A Framework to Detect Presentation Attacks

Laeticia Etienne

Follow this and additional works at: https://digitalcommons.kennesaw.edu/msit_etd

Part of the Computer and Systems Architecture Commons

Recommended Citation
Etienne, Laeticia, "A Framework to Detect Presentation Attacks" (2020). Master of Science in Information Technology Theses. 7.
https://digitalcommons.kennesaw.edu/msit_etd/7
A Framework to Detect Presentation Attacks

Laeticia Etienne

A Thesis Submitted for Partial Fulfilment
of the Master of Science in Information Technology

Kennesaw State University
April 2020
Biometric-based authentication systems are becoming the preferred choice to replace password-based authentication systems. Among several variations of biometrics (e.g., face, eye, fingerprint), iris-based authentication is commonly used in everyday applications. In iris-based authentication systems, iris images from legitimate users are captured and certain features are extracted to be used for matching during the authentication process. Literature works suggest that iris-based authentication systems can be subject to presentation attacks where an attacker obtains printed copy of the victim’s eye image and displays it in front of an authentication system to gain unauthorized access. Such attacks can be performed by displaying static eye images on mobile devices or iPad (known as screen attacks). As iris features are not changed, once an iris feature is compromised, it is hard to avoid this type of attack. Existing approaches relying on static features of the iris are not suitable to prevent presentation attacks. Feature from live Iris (or liveness detection) is a promising approach. Further, additional layer of security from iris feature can enable hardening the security of authentication system that existing works do not address.

To address these limitations, this thesis proposed iris signature generation based on the area between the pupil and the cornea. Our approach relies on capturing iris images using near infrared light. We train two classifiers to capture the area between the pupil and the cornea. The image of iris is then stored in the database. This approach generates a QR code from the iris. The code acts as a password (additional layer of security) and a user is
required to provide it during authentication. The approach has been tested using samples obtained from publicly available iris database. The initial results show that the proposed approach has lower false positive and false negative rates.
Acknowledgments

I would like to express my sincere appreciation for Dr. Hossain Shahriar’s supervision and guidance of this thesis including providing and directing me to the resources. I would also like to thank the committee members Drs. Chi Zhang and Seyedamin Pouriyeh for their thoughtful comments with regard to improving my work. Finally, I am grateful for my family for their support during my study in the MSIT degree program from beginning to end.
Table of Contents

Acknowledgments ........................................................................................................................................ iii

Chapter I. Introduction .......................................................................................................................... 5

Chapter II. Background and Related Work ...................................................................................... 7
  2.1 Attack on Iris-Detection System .......................................................................................... 7
  2.2 Related Work .......................................................................................................................... 8

Chapter III. Classifiers for Iris Detection System ...................................................................... 154
  3.1 Haar-Cascade Classifier ....................................................................................................... 14
  3.2 LBP Classifier ..................................................................................................................... 16

Chapter IV. Proposed Iris-Signature Generator Framework ....................................................... 20
  4.1 Authentication Process ........................................................................................................ 18
  4.2 Iris code and QR code generation ....................................................................................... 19

Chapter V. Implementation and Evaluation ................................................................................. 21

Chapter VI. Conclusions .................................................................................................................. 24

References ......................................................................................................................................... 25
Security is based on three principal elements commonly known under CIA trad: Confidentiality, Integrity, and Availability. Authentication is a security control that is used to protect the system with regard to the CIA properties. Authentication is an essential step for accessing resources and/or services. Authentication is an essential step for giving access to resources to authorized individuals and prevent leakage of confidential information while maintaining the integrity of a system. There are many forms of biometrics that are currently being used for authentication such as fingerprint matching, facial recognition, shape of ear, iris pattern recognition and gait movement [26]. Among all, iris pattern recognition is a widely used biometric-based authentication approach [1, 2]. In an iris-based authentication system, iris images are captured from users, and features are extracted to be matched at a later stage for authentication. Iris is unique for everyone. It has distinct textures and patterns that can be used for authentication. Iris-based authentication can overcome the limitations of traditional password-based authentication systems that are vulnerable to brute force and dictionary-based attacks. Several iris-based commercial tools are available, including Iridis [13] and Eyelock [12]. The research literature shows a rise in the application of iris-based authentication systems in areas such as immigration and border control [10], healthcare, public safety, point of sales and ATM [26], and finance and banking [8].

Recently, iris spoofing attacks have emerged as a significant threat against traditional iris-based authentication systems. For example, an attacker may obtain a printed copy of the iris of a victim or using a reconstructed iris image sample and display the image
in front of an authentication system to gain unauthorized access (known as presentation attack) [4, 18]. Such attack can be performed by displaying static eye images on mobile devices or iPad (known as screen attack) [3]. This attack would lead to the risk of the wrong person gaining access or being misidentified; therefore, render security vulnerability. There are approaches to prevent presentation attacks [4, 5, 6, 9]. However, most of them rely on static features of the iris. Feature from live Iris (or liveness detection) is a promising approach [14, 16, 19], where iris images are taken with high quality camera and features are extracted. Further, additional layer of security from iris feature can enable hardening the security of authentication system that existing works do not address.

This thesis proposes iris code generation between the area of the pupil and the cornea. Figure 1 shows the red and yellow circles, which represent the area of cornea and iris. Our approach analyzes live images taken in a camera in infra-red light.

![Iris area between cornea and pupil](image)

Figure 1: Iris area between cornea and pupil

Haar-Cascade [20] and LBP classifiers [7] are used to capture the area between the pupil and the cornea. The captured area is stored in database repository for future matching purpose. The approach generates QR code from the iris image. The code is then used as a password. During authentication, iris images are matched, and the user is required to provide the QR code to be authenticated. The combination of the QR code and the iris images make hacking harder. A prototype has been implemented using OpenCV library.
The approach has been tested using samples of iris images obtained from publicly available iris dataset [18]. The initial results show that the proposed approach has lower false positive and false negative rates. Furthermore, Haar Cascade classifier works better than LBP classifier [28, 29].

This thesis is organized as follows. Section 2 discusses related work that detect attacks against iris-based authentication systems. Section 3 provides an overview of Haar-Cascade and LBP classifiers. Section 4 discusses the proposed framework in detail. Section 5 highlights the implementation details and evaluation of results. Finally, Section 6 concludes the paper and discusses future work.

Chapter II

Background and Related Work

2.1 Attacks on Iris-Detection System

It has been found that Media based Forgery and Spoofing are the most common kind of attacks in biometric based authentication system. Similarly, we find replay attack against iris is common [25]. Those kinds of attack method can be detected as liveness detection. Liveness detection allows system to validate the authentication process of valid user by
real biometric identifiers. Below we define several attack types that this thesis is intended to mitigate.

1. **Media based forgery**: Media based forgery is one of the common intrusion methods to deceive any biometric based authentication or processing system. Intruder can present printed images or frames of images of authenticated user and slip out of liveness detection to get authenticated user’s access in the system. For fingerprint authentication system, attackers can use authenticated user’s printed fingerprint in polymer plastic to authenticated access in the system.

2. **Spoofing**: Spoofing is a method of biometric liveness attack against identification system where a dummy artificial object of a user is presented by an intruder to the system to imitate the identification feature which the process is designed to check so that it can allow authentication to attacker. It is like using the cloned biometric part of any authenticated user and apply a biometric part to get access in the system. Spoofing is mostly used by most attackers in biometric authentication attack. In context of our topic we can do face spoofing attack by using printed iris image or any cosmetic contact lens. These kinds of attacks can be crucial and alarming points for system authentication and cause a serious damage to system.

3. **Fake Iris**: Iris recognition system uses data stored in the system that are merely bits of code in binary form. Reverse engineering is possible to obtain the actual image of the iris. Genetic algorithm can be used to make different attempts using synthetic iris to be recognizable to iris detection. It takes about 100 to 200 iterations to produce a similar iris image that is stored in iris recognition system.
4. Presentation attacks: The presentation of biometric spoof is called presentation attack. Biometric spoof could be some image, video instead of a live person; or fake silicon or gelatin fingerprints or fake synthetic iris instead of real eye. Recognition system should be equipped with liveliness detection systems. It detects whether the presentation is alive or a spoof.

2.2 Related Work

In this section we describe related work and the approached used to detect attacks on iris-based authentication systems.

We searched in IEEE and ACM digital libraries with keywords “iris liveness detection” during year 2000 and 2019, which resulted in 67 papers. We further narrow down the list of papers that are intended for presentation attack detection and removed survey papers from the list. This led to the list of papers shown in Table I. The list may not be exhaustive but represents the common cited works from the literature.

Pacut et al. [4] detect liveness of iris by analyzing the frequency spectrum as it reveals signatures within an image. Ratha et al. [5] split images of biometric fingerprints known as shares. These shares are stored in different databases. During authentication, one of the shares acts as an ID while another share is retrieved from the central database to be matched with a known image. Andreas et al. [6] rely on PRNU which the difference between the response of a sensor and the uniform response from light is falling on camera sensor. This approach captures the noise level information (irrelevant data) from iris images. Given that a new iris image is required to authenticate, the PRNU fingerprints from stored images are compared with the given one.
Puhan et al. [19] detect iris spoofing attacks using texture dissimilarity. As the illumination level is increased to an open eye, the pupil size decreases. Printed iris does not demonstrate such change of the pupil. High value of normalized Hamming distance between a captured image and known image results in warning of spoofed image. Adam et al. [9] detect live iris based on amplitude spectrum analysis. In this approach, a set of live iris images are analyzed to obtain the amplitude levels while performing Fourier transformation. A fake iris image has dissimilar amplitude levels compared to the real iris image.

Karunya et al. [11] assess captured iris image quality to detect spoofing attacks. color, luminance level, quantity of information, sharpness, general artifacts, structural distortions, and natural appearance are qualities that can be used to differentiate between real images from fake images. Thavalengal [14] detects liveness of iris based on multi spectral information. This method exploits the acquisition workflow for iris biometrics on smartphones using a hybrid visible (RGB)/near infrared (NIR) sensor. These devices are able to capture both RGB and NIR images of the eye and iris region in synchronization. This multi-spectral information is mapped to a discrete feature space. The NIR image detects flashes in a printed paper and no image in case of a video shown for authentication. If a 3D live model is shown, an image shows ‘red-eye’ effect which could be used to detect iris liveness.

Huang et al. [15] rely on pupil constriction to detect iris liveness detection. The ratio of iris and pupil diameters is used as one of the considerations during authentication. Liveness prediction is evaluated based Support Vector Machine (SVM) classifier. A database of fake irises, printed images, and plastic eye balls is built for training and testing of SVM classifier.
As the intensity of light increases, the pupil size decreases. The SVM can differentiate the real iris from a fake one.

Kanematsu et al. [16] detect liveness based on variation of brightness. This approach relies on the variation of iris patterns induced by a pupillary reflex for various brightness levels of light. Like anti-virus programs that include database of viruses, this approach relies on database of fake irises to detect fake authentication attempts.

Mhatre et al. [17] extract features and encrypt with Bio-Chaotic Algorithm. The input image is divided into parts to apply the Bio-Chaotic algorithm. An image is segmented and randomly one block of image is selected to hide a secret message using a unique key. The entire image is encrypted. The graph of both original and encrypted iris image is generated so that one can see the difference after the encryption process. Only authorized user knows about the random block selected and the key so an attacker fails to fraud. The decryption process is the reverse of encryption process.

Gowda H D et al. [27] propose a CNN architecture modeling a robust and reliable biometric verification system using traits face (ORL dataset) and iris (CASIA dataset). The datasets are divided into small batches, then processed into the network. In the experiment, they resize the image to $60 \times 60 \times 1$ from the original size and use two convolution layers. The output of first convolution layer is the input for the next. After using suitable filters and the convolution process done, the rectified linear unit (ReLU) and Max pooling operations are carried out in each layer. The CNN framework architectures proposed performs feature extraction in just two convolution layers using a complex image.

Xu et al.[28] propose a deep learning approach to iris recognition using an iterative altered Fully Convolutional Network (FCN) for iris segmentation and a modified resnet-18
model for iris matching. The segmentation architecture is built upon FCNs that have been modified to accurately generate pixel-wise iris segmentation prediction. There are 44 convolutional layers and 8 pooling layers in this architecture. Two datasets (UBIRIS.v2 and CASIA-Iris-Interval) in this experiment where they show that generating a more accurate iris segmentation is possible by combining networks such as FCN and resnet-18. The results show that the architecture proposed outperforms prior methods on several datasets.

Le-Tien et al. [30] propose an iris-based biometric identification system using a modified CNN used for feature extraction combined with Softmax classifier. The system is based on the CNN model Resnet50 where the CASIA Iris Interval dataset is used as an input. The iris recognition consists of 2 separate processes: feature extraction and recognition. To obtain the normalized image with dimensions 100x100 and 150x150 pixels as the input image of CNN, the system starts by image preprocessing. During the image preprocessing, the system uses a threshold algorithm to estimate location of pupil regions and Hough transform after performing equalize histogram algorithm to calculate pupil center, pupil’s radius and iris boundary’s radius, iris boundary’s center. After image preprocessing, CNN and a Softmax classifier are combined to feature extraction and classification.

Şahin et al. [31] applied traditional and convolutional neural network based deep learning methods for iris-sclera segmentation. They compare performance on two distinct eye image datasets (UBIRIS and self-collected data). Their results show that deep learning based segmentation methods outperformed conventional methods in terms of dice score on both datasets. Our approach is different in the sense we design an iris-based authentication system instead.
<table>
<thead>
<tr>
<th>Work</th>
<th>Approach</th>
<th>Feature type</th>
<th>Performance (FP, FN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacut et al. [4]</td>
<td>Analysis of frequency of Iris images</td>
<td>Static</td>
<td>2.8%, 0%</td>
</tr>
<tr>
<td>Ratha et al. [5]</td>
<td>Splitting of data</td>
<td>Static</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Andreas et al.</td>
<td>Camera Photo Response Non-Uniformity (PRNU) Fingerprint</td>
<td>Dynamic</td>
<td>[0.21%-23.26%], [0.21%-23.26%]</td>
</tr>
<tr>
<td>Puhan et al. [19]</td>
<td>Liveness detection based on texture dissimilarity of Iris for contact lens</td>
<td>Static</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Adam et al. [9]</td>
<td>Liveness detection based on amplitude spectrum analysis</td>
<td>Static</td>
<td>N/A, 5%</td>
</tr>
<tr>
<td>Karunya et al.</td>
<td>Image Quality Assessment</td>
<td>Static</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Thavalengal [14]</td>
<td>Liveness detection based on multispectral information</td>
<td>Static</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Huang et al. [15]</td>
<td>Pupil constriction</td>
<td>Dynamic</td>
<td>0.3%-1.4%, N/A</td>
</tr>
<tr>
<td>Kanematsu et al.</td>
<td>Liveness detection based on variation of brightness</td>
<td>Dynamic</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Mhatre et al.</td>
<td>Feature Extraction and Encryption Using Bio-Chaotic Algorithm (BCA)</td>
<td>Static</td>
<td>N/A, N/A</td>
</tr>
<tr>
<td>Le-Tien et al.</td>
<td>Modified Convolutional Neural Network (CNN) for feature extraction combined with Softmax classifier</td>
<td>Static</td>
<td>4%, N/A</td>
</tr>
</tbody>
</table>
Table I shows a summary of related works and their characteristics, approaches, feature type, and performance measures (false positive and false negative rate). As illustrated, most works rely on static features of image, whereas we rely on dynamic response to light in the pupil area to generate iris code and subsequently the QR code.
Chapter III

Classifiers for Iris Detection System

In this section we discuss the two classifier that we use to detect iris patterns from images. These classifiers are Haar-Cascade and Local Binary Pattern. We choose these two classifiers as they are readily available with OpenCV development environment to access. Other classifiers can be used for evaluation as future work plan.

3.1 Haar-Cascade Classifier

Haar-cascade classifier is popular for iris detection as it can be trained to achieve higher accuracy. We rely on the classifier built in OpenCV platform to train 1000 positive samples images having eyes and 1000 negative sample images that are not related to eyes. More specifically, we configured the parameters of the classifier to achieve the highest level of accuracy to identify the iris region. The classifier is divided by three key contributors.

Integral Image: It allows fast computation and optimization to recognize objects of interests. For example, in Figure 2, the sum within D can be calculated using Equation (i).
In Equation (i), $W(D)$ represents the weight of the image and $L(i)$ is the value of color level at the $i^{th}$ point. The sum of pixel values over rectangular regions are calculated rapidly using integral images.

**Learning Features**: A minimum number of visual features are selected from a large set of pixels. Three common features are recognized: edge feature, line feature, and center-surround feature.

**Cascade**: It allows excluding background regions that are discarded based on integral image and learning features. The detection process generates a decision tree by boosted process (known as cascade). Figure 3 shows that each image is being processed by positive and negative images and having the similarity result by choosing True or False. The learning algorithm keeps matching to next available positive image until a match is found with a given image.
A positive result introduces the evaluation of second classifier which is adjusted to achieve high detection rates. A negative result leads to immediate rejection of images. Currently, the process uses Discrete Ada boost and a decision tree as basic classifier. The classifier builds a decision tree for the image environment. Cascade stages are built by training classifiers using Discrete Ada Boost [20]. Then it is adjusted for the threshold to minimize false negative rates. In general, a lower threshold yields to higher detection rates from positive examples and higher false position rates from negative examples. After the cascade classifier training is fully accomplished, it can be applied as a given reference to detect objects from new images.

3.2 LBP Classifier

Local Binary Patterns (LBP) [32] are visual descriptors for texture classification. It combines Histogram of Oriented Gradients (HOG) descriptor used for detection and recognition of objects. Figure 4 explains three neighborhoods to define texture and
calculate local binary pattern as per given steps. Steps for LBP cascade classifier feature
calculation is given below:

1. Divide the image under consideration into cells (small units). The more the cells, the
   more possibilities of detection.
2. Compare the pixel value of the center with each of the 8 neighboring pixels in a cell.
3. If the center pixel value is greater than the neighbor's value, consider "0". Otherwise,
   "1". This gives an 8-digit binary number.
4. Determine the histogram of the frequency of each "number" over the cell. This
   histogram can be seen as a 256-dimensional feature vector.
5. Concatenate histograms of all cells. This gives a feature vector for the entire window.

Like Haar-Cascade classifier, we trained LBP classifiers with a set of negative and positive
image samples. The feature vectors used were from OpenCV platform.

![Fig 4: Pixel calculated by LBP classifier](image-url)
Chapter IV.

Proposed Iris-Signature Generator Framework

At the heart of our proposed approach, we generate iris code using the classifiers discussed in Section III. The iris code is generated by enrolling real world users and the code is saved in a repository. The code is generated again from a new image during authentication for matching. We first discuss the authentication process followed by code generation process in subsections 4.1 and 4.2, respectively.

4.1 Authentication Process

Figure 5 shows the authentication process. In the proposed approach, there are two databases for each user; one for iris code and another for assigned user code. First, a camera is used to take images of the iris detection and recognition. Features are extracted from captured iris images and the user provides QR code (as a password). If there is a match between the iris of the user and the database of iris code, and user code matches the provided QR code, then the user is granted access.
4.2 Iris code and QR code generation

Here we discuss how we generate iris code (used as user ID) and the QR code (used as password) from given iris images. Figure 6 shows iris code generation process from live eye. Iris is the situated colored ring of muscle around the eye pupil which controls the diameter and the size of the pupil and the amount of light that could reach the retina. Using an iris scanner (a camera for scanning iris), a person’s eye is scanned. The data of the iris is unique to each person.

The camera takes a picture in infrared light. Most cameras (e.g., laptop camera) now support infrared lights have longer wavelengths than normal red lights and are not visible to the human eye. The infrared light helps to reveal unique features for dark colored eyes which cannot be detected by normal light.

Fig 5: Flowchart of iris code and QR code-based authentication
We implemented a prototype [32] using OpenCV [22] platform that detects iris region with pupil (using classifiers). Next, we identify the pupil area in the center of iris region and normalize the iris area image in black and white mode. We then subtract the iris area from the pupil area (which reflects the area based on pupillary response for current illumination level). An iris code is generated using the pupillary response area, which is a 512-digit number. The iris code is stored in the database for a new user during enrollment. It is checked for matching during the authentication process. For matching, we rely on Hamming distance between the two images. Hamming distance computes the number of dissimilar bits among two codes assuming the code length for both images is the same. For example, if image $A=1001$, and image $B=1100$, the $H(A, B) = 2$ (as the second and fourth bits of $A$ and $B$ are dissimilar).

One limitation of storing only iris code and relying on it for authentication is that the approach is vulnerable to presentation attack. If an attacker can obtain the printout of the iris image under correct illumination level, then the attacker would obtain access to the system. To prevent this, we generate a QR code to act as a password. Unlike traditional text-based password, the QR code is an image representation, it can be read by a reader.
and converted to a bit string to compare with known strings. We now discuss our proposed approach of generating the QR code. From the iris image, we separate the Red, Green, and Blue color planes. The color information is presented as matrix (Mat object in OpenCV [23]). We then generate Hash value by combining hashes for each of the planes as follows:

\[ H = H(R) \ XOR \ H(G) \ XOR \ H(B) \]

Here, H(R) is the hash generated from the Red color plane matrix, and XOR the Boolean operator. The length of the hash is 128 bits (16 bytes). We apply Message Digest (MD5) hash algorithm to generate hashes out of matrix information. We then generate a micro QR code using the hash information. A micro QR code can have 25 alphanumeric characters (for error correction level M [21]). The provided length is sufficient to our goal.
Chapter V.

Implementation and Evaluation

We implemented a prototype using OpenCV platform [32] to detect iris recognition and spoofing attack detection using the proposed framework. We collected a dataset of iris images from [18] to evaluate our approach. This dataset is commonly used by other literature works. It contains 2,854 images of authentic eyes and 4,705 images of the paper printouts collected from 400 sets of distinct eyes. The photographed paper printouts have been applied to successfully forge iris recognition system. For our evaluation, we randomly selected 300 samples from authentic eyes to train the classifiers, and then applied it to 200 samples of printed iris images.

Figure 6 shows a sample of images from the dataset where (a) real eye image, (b) printed image of the iris of same eye.

Figure 6: (a) real eye image (b) printed eye image from dataset

Figure 8 shows a set of results where (a) sample eye image, (b) iris recognition output of Haar-Cascade classifier (the yellow circle), and LBP classifier (red circle), (c) result of
iris center and its radius, (d) converting to iris code by normalization of the iris image.

Figure 9 shows a sample of QR code.

![QR Code](image)

**Fig 8: Screenshots of classifier output (top row) and iris code (bottom row)**

![Classifier Output](image)

**Fig 9: Screenshots of micro QR code**

### Table 2: Summary of Evaluation

<table>
<thead>
<tr>
<th>Classifier</th>
<th># of authentic samples</th>
<th>FP</th>
<th># of paper samples</th>
<th>FN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haar-cascade</td>
<td>300</td>
<td>4.5%</td>
<td>200</td>
<td>3.6%</td>
</tr>
<tr>
<td>LBP</td>
<td>300</td>
<td>5.7%</td>
<td>200</td>
<td>4.6%</td>
</tr>
<tr>
<td>Avg.</td>
<td>300</td>
<td>5.2%</td>
<td>200</td>
<td>4.3%</td>
</tr>
</tbody>
</table>
Table 2 shows a summary of the evaluation. Among 300 samples used for training, the reported false positive rate for Haar-cascade and LBP classifiers is 4.5% and 5.7%, respectively. The last row of Table II shows the average of Haar-cascade and LBP classifier FP rate (5.2%). The paper printed samples were replayed to test the system for attacks. The FN rate for Haar-cascade and LBP classifiers is 3.6% and 4.6%, respectively. The micro QR code could prevent this false acceptance of images as defense in depth. The underlying cause of FP and FN is due to classifier parameter tuning which can be improved further by considering large number of samples and other machine learning approaches.
Chapter VI.

Conclusions

Iris spoofing attacks have emerged as a significant threat against traditional iris-based authentication systems. In this thesis, an iris-based authentication framework has been developed which extracts iris patterns from live image followed by QR code. The information can be used to detect presentation attacks. The iris pattern recognition applied two common machine learning approaches namely Haar Cascade and Local Binary Pattern. A prototype tool using OpenCV library has been developed. The approach has been evaluated with a publicly available dataset and the initial results look promising with lower false positive and negative rates. The initial results look promising with lower false positive and false negative rates. The future work plan includes evaluating with more samples and employing other machine learning techniques.
References


[23] OpenCV Basic Structure, Accessed from
http://docs.opencv.org/2.4/modules/core/doc/basic_structures.html


Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, 2018, pp. 184-188.


[32] Adrian Rosebrock, Local Binary Patterns with Python and OpenCV,

[33] Iris Pupil Detection, https://github.com/mislam9/iris_pupil_detection