https://afrjcict.net

A Texture-based Method for Detecting Impostor Attacks using Printed Photographs

A. J. Jegede [1], G. I. O. Aimufua[2] and G. A. Thomas[3]
[1,3]Department of Computer Science, University of Jos, Nigeria.
[2]Department of Computer Science, Nasarawa State University, Keffi, Nigeria.
Email: [1]jegedea@unijos.edu.ng, [2]aimufuagio@yahoo.com, [3]thomasg@unijos.edu.ng

ABSTRACT

Conventional biometric systems do not possess the capability to detect whether a biometric image is acquired from a live subject or an artificial representation of his identity. This allows impostors to use different methods to fake the identities of legitimate users and compromise the security of biometric authentication systems. This paper proposed a texture-based anti-spoofing technique known as concatenated rotation invariant uniform local binary pattern, which uses textural properties to discriminate between images (face and iris) captured directly from live subjects and those obtained from secondary sources such as photographs or video images. The proposed approach extracts uniform local binary pattern features from an image at different scales and resolutions. The extracted features are further concatenated to obtain a composite feature representation of the image. The accuracy of proposed method is evaluated using face images from Nanjing University of Aeronautics and Astronautics (NUAA) normalized dataset and iris images from Audio, Temporal signals, Vision and Speech (ATVS) fake iris database. The programming environment used to implement the proposed technique is MATLAB 2014. The MATLAB environment provides the tools/utilities for creating the programs which implements the various tasks in the spoof detection system. Experimental results suggest that the proposed approach is capable of distinguishing genuine face and iris images from fake representations of the same image. The results also show the technique has better recognition accuracy and higher textural discriminative power for iris than it does for face. This is largely due to the fact that iris exhibits low intra-class variation and high inter-class distance; while face has high intra-class variation and low inter-class distance. The suitability of the proposed technique is not limited to only face and iris biometric data. The technique can be applied to any biometric modality whose textural features can be extracted. Examples include retina, palm, knuckle, fingerprint, lip and ear. We only used face and iris samples to verify the proposed method.

Keywords: *Anti-spoofing, Biometric, Liveness Detection, Security, Spoofing attack, Uniform local binary pattern*

African Journal of Computing & ICT Reference Format:

A.J. Jegede, G. I. O. Aimufua and G. A. Thomas (2020), A Texture-based Method for Detecting Impostor Attacks using Printed Photographs, *Afr. J. Comp. & ICT*, Vol. 13, No. 3, pp. 14 – 41.

I. INTRODUCTION

Biometrics is the method of measuring or the results obtained from the measurement of the unique physiological characteristics (such as fingerprints, face, iris, DNA, retina) and behavioral features (for example, keystroke dynamics, typing behavior, signature pattern) of the human body. It is the application of mathematical and statistical theory and methods to detect and recognize the physical characteristics of a person. This involves the use of an electronic device or system to perform automatic detection and recording of unique behavioural and biological features of an individual. The security of biometric system is a measure of the degree to which the system prevents unauthorized persons from claiming to be legitimated users. A secured biometric authentication system allows only valid users to gain access to a protected computer system or physical environment and denies unauthorized persons from accessing a sensitive system or location.

Spoofing is an attempt to fool a biometric system by presenting a fake version of the biometric modality of a legitimate user [1]. It is a direct attack against the user interface of a biometric authentication system and does not require an attacker to have any knowledge of the underlying recognition algorithm. A photograph imposter attack occurs when an attacker uses photographs or video streams which contain the face or eye image of a legitimate user to fool the biometric authentication system. An impostor can also use 3D artefacts such as face moulds, fingerprint moulds and fake eyeballs to fool the authentication system. Biometric systems which are susceptible to spoofing attack allow impostors to impersonate legitimate users and gain unauthorized access to the resources protected by the systems. Spoofed biometric representations can also be used to carry out authorized enrolment which undermines the integrity of the authentication system. The inability of a biometric system to detect fake representations may allow for repudiation. Repudiation makes it possible for an individual to deny transactions he actually performed, claiming that they are the results of attacks. Spoof detection or liveness detection is a process that uses specific discriminating features or characteristics to distinguish between a genuine biometric image and a fake representation of an identity. Anti-spoofing techniques automatically distinguish between real biometric data (acquired directly from the human body) and synthetically generated versions of genuine biometric credentials. These techniques rely on the theory that features or properties of a genuine biometric image are distinguishable from those of forged versions of the same image. Liveness detection can be integrated into biometric systems at sensor-level or feature-level [2]. Integrating liveness detection in biometric authentication systems prevents spoofing attack and repudiation. It also enhances the security and integrity of the authentication system. A uniform local binary pattern is a feature extraction technique which ensures that the binary pattern used to represent a biometric data is circular and that such pattern does not contain more than two bitwise transitions from 0 to 1 and vice versa. For examples, the patterns 00000000 (no transition), 01110000 (2 transitions) and 11001111 (2 transitions) are uniform, whereas the patterns 11001001 (4 transitions) and 01010011 (6 transitions) are not.

Deep learning, convolutional and recurrent neural networks are some of the recent techniques used for face spoof detection. For example, Li et al [3] used convolutional and recurrent neural networks to detect spoofed images captured from the photographs of genuine subjects. The proposed approach is a hierarchical feature learning strategy, which leverages the intra-block information and inter-block dependency. Experimental results on three databases showed that the method has significantly better performance than traditional handcrafted and deep learning-based approaches. Similarly, De Souza [4] proposed a robust face spoofing detection technique based on learning of deep local features. The work is based on a novel Convolutional Neural Networks (CNN) architecture trained in two steps. The first step involves each part of the neural network learning features from a given facial region. Afterwards, the whole model is fine-tuned by learning feature from the

entire facial image. Experimental results show that such pre-training step allows the CNN to learn different local spoofing cues. It also improves the performance and the convergence speed of the model. A related study detects presentation attacks based on spoofed faces by combining spatial and temporal information [5]. The approach integrates deep features extracted by a stacked convolutional neural network (CNN)-recurrent neural network (RNN) with handcrafted features. Experimental results showed that temporal information is sufficient for detecting spoofed faces. The results also confirmed that the handcrafted image features enhance the detection performance of deep features. A novel face anti-spoofing technique known as BIOPAD applied feature and score level fusion to information obtained from different spectral bands [6]. The model used Gabor features in a feedforward hierarchical structure of layers that progressively process and train visual information extracted from human faces.

A comparison of this model with other popular biologically-inspired layered models such as the "Hierarchical Model And X" (HMAX) and Convolutional Neural Networks (CNN) showed that it has better performance in all of the three presentation attack databases examined. Experimental results showed that the technique has promising detection rates and confirmed that near-infrared visual information significantly improves detection of presentation attacks. Li et al [7] applied deep learning to traditional local binary pattern to create a novel end-to-end learnable LBP network for face spoofing detection. The approach combines learnable convolutional layers with fixed-parameter LBP layers (that are comprised of sparse binary filters and derivable simulated gate functions) in order to achieve a significant reduction in the number of network parameters. A comparison with existing deep leaning-based detection methods showed a reduction in the number of parameters in the fully connected layers by a factor of 64. Experimental results based on two standard spoofing databases (that is, Relay-Attack and CASIA-FA) demonstrate that the proposed LBP network substantially outperforms existing state-of-the-art methods.

Spoofing attacks via printed eye images and contact lens can impair the accuracy of iris recognition systems. This is because the spoofed iris images from either the printed eye images or contact lens (or both) can have significant effects on the inter-class and intra-class variations and allow an imposter to compromise iris recognition systems [8]. However, the use of cost-effective descriptor methods approaches may help prevent such spoofing attacks. Spectral independent component analysis is a technique used to distinguish the natural iris texture from cosmetic contact lens (CCL) pattern, and restore genuine iris patterns from images contaminated by CCL pattern [9]. A proof of concept based on a database containing 200 test image pairs from 20 CCL-wearing subjects showed that the scheme has a good recognition accuracy with a false rejection rate of 0.57%.

Hybrid spoof detection techniques are based on a combination of two or more anti-spoofing methods. These approaches use two or more different methods to extract features from biometric images. Each type feature is fed separately into a classifier and a score is obtained. The outputs of various classifiers are then combined using score level fusion in order to determine whether an image is genuine or spoofed. Such hybrid techniques are based on combinations of texture and frequency analysis [10], texture and local shape analysis [11], Binarized Statistical Image Features (BSIF) and cepstral features [12], Multiscale Binarized Statistical Image Features on three orthogonal planes (MBSIF-TOP) and Multiscale Local Phase Quantization on three orthogonal planes (MLPQ-TOP) [13] as well as Binarized Statistical Image Features and local binary patterns [14]. These studies show that spoof detection schemes based on the hybrid approach have higher spoof detection rates than those based on only one anti-spoofing method.

The goal of this paper is to propose and implement a technique which prevents imposters from using stolen photographs of faces and eyes of legitimate users to compromise biometric authentication systems. The proposed approach known as concatenated rotation invariant uniform local binary pattern, uses textural properties to discriminate between images (face and iris) captured from live subjects and those obtained

from secondary sources such as photographs or video images. The technique leverages on the differences in the texture of images obtained directly from users and those captured from the photographs of legitimate subjects. The strategy is to extract uniform local binary pattern features from an image at different scales and resolutions. A composite feature set is obtained by concatenating the extracted at uniform local binary features. The goal is to show that concatenating LBPs of different scales and resolutions provides better classification results than just one LBP with a fixed scale and resolution. This ensures that the approach can perform efficient discrimination between genuine and fake face or iris images. The rest of the paper is organized as follows. Section 2 discusses related works and basic mathematical preliminaries on local binary pattern. The focus of Section 3 is the methodology used for the research. Section 4 presents the results and discussion, while Section 5 is the conclusion of the study.

II. RELATED WORK

Face spoof detection methods are based on any of the following approaches: physiological interaction or challenge response, frequency analysis or multi-spectral illumination and micro-texture analysis [15]. Challenge response approaches use physiological properties such as mouth movement [16], eye blinking [17-21], motion analysis [22] and head rotation [23-24] to distinguish a live face from a fake one. These approaches require user cooperation and suffer recognition inaccuracy. Frequency or multi-spectra illumination approaches are based on the theory that the frequency distributions of a live image are different from those of the spoof versions of the same image [1]. These approaches use "the illuminations beyond visible spectrum" [15] to show that spoofed face images and genuine ones have different properties when examined using multi-spectral illumination [24-26]. Multi-spectral-based approaches use different techniques such as reflectance (specular) or diffusion component decomposition [27] and Lambertian reflectance model [28] to detect fake face images. Spoof detection models based on micro-texture analysis use the differences in textural representation to distinguish between an authentic biometric image and a fake one. Two commonly used techniques for micro-texture analysis are Difference of Gaussian (DoG) filtering [16] and local binary patterns (LBP) [29]. Multimodal spoof detection systems based on the integration of face recognition with gait and speech are naturally more difficult to bypass than unimodal systems [18]. Figure 1 is an illustration of a face image and its spoofed (fake) counterpart obtained from a printed photograph of the original (genuine) image. Figure 1 is an illustration of a face image and its spoofed (fake) counterpart obtained from a printed photograph of the original (genuine) image.

A recently proposed face anti-spoofing method used local ternary patterns to leverage on the variations in contrast and textural characteristics of images acquired directly from live subjects and those obtained from photographs [30] This technique addresses the performance limitations of the basic local binary pattern caused by the noisy nature of the order of a pixel with respect to its neighbor in homogeneous region. Experimental results show that the proposed approach performs better than conventional texture-based methods. The same authors proposed an improved approach over conventional local ternary pattern which uses Weber's law to eliminate manual thresholding [31]. The results of experiments show that the technique has high accuracy and performs better than conventional local binary pattern and local ternary pattern. An enhancement of this approach produced a robust texture descriptor which uses local features based on Sign, Magnitude and Centre complementary components [32]. The approach which uses Weber's law for thresholding has better performance accuracy than the earlier proposed dynamic local ternary pattern. A novel approach integrates an enhanced version of LBP known as Gene LBP net with Convolutional Neural Network [33]. The results from experiments performed on NUAA database show that the technique possesses good accuracy in detecting face spoofing attacks.

The generic (or basic) LBP and its various extensions have been used to detect photograph imposter, printed photograph and video attacks in face recognition systems [1]. The basic LBP operator is defined as

$$LBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_c) \cdot 2^p \quad (1)$$

such that

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases}$$

where

g_p is grayscale value of the neighbour pixel,

g_c is the value of the central pixel,
p is the index of the neighbor
R is the radius of the circular region
P is the number of sample points in the neighbourhood of the central pixel [29].

The LBP thresholds a local neighborhood at the grayscale value of the center pixel into a binary pattern. $LBP_{P,R}$ operator is by definition invariant against monotonic transformation of the grayscale. This makes $LBP_{P,R}$ robust against changes in illumination. As long as the as the order of the gray values in the image stays the same, the output of the $LBP_{P,R}$ remains constant.

Some extensions of the basic LBP include transitional LBP, direction-coded LBP and modified LBP [34]. Other variants are rotation invariant LBP, uniform LBP and uniform rotation invariant LBP. Rotation invariant LBP is defined as

$$LBP_{P,R}^{ri} = min\{ROR(LBP_{P,R}^{ri}, i) \mid i = 0, 1, \cdots, P-1\} \quad (2)$$

where $ROR(x, i)$ performs a circular bit-wise right shift on the P-bit number $x\ i$ times [29]. In terms of image pixels, the equation simply corresponds to rotating the neighbor set clockwise so that a maximal number of the most significant bits starting from $gP - 1$, is 0. $LBP_{P,R}^{ri}$ quantifies the occurrence statistics of individual rotation invariant patterns corresponding to certain micro-features in the image; hence the patterns can be considered as feature descriptors. The pixels in the neighbor set are indexed so that they form a circular chain and the gray values of the diagonal pixels are determined by interpolation. This is necessary to obtain the circularly symmetric neighbor set, which allows for deriving a rotation invariant version of $LBP_{P,R}$. Practical experience, however, has shown that $LBPROR$ does not provide a very good discrimination [35].

Uniform LBP is defined as

$$U(LBP_{P,R}) = |s(gP - g_c) - s(g_0 - g_c)| + \sum_{p=1}^{P-1} |s(g_p - g_c) - s(g_{p-1} - g_c)| \quad (3)$$

Such that

$$s(gP - g_c), s(g_0 - g_c), s(g_p - g_c), s(g_{p-1} - g_c) = \begin{cases} 1 & gP \geq g_c, g_0 \geq g_c, g_p \geq g_c, g_{p-1} \geq g_c \\ 0 & gP < g_c, g_0 < g_c, g_p < g_c, g_{p-1} < g_c \end{cases}$$

where

g_0 is grayscale value of the first pixel along the circular region,
g_{p-1} is the grayscale value of the pixel preceding the neighbour pixel
gP is the grayscale value of the last pixel in the neighbourhood of the central pixel
g_c, g_p, p, R and P are as previously defined in equation (1) [29]

A local binary pattern is called uniform if the binary patterns contain at most two bitwise transitions from 0 to 1 and vice versa when the bit pattern is considered circular [36]. For examples, the patterns 00000000 (no transition), 01110000 (2 transitions) and 11001111 (2 transitions) are uniform, whereas the patterns 11001001 (4 transitions) and 01010010 (6 transitions) are not. In the computation of the LBP histogram, uniform patterns are used so that the histogram has a separate bin for all uniform patterns and all non-uniform patterns are assigned to a single bin. We use the following notation for the LBP operator: $LBP_{P,R}^{riu2}$. The subscript represents using the operator in a (P, R) neighbourhood. Superscript $u2$ stands for using only uniform patterns; while P is the number of sample

points in the neighbourhood of the central pixel and R is the radius of the circular region. Experimental results show that uniform LBP ($LBP_{3\times3}^{u2}$) provides the best results in terms of performance/complexity trade-off.

Uniform LBP is defined as

$$LBP_{P,R}^{riu2} = \begin{cases} \sum_{p=0}^{p-1} s(g_p - g_c) \\ P+1 \end{cases}, \text{ if } \begin{matrix} U(LBP_{P,R}) \leq 2 \\ otherwise \end{matrix} \quad (4)$$ [29]

The $LBP_{P,R}^{riu2}$ operator is an excellent measure of the spatial structure of local image texture, but it, by definition, discards the other important property of local image texture, i.e., contrast, since it depends on the gray scale. If only rotation invariant texture analysis is desired, i.e., gray-scale invariance is not required, the performance of $LBP_{P,R}^{riu2}$ can be further enhanced by combining it with a rotation invariant variance measure $VAR_{P,R}$ that characterizes the contrast of local image texture. The joint distribution of these two complementary operators, $LBP_{P,R}^{riu2}/VAR_{P,R}$, is a powerful tool for rotation invariant texture classification.

The proposed approach uses concatenated uniform rotation invariant LBPs to distinguish between real images (face and iris) and fake ones. Concatenated LBP is defined as

$$CONC[U(ROR(LBP)] = \sum_{i=1}^{n} LBP_{P_iR_i}^{riu2} \quad (5)$$

where each $LBP_{P_iR_i}^{riu2}$ represents features extracted from an image using uniform rotation invariant LBP of a certain scale and resolution. Image features extracted at different scales and resolutions are concatenated to form a composite feature set. That is,

$$\sum_{i=1}^{n} LBP_{P_iR_i}^{riu2} = LBP_{P_1R_1}^{riu2} + LBP_{P_2R_2}^{riu2} + \cdots + LBP_{P_nR_n}^{riu2} \quad (6)$$

Note that $LBP_{P,R}^{riu2} = \begin{cases} \sum_{p=0}^{p-1} s(g_p - g_c) \\ P+1 \end{cases}$ (From equation 4)

$$\therefore CONC[U(ROR(LBP)] = \sum_{i=1}^{n} \sum_{p=0}^{p-1} \frac{s\left(g_p - g_c\right)}{P+1} \quad (7)$$

The goal is to provide better classification results by combining LBPs of different scales and resolutions, rather than using just one LBP with a fixed scale and resolution. This provides an effective approach for discriminating between genuine and fake face or iris images.

The vulnerability of face recognition systems to spoofing using 3D masks has also been explored and the same extensions of LBP were proposed as possible solutions [37]. A related work [18] proposed multiscale LBP as a remedy for photograph imposter attack. A comparison of the proposed technique with similar texture-based approaches such as Local Phase Quantization (LPQ) [38] and Gabor wavelets [20] shows that multiscale LBP has better detection rate than the other two techniques. The colour local binary pattern descriptor [39] uses a combination of colour and texture information to detect replay attacks involving face images. This technique combines texture information which is extracted at different colour bands from the same image. Results from experiments show that the use of coloured images provides better performance than the use of greyscale images. A high level of discrimination between genuine and imposter face images was achieved by using DoG filtering to remove noise and preserve the high frequency component before applying local binary pattern variance (LBPV) [40] to extract face features. A recent work [41] distinguished spoofed face images from genuine ones using a low-level feature and shape analysis. The approach used Speeded-Up Robust Features (SURF) and Pyramid Histogram of Oriented Gradient (PHOG) as feature extraction techniques. An evaluation of the method on two scenarios (intra-database and cross-database), using 4 different publicly available datasets (MSU MFSD, NUAA Imposter, CASIA FASD, and IDIAP Replay-Attack) showed that the spoof detection techniques based on hybrid feature extraction

algorithm achieve better result than those based on single feature extraction algorithm.

Iris liveness detection is a technique used to distinguish the iris image of a live subject from that obtained from photograph or video images of the same subject. Figure 2 presents samples of genuine and fake iris images.

Techniques used for iris liveness detection include Fourier analysis [42] and the analysis of unique optical characteristics of the iris [43]. Other methods include pupillary motion [44] and challenge-response approaches in which a subject may be required to perform eye blink or eye movements in real time [45]. Komogortsev et al [18] proposed the use of eye movements to distinguish between genuine and fake iris samples. This approach performs liveness detection at feature and match-score levels. Experimental results show that liveness detection at feature level is resistant to spoofing attacks. The accuracy at match-score level depends on the type of biometric technique applied. Techniques based on the analysis of image frequency spectrum, controlled light reflection from the cornea and pupillary movements have been used to distinguish between genuine iris samples and those obtained from printed eye images [46]. The results of experiments show that these techniques have zero FAR for fake iris images. Analysis of image spectrum has FRR of 2.8% for genuine images while the other methods have zero FRR for genuine biometric samples. Sensor-level spoofing attacks can be prevented by detecting the statistical grey-level dependencies in both the local and global regions surrounding the iris [47]. Experiments based on 1,200 real and fake iris images achieved correct classification rate of 99.75%. Fake iris patterns from contact lenses can be detected using convolution network and fully-connected single layer with softmax regression [48]. This method has a 30% improvement in performance over state-of-the-art techniques. Genuine iris samples can be distinguished from fake versions by using pupil dynamics to monitor changes in pupil size in response to visible light stimuli [49]. This approach provides good classification rate and can distinguish between genuine and spoof images in 3 seconds. A novel approach for detecting video attacks in iris recognition systems uses Euclidean video magnification (EVM) to enhance video phase information in the eye region and a novel decision module to distinguish between genuine and fake iris images based on variation of phase spectrum information [50]. This technique has good accuracy with an average classification error rate of 0%. An enhanced solution is based on the integration of iris verification system with liveness detection and the use of static and dynamic sub-modules to perform experiments on MMU and CASIA iris databases [51]. The accuracy, FAR and FRR obtained for MMU database are 99.44%, 0.0277 and 0.0055 respectively. Experimental results on CASIA database showed accuracy of 97.77%, FAR of 0.0333 and FRR of 0.0222.

Kohli et al [52] proposed a unified framework, which uses structural and textural features to detect a variety of iris spoofing attacks. The approach encodes variations in the structure of an iris image by calculating multi-order dense Zernike moments across the image. Local Binary Pattern with Variance (LBPV) is utilized for detecting the textural differences between a genuine iris and a spoof version. The proposed approach has a maximum classification accuracy of 82.20% for distinguishing genuine and fake iris images in a combined iris spoofing database. Similarly, variations in local intensity based on a rotation-invariant feature-set comprising of Zernike moments and Polar harmonic transforms is also used for detecting of iris spoofing attacks [53]. Experimental results based on four publicly available iris spoofing databases (IIITD Contact Lens, IIITD Iris Spoofing, Clarkson LivDet-Iris 2015 and Warsaw LivDet-Iris 2015 that include both contact lens and print at- tack spoofing samples) demonstrate that the proposed system easily detects spoofing attacks even when such attacks involve multiple sensors. The accuracy of iris spoof detection mechanisms can be enhanced by combining features extracted from both local and global iris regions, rather than using only features extracted from global iris region image [54]. This hypothesis was verified by applying convolutional neural networks and support vector machines based on iris images captured using near-infrared (NIR) light camera. Extensive experiments using two well-known public datasets (LivDet-Iris-2017 Warsaw and Notre Dame Contact Lens Detection 2015) showed that the approach is efficient and has few detection errors.

III. METHODOLOGY

The flowchart in Figure 3 illustrates the various stages and processes used to implement and verify the proposed approach.

The tasks in the flowchart are implemented by writing appropriate programs using the MATLAB environment. The MATLAB environment provides the tools/utilities and language for writing the programs. MATLAB is considered a suitable implementation environment and programming language because of its flexibility and convenience. It also contains image processing toolbox which helps to simplify the preprocessing of biometric images.

3.1 Image Pre-processing and Feature Extraction

The pre-processing tasks normally carried out on face images prior to feature extraction include face detection, cropping and normalization. Figure 4 depicts the flow of activities in face image processing.

Face detection extracts local texture information from an image and uses a binary classifier to distinguish the facial part from other parts of the image. Cropping removes the non-face parts of the head (such as the ears and frontal hair) from the detected face image. Normalization eliminates variation in size, illumination and rotation from face images of the same or different subjects. The experiments in this work are carried out on preprocessed face images, which eliminate the need for face detection, cropping and normalization. Face features are extracted from normalized images using uniform rotation invariant local binary pattern. Figures 5(a) illustrate the original detected, cropped and normalized face image, while Figure. 5(b) is the LBP image obtained from the normalized image.

The technique is chosen because it is robust against variations in scale, illumination and image rotation. In addition to this, uniform features constitute a large percentage of dominant (or discriminant) features, which the LBP method extracts from images.

Iris image preprocessing involves two major tasks, namely segmentation and normalization. The flowchart in Figure 6 illustrates the activities involved iris preprocessing.

Segmentation is a process used to isolate the iris from other eye structures such as pupil, sclera, eyelids and eye lashes. The technique removes non-iris features that can affect the accuracy of the recognition process. This is accomplished by detecting the inner and outer boundaries of the iris. It also involves detecting the eyelids and the eye lashes that can interrupt the circular contour of the limbus boundary. A higher weight is assigned to the vertical gradient for the iris/sclera boundary [55], while equal weights are assigned to the horizontal and vertical gradients for the iris/pupil boundary. A modified version of Kovesi's Canny edge detection method [56] was used to assign weight to the gradients. Circular Hough transform is used for detecting the iris and pupil boundaries. Hough transform is defined as $x^2 + y^2 = r^2$, where (x, y) are the coordinates of the centre of the iris and pupil and r is the radius of the circular iris/pupillary boundaries. Figure 7 and 8 show an eye image (captured using a near infra red camera) and a segmented iris respectively.

The segmented iris usually contains noise as depicted in Figure 9.

Normalization transforms the segmented iris structure from cartesian coordinates to pseudo-polar coordinates. Most iris processing tasks use the rubber sheet model [57] to carry out normalization. Figure 10 illustrates the operation of the rubber sheet model**.**

Normalization is defined as

$$I(x(r,\theta),\ y(r,\theta)) \rightarrow I(r,\theta) \quad (6)$$

such that

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta) \text{ and } y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta)$$

where $I(x, y)$, (x, y) and (r, θ) are the iris image, original cartesian coordinates and corresponding normalized polar coordinates respectively; while (x_p, y_p) and (x_l, y_l) denote the respective coordinates of the pupil and iris boundaries along the θ direction

[58]. The model unwraps the iris by translating each point within the Cartesian coordinate to a pair of polar coordinates (r, θ), where r falls within the range [0, 1] and θ is an angle in the range [0, 2π]. Figure 11 illustrates a Cartesian iris image.

Normalization addresses variations in pupil size across the subjects and eliminates the effect of such variations in the size of the iris. It also maps irises of different subjects into a common domain, thus providing for translation and scale invariance. The rubber sheet model uses pupillary dilation and variations in pupil size to produce normalized irises of fixed dimension. A normalized iris image is illustrated in Figure 12.

It is necessary to remove noise from the polar iris image in order to minimize errors in the recognition process. Figure 13 is the unwrapped, noiseless iris image.

Uniform rotation invariant Local Binary Pattern is applied on the pre-processed image to obtain its feature representation. For example, Figure 14 presents the feature distribution plot of the uniform patterns of face images in the (8,1) neighbourhood.

The values on the vertical axis represent the bins in the feature distribution as well as the number of features in each bin. The values on the horizontal axis represent the labels of each bin. There are 10 bins in the feature distribution. The figure shows that bin 3 contains about 200 features, while bin 7 is made up of about 7,500 features.

The extracted LBP features are represented by the histogram in Figure 15.

The horizontal axis represents number of features in each LBP bin, while the values on the vertical axis represent the labels of each bin. There are 10 bins in the feature distribution. Our LBP histogram is not normalized since the window sizes of face images in the dataset are the same. The bins of the LBP distribution are used as features for the SVM classifier.

The proposed approach is based on LBP features extracted at three different scales and resolutions, namely $LBP_{8,1}, LBP_{8,2}$ and $LBP_{16,2}$. The three scales are selected because [29] noticed that in their experiments with texture images, uniform patterns account for a bit less than 90 percent of all patterns when using the (8,1) neighbourhood, and for around 70 percent in the (16,2) neighbourhood. Experimental results showed that 90.6 percent of the patterns in the (8,1) neighbourhood and 85.2 percent of the patterns in the (8,2) neighbourhood are uniform in case of preprocessed FERET facial database [36]. The extracted features are concatenated to form a composite feature of the face or iris image. That is, $LBP_{8,1}, + LBP_{8,2} + LBP_{16,2}$, where the operator, + represents concatenation.

3.2 Training and Classification

Classification is used to distinguish between a genuine (real) image and a fake (photograph) image. This involves using a classifier to partition a dataset into genuine and imposter classes. The classifier used in this study is the linear support vector machine (SVM). Support vector machines [59] are supervised learning models comprising machine learning algorithms that analyze data used for classification and regression analysis. A supervised learning model uses a set of training data, each of which is labelled as belonging one or the other of two classes to build a model that assigns new data to class or the other. An SVM model maps data to points in space and ensures that the data of the different classes are separated by a clear gap that is as wide as possible. New data are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall. Linear SVM is chosen as a classification method because it is a fast, scalable and an accurate technique for solving multiclass classification problems involving large datasets [60]. It is also an effective dimensionality reduction technique, which selects only the most stable and discriminant values from the feature set [61]. The approach can handle multiclass classification problems containing any number of classes and is efficient in dealing with very large data sets containing several millions training data pairs. It is also effective for both sparse and dense high dimensional data containing a large number of features and attributes. Linear SVM is economical to implement as personal computer is the standard platform to run the algorithm. Figure 16 is the screenshot of the feature extraction and the computation of target feature set which SVM uses for classification.

Holdout cross-validation is the underlying machine learning technique used to evaluate the linear SVM classifier. The evaluation process is used to train and test the classifier. Validation is a process used to find the best parameters for a model and to prevent the model from being overfitted. The screenshot of the code segment for classification is shown in Figure 17.

This study used the holdout method because it is "the simple, suitable for fully independent data and has low computational overhead as it only needs to be run once in order to obtain classification results [62 - 63]. A conventional holdout technique involves a single run (on a pair of training and testing set), which may lead to highly misleading results. The cross-validation variant of holdout used in this study averages the results of multiple runs on different pairs of training and testing sets. This is in contrast to the generic holdout method whose results are based on a single run.

The computation of classification accuracy is performed by a function named *ConRotInvLBP.m* which calls other functions in the application to perform feature extraction, feature reshaping, feature concatenation and computation of predicted label(s). The screenshot of this operation on LBP face features extracted in the (8,1) neighbourhood and (8,2) neighbourhood are presented in Figures 18 and 19 respectively.

The accuracy is computed in terms of the number of correctly predicted labels and the total number of labels in the feature set obtained for both genuine and imposter datasets. That is

$$Accuracy = \frac{number\ of\ correctly\ predicted\ labels}{total\ number\ of\ feature\ labels} \times 100\%$$

The number of correctly predicted labels and total number of feature labels and total number of feature labels in Figure 17 (8,1 neighbourhood) are 1900 and 3421 respectively; hence the classification accuracy is 55.5393%. On the other hand, the respective values of correctly predicted labels and total number of feature labels in case of (8,2) neighbourhood are 1858 and 3421 (see Figure 18); hence the classification accuracy is 54.3116%.

The screen shot of this operation on concatenated features extracted in the (8,1) and (8,2) neighbourhoods is presented in Figure 20. The same function is used to compute the classification accuracies for various face and iris features obtained in different LBP neighbourhoods as shown in Tables 1and 2.

The figure shows that the respective values of the number of correctly predicted labels and total number of feature labels and total number of feature labels are 1858 and 3421 respectively; hence the classification accuracy is 54.3116%. It is important to note that the values obtained in each case can vary slightly when the experiments are carried out at different times using the same or different datasets. This is due to variations in the accuracies of LBP feature extraction and SVM classification when experiments are carried out with the same or different datasets.

3.3 Experimental Dataset

The experimental datasets consist of face images obtained from the NUAA normalized face database [28] and ATVS iris database [64]. The NUAA face database consists of two datasets, namely ClientNormalized and ImposterNormalized. The ClientNormalized set contains 5,104 genuine images of 15 subjects, while the ImposterNormalized set contains 6,298 fake (scanned photograph) images of 15 subjects. The ATVS iris database also consists of 800 genuine iris images of 50 subjects and 800 fake (printed photograph) iris images of 50 subjects.

IV. RESULTS AND DISCUSSION

The experiments were performed by applying uniform rotation invariant LBP on face and iris images under seven different scenarios. These include $LBP_{8,1}^{riu2}$, $LBP_{8,2}^{riu2}$, $LBP_{16,2}^{riu2}$, $LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2}$, $LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2}$, $LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$ and $LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$. The goal is to evaluate and compare the textural discriminative power of LBP under different scales and resolutions and when LBPs of different scales and resolutions and combined together. The performance results of various LBPs are presented in terms of accuracy, which represents rate at which each LBP discriminates between genuine and imposter images. Table 1 presents the performance of various LBPs on NUAA normalized face images.

The table shows that the classification accuracies for $LBP_{8,1}^{riu2}$, $LBP_{8,2}^{riu2}$ and $LBP_{16,2}^{riu2}$ are 56.3%, 55.8% and 55.5% respectively. $LBP_{8,1}^{riu2}$ has the highest classification rate and accuracies compared to $LBP_{8,2}^{riu2}$ and $LBP_{16,2}^{riu2}$ because it contains more uniform patterns than $LBP_{8,2}^{riu2}$ and $LBP_{16,2}^{riu2}$. This supports the findings in previous works by Ojala et al [29] and Ahonen et al [36]. This implies that $LBP_{8,1}^{riu2}$ has higher textural discriminative power than the other two techniques. The concatenation of LBPs of different scales and resolutions shows the same or lower classification accuracy compared to when each LPB is evaluated individually. This is because the average amount of uniform patterns in the concatenated LBP is less than or almost equal to those of the individual LBPs. This implies that the textural discriminative power of the individual LBPs is higher than that of the concatenated approaches.

The performance of the proposed approach on ATVS iris database is presented in Table 2.

The respective accuracies of uniform rotation invariant LBPs in the (8,1), (8,2) and (16,2) neighbourhoods are 64.1%, 62.33% and 65.42%. This shows that the number of uniform patterns extracted by the uniform rotation invariant LBP in the (16,2) neighbourhood are more that those obtained by uniform rotation invariant LBPs in (8,1) or (8,2) neighbourhood. Hence, the textural discriminative power of $LBP_{16,2}^{riu2}$ is higher than that of $LBP_{8,1}^{riu2}$ and $LBP_{8,2}^{riu2}$. The concatenation of LBPs in (8,1) and (8,2) neighbourhoods produces a lower accuracy than using LBP in the (8,1) neighbourhood and a higher accuracy than using LBP in the (8,2) neighbourhood. This is because the high textural discriminative power of $LBP_{8,1}^{riu2}$ is degraded by the lower discriminative power of $LBP_{8,2}^{riu2}$ and the low textural discriminative power of $LBP_{8,2}^{riu2}$ is enhanced by the high discriminative power of $LBP_{8,1}^{riu2}$. The concatenation of LPBs in the (8,1) and (16,2) neighborhoods produces a higher discriminative power and hence better classification accuracy than using the individual LBP separately. The same applies to concatenated LPBs in the (8,2) and (16,2) neighborhoods. Experimental results show that concatenating LBPs in the (8,1), (8,2) and (16,2) neighbourhoods produce better classification accuracy and higher textural discriminative power than individual LBPs in the (8,1) and (8,2) neighbourhoods. On the other hand, the concatenated approach is less accurate and has lower textural discriminative power than using the LBP in the (16,2) neighbourhood.

The results in Tables 1 and 2 show that the proposed approach has better recognition accuracy and higher textural discriminative power for iris than it does for face. This is largely due to the fact that the human iris exhibits low intra-class variation and high inter-class distance. That is, the textural information in irises of the same person is very similar, while iris images of different subjects have significant differences [65]. Conversely, the human face exhibits large intra-class variation and low inter-class distance [66]. This implies that face images of the same person have high textural differences, while faces belonging to different subjects have low similarity in textural information. Generally, the results vary with the scale and resolution of the LBP used for the experiments and whether simple or composite (concatenated) feature sets are used as input of the classifier.

V. CONCLUSION AND FUTURE WORK

This paper proposed a texture-based technique known as concatenated rotation invariant uniform local binary pattern. The approach is based on the theory that textural features (or properties) of face and iris images captured directly from a live subject are distinguishable from those obtained from secondary sources such as photographs or videos of the same subject. The proposed approach prevents attackers from impersonating legitimate users and gaining unauthorized access to the resources protected by the systems. It also preserves the integrity of the biometric authentication system by detecting unauthorized enrolment. The ability to detect fake representations of a user's biometric facilitates nonrepudiation. This makes it difficult for an individual to claim that the transactions he actually performed are the results of attacks. Integrating liveness detection in biometric authentication systems prevents spoofing attack and repudiation. The suitability of the proposed technique is not limited to only face and iris biometric data. The technique can be applied to any biometric modality whose textural features can be extracted. Examples include retina, palm, knuckle, fingerprint, lip and ear. We only used face and iris samples to verify the proposed method. Overall, the proposed approach

enhances the security and integrity of the authentication system. A future work will integrate deep learning, convolutional and recurrent neural networks with concatenated rotation invariant uniform LBP to enhance the discriminative power of the proposed approach. This will be achieved by applying convolutional and recurrent neural network-based classifier on deep features extracted from local and global face or iris regions.

REFERENCES

[1] I. Chingovska, A. Anjos and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *2012 International Conference of the Biometrics Special Interest Group*, Darmstadt, Germany, 2012, pp. 1-7.

[2] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," *IEEE International Conference on Biometrics and Forensics*, Limassol, Cyprus, 2016, pp. 1-6.

[3] H. Li, S. Wang and A.C. Kot, "Image recapture detection with convolutional and recurrent neural networks," in *IS&T International Symposium on Electronic Imaging, Media Watermarking, Security, and Forensics*, Burlingame, CA., USA, 2017, pp. 87-91.

[4] G.B. De Souza, J.P. Papa, and A.N. Marana, "On the learning of deep local features for robust face spoofing detection," in *Proceedings of 2018 31st IEEE SIBGRAPI 2018 Conference on Graphics, Patterns and Images*, Purana, Brazil, 2018, pp. 258-265.

[5] D.T. Nguyen, T.D. Pham, M.B. Lee, and K.R. Park, "Visible-light camera sensor-based presentation attack detection for face recognition by combining spatial and temporal information," *Sensors*, vol. 19, no. 2, pp. 1-27, Jan2019.

[6] A. Tsitiridis, C. Conde, B.G. Aylon and E. Cabello, "Bio-inspired presentation attack detection for face biometrics," *Frontiers in Computational Neuroscience*, vol. 13, no. 34, pp. 1-17, Dec2019.

[7] L. Li, X. Feng, Z. Xia, X. Jiang, and A. Hadid, "Face spoofing detection with local binary pattern network," *Journal of Visual Communication and Image Representation*, vol. 54, pp. 182-192, Jul2018.

[8] P. Gupta, S. Behera, C. Vatsa and R. Singh, "On iris spoofing using print attack," in *2014 22nd International Conference on Pattern Recognition*, Stockholhm, Sweden, 2014, pp.1681-1686.

[9] S-H. Hsieh, Y-H. Li, W. Wang and C-H. Tien, "A novel anti-spoofing solution for iris recognition toward cosmetic contact lens attack using spectral ICA analysis," *Sensors*, vol. 18, no. 1, pp. 1-15, Jan2018

[10] G. Kim, S. Eum, J.K. Suhr, D.K. Kim, K.R. Park, and J. Kim, "Face liveness detection based on texture and frequency analysis," in *2014 International Conference on Advances in Engineering and Technology Research*, Singapore, 2014, pp. 1-4.

[11] J. Maatta, A. Hadid and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *2011 International Joint Conference on Biometrics*,Washington DC, USA, 2011, pp. 1-7.

[12] R. Raghavendra, C. Busch, "Presentation attack detection algorithm for face and iris biometrics," in *2014 22nd European Signal Processing Conference*, Lisbon, Portugal, 2014, pp. 1387-1391.

[13] S.R. Arashloo, J. Kitler and W. Christmas, "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features, *IEEE Transaction on Information Forensics and Security*, vol, 10, no. 11, pp. 2396-2407, Oct2015.

[14] R. Raghavendra, C. Busch, "Robust 2D/3D face mask presentation attack detection scheme by exploring multiple features and comparison score level fusion," in *2014 17th International Conference on Information Fusion*, Salamanca, Spain 2014, pp. 1-7.

[15] J. Yang, Z. Lei, S. Liao, S.Z. Li, "Face liveness detection with component descriptor," in *2013 International Conference on Biometrics*, Madrid, Spain, 2013, pp. 1-6.

[16] K. Kollreider, H. Fronthaler, M.I. Faraj, J. Bigun, "Real-time face detection and motion analysis with application in liveness assessment," *IEEE Transaction on Information Forensics and Security*, vol. 2, no. 3, pp. 548-558, Mar2007.

[17] L. Sun, G. Z. Pan, W. Tan, S. Lao, "Blinking-based live face detection using conditional random fields," in *Lecture Notes in Computer Science: Advances in Biometrics*, vol. 4642, S.W. Lee, S.Z. Li (Eds.), Germany, Springer, 2007, pp. 252-260.

[18] O.V. Komogortsev, A. Karpov, C.D. Holland, "Attack of mechanical replicas: liveness detection with eye movements," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 716-725, Apr2015.

[19] G. Pan, L. Sun, Z. Wu, S. Lao, "Eyeblink-based anti-spoofing in face recognition from generic webcamera," in *2007 IEEE 11th International Conference on Computer Vision*, Rio de Janeiro, Brazil, 2007, pp. 1-6.

[20] G. Pan, Z. Wu, L. Sun, "Liveness detection for face recognition," in Recent Advances in Face Recognition, K. Delac et al (Eds), Vienna, Austria, I-Tech, 2008, pp. 236.

[21] H.K. Jee, S.U. Jung, J.H. Yoo, "Liveness detection for embedded face recognition system," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 2, no. 6, pp. 2142-2145, Feb2008.

[22] K. Kollreider, H. Fronthaler, J. Bigun, "Verifying liveness by multiple experts in face biometrics," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Anchorage, Alaska, USA, 2008, pp. 1-6.

[23] K. Kollreider, H. Fronthaler, J. Bigun, "Non-intrusive liveness detection by face images," *Image and Vision Computing*, vol. 27, no. 3, pp. 233-244, Mar2009.

[24] W. Bao, H. Li, N. Li, W. Jiang, "A liveness detection method for face recognition based on optical flow field," in *2009 International Conference on Image Analysis and Signal Processing*, Vietri sul Mare, Italy, 2009, pp. 233-236.

[25] I. Pavlidis, P. Symosek, "The imaging issue in an automatic face/disguise detection system," in *IEEE Conference on Computer Vision Beyond the Visible Spectrum: Methods and Applications*, New York, USA, 2006, pp. 15-24.

[26] Z. Zhang, D. Yi, Z. Lei, S.Z. Li, "Face liveness detection by learning multi spectral reflectance distribution," in *2011 IEEE International Conference on Automatic Face and Gesture Recognition and Workshops*, Ljubjana, Slovenia, 2011, pp. 436-441.

[27] J. Bai, T.T. Ng. X. Gao, Y.Q. Shi, "Is physics-based liveness detection only possible with a single image? in *IEEE International Symposium on Circuits and Systems*, Paris, France, 2010, pp. 3425-3428.

[28] X. Tan, Y. Li, J. Liu, L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discrimination model," in *11th European Conference on Computer Vision, Part VI*, K. Danilidis et al (Eds), Germany, Springer-Verlag, 2010, pp. 504-517.

[29] T. Ojala, M. Pietikainen, T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, Jul2002.

[30] S. Praveen, SMS, Ahmed, NH, Abbas, N. Naeem, M. Hanafi, "Texture analysis using local ternary patterns for face anti-spoofing," *Sci. Int. (Lahore)*, vol. 28, no. 2, pp. 965-971, Feb2016.

[31] S. Praveen, SMS. Ahmed, WAW. Adnan, NH. Abbas, N. Naeem, M. Hanafi, "Face liveness detection using dynamic local ternary pattern (DLTP)," *Computers 2016*, vol, 5, no. 10, pp. 1-15, Oct2016.

[32] S. Praveen, SMSA. Abdul Rehman, N. Naeem, J. Devi, M. Ahmed, "Improved complete dynamic local ternary pattern texture descriptor for face spoof attacks," *International Journal of Computer Science and Network Security*, vol. 18, no. 12, pp. 102-110, Dec2018.

[33] K. Grover, R. Mehta, "Face spoofing detection using enhanced local binary pattern," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 2, pp. 3365-3371, Dec2019.

[34] J. Terfny, J. Matas, "Extended set of local binary patterns for rapid object detection," in *Computer Vision Winter Workshop*, L. Sparcek, V. Franc (Eds), Czeck Republic, 2010 pp. 1-7.

[35] M. Pietikainen, T. Ojala, Z. Xu, "Rotation invariant texture classification using feature distributions," *Pattern Recognition*, vol. 33, no. 1, pp, 43-52, Jan2000.

[36] T. Ahonen, A. Hadid M. Pietikainen, "Face description with local binary patterns: application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037-2041, Dec2006.

[37] N. Erdogmus, S. Marcel, "Spoofing face recognition with 3D masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084-1097, Jul2014.

[38] B. Ojansivu and J. Heikkila, "Blur insensitive texture classification using local phase quantization," in *The 3rd International Conference on Image and Signal Processing*, A. Elmoataz et al (Eds) pp. 236-243. Germany, Springer-Verlag, 2008, pp. 2636-2640.

[39] Z. Boulkenafet, J. Komulainen, A. Hadid, "Face spoofing detection using colour texture analysis," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1818 – 1830, Aug2016.

[40] N. Kose, J.L. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," in *IEEE/OSA/IAPR International Conference on Informatics, Electronics and Vision*, Dhaka, Bangladesh, 2012, pp. 1027-1032.

[41] D.D. Arini, KN. Ramadhani, F. Sthevanie, "Detection of face spoofing using low-level features and shape analysis," *Journal of Physics: Conf. Series*, vol. 1192, pp. 1-7, May2019.

[42] A.K. Jain, R. Bolle, S. Pankanti, "*Biometrics: Personal Identification in Networked Society*," Amsterdam: Kluwer Academic Publishers, 1999.

[43] Interview with Dr. John Daugman, Cambridge University, UK, 2004**.** October 20, 2019 Availabble: www.FindBiometrics.com.

[44] J. Daugman, "*Liveness Detection Countermeasures*," United Kingdom: University of Cambridge, 2005.

[45] A. A. Ross, K. Nandakumar, A. K. Jain, "*Handbook of Multibiometrics*," Germany: Springer, 2006.

[46] A. Pacut, A. Czajka, "Aliveness detection for iris biometrics," in *40th Annual IEEE International Carnahan Conference on Security Technology*, Lexington, KY, USA, 2007, pp. 1-8.

[47] C-W. Tan, A. Kumar, "Integrating ocular and iris descriptors for fake iris image detection," in *2014 International Workshop on Biometrics and Forensics*, Madrid, Spain, 2014, pp. 1-4.

[48] P. Silva, E. Luz, R. Baeta, D. Menotti, H. Pedrini, A.X. Falcao, "An approach to iris contact lens detection based on deep image representations," in *2015 28th SIBGRAPI Conference on Graphics, Patterns and Images*, Salvador, Brazil, 2015, pp. 1-8.

[49] A. Czajka, "Pupil dynamics for iris liveness detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 726 – 735, Apr2015.

[50] K.B. Raja, R. Raghavendra, C. Busch, "Video presentation attack detection in visible spectrum iris recognition using magnified phase information," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2048-2056, Oct2015.

[51] H.M. Ahmad, B.J.Abdulkareem, "Integrate liveness detection with iris verification to construct support biometric system," *Journal of Computer and Communications*, vol. 4, no. 1, pp. 22-32, Jan2016.

[52] N. Kohli, D. Yadav, M. Vasta, R. Singh, A. Noore, "Detecting medley of iris spoofing attacks using DESIST," in *2016 IEEE 8th International Conference on Biometrics: Theory, Applications and Systems*, Niagara Falls, NY, USA, pp. 1-6.

[53] B. Kaur, S. Singh, J. Kumar, "Cross-sensor iris spoofing detection using orthogonal features," *Computers and Electrical Engineering*, vol. 73, pp. 279 –288, Jan2019.

[54] D.T. Nguyen, T.D. Pham, Y.W. Lee, K.R. Park, "Deep learning-based enhanced presentation attack detection for iris recognition by combining features from local and global regions based on NIR camera sensor," *Sensors*, vol. 18, no. 8, pp. 1-32, Aug2018.

[55] R. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348-1363, Sep1997.

[56] http://www.cs.uwa.edu.au/~pk/Research/MatlabFns/index.html

[57] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21-30, Jan2004.

[58] L. Masek, "Recognition of human iris for biometric identification," Upublished MSc Thesis, Department of Computer Science, University of Western Australia, 2003.

[59] C. Cortes, V.N. Vapnik, "Support vector networks. Machine learning," vol. 20, no. 3, pp. 273-297, Sep1995.

[60] T-M. Huang. V. Kecman, "Linear support vector machine," October 15, 2019. Available: http://www.linearsvm.com.

[61] A.K. Oladejo, T.O. Oladele, Y.K. Saheed, "Comparative evaluation of linear support vector machine and k-nearest neighbour algorithm using microarray data and leukemia cancer datatset," African Journal of Computing and ICT, vol. 11, no. 2, pp. 1-10, Jun2018.

[62] Cross validation, October 15, 2019. Available: http://www.cs.cmu.edu/~schneide/tut5/node42.html.

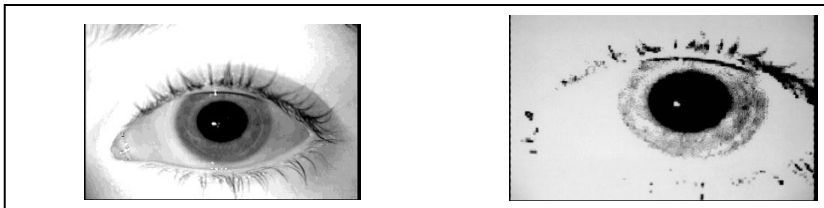
[63] R. Kelley, "Making predictive models robust: holdout vs cross-validation," October 21, 2019 Available: https://www.kdnuggets.com/2017/08/dataiku-predictive-model-holdout-cross-validation.html.

[64] J. Galbally, S. Marcel, J. Fierrez, J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *5th IAPR International Conference on Biometrics*, New Delhi, India, 2012, pp. 271-276.

[65] K. Bowler, K. Hollingsworth, P. Flynn, "Image watermaking for iris: a survey," *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281-307, Jun2007.

[66] L. Wu, S. Yuan, "A face based fuzzy vault scheme for secure online authentication," in 2010 Second International Symposium On Data, Privacy And E-Commerce, Buffalo/Niagara Falls, NY, USA, 2010, pp. 45-49.

Fig. 1 Genuine and spoofed face images



Genuine face image Fake iris image

Fig. 2 Genuine and fake iris images

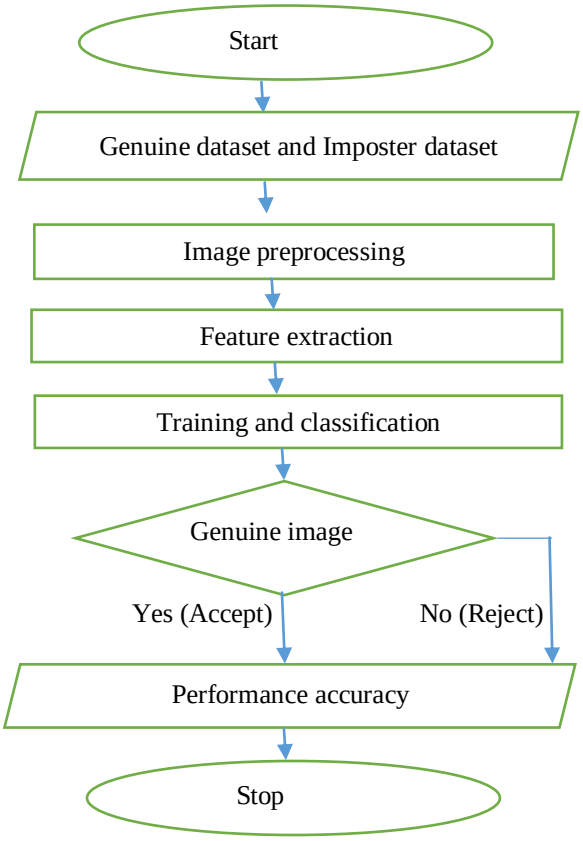


Fig. 3 Flowchart of the proposed approach

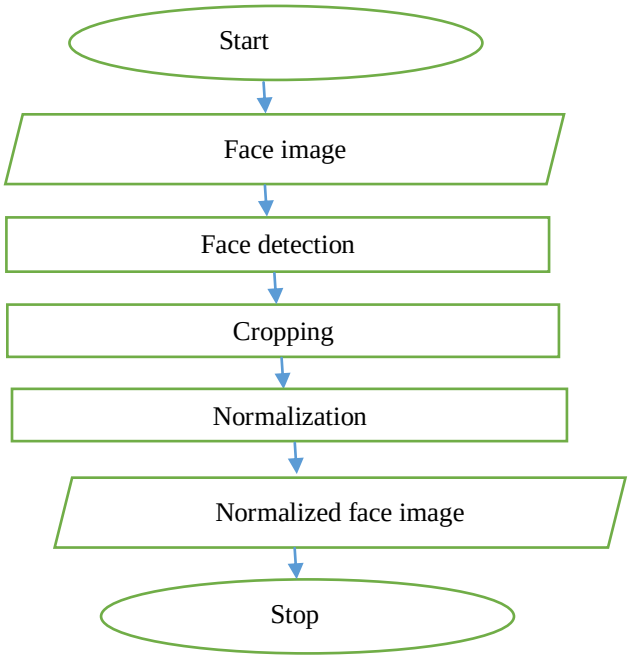


Fig. 4 Face image preprocessing

Fig. 5(a) Original face image.

Fig. 5(b) LBP face image

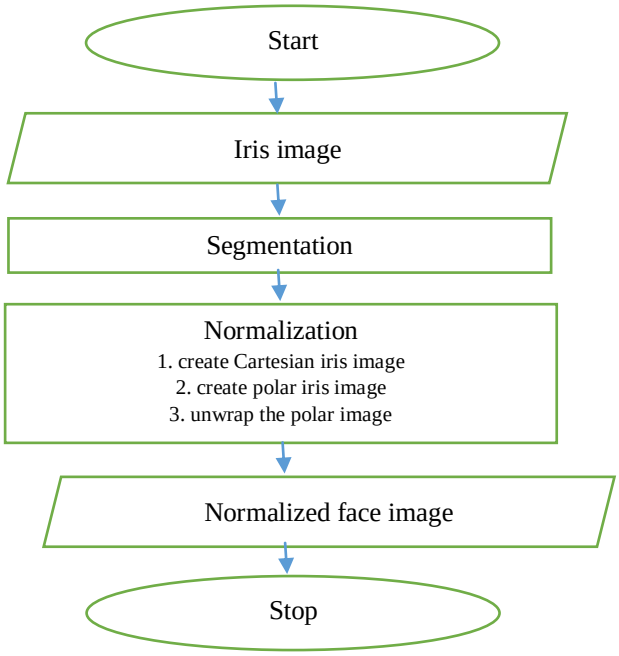


Fig. 6 Iris image preprocessing

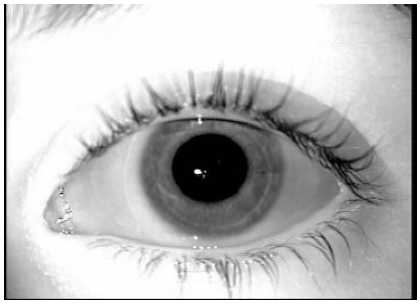


Fig. 7 Original eye image

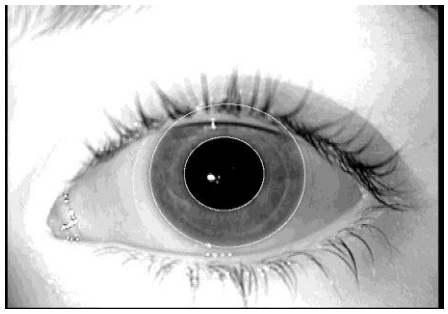


Fig. 8 Segmented iris

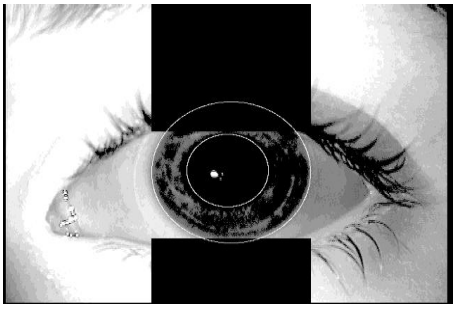


Fig. 9 Segmented iris image with noise

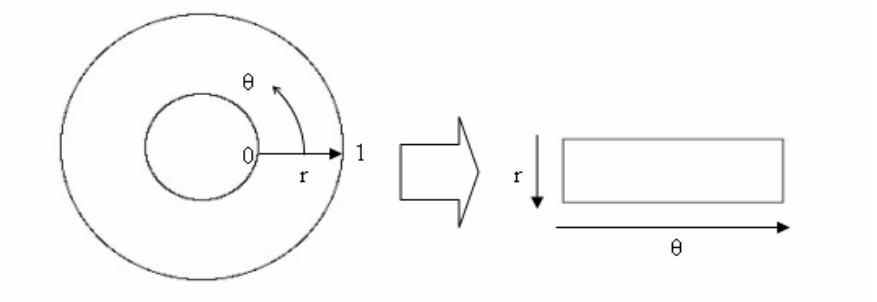


Fig. 10 Rubber sheet model

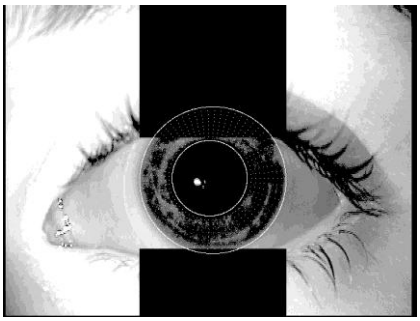


Fig. 11 Cartesian iris image

Fig. 12 Polar image with noise

Fig. 13 Unwrapped iris image

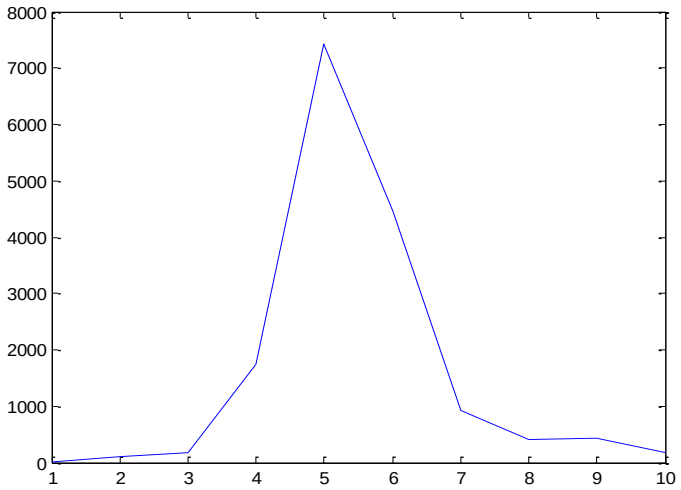


Fig. 14 LBP feature distribution plot

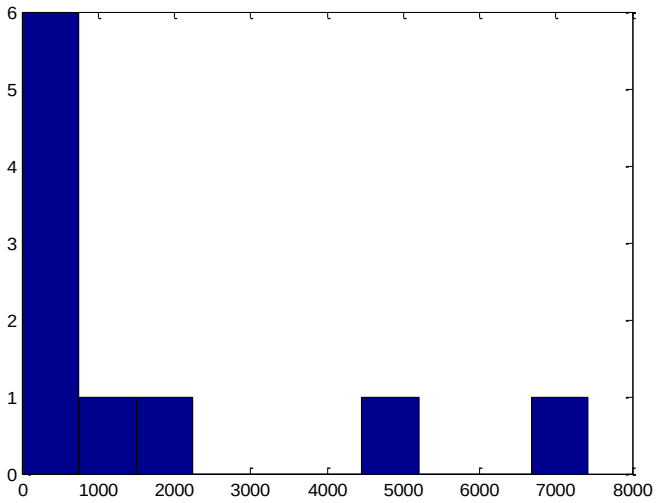


Fig. 15 LBP feature histogram

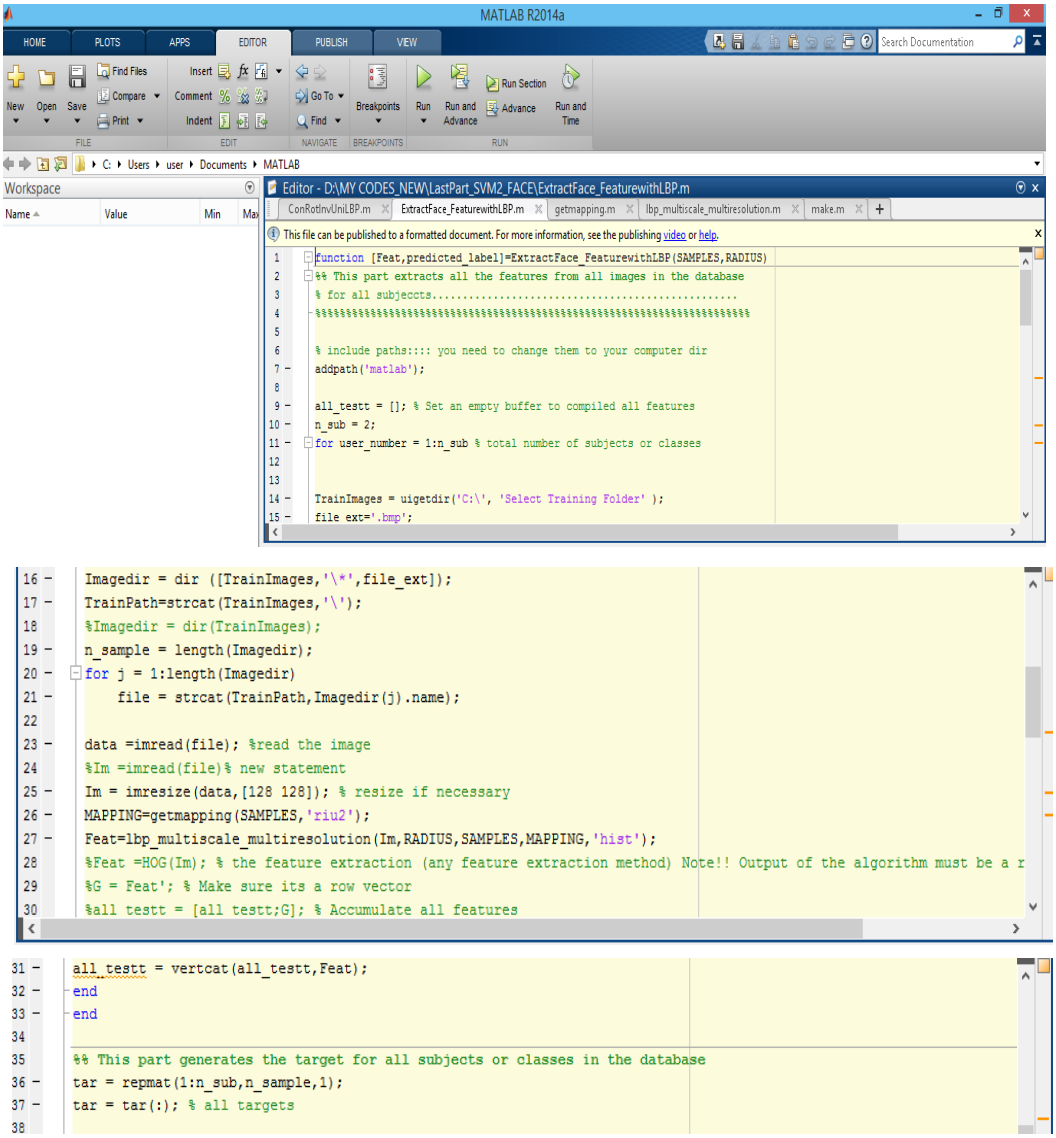


Fig. 16 Code segment for feature extraction and computation of target feature set

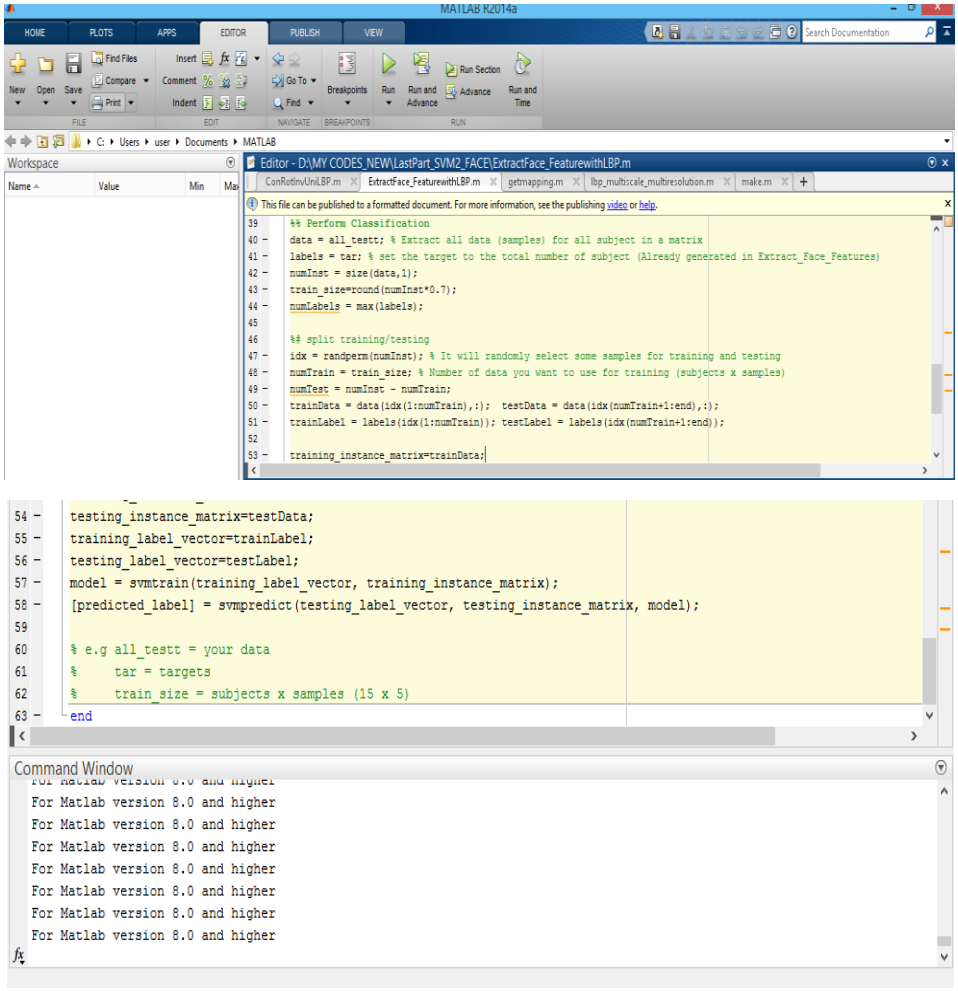


Fig. 17 Code segment for training and classification

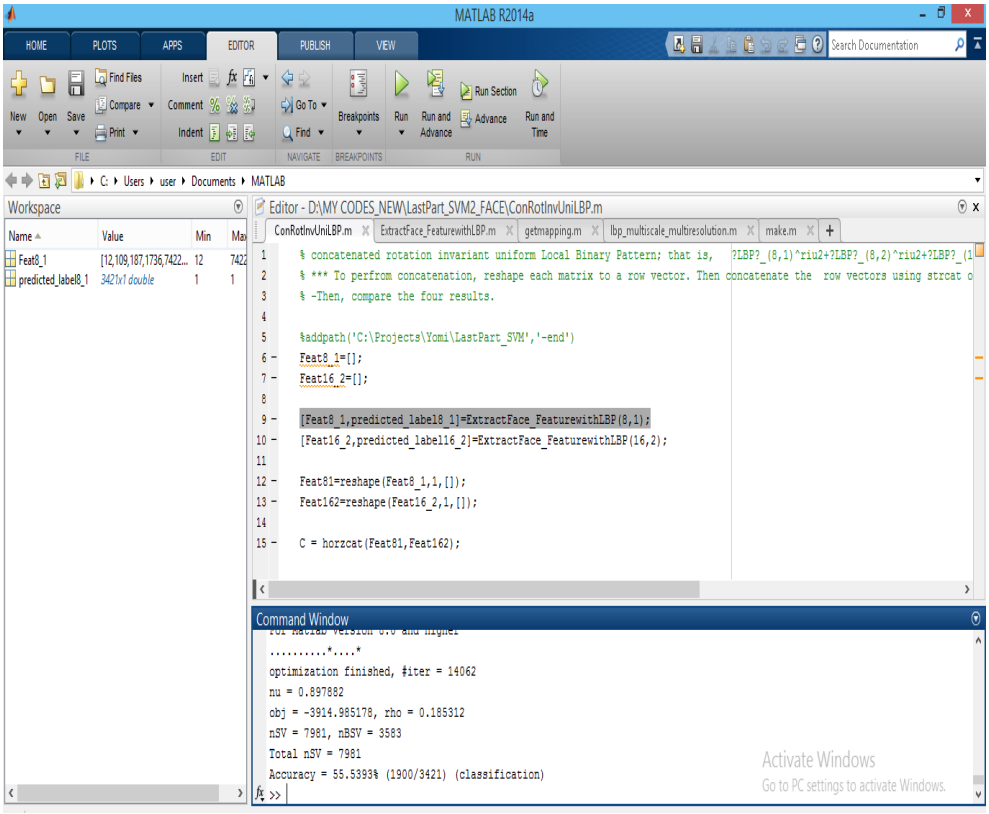


Fig. 18 Code segment for computation of classification accuracy of non-concatenated feature set in the (8,1) neighbourhood

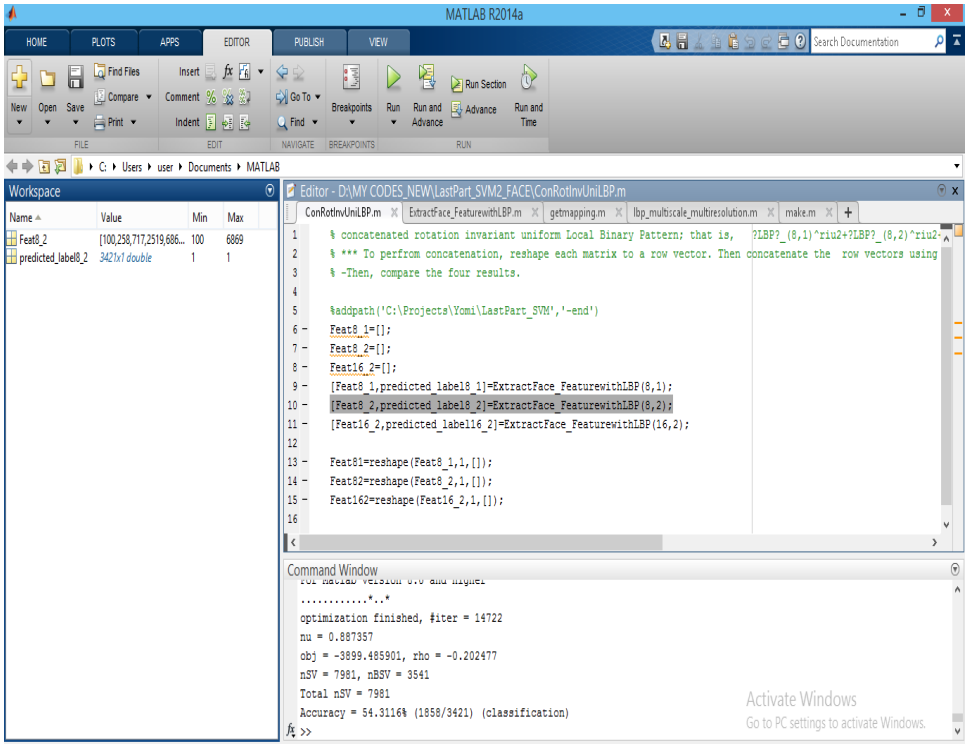


Fig. 19 Code segment for computation of classification accuracy of non-concatenated feature set in the (8,2) neighbourhood

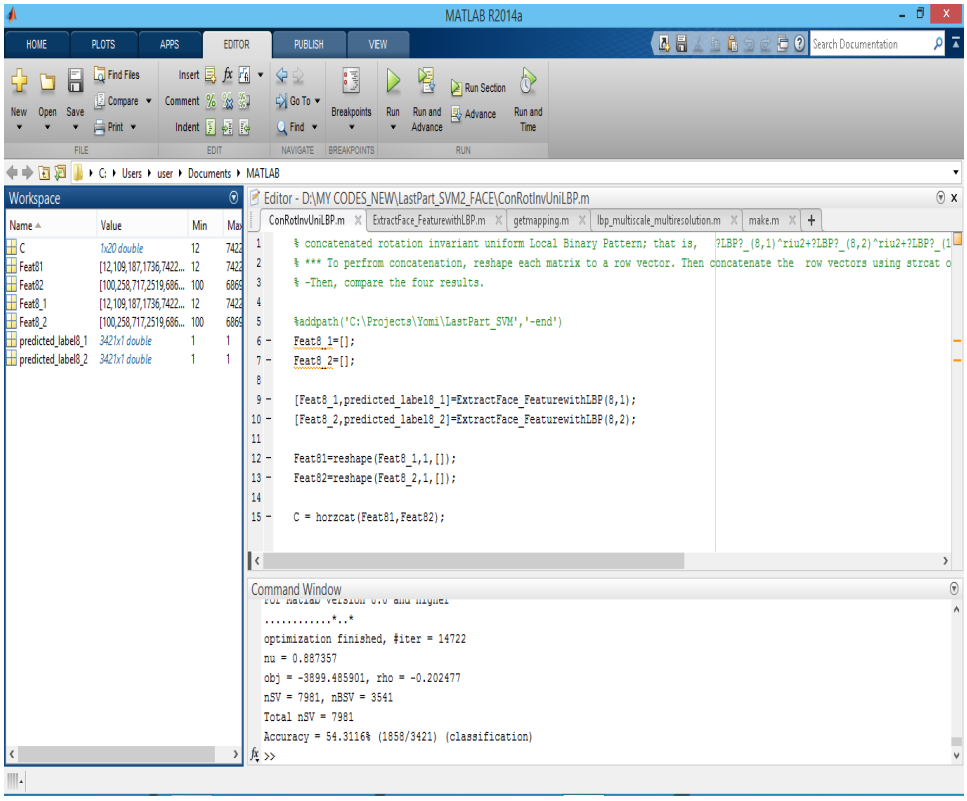


Fig. 20 Code segment for computation of classification accuracy for concatenated feature set

Table 1. Evaluation of the proposed approach on NUAA face database

Technique	Classification	Accuracy (%)
$LBP_{8,1}^{riu2}$	(1926/3421)	56.2993%
$LBP_{8,2}^{riu2}$	(1910/3421)	55.8316%
$LBP_{16,2}^{riu2}$	(1900/3421)	55.5393%
$LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2}$	(1856/3421)	54.3116%
$LBP_{8,1}^{riu2} + LBP_{16,2}^{riu2}$	(1858/3421)	54.3116%
$LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$	(1900/3421)	55.5393%
$LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$	(1839/3421)	53.7562%

Table 2 Evaluation of the proposed approach on ATVS iris database

Technique	Classification	Accuracy (%)
$LBP_{8,1}^{riu2}$	291/454	64.0969%
$LBP_{8,2}^{riu2}$	283/454	62.3348%
$LBP_{16,2}^{riu2}$	297/454	65.4185%
$LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2}$	284/454	62.5551%
$LBP_{8,1}^{riu2} + LBP_{16,2}^{riu2}$	316/454	69.6035%
$LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$	310/454	68.2819%
$LBP_{8,1}^{riu2} + LBP_{8,2}^{riu2} + LBP_{16,2}^{riu2}$	292/454	64.3172%