Spoofing and Security of Iris Biometrics

By-Sonam Dhadiwal

Abstract

Spoofing of iris biometric is a challenge to an iris feature of biometric system. There are numerous attacks and so a challenge to accept this system in real life scenario. In this paper we will discuss how spoofing is carried out by various methods and its effect on false acceptance and rejection rate. We will also see the security concern and implementation of few algorithms that reduces spoofing attack.

I. Introduction

Whenever people log onto computers, access an ATM, pass through airport security, use credit cards, or enter high-security areas, they need to verify their identities [1]. Biometric methods, which identify people based on physical or behavioral characteristics, are of interest because people cannot forget or lose their physical characteristics in the way that they can lose passwords or identity cards. Biometric methods based on the spatial pattern of the iris are believed to allow very high accuracy, and there has been an explosion of interest in iris biometrics in recent years. Using biometric feature (Iris) has been a core technology component in very large scale deployments such as the Indian UIDAI (Aadhaar) project. However despite many advantages including reliable identity recognition, iris biometric systems are highly vulnerable especially at the sensor level to various kinds of presentation attacks. Iris is one of the best and powerful methods of system verification. But the technology can be fooled by using the good print quality of an iris of a person for verification of a system. As the print quality is good it matches with the image in database and spoofing takes place.

II. Benchmarks and Methods of Spoofing

Iris spoofing benchmark.

1) Biosec: In this benchmark 50 users were considered and each user had 16 images.
(2 sessions * 2 eyes * 4 images). So a total of 50 * 16 =800 valid access images[3].To create spoofing attack there was a need to have good quality of images so the original images were taken and preprocessed to improve the quality and printed using high quality printer so that it looks similar to original image. Finally, the iris images were recaptured with same iris camera used to capture the original images.

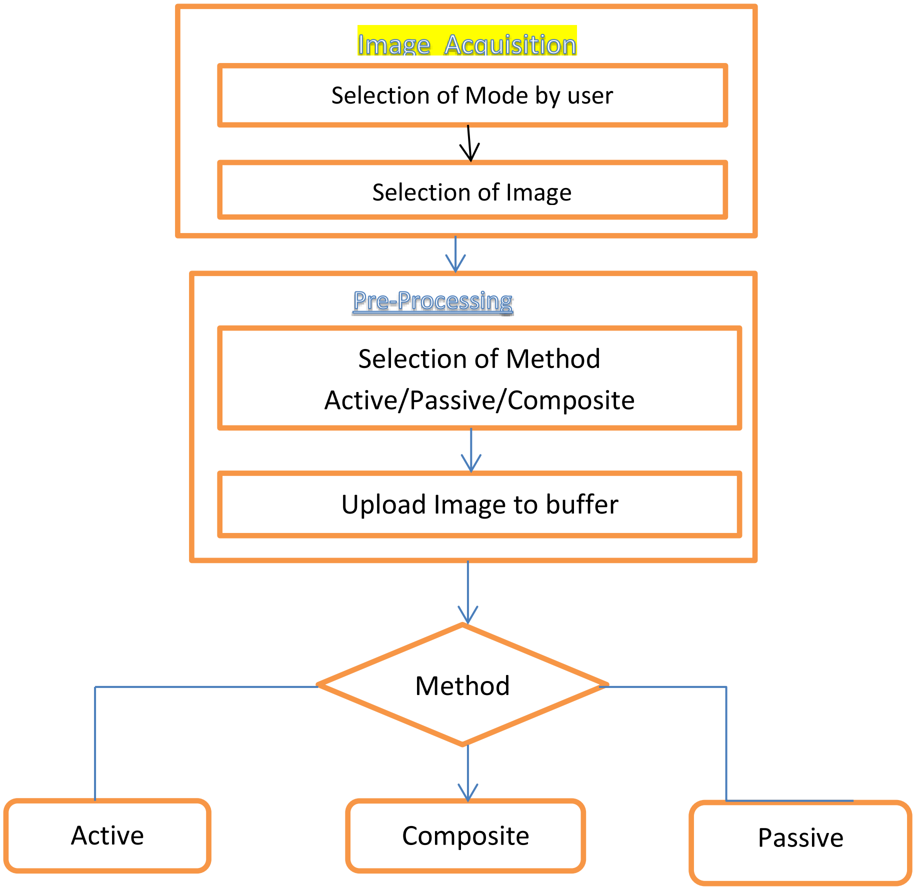
2)Warsaw: In this benchmark there were 237 volunteers and total of 1274 images with 729 spoofing attempts generated using high quality printer(HP LaserJet 1320 and Lexmark C534DN). Both real and fake images were captured by an Iris Guard AD100 biometric device.

3)MobBIOfake: In this benchmark the images were captured using mobile device and this images were edited by giving some contrast effects and then were printed with professional high quality printer and then used for spoofing.

In all above benchmarks less than half the data was used as training data and remaining data as testing data sample. In this way experiment was carried out and data was tested

4) Electronic Screen Attack Using iPad: In this attack normal samples are captured and used for enrollment. These samples are displayed using iPad. This attack will simulate the scenario where an attacker can get access to the biometric samples stored in the visible iris system that in turn are presented using electronic screen to subvert the system. We stored all normal samples in the iPad which is then fixed on the holder and presented to the visible iris sensor in a similar lighting condition as the normal (or real or live) samples were captured. Thus, this attack dataset is comprised of 110 × 5 = 550 samples representing all normal (or real or live) samples.

III. Diagrammatic representation of spoofed system[2]:



In image acquisition module image is acquired and in pre-processing module image is processed. It is the iris segmentation unit that extracts the iris accurately from eye image. The last module tests whether iris is fake or alive and then recognition is carried out by combination method

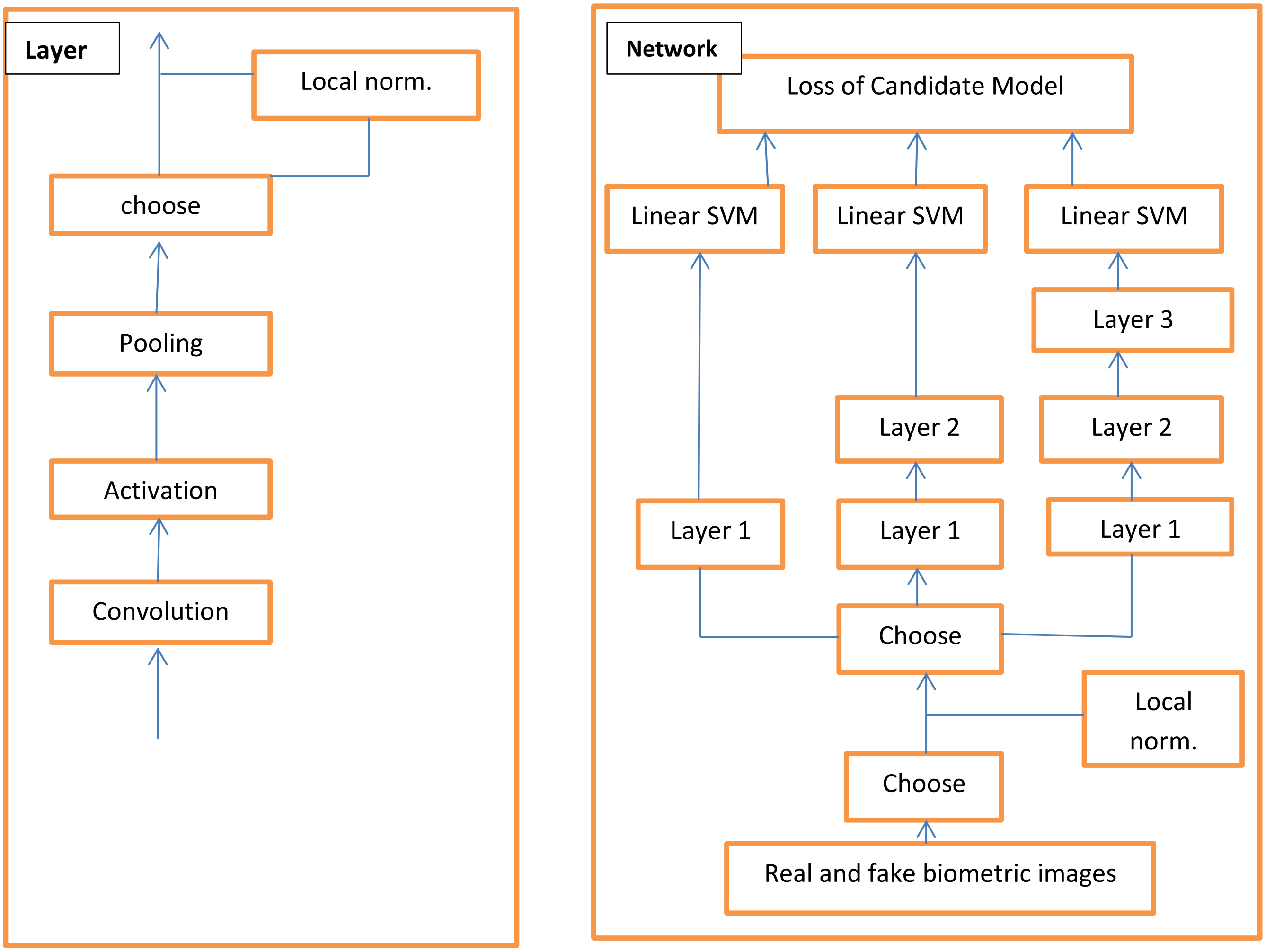
IV. Proposed Algorithm and Architecture:

This algorithm consists of two phases' liveness detection and iris verification phase [1]

liveness detection:This technique requires good hardware and software components. By considering following properties fake and real image can be distinguished. Real eye is image (degree of focus) is 3D and fake image is 2D. Pupil variation of two images

Iris verification: when both images are submitted we check the matching score using threshold value. If the score is >=85% accepted else rejected

Conclusion: increase in D increases security.



Operation	Hyperparameter	values

Convolution	Filter size
	Number of filters
		{3,5,7,9}
		{32,64,128,256}

Activation	------	

Pooling	Size
	Stride
	Strength
		{3,5,7,9}
		{1,2,4,8}
		{1,2,10}

Local norm.	Apply(yes/no)
	Size
		{yes/no}
		{3,5,7,9}

Diagram to the left indicate AO and to the right indicate FO

In this paper we will study architecture optimization (AO), filter optimization (FO) and how benchmark images are preprocessed.

Convolution: Convolution neural network is a part of Feature learning algorithm. In this network given image or extracted image is recognized to other tasks like segmentation, iris recognition, object detection etc. The image is fed to this algorithm and the algorithm detects best set of features from the image.

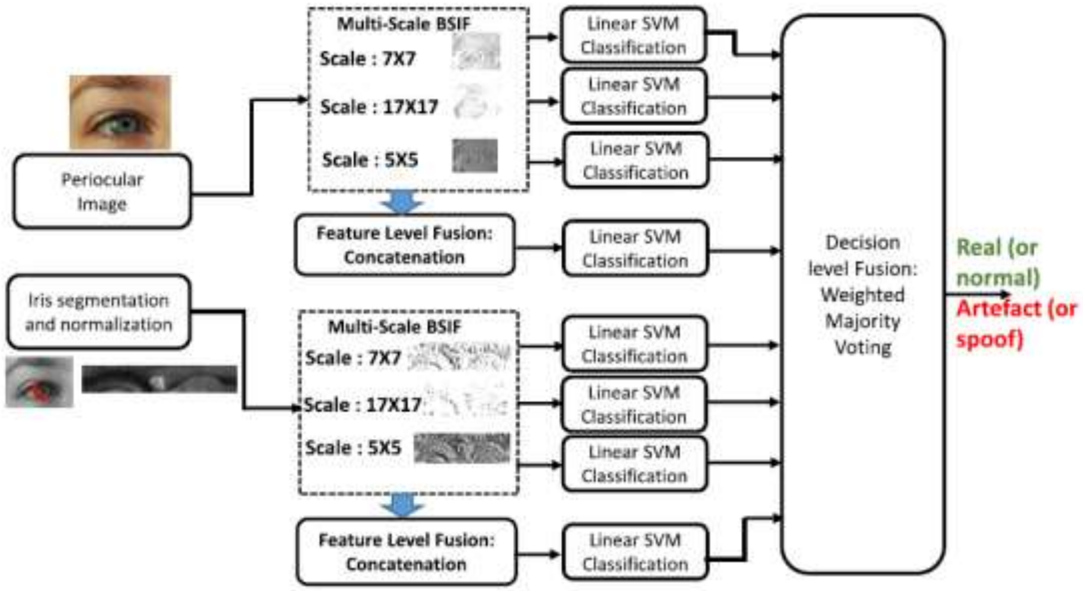
Activation: Difference between computational neuroscience models and machine learning neural network models can be bridged using rectified linear activation function.

Max (0, x) -> is the activation function.

This activation function of a node gives a single corresponding output node on series of inputs. This function contains number of functions in it like identity function, Binary step function, bipolar step function, sigmoidal function, Ramp function. Features from convolution are feed to activation function.

Pooling: spatial pooling is algorithm in which spatial parse machine kernel is used to classify the image. This method treats an image as collection of unordered appearance descriptors extracted from local patches, quantizes them into discrete visual words and then computes a compact histogram representation for semantic image classification, e.g. object detection or scene categorization.
Linear SVM: It is a machine learning algorithm that analyzes the data used for classification and regression analysis.

V. Security concerns[4]:


Periocular Image
Multi-Scale BSIF
Scale : 7X7
Scale : 17X17
Scale : 5X5
Linear SVM Classification
Linear SVM Classification
Linear SVM Classification
Feature Level Fusion: Concatenation
Linear SVM Classification
Iris segmentation and normalization
Multi-Scale BSIF
Scale : 7X7
Scale : 17X17
Scale : 5X5
Linear SVM Classification
Linear SVM Classification
Linear SVM Classification
Feature Level Fusion: Concatenation
Linear SVM Classification
Decision level Fusion: Weighted Majority Voting
Real (or normal)
Artefact (or spoof)

Proposed Presentation Attack Detection (PAD) Algorithm

Above figure shows the overview of the proposed PAD algorithm. Figure explores both periocular iris regions to accurately identify the presentation attacks on the iris recognition system. The proposed scheme can be structured in the following two important components namely:

1) Multi-Scale Binarized Statistical Image Feature Extraction (M-BSIF): This is unsupervised filter learning algorithm. It is widely used to learn a new filter by exploring the statistics from the natural images. These methods are alternative to the manually design filters like ICA. Use of ICA overcomes the tuning of large sets of hyper-parameters and can also provide a statistically independent basis that in turn can be utilized as the filter to extract the features from the given image. These learned filters represent each pixel of the given image as a binary string by simply computing its response to the learned filters. The binary code corresponding to the pixel can be considered as a local descriptor of the image intensity pattern in the neighborhood of pixel. Finally, the histogram of the pixels code values allow one to characterize the texture properties within the image sub-regions. Thus, the applicability of the BSIF especially for the visible iris presentation attack detection appears to be an elegant choice as it effectively captures the micro-texture information that can be used to detect the artefact. BSIF filters involves three main steps

(1) Mean subtraction of each patch

(2) Dimensionality reduction using Principle Component Analysis (PCA)

(3) Estimation of statistically independent filters (or basis) using Independent Component Analysis (ICA).

The use of M-BSIF will allow one to combine various filter responses that in turn extract not only a rich set of information but also allows one to generalize the BSIF for presentation attack detection of iris on both visible and NIR spectrum.

Generalization: Since M-BSIF filters are designed using a set of natural image patches, it overcomes the need of manual tuning of filter parameters. Furthermore, the use of pre-learnt filter will overcome the need of application specific learning. Finally, the use of multiple scales filters further captures the prominent information from the given image and thus best suited for different kinds of artefact detection. Thus, the M-BSIF forms the generic representation to address different kinds of iris artefacts in real-life scenario.

Statistical Independence*:* Since the filters are learned using ICA that can maximize the statistical independence between the learned filters and therefore ensures the effective information encoding.

Robustness: The use of multiple scales improves the robustness of the proposed scheme to both visible and near infrared iris presentation attack detection. It is observed that the use of large scale filter will capture the coarse texture information while the small scale filters will capture the micro texture information. Thus, combining this information in an effective manner will allow one to capture all distinctive information to identify the presentation attacks on the iris recognition system.

Decision Level Fusion*:* In this work, we employed 8 independent linear Support Vector Machine (SVM) classifiers corresponding to both iris and periocular biometrics whose decisions are combined using weighted majority voting as illustrated in the Figure below. Out of 8 different linear SVM classifiers, the first four are applied on periocular and the remaining four on the iris modality. Among four different linear SVM classifiers that are used on the periocular modality are distributed such that, one each is used on the three independent M-BSIF features and one on the feature level fusion of these M-BSIF features. Similarly, out of four linear SVM classifiers that were used on the iris modality, three classifiers are used on three independent M-BSIF features and one on the feature level fusion of M-BSIF features. The combination of all 8 SVM classifiers is illustrated in the Figure below. Each of these linear SVM classifiers is first trained using a set of positive (either with normal (or real) iris or periocular samples) and negative (or artefact or spoof) samples according to the standard protocol described for each of the database used in this work. Given a probe periocular sample *P*, we first extract M-BSIF features and perform the feature level fusion, which in turn is tested with their corresponding SVM classifier to obtain a decision as *DPk*, where $k = \{1, \ldots, 4\}$. A similar procedure is also carried out on the iris probe sample *II N* to obtain a decision *DIk*, where $k = \{1 \ldots 4\}$. We then combine these 8 decisions using weighted majority voting as follows:

$FD = NC$ max

k=1

NE

_

r=1

Where, *FD* denotes the fused decision,

Drk denotes the decision of the rth expert (either periocular or iris),

NE denotes the number of experts,

NC denotes the number of class to be combined and

wr denotes the weights.

In this work, weights wr for the individual classifiers (or experts) are computed according to their performance such that larger weights are assigned to the expert with high accuracy and vice-versa. The weight assignment scheme will consider the individual performance of the expert and depending upon their performance the method will compute the weights such that _r wr = 1. These weights are assigned on the development dataset from VSIA database and kept constant throughout our experiments.

VI. Effect of increasing and decreasing FAR and FRR of a system:

Iris is the pigmented, connective tissue that controls the pupil. Iris is formed in early life process and remains stable throughout life. So the pattern of iris is unique and it varies from person to person. Eye color is the color of iris. FAR is the false acceptance rate and FRR is the False Rejection Rate. If the original images shows match with fake image then it is said as falsely accepted and false acceptance rate is the ratio of total number of falsely accepted images to total number of images. Similarly if the original image does not match to its own image in database then it is called as falsely rejected. False Reject Rate is the ratio of falsely rejected images to total number of images.

Ideal FAR and FRR is zero. It is very difficult to achieve zero rates. If the FAR and FRR are increased it means the system is less secure and attack on system is not difficult. Less the FAR and FRR more secure the system.

There are some applications where security is most important priority than cost and other factors. For instance say application with government military weapons records. This system should be highly secured because if the enemy gets all the information then it may lead to disaster. So FAR and FRR should be zero. There are also some applications where security is not the priority. For instance say Wikipedia content on internet. It is publicly made available and doesn't matter if someone attacks the system. Here cost can be a factor of importance.

There are numerous biometric modalities. We have to choose that modality of system which is more suitable for our system. 1 chances in 10^{78} that iris pattern of two individual's match which is almost negligible. It is highly scalable as iris structure remains same throughout the lifetime. Also the template size is small so matching takes place at faster rate. The problem with this system is that it is relatively expensive but is most suitable and accurate where security is the highest priority. Another problem with this modality can be scanners can be fooled by high quality image. This is the biggest problem with many biometrics. There is constant efforts being put to make cell-phones secured and also tracing the attacker easily from this biometrics if system is attacked. Also multimodalities are used where application is security concerned. Fooling all modalities at the same time is too difficult .Also we can design scanners which detects fake image. Aadhaar card the biggest secured application has taken iris trait for recognition. Google uses iris scanners to control access to their datacenters.

From experiments we come to conclusion:

	Security		Practicality				
	Anti-forgery	Accuracy	Speed	Enrollment	Convenience	Cost	Size
Iris	Average	Good	Average	Average	Poor	Poor	Poor

Fig: Qualitative Measures of Biometric System

The above figure shows current measures of iris biometrics. Compromise between security and practicality will be uncomfortable and getting wrong comprised can lead to failure of a system.

References:

1) Hanaa Mohsin Ahmad, Bushra Jabbar Abdulkareem**-** Integrate Liveness Detection with Iris Verification to Construct Support Biometric System
Computer Science, University of Technology, Baghdad, Iraq

2) Fake Iris Detection: A Holistic Approach Rajesh Bodade Associate Professor FCE, MCTE Mhow, India Sanjay Talbar Professor SGGS IE&T Nanded, India

3) Deep Representations for Iris, Face, and Fingerprint Spoofing Detection
David MenottiY, Member, IEEE, Giovani ChiachiaY, Allan Pinto, Student Member, IEEE, William Robson Schwartz, Member, IEEE, Helio Pedrini, M

4)Robust Scheme for Iris Presentation Attack Detection using Multiscale Binarized Statistical Image Features.- R.Raghvendra and Christoph Busch vol.10 April 2015