Face Anti-Spoofing System using Motion and Similarity Feature Elimination under Spoof Attacks

Aditya Bakshi
Department of Computer Science and Engineering,
Shri Mata Vaishno Devi University, India
addybakshi@gmail.com

Sunanda Gupta
Department of Computer Science and Engineering,
Shri Mata Vaishno Devi University, India
sunanda.gupta@smvdu.ac.in

Abstract: *From border control to mobile device unlocking applications, the practical utility of biometric system can be seriously compromised due face spoofing attacks. So, face recognition systems require greater attention to combating face spoofing attacks. As, face spoofing attacks can be easily propelled through 3D masks, video replays, and printed photos so we are presented face recognition system using motion and similarity features elimination under spoof attacks against the Replay Attack and Institute of Automation, Chinese Academy of Sciences (CASIA) databases. In this paper a calculative analysis has been done by firstly segmenting the foreground and background regions from the input video using Gaussion Mixture Model and secondly by extracting features i.e., face, eye, and nose and applied 26 image quality assessment parameters on spoof face videos under different illumination lighting conditions. The results attained using Replay Attack and CASIA databases are extremely competitive in discriminating from fake traits with paralleled viz-a-viz other approaches. Different machine learning classifiers and their comparative analysis with existing approaches has been shown.*

Keywords: *Linear discriminant analysis, support vector, gaussian mixture model, image quality assessment*.

Received January 13, 2021; accepted December 9, 2021
https://doi.org/10.34028/iajit/19/5/6

1. Introduction

The physiological or behavioral characteristics for recognizing a person uniquely is called biometrics. It is an essential mechanism to authenticate the user's identity. There are different types of biometrics such as fingerprints, iris, face, and so on, are used to build various access control system. The major advantage of biometrics is that information that can be acquired from keys, biometric fingerprints, face, and iris cannot be stolen easily because of unique identification attributes of the user's body. Biometric authentication systems are becoming very popular as lots of advancements are there in image analysis techniques [9, 16]. However, it can be the possibility that face, or fingerprints information can be copied or stolen from captured images as users often touching the doors or visiting the banks or markets [25]. So, spoofing attacks are the most common attacks to fool biometric system using fake biometric information. For this, imposters use copies of 3D face models, recorded videos and face images, etc.

Many techniques and approaches have already been proposed against detection of spoof attacks [30]. So, a novel approach is presented for biometric face recognition system to prevent image and video attacks.

As a summary, the classifications of the approaches that are discussed in Table 1, are generally weak for video attacks. For example, the user might be fooled as eye-blinking, frequency analysis, and structure tensor-based methods are used for the recording of fake videos that can be displayed by a high-resolution mobile device. Additional light sources are also used in many approaches which is also a weak point.

1.1. Scope of the Study

A brief introduction to motion-based face anti-spoofing detection and other existing work is shown in this section. Wang *et al*. [26], proposed simple motion measures and multi-scale matching in a wavelet domain to form a discriminative face similarity measure. The proposed approach demonstrates the great results in diverse image capture conditions and large consumer image database. In [6], the author proposed a visual tracking of non-rigid objects where localization and target representation is the central component. The newly proposed mechanism has worked well with the exploitation of background information and face tracking.

Wei *et al*. [28], proposed a high-level feedback mechanism with foreground detection. In this, two kinds of feedback knowledge are introduced to eliminate the destructive impacts i.e., positive and negative prior. The high-level modules for the rough foreground objects provide positive information using optical flow whereas Dirichlet distribution provides negative information by

coping dynamic scenes to suppress the fake Gaussian components. Kim *et al*. [15], presented a fake detection algorithm for face recognition systems by detecting the motion and similarity of an input video sequence. First, foreground and background regions are segmented from an input video. Second, the similarity is measured by recording an original background region and a region without a face and upper body between background regions. Third, a calculative comparison had been done between foreground and background regions concerning motion. In [8], the author designed a system that delivers a reliable and transparent detection service in real time scenario. In this, a device-free Motion detection system (MoSense) with Radio Frequency (RF) is designed by leveraging the dwindling of ubiquitous WiFi signals induced by motions. Table 2 presents a difference (i.e., in terms of extracted features and database) between the pre-existing work and proposed method.

1.2. Motivation

As work on the field of biometric security has been greatly achieved but after going through above-mentioned literature, new research mechanisms are required for today's research culture. So, there is an essential requirement of an exhaustive calculative analysis based on different estimation metrics for designing a face anti-spoofing model that helps to differentiate between the legitimate and illegitimate users. After getting evidence from the above-mentioned existing work, a new biometric system is proposed that provides a secure environment that had been created by considering the system with lots of fraudulent actions. The brief summarization of the objectives in the proposed model is as follows:

- As per the defined nomenclature, a complete discussion on Gaussian Mixture Model, Structural Similarity index, Background motion index, Image Quality Assessment (IQA) parameters, and Machine Learning Classifiers has been done.
- Emphasize the work on detecting the real and fake images by segmenting the foreground and background regions from the live videos, the effect of detection under different lighting conditions, etc. The performance degradation has been greatly improved for detection after going through gaps in the literature.

1.3. Contribution

In this paper, a new approach is presented that overcomes the problems of image and video attacks. After going through different existing approaches, a novel face anti-spoofing detection model is proposed. Our primary focus is to design a novel face anti-spoofing detection model and comparing them with different existing approaches. Based on the above discussion, the significant contributions related to paper are as follows.

To be the best of my knowledge, detection of image and video attacks by extracting nose, eyes, and face features a fake detection approach is proposed and

- IQA parameters are applied to these extracted features. Building a mechanism for detection of the motion in the background region is extracted from the foreground region of the live videos using the Gaussian Mixture Model (GMM).
- A discussion on threshold calculation using LDA for the original image and images under different illuminations conditions. Therefore, the estimated threshold is then matched with attack images from the database and imposter is detected by comparing the threshold values
- Demonstrating the detailed experimental results by validating the performance through the calculation of Half Total Error Rate and accuracy using normal and cross databases (i.e., REPLAY ATTACK and Automation, Chinese Academy of Sciences ((CASIA).

1.4. Organization

The arrangement of the paper is as shown in the FIGURE. The organization of the rest of the paper is as follows. In section 1, the basic overview of Biometrics and classifications of different approaches. In section 2, we discuss the proposed model i.e., for detecting fake user's detection. Section 3 highlights the simulation results of the proposed work and comparison with other approaches. Section 4 discussed the future scope and challenges in implementing other approaches. Then the paper is concluded in section 5.

2. Proposed Model: Face Recognition System Using Motion and Similarity Features Elimination under Spoof Attacks

The viola jones algorithm [27] is used for detecting the features from the user's picture. In the training phase, the feature extraction algorithm is used for extracting the face, eye, and nose from the videos of different illuminations of REPLAY and CASIA databases. The proposed model covers the training and testing phase in which the whole process is divided. After detecting the features using the viola jones algorithm, the Background region (BGcur) [15] is extracted from the current video sequences. After that, the Gaussian Mixture Model (GMM) is used for extracting the background that includes the face and upper body from the foreground region.

Table 1. Classifications of the approaches.

Approaches	Ref No	Feature Type	Proposed Methodology	Database
Face captured by USB or camera	[24]	Face	Proposed a human face detection method for eye blinking using Conditional Random Fields (CRFs).	Video clips captured from Logitech Pro5000
	[23]	Face	Presented an algorithm for live face detection using structural information.	Face image database using the Logitech QuickCam Pro 4000 camera.
	[13]	Face	Proposed a novel face motion optical flow model based on SVM and local Gabor decomposition.	XM2VTS database
Light sources or sensing devices	[14]	Face	Presented a novel reflectance disparity 2D feature model that discriminates between real faces and fake faces.	Albedo facial and mask images
Multi-modal approaches	[29]	Face	Proposed a multimodal audio-video speaker identification model by decomposing the information from the existing video	Sony DSR-PD150P Video Camera at multimedia vision and graphics laboratory
	[5]	Face	Proposed a novel audio-lip features and tensor lip-motion features that are correlated for person identity authentication systems.	VidTIMIT and AVOZES 3D stereovision database
Neuro AI based approaches	[22]	Face	Using error plot, error histogram and confusion matrix, emotional state and trauma of a person identified for detection	Live Database
	[18]	Face	Adaptive neuro fuzzy inference system-based analysis of facial expressions and the recognition of emotions	JAFFE Database

Table 2. Summary of Pre-Existing work with the proposed method on fake biometric detection.

Ref.	Motion and Similarity: Extraction of foreground and background regions	Extracted Features			Calculation of threshold using LDA	Database	
		Face	Nose	Eye		Replay Attack	CASIA
[26]	No	✓	×	×	No	×	×
[6]	No	✓	×	×	No	×	×
[30]	Yes	✓	×	×	No	×	×
[15]	Yes	✓	×	×	No	×	×
[8]	No	✓	×	×	No	×	×
Proposed solution	Yes	✓	✓	✓	Yes	✓	✓

A.

2.1. Explanation of Gaussian Mixture Model (GMM) and on-Line EM

If a foreground object must be detected from a video stream, a technique called Background subtraction is used. The video stream is taken from REPLAY ATTACK and CASIA databases. Over the years, for solving this problem, numerous algorithms have been proposed. But the GMM [28] is the most common state of the art for background subtraction. GMM uses a probability density function for separating each pixel of foreground and background region

The animated textures to be accountable that contains background, GMM has come into the picture [28]. The pixels in this model have a mixture of N Gaussians [23]. Therefore, at time q, the pixel value y for finding the probability of occurrence can be represented as:

$$z(q;\theta) = \sum_{i=1}^{M} p_i G_i \tag{1}$$

Where $G_i \sim M(\mu_i, \sigma_i)$ is i-th Gaussian model and has N components, p_i is the weight of the i-th component which is non-negative and count up to one. μ_i and σ_i are the mean and variance of G_i respectively.

$\theta = \{p_1, . p_2, .., p_N, \mu_1, . \mu_2, .. \mu_N, \sigma_1, . \sigma_2, .. \sigma_N\}$ Is the model parameter.

For a certain pixel, $\{q_1, q_2, q_3, q_r\}$ are pixel values denoted by r, estimation i.e., θ can be maximum calculated using on-line EM algorithm. The algorithm is defined in two steps i.e., E step and M step respectively [19].

E-step: Calculate the posterior probability that the i-th component is responsible for generating q_r.

$$z(i|q_r;\theta_{r-1}) = \frac{p_{i,r-1} G_i(q_r|\mu_i, \sigma_i)}{\sum_{j=1}^{N} p_{j,r-1} G_j(q_r|\mu_i, \sigma_i)} \tag{2}$$

M-step: maximize the likelihood function with respect to the estimator θ, we get

$$p_{i,r} = \ll 1 \gg_i (r) \tag{3}$$

$$\mu_{i,r} = \ll p \gg_i (r) / \ll 1 \gg_i (r) \tag{4}$$

$$\sigma_{i,r} = \ll p^2 \gg_i (r) / \ll 1 \gg_i (r) - \mu_{i,r}^2 \tag{5}$$

Here, the weighted mean $\ll . \gg_i (r)$ with respect to the posterior probability, a recursive form of which can be rewritten as a function of the estimate $\ll . \gg_i (r-1)$ values. The details about the estimation can be seen in [15].

For each pixel, GMM parameters contained in θ can be matched with on-line EM algorithm. For classification of new pixel, following rule is used [19]:

$$\{z(r|BG) = \sum_{i=1}^{B} p_i G_i\} > d_{thr} \tag{6}$$

Where d_{thr} is the constant threshold. If Equation (6) is satisfied, background pixel can be classified as a new pixel. The components are sorted in descending order weight p_i and $z(r|BG)$ is the background model which is represented by B largest Gaussian components. B can be determined by

$$B = \arg\min_b \left(\sum_{j=1}^{b} p_j > d_b\right) \tag{7}$$

Where d_b is a measure of the minimum portion of the pixels that can approximate to the background image.

In this paper, I have further enhanced my work by implementing the model for detecting the background and foreground motion of a video. The block diagram is divided into 2 phases i.e., Training and testing phase. In Training Phase, the features (i.e. face, eye, and nose) are extracted using the viola jones algorithm from videos of REPLAY-ATTACK and CASIA database. Also, features (i.e. face, eye, and nose) are extracted from the user images under different illumination conditions. After extraction, image quality assessment parameters are applied and with the help of the Linear Discriminant Analysis (LDA) threshold is calculated.

In the Testing phase, detection can be defined using two parts i.e., Foreground Detection Testing and Background Detection Testing. In Foreground Detection testing, features of the foreground image are extracted from the database. The foreground image of an imposter is also extracted and applied to image quality assessment parameters. By using the threshold concept using LDA, the imposter can be detected.

In background detection testing, the background of the image is extracted using the Gaussian mixture model from the database. After that, the Structure Similarity index (SSIM) is calculated for the background image. Initial background region and current background region mainly uses mean square error for measuring the similarity between them. In our proposed model, SSIM is used to measure the similarity between two images by measuring a structural component under different illumination conditions [32]. For two image signals and b, SSIM can be defined as (8), (9), and (10) which comprises of three constituents, i.e., luminance, contrast, and structure.

$$m(a,b) = \frac{2\mu_a\mu_b+N_1}{\mu_a^2+\mu_b^2+N_1} \tag{8}$$

$$p(a,b) = \frac{2\sigma_a\sigma_b + N_2}{\sigma_a^2 + \sigma_b^2 + N_2} \tag{9}$$

$$q(a,b) = \frac{\sigma_{ab} + N_3}{\sigma_a + \sigma_b + N_3} \tag{10}$$

Where N_1, N_2, and N_3 are constants, the mean intensity and the standard deviation of luminance's a and b can be denoted as μ_a, μ_b, and σ_a, σ_b respectively. By combining these three components, the equation for SSIM is

$$SSIM(a,b) = [m(a,b)]^{\alpha} \cdot [p(a,b)]^{\beta} \cdot [q(a,b)]^{\gamma} \tag{11}$$

Where the components $\alpha > 0$, $\beta > 0$, and $\gamma > 0$ are used to set the relative importance. The values $\alpha=\beta=\gamma=1$ and $N_3 = N_2/2$ are set to make an SSIM index

$$SSIM(a,b) = \frac{(2\mu_a\mu_b + N_1) + (2\sigma_{ab} + N_2)}{(\mu_a^2 + \mu_b^2 + N_1)(\sigma_a^2 + \sigma_b^2 + N_2)} \tag{12}$$

In the current situation, the current background and background of the original image should be close to 1.

After calculating SSIM, the background motion is extracted from an imposter image. The Background Motion Index (BMI) can be implemented by calculating the foreground and background motion from foreground feature extraction and background feature extraction. For the authentication process, images are extracted from the REPLAY ATTACK and CASIA database. After examining the input video sequences, the segmentation between a background region and foreground region (including a face and upper body) had been done on input video. As, nothing is moving around the background region and foreground region which has some motion, the fake or real is detected on input video by calculating the BMI value between them. Thus, BMI is defined as:

$$MV_{bg} = \frac{1}{Z_{bg}} \sum_{i=1}^{Z_{bg}} \left| R_{i_{bg}}(x) - R_{i_{bg}}(x-1) \right|, \tag{13}$$

$$MV_{fg} = \frac{1}{Z_{fg}} \sum_{i=1}^{Z_{fg}} \left| R_{i_{fg}}(x) - R_{i_{fg}}(x-1) \right|, \tag{14}$$

$$\text{BMI} = MV_{bg}/MV_{fg} \tag{15}$$

Where background and foreground regions are detected by the feature points denoted by Z_{bg} and Z_{fg} respectively, and MV_{bg} and MV_{fg} denote the average value between background and foreground regions which is calculated based on motion vector magnitude, respectively. By using a feature tracker [21], feature points $R_{i_{bg}}(x)$ and $R_{i_{fg}}(x)$ have decided automatically by selecting the background and foreground regions at time *x*. The BMI value is maximum when it is 1, and the BMI value is minimum when it is 0. The decision of the detection of imposter depends on the combined linearly results of SSIM and BMI. After that, the extracted features of the face, nose, and eye are applied to IQA measures.

2.2. Explanation of Image Quality Assessment Parameters

In this paper, 26 image quality measures are used which comprises of both reference and no reference parameters. As it would be difficult to cover all the approaches and methods, the set of 26 IQMs has been used for the initial feature selection process

Table 3. Image quality assessment parameters.

	Type	Name	Description
Image Quality Assessment Parameters	Full Reference	Mean Squared Error (MSE)	$MSE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2$
		Peak Signal to Noise Ratio (PSNR)	$PSNR(I,\hat{I}) = 10\log(\frac{\max(I^2)}{MSE(I,\hat{I})})$
		Signal to Noise Ratio (SNR)	$SNR(I,\hat{I}) = 10\log(\frac{(\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N.M.MSE(I,\hat{I})})$
		Structural Content (SC)	$SC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{I}_{i,j})^2}$
		Maximum Difference (MD)	$MD(I,\hat{I}) = max\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
		Average Difference (AD)	$AD(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})$
		Normalized Absolute Error (NAE)	$NAE(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j} - \hat{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}\rvert}$
		R-Averaged MD(RAMD)	$RAMD(I,\hat{I},R) = \frac{1}{R}\sum_{r=1}^{R} max_r\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
		Laplacian MSE	$LMSE(I,\tilde{I}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(I_{i,j}) - h(\hat{I}_{i,j})}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(I_{i,j})^2}$
		Normalized Cross-Correlation (NCC)	$NXC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j}\cdot\hat{I}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}$
		Mean Angle Similarity (MAE)	$MAS(I,\tilde{I}) = 1 - \frac{1}{NM}\sum_{i-1}^{N}\sum_{j-1}^{M}(\alpha_{i,j})$
		Mean Angle Magnitude Similarity (MAMS)	$MAMS(I,\tilde{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1 - [1 - \alpha_{i,j}][1 - \frac{\lVert I_{i,j} - \hat{I}_{i,j}\rVert}{255}$
		Total Edge Difference (TED)	$TED(I,\tilde{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{E_{i,j}} - \hat{I}_{E_{i,j}}\rvert$
		Total Corner Difference (TCD)	$TCD(I,\tilde{I}) = \frac{\lvert N_{cr} - \hat{N}_{cr}\rvert}{\max(N_{cr} - \hat{N}_{cr}}$
		Spectral Magnitude Error (SME)	$SME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert F_{ij}\rvert - \lvert\hat{F}_{i,j}\rvert)^2$
		Spectral Phase Error (SPE)	$SPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(F_{i,j}) - \arg(\hat{F}_{i,j})\rvert^2$
		Gradient Magnitude Error (GME)	$GME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert G_{i,j}\rvert - \lvert\hat{G}_{i,j}\rvert)^2$
		Gradient Phase Error (GPE)	$GPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(G_{i,j}) - \arg(\hat{G}_{i,j})\rvert^2$
		Structural Similarity Index (SSIM)	Practical implementation available in [37]
		Visual Information Fidelity (VIF)	Practical implementation available in [37]
		Reduced Ref, Entropic Difference	Practical implementation available in [37]
	No Reference	Haar Wavelet Transformation Error (HWTE)	$HWTE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert H_{i,j}\rvert - \lvert\hat{H}_{i,j}\rvert)^2$
		JPEG Quality Index (JQI)	Practical implementation available in [37]
		High-low Frequency Index (HFI)	$SME(I,\tilde{I}) = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}\lvert F_{i,j}\rvert - \sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\lvert F_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert F_{i,j}\rvert}$
		Blind Image Quality Index (BIQI)	Practical implementation available in [37]
		Naturalness image Quality Estimator	Practical implementation available in [37]

There are two types of IQ measures which are following [7]:

1. Full-Reference IQ Measures: Full-Reference (FR) IQA methods are used to check the quality of the test sample to estimate the clear reference between distorted and undistorted images. As the detection system has only access to the input sample, the major problem in fake detection is that the reference image is unknown for the user. In field of steganalysis and for image manipulation detection, full reference IQ measures are extensively and successfully implemented.
2. No-Reference IQ Measures: in the absence of a reference, No-Reference Image Quality Assessment (NR-IQA) is used to assess quality of images in visual form which are very complex and challenging problem. These references are used to check the quality level of an image according to some pre-trained statistical models. Table 3 shows the detailed

practical implementation of image quality assessment parameters.

After applying IQA measures, LDA [10] which is a basic method that is used in various image processing applications for the calculation of threshold value and authentication for differentiate between legitimate and illegitimate users. For solutions against spoofing attacks, LDA and its variations are the most successful technique that can be used as countermeasures for detection between legitimate and illegitimate users.

After implementing the training phase, let's discuss the next phase which is the testing phase. So, in the testing phase, again feature extraction mechanism is applied for the extraction of features (i.e., face, eye, nose) of an original user, and IQA measures are applied. After that, with the help of viola jones algorithm IQA measures are applied to the extracted features (i.e., face, eye, and nose) of an attacker image from the database. In the replica of the training phase, a threshold value is calculated for the detection of an imposter that is applied on the values of IQA parameters for measuring the False Fake Rate (FFR) and False Genuine Rate (FGR) and Half Total Error Rate (HTER) in a testing phase.

In the next part, for checking the accuracy of the system machine learning classifiers are applied after the combined calculation Half Total Error Rate for face, nose, and eye.

2.3. Explanation Machine Learning Classifiers

The essential mechanism required for data analytics, pattern recognition, and machine learning is called classification. Classification is done in two phases. First, the performance and accuracy are measured between the training data set and extracted model that can be validated against a labeled test data. The document classification, spam filtering, image classification, fraud detection, risk analysis are the various applications of classification [21]. By finding the common features and finding patterns for each testing and training instances of a class is called a supervised learning technique.

There are two types of machine learning classification

a) Supervised machine learning classification.
b) Unsupervised machine learning classification.

Supervised machine learning is the construction of algorithms that predicts future instances from the externally supplied instances that can be produced by general patterns and hypotheses. Supervised Machine learning classifiers are further divided as:

a) Bayesian Networks

The probability relationship among the set of variables that can be graphically represented is called Bayesian Networks. These networks are very difficult to implement as it is impossible to depict the parameters in Directed Acyclic Graphs. Prior information about the problem can be represented as a structural relationship among its features. The main drawback of Bayesian Networks is that it is very difficult to design in larger networks i.e., in terms of time and space.

b) Naïve Bayes

It is a type of Bayesian Network having relationship between parent and children in which child nodes are independent of each other i.e., Class conditional independence. Naïve Bayes is a type of classifier which converges at a very faster rate than logistic regression if class conditional independence assumption holds. It takes very less computational time for the training of data. Naïve Bayes can be applying to a very wide variety of tasks as it returns a simpler probability function. If the user wants to consider the features, then naïve bayes are not greatly applicable.

c) Logistic Regression

The logistic model has a very nice probabilistic interpretation and helpful for updating new data very easily. The threshold can be easily adjusted as it works on probability. In place of discriminative analysis, the logistic model produces better results. It can handle interaction effects, nonlinear effects, and power terms. For achieving stable results, logistic regression requires a very large sample size [21].

d) Decision Tree and Random Forests

The explanation and interpretation of decision trees are very easy because of the interaction between its features. Decision trees can be used to find missing or redundant values and have good generalization ability [20]. Decision trees can handle a variety of data and provide high performance for relatively small computational efforts. For building a tree, it takes very less computational time but very high considerable time. Therefore, it is very difficult to handle high dimensional data in decision trees. These use divide and conquer approach for solving problems but doesn't give fruitful results if problems are very complex [21].

In this section, the face spoofing detection model using motion and similarity features elimination has been proposed in Figure 1 using foreground and background detection testing mechanism followed by an algorithm. The description of an algorithm and its symbolization are mentioned in Table 4.

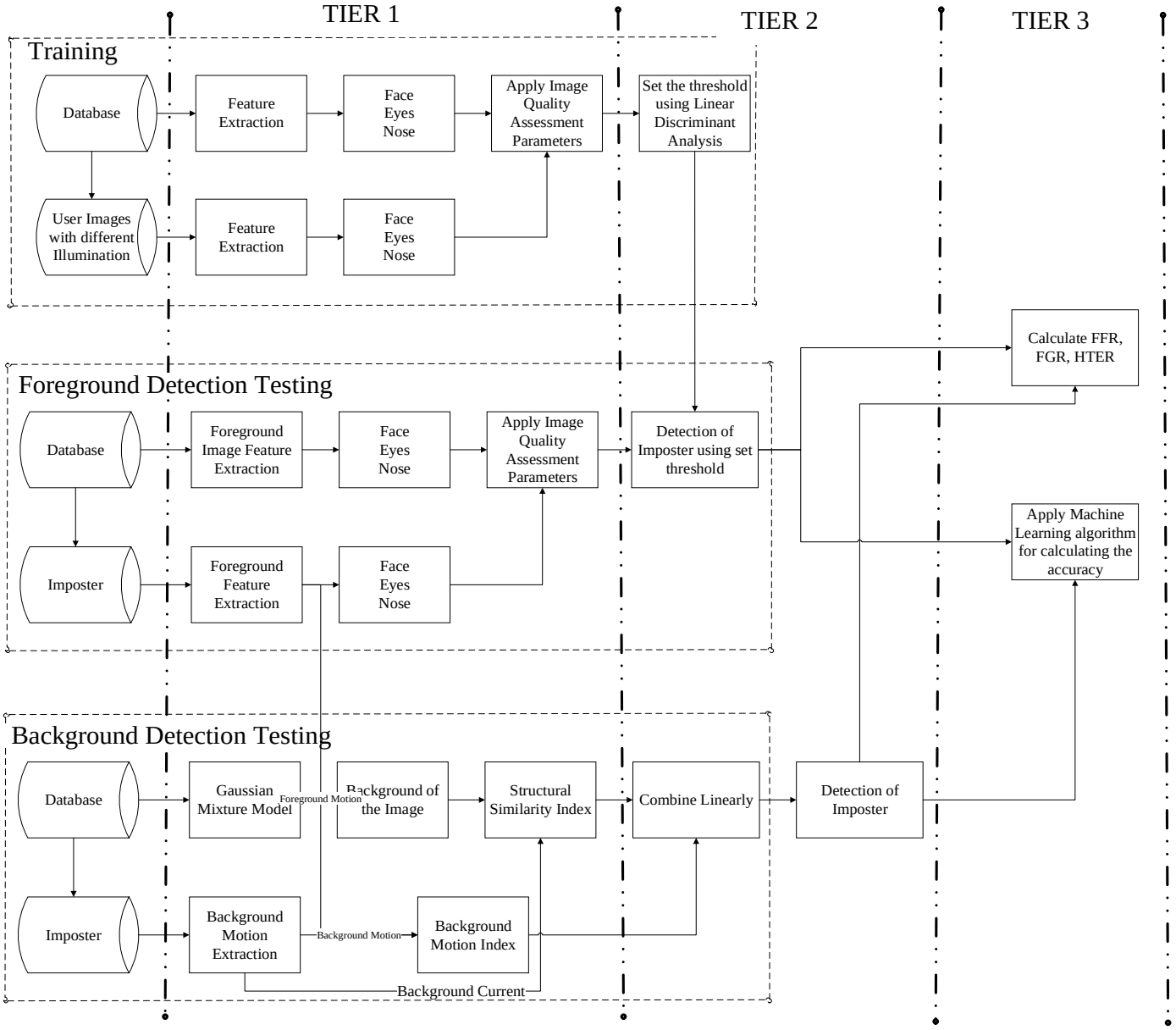

Figure 1. Proposed face spoofing detection model using motion and similarity features elimination.

Algorithm for the Face Recognition System using Motion and Similarity Features Elimination under Spoof Attack

1: For legitimate user, select Replay Attack and CASIA database
$P = [I_1, I_2, I_3 \dots \dots I_N]$

Algorithm1: For Training Phase

Tier-1:
1: For taking out the features from database, apply Voila jones algorithm
$P_v = [P_f, P_e, P_n]$
$P_f = [I_1^f, I_2^f, I_3^f \dots \dots . I_N^f]$
$P_e = [I_1^e, I_2^e, I_3^e \dots \dots . I_N^e]$
$P_n = [I_1^n, I_2^n, I_3^n \dots \dots . I_N^n]$
2: Apply user image under changed lighting condition from database
3: For feature extraction of an image I_q again Voila-Jones algorithm is applied
$I_q \rightarrow I_q^f, I_q^e, I_q^n$
4: Apply IQA Parameters
$IQA = [IQA_1, IQA_2, IQA_3 \dots \dots IQA_{26}]$, *where,*
$IQA_1 = MSE(I_1^f, I_q^f) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{1,ij}^f - I_{q,ij}^f)^2$

Tier-2:
1: Using Linear Discriminant Analysis (LDA), value of threshold is calculated
$Thr = [Thr_1, Thr_2, Thr_3 \dots \dots Thr_{26}]$
Where, $Thr_1 = \frac{MSE(I_1^f, I_q^f) - MSE(I_1^f, I_1^f)}{}$
$f(G) = trace((G^T P_v G)^{-1}{}^2 G^T P_u G)$

Algorithm 2: For Testing Phase

Tier-1: Foreground Detection Testing
1: For taking out the foreground features from database apply Voila jones algorithm
$L_v = [L_f, L_e, L_n]$
$L_f = [I_1^f, I_2^f, I_3^f \dots \dots . I_N^f]$
$L_e = [I_1^e, I_2^e, I_3^e \dots \dots . I_N^e]$
$L_n = [I_1^n, I_2^n, I_3^n \dots \dots . I_N^n]$
2: Imposter attack can be generated as image I_r

3: For feature extraction of an image I_r again Voila-Jones algorithm is applied

$I_r \rightarrow I_r^f, I_r^e, I_r^n$

4: Apply IQA Parameters

$IQA = [IQA_1, IQA_2, IQA_3 \dots \dots IQA_{26}]$, *where,*

$IQA_1 = MSE(I_1^f, I_r^f) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{1,ij}^f - I_{r,ij}^f)^2$

Tier-2:

1: Using Linear Discriminant Analysis (LDA), value of threshold is calculated for an imposter

$Thr = [Thr_1, Thr_2, Thr_3 \dots \dots Thr_{26}]$,

Where, $Thr_1 = \frac{MSE(I_1^f, I_r^f) - MSE(I_1^f, I_1^f)}{2}$

$f(G) = trace((G^T P_v G)^{-1} G^T P_u G)$

2: Finding of Counterfeit Biometric

Set the IQA Vector

for j=1:1:26

if $IQA_j > Th_i$ *then*

$IQA_j = 1$

IQA = [IQA IQA_j*]*

end

j=j+1

end

if IQA is Unison then

Block imposter after detection

else

Legitimate User

end

Tier 1: Background Detection Testing

1: For taking out the features from the database, apply the Voila jones algorithm.

$S_v = [S_f, S_e, S_n]$

$S_f = [I_1^f, I_2^f, I_3^f \dots \dots I_N^f]$

$S_e = [I_1^e, I_2^e, I_3^e \dots \dots I_N^e]$

$S_n = [I_1^n, I_2^n, I_3^n \dots \dots I_N^n]$

2: Apply a Gaussian Mixture Model for extracting the Background of an Image

$B = arg\min_b(\sum_{j=1}^{b} p_j > d_b$

3: Calculate the Structural Similarity Index (SSIM) of the current background image and the original image

$SSIM(a,b) = \frac{(2\mu_a\mu_b + N_1) + (2\sigma_{ab} + N_2)}{(\mu_a^2 + \mu_b^2 + N_1)(\sigma_a^2 + \sigma_b^2 + N_2)}$

4: Attack of an Imposter, I_j

5: Calculate Background Motion Index (BMI) between foreground motion and background motion of an image.

$BMI = MV_{bg}/MV_{fg}$

Tier 2:

1: Detection of imposter by linearly combining the result of SSIM and BMI

Tier 3:

a) Exploration of errors by calculating False Fake Rate, False Genuine Rate and Half Total Error Rate:

$False\ Fake\ Rate = \frac{Number\ of\ FRs}{Number\ of\ true\ claim\ attempts}$

$False\ Genuine\ Rate = \frac{Number\ of\ FAs}{Number\ of\ imposter\ attempts}$

$Half\ Total\ Error\ Rate = \frac{False\ Fake\ Rate + False\ Genuine\ Rate}{2}$

b) Estimation of an Algorithm

Using different machine learning classifiers, calculate the estimation of an algorithm.

Table 4. Description of an algorithm and its symbolizations.

Symbols	Description
P	Database of a valid user
$I_1, I_2, I_3 \dots \dots I_N$	Valid user images
P_v, L_v, S_v	Features extraction for valid users from the database
P_f, L_f, S_f	Features extraction for the face of valid users from the database
P_e, L_e, S_e	Features extraction for the eye of valid users from the database
P_n, L_n, S_n	Features extraction for the nose of valid users from the database
$I_1^f, I_2^f, I_3^f \dots \dots I_N^f$	Face images of valid users
$I_1^e, I_2^e, I_3^e \dots \dots I_N^e$	Eye images of valid users
$I_1^n, I_2^n, I_3^n \dots \dots I_N^n$	Nose images of valid users
I_q, I_r	User image of an Imposter
I_q^f, I_r^f	Face image of an Imposter
I_q^e, I_r^e	Eye image of an Imposter
I_q^n, I_r^n	Nose image of an Imposter
G	Dimensionality-diminished space
LDA	Linear Discriminant Analysis
IQA	Image Quality Assessment Parameter
Thr	Threshold
MSE	Mean Square Error
FFR	False Fake Rate
FGR	False Genuine Rate
HTER	Half Total Error Rate
SSIM	Structural Similarity Index
BMI	Background Motion Index

e) Support Vector Machines

The accuracy of support vector machines is very high, but implementation is very complex. If there is no linear separability of data in feature space, the support vector machine gives great results. A support vector machine is used to find out the nearest sample point with minimum distance in a hyperplane. In SVM, the accuracy and performance depend on the number of training cycles that are independent of data and size. The text classification problems and high dimensional data can be easily handled in SVM. The choice of parameters is very important in the training of data as it directly affects the performance. It has good generalization ability and robust to high dimensional data [17]. As SVM's training speed is very less, therefore the performance depends on the choice of parameters.

f) K- Nearest Neighbour

K- Nearest Neighbour assigns to an unlabeled sample point which is nearest to set of previously labeled points. Therefore, it is called a non-parametric classification algorithm. For sampling points, K- Nearest Neighbour classification is independent of the joint distribution. It is used in applications where objects can have many labels and suits for multi-modal objects. The other name of this algorithm is a simple lazy learning method because its efficacy is very low. The performance can also be measured by selecting the good value of 'k'. The features are adversely affected by noise too.

3. Simulation Results

To get reproducible results, we have implemented a face

recognition system using motion and similarity features elimination under spoof attacks which are implemented on different databases accessible with a well-described evaluation mechanism. The execution of the proposed model is compared with other available state of the art databases such as the REPLAY-ATTACK database, CASIA, etc.

3.1. Replay Attack and CASIA Database

The REPLAY-ATTACK Database [31], face a spoofing database that can be accessed through the IDIAP Research Institute. There are a total of 50 videos of deceiving and true attacks of dissimilar users in the database. In the database, the attacks were reflected which are mainly three types:

a) Print, genuine users digital photographs are taken for illegitimate access attempts.
b) For attack purpose, mobile pictures and videos are captured from the phone.
c) High-def, higher resolution pictures and videos that were similarly captured from the mobile. Therefore, through testing and training REPLAY-ATTACK database is used for face anti-spoofing detection.

A total of 600 video clips of 50 peoples can be accessed by the CASIA database. For multiple fake samples, high-quality real face recordings are there in the database. To record changes three different imaging qualities are exploited in the database [4].

Table 5 shows the acquired outcomes (in percentage) on the REPLAY ATTACK database with different situations.

Table 5. Comparison of the proposed model with another framework on the replay attack database.

Ref.	Real			Print			Mobile			High definition		
	False Fake Rate	False Genuine Rate	Half Total Error Rate	False Fake Rate	False Genuine Rate	Half Total Error rate	False Fake Rate	False Genuine Rate	Half Total Error rate	False Fake Rate	False Genuine Rate	Half Total Error rate
[7]	-	-	-	11.6	4.1	7.9	2.4	3.9	3.2	14.0	10.2	12.1
[4]	-	-	-	8.2	11.53	9.87	3	4.9	3.95	-	-	-
[1]	2.31	7.5	4.9	7.9	2.9	5.1	1.8	2.7	2.25	12.2	8.2	10.2
Proposed solution	2.11	6.5	4.3	6.9	2.1	4.5	1.2	2.2	1.7	11.2	7.9	9.5

Table 4 reflects the results attained from the test set by the proposed model. The results clearly show the Half Total Error Rate of the proposed method gives better performance by using a standard LDA classifier. After extracting the samples from three datasets such as mobile, print, and high-def, the values in percentage for False Genuine Rate, False Acceptance Rate, and Half Total Error Rate are shown in the proposed solution. In [7], an anti-spoofing face mechanism is proposed with Half Total Error Rate values 7.9%, 3.2% for print, mobile attack type respectively. Chingovska and Dos Anjos [4], the author proposed a client identity anti-spoofing approach for face in which Half Total Error Rate values 9.87% and 3.95% respectively are shown for print and mobile attack type. Similarly, in [1] the same Half Total Error Rate values 5.1% and 2.25% respectively for print and mobile attack type using 3-Tier face anti-spoofing detection model are shown. But our model has Half Total Error Rate values 4.5 % and 1.7 % respectively which are better after comparing with other state of art algorithms. After that, we calculate the Half Total Error Rate in percentage on different IQA measures.

In the subsequent result section, the comparison using a cross-database setup with an attack-specific mechanism for face anti-spoofing detection is analyzed. Two broad classes of attacks are being considered here, i.e., print and display attacks, because they are present in both the databases.

Table 6. Comparison in term of HTER percentage of the proposed model in cross-database.

Ref	Train on	CASIA	Train on	REPLAY ATTACK
	Test on	REPLAY ATTACK	Test on	CASIA
[1]		7.6		30.2
[3]		14.0		32.7
[3]		9.6		39.2
Proposed solution		6.9		29.6

The summary of attained cross-database results is available in Table 6.

Table 6 shows the comparison between Half Total Error Rate values attaining the cross-database set-up. In the cross-database scenario, the values of Half Total Error Rate are calculated when trained and tested on both REPLAY ATTACK and CASIA database. So, in [1] a 3-Tier face anti-spoofing model is proposed where Half Total Error Rate value is 7.6% and in [3], Color Texture-based Face Anti-spoofing Presentation Attack model and Rotation Invariant- Local binary pattern is proposed and Half Total Error Rate values are 14 % and 9.6 %, respectively. Similarly, when the train on REPLAY ATTACK and test on CASIA database, the Half Total Error Rate values are 30%, 32 % and 39.2 %, respectively for the same functionality explained in [1, 3]. But the Half Total Error Rate values 6.9 % and 29.6 % of the proposed model earn more vigorous performance on average than other models. For getting these robust results, different values IQA parameters are

calculated.

The accuracy of the proposed model is shown in a further section with diverse machine learning classifiers. For comparing the accuracy of the model, we have implemented four classifiers, i.e., Logistic Regression, Support Vector Machine, Random Forest, and Decision Tree, etc., After implementing LDA, the threshold is calculated for each extracted feature where all these classifiers are applied in the form of 0 and 1 values.

The experimental outcomes in Figure 2 show Support Vector Machine (SVM) classifier gives better results in terms of accuracy by implementing the proposed model. After equating the results with other classifiers, the SVM provides 98 percent accuracy. Figure 3 represents the comparison of the proposed model with available work in terms of accuracy using the SVM classifier.

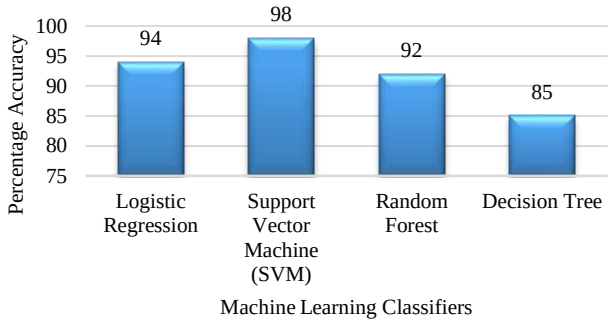

Figure 2. Comparison of machine learning classifiers in terms of accuracy (percentage) in the proposed model.

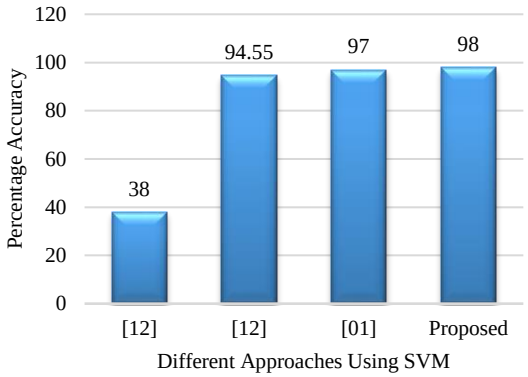

Figure 3. Comparison of accuracy with other approaches on the SVM classifier.

In [12], the accuracy of the proposed model i.e., a multi-directional local gradient descriptor using the SVM classifier is 38 % and 94.55% respectively. Bakshi *et al*. [1], the author has proposed 3-Tier face anti-spoofing detection model in which SVM classifier is applied and maximum accuracy attained is 97%. But the accuracy of our proposed model Figure 3 is greatly improved by 98% when SVM classifier is implemented.

Apart from the accuracy, the detection rate, false positives are calculated using SVM classifiers and compared with different state of art approaches. In [2], 94.68 % detection rate and 3.68 % false positives is obtained using SVM classifier. In [11], 74.2% - 88.7% detection rate has been obtained using single SVM based classifier. But, proposed model gives 98.87 % detection rate and 3.47 % false positives after applying the SVM classifier. So, proposed model gives reduced computational complexity with less training time thus allowing better generalization in results.

4. Future Scope

While outstanding results have already been obtained in face anti-spoofing detection, we are addressing some future directions that help other authors to enhance the work in this field.

First, the proposed model gives better results, but the accuracy will be improved if a more sophisticated object detection approach can be applied. For improving the performance of the system, there is a need for the computationally cheap mechanism is required that can be used in various consumer electronics solutions

Second, the motion and similarity approach might give efficient results on mobile, print, and high-definition videos. But work can be enhanced by using MSU MFSD and Yale databases with their comparative analysis too. Also, many descriptors like PCA and QDA can be used for recognition and spoofing detection evaluations.

Third, lots of new direction has already been done in face anti-spoofing but multimodal biometric systems are not greatly implemented as it would be difficult to falsify multiple biometrics features at the same time. So, to avoid spoof attacks multimodality cab is used as a special case to enhance current countermeasures for industrial applications in the field of facial biometrics.

5. Conclusions

After going through previously instances of hidden procurement circumstances and attack forms, amazing results had been drafted from distinct databases against face anti-spoofing methods but in realistic setup it fails to give more generalize results. So, motivated by the instances and read different approaches, face recognition system using motion and similarity features elimination under spoof attacks is proposed. The proposed solution can be presented as the following:

1. Foreground and background regions are segmented from input video using the Gaussian mixture model.
2. A Structural Similarity Index (SSIM) is calculated based on the content of the video sequences (i.e., motion and similarity) which linearly combines the information.
3. The movement of motion between background and foreground can be calculated using BMI. Extensive experimentation has been explained that involves a generalization of image quality assessment parameters for calculation of FFR, FGR, and HTER which are associated with the other state of art

algorithms in the cross-database scenario. The model also showed an accuracy of 98 percent by applying the SVM classifier for the detection of real and fake users. Therefore, the proposed model produces favorable results which are compared with other approaches in face anti-spoofing.

Abbreviations

Abbreviations	Full form
IQA	Image Quality Assessment
LDA	Linear Discriminant Analysis
FFR	False Fake Rate
FGR	False Genuine Rate
HTER	Half Total Error Rate
SVM	Support Vector Machine
MSE	Mean Squared Error
PSNR	Peak Signal to Noise Ratio
MD	Maximum Difference
SNR	Signal to Noise ratio
SC	Structural Content
CQ	Correlation Quality
AD	Average Difference
NAE	Normalized Absolute Error
PMSE	Peak Mean Square Error
RAMD	R-Averaged Maximum Difference
NXC	Normalized Cross-Correlation
HWTE	Haar Wavelet Transformation Error
TED	Total Edge Difference
TCD	Total Corner Difference
SME	Spectral Magnitude Error
SPE	Spectral Phase Error
GME	Gradient Magnitude Error
GPE	Gradient Phase Error
JQI	JPEG Quality Index
HLFI	High Low-Frequency Index
BIQI	Blind Image Quality Index
GMM	Gaussian Mixture Model
SSIM	Structural Similarity Index
BMI	Background Motion Index

References

[1] Bakshi A., Gupta S., Gupta A., Tanwar S., and Hsiao K., "3T-FASDM: Linear Discriminant Analysis-Based Three-tier Face Anti-spoofing Detection Model Using Support Vector Machine," *International Journal of Communication Systems*, vol. 33, no. 12, pp. e4441, 2020.

[2] Boia R., Dogaru R., and Florea L., "A Comparison of Several Classifiers for Eye Detection on Emotion Expressing Faces," *in Proceeding of the 4th International Symposium on Electrical and Electronics Engineering*, Galati, pp. 1-6, 2013.

[3] Boulkenafet Z., Komulainen J., and Hadid A., "On The Generalization of Color Texture-based Face Anti-Spoofing," *Image and Vision Computing*, vol. 77, pp. 1-9, 2018.

[4] Chingovska I. and Dos Anjos A., "On the Use of Client Identity Information for Face Antispoofing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 787-796, 2015.

[5] Chetty G. and Wagner M., "Biometric Person Authentication with Liveness Detection Based on Audio-Visual Fusion," *International Journal of Biometrics*, vol. 1, no. 4, pp. 463-478, 2009.

[6] Comaniciu D., Ramesh V., and Meer P., "Kernel-Based Object Tracking," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 5, pp. 564-577, 2003.

[7] Galbally J., Marcel S., and Fierrez J., "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," *IEEE transactions on image processing*, vol. 23, no. 2, pp. 710-724, 2013.

[8] Gu Y., Zhan J., Ji Y., Li J., Ren F., and Gao S., "MoSense: An RF-based Motion Detection System Via Off-the-shelf WiFi Devices" *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2326-2341, 2017.

[9] Jain A., Bolle R., and Pankanti S., *Biometrics: Personal Identification in Networked Society*, Springer Science and Business Media, 2006.

[10] Ji S. and Ye J., "Generalized Linear Discriminant Analysis: a Unified Framework and Efficient Model Selection," *IEEE Transactions on Neural Networks*, vol. 19, no. 10, pp. 1768-1782, 2008.

[11] Jones S. and Capson D., "Two-Stage Classification Using Selective Attention for Fast Face Detection," *in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, pp. v-465, 2005.

[12] Kagawade V. and Angadi S., "Multi-Directional Local Gradient Descriptor: A New Feature Descriptor for Face Recognition," *Image and Vision Computing*, vol. 83, pp. 39-50, 2019.

[13] Kollreider K., Fronthaler H., and Bigun J., "Evaluating Liveness By Face Images and the Structure Tensor," *in Proceeding of the 4th IEEE Workshop on Automatic Identification Advanced Technologies*, Buffalo, pp. 75-80, 2005.

[14] Kim Y., Na J., Yoon S., and Yi J., "Masked Fake Face Detection Using Radiance Measurements," *JOSA A*, vol. 26, no. 4, pp. 760-766, 2009.

[15] Kim Y., Yoo J., and Choi K., "A Motion and Similarity-based Fake Detection Method for Biometric Face Recognition Systems" *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 756-762, 2011.

[16] Lee K. and Byun H., "A New Face Authentication System for Memory-constrained Devices," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1214-1222, 2003.

[17] Li J., Wang Y., Tan T., and Jain A., "Live Face Detection Based on the Analysis of Fourier Spectra," *in Proceeding of the Biometric Technology for Human Identification*, Orlando, pp. 296-303, 2004.

[18] Perikos I., Paraskevas M., and Hatzilygeroudis I., "Facial Expression Recognition Using Adaptive Neuro-fuzzy Inference Systems," *in Proceeding of*

the IEEE/ACIS 17th International Conference on Computer and Information Science, Singapore, pp. 1-6, 2018.

[19] Sato M. and Ishii S., "On-line EM Algorithm for the Normalized Gaussian Network," *Neural computation*, vol. 12, no. 2, pp. 407-432, 2000.

[20] See Y., Liew E., and Noor N., "Gabor and Maximum Response Filters with Random Forest Classifier for Face Recognition in the Wild" *The International Arab Journal of Information Technology*, vol. 18, no. 6, pp. 797-806, 2021.

[21] Singh A., Thakur N., and Sharma A., "A Review of Supervised Machine Learning Algorithms," *in Proceeding of the 3rd International Conference on Computing for Sustainable Global Development*, New Delhi, pp. 1310-1315, 2016.

[22] Sofia R. and Sivakumar D., "Developing a System for Trauma Identification Based on the Difference from the Normal Human Emotion with Adaptive Neuro Fuzzy Inference System," *in Proceeding of the International Conference on Communication and Signal Processing*, Chennai, pp. 0672-0678, 2019.

[23] Stauffer C. and Grimson W., "Adaptive Background Mixture Models for Real-time Tracking," *in Proceedings of the IEEE Computer Society Conference on Computer Vision And Pattern Recognition*, Fort Collins, pp. 246-252,1999.

[24] Sun L., Pan G., Wu Z., and Lao S., "Blinking-based Live Face Detection Using Conditional Random Fields," *in Proceeding of the International Conference on Biometrics*, Seoul, pp. 252-260, 2007.

[25] Toth B., "Biometric Liveness Detection," *Information Security Bulletin*, vol. 10, no. 8, pp. 291-297, 2005.

[26] Wang R., Huang T., Stubler P., and Mehrotra R., "Robust Face Recognition Based on Motion Pursuit," *in Proceedings of the IEEE International Conference on Multimedia and Expo*, Lausanne, pp. 153-156, 2002.

[27] Wang Y., "An analysis of the Viola-Jones Face Detection Algorithm," *Image Processing Online*, vol. 4, pp. 128-148, 2014.

[28] Wei W., Hui Q., Peng C., and Shenyi C., "High Level Feedback for Foreground Detection," *in Proceeding of the IEEE Youth Conference on Information, Computing and Telecommunication*, Beijing, pp. 323-326, 2009.

[29] Yemez Y., Kanak A., Erzin E., and Tekalp A., "Multimodal Speaker Identification with Audio-Video Processing," *in Proceedings of the International Conference on Image*, Barcelona, pp. III-5, 2003.

[30] Zhang D., *Biometric Solutions: for Authentication in an E-World*, Springer Science and Business Media, 2012.

[31] Zhang Y., Dubey R., Hua G., and Thing V., "Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern," *in Proceeding of the TENCON IEEE Region 10 Conference*, pp. 0309-0314, 2018.

[32] Zivkovic Z. and Van Der Heijden F., "Efficient Adaptive Density Estimation per Image Pixel for the Task of Background Subtraction," *Pattern Recognition Letters*, vol. 27, no. 7, pp. 773-780, 2006.

Aditya Bakshi received a B.Tech degree in computer science and engineering from Kurukshetra University, Haryana, India, in 2010, an M.Tech degree in computer science and engineering from the YMCA University of Science and Technology, Faridabad, India, in 2012. He is currently pursuing a Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Jammu and Kashmir, India, and an Assistant Professor in the School of Computer Science and Engineering, Lovely Professional University, Punjab, India.

He is currently involved in research work on biometric security and manet applications. His research interests include the security of next-generation biometric systems using image processing. Mr.Bakshi is a member of the International Association of Engineers and the Universal Association of Computer and Electronics Engineers.

Sunanda Gupta received the Bachelor's degree in Sciences and Master's degree in Computer Applications from the University of Jammu, and the Ph.D. degree in Computer Science and Engineering from Shri Mata Vaishno Devi University, Jammu and Kashmir, India, in 2014. She is currently an Assistant Professor in the Department of Computer Science & Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India with more than twelve years of teaching experience.

She has authored several research articles in international journals of repute and presented papers in several international/ national conferences. She has also been invited as an expert to various international conferences as a reviewer/ technical program committee member. Her research interests include combinational optimization problems, genetic algorithms, and image processing.