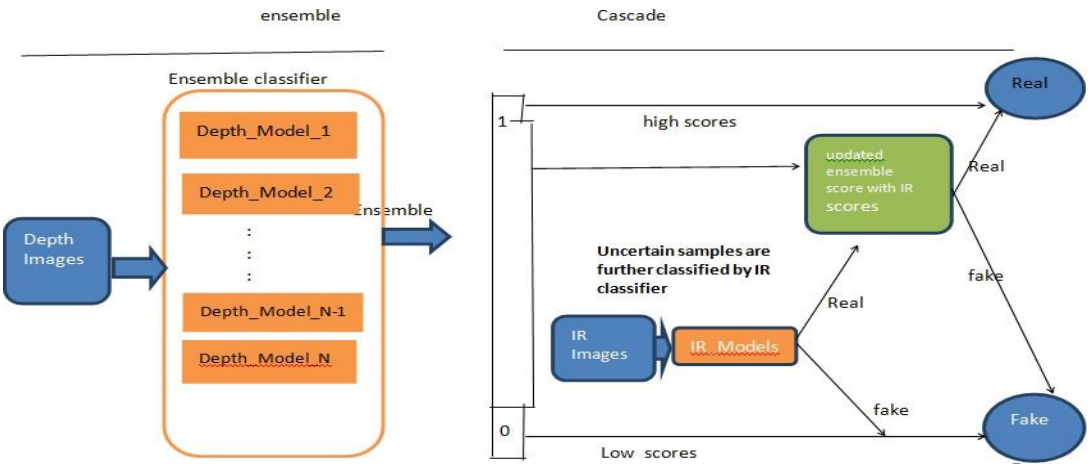

Figure 4: Multi-Modal Fusion Strategy

The principle thought for the combination strategy is to utilize course surmising on various models: profundity pictures and IR pictures. As indicated by our investigations, the IR information could give excellent Performance in phony judgment for those examples that the profundity modular isn't certain about. The course structure has two phases, as appeared in Figure4.

Phase 1: An ensemble classifier comprising various models is utilized to create the expectations. The models are prepared on profundity information and from a few registrations of various organizations, including Feather Nets. If the models' weighted normal of scores is almost 0 or 1, the info test will be delegated phony or genuine.

Stage 2: Feather Net B gained from IR information will be utilized to characterize the questionable samplesfromstage1.The counterfeit judgment of the IR model is spoken to as the end-product. For the genuine choice, the last scores are chosen by both phase 1 and IR models.

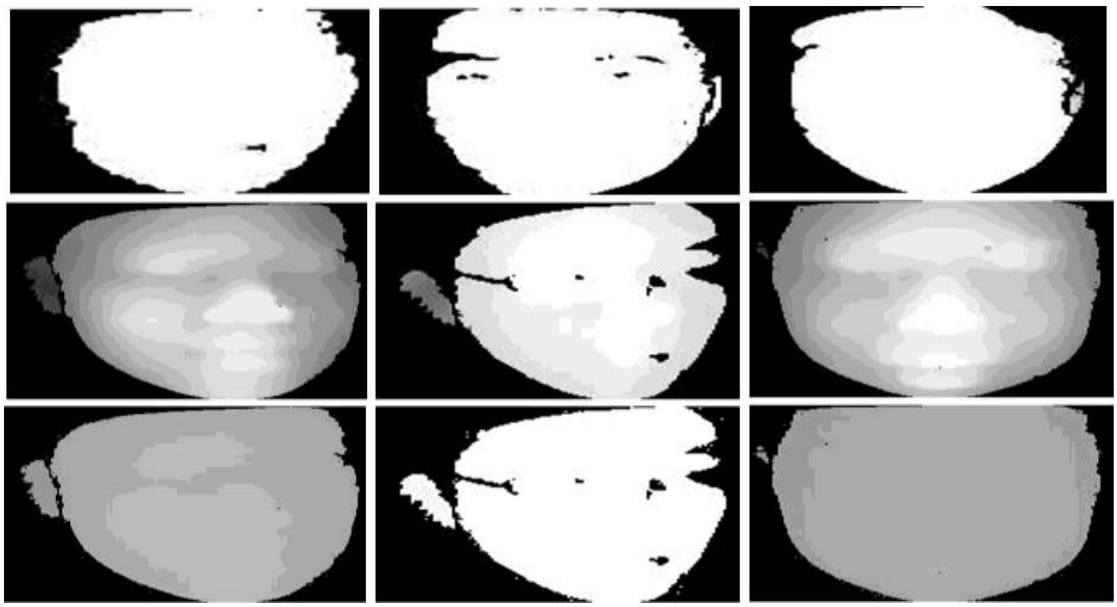

Figure 5: Image Augmentation

There are a few contrasts in the pictures obtained by various gadgets, regardless of whether a similar gadget model is utilized. As appeared in Figure 5. Human eyes can't recognize whether the face has a shape profundity. To diminish the gadget's information contrast, the focal point of genuine face pictures is scaled, as appeared in Figure 5. The method of information increase Algorithm is as follows: Data Augmentation Algorithm

```
1: scalar ← a random value in range [1/8, 1/5]
2: offset ← a random value in range [100, 200]
3: OutImg ← 0
4: for y = 0 → Height − 1 do
5: for x=0→Width−1 do
6: if InImg(y,x)>20 then
7: off←offset
8:    else
9:    off←0
10:   endif
11: OutImg(y,x)←InImg(y,x) * scalar + off
12:  end for
13:  end for
14:  return OutImg
```

Two random values for scalar and offset are selected in the specific range, height and width of the image are assigned to variables x and y; if the input image size more significant than the threshold value, then the output image size determined using the formula by multiplying a scalar value with the input image.

RESULTS AND DISCUSSION

Two datasets are used in the experiments: CASIA- SURF and the proposed Multimodal Face Dataset (MMFD). The training is performed on the GPU of high Performance and implemented in Tensor flow; it takes 105 iterations. Each iteration costs about 0.5seconds.

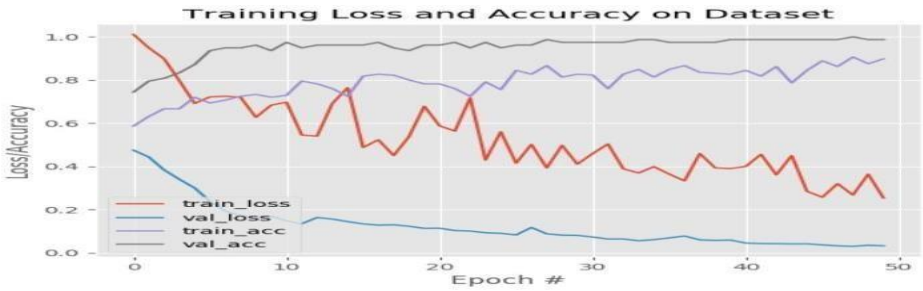

Figure 6: Training loss and accuracy of the dataset

The training loss and accuracy curves have appeared in figure 7. Training loss starts decreasing after 25 epochs, validation loss decreased after 10 epochs, training accuracy starts increasing after 25 epochs and validation accuracy increased after 30 epochs.

Figure 7: Input images

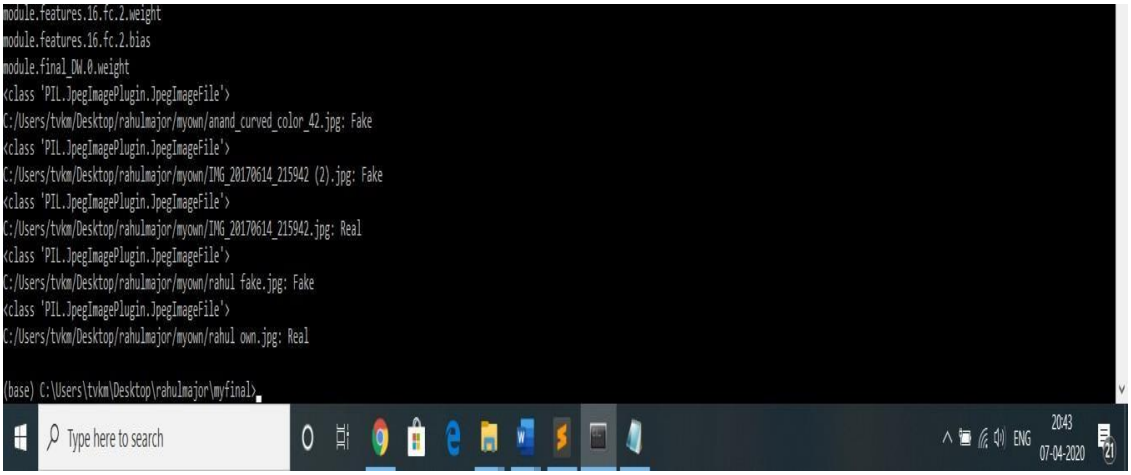

Figure 8: output for given input images

Figure 7 shows the input images, and the comparing yield appears in figure 8, where the outcome is appeared as genuine for live pictures and phony for the phony photographs. For the display evaluation, the going with usually used estimations will be introduced: Attack Presentation Classification Error Rate (APCER) and Average Classification Error Rate (ACER).

Table 1: Performance of Feather Net B

Model	ACER	TPR@FPR=10E-2	TPR@FPR=10E-3	Params	FLOPS
ResNet18[9]	0.05	0.883	0.272	11.18M	1800M
Baseline[9]	0.0213	0.9796	0.9469	–	–
FishNet150(our impl)	0.00144	0.9996	0.998330	24.96M	6452.72 M
MobilenetV2(1)(our impl)	0.00228	0.9996	0.9993	2.23M	306.17M
ShuffleNetV2(1)(our impl)	0.00451	1.0	0.98825	1.26M	148.05
FeatherNetA	0.00261	1.0	0.961590	0.35M	79.99M
FeatherNetB	**0.00168**	**1.0**	**0.997662**	**0.35M**	**83.05M**

Table 1 is the Performance in the endorsement dataset. Just significance data is used

for getting ready in various organizations. Feather Net A and B achieved better with less limit. It shows that the best decision is to set up the association with both data. The eventual outcomes of using our Feather Net B are far better than the baselines that usage multimodal data mix, demonstrating that our system has ideal adaptability over the third stream ResNet18 for standard.

Table 2: Performance of Feather Net B trained by different datasets

NETWORK	TRAINING DATASET	ACERIN VALIDATION
BASELINE	CASIO-SERF	0.02
FEATHERNET-B	CASIO-SERF DEPTH	0.09
FEATHERNET-B	MMFD DEPTH	0.06

Table 2 is the Performance of Feather Net B getting ready by different datasets. The presentation is better than the standard procedure using multimodal combination, as showed up in Table 2; tests are executed to differentiate and other association's Performance. It might be seen from the table1 that our limit size is significantly more unassuming, simply 0.35M, while the Performance on the affirmation set is the best in Block B, as showed up in Figure 3, which feasibly improves Performance with few limits.

CONCLUSION

The proposed unbelievable light network architecture (Feather Net A/B) with the Streaming module achieved a nice trade-off among execution and computational multifaceted nature for multimodal face anti-spoofing. Plus, a novel mix classifier with a "group + course" structure is proposed to introduce supported use cases. Execution of CNN with ethernet designingfollowedbymixanddataexpansionachievedTPR@FPR=10E-2=1.0 and TPR@FPR=10E-3=0.9976. Later on, the exactness can be extended by fusing more features close by these two features. Subsequently, the arranged system can give a higher movement of Performance concerning security.

REFERENCES.

Abdenour Hadid, and MattiPietika¨inen.Contextbasedfaceanti-spoofing. In2013IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pages 1–8.IEEE,2013.

Abdenour Hadid and MattiPietika¨inen. Face spoofing detection from single images using micro-texture analysis. In 2011 joint international conference on Biometrics (IJCB), pages 1–7.IEEE,2011.

Andre' Anjos, Jose' Mario De Martino, and Se'bastien Marcel. “Can face antispoofingcoun- termeasures work in a real-world scenario?” International conference on biometrics (ICB), pages 1–8.IEEE,2013.

AbdenourHadid. Face antispoofing using speeded-up robust features and fisher vector enAtoum, YaojieLiu, Amin Jourabloo, and Xiaoming Liu. Face antispoofing

using patch and depth-based cnns. In 2017 IEEE International Joint Conference on Biometrics (IJCB), pages 319–328.IEEE,2017.

LitongFeng, Lai-Man Po, YumingLi, XuyuanXu, Fang Yuan, Terence Chun-Ho Cheung, and Kwok-WaiCheung. Integration of image quality and motion cues for face antispoofing: A neural network approach. Journal of Visual Communication and Image Representation, 38:451–460,2016.

Lei Li, XiaoyiFeng, ZinelabidineBoulkenafet, Zhaoqiang Xia, Mingming Li, and AbdenourHadid. An original face antispoofing approach using partial convolutional neural network. In 2016 Sixth International Conference on Image ProcessingTheory, Tools and Applications (IPTA), pages 1– 6. IEEE, 2016.coding. IEEE Signal Processing Letters,24(2):141–145,2017.

KeyurkumarPatel,HuHan,andAnilKJain.Cross-database face antispoofing with robust feature representation. In Chi- nese Conference on Biometric Recognition pages 611– 619.Springer,2016.

ShifengZhang, XiaoboWang, AjianLiu, ChenxuZhao, JunWan, Sergio Escalera, Hailin Shi, ZezhengWang, and Stan Z Li. Casia-surf: A dataset and benchmark for large-scale multimodal face antispoofing. arXivpreprintarXiv:1812.00408,2018

Keyurkumar Patel, Hu Han, and Anil K Jain. Secure face unlocks Spoof detection on smartphones. IEEE Transactions on Information Forensics and Security, 11(10):2268– 2283,2016

SaptarshiChakraborty and Dhrubajyoti Das. An overview of face liveness detection. arXiv preprintarXiv:1405.2227,2014.

ZezhengWang, Chenxu Zhao, YunxiaoQin, QiushengZhou, and Zhen Lei. Exploiting temporal and depth information for multi-frame face antispoofing. arXivpreprint arXiv:1811.05118,2018.