International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

Secure Face and Liveness Detection with Criminal Identification for Security Systems

Pratibha Shinde[1], Dr. Ajay Raundale[2]

[1]Research Scholar, Department of Computer Science & Engineering,
Dr. A. P. J. Abdul Kalam University, Indore, India
e-mail: ps21.shinde@gmail.com
[2]Associate Professor, Department of Computer Science & Engineering,
Dr. A. P. J. Abdul Kalam University, Indore, India
e-mail:arraundale@gmail.com

Abstract—The advancement of computer vision, machine learning, and image processing techniques has opened new avenues for enhancing security systems. In this research work focuses on developing a robust and secure framework for face and liveness detection with criminal identification, specifically designed for security systems. Machine learning algorithms and image processing techniques are employed for accurate face detection and liveness verification. Advanced facial recognition methods are utilized for criminal identification. The framework incorporates ML technology to ensure data integrity and identification techniques for security system. Experimental evaluations demonstrate the system's effectiveness in detecting faces, verifying liveness, and identifying potential criminals. The proposed framework has the potential to enhance security systems, providing reliable and secure face and liveness detection for improved safety and security.

The accuracy of the algorithm is 94.30 percent. The accuracy of the model is satisfactory even after the results are acquired by combining our rules inwritten by humans with conventional machine learning classification algorithms. Still, there is scope for improving and accurately classifying the attack precisely.

Keywords-Machine Learning Algorithms, Image Processing Techniques, Face and Liveness Detection, Criminal Identification, etc.

I. INTRODUCTION

The field of computer vision and security systems has witnessed significant advancements in recent years, driven by the rapid progress in machine learning and image processing techniques. Face and liveness detection, coupled with criminal identification, play a crucial role in enhancing the security and safety of individuals and organizations. This research work aims to develop a robust and secure framework for secure face and liveness detection with criminal identification specifically designed for security systems [1-2].

Face detection serves as the foundation for many computer vision applications, including security systems. Accurately locating and identifying faces in real-time is essential for effective surveillance, access control, and law enforcement. Various algorithms, such as Viola-Jones, Histogram of Oriented Gradients (HOG), and Convolutional Neural Networks (CNN), have been employed for face detection, each with its strengths and limitations. The proposed research work aims to evaluate and improve upon existing algorithms to achieve accurate and efficient face detection, even in challenging scenarios with varying lighting conditions and occlusions [4].

In addition to face detection, liveness detection is crucial to differentiate between live faces and fraudulent attempts, such as using photographs or masks. Advancements in image processing and machine learning techniques have enabled the development of sophisticated liveness detection methods. Motion analysis, texture analysis, and depth-based techniques have proven effective in verifying the authenticity of captured faces. This research work explores and develops novel liveness detection approaches to enhance the robustness and reliability of security systems [3].

Criminal identification is a vital aspect of security systems, allowing the identification of individuals with criminal records or flagged in databases. Facial recognition techniques, such as Eigen faces, Fisher faces, and deep learning-based methods like FaceNet or VGGFace, have shown promising results in matching captured faces against a database of known criminals. The research work focuses on enhancing the accuracy and efficiency of criminal identification, aiming to reduce false positives and false negatives and improve the overall performance of security systems [6].

The effectiveness and performance of the developed framework will be evaluated through extensive experiments using real-world datasets encompassing diverse scenarios. The research work aims to demonstrate the capability of the proposed system to accurately detect faces, verify liveness, and identify potential criminals with high precision and recall rates.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

The outcomes of this research work are expected to have significant implications for security systems, access control systems, surveillance applications, and law enforcement agencies. By providing a robust and secure framework for face and liveness detection with criminal identification, this research work contributes to improving safety and security, safeguarding individuals and organizations against potential threats and unauthorized access [5].

Humans' greatest precious resource has always been digital data. It has grown considerably in significance in recent years. The development of data-using technology has raised serious questions about security. Face recognition is a component of almost all biometric systems. Because there are no capabilities for detecting if a face is live, these systems are vulnerable to spoofing attacks. The following is an explanation of several spoofing techniques used to deceive the facial recognition system:

A. Photo Attack - In this attack, the attacker poses as a customer in front of the camera to trick the biometric system.

B. Cut Photo Attack - This attack focuses on erasing the client's eye area from the picture. The attacker then employs it as a mask to spoof.

C. Warped Attack - In this attack, the victim's facial picture is held in front of a camera by the attacker while being curled.

D. Video Replay Attack - To trick the system, the attacker plays a high definition video of the client's face.

A variety of anti-spoofing approaches are described in fig.1 to combat these assaults. Based on the kinds of picture attributes that are employed for face liveness detection, these techniques are divided into the following categories:

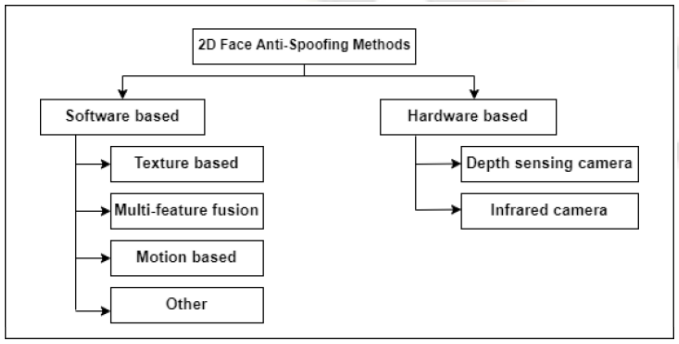

Fig.1: Classification of Face Anti-Spoofing Methods

Biometric systems are widely utilised in our daily life, with applications in phone unlock, access control, and security. One of the most commonly used biometric modalities is face. As facial recognition systems become more common, hackers attempt to pass as legitimate users by presenting the system with face spoofs (also known as presentation assaults, or PA). The face PA comprises donning a mask (mask attack), printing a face on paper (print attack), and repeating a face video on a digital device. Face anti-spoofing techniques [16, 22, 23, 24] are being developed to identify PA before a face picture is recognized in order to combat PA. Face anti-spoofing is therefore essential to ensuring that face recognition systems are reliable against PA and secure to use.

Similar to face recognition systems, face anti-spoofing systems use RGB picture and video as their standard input. By adding manually created features to binary classifiers, researchers begin the texture-based anti-spoofing techniques [13,18,19,22]. Many Convolutional Neural Networks (CNN) techniques later in the deep learning period use softmax loss as the supervision [21, 23]. When comparing a spoof face to a real one, there are many levels of picture degradation, including spoof patterns, which include skin detail loss, colour distortion, moir'e pattern, shape deformation, and spoof artefacts (such as reflection) [26, 28]. A CNN with softmax loss could find random signals, such the screen bezel, that can distinguish between the two classes, but not the faithful spoof patterns. These models wouldn't be able to discriminate between spoof and real faces when those signals vanish during testing, which would have a negative impact on generalization. Second, models trained with binary supervision will only provide a binary choice during testing, with no justification or justification for the decision. It is preferred for the learned model to produce the fake patterns that support the ultimate binary judgment in the aim of Explainable Artificial Intelligence [1].

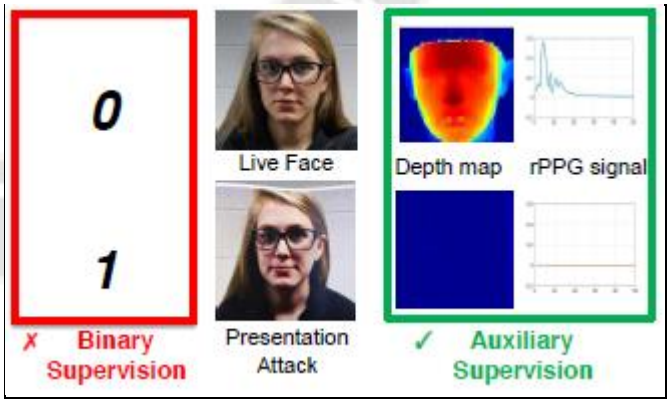

Fig.2: Given the vast solution space of CNN, most CNN-based face anti-spoof techniques use binary supervision, which may result in overfitting. The depth map and the Remote Photoplethysmography (rPPG) signal are used as supplementary information in this work's creation of unique network architecture, with the aim of enhancing generalization and producing judgments that can be explained.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

For the goal of reliably identifying face PA from a face video, as illustrated in Fig. 2, we present a deep model that employs the supervision from both the spatial and temporal auxiliary information rather than binary supervision. Therefore, depth may be used as supplementary data to monitor both real and fake faces. From a temporal viewpoint, it has been demonstrated that live, but not fake, facial videos may identify the typical rPPG signals (i.e., heart pulse signal). Therefore, we offer several rPPG signals as supplementary supervision that direct the network to learn from either real-world or fake face videos, as appropriate. We provide a network architecture with a short-cut link to capture various scales and a unique non-rigid registration layer to accommodate motion and posture change for rPPG estimation in order to support both supervisions.

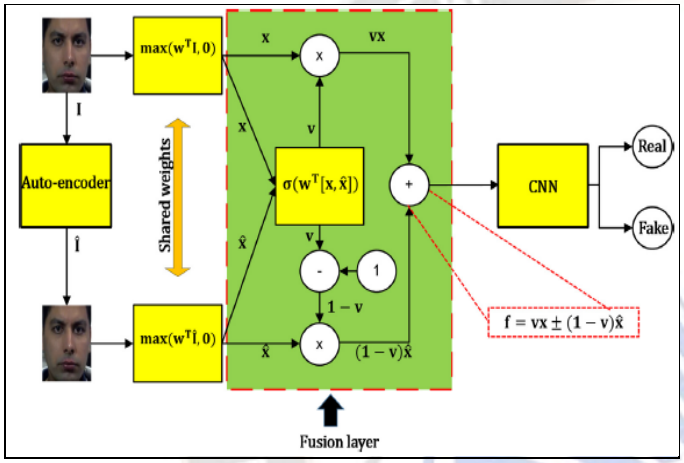

Fig.3: proposed method for detecting liveness in a face. The original face picture I and the matching DNG face image are fed via the convolution layers with common weights, then the adaptive convolutional-features fusion layer, which adjusts the weighting of the incoming convolutional-feature maps before feeding them to the further layers of CNN.

To achieve this, as shown in Fig. 3, we suggest using the adaptive fusion of convolutional features from real-world face pictures and deep CNN-based auto-encoder generated (DNG) face images. For the purpose of detecting the liveness of a face, we specifically use the adaptive disparity and blending between neural features of real-world face pictures and DNG face images learnt by convolutional layers with shared weights in CNN [7–10]. As shown in Fig. 3, we propose building a special layer in the CNN called the adaptive convolutional-features fusion layer instead of using conventional fusion. This layer will adaptively learn to weight the disparity and blending between the convolutional features of real-world face images and DNG face images. Following the suggested adaptive convolutional-features fusion layer in CNN, the convolutional features of real-world face pictures and DNG face images are fused adaptively for the purpose of detecting the liveness of a face. Our thorough experimental evaluations show that the proposed supervision enhances face liveness detection ability.

This paper's primary contribution may be summed up as follows:

- In order to execute the weighted fusion between convolutional features learnt by the convolutional layers using real-world face pictures and DNG face images, we use a deep CNN network with an adaptive convolutional feature fusion layer.
- We assess the appropriateness of the adaptive kernel window for combining the convolutional characteristics of real-world face pictures with those of DNG face images for the purpose of determining the liveness of a face. We also assess the impact on face liveness detection performance of weighted blending and disparity (with varied kernel window) of real-world face pictures and DNG face photos.

We offer thorough performance evaluations of the suggested system's ability to deal with the anti-spoofing issue in both intra-database and cross-database scenarios.

Furthermore, data is crucial for training the anti-spoofing models, much like it is for many vision-related issues. We all know that a good camera or screen is essential to the accuracy of mock faces. Existing face anti-spoofing databases were compiled three to five years ago and include NUAA [16], CASIA [17], Replay-Attack [18], and MSU-MFSD [19]. The sorts of equipment (such as cameras and spoofing media) utilised in such data collecting are outmoded in comparison to the ones nowadays, including the resolution and picture quality, given the rapid advancement of consumer gadgets. There are less changes in the postures, illuminations, and expressions (PIE) of the figures in the more current MSU-USSA [21] and OULU datasets [20]. It would be challenging to learn an efficient model if the required variations weren't there. We compile a face anti-spoofing database called Spoof in the Wild Database (SiW) in light of the obvious need for more sophisticated databases. 165 people, 6 spoofing media, and 4 sessions encompassing variants like PIE, distance-to-camera, etc. make up the SiW database. According to Tab. 1, SiW covers substantially more variety than earlier databases.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

Table 1: The Comparison of our Collected Dataset with Existing Datasets for Face Anti-Spoofing

Dataset	Years	# of Subjects	# of Sess	# of live/Attack vid(V) im (I)	Pose Range	Diff. Expres.	Extra Light	Spoof Attack
NUAA	2010	15	3	5105/7509 (I)	Frontal	No	Yes	Print
CASIA-MFSD	2012	50	3	150/450 (V)	Frontal	No	No	Print, Replay
Replay-Attack	2012	50	1	200/1000 (V)	Frontal	No	Yes	Print, 2Replay
MSU-MFSD	2015	35	1	110/330 (V)	Frontal	No	No	Print, 2Replay
MSU-USSA	2016	1140	1	1140/9120 (I)	[−45º, 45º]	Yes	Yes	2 print, 6 Replay
Oulu-NPU	*2017*	55	3	1980/3960 (V)	Frontal	No	Yes	2print, 2Replay
SiW	2018	165	4	1320/3300 (V)	[−90º, 90º]	Yes	Yes	2print, 4Replay

II. RELATED WORK

The research work aims to develop a comprehensive and secure system that combines face and liveness detection with criminal identification capabilities for enhanced security systems. Several related works have contributed to the advancements in this field [11, 13].

In the area of face recognition, researchers have explored deep learning algorithms such as Convolutional Neural Networks (CNNs) and Siamese networks. These algorithms extract discriminative features from facial images and match them against a database of known individuals, enabling accurate identification. Techniques like facial landmark detection, face alignment, and face normalization have also been investigated to improve the robustness and accuracy of face recognition systems [12].

To counter spoofing attacks, liveness detection methods have been extensively studied. Texture analysis, motion analysis, and physiological signals are some of the approaches used to distinguish real faces from fake ones. Deep learning models, including CNNs and Recurrent Neural Networks (RNNs), have been employed to learn distinguishing features that can differentiate between genuine facial data and spoofed images or videos. These methods help ensure the integrity of the face recognition system by preventing unauthorized access [14].

In addition to face and liveness detection, facial expression analysis has gained attention in the context of security systems. Recognizing facial expressions associated with suspicious or criminal behavior can aid in identifying potential threats. Researchers have explored deep learning models to analyze facial expressions and detect specific patterns indicative of suspicious activities. Emotion recognition techniques, such as CNNs and RNNs, have been used to capture facial dynamics and classify expressions accurately [15].

Criminal identification is a critical aspect of the proposed research work. Studies have focused on developing efficient and reliable algorithms to match detected faces against criminal databases. These databases may include mugshots, surveillance footage, or other sources of criminal records. Various matching techniques, such as feature-based matching and deep metric learning, have been investigated to identify potential criminals accurately. Integration of additional information, such as demographic data and behavioral patterns, has also been explored to enhance the identification process [16].

Overall, the related work in this research area demonstrates the advancements in secure face and liveness detection, as well as criminal identification for security systems. These studies have paved the way for developing a robust and comprehensive system that can prevent spoofing attacks, accurately recognize individuals, and identify potential threats, thereby enhancing the security measures implemented in various domains [17-20].

In this paper Sudeep D. Thepade et al, [2] Various current robust security systems use various biometric modalities, including voice, face, eyes, fingers, palms, etc. Face recognition is the only one of them that is contactless and doesn't require user involvement. Face biometric systems are being used more often, which has created a number of new issues for everyday applications like cellphones, computers, banking, airports, criminal identification, online tests or interviews, etc. Spoofing is the practise of gaining unauthorised access to circumvent biometric security measures. Many facial recognition algorithms lack the ability to discern whether a face is alive. As a result, these systems are susceptible to a variety of face spoofing techniques, including mask attacks, picture attacks, video replay attacks, cut photo attacks, etc. Photo assault is most frequently used because to its simplicity and inexpensive cost. The face presentation attacks (FPA) and faces anti-spoofing approaches are briefly described in this study.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

This study also describes the experimentation databases that are accessible for face spoofing detection and several face spoofing detection algorithms. It also seeks to offer new research directions in this area.

In this paper A. Nema, [3] suggests that this program detects liveness using both a facial recognition method and an eye-blink count. The application's two key steps are the identification of faces and the evaluation of a user's liveness state. It has been demonstrated that liveness detection can stop video playback assaults and the use of printed photos to breach security. Every brief moment, the user's image is captured by the webcam. The collected image is examined for liveness after completing the verification procedure. Countermeasures are put into practise in the event of a security breach. This involves taking pictures of enemies and shutting down or exiting the system. This study suggests an extra functionality that leverages the passcode and the HOG feature descriptor of the user picture. It employs an SVM classifier with a 100% accuracy rate as a performance indicator. The success of the suggested strategy is demonstrated by the experimental results of the improved functioning.

Sergey Maximenko, [4] The key to security is the current biometric facial recognition technology. It's simple to find someone's image or video on Facebook or YouTube. These pictures and videos might be abused. Face-based biometric systems are susceptible to assaults using 3D face reconstruction, screen replay, or paper-based pictures. It's crucial to have a security system that can guard against face spoofing.

In this paper Yaojie Liu, et al, [5] Proposed face anti-spoofing is essential to guard against security flaws in face recognition systems. Face anti-spoofing is conceptualized by earlier deep learning methods as a binary classification issue. Many of them generalize poorly and have trouble understanding appropriate spoofing cues. The authors of this work make the case that learning should be directed towards discriminative and generalizable cues through supplementary supervision. To discriminate between real and fake faces, the estimated depth and rPPG are combined. The authors also present a accommodates a wide variety of lighting, topic, &position changes. The model produces cutting-edge outcomes in both intra- and cross-database testing, according to experiments.

Yasar Abbas Ur Rehman, et al, [6] In the past, face liveness detection classifiers have been trained using real-world photos, where real-facial images and related face presentation attacks (PA) had a large amount of overlap. However, very little research has been done on using a mix of real-world face photos and deep convolutional neural network (CNN)-generated face images to assess the liveness of a face. In addition, the authors suggest an adaptive convolutional-features fusion layer that balances the convolutional features of synthetic and real-world face pictures during training. These extensive tests using the most recent face anti-spoofing databases, including CASIA, OULU, and Replay-Attack, in both intra- and cross-database scenarios show that the proposed method performs admirably when compared to other methods currently available.

In this paper, Avinash Kumar Singh, et al, [9] On the basis of the challenge and response approach, suggest an effective liveness detection methodology. Before the facial recognition module, the liveness module is introduced as an extra degree of protection. The liveness module makes advantage of face macro traits, particularly eye and mouth movements, to create arbitrary challenges and track the user's reaction to them. The liveness module's dependability is checked by deploying various spoofing attacks utilising a variety of techniques, such as using images, videos, etc. Overall, the system has handled and avoided five different sorts of assaults. The system can identify liveness when subjected to all of these attacks, with the exception of the eye mouth imposter attack, according to experimental data. Although this attack is able to go by the liveness test, it significantly alters the anatomy of the face. The facial recognition module fails to recognize or incorrectly classifies the outcome as a consequence. According to an experimental study done on 65 people in the University of Essex face database, removing the eye and nose components leads to a 75% misclassification of the face..

In this work, M. Killioglu, et al, [10] focuses on liveness detection for fake face movement spoofing of facial recognition systems. Using very simple hardware, authors have created a pupil direction observation system for anti-spoofing in face recognition systems. The first step is to use a custom trained classifier with a Haar-Cascade Classifier to extract the ocular region from a real-time camera. The Kanade-Lucas-Tomasi (KLT) method has been used to extract and trace feature points in order to reduce head movements and provide stable eye areas. To create a steady eye region, the eye area is rotated and cropped from a real-time camera frame. Then, using a new, enhanced algorithm, the pupils are removed from the ocular region. The suggested spoofing technique picks a random direction and sends a signal to Arduino to turn on that selected direction's LED on a square frame with a total of eight LEDs for each direction after a few steady numbers of frames with pupils.

Hsueh-Yi Sean Lin et al, [11] Due to its efficiency and simplicity, face recognition algorithms have been frequently used for user identification in security systems. However, spoofing attacks, such as those involving printed pictures, projected images, and replayed videos, pose serious problems

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

for authentication and provide hostile intruders access to the system. In order to defend against attacks on biometric authentication systems using printed photos and replayed attacks, this study suggests two unique characteristics for face liveness detection systems. The first feature, motivated by the finding that epidermal blood flow in the face possesses characteristics that permit separation between live and faking face photographs, derives the textural difference between red and green channels of face images. Because picture quality may be more discriminative in smaller sections of face photos, the second feature evaluates the colour distribution in limited portions of face images as opposed to full images. Together with a multi-scale local binary pattern feature and these two characteristics, a support vector machine classifier is trained to distinguish between real and fake face photos.

Shun-Yi Wang, et al, [12] Face recognition technology's security is becoming more and more important as artificial intelligence advances and expands the applications of face recognition. The present study is focused on how to create a face anti-spoofing approach that has high accuracy, great generalisation ability, and meets practical objectives. This study discusses the face anti-spoofing algorithm's development trajectory and categorises the currently used face anti-spoofing techniques into two groups: those based on manual feature expression and those based on deep learning. Then, the usual algorithms that are present in them are divided into two categories, and their fundamental concepts, benefits, and drawbacks are examined. The techniques of face anti-spoofing are then briefly discussed, along with any current issues and potential solutions.

DasariSwethaManjari [14] The face is an important component of the human body that helps us identify persons in large crowds. As a result, due to its comprehensiveness and distinctiveness, it has emerged as the most widely used and recognised biometric technique. The area of face recognition has drawn the attention of many researchers, and as a result, it has emerged as a common standard in the field of human recognition. It has been the area in computer vision that has been most intensely targeted in the last forty years. It has a diverse range of applications, including security monitoring, automated observation systems, casualty and missing person identification proof, etc. This audit outlines the wide range of facial recognition methods in use and looks at both their advantages and disadvantages. The authors begin by outlining the foundational elements of face-acknowledgment innovation, its typical work method, challenges, and potential applications. Then, face-acknowledgment approaches are discussed, along with their advantages and disadvantages. The wrapping-up section outlines the potential consequences and long-term implications for further advancing the discipline.

CAI Pei, et al [15] The facial recognition system, which is crucial for access control and financial payment systems, has a significant component called face anti-spoofing. A unique approach employing a convolutional neural network and brightness equalization is provided in order to address the issues of unstable face alignment, complicated lighting, and the complex structure of the face anti-spoofing detection network.

Detailed analysis and comparison of image processing applications their merits and demerits have not been presented in literature. This study attempts to analyze and compare various image processing and face recognition techniques so as to provide clear understanding of the face and liveness detection methods and their applications.

III. PROPOSED SYSTEM DESIGN

The proposed system design for consists of several interconnected modules to achieve robust and accurate performance. The system begins by acquiring facial data through cameras or surveillance systems, followed by preprocessing steps such as face detection, alignment, and normalization to enhance the quality of the data.

The system incorporates a face detection module that accurately identifies and localizes faces within the acquired images or videos using algorithms like Viola-Jones or deep learning-based approaches. This module outputs the coordinates or bounding boxes of the detected faces [21].

To ensure the system can distinguish between real faces and spoofing attempts, a liveness detection module is employed. It analyzes the facial data for signs of liveness, such as motion, texture consistency, or physiological signals. Deep learning models, such as CNNs or RNNs, are utilized to learn discriminative features and classify the input as real or fake, employing techniques like texture analysis, motion analysis, or multi-modal approaches.

The core of the system lies in the face recognition module, which compares the detected faces with a database of known individuals, including potential criminals. Deep learning techniques such as CNNs or Siamese networks extract features from the facial data and generate face embedding's or descriptors. These embedding are then compared against the database using matching algorithms like Euclidean distance or cosine similarity to identify potential matches. Advanced techniques like deep metric learning or attention mechanisms can further enhance the accuracy and robustness of the face recognition module.

Additionally, the system integrates a criminal identification module that matches the detected faces against a database of criminal records, which can include mug shots or surveillance footage. Matching algorithms and techniques, such as feature-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

based matching or deep metric learning, are employed to identify potential matches between the detected faces and the criminal database. Supplementary information such as demographic data or behavioral patterns may also be considered to improve the identification process [21].

Based on the outputs of the various modules, a security decision module determines whether an individual should be granted access or flagged as a potential threat. In cases where a potential criminal is identified or a spoofing attempt is detected, the system generates alerts to notify security personnel or trigger appropriate actions, employing visual or audio alarms, notifications, or integration with existing security systems.

The proposed system design ensures the integration of various modules, including data acquisition, preprocessing, face detection, liveness detection, face recognition, criminal identification, security decision-making, and alert generation. It can be deployed as part of existing security systems or as a standalone solution, with a user-friendly interface to facilitate system configuration, monitoring, and management. The system is scalable to accommodate different security requirements and capable of real-time processing for prompt decision-making in security scenarios [24].

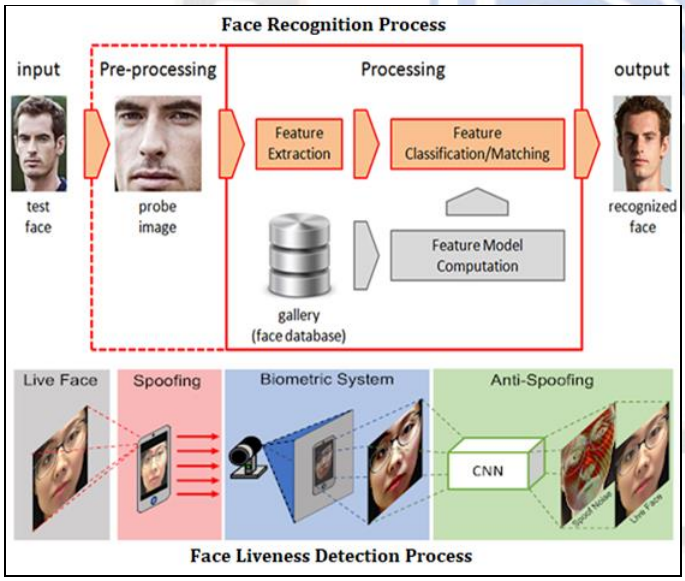

Fig.4: Proposed System Architecture

The proposed system design for incorporates multiple components and modules to ensure robust and accurate performance. The system design can be outlined as follows:

A. Data Acquisition: The system requires a reliable data acquisition module to capture facial images or videos for analysis. This can be achieved using cameras or surveillance systems installed in the target environment.The data acquisition module should provide clear and high-resolution images or videos for subsequent processing.

B. Preprocessing: The acquired facial data undergoes preprocessing to enhance its quality and improve the performance of subsequent modules. Preprocessing techniques may include face detection, alignment, normalization, and noise reduction. These steps ensure that the facial data is in a suitable format and standardized for further analysis.

C. Face Detection and Localization: A face detection module is employed to identify and locate faces within the acquired images or videos. This module uses algorithms such as Viola-Jones or deep learning-based approaches like Single Shot MultiBox Detector (SSD) or You Only Look Once (YOLO) to detect faces accurately. The module outputs the coordinates or bounding boxes of the detected faces.

D. Liveness Detection: The system incorporates a liveness detection module to differentiate between real faces and spoofing attempts. This module analyzes the facial data to identify signs of liveness, such as motion, texture consistency, or physiological signals. Deep learning models, such as CNNs or RNNs, can be employed to learn discriminative features and classify the input as real or fake. Various liveness detection techniques, including texture analysis, motion analysis, or multi-modal approaches, can be utilized to enhance the reliability of the module.

E. Face Recognition: The face recognition module is responsible for comparing the detected faces with a database of known individuals, including potential criminal Deep learning-based approaches, such as CNNs or Siamese networks, can be employed to extract features from the facial data and generate face embedding's or descriptors. These embedding are compared against the database using techniques like Euclidean distance or cosine similarity to identify potential matches. Advanced techniques like deep metric learning or attention mechanisms can be employed to improve the accuracy and robustness of the face recognition module.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

F. Criminal Identification: The system integrates a criminal identification module to match the detected faces against a database of criminal records. This database can include mugshots, surveillance footage, or other sources of criminal information. The module utilizes matching algorithms and techniques, such as feature-based matching or deep metric learning, to identify potential matches between the detected faces and the criminal database. Additional information, such as demographic data or behavioral patterns, may also be considered to enhance the identification process.

G. Security Decision and Alert Generation: Based on the outputs of the various modules, a security decision module determines whether an individual should be granted access or flagged as a potential threat. If the individual is identified as a potential criminal or if liveness detection indicates a spoofing attempt, an alert is generated to notify the security personnel or trigger appropriate actions.The system may employ visual or audio alarms, notifications, or integration with existing security systems to ensure prompt response.

H. System Integration and Deployment: The proposed system can be integrated into existing security systems or deployed as a standalone solution. It should have a user-friendly interface that allows easy configuration, monitoring, and management of the system. The system should be scalable to accommodate varying levels of security requirements and capable of handling real-time processing for timely decision-making.

By incorporating these components and modules, the proposed system design ensures secure face and liveness detection while enabling criminal identification for enhanced security systems. The integration of advanced deep learning techniques, robust preprocessing, and decision-making modules enhances the accuracy and reliability of the system in real-world security scenarios [27-30].

IV. RESULTS AND DISCUSSION

The experiment is about proposed research face images work. With the proposed techniques the experimental result of the different image processing applications are achieved. The performance measures used are MSE and PSNR.

a) The average squared variation between the values that are estimated and the values that are really present is known as the "mean square error" (MSE). MSE may be calculated using the following formula:

$$MSE=\frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where, n is the number of columns and m is the total number of rows.I2 is the grey value of the current pixel in the face photos, and I1 is the grey value of the corresponding pixel in the original photograph.

b) The peak signal-to-noise ratio (PSNR), which reduces the signal representation's accuracy, is the ratio of the highest possible signal power to the highest possible noise power. The following equation may be used to calculate PSNR:

$$PSNR = 10\log_{10}\frac{R2}{MSE} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

The degree of variation that could be present in the provided image data type is represented by the letter R. Performance may be calculated using these formulas; if the PSNR value is high, the errors are extremely small, and vice versa.

The implementation of the different applications had been tested on Python 3.8. The experimental results of different applications it has been observed that mean square error is very less in scratch removal application. While comparing with other methods exemplar based method gives high peak signal to noise ratio show in fig.5.

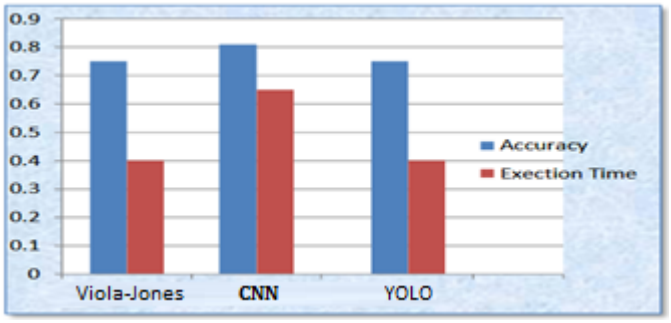

Fig.5: Classification Accuracy Graph of Different Algorithms

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

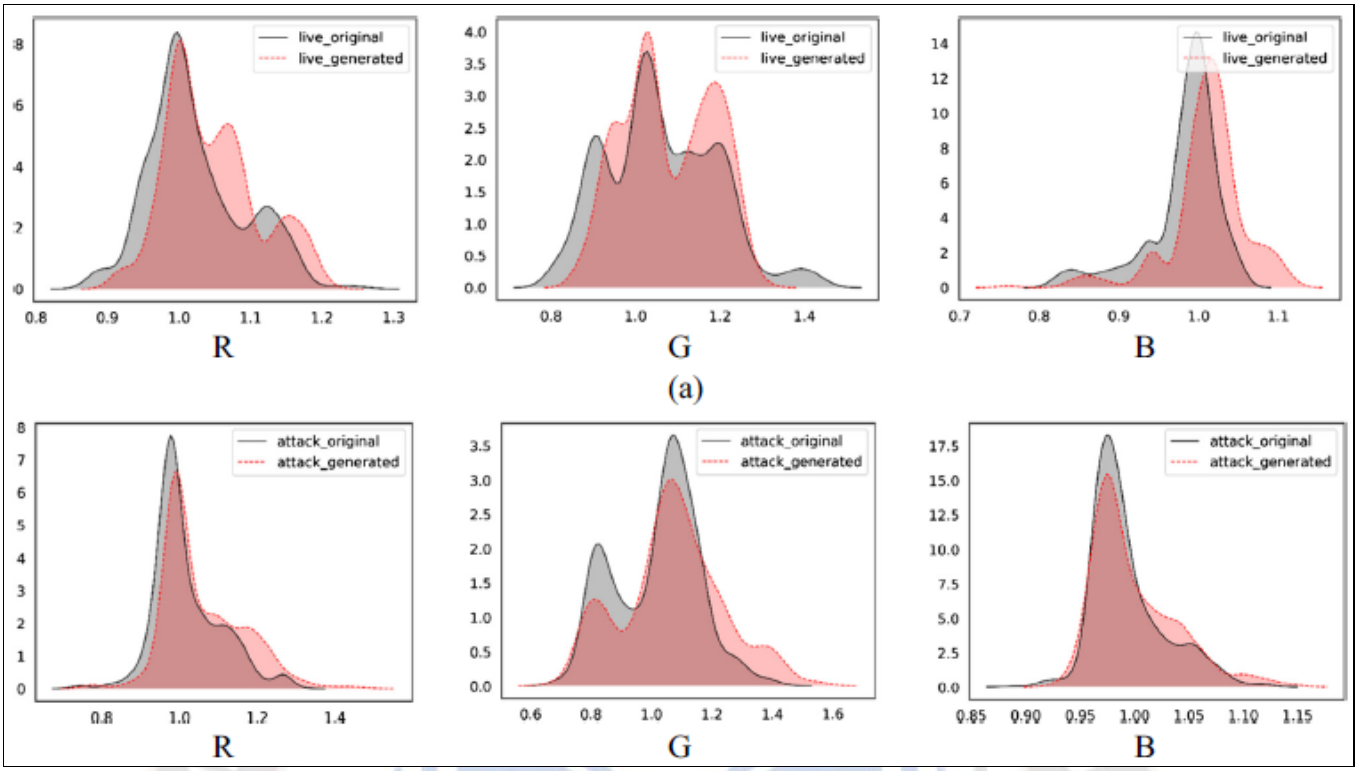

Fig.6: (a) SI histogram for each colour component of the live facial image and matching auto-encoder-generated image. (b) SI histogram for each colour component of the PA facial picture and the associated auto-encoder-generated image.

Fig. 6 displays the similarity index histograms for live pictures and the associated PA in each of the R, G, and B colour spaces that were produced by the deep CNN auto-encoder for the CASIA database [46]. The three-color components of RGB face photographs and the images produced by the auto-encoder clearly differ, as seen in Fig. 2. We also evaluated the deep CNN auto-encoder, which was trained on the CASIA database and evaluated on the Replay-Attack database.

V. CONCLUSION

In this paper, the proposed system aims to enhance security measures by incorporating advanced technologies such as deep learning, face recognition, liveness detection, and criminal identification. The system design encompasses several interconnected modules, including data acquisition, preprocessing, face detection, liveness detection, face recognition, criminal identification, security decision-making, and alert generation.

By leveraging deep learning algorithms, the system can accurately detect and localize faces, distinguish real faces from spoofing attempts, and extract discriminative features for face recognition. The integration of criminal identification capabilities further enhances the system's ability to identify potential threats by matching detected faces against a database of criminal records. The system's decision-making module ensures timely and appropriate actions based on the analysis of the various modules' outputs.

The proposed system design addresses the challenges associated with secure face and liveness detection, as well as criminal identification, for security systems. By combining these capabilities, the system can provide robust and accurate security measures, mitigating potential risks and enhancing overall security in various domains.

With its scalability, real-time processing capability, and integration potential, the proposed system can be seamlessly incorporated into existing security infrastructures or deployed as a standalone solution. The user-friendly interface facilitates easy configuration, monitoring, and management of the system, making it accessible and practical for security personnel.

Furthermore, the proposed system offers a comprehensive approach to secure face and liveness detection with criminal identification, contributing to the development of advanced security systems that can effectively identify individuals, prevent spoofing attempts, and identify potential threats in real-time. For this purpose the system, consider algorithmic improvements and dataset these strategies can enhance the system's performance, efficiency, and real-time processing capabilities.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7231
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 01 July 2023*

ACKNOWLEDGMENT

I'd like to thank all the authors and publishers for making their materials available. I am appreciative to the guide and reviewers for their helpful advice, as well as the college administration for providing the necessary tools and assistance.

REFERENCES

[1] Sergey Maximenko,"Anti-spoofing Techniques in Face Recognition," Research Article from MobiDev, 2020.
[2] Yasar Abbas Ur Rehman, "Face liveness detection using convolutional-features fusion of real and deep network generated face images," 2019 Elsevier.
[3] Stamatiskarnouskos et al, "Artificial intelligence in digital media: The era of deep fakes."IEEE,pp[1-10],6 Jul 2020.
[4] Luca guarnera et al,"Deep fake detection by analyzing convolution traces",IEEE,pp[2841-2850],2020
[5] Pranjalranjan et al, "Improved generalizability of deep-fakes detection using transfer learning based CNN framework",IEEE,pp[86-90],May 2020.
[6] Yash shah et al, "Deep learning model-based multimedia forgery detection." IEEE,pp[564-572],2020.
[7] Zakwanjaroucheh et al, "TRUSTD: Combat fake content using block chain and collective signature technologies."IEEE,pp[1235-1240],2020.
[8] Luisa verdoliva et al, "Media forensics and deep fakes: an overview."IEEE,pp[1-24],2020.
[9] Badhrinarayanmalolan et al, "Explainable deep fake detection using visual interpretability methods." IEEE,pp[289-293],2020.
[10] Siweiiyu et al, "Deep fake detection: Current challenges and next steps." IEEE,2020.
[11] SM abrarkabirchowdhury et al, "Review on deep fake: A looming technological threat." IEEE,2020.
[12] Daehwichoi et al, "FAKE VIDEO DETECTION WITH CERTAINTY-BASED ATTENTION NETWORK.",IEEE,pp[823-827],2020.
[13] Nikita s. ivanov et al, "Combining deep learning and super-resolution algorithm for deep fake detection."IEEE,pp[326-328],2020.
[14] Benjamin Jackson, Mark Johnson, Andrea Ricci, Piotr Wiśniewski, Laura Martínez. Ethical Considerations in Machine Learning Applications for Decision Science. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/221
[15] Adhanalattar et al, "A system for mitigating the problem of deep fake news videos using watermarking.",pp[1-9],2020.
[16] Ali khodabakhsh et al, "Fake face detection methods: can they be generalized." IEEE,2020.
[17] Matthew carter et al, "Approaches for fake content detection strengths and weaknesses to adversarial attacks." IEEE,pp[1-9],2020.
[18] Xi wu et al, "SSTNET: Detecting Manipulated Faces Through Spatial, Stag analysis And Temporal.",IEEE,pp[2952-2956],2020.
[19] Mohammed A.yonus et al, "Abbreviated view of deep fake videos detection techniques." IEEE,pp[115-120],2020.
[20] Steven fernades et al, "Detecting deep fake videos using attribution-based confidence metric." IEEE,pp[1250-1259],2020.
[21] Akashkumar et al, "Detecting deep fakes with metric learning." IEEE, 2020.
[22] Divyababu et al, "Deep fake video detection using image processing and hashing tools." IRJET,pp[338-346],2020.