International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-6, Issue-7, July 2020
ISSN: 2395-3470
www.ijseas.com

FACE TAMPERING DETECTION USING GRADIENT FEATURES

[1]Shabreen Fathima T,[2]Shenbaga Priyanka M,[3]ShanmugiB,[4]Parisa Beham M and [5]Tamilselvi R

[1,2,3] UG students, [4,5]Professor, Department of ECE

Sethu Institute of Technology, Virudhunagar, Tamilnadu, India
shabreenfathima77@gmail.com, priyankaaa288@gmail.com, bshan03031999@gmail.com

Abstract **–Face authentication method, currently is emerging in biometrics, but still now it is not considered as most secure authentication, when compared to all other biometric system. Face detection is most exposed to vulnerability and can be easily hacked through various techniques like masking, recording even through photos, by any means of these, hackers can gain access unauthorised data. Motivated by these issues, in this paper, a new method of face tampering detection using gradient features is proposed. Inspired by the success of Histogram of Oriented Gradient (HOG)algorithm, here from the tampered face, the gradient features are extracted followed by image pre processing using difference of Gaussian (DoG) method. Experimentation has been done with all kind of face tampering attacks given in CASIA, NUAA, Kaggle and Rose-Yutu datasets. Sparse Representation Classifier (SRC) is employed to classify the test image as real or tampered image. Our proposed method yields better classification accuracy than the benchmark methods in the literature.**

Keywords: Face Tampering detection – DoG preprocessing- HOG feature – SRC classifier - accuracy.

1. INTRODUCTION

In authentication methods the most innovative authentication is a face recognition, but still not deployed at where security is the top most priority. Face authentication available in mobile phones also, yet still it can be unlocked with photographs, video, or 3D masks [7] of person , thus it makes unsecured authentication. Due to these risks, the face authentication can be compromised by fraudster using some techniques. The act of using an artifact for fooling a biometric system is spoofing [4]. To overcome this situation face tampering detection techniques has been proposed earlier, but still efficient technique with a high accuracy is unavailable which still makes the face recognition insecure. The masquerade technique [13] use for spoofing is classified into two type namely 2D and 3D attacks. In the fig. 1, real and fake faces include eye cut attack, video attack, warped attack, photo attack and mask attack are shown. The 2D attack includes eye cut attack, video attack, warped attack and photo attack are shown in figure 1 of CASIA-FASD dataset and 3D attack include mask attack is shown in figure 1 of Kaggle dataset. There are many techniques for face spoofing detection. In existing paper [18], face tampering detection is not suitable for the video attack and mask attack, and it also requires only one input.

(a) Real face **(b)**Eye cut attack **(c)**Video attack

(d) Warped attack **(e)**Photo attack **(f)** Mask attack

Fig. 1 Different types of spoofing attacks

The system works to verify that the challenge occurred during a video sequence using the challenging dataset, and producing high accurate output values. It also relies system on a series of challenges to validate an individual's identity. Face tampering detection guard the system [11] against the attack, and the fraudulent user will not be able to access the system. So this proposed model can detect the video attack and mask attack and also, it uses a sequence of input to attain high accuracy.

The objective of this paper is accuracy of the true face is determined by machine learning techniques, a Histogram of Oriented Gradient (HOG) feature extraction, Sparse Representation Classifier, and it determines the classification accuracy. This paper is also focused on reducing the time consumption. The main contribution of this paper is it achieved the high accuracy comparing to the existing papers.

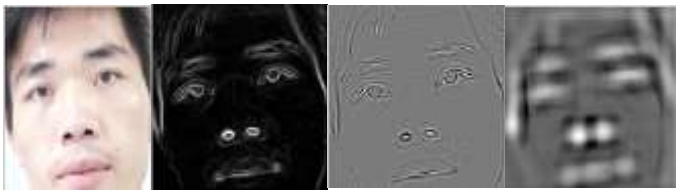
This paper is organized as follows. Section 2, briefly reviews the related works and recent spoofing detection methods. In section 3, we present our basic counter measures of calculating Gmag, LOG and DoG. Section 4, details our proposed methodology of preprocessing, feature extraction and classifier. Section 5, presents the face spoofing dataset. Section 6 analyses our experimental results, and finally, we conclude in section 7.

2. RELATED WORKS

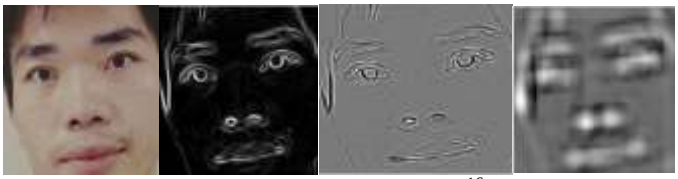
Face recognition has become important in our everyday life then security issues of face recognition also increasing prominent. Therefore, face tampering detection has become a crucial part for reliable authentication systems. Common face liveness detection based on texture [18, 10, 3, 19] gradient, different sensors, eye blinking detection [15], Infrared Radiation [15], heartbeat [16], pupil tracking [9], image quality [2] and deep learning [3, 17, 8, 17]. Live faces have complex 3D structures, while photo and video attacks have 2D planar structures. Detection method on texture mainly used Local Binary Pattern (LBP) [18, 10, 3, 19] as a feature extraction. Accuracy will have decreased when the image quality is poor [15]. Jie Zhou et al. [7]., discussed the accuracy of the face recognition system is increased by using DMF face anti spoofing technique and then a replacement blink detection method is employed to eliminate 3D print head spoofing. Shuhua Liu et al [15], discussed the proposed liveness detection method based on infrared radiation (IR) images can deal with face spoofs. Face pictures were acquired by a Kinect camera and converted into IR images and have feature extraction and classification. It's administered by a deep neural network to differentiate between real individuals and face spoofs. Yousef Atoum et al. [17], discussed the face spoofing detection using patch and depth based Convolutional Neural Network(CNN). Sandeep Kumar et al. [13], discussed there's a requirement to supply more generalized algorithms for detection of unpredictable spoofing attacks to make the system more secure, computationally efficient and reliability**.** Junying Gan et al. [8], discussed rather than extracting features from a single image, features are learned from a video frames and it realizes face anti-spoofing, the spatio-temporal features of continuous video frames are extracted using 3D convolution neural network (CNN) from the short video frame level. Navneet Dalal et al. [12], discussed HOG descriptors significantly outperform existing feature sets for human detection and study the influence of every stage of the computation on performance, high quality local contrast normalization in overlapping descriptor blocks are all necessary for good results**.** Therefore, we are using this new approach of Histogram of Oriented Gradient [12] as our feature extraction.

3. BASIC COUNTER MEASURE

Face analyzing between real and fake image is complicated by machine, but it can be achieved by using counter measures and algorithms. The counter measures include Gradient magnitude (Gmag), Laplace of Gaussian (LOG), Difference of Gradient (DoG) for real and fake images are calculated. In this fig.2, The Gmag, LOG and DoG are calculated and there output are shown. The live image and fake images are varying in a high discrimination value.



Live image Gmag=56.816 LOG=3.48e^{-16} DoG=0.0859



Warped attack Gmag=39.948 LOG=5.86e^{-16} DoG=0.0486

Eye cut attack Gmag=40.891 LOG=6.33e^{-16} DoG=0.0573

Fig. 2 Basic counter measure of CASIA-FASD dataset.

Table 1 Output of CASIA-FASD dataset with calculating Gmag value

Image Type	Gmag	LOG	DoG [10]
Live image	56.6181	3.485e^-16	0.1025
High eye cut attack	42.8637	1.5687e^-15	0.0642
High video attack	43.3822	1.768e^-15	0.0778
High warped attack	39.9482	5.8634e^-16	0.0486
Low eye cut attack	40.8910	6.3371e^-16	0.0573
Low video attack	43.3822	1.7681e^-16	0.0778
Low warped attack	39.8772	5.6724e^-16	0.0445

From table 1 and table 2, when we are calculating the value of Gradient magnitude before calculating the value of LOG and DoG, the results of LOG and DoG will vary with a high discrimination difference between live and fake images. Therefore, we are calculating a Gradient magnitude before calculating LOG and DoG value.

Table 2 Output of Kaggle dataset with calculating Gmag value

Image type	Gmag	LOG	DoG [10]
Live image	67.6529	1.3623e^-15	0.0766
Live image	95.5393	1.1015e^-15	0.0660
Live image	81.0651	1.0148e^-16	0.1019
Live image	67.0985	1.5933e^-15	0.0163
Fake image	91.552	3.8554e^-16	0.0483
Fake image	56.8048	3.4702e^-15	0.0553
Fake image	90.7539	6.7654e^-17	0.0572
Fake image	96.9875	4.8763e^-16	0.0432

4. PROPOSED METHODOLOGY

Spoofing with fake face is a major threat in a face detection where the real and fake look similar to each other, and thus hard to distinguish by machine. But there are some parameters that a fake image won't have as the real images such as motion [18, 10, 3], texture [18, 10, 3], distortion based methods [3], gradients, frequency, reflection, refraction of light with human skin and other optical qualities of the real human faces. By analyzing the particular texture and gradient of images spoofing can be easily detected. In the fig 3, it shows the overflow of software implementation of the face tampering detection project. The face will be captured when the person stood in front of the camera. The images are then processed with HOG algorithm for feature extraction and then SRC classifier is used for classifying the face pattern and at last, the captured image is matched with the previous database to check whether it is authenticated person or not. Now with help of classifier it is able to determine whether the test image is a real or fake image.

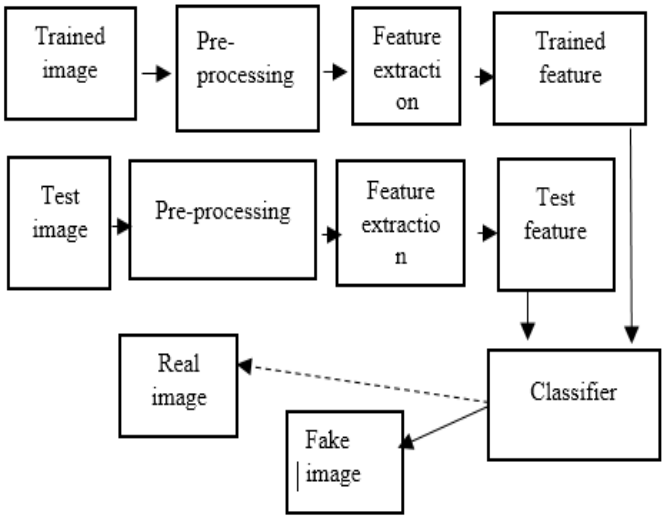


Fig. 3 Overall block diagram of the proposed method.

4.1 Pre-Processing

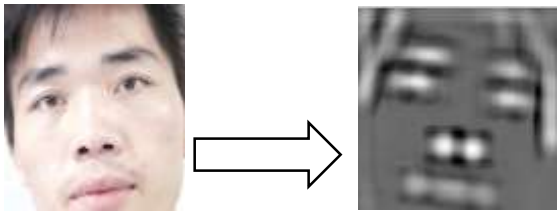
The Pre-processing involves four steps. They are

- RGB2gray conversion
- Resizing Image
- Difference of Gradient
- Histogram equalization

In RGB to gray conversion the image is converted into a gray scale by removing the hue and saturation of the image. Thus image will contain no color which is used to extract the gradients . Then image captured must be resized to proceed further process, thus the image transformed geometrically by the MATLAB function imresize. This function points out each pixel and do a point transformation with corresponding point in output images. In this project, the final size of the image will be 80×80.

4.2 Difference of Gradient (DoG)

Difference of Gradient [16] is a feature enhancement algorithm. In this where two images are taken, an original one and a blurred version of the original image, the algorithm involves in subtraction of both the images to get the blurred images a convolving process carried out with original scale images with Gaussian kernel having different standard deviations. In the fig 4, the live image is converted into gray scale image, and then it is resized and then the pre-processing of DoG [10] will be performed.



Live image DoG image

Fig .4 Difference of Gradient image

Histogram equalization is a contrast adjustment of the image histogram. It enhances the image with no loss in information. It increases the global contrast when usable data has contrast values and intensities are distributed better on the histogram, lower local contrast areas can gain higher contrast and also effectively spread out frequent intensity values. Even though background or foreground is light or dark it is still applicable effectively. Values of the color map index image or value in an intensity image is transformed for enhancement.

4.3 Feature Extraction

Feature extraction is a reduction process where it represents the important feature of the image as a compact one by reducing the useless features from the images. Reducing image as a compact feature is required to reduce time of process such as matching image and retrieval.

4.3.1 HOG Algorithm:

The Histogram of Oriented Gradients [12] is a descriptor of feature of the images to the machine. This algorithm is excellent in analyzing the human face in images and videos. HOGs are rotationally invariant descriptors of features of the images [4] especially used in optimization problems and it is robust [5]. HOG is likely Edge Orientations and scale-invariant feature transform descriptors, but HOG differs in computation on a dense grid of space cells, and also uses overlapping local contrast normalization for improved accuracy. It divides the images into 4 × 4 block cells which have 8 × 8pixels. Fixed number of gradient oriented bins are owned by each cells. The pixel's votes are bilinear interpolated to reduce aliasing. The interpolation may positions or orientation and thus, HoG[5] are obtained.

4.3.2 Process of calculating HOG

The Gradients are a small change that occurs in x and y directions. Further process is to calculate gradient of each pixel. The matrix shown in fig 5 is used as an example and these pixel values are used for the given patch. The pixel value of 85 is highlighted. Now, to determine the gradient in the x-direction, we need to subtract the value on the left from the pixel value on the right.

121	10	78	96	125
48	152	68	125	111
145	78	85	89	65
154	214	56	200	66
214	87	45	102	45

Fig. 5 HOG Descriptor

Similarly, we will subtract the pixel value below from the pixel value above the selected pixel, and then the gradient through y-axis will be calculated. Now it gives two new matrices, which stores the gradient in x and y directions respectively. Using this process, the remaining pixel values are calculated.

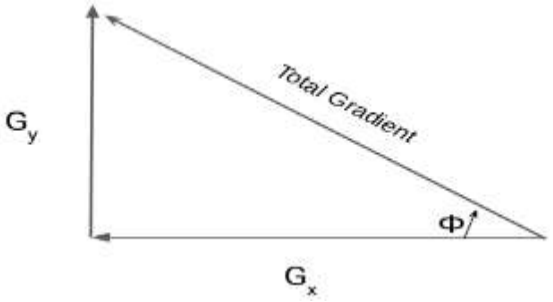


Fig. 6 Magnitude and Orientation calculation

Then we determine magnitude and direction for each pixel value using the calculated gradient. For this step, we will be using the Pythagoras theorem and the base and perpendicular is used as a gradient in fig 6.

Total Gradient Magnitude

$$= \sqrt{[(Gx)2 + (Gy)2]} \quad (1)$$

Next, calculate the Orientation for the same pixel. We know that we can write the tan for the angles:

$$tan(\emptyset) = Gy/Gx \quad (2)$$

Hence, the value of the angle would be

$$\emptyset = a\ tan(Gy/Gx) \quad (3)$$

Now, for every pixel value, we have the total gradient (magnitude) and the orientation (direction).

Live image Gx of input image Gy of input image

Photo attack Gx of input image Gy of input image

Fig. 8 Output of Gx and Gy of live and fake image

Table 3 Gx and Gy values of CASIA-FASD dataset

Image type	Gx	Gy
Live image	1.6567	7.3086
Live image	1.5288	6.9798
Live image	1.6602	7.4922
Live image	1.8203	7.5576
Live image	1.5708	7.6196
Low eye cut attack	5.4844	4.3896
Low warped attack	2.6074	5.1006
Low video attack	9.3013	5.7021
High video attack	3.1577	4.0576
Normal video attack	10.547	6.4875

From equation (1), (2) and (3) for calculating the value of total Gradient magnitude, tan for the angle ($\tan(\varphi)$) and value of the angle (φ). We need the value of Gx, Gy and calculate it. The output image of Gx and Gy are shown in fig.8. In this way, we calculated the total gradient and the orientation.

4.4 Classifier

The Classifier is used to distinguish between the real and the fake image. The classifier has three phases, the first is training phase where the real image is processed in training instances and classification of algorithm is used to find the relationships between predictors and targets objects in an image. Next is testing phase, here a test sample class labels are known but it neglected in the training model. The third phase is the usage phase where it uses the classification of new model which class labels are unknown.

4.4.1 Sparse Representation Classifier(SRC)

In this proposed model Sparse Representation classifier [1] is used. It is popularly known for various task classification, and robust face detection. The matrix regularization is processed predominantly using optimization algorithms. It has achieved better performance and became more efficient [6]. SRC is also effective in classifying data with corrupted by noise and occlusion. In the context of the current work, a descriptor derived from a test sequence is approximated as a sparse linear combination of all training samples. SRC modifies k-NN classifier and have relationship between different training samples and provides high accuracy. Therefore, we are using this classifier. This is represented as

$$\hat{a} = \arg_{\alpha} min \|\alpha\|_p s.t. \|y - X\alpha\|_2^2 \leq \epsilon \quad (4)$$

From eqn(4), X refers the set of training samples, y refers the probe sample, α refers the sparse coefficients vector and ϵ refers a small threshold. Depending on ρ, different algorithms [14] have been proposed

5. DATABASE COLLECTION

The proposed face liveness detection system was evaluated using four databases are CASIA-FASD dataset [15], Kaggle dataset, NUAA dataset [10] and ROSE Youtu dataset [3].

5.1 CASIA Face Anti-Spoofing Dataset

In CASIA-FASD dataset [15], images are available in high,normal and low resolution. In fig 9 , the spoofed images of eye cut attack [13], video attack and warped attack are shown. In eye cut attack, attackers cut eye regions from picture and exhibits blinking behaviour manually. Then, in video attack attacker uses a short video/GIF of the owner and loops it on a screen.

Fig. 9 Samples of eye cut attack **(top row),** video attack **(middle row)** and warped attack **(bottom row)**

5.2 Kaggle Dataset

In Kaggle dataset, fake images include mask attack, and it is spoofed by using an extra layer. This attack is more sophisticated attack than playing a face video. In fig.10, the live images and mask attack are shown.

Fig. 10 Samples of live images **(top row)** and mask attack (**bottom row)** in Kaggle dataset**.**

5.3 NUAA Photograph Imposter Dataset

NUAA Dataset [10] used the webcams to capture a series of face images. During image capturing, each subject was asked to look at the webcam frontally and with neutral expression and no apparent movements such as eye blink or head movement. They captured the images of both live subjects and their photographs are shown in fig. 11.

Fig. 11 Samples of live images **(top row)** and photo attack images **(bottom row)** of NUAA dataset.

5.4 ROSE-Youtu Dataset

ROSE-Youtu Face Liveness Detection Dataset [3], covers a large variety of illumination conditions, camera models, and attack types. It consists of 4225 videos with 25 subjects in total. They consider three spoofing attack types including printed paper attack, video replay attack, and masking attack. The live and spoofed image are shown in fig 12.

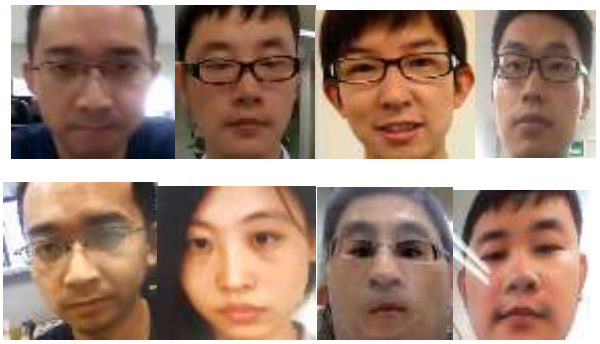


Fig. 12 Samples of live images **(top row)** and fake images (**bottom row)** of ROSE Youtu dataset

6. EXPERIMENTAL RESULTS

The performance of proposed algorithm showed a powerful identification rate on the dataset.Firstly, read the image from the database. Then Performing the pre-processing steps for the images such as resizing the image and converting the images from RGB to gray. Then performing the pre-processing process on gray image such as DoG and histogram equalization. Divide the database into training and testing sets. HOG feature undergoes matching with face pattern which are already stored with the details. SRC classifier is used to classify live and fake images. Compute the result in accuracy (in percentage) and its time consumption (in seconds). Finally, confusion matrix is determined.

6.1 Training and Testing Phase:

Training and testing phase is a data division for generating training and testing. For machine learning we must provide the training data to build and train up model for spoof detection. In testing phase this model is used to validate the images. From table 4, it has been shown CASIA-FASD has a high accuracy and low time consumption compared to other datasets.

Table 4 Calculation of accuracy and time consumption

Dataset name	Training images	Testing images	Accuracy (in %)	Time consumpti -on(in sec)
CASIA-FASD	434	432	100	351.7615
NUAA	369	368	99.7685	471.7336
Kaggle	521	520	99.8077	363.4454
ROSE-Yutu	388	387	99.7416	616.0946

From fig. 13, CASIA-FASD shows a high accuracy value and NUAA shows minimal accuracy values compared to other datasets. In fig 14, CASIA-FASD shows low time consumption compared to other datasets.

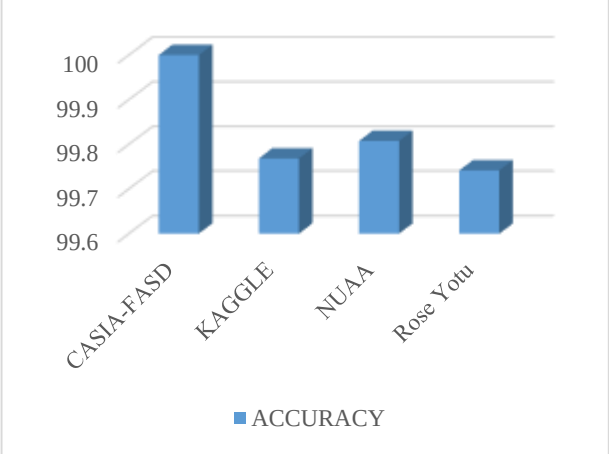
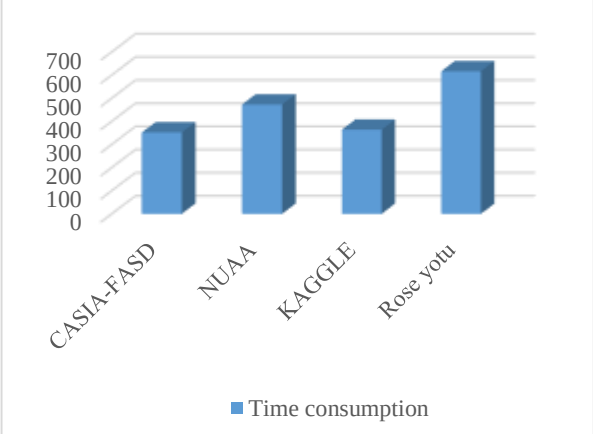


Fig. 13 Graphical Representation on accuracy



.

Fig. 14 Graphical Representation of Time Consumption.

6.2 Confusion Matrix

The Confusion matrix is an error matrix it is a layout of a table which allows to visualize the performance of the algorithms. A Confusion matrix provides the number of success and un-success prediction as a summary of the predicted result in classification problem. It makes prediction when our classification model is confused.

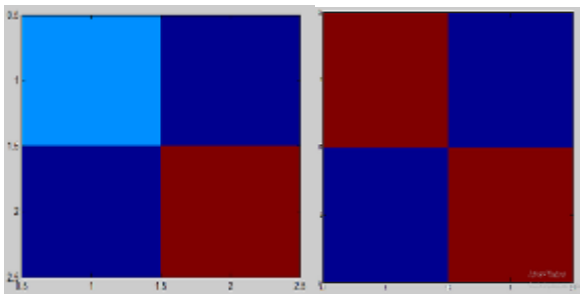
Table 5 Confusion matrix prediction.

	Class 1 predicted	**Class 2 predicted**
Class 1 actual	TP	FN
Class 2 actual	FP	TN

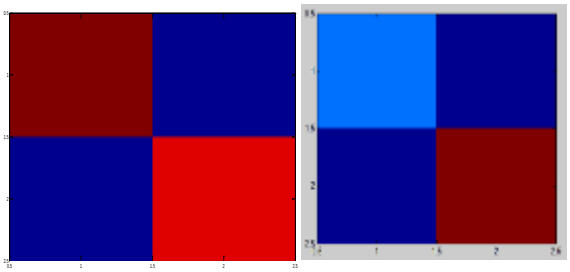
It gives us insight not only into the errors being made by a classifier but more importantly the types of error that are being made are shown in table 5. The confusion matrix of the four datasets are calculated and shown in table 6. From table 5, Class1 is Positive and Class2 is Negative. Positive (P) refers when an Observation is positive. Negative(N) refers when an Observation is not positive. Positive (TP) refers when an Observation is positive, and is predicted to be positive. False Negative (FN) refers when an Observation is positive, but is predicted negative. True Negative (TN) refers when Observation is negative, and is predicted to be negative. False Positive (FP) refers when Observation is negative, but is predicted positive.

Table 6 Output values of the confusion matrix.

Dataset Name	**Confusion Matrix**
CASIA-FASD dataset	[76,0;1,292]
Kaggle dataset	[258,0;1,261]
ROSE-Youtu dataset	[204,0;1,182]
NUAA dataset	[78,0;1,353]



(a) Confusion matrix of CASIA-FASD dataset **(b)**Confusion matrix of Kaggle dataset



(c) Confusion matrix of ROSE-Yutu dataset **(d)** Confussion matrix of NUAA dataset

Fig.15 Output of confussion matrix

The true positive, false negative, true negative, false positive values are calculated are calculated for four dataset and shown in fig.15.

7. CONCLUSION

Biometrics identification is mainly used for security purpose. The face recognition is the best technique. Among various image processing algorithm and classifier. HOG algorithm is used and SRC classifier

is used. From the above results it shows that the in CASIA-FASD dataset it provides the accuracy rate of 100%, NUAA dataset provides the accuracy rate of 99.76%, Kaggle dataset provides the accuracy of 99.9019% and ROSE-Yutu dataset provides the accuracy of 99.7416. The algorithm is used for different database and the experimental results clearly shows using this algorithm we have achieved the best accuracy recognition rate. Then there is no chance for any kind of malpractice. Thus, the authenticated user's alone allowed to access. As a future direction, the proposed approach can also be extended to reduced the time consumption to a minimal level and also detection accuracy can be further increased in a challenging wild datasets.

REFERENCES

[1]. Arockia Panimalar et al."Sparse Representation for Image Classification", International Research Journal of Engineering and Technology (IRJET), 2017, vol 4, issue 17, -ISSN: 2395-0072.

[2]. Emna Fourati et al." Face anti-spoofing with image quality assessment", 2nd international conference on bio engineering in smart technologies, 2017, DOI 10.1109 / biosmart .2017.8095313

[3]. Haoliang Li and Wen Li, "Unsupervised Domain Adaptation for Face Anti-Spoofing", IEEE transaction on information forensics and security, 2018, vol 13, no7.

[4]. Francisco et al. "Entropy-Based Face Recognition and Spoof Detection for Security Applications", Sustainability, 2020, DOI:10.3390 / su12010085.

[5]. Huda Mady and Shadi M. S. Hilles "Face recognition and detection using Random forest and combination of LBP and HOG features", International Conference on Smart Computing and Electronic Enterprise. (ICSCEE2018), 2018

[6]. Jian Yang et al. "Sparse Representation Classifier Steered Discriminative Projection with Applications to Face Recognition", IEEE transaction of neutral networks and learning system.

[7]. Jie zhou et al. "Research and application of face anti spoofing based on depth camera", IEEE, 2019, ISBN 978-1-7281-4091-9/19

[8]. Junying Gan et al. "3D Convolutional Neural Network Based on Face Anti-Spoofing ", 2nd international conference on multimedia and image compression, 2017, ISBN: 978-1-5090-5954-6/17

[9]. M. Kolliuolu et al." Anti-Spoofing in Face Recognition with Liveness Detection Using Pupil Tracking", 15th International Symposium on Applied Machine Intelligence and Informatics (IEEE), 2017, ISBN:978-1-5090-5655-2/17

[10]. Md Rezwan Hasan et al. "Face anti spoofing using texture based technique and filtering method", Journal of Physics, 2019, Conf. Ser. 1229 012044

[11]. Meenakshi Sai and Dr. Chander Kant ,"Liveness Detection for Face Recognition in Biometrics", IOSR Journal on computer engineering, ISSN:2278 0668

[12]. Navneet Dalal and Bill Triggs" Histograms of Oriented Gradients for Human Detection", Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), ISBN: 1063-6919/05

[13]. Sandeep Kumar et al." A Comparative Study on Face Spoofing Attacks", International Conference on Computing, Communication and Automation (IEEE), 2017, ISBN: 978-1-5090-6471-7/17/

[14]. Shervin Rahimzadeh Arashloo et al. "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol", IEEE access, Digital Object Identifier:10.1109 vol5.

[15]. Shuhua Liu et al. "An Identity Authentication Method Combining Liveness Detection and Face Recognition", Journal on sensors, 2019, DOI: 10.3390/19214733

[16]. Xiaobai Li et al." Generalized face anti-spoofing by detecting pulse from face videos", 23rd international conference on pattern recognition IEEE, 2016, ISBN: 970-1-5090-4847-2/16

[17]. Yousef Atoum et al. "Face Anti-Spoofing Using Patch and Depth-Based CNNs",International Joint Conference on Biometrics,2017,ISBN:978-1-5386-1124-1/17

[18]. Zahid Akhtar and GianLuca Foresti," Face Spoof Attack Recognition Using Discriminative Image Patches", Journal on electrical and computer science engineering, 2016, article no 47241629.