

SCNN Based Classification Technique for the Face Spoof Detection Using Deep Learning Concept

Abhishek Dwivedi and Shekhar Verma

Department of Computer Applications, University Institute of Engineering and Technology, C.S.J.M University, Kanpur (Uttar Pradesh, India) Corresponding author: abhishekdwivedi@csjmu.ac.in, shekharverma@csjmu.ac.in

ABSTRACT:

Face spoofing refers to "tricking" a facial recognition system to gain unauthorized access to a particular system. It is mostly used to steal data and money or spread malware. The malicious impersonation of oneself is a critical component of face spoofing to gain access to a system. It is observed in many identity theft cases, particularly in the financial sector. In 2015, Wen et al. presented experimental results for cutting-edge commercial off-the-shelf face recognition systems. These demonstrated the probability of fake face images being accepted as genuine. The probability could be as high as 70%. Despite this, the vulnerabilities of face recognition systems to attacks were frequently overlooked. The Presentation Attack Detection (PAD) method that determines whether the source of a biometric sample is a live person or a fake representation is known as Liveness Detection. Algorithms are used to accomplish this by analyzing biometric sensor data for the determination of the authenticity of a source.

Keywords: Liveness Detection, Convolutional Neural Network, Face recognition.

INTRODUCTION

It has been shown that the great majority of current facial recognition systems are vulnerable to spoofing attacks. Spoofing occurs when someone attempts to trick a biometric face technology by posing in front of the lens with a false face. Face-spoofing location is typically used as a pre-processing step in face recognition frameworks to determine if the face image is taken from a genuine human or a print photograph (replay video). As a result, face spoofing identification is a two-pronged problem. It is also known as face-liveness discovery. The spoofing attack entails the use of fabricated biometric traits to gain unauthorized access to assets guarded by a biometric recognition framework.

It is a direct attack on the tangible contributions of a biometric framework, as well as the adversary does not require previous knowledge of the acknowledgment calculation. With the amazing inclusion of video and image resources, there is an incredible requirement for programmed understanding and analyzing of information from the savvy architecture as practically it is obtaining the chance to be far away. As a result, the programmable face discovery framework plays an important role in face recognition, outer appearance recognition, head-present evaluation, sense of community, and so on. Nowadays, enterprises have fully realized the value of data that they have about their customers in Customer Relationship Management (CRM) systems and transactional systems (Mondal et al.). Face anti-spoofing is gaining popularity in academia and industry as a security technique for face recognition systems. However, due to the variety of Face Spoofing kinds, such as print-attacks, replay-attacks, mask assaults, and so on, distinguishing diverse phony faces remains challenging. Face spoofing is frequently used as a pre-processing phase in face recognition frameworks to determine if the face image is received from a genuine human or a printing photograph. As a result, face spoofing

identification is a two-pronged problem. It is also known as face liveness discovery.

The spoofing attack utilizes fabricated biometric qualities to get unauthorized access to assets safeguarded by a biometric authentication approach. It is a direct attack on the actual commitment of a given frame, and the attacker does not require prior knowledge of the acknowledgment calculation. With the dazzling inclusion of video and image datasets, there is a tremendous need for programmed understanding and assessment of data from the savvy architecture as practically it is discovering the possibility to be unquestionably far. As a result, the programmable face discovery framework plays an important role in face recognition, outer appearance recognition, head-present evaluation, emotional intimacy, etc.

It is using an artificial neural network (ANN) to combat face spoofing in this research. When compared to other manually constructed features such as local binary pattern (LBP), histogram of oriented gradients (HOG), LBP-TOP, and difference of Gaussian (DoG), characteristics using Artificial Neural Network (ANN). Facial spoofing attacks have grown in popularity as face recognition systems have grown in use. Face spoofing identification is now required in all face recognition systems, as technology for cloning human faces has evolved significantly. However, location-based POI recommendation still faces three major challenges.

IMAGE QUALITY ANALYSIS BASED METHODS

Biometric liveness detection for iris, fingerprints, and face pictures was recently proposed utilizing 25 quality measures, 21 of which are comprehensive measures and four that are not. It is in these areas that our work differs from that of our competitors; Face-specific information has not been addressed while developing relevant features for face spoofing detection, even though 25 characteristics are necessary to produce decent results. This technique, on the other hand, includes four characteristics that are specially developed to represent facial traits, and we demonstrate their efficiency in detecting spoof faces. Idiap and CASIA are two prominent public-domain datasets that the authors assessed their approach on, whereas we utilized the Idiap-Replay database. When building a general liveness detection system, the training process of each biometric modality was still conducted in intra-database settings. By contrast, the proposed approach aims to improve the generalization ability under cross-database scenarios, which has seldom been explored in the biometrics community (Wen et al. 2015), the unique characteristics of VANETs such as high mobility and volatility make them vulnerable to various kinds of attacks. Security, privacy, and trust should be considered from the beginning stages of designing VANET (Lu et al., 2018).

Methods based on other Cues

The use of cues obtained instead from 2D intensity images, such as 3D perspective, IR images, spoofing context, and speech as face spoof defenses have also been suggested. Face recognition systems like these, on the other hand, place additional burdens on the user or system and so have a more limited scope of use, for instance, an IR sensor, a microphone, and a speech analyzer were all required, as were several photographs of the subject's face captured from various angles. Another way to get around the spoofing context approach described it is to disguise the media used to spoof.

ANN

Artificial neural networks are the inspiration for this highperformance computing gadget. It is common to refer to ANNs as massively parallel processing systems, recurrent neural systems, or artificial neural systems. A huge number of units are brought together in a variety of ways to facilitate communication among them. These modules, also known as neurons or nodes, are basic processors that run in parallel. Every neuron is connected to another neuron via a "connection relation." Each link in the chain of communication has a weight assigned to it, and this weight offers information about the signal it receives as it enters the system. An important piece of information for neurons is whether the signal is being conveyed because of the weight. An activation signal describes the internal status of every neuron. Input signals are combined with the activating rule to generate output signals, which may then be routed to other devices. ANN models are useful in assessing driven pile bearing capacity in several investigations. Many different issue areas, including finance and business, architecture, material science, and geography, can all benefit from this newfound interest in the past few years. Sites like Statsoft.com are all about data and statistics. It all began in 1943 after Pitts and McCullock demonstrated that a neuron may have two countries, each of which is relative to the value of a limit. Figure 1 shows the ANN architecture (Kartchner et al 2021).

Cunning devices were made possible by the discoveries of McCullock and Pitt. For example, if the human mind could be a CPU workstation with the use of the technique, which works automatically as the brain, it would be easy to use.



Figure 1. ANN Structure

Almost every human being will at some time in their lives have been like this. They may all have made the same decisions in these scenarios. Individual concerns, which might act identically in different settings, maybe the differentiating feature responsible for the wide range of people's viewpoints and behaviors. When the human intellect, in my opinion, separates itself from a machine.

Functioning of ANN

It is possible to visualize the path of information flow in the brain by using a topological system with arrows pointing right. Weights are integer numbers that represent the symbol variance between two neurons. The gadget changes the weights to enhance the impact of the system has a poor or unpleasant output if there is a failure. In the absence of any flaws, the number of weights associated via nodes is performed out, leading to the best possible interpretation of the data (Moayedi et al. 2018).

RELATED WORK

Ma et al. stated that Deep learning-based face presentation assault detection has already shown notable results. As a result, they perform poorly against classical attacks and leave the system exposed to adversarial example assaults. This research introduces a multi-regional convolutional neural network that incorporates the concept of local transmission losses into patches to maximize data input throughout the whole face region while avoiding overemphasizing local sections. The suggested technique outperforms previous methods in terms of robustness against adversary example assaults and classical attacks.

Hasan et al. depicted that today, precise biometric user authentication is required. When someone attempts to mimic another person by presenting a false face or video at the front of the facial recognition camera, this is referred to as a face presenting assault. Face recognition and antispoofing technologies are critical elements of effective privacy protection. This study provides a novel and attractive technique for detecting face spoofs based on an assessment of the contrasted and dynamic special ability of both genuine and manufactured pictures. This study used a modified DoG filtering technique and a variancebased strategy based on rotation-invariant binarization. To obtain vectors for further analysis, SVM is utilized. The system makes use of the publically available NUAA photoimposter dataset, which contains photographs of faces in various lighting and area conditions. The accuracy of the approach is quantified using either the flawed acceptance or even the false rejection ratio (FRR). Overall, this strategy outperforms other strategic options on key indices when evaluated against a similar dataset.

Marra et al. suggested that Fake photographs and videos are quickly spreading on social media. Using commercial media editing software, anybody may delete, add, or clone persons and things. Traditional fakes have been detected many times, but new assaults appear daily. Image-to-picture translation using generative adversarial network connections (GANs) looks to be the most harmful since it permits realistically changing image context and meaning. They monitor the efficiency of numerous photo forgery detection using image-to-image translations in ideal and constrained settings in this research. The study found that both standard and learning-based detectors can reach up to 95% detection accuracy on uncompressed data, while only deep learning detectors can achieve up to 89% accuracy on compressed data.

Ramprasath et al. stated that with the rapid expansion of digital content identification, automated picture categorization has become the hardest job in computer vision. Unlike human eyesight, machines struggle to grasp and analyze pictures. Existing categorization systems have been researched; however, the output has been limited to low-level picture primitives. But those methods lack reliable picture categorization. This approach leverages deep learning to obtain predicted results in computer visions. This method uses Deep Neural Network for picture categorization. The method uses the MNIST Digit data set to classify grayscale photos. That training dataset has grayscale pictures which demand greater processing capacity to classify. In the experimental section, their model achieves 98 percent accuracy by training photos with Deep CNN.

Li et al. introduced a unique framework for detecting face spoofing that makes use of deep learning's representational capabilities and domain generalization. Specifically, a 3D Fully Convolutional (3D CNN) architecture suited for spatial-temporal inputs is described. A specially developed adaptation loss, which serves as the regularisation term, is used to train the network using augmented facial examples based on cross-entropy loss. Using feature distribution distances, training samples from diverse domains may easily learn the generalized feature representation. Researchers test the suggested framework on numerous databases. This technique can learn additional discriminative and stereotyped information than other methods.

Liu et al. suggested that Face anti-spoofing is essential to protect face recognition systems. Anti-spoofing is a binary classification issue. Many of them have trouble with faking cues and generalization. They advocate for supplemental supervision to help learners learn discriminative and generalizable signals. A CNN-RNN classifier is constructed to estimate face depth pixel-bypixel and rPPG signals sequence-by-sequence. Faces are identified by their estimated depth and their rPPG. The new picture anti-spoofing database supports a wide variety of lighting, topic, and position changes. Our model outperforms the competition for both intraspecific & cross-database testing.

Alotaibi et al. stated that Facial spoofing happens when an impostor presents a 2D printed picture or video recording to a facial detection and authentication system to obtain access as a valid user. This project presents a fast and non-intrusive approach for detecting face-spoofing assaults using a single photograph. They use nonlinear diffusion with additive operator splitting. Additionally, they show a deep learning model capable of extracting discriminative and high-level features from the input diffused image to identify a false face from a real face. Compared to the previously mentioned procedures, their suggested method is both easy and effective. On the widely recognized NUAA dataset, they reached 99 percent accuracy. Their technique was also evaluated just on the Replay Attack dataset, which contains 1200 short films of actual and spoofing assaults. A detailed experimental examination revealed better outcomes than earlier static methods. Using a sparse auto-encoder learning technique produces a more distinct diluted picture.

Akbulut et al. suggested that for user authentication, the human face is a critical biometric quantity. Avoid obtaining human face photographs via smartphone camera devices or social media. That is, a reputable face-based control system can determine both identity and vitality. Numerous strategies for spoofing facial recognition based on features have been presented. These techniques determine the liveness of a face by performing numerous operations on the input photos. This study presents a method for detecting fake faces using deep learning. Locally receptive fields (LRF)-ELM with CNN are employed to achieve this. LRF-ELM is a new model with a fast convolutional and pooling layers surface before fully connected layers. But CNN has convolution operation layers. The CNN architecture may have more connected layers. They tested the two most popular spoof image recognition datasets, NUAA and CASIA. The LRF-ELM method outperformed both databases.

Farmanbar et al. depicted that Biometric systems are vulnerable to non-real image spoofing attacks. To discriminate between real and fake identities, this work combines texture-based algorithms with picture quality evaluation metrics. To extract texture features from apicture, researchers employed LBP or HOG texture descriptors. The peak signal-to-noise ratio, autocorrelation, meansquared error, standardized cross-correlation, maximal difference, normalized error percentage, and average difference are also investigated. By scanning the PolyU palmprint database, they constructed a palmprint spoofing database. The proposed technique is demonstrated to be effective on three public-domain face spoofing datasets (Idiap Print-Attack, Replay-Attack, and MSU MFSD).

Akhtar et al. suggested that face recognition technology is now routinely used at border crossings, in banking, and with mobile payments. The growing use of facial recognition systems has generated worries about spoofed attacks, in which a photograph, video, or 3D mask of a genuine user's face is exploited to gain unauthorized access to treatment or data. The topic remains unsolved due to the difficulty of discovering discriminative and computationally economical spoof attack features and tactics. Existing techniques also make use of full-face photos or videos to determine the presence of a person.

However, certain portions of the face (video frames) are frequently repeated or match the visual clutter, leading to suboptimal outcomes. So, they present seven new approaches for finding prominent, instrumental, and classspecific picture patches. Using a voting-based system, four well-known classifiers are utilized to discriminate between authentic and spoof faces: SVM, Naive-Bayes, QDA, and Ensemble. Comparing findings from two publicly available datasets (Idiap REPLAY-ATTACK & CASIA-FASD) seems encouraging. Table 1 shows the summarized table for the Literature review.

A (1		0.4
Author	Technique	Outcome
Ma et al.,2020	multi-regional convolutional neural networks	More resistant to adversarial example assaults, and improved performance versus classic attacks
Hasan et al.,2019	The DoG filtering approach and a strategy based on local binary pattern variation (LBPV)	Performed best on key indices than other approaches
Marra et al.,2018	Image-to-image translation using generative adversarial networks	Demonstrates that both conventional & deep learning detectors may reach detection accuracies of up to 95%.
Ramprasath et al.,2018	Convolutional Networks (CNN), a computational intelligence system used for picture categorization.	The grayscale photos in the given dataset used for training necessitate additional processing capacity for image categorization.
Li et al.,2018	a 3-dimensional fully convolutional architecture customized for spatial-temporal input	The generalized feature representation may be learned using training data from several domains.
Liu et al.,2018	A CNN-RNN technique is implemented.	Offer a new faced anti- spoofing database with a wide range of lighting, topic, and position variations
Alotaibi et al.,2017	An AOS-based model with a significant time step size was utilized.	Increasing the number of iterations leads to reduced accuracy
Akbulut et al.,2017	LRF-ELM, local receptive fields, were utilized.	For both datasets, the LRF-ELM approach was shown to be more accurate than the other methods.
Farmanbar et al.,2017	used LBP and HOG texture descriptors	The suggested approach should be demonstrated to be effective in the detection of the face and palmprint spoofing
Akhtar et al.,2016	Utilizing Multiresolution Local Binary Pattern in conjunction with SVM	The ultimate categorization of authentic and fake faces is based on a majority voting system.

Table 1. Summarize Table of Literature Review

BACKGROUND STUDY

Use the SCNN with Inception v4 to test the efficiency of their combined strategy on the Replay-Attack database

and the Replay-Mobile dataset. The entire architecture has been designed so that face liveness detection may be performed in real-time once trained. Using the SCNN and the Inception v4 on the Replay-Attack and Replay-Mobile datasets, they reach encouraging findings of 96.03 percent and 96.21% facial liveness detection performance, respectively. Using a Convolutional Neural Networks (CNN) or a Long Short-Term Memory (LSTM), they create a unique deep architecture for face real-time intrusion recognition on video frames that leverages the diffusion of pictures to determine if a video sequence is real or false. However, even if the usage of CNN accompanied by LSTM isn't new, the combination of diffusion (the best strategy for single picture liveness detection) with it is unique. Testing on the REPLAY-ATTACK and REPLAY-MOBILE datasets showed that our design achieved 98.71 percent test accuracy and 2.77 percent Halfway Total Error Rate (HTER) (Koshy et al., 2020).

PROBLEM FORMULATION

Facial spoofing is a form of face recognition attack. The entering picture is first subjected to non-linear anisotropic diffusion, and then a deep network is used to determine liveness. This method cannot recognize live faces in real-time. Researchers present two end-to-end realtime methods that use nonlinear anisotropic diffusion to improve edges and surface texture while preserving boundary positions in the real picture. local receptive fields, weight sharing, and temporal and spatial subsampling to assure shift, scale, and distortions invariance. To improve accuracy, they employ a learning algorithm by first training the SCNN network on dispersed colour texture analysis. The picture is transformed to L*a*b*. The image's texture and distortion are extracted. The method is improved by identifying the person's face if it is real. This suggested solution can protect accounts or devices from spoofing.

IMPORTANT TECHNIQUE USED IN RESEARCH METHODOLOGY

Viola-Jones technique with Haar-Cascade features

In 2001, Paul Viola and Michael Jones developed the Viola-Jones face detector, which is the first framework on object detection that achieves real-time detection rates. The Cascade Object Detector approach has been used to implement this process in a MATLAB-based program. There are three methods in the Viola-Jones for detecting face features (Rahmad et al 2020):

- 1. An integral picture is used to find the rectangular Haar-like features for feature extraction.
- 2. Face detection is aided with Ada Boost, a

machine-learning algorithm. Boosted classifiers are those that use one of four boosted strategies to construct more complicated classifiers at each level.

3. The cascade classifier was used to efficiently merge several characteristics. Cascade is a word used in a classifier to indicate the number of filters that can be applied to a final classifier.



Figure 2 shows the several stages that go into determining whether a face may be seen in the image. The supplied image is transformed into a single, unified image by the algorithm. The integral image makes it possible to determine a calculation's outcome in a fixed amount of time. An image's facial regions may be identified using a variety of Haar features. Accumulation of weak classifiers is used to build a stronger one, using the machine learning AdaBoost algorithm. An advanced classifier is used in the cascading classification process.

Specialized Convolutional Neural Network (SCNN)

To learn about the smoothness of the diffused parameter, also built a specific end-to-end diffusion-CNN network (with batch normalization). The architectural elements of the local visual field shared weights, and spatially or temporal subsampling is used in Convolutional (Convnets) to provide some element of shifting, scale, and distortions invariance in the design. First training a CNN network using diffuse pictures obtained with a fixed smoothing of diffusing parameter of 15, can attain greater accuracy. Using batch normalization in the integrated diffused architecture, they retrain the pre-trained algorithm to improve its accuracy (Ovtcharov et al. 2015).

To determine the smoothness of diffusion, the original picture is first input into an alpha network (alpha). This neural network has a hidden state of 15 neurons, followed by a deep network of one neuron, which outputs the alpha frequency. They are activated by applying a ReLU activation function to those neurons. There are three convolutional layers in the SCNN model, with kernel sizes of 15*15, 7*7, and 5*5 being employed in the convolutions.

These layers include 16, 32, & 64 feature maps, respectively. To reduce the resolution, the C1 & C2 layers are subjected to maximum pooling following batch normalization. Diffusion-enhanced features for liveness identification must be extracted using the C1 layer's larger filter sizes. Batch normalization is accompanied by another dense layer of 64 neurons, then dense hidden layers of just one neuron. In the convolution operation, the hidden units, and in the output layer, the sigmoid function is used. With a learning basics rate of 0.001, the SCNN is training to use the binary-cross-entropy gradient descent and Adam's optimizer. Figure 3 shows the end-to-end architecture using the Specialized Convolutional Neural Network (SCNN).



Figure 3. End-to-end architecture using the SCNN

Proposed Methodology

Step 1: Input Image

In the first step, an image is used as an input for preprocessing and Feature extraction.

Step 2: Image Pre-processing and Feature Extraction

In this step 2, image pre-processing and feature extraction is done for reducing a large amount of dataset and need to reduce the number of resources. This step also includes image diffusion, L*a*b* colour space, Geometric Features, and Independent Component Analysis.

Step 3 Face Alignment Detection

In this step, alignment of the face is detected.

Step 4: Face detection using improved viola- Jones Technique with Haar Cascade features and SCNN

For detecting the face using improved viola-Jones Techniques with Haar Cascade features and SCNN.

Step 5: Train & Test Model for VGNN 16 Model

In this step, Training and Testing are done for VGNN 16 model for displaying the output accurately.

Step 6: Display the Output

In this step, Finally, the required output is achieved. Figure 4 shows the proposed methodology.



Figure 4. Proposed Methodology

EXPECTED OUTCOME

- 1. Results will develop face liveness detection architectures for static as well as video frames.
- 2. Proposed Approach is an end-to-end real-time solution to the face liveness detection problem.

- 3. The proposed framework gives better results with lower values of the smoothness parameter.
- 4. will improve the accuracy by experimenting with various hyper-parameters as well as deeper architectures

CONCLUSION

This paper has achieved the highest accuracy, which is far improvement than older research and studies. In the future by using the proposed model we can achieve much better accuracy. We can also use the first proposed model structure to improve. The purpose of this paper is to improve the accuracy, introduce briefly about methods, implementation and application of face spoof detection using deep learning techniques.

ACKNOWLEDGEMENT

I am extremely grateful to Smt. Usha Dwivedi (Mother) and Smt. Shivangi Dwivedi (Wife) For Encouraging Me

Declaration: We also declare that all ethical guidelines have been followed during this work and there is no conflict of interest among authors.

REFERENCES

- Akbulut, Y., Şengür, A., Budak, Ü., & Ekici, S. (2017, September). Deep learning-based face liveness detection in videos. In 2017 international artificial intelligence and data processing symposium (IDAP) (pp. 1-4). IEEE.
- Akhtar, Z., & Foresti, G. L. (2016). Face spoof attack recognition using discriminative image patches. Journal of Electrical and Computer Engineering, 2016.
- Alotaibi, A., & Mahmood, A. (2017). Deep face liveness detection based on nonlinear diffusion using convolution neural network. Signal, Image and Video Processing, 11(4), 713-720.
- Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on the face and palmprint biometrics. Signal, Image and Video Processing, 11(7), 1253-1260.
- Hasan, M. R., Mahmud, S. H., & Li, X. Y. (2019, May). Face anti-spoofing using texture-based techniques and filtering methods. In Journal of Physics: Conference Series (Vol. 1229, No. 1, p. 012044). IOP Publishing.
- Kartchner, D. R., Palmer, R., & Jayaweera, S. K. (2021, June). Satellite Navigation Anti-Spoofing Using Deep Learning on a Receiver Network. In 2021 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW) (pp. 1-5). IEEE.
- Koshy, R., & Mahmood, A. (2020). Enhanced deep learning architectures for face liveness detection for static and video sequences. Entropy, 22(10), 1186.
- Li, H., He, P., Wang, S., Rocha, A., Jiang, X., & Kot, A.

C. (2018). Learning generalized deep feature representation for face anti-spoofing. IEEE Transactions on Information Forensics and Security, 13(10), 2639-2652.

- Liu, Y., Jourabloo, A., & Liu, X. (2018). Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 389-398).
- Lu, Z., Wang, Q., Qu, G., & Liu, Z. (2018, August). BARS: A blockchain-based anonymous reputation system for trust management in VANETs. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 98-103). IEEE.
- 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.
- Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. (2018, April). Detection of gan-generated fake images over social networks. In 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (pp. 384-389). IEEE.
- Moayedi, H., & Jahed Armaghani, D. (2018). Optimizing an

ANN model with ICA for estimating the bearing capacity of the driven pile in cohesionless soil. Engineering with Computers, 34(2), 347-356.

- Mondal, A., Kakkar, A., Padhariya, N., & Mohania, M. (2021). Efficient Indexing of Top-k Entities in Systems of Engagement with Extensions for Geotagged Entities. Data Science and Engineering, 6(4), 411-433.
- Ovtcharov, Kalin, et al. "Accelerating deep convolutional neural networks using specialized hardware." *Microsoft Research Whitepaper* 2.11 (2015): 1-4.
- Ramprasath, M., Anand, M. V., & Hariharan, S. (2018). Image classification using convolutional neural networks. International Journal of Pure and Applied Mathematics, 119(17), 1307-1319.
- Rahmad, C., Asmara, R. A., Putra, D. R. H., Dharma, I., Darmono, H., & Muhiqqin, I. (2020). Comparison of Viola-Jones Haar Cascade classifier and histogram of oriented gradients (HOG) for face detection. In *IOP conference series: materials science and engineering* (Vol. 732, No. 1, p. 012038). IOP Publishing.
- 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.