Grenze International Journal of Engineering and Technology, June Issue

Hybrid Face Anti-Spoofing Framework using Surface Texture Feature

Jeya R[1], Mehul Saini[2] and Shivank[3]
[1]Associate Professor, Dept. of Computing Technologies, SRMIST, Kattakullathur, Chennai
Email: jeyar@srmist.edu.in
[2-3]Dept. of Computing Technologies, SRM Institute of Science and Technology, KTR, Chennai
Email: ms0034@srmist.edu.in, sq2474@srmist.edu.in

***Abstract*— There are various techniques for extracting features from images, such as Grayscale Pixel Value Features, Mean Pixel Value of Channels, Extracting Edge Features, Image Surface Texture Features, LBP and GLCM Surface Texture Features. Respective approaches are critical for computer vision (CV2) and image processing and classification.**

Among these LBP-based algorithms and their variations, GLCM-based algorithms and there variations are widely accepted and used just because of their simplicity, understanding and high efficiency. GLCM is very powerful algorithm which can tell every aspects of any image because this algorithm studies the detailed features of an image. However, the native LBP based algorithm calculates the significant difference between local centre of the LBP kernel and its adjacent pixel which is deffiend as neghibours of the central pixel and the magnitude difference is what called the surface texture of an image. Furuthere more to obtain detailed surface texture featuresof image without augmenting the feature dimensions of LBP objects, this paper proposes a nobel surface texture extraction method where the features are extracted with different LBP objects having other parameters and concatenated along the x-axis, e.g., (LBP1+LBP2+...). Furthermore, they are combined with GLCM features.

I. Introduction

The LBPH and GLCM are the most commonly used frontal and side face recognition and liveness detection techniques. Several studies suggest that these systems are vulnerable to spoofing attacks, a flaw that may restrict their use in many circumstances. Many anti-spoofing strategies have been developed to defend recognition systems from spoof assaults. We have proposed a hybrid of LBP and GLSM to improve performance in this work. LBP histogram is concatenated with the feature from GLCM and experimented with the different joining ratios of LBP features and GLCM features. Hence, the hybrid model gives better accuracy, up to 98.7%. However, LBP alone provides 91%, and GLCM offers 80%. Experiments have been done on the celeb-A spoof dataset.

A. Problem Statement

There are various types of biometric assaults. Forced registration, enrolling on the system using a deceased person, utilising shortened bodily in which the data of registered users is faked, as well as genetic cloned components of attacks. Identical twins must have distinct biometric traits than other registered users. To overcome those discrepancies, using merely algorithms is insufficient. The spoofing assault is the subject of this study. Anyone who attempts to manipulate existing data, such as a registered user's face image, in order to fool the system is said to be "spoofing." The attacker enters the biometric security access using an imprinted face image of the registered

Grenze ID: 01.GIJET.10.2.256

user and subsequently gains access to the systemanti-spoofing component is essential to ensure that the recognition system is not subject to attack. Liveness detection can be used to create an anti-spoofing technique. If a liveness indication is used to discriminate between the original face and the imprinted image, spoof detection may be established. Human faces, on the other hand, are composed of a variety of intricate 3D features that aren't as hard as the imprinted facial image. Texture features may be used to identify these variances. As a result, we can detect spoofing attempts on human face photos using texture analysis.

B. Objective

Single face recognition has been one of the most challenging topics in computer vision in the last decade. Law enforcement agencies, on the other hand, are still unable to identify and recognise anybody utilising video surveillance cameras successfully; blur conditions, illumination, resolution, and lighting are all critical concerns in face recognition. Our objective is to build a face detection and recognition system that can perform in critical conditions with low specification requirements and any environment. The main focus is on face recognition and its antispoofing. We have to research the best feature extraction method to classify the real face and the spoofed face coming from the video source.
Objectives are listed below-

- Cost-efficient face recognition/antispoofing/detection model.
- Selection of the robust dataset for higher reliability and accuracy.
- Improving face detection models like harr-cascade and Mtcnn for face cropping,
- Built with less high-end specification requirements.
- Use of low wight models with high performance.
- Antispoofing detection of face data.

C) Research Methodology

The experiment's primary purpose is to discriminate between the various outputs generated. The framework utilised is a deep learning classifier.:
Stage 1: Examine the literature where this research will be conducted, namely, deep learning and Speech Emotion Recognition Systems.
Stage 2: Then, using the literature review, identify the problem.
Stage 3: Then, we will proclaim our work's goal.
Stage 4: Acquire the data from open source.
Stage 5: The system's design and evolution under it. The suggested approach will then be examined to see if it generates the desired results.
Stage 6: Calculate the accuracy and compare it to other systems to enhance or develop the plan in the future

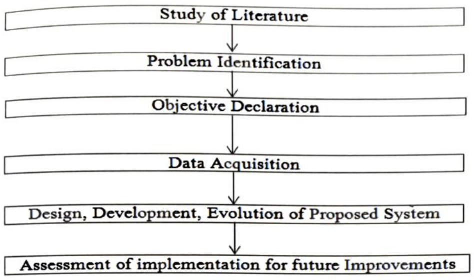


Figure 1:- Research Methodology

Above fig 2 depicts our system's research process and many stages of the study, for example, first studying the literature on the linked subject and identifying its problem. Following that, the research objective will be declared based on the problem identification, and the first step in work will be to collect data to design and develop the system. Then this study will evaluate the proposed method, and finally, this work will be assessed for future improvements.
1) There are two stages to this investigation. Modeling is the initial stage. The modeling step is performed to develop a model of the training data format feature (not spoof and cheat) and to enter the features into the database. The database of texture characteristics of training data is the result of this stage. Figure1 shows the modelling process's flowchart.

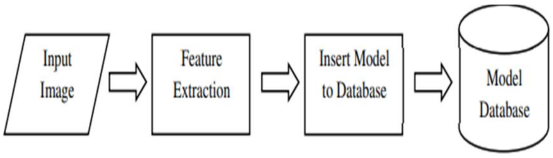


Figure 2:- Modelling Step

II. Domain

A. Computer Vision

The reliability and precision of computer vision and biometric identification systems have greatly increased during the last several decades. researcher all over the world is actively participating in this area of development to make it more accurate and efficient in every way possible. There are several real-world applications, including border control, money transfers, and cyber security, where this technology is now considered mature. Figure 3 is the general flow chart of computer vision.

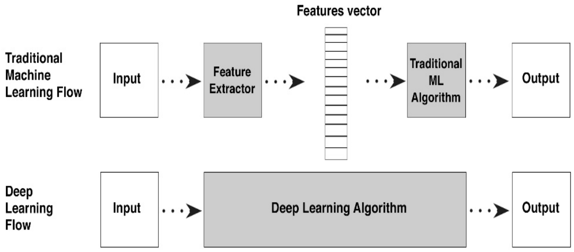


Figure 3. Computer vision flow charts

There have been several applications for computer vision in numerous fields.

- Identify objects and behavior.
- Self-driving cars.
- Analysis and diagnosis of medical images.
- Tagging photos.
- Facial recognition

Many vision applications begin with the acquisition of pictures and data, then processing that data, some analysis and recognition stages, and lastly, the execution of an action. figure 4 shows the flow chart of the computer vision process.

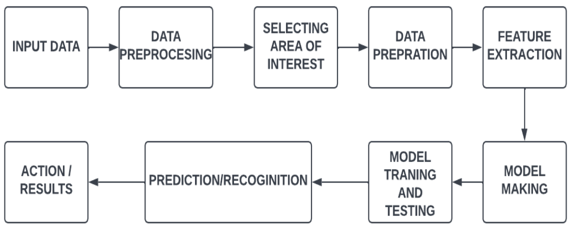


Figure 4. General Computer Vision flow chart.

As an illustration, consider the following instances of well-known computer vision tasks:-

1. Image classification

Image categorization can identify a dog, an apple, or even a person's face if it is spotted. An picture may be categorically assigned to one of many classes using this method. For example, a social media company may use it to automatically identify and sort out potentially harmful images submitted by users.

2. Object detection

Prior to identifying and tabulating an object's appearance in an image or video, image classification may be used to determine a certain picture class. A production line that has been damaged or a piece of equipment that has to be repaired are two examples.

3. Object tracking

Tracking an object once it has been discovered is known as object following. Photos and videos are often utilised in this kind of activity. So, in order to prevent crashes and follow traffic regulations, autonomous vehicles must be able to monitor moving things such as other vehicles and road infrastructure in addition to recognising them.

4. Content-based image retrieval

In content-based image retrieval, computer vision is used to search, explore, and retrieve photographs from large data repositories based on image content rather than metadata tags. This project might incorporate the use of automated image annotation, which would replace human image labelling. Improved search and retrieval accuracy may be achieved by incorporating these operations into digital asset management systems.

B. Sub-Domain

1. Local Binary Pattern (LBP)

The local Binary Pattern (LBP) A technique for describing the texture of a picture was presented. It was employed in a variety of computer vision research projects, including face identification, facial expression detection, movement and action modelling, and medical picture analysis. Pixels' neighbouring radiuses are taken into account while calculating LBPs. Calculation of the LBP value begins with an angle comparison and is then repeated for each subsequent neighbouring pixel until the desired LBP value has been obtained for the whole image.

1 or 0 is the outcome of a binary comparison. You get a value of 1 in this case, whereas you get zero in this case. If you're looking at two adjacent pixels that have different intensities, you'll get different values for each of these two pixels.

2. Gray Level Co-occurrence Matrix (GLCM)

The Gray-Level Co-Accuracy Matrix (GLCM) has proven to be one of the most effective methods for tissue analysis of various statistical methods. An image's grey value distribution and frequency of grey occurrences.

One of the most significant aspects of computer vision is face recognition. which the face of humans are identified and verified with their real ID proof.

there are lots of research and implementation of face recognition is going on but getting the accuracy and reliability of this model is still a great challenge to the researchers and scientists.

Face detection and recognition in real-life scenarios are very critical because spoofing this technology is sometimes easy and one can not rely completely on this new technology. Face authentication is one of the biometric authentications like fingerprints and retina prints. and in terms of complexity face authentication is much more convenient and contactless. in terms of fracture requirement and technical specification, the currently available systems are expensive. in this paper, we are trying to minimize the fracture cost as well as the specification requirement of the system with greater accuracy and reliability.

to achieve the above objective several experiments are done with the LBP feature histogram and GLCM features to obtain precision and minimum chance of error in model performance.

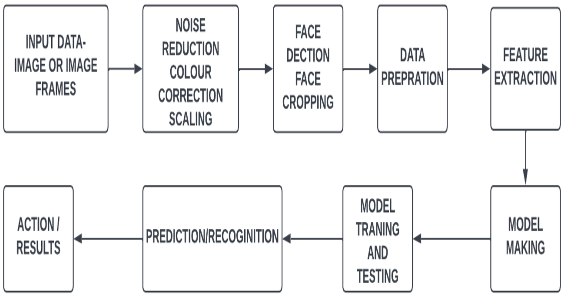


Figure 5. Facial Recognition flow chart.

The most difficult challenge in computer vision has been automated individual face detection during the last decade. On the other hand, law enforcement agencies are still unable to accurately recognise All people employing CCTV video surveillance; blurred conditions and lighting are all key considerations in face recognition.

To increase the effectiveness and precision of the face spoofing detector in the face recognition model, multiple approaches and algorithms are being tested and applied in various sectors such as public place surveillance, face authentication based bio-metric locks, and proctor verification in online examinations.

C. *Workflow Of The Face Recognition System*

The native face recognition system involves face detection, face alignment, face encoding, and face matching steps but in this paper, we are going to change this method from face detection to face liveness detection, so to obtain liveness detection the separate model is built using GLCM, LBP features and deep learning classification model and attached directly into face matching step to detect if the input face from the recognition model is real or fake face figure 6 below shows the flow chart of the native face detection model with an improved liveness detection model directly to the face matching stage.

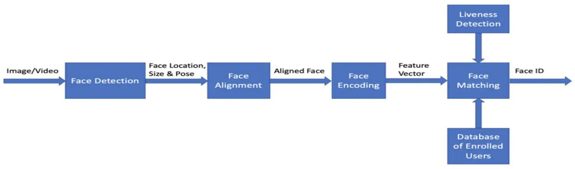


Figure 6. Facial recognition flow chart []

1. Face Recognition Applications

There are several uses for facial recognition technology, some of which have previously been mentioned. It isn't solely for security reasons, though it is one of them. The following are a few examples:

- Mobile device owner authentication
- School security
- Airline customs
- Entertaining apps
- Forensic science
- Recognizing shoplifters
- Face Anti Spoofing Detection

2. Face Recognition Algorithms

Any facial detection and recognition system or program relies on a face recognition algorithm as its foundation. In the eyes of the specialists, there are two basic types of algorithms. There are distinct differences between the geometric technique and other approaches. Photometric statistical methods are used to extract data from a photograph. These results are then contrasted against predefined templates in order to identify and eliminate any outliers. As well as feature-based and holistic models, the algorithms may be divided down into subsets. When it comes to facial landmarks and their connection to other facial features, the former is more concerned with its spatial qualities, whereas holistic approaches look at the face as a whole unit. here we have discussed some commonly used face detection and recognition algorithms:

- CONVOLUTIONAL NEURAL NETWORK(CNN)
- EIGENFACES
- FISHEFACES
- KERNEL METHODS: PCA(The Principal component analysis) AND SVM(Support Vector Machine)
- HARR CASCADES(for face crop, frontal face recognition)
- MTCNN(for face crop, frontal face, eye, lips, recognition)
- SKIN TEXTURE ANALYSIS
- THERMAL CAMERA(thermal image processing)
- ANFIS
- THREE DIMENSIONAL RECOGNITION
- FACENET
- LOCAL BINARY PATTERNS HISTOGRAM (LBP-H)
- GREY LEVEL CO-OCCURRENCE MATRIX(GLCM)

Lets see some breaf introduction to algorithms used in face recognition and detection:

a. Convolutional Neural Network(Cnn)

The convolutional neural network (CNN) is a major advancement in artificial neural networks (ANN) and artificial intelligence (AI) research (CNN). The most popular deep learning approach teaches a model to do classification tasks on images, videos, texts or sounds by observing how they change over time.

Model (ImageNet) supports a wide variety of applications, including computer vision, natural language processing (NLP) and the world's largest image classification data. There are two additional layers to the typical neural network: convolutional and pooling. Hundreds or thousands of these layers may be found in a CNN, and each one learns to recognise unique visual properties.

b. Kernel Methods: Pca(The Principal Component Analysis) And Svm(Support Vector Machine):

PCA(The Principal component analysis)

There are several uses for principal components (PCA) analysis, which is a commonly used statistical technique. To reduce the amount of source data while yet retaining the necessary information, PCA is used in face recognition. An vast library of various human face images is generated by combining weighted Eigenvectors with the resulting Eigenfaces. For each image in the training set, a linear set of eigenfaces is used to represent it. From the covariance matrix of training images, these eigenvectors are extracted using the PCA. The most important aspects of each photograph are calculated (from 5 to 200). The rest of the characteristics are used to encode tiny differences in the appearance of faces and noise. Recognition begins by comparing the unknown image's principal component to the characteristics of all other pictures.

c. SVM(Support Vector Machine)

SVM is a machine learning approach that uses a two-group classification notion to discriminate between faces and "not-faces." Training data sets for each category are provided to an SVM model so that it can categorise fresh test data. Researchers employ both linear and non-linear SVM training models while developing face recognition algorithms. Recent research shows that the nonlinear training machine has a larger margin and produces better results in terms of identification and classification than linear training.

d. Skin Texture Analysis

Face identification techniques, undesirable picture filtering, hand motion analysis, and more applications of skin recognition technologies exist. High-resolution photos are commonly used. The Different characteristics, such as moles, skin colour, skin tones, and others, are used in certain circumstances of skin texture analysis. A recent study based on textural characteristics and skin tone revealed some intriguing findings. A neural network was utilised to design and test the researchers' skin identification system. The feed-forward neural networks operated in the experiment performed admirably, classifying input texture pictures as "skin" or "non-skin."

e. Local Binary Patterns Histogram (Lbp-H):

A formatting factor in computer vision to label pixels in an image by adjusting the adjacent threshold of each pixel and treating the result as a binary integer, called local binary patterns (LBP). A histogram for each tagged and classified image is generated by the LBPH algorithm during learning. In the practise set, each picture is represented by a histogram.

f. Grey Level Co-Occurrence Matrix (Glcm)

GLM is a second-order statistical texture analysis method. To find out how often a certain set or combination of pixels occurs in an image, this algorithm examines the relationship between pixels in terms of their spatial location and distance.

g. Limitation Of Facial Recognition

The capability and accuracy of facial recognition systems have drastically improved in only a few years. However, there are still restrictions – particularly when the suggestions mentioned above are followed. Face-recognition software has the potential to attain 99.97% accuracy in the optimal conditions. On the other hand, excellent photographs are seldom obtained in the actual world. The subject's face characteristics must be clearly seen due to the lighting and setting of the photograph. Error rates might also rise with age. The technology will be less likely to match a subject's face with a photo from a database as their face ages.

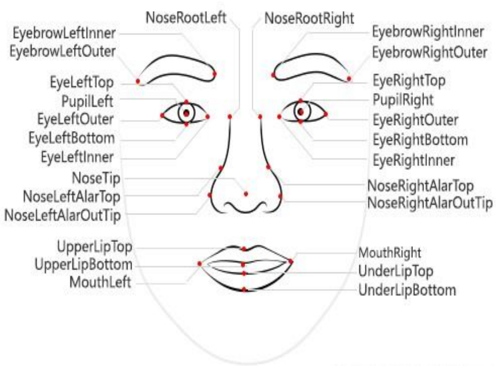
Another issue is the enormous disparity in vendor accuracy. Some companies have created algorithms that produce incredibly accurate outcomes.

On the other hand, the typical market supplier is not that precise. Many years remain before facial recognition software is generally accessible.

h. Drawback Of Facial Recognition:

Machine learning algorithms have shown impressive achievements in face identification and recognition. The machine learning architecture like harr cascade and MTCNN can detect the facial region in images, photographs

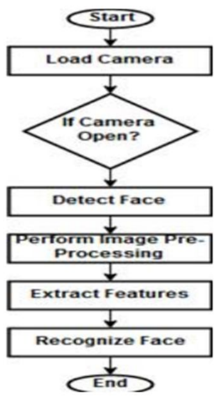
and videos coming from the source like cameras, mobile phones, and paper images. Harr cascade model in open computer vision has different pre-trained architecture like frontal face, frontal face eyes, frontal face nose and frontal face ears detectors.
Similarly, MTCNN is also a pre-trained architecture that coordinates the edges of eyes, nose, eyebrows, ears, and many more facial features described below.



But the accuracy of these machine learning models for face cropping is not up to the mark, so one can not rely on it on them entirely. And the classification models in machine learning need to be fed with the features of facial images, which again can be done with lots of machine learning architecture.
The machine learning architecture or algorithms can only perform best if the data fed into them have an excellent co-relation, features are extracted based on research over data, and good infrastructure to train machines.
As per the technical aspects, facial recognition systems have a few drawbacks.

- Infrastructure to set up a face recognition system can be expensive.
- The face recognition system can’t tell the difference between identical twins.
- The problem with false rejection is when people change their hairstyles and wear eyeshades and caps.
- Storage of data can be problematic.
- The recognition system can be affected by the environment.
- They can be easily spoofed by a photo attack, 3D mask attack, or video attack.
- The system can not detect the liveness of the source object to be identified.

3. Workflow



III. PROPOSED SYSTEM

Facial texture analysis is the study of surface textural features of the image. Image is converted to different colour spaces and the surface texture of the image is obtained by LBP and GLCM methods, Different combinations of LBP and GLCM along with specific colour spaces are tested and analyzed for better results and accuracy.
The proposed framework consists of these steps:
Face capture, Face region Cropping, feature extraction, feature vector concatenation, model training and validation, model testing, and Classification report. The proposed framework captures the face from the input

camera or from the data folder and identifies the facial region, then cropping the of the face area is done and cropped images are saved into a new dataset with different sizes and dimensions for data augmentation and producing a variation in the data, then model training is done with newly prepared data and validated with the part of the dataset to produce classification report. Classification report contains training loss, testing loss, validation loss, and accuracy, f1 score, precision. The trained model is saved and used for real-life testing with the different architecture of open cv.

A. Proposed Model Architecture

The proposed noble approach captures the face from the camera and then face detection and face cropping functions containing harr-cascade and MTCNN detects and crop the face and the new database is created then after extracting LBP features and GLCM features a deep neural network is trained and validated with the validation dataset. after that, it extracts the feature of the input image and establishes a histogram, and compares it with the predicted features to classify it as fake or real. figure. represents the flow chart of the proposed technique.

B. Real-Time Testing Model

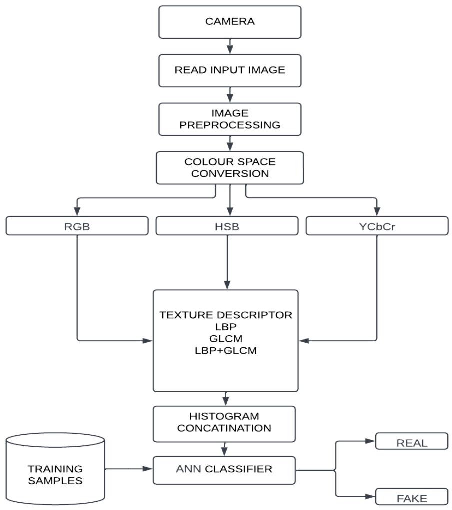


Figure 7: Training Model of proposed technique

1. Training And Validation Model

In the training and validation phase first the data is further split into a training set and a validation set. Both the data are split from Concatinated histogram data which is being extracted from the training and validation image samples. The major objective while preparing the data is to split it into a balanced set of training, testing, and validation. To obtain balance we have used the train_test_split function from sickit learn python machine learning library. Further after dividing the data now, the Model is trained and validated with training and validation data. Model is deep learning Sequential fully connected feed-forward artificial neural network which has five dense layers with RELU as an activation function which represents amended direct unit and one result layer with sigmoid actuation work which computes the probability of image classified in the scale of [0,1]. now the role of the threshold comes into play when the testing model has to decide a picture is either genuine or a computer-generated image, Threshold can be set after experimentation and analysing the results. The threshold for our model is 80% for real and if the probability is lower than the threshold the images are classified as fake figure. shows the proposed architecture of the artificial neural network classifier.

our method's outcomes are superior to those achieved by other methods, but they fall short of the standards required for real-world applications. Thus, to help develop full-face anti-spoofing methods, the data from different sources are used and a new database is created using cropped facial regions from the images. we have effectively increased the accuracy of the prediction model using fully connected deep neural network architecture and also improved the method of harr-cascade and MTCNN model to crop the face region.

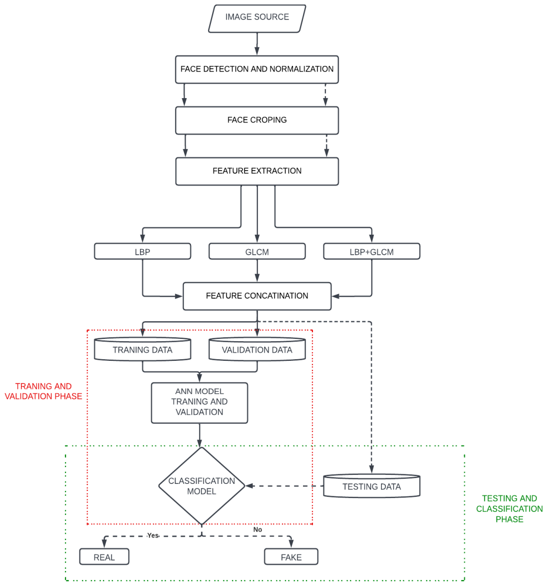


Figure 8. The framework of the proposed work

Our Proposed workflow of methodology

In this work, we have proposed a hybrid algorithm, which combines the GLCM and LBPH. For feature matching and prediction an ANN architecture is being introduced with a new combination of layers. The step by step procedure is given below:

Step 1: A query face image is inputted to the system via camera or database

Step 2: Then pre-processing techniques are applied for image normalization ie. (RGB-BGR) and colour space conversion (YCbCr)[], RGB[], HSB[] are used.

Step 3: Image face region cropping with pre-trained MTCNN, Harr-Cascade.

Step 4: Cropped Images are saved into a new database with their actual labels.

Step 5: Face image texture features are extracted using LBP and GLCM algorithms. And different sets of feature vectors are created combining LBP and GLCM features

Step 6: The dataset is obtained by concatenating the histogram. After that, separate into training, validation, and testing groups.

Step 7: The model is trained with a training set and validated with the validated set.

Step 8: Trained model is saved with epochs history and weights.

Step 9: Testing is done with the saved model and a classification report is obtained.

Step 10: Real-time architecture is built using Open-computer vision to test the model in a real-life scenario.

Dataset

1. CelebA-Spoof

There are 625,537 photos from 10,177 people in CelebA-Spoof, which is a large-scale face anti-spoofing dataset with 43 extensive characteristics on the face, lighting, surroundings, and spoof categories. The CelebA dataset was used to choose a live image. We gather and comment CelebA-Spoof spoof pictures. Live images include 40 of the 43 traits, including all face components and accessories such as skin, nose and eyes; eyebrows; lip; hair; hat; and glasses. There are three characteristics of spoof photographs, namely spoof kinds, environments, and lighting settings. Algorithms that are trained and evaluated using CelebA-Spoof may be used to prevent facial impersonation.

2. NUAA database

At a resolution of 640 x 480 pixels, a generic camera was used to capture 5,105 valid access photographs and 7,509 presentation assaults for the 15 individuals included in the NUAA Photo Imposter Dataset (Tan and colleagues, 2010). As a result, the subjects were photographed in three distinct locations and under varying lighting circumstances. The Canon digital camera was used to capture high-resolution images of attack models.

3. *Casia-Fasd*

In Zhang et al. (2012)'s CASIA-FASD dataset, there are a total of 600 movies from 50 distinct participants, each representing a different presentation attack type. One user may view the movies in twelve distinct ways, each of which includes three authentic and three fraudulent accesses. High, ordinary, and low-resolution cameras were employed to record the scene. Three different types of attacks were also used (normal, printed, printed and clumsy attacks, printed with cut-outs in the eye area, and video-based attacks).

4. *Oulu-NPU*

There are 4950 movies in the database of Oulu-NPU face presentation assault detection. These films were shot utilising the front-facing cameras of six mobile smartphones (Samsung Galaxy S6 edge, HTC Desire EYE, MEIZU X5, ASUS Zenfone Selfie, Sony XPERIA C5 Ultra Dual, and OPPO N3) in three distinct lighting and backdrop settings (Session 1, Session 2 and Session 3). There are just two presentation attack types that are included in the OULU-NPU database. To create attacks, two printers (Printer 1 and Printer 2) and two displays (Display 1 and Monitor 2) were used. Actual access and assault photographs recorded by the Samsung Galaxy S6 edge smartphone are shown in Figure 1.
The motion pictures of the 55 members were isolated into three separate sets for preparing, advancement, and testing. The following table provides a comprehensive breakdown of this database's partitioning.

Features extracted using GLCM are Formulated as below:

1. Converting a colour image to a grayscale image.
2. A 5 x 5 Gaussian filter is applied to the input picture.
3. The filtered image is separated into 4 x 4 square chunks.
4. It calculates the energy, standard deviation, mean value and homogeneity for each block. It is possible to calculate these qualities in four different directions: diagonally (45 and 135 degrees), vertically (0 degrees), or horizontally (90 degrees).
5. A database is used to keep track of the gleaned information.

we have considered Contract, correlation, energy and entropy.

Sl.No	**GLCM Feature**	**Formula**
1.	*Contrast*	$\sum_{i,j=0}^{N-1} P_{i,j}\,(i-j)^2$
2.	*Correlation*	$\sum_{i,j=0}^{N-1} P_{i,j}\left[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{(\sigma_i^2)(\sigma_j^2)}}\right]$
3.	*Dissimilarity*	$\sum_{i,j=0}^{N-1} P_{i,j}\,\lvert i-j\rvert$
4.	*Energy*	$\sum_{i,j=0}^{N-1} P_{i,j}^2$
5.	*Entropy*	$\sum_{i,j=0}^{N-1} P_{i,j}\,(-\ln P_{i,j})$
6.	*Homogeneity*	$\sum_{i,j=0}^{N-1} \frac{P_{i,j}}{1+(i-j)^2}$
7.	*Mean*	$\mu_i = \sum_{i,j=0}^{N-1} i\,(P_{i,j})\ ,\ \mu_j = \sum_{i,j=0}^{N-1} j\,(P_{i,j})$
8.	*Variance*	$\sigma_i^2 = \sum_{i,j=0}^{N-1} P_{i,j}\,(i-\mu_i)^2\ ,\ \sigma_j^2 = \sum_{i,j=0}^{N-1} P_{i,j}\,(j-\mu_j)^2$
9.	*Standard Deviation*	$\sigma_i = \sqrt{\sigma_i^2}\ ,\ \sigma_j = \sqrt{\sigma_j^2}$

IV. Conclusion And Future Scope

The model is not tested in various other environmental scenarios like movement, or weather conditions. We have only considered the luminous criteria to test the validation. We have considered approx 3L of validation data and the accuracy is almost 99% in static mode. In real-time the model is validated as shown in Figures 1 and 2, it clearly shows fake and real.

REFERENCES

[1] Boulkenafet, Zinelabidine, Jukka Komulainen, and Abdenour Hadid. "Face anti-spoofing based on color texture analysis." 2015 IEEE international conference on image processing (ICIP). IEEE, 2015.

[2] An introduction to computer vision. Available online: https://www.analyticsvidhya.com/blog/2021/07/an-introduction-to-computer-vision-with-opencv/(accesed on 27 May 2022).

[3] Localbinary pattern for texture classification. Available online:https://scikit-image.org/docs/stable/auto_examples/features_detection/plot_local_binary_pattern.html(accesed on 27 May 2022).

[4] GLCM texture features. Available online:https://scikit image.org/docs/dev/auto_examples/features_detection/plot_glcm.html(accesed on 27 May 2022).

[5] De Carrera, Proyecto Fin, and Ion Marques. "Face recognition algorithms." Master's thesis in Computer Science, Universidad Euskal Herriko 1 (2010).

[6] Park, Sung Won, and Marios Savvides. "Breaking the limitation of manifold analysis for super-resolution of facial images." 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. Vol. 1. IEEE, 2007.Park, Sung Won, and Marios Savvides. "Breaking the limitation of manifold analysis for super-resolution of facial images." 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. Vol. 1. IEEE, 2007.

[7] Woodward Jr, John D., et al. Biometrics: A look at facial recognition. RAND CORP SANTA MONICA CA, 2003.

[8] Chingovska, Ivana, André Anjos, and Sébastien Marcel. Anti-spoofing: Evaluation methodologies. No. BOOK_CHAP. Springer US, 2014.

[9] Wang, Xuerui, et al. "Attacks and defenses in user authentication systems: A survey." Journal of Network and Computer Applications 188 (2021): 103080.

[10] Pinto, Allan, et al. "Using visual rhythms for detecting video-based facial spoof attacks." IEEE Transactions on Information Forensics and Security 10.5 (2015): 1025-1038.

[11] EX, LP, and NOTIVA INNO. "IJRT_Volume-7_Issue-6_March_30_2019. pdf.".

[12] Shu, Xin, Hui Tang, and Shucheng Huang. "Face spoofing detection based on chromatic ED-LBP texture feature." Multimedia Systems 27.2 (2021): 161-176.

[13] Parmar, D.N., Mehta, B.B.: Face recognition methods & applications. Int. J. Comput. Appl. Technol. 4(1), 84–86 (2014).

[14] Li, L., Feng, X., Jiang, X., Xia, Z., Hadid, A.: Face anti-spoofing via deep local binary patterns. In IEEE International Conference on Image Processing (ICIP). pp. 101–105 (2017).

[15] Zhang, Yuanhan, et al. "Celeba-spoof: Large-scale face anti-spoofing dataset with rich annotations." European Conference on Computer Vision. Springer, Cham, 2020.

[16] Zhang, Zhiwei, et al. "A face antispoofing database with diverse attacks." 2012 5th IAPR international conference on Biometrics (ICB). IEEE, 2012.

[17] Damer, Naser, et al. "Practical View on Face Presentation Attack Detection." BMVC. 2016.

[18] Peng, Fei, Le Qin, and Min Long. "Face presentation attack detection using guided scale texture." Multimedia Tools and Applications 77.7 (2018): 8883-8909.

[19] Zhang, Bowen, Benedetta Tondi, and Mauro Barni. "Attacking CNN-based anti-spoofing face authentication in the physical domain." arXiv preprint arXiv:1910.00327 (2019).

[20] Boulkenafet, Zinelabidine, Jukka Komulainen, and Abdenour Hadid. "Face spoofing detection using colour texture analysis." IEEE Transactions on Information Forensics and Security 11.8 (2016): 1818-1830.