International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988Volume 12 (2020) pp. 374-386

Received: 28 May, 2020; Accepted: 30 Oct, 2020; Publish: 4 Nov, 2020

Improved Face Spoofing Detection Using Random Forest Classifier with Fusion of Luminance Chroma Features

Sudeep D. Thepade[1], Piyush Chaudhari[2], Mayuresh Dindorkar[3], Shalakha Bang[4] and Rohit Bangar[5]

[1, 2, 3, 4, 5] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India
[1]*sudeepthepade@gmail.com*
[2]*piyushrc26@gmail.com*
[3]*dmayuresh99@gmail.com*
[4]*shalakhabang99@gmail.com*
[5]*bangarrohit7057@gmail.com*

Abstract: **Ambient computing applications verify identity of an individual using biometric identity in addition to conventional security measures. The cyber applications do have provision of face identification to strengthen the secure access for financial and other critical applications. Face recognition is more susceptible to spoofing / face presentation attacks, where the print of face or face video replay is used to spoof the identity of an individual. The paper proposes performance improvisation of existing face presentation attack detection technique using machine learning algorithms and fusion of luminance-chromaticity (Kekre-LUV, CIE-LUV, YCrCb) face features. The paper does empirical assessment of color space combinations that are used for feature extraction to decide whether face is real or spoofed. Along with the earlier advocated use of ExtraTree classifier, the paper explores using Random Forest and other ensembles of machine learning algorithms (classifiers) in detection of face presentation attack and Random Forest significantly improves the performance of face spoofing detection as it is clearly evident form articulated results. The paper also proposes use of Kekre-LUV color space which is computationally lighter than earlier used CIE-LUV, experimental analysis shows that almost similar performance of face presentation attack detection is observed using Kekre's LUV color space. Further the fusion of the luminance chroma features are proposed to be used for higher accuracy. The proposed method is validated using two datasets as 'Replay Attack' and 'NUAA', with help of 'accuracy' and 'half total error rate' (HTER) as performance measures. The achieved accuracy and HTER have proved the worth of proposed methodology.**

Keywords**:** Object Spoof Detection, Face Liveness Detection, Color Space, Machine Learning**.**

I. Introduction

In today's era, tenths of quintillion bytes of data is generated per day and securing this data is a big challenge for a mankind. Countless efforts are being taken by researchers to preserve the integrity of this data. Digital security is an important aspect as it improves the automated task of managing an individual's privacy. Such security is primarily based on biometric traits like iris, thumb, palm print and face. Face recognition is usually preferred because of its simplicity, rapid response to stimuli and contactless acquisition. Thus, a major portion of biometrics is covered by face recognition but it is susceptible to various spoofing attacks such as photo, cut-photo, video and mask attacks. In order to counteract these attacks different face anti-spoofing techniques are discovered, focusing on varied domains like making use of texture features, motion based features, frequency based features, convolutional neural networks (CNN) etc. are developed till date. Image based object spoofing detection technique uses mostly texture features but it is found that there is a need of improvement.

The remaining paper organization has Introduction in section-1, Literature Review in section-2, Proposed method in section-3, Experimentation Environment in section-4, Results and Discussion in section-5 and paper concluding remarks in section-6.

II. Literature Survey

Every security system using face recognition for user identify verification has the threat of being attacked. Various photo, video, cut-photo, mask attacks are targeted to delude the face recognition systems. Among all the face spoofing methods proposed till date, object-spoofing is one of the methods and finds the need of improvisation in performance accuracy and HTER.

In [1] authors have proposed the image based object spoofing detection which is experimented on objects: cork and face by extracting global color features from YCrCb and CIE-LUV color spaces and ExtraTree classifier is used for distinguishing between genuine and fake access attempts. But the validation is done only on one dataset. The performance of the proposed method can be evaluated on other available datasets (e.g. NUAA dataset) that will help to build a racial invariant method.

In [2] the color and texture features are extracted from the image using ULTP (Uniform Local Ternary Pattern), ULBP

(Uniform Local Binary Pattern), R-G and COLOR (COLOR-INF and COLOR-MMT). After feature fusion, features vector is provided to SVM (Support Vector Machine) for identifying real and spoofed faces. Among all considered datasets, good results are achieved on CASIA-FASD. The method is complex and computationally heavy due to involvement of local binary pattern calculation.

The method proposed in [3] extracts the LBP features from YCrCb and Gray color space. Further, COALBPs (Co-occurrence of Adjacent Local Binary Patterns) is computed from Gray scale image. These features are combined and passed to SVM for binary classification of input face images. Method is assessed only on NUAA dataset.

A state-of-the-art CNN architecture called DeepColorFASD is proposed in [4]. Input face image is transformed into three color spaces (YCrCb, RGB, HSV) which is further provided to DeepFASD for feature extraction. The extracted features are classified by softmax which yields color space scores on which fusion based voting is applied for face-liveness detection. Method is evaluated only on CASIA-FASD dataset

The technique proposed in [5] aims to solve the problem of face spoofing by extracting color texture features. The author tries to find out which color space amongst YCrCb, RGB and HSV can well distinguish a face into true or fake classes by using color LBP features extracted from each individual channel.

Paper [6] proposes a methodology in which Rotation-Invariant Local Binary Pattern (RI-LBP) is used to extract local features whereas ResNet architecture is used to extract global features from an input face image. Applied Feature fusion technique yields final feature vector which is then provided to SVM for classifying face images as real or spoof. Proposed technique gives outstanding results for cross-database evaluation.

Input RGB face image is transformed into YCrCb and LUV to extract LBP features and into HSV to extract CM (Color Moment) features in [7]. The extracted features are cascaded and passed to SVM for classification. Proposed method is simple and efficient in terms of computation.

To eliminate irrelevant components, the input image is transformed into guided scale space in [8]. Then Guided Scale Based Local Binary Pattern (GS-LBP) and Local Guided Binary Pattern (LGBP) descriptors are used to extract texture features which are then concatenated and classified using SVM. Unnecessary noise is minimized by using GS-LBP.

Author in [9] uses chromatic co-occurrence of local binary pattern (CCoLBP) and ensemble learning (EL) to improve existing face presentation attack detection (FPAD) methods. CCoLBP features are extracted from an input face image, used to detect chromatic discrepancies between bona fide faces and artifacts. Finally these features are used for binary classification by implementing ensemble learning technique.

A new approach to handle face spoofing attacks that combines image distortions as well as image quality features with color-texture features has been proposed in [10]. The author performs RGB to HSV color space conversion to extract features. LBP is used to extract color-texture features. The Multiclass SVM algorithm classifies the face image as real or spoofed and also detects the type of presentation attack. The authors have used their self-created datasets for evaluation.

CNN architecture called ResNet-18 is used in [11] which outputs class probabilities based on Temporal, Color-based and Patch-based features. These class probabilities are fed to SVM for detecting face spoofing. Use of three color spaces (RGB, HSV and YCrCb) and pre-trained CNN makes the method more robust.

There are many methods proposed in literature for Face liveness detection. Most of these use computationally complex features, stressing need of simple features getting explored. The paper here explores simplified features. Most of the existing methods are experimented using single machine learning classifier, here paper attempts more algorithms. Most of the proposed methods are validated using single dataset, the paper attempts performance validation over two benchmark datasets.

III. Proposed Method

Different color spaces do represent the face image luminance and chromaticity in different way, these compiled as histogram can be used to classify the face image as genuine (live) or fake (spoofed one). Hence, the combination of features across color spaces can be used to extract useful information needed for detecting live faces. The proposed method emphasizes on the available distribution of color pixel values over color channels of respective color space in the face image.

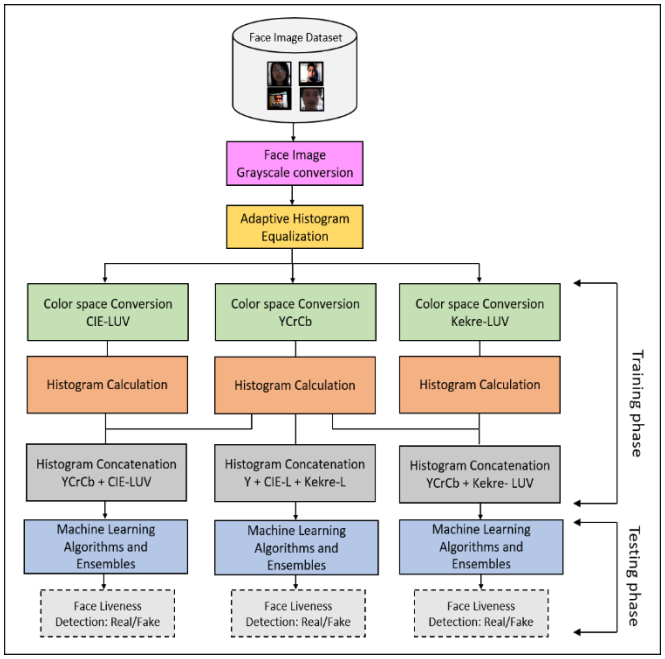

Figure 1. Block diagram of proposed Improved image based Face Spoofing Detection technique comprising of steps with color space conversion followed by histogram calculation and histogram concatenation for feature extraction and training-testing of machine learning algorithm or ensemble

A. Training phase

During the training phase, Input RGB face image is converted into Grayscale then Adaptive Histogram Equalization is applied. Further, the contrast enhanced gray image is passed through HaarCascade classifier for detecting the face region.

The extracted RGB face image is converted into three different color spaces namely YCrCb [12], CIE-LUV [13] and Kekre-LUV [14, 16] to extract global features.

B. Feature Extraction

Three feature vectors are extracted from different combinations of YCrCb, CIE-LUV and Kekre-LUV color planes. The first feature vector is formed by concatenating histograms of all planes of YCrCb and CIE-LUV color spaces having dimensions of 1536. By combining the histograms of Y, CIE-L, and Kekre-L planes, the second feature vector is created of size 768. For the third feature vector of size 1536, histograms of all planes of YCrCb and Kekre-LUV are fused. Further, each feature vector is provided for training to machine learning algorithms and considered ensembles.

C. Testing Phase

In the testing phase, trained classifiers are used to classify input face image as real or fake. The machine learning algorithms like 'ExtraTree', 'RandomForest' and ensembles as 'ExtraTree + RandomForest + NaiveBayes', 'ExtraTree + RandomForest + RandomTree', 'ExtraTree + RandomForest + SimpleLogistic'.

IV. Experimentation Environment

The proposed method and variations are experimented using two standard datasets as NUAA [17] and Replay-Attack [18].

Figure 2. Photos in Column 1 and 2 consists of Real face images and of Columns 3 and 4 consists of Fake face images spoofed by various means (NUAA dataset examples)

The NUAA Dataset [17] is created by is Nanjing University of Aeronautics and Astronautics. Genuine and Fake faces of 15 contenders are present in the database [19] which are captured using a web camera. Size of each face image is 640 × 480 pixels. Overall dataset consists of 7509 imposter and 5105 real face images. Dataset includes appearance changes which are commonly experienced by a face recognition system such as illumination, gender and with or without spectacles. Training and testing datasets were combined to form total of 12614 face images that were used for performance evaluation of improvised method on NUAA dataset using 80-20, 10-fold cross validation and 70-30 splits.

Replay attack dataset [18] is created by IDIAP Research Institute. It mainly comprises 1300 videos of 50 contenders [20]. Frame rate of each video in the dataset is approximately 25 Hz. Dataset is segregated into 4 sections: training (60 real and 300 attack), development (60 real and 300 attack), testing (80 real and 400 attack), enrollment (100 real) videos. Adverse and Controlled are the two lighting conditions considered while filming the videos. Videos of train, test and development set were combined to acquire total 200 real videos and 1000 fake videos.

Figure 3. Photos in the first row are captured in Adverse Scenario whereas photos in second row are captured in Controlled Scenario. Column 1 in Figure 3 represents LCD Photo Attack, Column 1 in Figure 3 represents HD Photo Attack, and Column 1 in Figure 3 represents Print Photo Attack (Replay-Attack dataset examples)

Further, 10 images were extracted from the first 10 seconds (1 image per second) of each 200 real videos to get 2000 (10 * 200) real face images. Similarly, 2 images were extracted from first two seconds (1 image per second) of each fake video to obtain total 2000 (2 * 1000) fake face images. Henceforth, the dataset of 4000 face images is used to evaluate the improvised method using 80-20, 10-fold cross validation and 70-30 splits.

The performance qualification is done using face liveness detection accuracy and HTER. Let 'Tn', 'Tp', 'Fp' and 'Fn' be respectively 'Number of Fake Faces predicted as Fake', 'Number of Real Faces predicted as Real', 'Number of Fake Faces predicted as Real' and 'Number of Real faces predicted as Fake'. Here equations 1, 2, 3 and 4 respectively shows false acceptance ration (FAR), false rejection ratio (FF), HTER and face liveness detection accuracy.

$$FAR = \frac{Fp}{Tn + Fp} \tag{1}$$

$$FRR = \frac{Fn}{Tp + Fn} \tag{2}$$

$$HTER\ (\%) = \frac{FAR + FRR}{2} * 100 \tag{3}$$

$$Face\ Liveness\ Detection\ Accuracy\ (\%) = \frac{Tn + Tp}{Tn + Fp + Tp + Fn} * 100 \tag{4}$$

V. Results and Discussion

The proposed face liveness detection method is experimented on Replay-Attack dataset [20] and NUAA dataset [19] using two machine learning algorithms and three ensemble combinations. Global color features are extracted using concatenated histograms from input face image by considering three color space combinations 'YCrCb + CIE-LUV', 'YCrCb + Kekre-LUV' and 'Y + CIE-L + Kekre-L'. These features are used to classify the access attempt as real face or fake spoofed face.

Figure 4 demonstrates percentage accuracy for YCrCb + CIE-LUV color space combination across considered machine learning algorithms and ensembles for replay attack database, the proposed face spoofing detection method. As per results, RandomForest has outperformed among the considered algorithms and ensembles while second best percentage accuracy is obtained from the ensemble "ExtraTree + RandomForest + RandomTree". Table 1 verifies that RandomForest outputs a minimum average HTER of

0.017.

Figure 5 comprises performance based on accuracy for YCrCb + Kekre-LUV color space across considered machine learning algorithms and ensembles for Replay-Attack database. According to computed results, RandomForest indicates highest percentage accuracy across considered combinations of machine learning algorithms. Minimum average HTER of 0.033 is obtained for RandomForest classifier as per Table.2.

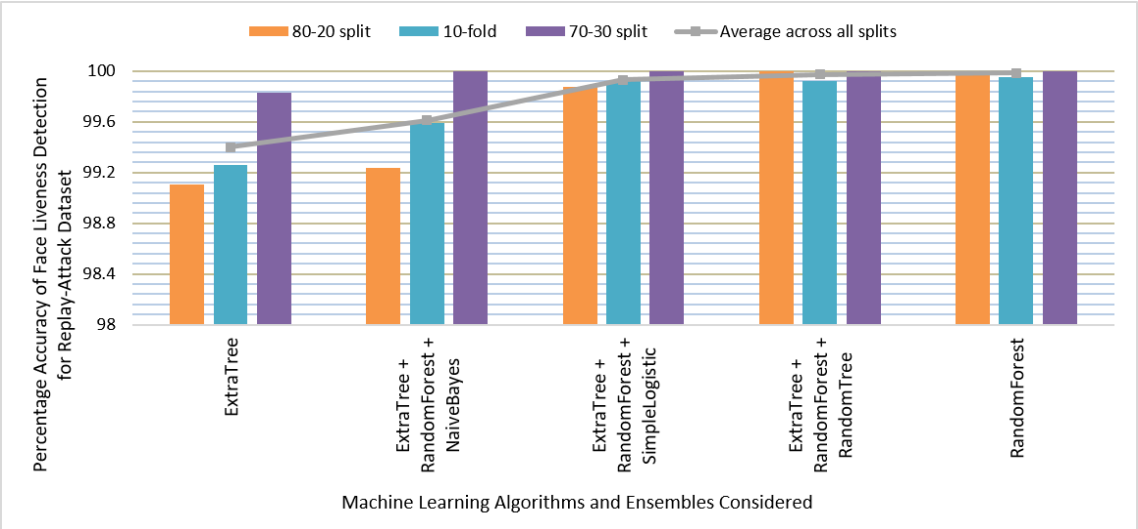

Figure 4. Percentage accuracy for YCrCb + CIE-LUV color space combination across considered machine learning algorithms and ensembles explored on Replay-Attack Dataset

Machine Learning Algorithms and Ensembles	80-20 split	10-fold	70-30 split	Average across all splits
ExtraTree	0.93	0.74	0.17	0.613
ExtraTree + RandomForest + NaiveBayes	0.8	0.41	0	0.403
ExtraTree + RandomForest + SimpleLogistic	0.14	0.08	0	0.073
ExtraTree + RandomForest + RandomTree	0	0.08	0	0.027
RandomForest	0	0.05	0	0.017

Table 1. HTER (%) for YCrCb + CIE-LUV color space combination across considered machine learning algorithms and ensembles explored on Replay Attack Dataset.

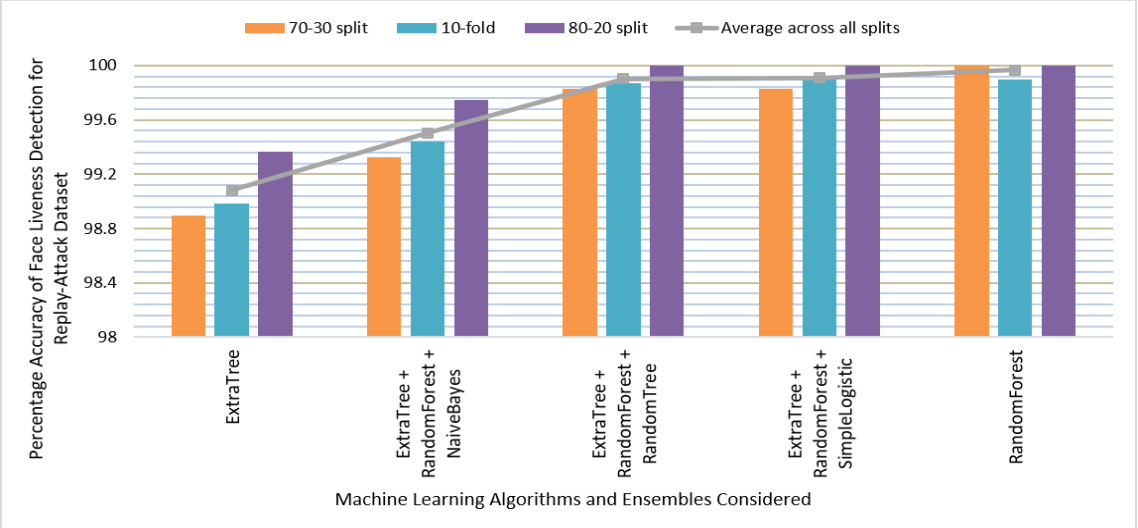

Figure 5. Percentage accuracy for Y + CIE-L + Kekre-L color space combination across considered machine learning algorithms and ensembles explored on Replay Attack Dataset

As per Figure 6, for the concatenated features of 'Y+CIE-L+Kekre- L' in proposed face spoofing detection method, the ensemble of "ExtraTree + RandomForest + SimpleLogistic" performs best as compared to considered individual machine learning algorithms and ensembles. Same combination gives minimum average HTER as per Table 3.

Machine Learning Algorithms and Ensembles	70-30 split	10-fold	80-20 split	Average across all splits
ExtraTree	1.11	1.01	0.66	0.927
ExtraTree + RandomForest + NaiveBayes	0.64	0.56	0.28	0.493
ExtraTree + RandomForest + RandomTree	0.18	0.13	0	0.103
ExtraTree + RandomForest + SimpleLogistic	0.18	0.1	0	0.093
RandomForest	0	0.1	0	0.033

Table 2. HTER (%) for YCrCb + Kekre-LUV color space combination across considered machine learning algorithms and ensembles explored on Replay-Attack Dataset.

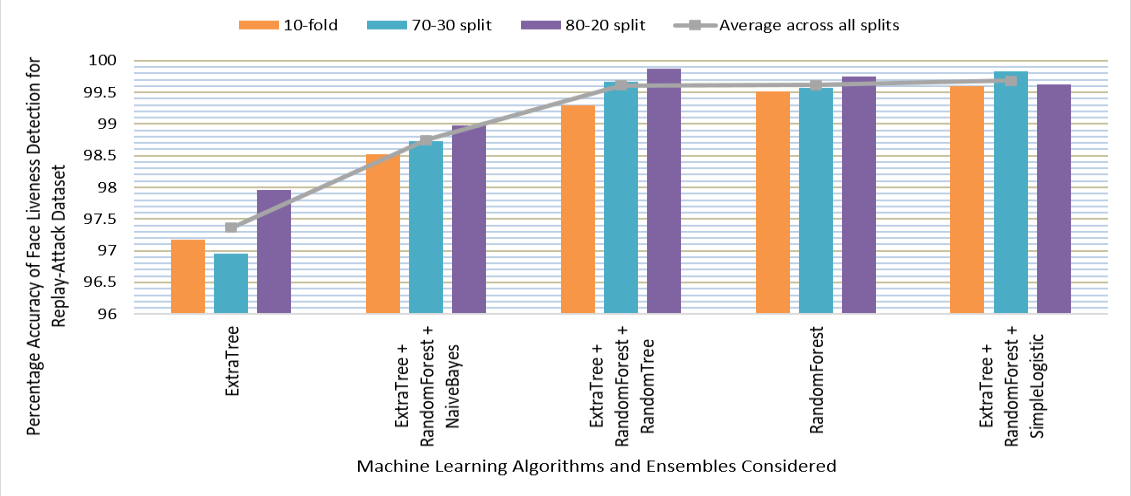

Figure 6. Percentage accuracy for Y + CIE-L + Kekre-L color space combination across considered machine learning algorithms and ensembles explored on Replay Attack Dataset

Machine Learning Algorithms and Ensembles	10-fold	70-30 split	80-20 split	Average across all splits
ExtraTree	2.86	3.06	2.07	2.663
ExtraTree + RandomForest + NaiveBayes	1.46	1.29	1.06	1.27
ExtraTree + RandomForest + RandomTree	0.71	0.35	0.12	0.393
RandomForest	0.48	0.44	0.26	0.39
ExtraTree + RandomForest + SimpleLogistic	0.41	0.17	0.4	0.327

Table 3. HTER (%) for Y + CIE-L + Kekre-L color space combination across considered machine learning algorithms and ensembles explored on Replay-Attack Dataset.

Color-space Combinations	ExtraTree	ExtraTree + RandomForest + NaiveBayes	ExtraTree + RandomForest + RandomTree	ExtraTree + RandomFores+ SimpleLogistic	RandomForest
YCrCb + CIE-LUV	99.401	99.61	99.975	99.932	99.983
YCrCb + Kekre-LUV	99.082	99.503	99.901	99.91	99.966
Y + CIE-L + Kekre-L	97.364	98.745	99.607	99.681	99.613
Average across color space combinations	98.616	99.286	99.828	99.841	99.854

Table 4. Accuracy (%) comparison of different classifiers for considered color space combinations explored on Replay-Attack Dataset.

Color-space Combinations	ExtraTree	ExtraTree + RandomForest + NaiveBayes	ExtraTree + RandomForest + RandomTree	ExtraTree + RandomFores + SimpleLogistic	RandomForest
YCrCb + CIE-LUV	0.613	0.403	0.027	0.073	0.017
YCrCb + Kekre-LUV	0.927	0.493	0.103	0.093	0.033
Y + CIE-L + Kekre-L	2.663	1.27	0.393	0.327	0.39
Average across color-space combinations	1.401	0.722	0.174	0.164	0.147

Table 5. HTER (%) comparison of different classifiers for considered color space combinations explored on Replay-Attack Dataset.

Each cell in table 4 shows average accuracy across different dataset splits as '10-fold', '80%-training and 20%-testing' and '70%-training and 30 %-testing' for corresponding color space combinations base features of face images. Averaging this accuracy across color space combinations gives us idea about the best performing machine learning classifier among considerations. In this case of validation with Replay-Attack dataset, it can be inferred that RandomForest performs better than other classifiers. The accuracy achieved by the RandomForest classifier is better than the ExtraTree classifier used in [1]. The HTER is summarized in table 5 for Replay attack dataset based experimentation, in a similar way as accuracy is summarized in table 4. Similar trend like table 4 is observer even in case of average HTER in table 5, where RandomForest outperforms other classifiers.

Each cell in table 6. shows the face spoofing detection accuracy averaged across different dataset splits as '10-fold', '80%-training and 20%-testing' and '70%-training and 30%-testing' for corresponding machine learning algorithms for respective color space combinatorial feature sets. The random Forest with YCrCb +CIE-LUV has shown better performance in face spoof detection over Replay Attack dataset. Here though the features of 'YCrCb + Kekre-LUV' gives slightly lesser accuracy than 'YCrCb + CIE-LUV', it is computationally more efficient. Similar conclusion is derived from the observations of HTER from table 7.

The accuracy comparison obtained from the validation of variations of proposed face spoofing detection method on NUAA dataset shown in Figure 7 depicts that, proposed use of RandomForest classifier performs best for 'YCrCb + CIE-LUV' color space based features. The similar observation of RandomForest being better in performance across all considered machine learning algorithms, is made from the HTER values obtained for NUAA dataset across variations of training testing splits as shown in table 8.

Machine Learning Algorithms and Ensembles	Y + CIE-L + Kekre-L	YCrCb + Kekre-LUV	YCrCb + CIE-LUV
ExtraTree	97.364	99.082	99.401
ExtraTree + RandomForest + NaiveBayes	98.745	99.503	99.61
ExtraTree + RandomForest + SimpleLogistic	99.81	99.91	99.932
ExtraTree + RandomForest + RandomTree	99.607	99.901	99.975
RandomForest	99.613	99.966	99.983
Average across Machine Learning Algorithms and Ensembles	99.028	99.672	99.78

Table 6. Accuracy (%) comparison of different color space combinations for considered classifiers explored on Replay-Attack Dataset.

Machine Learning Algorithms and Ensembles	Y + CIE-L + Kekre-L	YCrCb + Kekre-LUV	YCrCb + CIE-LUV
ExtraTree	2.663	0.927	0.613
ExtraTree + RandomForest + NaiveBayes	1.27	0.493	0.403
ExtraTree + RandomForest + SimpleLogistic	0.327	0.093	0.073
ExtraTree + RandomForest + RandomTree	0.393	0.103	0.027
RandomForest	0.39	0.033	0.017
Average across Machine Learning Algorithms and Ensembles	1.009	0.33	0.227

Table 7. HTER (%) comparison of different color space combinations for considered classifiers explored on Replay-Attack Dataset.

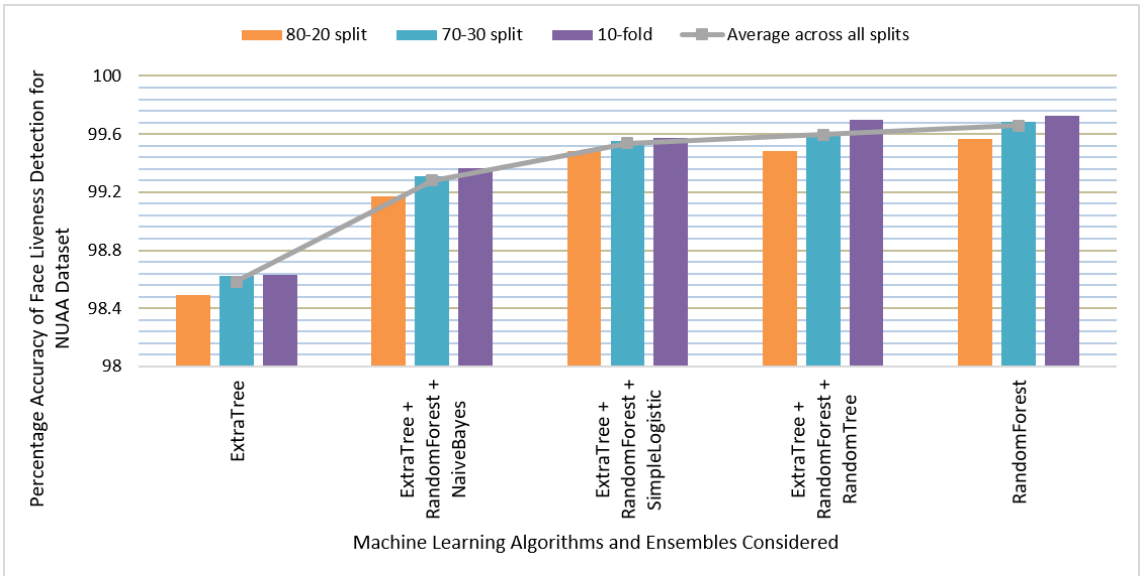

Figure 7. Percentage accuracy for YCrCb + CIE-LUV color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset

Machine Learning Algorithms and Ensembles	80-20 split	70-30 split	10-fold	Average across all splits
ExtraTree	1.57	1.46	1.44	1.49
ExtraTree + RandomForest + NaiveBayes	0.9	0.75	0.67	0.773
ExtraTree + RandomForest + SimpleLogistic	0.53	0.49	0.47	0.497
ExtraTree + RandomForest + RandomTree	0.56	0.41	0.32	0.43
RandomForest	0.47	0.32	0.3	0.363

Table 8. HTER (%) for YCrCb + CIE-LUV color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset.

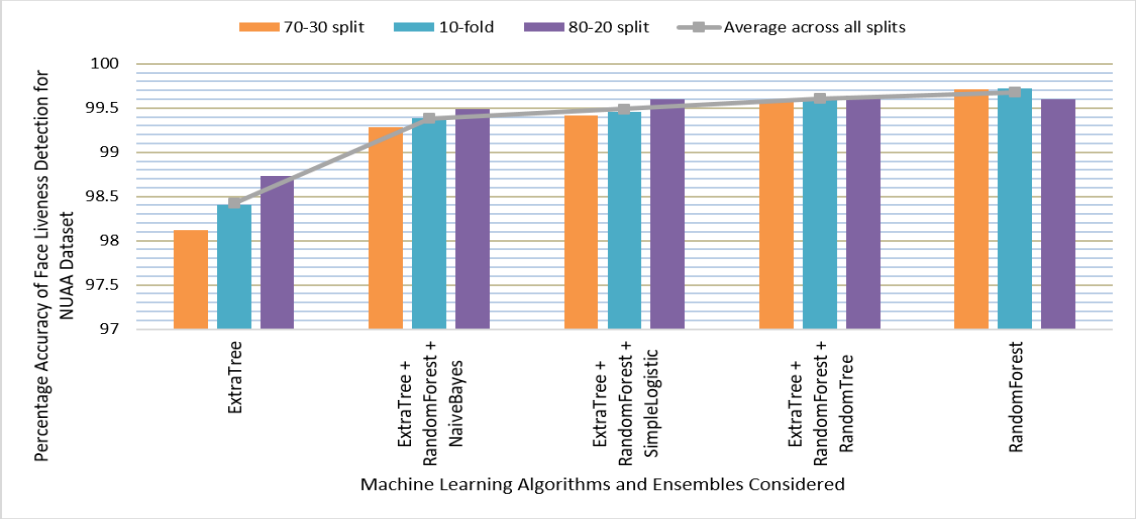

Figure 8. Percentage accuracy for YCrCb + Kekre-LUV color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset

Machine Learning Algorithms and Ensembles	70-30 split	10-fold	80-20 split	Average across all splits
ExtraTree	1.9	1.69	1.31	1.633
ExtraTree + RandomForest + NaiveBayes	0.72	0.67	0.56	0.65
ExtraTree + RandomForest + SimpleLogistic	0.6	0.58	0.43	0.537
ExtraTree + RandomForest + RandomTree	0.44	0.43	0.38	0.417
RandomForest	0.31	0.3	0.43	0.347

Table 9. HTER (%) for YCrCb + Kekre-LUV color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset.

In Figure 8, showing reflections of experimentation performed on NUAA dataset; RandomForest performs best among the considered classifiers for 'YCrCb+ Kekre-LUV' color space combination based features for face spoofing detection. Table 9 confirms the best performance given by RandomForest having a minimum average HTER of 0.347 for

the considered color feature combination in NUAA dataset.

In case of 'Y + CIE-L + Kekre-L' color space combination based features tested across various training testing splits of NUAA dataset, RandomForest is observed to have provided the best performance as compared to other machine learning algorithms and ensembles used as clearly seen in Figure 9.

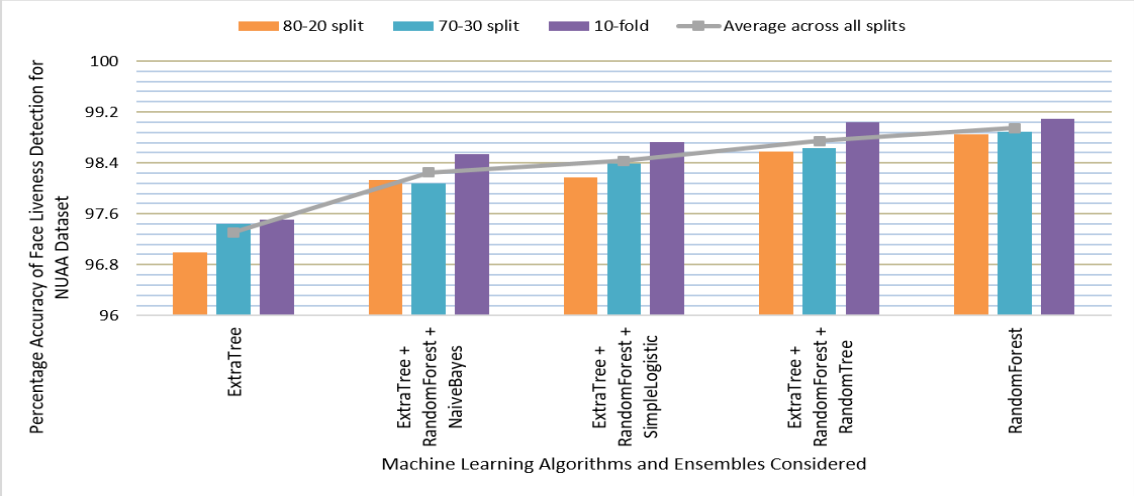

Figure 9. Percentage accuracy for Y + CIE-L + Kekre-L color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset.

Machine Learning Algorithms and Ensembles	80-20 split	70-30 split	10-fold	Average across all splits
ExtraTree	3.16	2.65	2.62	2.81
ExtraTree + RandomForest + NaiveBayes	1.96	1.97	1.54	1.823
ExtraTree + RandomForest + SimpleLogistic	1.86	1.63	1.31	1.6
ExtraTree + RandomForest + RandomTree	1.5	1.34	0.99	1.277
RandomForest	1.18	1.12	0.93	1.077

Table 10. HTER (%) for Y + CIE-L + Kekre-L color space combination across considered machine learning algorithms and ensembles explored on NUAA Dataset.

Color-space Combinations	ExtraTree	ExtraTree + RandomForest + NaiveBayes	ExtraTree + RandomForest + SimpleLogistic	ExtraTree + RandomForest + RandomTree	RandomForest
YCrCb + CIE-LUV	98.583	99.282	99.536	99.596	99.657
YCrCb + Kekre-LUV	98.421	99.385	99.492	99.608	99.679
Y + CIE-L + Kekre-L	97.309	98.247	98.43	98.747	98.946
Average across color-space combinations	98.104	98.971	99.153	99.317	99.427

Table 11. Accuracy (%) comparison of considered machine learning classifiers and ensemble for considered color space combinations explored on NUAA Dataset.

Similar better performance of RandomForest is observed in same case of experimentation using HTER values shown in Table 10.

In table 11, each cell shows average accuracy of face spoofing detection across different NUAA dataset splits such as '10-fold', '70%-training and 30%-testing' and '80%-training and 20%-testing' for corresponding color space

combinations and machine learning algorithms or ensembles. Best classifier is identified by averaging the accuracies over the considered color space combinatorial features. From the observations here, it can be concluded that RandomForest outperforms other classifiers and ensembles. Same trend is observed to have been followed for HTER obtained with NUAA dataset as shown in table 12.

Color-space Combinations	ExtraTree	ExtraTree + RandomForest + NaiveBayes	ExtraTree + RandomForest +SimpleLogistic	ExtraTree + RandomForest + RandomTree	RandomForest
YCrCb + CIE-LUV	1.49	0.773	0.497	0.43	0.363
YCrCb + Kekre-LUV	1.633	0.65	0.537	0.417	0.347
Y + CIE-L + Kekre-L	2.81	1.823	1.6	1.277	1.077
Average across color-space combinations	1.978	1.082	0.878	0.708	0.596

Table 12. HTER (%) comparison of considered machine learning classifiers and ensemble for considered color space combinations explored on NUAA Dataset.

Machine Learning Algorithms and Ensembles	Y + CIE-L + Kekre-L	YCrCb + Kekre-LUV	YCrCb + CIE-LUV
ExtraTree	97.309	98.421	98.583
ExtraTree + RandomForest + NaiveBayes	98.247	99.385	99.282
ExtraTree + RandomForest + SimpleLogistic	98.43	99.492	99.536
ExtraTree + RandomForest + RandomTree	98.747	99.608	99.596
RandomForest	98.946	99.679	99.657
Average across Machine Learning Algorithms and Ensembles	98.336	99.317	99.331

Table 13. Accuracy (%) comparison of different color space combinations for considered classifiers explored on NUAA Dataset.

Machine Learning Algorithms and Ensembles	Y + CIE-L + Kekre-L	YCrCb + Kekre-LUV	YCrCb + CIE-LUV
ExtraTree	2.81	1.633	1.49
ExtraTree + RandomForest + NaiveBayes	1.823	0.65	0.773
ExtraTree + RandomForest + SimpleLogistic	1.6	0.537	0.497
ExtraTree + RandomForest + RandomTree	1.277	0.417	0.43
RandomForest	1.077	0.347	0.363
Average across Machine Learning Algorithms and Ensembles	1.717	0.717	0.711

Table 14. HTER (%) comparison of different color space combinations for considered classifiers explored on NUAA Dataset.

In table 13 each cell shows average accuracy across different splits of NUAA dataset such as '10-fold', '70%-training and 30 %-testing' and '80%-training and 20%-testing' for corresponding machine learning classifiers and color features extracted with respective combinatorial color spaces. The observation decision for best color space combination as 'YCrCb+CIE-LUV' be clearly noted from table 13. Similar conclusion can be drawn from HTER values mentioned in table 14.

In this paper, 15 different combinations of 3 color space combinatorial features and 5 classifiers or ensembles are experimented. Out of which the comparison of average HTER for top five color space combinations across considered classifiers along with existing method [1] for both datasets is

shown in table 15. From the table, it is inferred that the color space combination of YCrCb and CIE-LUV with RandomForest classifier has performed better than the existing method [1]. The existing method was experimented

Variations of proposed face spoofing detection method with Color space combinations across [machine learning models]	Replay-Attack	NUAA
YCrCb_CIE LUV + [ExtraTree]	0.59	--
YCrCb + CIE-LUV + [RandomForest]	0.017	0.363
YCrCb + CIE-LUV + [ExtraTree + RandomForest + RandomTree]	0.027	0.43
YCrCb + Kekre-LUV + [RandomForest]	0.033	0.347
YCrCb + CIE-LUV + [ExtraTree + RandomForest + SimpleLogistic]	0.073	0.497
YCrCb + Kekre-LUV + [ExtraTree + RandomForest + SimpleLogistic]	0.093	0.537

Table 15. Comparison of average HTER (%) between top 5-best performance color space combinations over considered machine learning models, ensembles and existing method [1]

Method	Replay-Attack HTER (%)
Radiometric transforms [21]	0.80
Color texture CNN + SVM [22]	0.90
LBP+DoG+HOG+IQA [23]	1.00
FASNet [24]	1.21
GIF + IQA [25]	1.31
HSV-YCbCr+C-SURF+PCA [26]	2.20
YCbCr+HSV+SVM [27]	2.90
YCrCb + CIE-LUV + [ExtraTree] [1]	0.59
YCrCb + CIE-LUV + [RandomForest]	**0.017**
YCrCb + Kekre-LUV + [RandomForest]	**0.033**

Table 16. Comparison of average HTER (%) between top 5-best performance color space combinations over considered machine learning models, ensembles and existing method [1]

using Replay attack dataset only. In proposed method variations, the validation is done on two datasets as NUAA and Replay-Attack. Table 15 shows HTER observed for both datasets in case of proposed methods.

Table 16 shows the comparison of the proposed face spoofing detection with other existing methods taken from literature. Here point to be noted is the methods available in literature have used only single dataset as replay attack dataset from the available datasets for validation. The existing methods are complex with respect to the feature extraction [1, 21, 23, 25, 26, 27] and few of the existing methods even use deep neural network architectures [22, 24] making them more computational resource dependent, than the one proposed in this paper. In spite of being relatively simple in feature extraction and having no extra computational resource requirement as that of deep network based methods, the proposed method have shown lower HTER values indicating better performance in face spoofing detection as shown in table 16. Here proposed RandomForest and 'YCrCb+CIE-LUV' combinational feature based face spoof detection is showing least HTER as 0.017, closely followed by other variant of proposed method with RandomForest and 'YCrCb+Kekre-LUV' features. The Kekre-LUV is lighter in computations for feature extraction compared to CIE-LUV; making Kekre-LUV the better choice with slightly increased HTER.

RandomForest gives better performance the ExtraTree classifier used in image based object spoofing detection technique because of following reasons: (i) Enabling boostrapping, (ii) Splitting nodes on the best split.

VI. Conclusion

In today's advanced digital age of ambient computing, most of the security is reliant on person identification using biometric traits. Spoofing the security of such systems with fake biometric identity has become a major threat. The paper discussed performance improvement in relatively simpler face spoofing detection method with variants. The paper explored the use of concatenated histograms of face image

objects created using various color spaces as 'YCrCb', 'Kekre-LUV', CIE-LUV' for face spoofing detection using machine learning algorithms and their ensembles. Experimentation conducted on two of the standard face liveness detection datasets alias 'Replay Attack' and 'NUAA' with performance measures used as accuracy of face liveness detection and half total error rate (HTER) have shown that the proposed use of RandomForest performs superior with 'YCrCb + CIE-LUV' combinatorial features; closely followed by the Random Forest with 'YCrCb+Kekre-LUV' combinational feature extraction. Kekre-LUV gets an edge over CIE-LUV due to lesser computational complexity at the cost of slight decrease in accuracy. Thus the proposed method is observed to have given improved face object spoofing detection over existing by means of higher accuracy and lower HTER values obtained over two datasets. In future, proposed method can be validated on dataset containing mask attack to access its robustness.

References

[1] Valter Costa, Armando Sousa, and Ana Reis. "Image-Based Object Spoofing Detection". 19th International Workshop on Combinatorial Image Analysis, Porto, Portugal, 2018 November 22-24.

[2] Song, Li and Ma, Hongbin. "Face Liveliness Detection Based on Texture and Color Features". Conference: 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), April pp. 418-422, 2019.

[3] Khurshid, Aasim and Cleger-Tamayo, Sergio and Fernandes, Everlândio and Ramalho, Mikhail and Teofilo, Mauro**.** "A Robust and Real-Time Face Anti-spoofing Method Based on Texture Feature Analysis". HCI International 2019 – Late Breaking Papers, pp. 484-496, 2019.

[4] K. Larbi, W. Ouarda, H. Drira, B. Ben Amor and C. Ben Amar. "DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN". 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, pp. 4011-4016, 2018.

[5] Z. Boulkenafet, J. Komulainen and A. Hadid. "Face anti-spoofing based on color texture analysis". 2015 IEEE International Conference on Image Processing (ICIP), Quebec City, QC, pp. 2636-2640, 2015.

[6] F. Chen, C. Wen, K. Xie, F. Wen, G. Sheng and X. Tang. "Face liveness detection: fusing colour texture feature and deep feature", In IET Biometrics, vol. 8, no. 6, November, pp. 369-377, 2019.

[7] J. He and J. Luo. "Face Spoofing Detection Based on Combining Different Color Space Models". 2019 IEEE 4th International Conference on Image, Vision and Computing (ICIVC), Xiamen, China, pp. 523-528, 2019.

[8] Peng, F., Qin, L. and Long, M. "Face presentation attack detection using guided scale texture". Multimed Tools Appl **77,** pp.8883–8909, 2018.

[9] Peng, Fei and Qin, Le and Min, Long. "Face Presentation Attack Detection Based on Chromatic Co-occurrence of Local Binary Pattern and Ensemble Learning", Journal of Visual Communication and Image Representation, vol no. 66, December pp. 102746, 2019.

[10] Boulkenafet, Zinelabidine and Komulainen, Jukka and Hadid, Abdenour. "Face Spoofing Detection Using Colour Texture Analysis", IEEE Transactions on Information Forensics and Security, vol no. 11, August, pp. 1-1, 2019.

[11] Tang, Yan and Wang, Xing and Jia, Xi and Shen, Linlin. "Fusing Multiple Deep Features for Face Anti-spoofing". 3th Chinese Conference, CCBR 2018, Urumqi, China,August pp. 321- 330, 2018.

[12] F.W., Billmeyer. Color Science: Concepts and Methods, Quantitative Data and Formulae, 2nd ed., by Gunter Wyszecki and W. S. Stiles, John Wiley and Sons, New York, 1982.

[13] ITU: ITU-R Recommendation BT.601-5. "Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios". Technical report, ITU, Geneva, Switzerland, 1995.

[14] Thepade, S.D. Patil, P.H., "Novel video keyframe extraction using KPE vector quantization with assorted similarity measures in RGB and LUV color spaces", International Conference on Industrial Instrumentation and Control, ICIC 2015, 2015, pp. 1603-1607.

[15] H.B. Kekre and S.D. Thepade. "Improving Color to Gray and Back' using Kekre- luv color space". In 2009 IEEE International Advance Computing Conference, March, pp. 1218-1223, 2009.

[16] H.B. Kekre and S.D. Thepade. "Color Traits Transfer to Grayscale Images". In 2008 First International Conference on Emerging Trends in Engineering and Technology, July, pp. 82-85, 2008.

[17] X.Tan, Y.Li, J.Liu and L.Jiang. "Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model". 11th European Conference on Computer Vision (ECCV'10), Crete, Greece, September 2010 5-11, 2010.

[18] Ivana Chingovska, Andre Anjos and Sebastien Marcel. "On the Effectiveness of Local Binary Patterns in Face Anti-spoofing". Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), January, Darmstadt, pp. 1-7, 2012.

[19] NUAA dataset available at website http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html (last referred on 10 April 2020).

[20] Replay Attack dataset available at website-https://www.idiap.ch/dataset/replayattack (last referred on 10 April 2020).

[21] Edmunds, T., Caplier, A. "Face spoofing detection based on colour distortions", IET Biometrics, Vol no. 7**,** pp. 27–38, 2018.

[22] Zhao, X., Lin, Y., Heikkila, J. "Dynamic texture recognition using volume local binary count patterns with an application to 2D face spoofing detection", IEEE Trans. Multimed. Vol no. 20(3)**,** pp. 552–566, 2018.

[23] Farmanbar, M., Toygar, O. Spoof detection on face and palmprint biometrics, Signal Image Video Process. Vol no. 7, pp. 1253-1260, 2017.

[24] Karray, F., Campilho, A., Cheriet, F. (eds.). "Image Analysis and Recognition", LNCS, vol. 10317. Springer, Cham 2017.

[25] Peng, F., Qin, L., Long, M, "POSTER: non-intrusive face spoofing detection basedon guided filtering and image quality analysis",In: Deng, R., Weng, J., Ren, K., Yeg-neswaran, V. (eds.) SecureComm(2016). LNICST, vol. 198, pp. 774–777. Springer.Cham, 2017.

[26] Boulkenafet, Z., Komulainen, J., Hadid, A.. "Face anti-spoofing using speeded-uprobust features and fisher vector encoding". IEEE Signal Process. Lett. 1, 2016.
[27] Li, L., Correia, P.L., Hadid, A.. "Face recognition under spoofing attacks: countermeasures and research directions", IET Biom. 7(1), 3–14, 2018.

Author Biographies

Dr.Sudeep D. Thepade is currently Professor in Computer Engineering Department at Pimpri Chinchwad College of Engineering affiliated to Savitribai Phule Pune University, Pune, Maharashtra, India. He has completed Ph.D. in 2011. He has more than 370 research papers to his credit published in International/ National Conferences and Journals. His domain of interest is Image Processing, Image Retrieval, Video Analysis, Video Visual Data Summarization, Biometrics and Biometric Liveness Detection. He is member of International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT). He has served as Technical Program Committee member and Reviewer for Several International Conferences and Journals.

Piyush Rajendra Chaudhari is currently pursuing Bachelor of Engineering in Computer Engineering field from Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune. His research interest are Image Processing, Machine Learning. He is an avid open-source contributor, contributed to various open source organizations.

Mayuresh Rajesh Dindorkar receiving his Bachelor of Engineering (B.E) degree in Computer Engineering from Savitribai Phule Pune University (SPPU), Maharashtra, India. His research areas are Image Processing, Machine Learning and Deep Learning.

Shalakha Vijaykumar Bang is currently pursuing her B.E in Computer Engineering Department from Pimpri Chinchwad College of Engineering, SPPU, Pune, India. Her areas of Interest are Data Science and Analytics, Deep Learning, Image processing, Automation and MATLAB Simulations.

Rohit Balasaheb Bangar has completed diploma in Computer Engineering and currently studying in B.E Computer Engineering stream at Pimpri Chinchwad College of Engineering, Nigdi, Pune. His areas of interest is Image Processing and Machine Learning.