2019

On Generative Adversarial Network Based Synthetic Iris Presentation Attack And Its Detection

Naman Kohli
West Virginia University, nakohli@mix.wvu.edu

On Generative Adversarial Network Based Synthetic Iris Presentation Attack And Its Detection

Naman Kohli

Thesis submitted to the
Benjamin M. Statler College of Engineering and Mineral Resources
at West Virginia University

in partial fulfillment of the requirements for the degree of

Masters of Science
in
Computer Science

Afzel Noore, Ph.D., Chair
Mayank Vatsa, Ph.D.
Richa Singh, Ph.D.

Lane Department of Computer Science and Electrical Engineering

Morgantown, West Virginia
2018

Keywords: Iris Recognition, Presentation Attack, Deep Learning

Abstract

On Generative Adversarial Network Based Synthetic Iris Presentation Attack And Its Detection

by

Naman Kohli

Human iris is considered a reliable and accurate modality for biometric recognition due to its unique texture information. Reliability and accuracy of iris biometric modality have prompted its large-scale deployment for critical applications such as border control and national identification projects. The extensive growth of iris recognition systems has raised apprehensions about the susceptibility of these systems to various presentation attacks.

In this thesis, a novel iris presentation attack using deep learning based synthetically generated iris images is presented. Utilizing the generative capability of deep convolutional generative adversarial networks and iris quality metrics, a new framework, named as iDC-GAN is proposed for creating realistic appearing synthetic iris images. In-depth analysis is performed using quality score distributions of real and synthetically generated iris images to understand the effectiveness of the proposed approach. We also demonstrate that synthetically generated iris images can be used to attack existing iris recognition systems.

As synthetically generated iris images can be effectively deployed in iris presentation attacks, it is important to develop accurate iris presentation attack detection algorithms which can distinguish such synthetic iris images from real iris images. For this purpose, a novel structural and textural feature-based iris presentation attack detection framework (DESIST) is proposed. The key emphasis of DESIST is on developing a unified framework for detecting a medley of iris presentation attacks, including synthetic iris. Experimental evaluations showcase the efficacy of the proposed DESIST framework in detecting synthetic iris presentation attacks.

Dedication

|| जय श्री राम ||

Dedicated to,
my parents Kavita and Adarsh,
my sister and brother-in-law Jalaj and Gaurav,
my loving nephew Nevaan,
my paternal grand-parents, Usha and Onkar,
and my maternal grand-parents, Krishna and Satya Pal

Acknowledgements

I would like to take the opportunity to thank the people who I have met during this phase of my career and who have helped me in achieving this degree. There are many whom I will be unable to mention here but do know, that each and every interaction has helped me in maturing and becoming the person who I am now. I would like to thank my committee members Dr. Afzel Noore, Dr. Mayank Vatsa, and Dr. Richa Singh as without their guidance, this thesis would not be possible.

Finally, I thank my **parents, sister, and brother-in-law** whose sacrifices and prayers deserve a special mention. My mother, **Kavita**, has always backed me to go for what I dream and has always kept a brave face on for me. My father, **Adarsh** whose resolute confidence in me has always guided me back to my path. My sister **Jalaj** has been a strength of pillar for me. I could not have reached this stage without their faith in me and their unwavering support. I also want to thank my relatives back in India who have always been considerate and ever ready to provide their guidance.

Contents

List of Figures

List of Tables

Publications

1. **Naman Kohli**, Daksha Yadav, Mayank Vatsa, Richa Singh, and Afzel Noore. *Synthetic iris presentation attack using iDCGAN*. In International Joint Conference on Biometrics, pages 1–7, 2017.

2. David Yambay, Benedict Becker, **Naman Kohli**, Daksha Yadav, A. Czajka, K. W. Bowyer, S. Schuckers, R. Singh, M. Vatsa, A. Noore, D. Gragnaniello, C. Sansone, L. Verdoliva, L. He, Y. Ru, H. Li, N. Liu, Z. Sun, and T. Tan. *Livdet iris 2017 - Iris liveness detection competition*. In IEEE International Joint Conference on Biometrics, pages 733–741, 2017.

3. **Naman Kohli**, Daksha Yadav, Mayank Vatsa, Richa Singh, and Afzel Noore. *Detecting medley of iris spoofing attacks using DESIST*. In IEEE International Conference on Biometrics Theory, Applications and Systems, pages 1–6, 2016.

4. David Yambay, Adam Czajka, Kevin Bowyer, Mayank Vatsa, Richa Singh, Afzel Noore, **Naman Kohli**, Daksha Yadav, and Stephanie Schuckers. *Review of iris presentation attack detection competitions*. In Handbook of Biometric Anti-Spoofing, pp. 169-183. Springer, Cham, 2019.

Chapter 1

Introduction

Traditional means of authentication require the use of passwords, identity cards or simple metallic keys. However, these methods may not prevent an intruder from obtaining unauthorized access and hence, circumventing the security of the system. On the other hand, biometric systems rely on the intrinsic physical or behavioral traits of an individual to establish their identity [13]. Biometric systems achieve this goal by utilizing traits such as fingerprint, iris, face, ear, or voice.

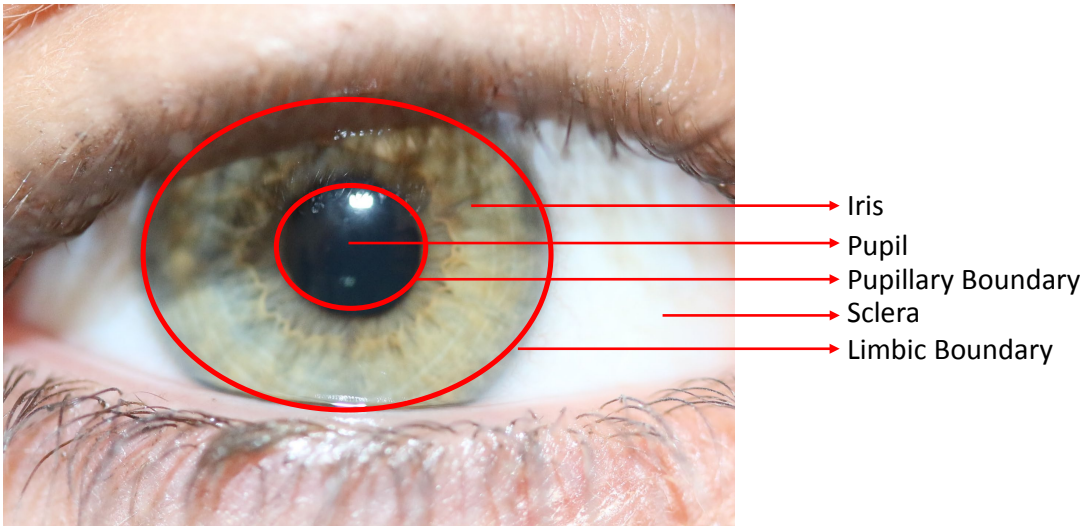

Figure 1.1: Anatomy of the human eye.

1.1 Iris as a Biometric Modality

Iris is considered one of the most reliable and accurate biometric modalities due to the highly unique character of iris tissue texture. Figure 1.1 shows the different parts of the human eye along with the iris. The majority of iris recognition systems operate in the near-infrared (NIR) spectrum (as opposed to the visible spectrum) because NIR light does not excite the pupil which minimizes the pupil dilation and the texture of dark-colored irides is better captured in the NIR spectrum [14].

A typical biometric system consists of the acquisition sensor, pre-processing unit, feature extractor, database, and matcher modules [15]. For iris recognition, the image acquisition module captures the iris image using a NIR sensor. The pre-processing unit enhances the input iris image for segmenting the actual iris region. Next, the normalization is performed which converts the segmented iris image into a normalized iris image space. The feature extractor module extracts relevant iris features (such as Hamming code) and encodes them as a template. The matcher module compares the input/query iris features with the gallery templates to compute a match score. Figure 1.2 shows the diagram of a typical iris recognition system.

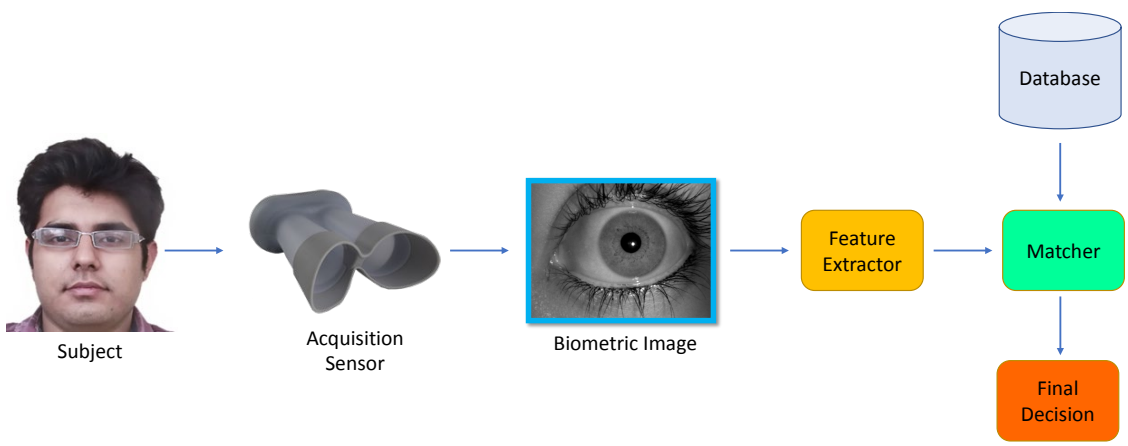

Figure 1.2: Block diagram of a typical iris recognition system.

The first successful iris recognition algorithm was patented by John Daugman [16]. The key idea of Daugman's algorithm was a test of statistical independence of the phase of Gabor wavelets fitted on a grid of locations superimposed on a pseudo-polar transformation of the iris texture. His algorithm has been the dominant and most popular iris recognition method for years. It has been used successfully in numerous applications such as border control, national ID projects such as Aadhar, and access control.

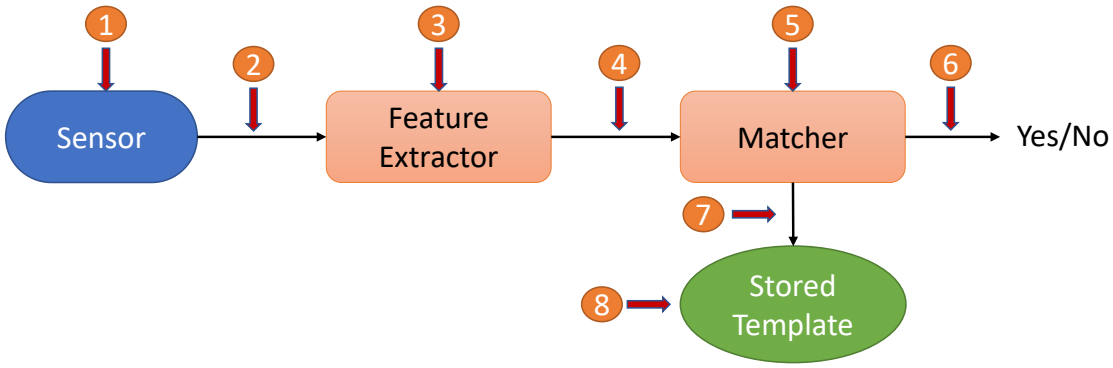

Figure 1.3: Avenues for attack in a biometric pipeline [1].

1.2 Presentation Attacks in Biometrics

Even though biometric systems are being widely used worldwide, Ratha et. al. [1] presented several avenues of attack on a biometric system and suggested different steps to mitigate such attacks. Figure 1.3 showcases the vulnerable areas in the traditional biometric pipeline. One potential points of attacks in a biometric system is the transmission channel between the sensing device and the feature extraction module [1]. A man-in-the-middle attack on this channel can be utilized to replace the original image with a new synthetic image before the template extraction process. More importantly, one of the avenue of attack is through presentation attacks at sensor level which can be used both for identity impersonation and identity evasion. The consequences of such an attack maybe wide-ranging as an individual may enroll with different identities and avail facilities associated with the unique identity multiple times.

Presentation attacks have been widely studied in the field of face and fingerprint biometrics. With the increasing usage of face authentication systems, presentation attacks are becoming a serious point of concern, particularly for unmanned applications such as ATM machines. As faces are easy to acquire without the subject's consent or awareness, impersonating someone's identity is easy [17]. With faces, impostors can present to the acquisition sensor a photo or a digital video [18]. Similarly, identity hiding is also less challenging with the usage of 3D hard masks [19] or more sophisticated silicone masks [20]. With respect to fingerprints, the most common presentation attack consists of using artificial replicas [21] of valid subjects. This can be achieved using a cooperative method or non-cooperative method. In the cooperative method, the user provides an impression of their fingerprint to replicate their finger-

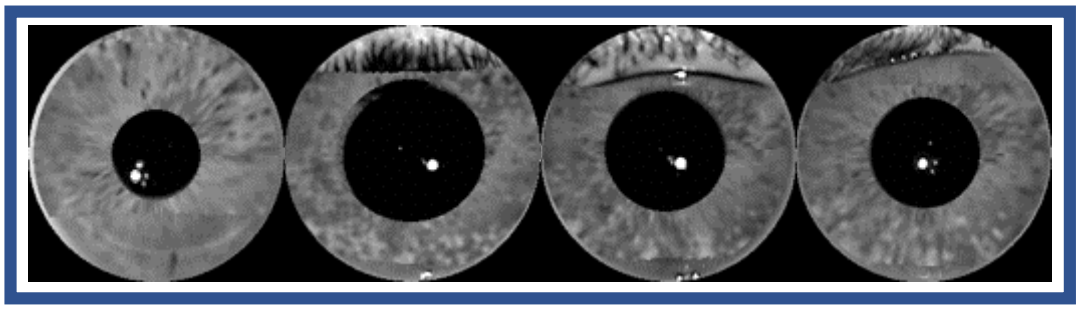

Figure 1.4: Sample images from Synthetic Database [2].

print with various materials such as gelatin, latex or silicone. On the other hand, in the non-cooperative method, a latent fingerprint may be enhanced to create a mold.

Presentation attacks on iris modality can be divided into two subsets: physical attacks and synthetic attacks. Physical presentation attacks include textured contact lenses [22, 23] and print attacks [24] and have been widely explored in the literature. Synthetic iris presentation attacks are conducted by synthetically generating iris [2]. The idea of generating synthetic iris images was initially introduced by Cui et al. [25] with the intention of increasing the number of available iris images for developing iris recognition algorithms. Figure 1.4 shows sample synthetic iris images from Synthetic DataBase (SDB) by Galbally et al. [2]. In the next section, we look at the problem of synthetic generation of images in biometrics which can be used as a presentation attack to spoof a biometric sensor.

1.3 Synthetic Image Generation in Biometrics

Earlier, the purpose of generating synthetic biometric samples was to supplement the number of publicly available images. An advantage of this was circumventing privacy concerns as these synthetic samples were not directly related to a particular person. However, with the introduction of new deep learning based techniques such as generative adversarial networks and their ability to create *real looking* synthetic images, these images may be utilized as presentation attacks for various biometric systems.

Cappelli et al. [26] introduced the problem of synthetically altered fingerprints and they used the SFinGe framework for generating artificial fingerprints. With respect to fingerprint presentation attacks, the idea of *masterprint* [27] was introduced

which consisted of creating synthetic fingerprints which match with one or more of the stored templates of various users in the database. Moreover, Ferrara et al. [3] explored the possibility of creating a new fingerprint by combining features from two different fingers. In this manner, the synthetic fingerprint has a high probability of falsely matching with the fingerprints from the source prints. Fake/synthesized face generation has received exceptional attention due to the advancement in generative adversarial networks. These generative adversarial networks are based on competition between two convolutional neural networks: discriminator and generator, to generate realistic synthetic face images.

Similar to face and fingerprint biometric modalities, different researchers have proposed various techniques to generate synthetic iris images. Shah and Ross [9] employed Markov Random Field to generate initial texture of the iris images followed by embedding iris features such as radial and concentric furrows to create the final synthetic iris image. Zuo et al. [28] developed an anatomy-based model to create new irises similar to real-world iris images. Galbally et al. [2] reconstructed synthetic iris images from the feature template to successfully match the original genuine iris image. However, it is seen that these images do not resemble real iris images and appear *fake*.

1.4 Contributions of the Thesis

In this thesis, we propose a new iris presentation attack by synthesizing iris images through a deep convolutional generative adversarial network. As described earlier, recently, improvements in techniques such as generative adversarial networks and variational autoencoders have provided a breakthrough in generating new images. These approaches have paved the path for generating realistic looking synthetic images for different applications. In this thesis, we have proposed a novel synthetic iris image generation method using the generative adversarial network and demonstrated that it can attack iris recognition systems. Additionally, a novel presentation attack detection algorithm has been proposed to detect multiple iris presentation attacks including synthetic iris presentation attack. The major contributions of this thesis are:

- A novel domain-specific generative adversarial network (GAN) named as iDC-GAN for generating synthetic iris images is proposed. We adapt deep convolutional generative adversarial network by utilizing iris quality assessment for

synthesizing realistic looking iris images.

- Analysis is performed using quality score distributions of real and synthetically generated iris images to understand the effectiveness of the proposed approach. We also demonstrate that synthetically generated iris images can be used to attack existing iris recognition systems.
- We propose a novel framework utilizing structural and textural features to detect multiple iris presentation attacks, including synthetic iris.
- Evaluation using the proposed iris presentation attack detection algorithm is performed to ascertain its efficacy in distinguishing synthetically generated images from real images.

1.5 Organization of the Thesis

In the next chapter, the literature review of synthetic presentation attacks in biometrics and iris presentation attacks is presented. Chapter 3 describes the technique for synthetic iris presentation attack using the proposed iDCGAN (iris Deep Convolutional Generative Adversarial Network). Chapter 4 presents a novel framework utilizing structural and textural features to detect multiple iris presentation attacks, including synthetic iris images. Finally, in Chapter 5, conclusion and future work of this thesis are presented.

Chapter 2

Literature Review

Synthetic biometrics is defined as artificially generated biometric data, which exhibits meaningful biological characteristics and thus, can fool existing biometric sensors. The advancement in generative modeling algorithms has led to a variety of frameworks in generating synthetic images in the field of biometrics. The subsequent sections in this chapter focus on the literature of generating synthetic biometric images and presentation attacks in iris recognition.

2.1 Synthetic Presentation Attack in Biometrics

Previously, the focus of generating these synthetic biometric images was for increasing the count of images alongside publicly available databases. These synthetic images also helped in reducing privacy constraints as they were not directly linked to any physical identity. However, with the generation of realistic looking images, the focus has shifted to the usage of these images for presentation attack. The synthesis process of generation has been seen across all three biometric modalities: fingerprint, face, and iris.

The problem of synthetically altered fingerprints was introduced by Cappelli et al. [26] and they proposed the SFinGe framework for generating artificial fingerprints. Since then, different approaches have been introduced to generate synthetic fingerprints. Zhao et al. [29] utilized statistical models to generate realistic fingerprint images. Johnson et al. [30] used texture characterizing features such as ridge intensity along the ridge center-lines with seven frequency components, ridge width, ridge cross-sectional slope, ridge noise, and valley noise for creating new fingerprint images. With respect to presentation attack, the concept of master print [27] has been intro-

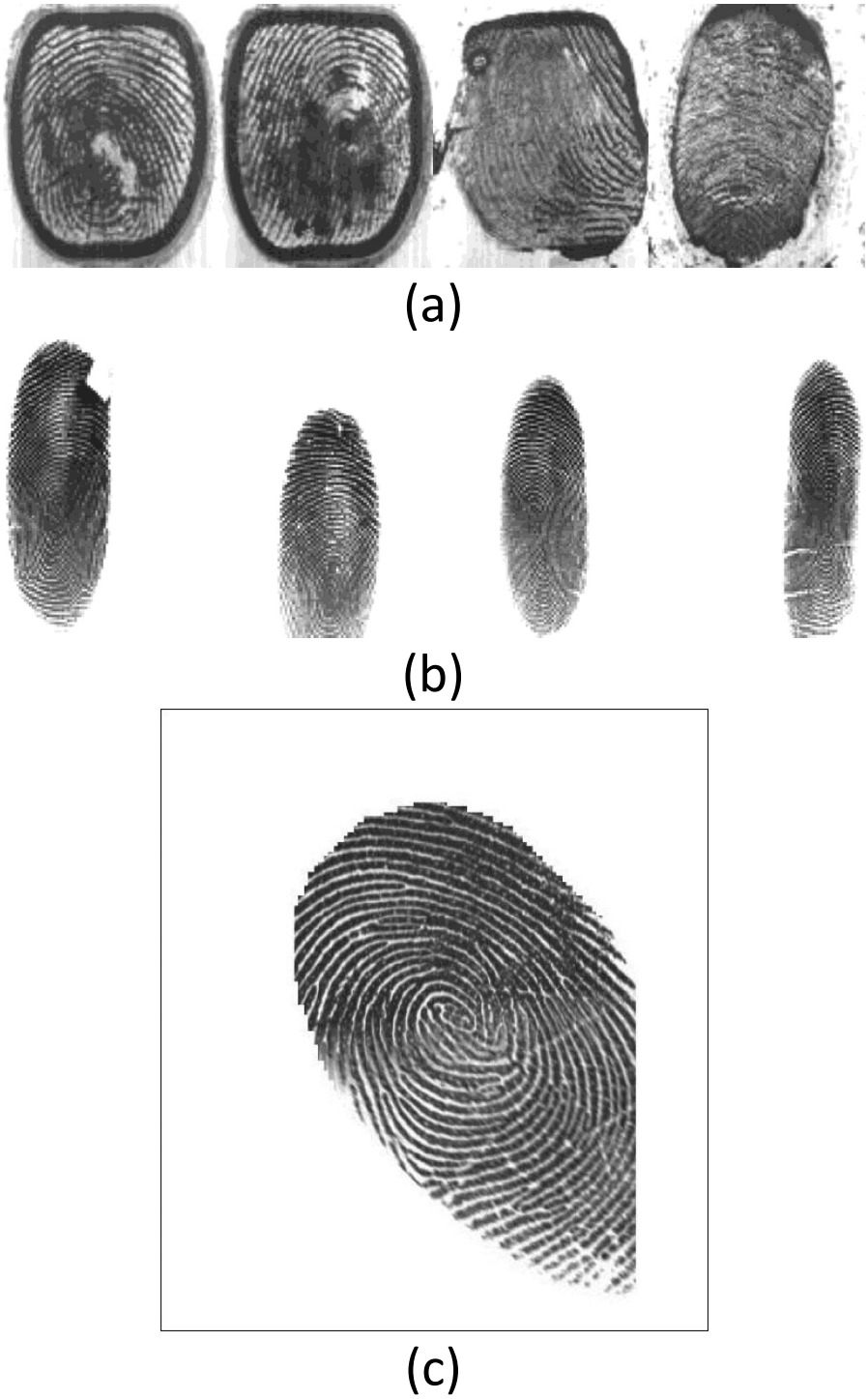

Figure 2.1: Sample images depicting different types of synthetic fingerprints: (a) LivDet 2013, (b) CASIA DB and (c) Joint fingerprint created from two fingerprints [3]

duced which consist of creating a synthetic fingerprint that matches one or more of the stored templates for a significant number of users. Ferrara et al. [3] have also explored the feasibility of creating a fingerprint combining features from two different fingers so that it has a high chance to be falsely matched with fingerprints from both fingers and reported successful results. Figure 2.1 showcases different types of synthetic fingerprints produced in the literature.

Different approaches have been proposed to simulate aging in faces [31, 32]. However, synthesis of faces has received tremendous amount of interest due to advancement in generative adversarial networks. Generative adversarial networks rely on competition between two networks - discriminator and generator to generate realistic images. The goal of the discriminator network is to identify whether an input face image is real or fake while the goal of the generator network is to generate realistic looking images that should be able to fool the discriminator.

Radford et al. [4] presented a deep convolutional neural network in a generative adversarial network framework. They removed max-pooling layers and showed realistic looking images for different databases including faces. Berthelot et al. [6] proposed an equilibrium enforcing method paired with a Wasserstein loss distance function.

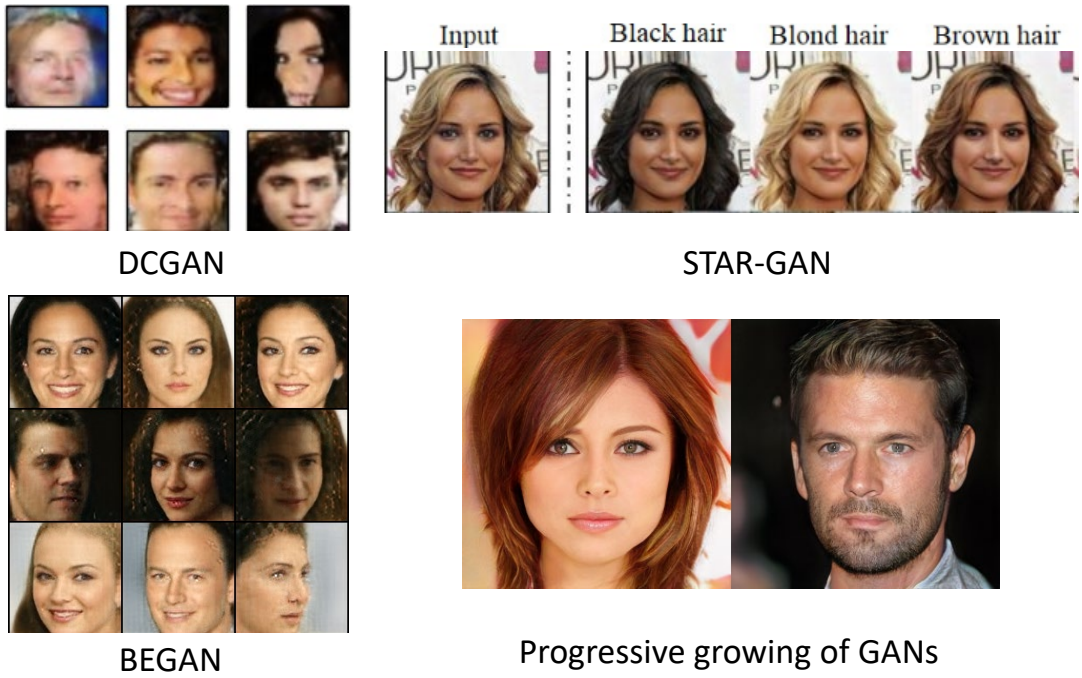

Figure 2.2: Sample images depicting synthetic faces generated from different types of generative adversarial networks. Image source: [4], [5], [6], and [7].

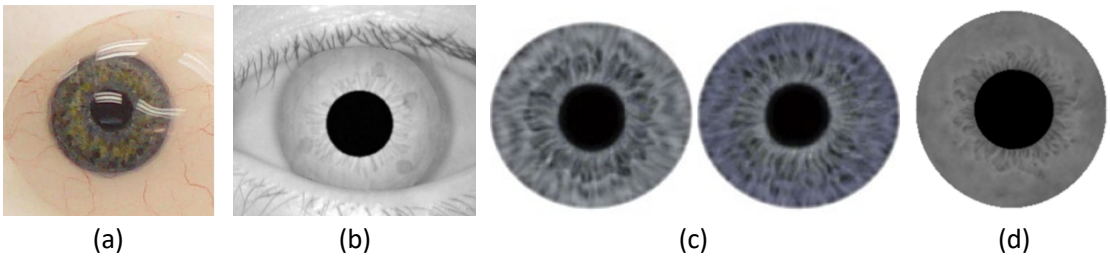

Figure 2.3: Sample images depicting synthetic irises: (a) Lefohn et al. [8], (b) Shah and Ross [9] , (c) Cardoso et al. [10], and (d) Wei et al. [11] .

Choi et al. [5] introduced STAR-GAN, a scalable image-to-image translation model among multiple domains using a single generator and a discriminator. Finally, Karras et al. [7], showcased a new methodology for training generative adversarial networks by progressively growing both the generator and discriminator networks. Figure 2.2 displays the synthetic faces generated by these network models.

Similar to the other face and fingerprint biometric modalities, several authors have proposed new techniques to generate synthetic iris images. Lefohn et al. [8] proposed a method to create a fake eyeball that matches the texture of a real human iris. Other researchers [9, 28] have proposed texture based and model-based methods to generate iris patterns followed by artificially adding other eye regions. More recently, Cardoso et al. [10] described a stochastic method to synthesize ocular data. Figure 2.3 showcases examples of synthetic iris images found in the literature.

Particularly, the idea of generating synthetic iris images was initially introduced by Cui et al. [25] with the intention of increasing the number of available iris images for developing iris recognition algorithms. They employed principal component analysis and super-resolution techniques to create new images for iris synthesis. Shah and Ross [9] generated the initial texture of the iris images by utilizing Markov Random Field. Other iris features such as radial and concentric furrows were embedded to create the final synthetic iris image. Zuo et al. [28] developed an anatomy-based model for generation of realistic iris images. Galbally et al. [2] used the feature template to reconstruct synthetic iris images where the main goal was to match the generated iris image to the original genuine iris image.

2.2 Iris Presentation Attack

The success of large-scale iris recognition based identity application has increased its susceptibility to individuals who, by means of presentation attack or spoofing, can

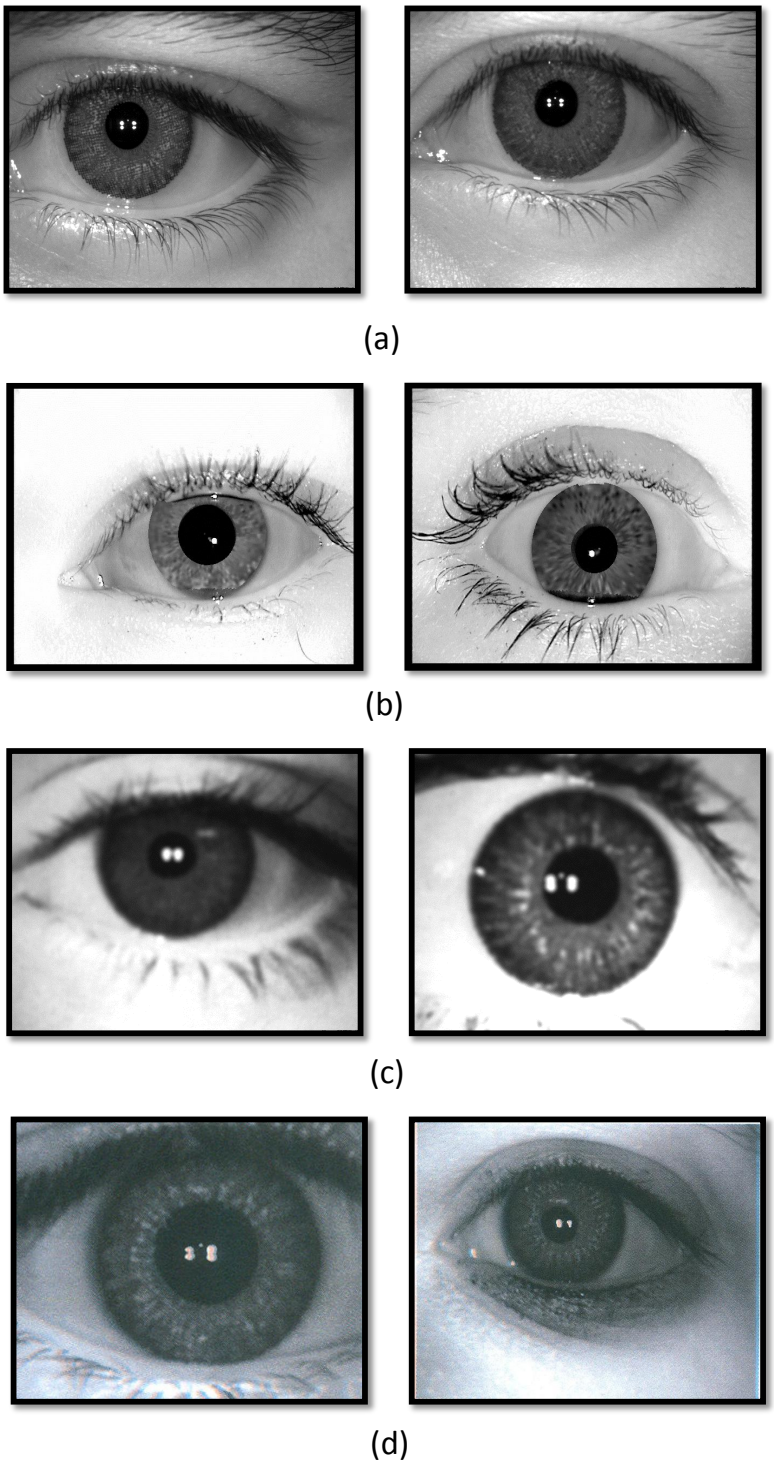

Figure 2.4: Sample images depicting different types of presentation attacks: (a) textured contact lens, (b) synthetic iris, and (c) and (d) print attack

gain unauthorized access to locations or escape recognition as a person of interest. Detecting such presentation/spoofing attacks has become a key objective in designing such systems and is the topic of ongoing standards efforts, e.g. ISO/IEC 30107-1:2016. Presentation attacks in iris modality can be divided into physical attacks and synthetic attacks. Some typical iris presentation attack methods are illustrated in Figure 2.4 and briefly described herewith:

- Printed Iris Images: This physical attack is easiest to instigate as it involves presenting an image of a real iris to the sensor. The image could be a scanned or printed copy of the original iris/eye image that can be used with the intention of impersonating another person's identity. Using a good quality paper, printer and high-resolution iris images, spoofed iris images can be generated to exploit recognition systems [33]. The study by Gupta et al. [24] had shown that both print+scan and print+capture attacks can reduce the verification accuracy to less than 10% at 0.01% false accept rate (FAR).

- Textured Contact Lenses: With the advances in technology and low costs, contact lenses are gaining popularity around the world. Apart from being used for eyesight correction, they are increasingly being used for cosmetic purposes as well. These textured (cosmetic) lenses cover the original texture of the iris with a thin textured lens which can severely degrade the performance of iris recognition systems. Several studies [34, 22, 23, 35] have demonstrated the need for detecting contact lenses as both transparent (soft) and textured (cosmetic) lenses have been shown to affect iris recognition systems.

- Synthetic Iris Images: Venugopalan and Savvides [36] described a novel presentation attack by creating synthetic "natural" iris images that can fool iris recognition systems. They embedded features in the iris to spoof another person's iris and assumed that the feature extraction mechanism of the iris system is known. Galbally et al. [37] proposed a genetic algorithm based synthetic iris creation technique. Their probabilistic approach generated iris-like pattern whose corresponding iriscode matched with a genuine user. Table 2.1 summarizes publicly available iris databases that consist of synthetic iris images.

Table 2.1: Databases for synthetic iris images.

Database	Unique Iris		Num Samples	
	Real	fake	Real	fake
Synthetic Iris Texture Based [9]	0	1000	0	7000
Synthetic Iris Model Based [28]	0	10000	0	160000
CASIA-Iris-Syn-V4 [11]	0	1000	0	10000
CASIA-Iris-Fake [38]	1000	815	6000	4120
IIITD Combined Spoofing Database [39]	1744	2000	9325	11368

2.3 Iris Presentation Attack Detection

Several studies in the literature have been published to detect these presentation attack in iris images as shown in Table 2.2. In their paper, Sun et al. [38] developed a new synthetic database, CASIA-Iris-Fake, and demonstrated the performance of their algorithm, Hierarchical Visual Codebook (HVC) which is based on textural analysis. The HVC method utilizes a mixture of two Bag-of-Words models, Vocabulary Tree and Locality-constrained Linear Encoding. They showcased the performance of their algorithm on iris liveness detection as well as race classification.

Akhtar et al. [12] proposed LUCID descriptor and evaluated its efficacy on ATVS-FIr database of printed iris images. Gragnaniello et al. [40] investigated different local descriptors such as LBP, BSIF, LPQ, DAISY etc for their effectiveness in capturing the differences between real and fake biometric samples. They concluded that local descriptors work surprisingly well in such tasks.

Silva et al. [41] introduced a three layer convolutional neural network to detect images with textured contact lens. They showcased an improvement of 30% over the state-of-the-art algorithm on two iris databases. Komogortsev et al. [42] perform iris liveness detection at the feature and match score levels for several existing forms of eye movement biometrics such as fixations and saccades. Their results concluded that eye movement biometrics are highly resistant to circumvention.

Menotti et al. [43] focus on designing optimal deep neural networks by optimizing search space in figuring out the topology and optimizing filters for detecting presentation attacks. They showcase improvement in results across all three biometric modalities: face, fingerprint and iris. Doyle and Bowyer [44] proposed BSIF features for detection of textured contact lenses in iris images. Raghavendra and Busch [45] proposed a multi-scale binarized statistical image feature (m-BSIF) on iris and periocular images along with linear support vector machines to detect image print attack and screen attack.

Table 2.2: Selected software-based iris presentation attack detection algorithms proposed in the literature since 2014.

Year	**Authors**	**Algorithm**	**Attack**
2014	Sun et al. [38]	Hierarchical visual codebook	Print, Lens, Synthetic
2014	Akhtar et al. [12]	LUCID	Print
2015	Gragnaniello et al. [40]	Combination of local descriptors	Textured contact lens, print
2015	Silva et al. [41]	Convolutional neural network based representation learning	Textured contact lens
2015	Komogortsev et al. [42]	Feature-level and score-level liveness detection	Replay
2015	Menotti et al. [43]	Deep learning and filter optimization based framework	Print
2015	Doyle and Bowyer [44]	Local texture descriptors	Textured and transparent contact lens
2015	Raghavendra and Busch [45]	Multiscale Binarized Statistical Features	Textured contact lens
2016	Raja et. al [49]	Adaptive texture patterns computed by local microfeatures and globalspatial features	Print
2016	Hu et al. [46]	Regional feature computation via spatial pyramid and relational measure features	Textured contact lens, Print
2018	Yadav et al. [47]	Alexnet based deep features	Textured contact lens
2019	Kuehlkamp et al. [48]	Ensemble of multi-view learners	Textured contact lens, Print

Hu et al. [46] utilized spatial pyramid based features and feature level convolutional operators for relational measures to detect iris presentation attacks. Yadav et al. [47] introduced a large textured contact lens iris database in unconstrained environment and showcased the effectiveness of deep learning features in detecting such presentation attacks. Kuehlkamp et al. [48] combined lightweight CNNs to classify multiple views of BSIF features in order to categorize presented iris image as real or spoofed.

However, most of the algorithms, focus on detecting a single type of iris presen-

tation attack. Thus, it is important to design an algorithm that can detect multiple types of iris presentation attacks which depicts a realistic scenario. In the next chapter, we present a novel way to generate synthetic iris images and compare them with real iris images with respect to iris quality measures. Subsequently, we showcase a novel iris presentation attack detection algorithm that can detect multiple types of iris presentation attacks.

Chapter 3

Synthetic Presentation Attack using Generative Adversarial Networks

The advent of deep learning algorithms has led to state-of-the-art results in discriminative tasks in various research areas such as image classification, face verification, and speech recognition. On the other hand, deep generative models have had limited success due to intractable probabilistic computations arising in maximum likelihood estimation. However, improvements in techniques such as generative adversarial net-

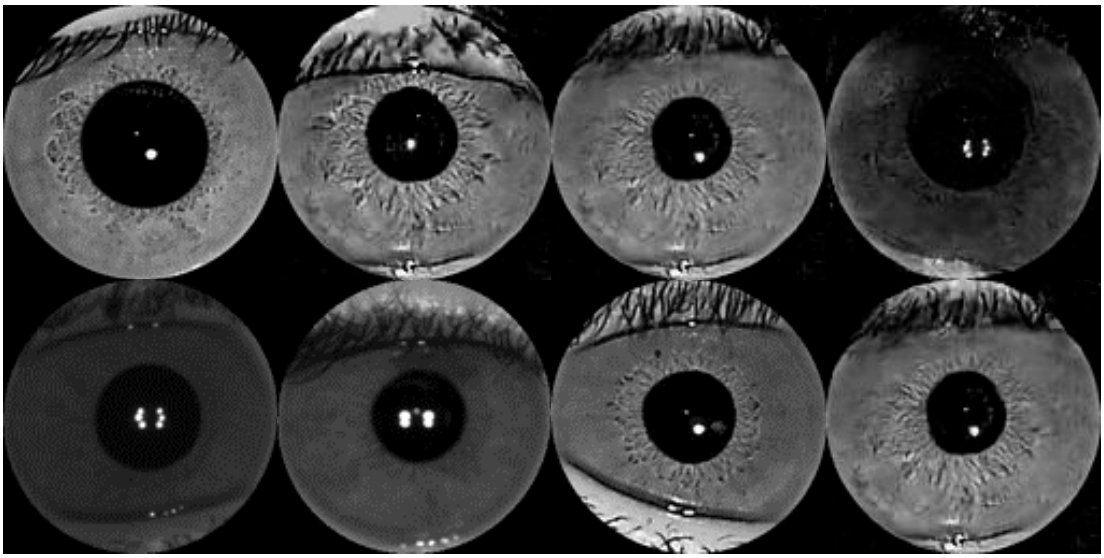

Figure 3.1: A mixture of real and synthetic iris images generated from the proposed iDCGAN framework are shown above. We encourage the readers to identify which of these iris images are real and synthetic. The solution is shown in Figure 3.10 at the end of this chapter.

works [50] and variational autoencoders [51] have provided a breakthrough in generative modeling.

Generative adversarial networks have paved the path for generating realistic looking synthetic images for different applications. In this thesis, a new iris presentation attack is proposed by synthesizing iris images through a deep convolutional generative adversarial network. It is also demonstrated that these novel iris images can be utilized to attack iris recognition systems. The major contributions of the chapter are:

1. A novel domain-specific generative adversarial network (GAN) named as iDCGAN for generating synthetic iris images is proposed. We adapt deep convolutional generative adversarial network by utilizing iris quality assessment for synthesizing *realistic looking* iris images.

2. Analysis is performed using quality score distributions of real and synthetically generated iris images to understand the effectiveness of the proposed approach.

3. We also demonstrate that synthetically generated iris images can be used to attack existing iris recognition systems. A merit of the proposed framework as compared to Galbally et al. [2] is that there is no requirement of binary feature templates for creating the synthetic iris images using the proposed framework.

3.1 Synthetic Iris Image Generation Framework

In this thesis, we adapt the generative adversarial network for synthesizing realistic iris images to propose iris Deep Convolutional Generative Adversarial Network (iDCGAN). Figure 3.2 shows the steps involved in the proposed approach.

3.1.1 Generative Adversarial Network

Goodfellow et al. [50] introduced the concept of generative adversarial networks (GANs) where the generative model is pitted against an adversarial *discriminator* to generate representations which cannot be differentiated by the discriminator. The aim of the *generator* is to learn the probability distribution of the input data perfectly enough to *fool* the discriminator.

Let $\mathbf{x}$ be the input data which has a true probability distribution $p(\mathbf{x})$. Let $\mathcal{G}$ be the generative network which takes an input latent vector $\mathbf{z}$, drawn from a noisy

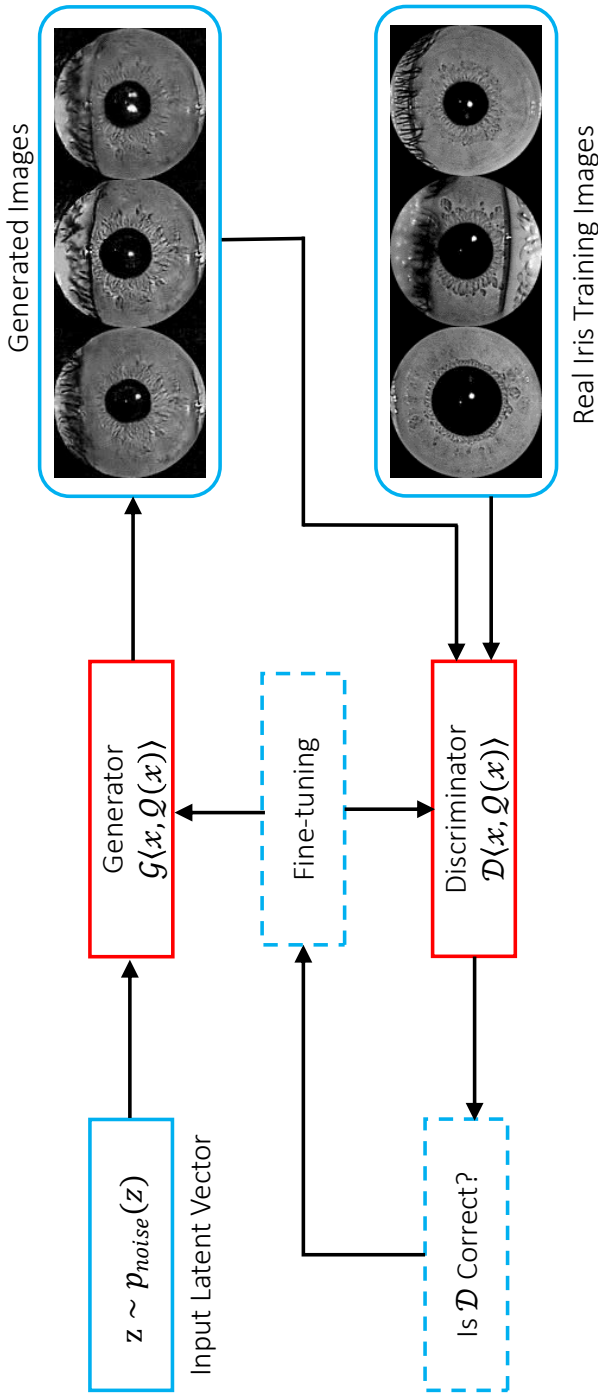

Figure 3.2: Illustrating the proposed iDCGAN framework for generating synthetic iris images.

probability distribution $p_{noise}(\mathbf{z})$ and outputs a new image $\bar{\mathbf{x}}$. Then, the discriminator network $\mathcal{D}$ has to discern if the input image, randomly chosen from $\mathbf{x}$ or $\bar{\mathbf{x}}$, is generated from the true probability distribution $p(\mathbf{x})$ or not. The two models are trained using a minimax objective and the loss function L is shown in Eq. 3.1.

$$\begin{aligned} L = \min_{\mathcal{G}} \max_{\mathcal{D}} \mathbb{E}_{\mathbf{x}\sim p(\mathbf{x})}[log(\mathcal{D}(\mathbf{x}))] \\ + \mathbb{E}_{\mathbf{z}\sim p_{noise}(\mathbf{z})}[log(1-\mathcal{D}(\mathcal{G}(\mathbf{z}))] \end{aligned} \tag{3.1}$$

A number of variants of GANs have been introduced such as conditional GANs [52], Laplacian GANs [53], and InfoGANs [54]. These variants have been successfully utilized in image inpainting [55], style transfer [56], and super-resolution [57] applications. Shrivastava et al. also proposed SimGAN [58] which uses a refiner network to improve appearance of synthetically generated eye images to make them indistinguishable from real eye images.

3.1.2 Proposed iDCGAN for Iris Image Synthesis

Radford et al. [59] introduced deep convolutional generative adversarial networks (DCGAN) for unsupervised learning of features by utilizing convolutional neural networks as the generator and discriminator network. They also applied constraints on architectural topology of convolutional neural networks in the generator and discriminator networks for stable training. Specifically, pooling functions were replaced with strided convolutions which allowed the resultant network to learn its own spatial upsampling. Additionally, the fully connected layers at the top of convolutional neural networks were removed and batch normalization was utilized for improving model stability by normalizing each unit to have zero mean and unit variance.

In this thesis, we propose an extension to DCGAN by utilizing domain (iris) specific knowledge. The new generative adversarial network is termed as iDCGAN (iris Deep Convolutional Generative Adversarial Network). Similar to the idea of conditional GANs [52], it uses auxiliary information of iris quality to improve the performance of both discriminator and generator deep convolutional networks.

In an iris recognition system, iris image quality assessment is an integral step as the quality of iris images can greatly impact the performance of iris recognition. It has been ascertained that different artifacts such as occlusion, off-gaze direction, motion blurriness, and specular reflection can affect iris recognition performance [60, 61]. Thus, incorporating quality metrics in generative adversarial network can improve

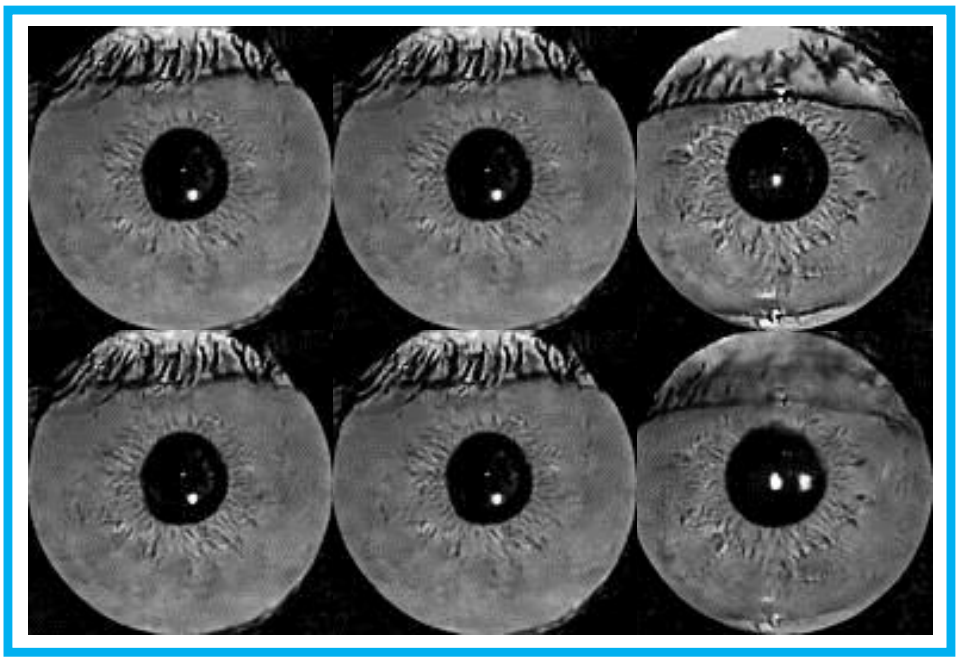

Figure 3.3: Sample synthetic iris images generated from the proposed iDCGAN framework.

the synthesis process. Eq. 3.2 shows the objective function of the proposed iDCGAN framework.

$$
\begin{aligned}
L = \min_{\mathcal{G}} \max_{\mathcal{D}} \mathbb{E}_{\mathbf{x}\sim p(\mathbf{x})}[\log(\mathcal{D}(\langle \mathbf{x}, Q(\mathbf{x})\rangle))] \\
+ \mathbb{E}_{\mathbf{z}\sim p_{noise}(\mathbf{z})}[\log(1 - \mathcal{D}(\langle \mathcal{G}(\mathbf{z}), Q(\mathcal{G}(\mathbf{z}))\rangle))]
\end{aligned}
\tag{3.2}
$$

where, $Q(\mathbf{x})$ is a quality evaluating function that takes an input iris image and assigns a corresponding quality score. Thus, in the proposed iDCGAN framework the generator network $\mathcal{G}$, spawns new images of iris conditioned on high quality scores.

The input latent vector is generated from a noisy distribution $p(\mathbf{z})$. This is provided as input to the generator network, where the generator generates iris images according to the learned representations. Quality assessment of the iris images created by the generator $\mathcal{G}$ is performed. The quality of the iris images in the first quartile is removed from the set to be passed to the discriminator network $\mathcal{D}$. Similar to the above step, the real iris image input to the discriminator network $\mathcal{D}$ is filtered such that the training set contains iris images whose quality scores are above the first quartile. The new samples are continuously generated to train the proposed iDCGAN generator and discriminator. Figure 3.3 showcases sample iris images generated from the proposed iDCGAN framework.

3.1.3 Implementation Details

Three existing real iris image databases are utilized and combined together to form the training set for the proposed iDCGAN framework:

IIITD Contact Lens Database [23] This database consists of iris images of 101 subjects. The database includes iris images of subjects with and without contact lens. For training the proposed iDCGAN, only the real images (without contact lens) belonging to these subjects are chosen.

IIT Delhi Iris Database [62] This database consists of real iris images pertaining to 224 subjects.

MultiSensor Iris Database [39] Iris images of 547 subjects collected in multiple sessions are utilized for training the proposed iDCGAN framework.

The input iris images are segmented so that only the iris and pupil regions are considered as input to the iDCGAN framework. The framework is implemented in Python language utilizing the TensorFlow library[1]. Both the generator and discriminator networks are deep convolutional neural networks. The discriminator network consists of four convolutional layers with a kernel size of 5×5 and strides of 2, batch normalization and leaky rectified units. The generator network consists of four strided transposed convolutional layers with a kernel size of 5×5 and strides of 2, batch normalization and rectified units. The size of the final synthetic iris images is 128×128. A learning rate of 0.0002 and Adam optimizer are utilized to train the proposed iDCGAN.

3.2 Analysis of Synthetically Generated Iris Images

The synthetic iris images produced by the proposed iDCGAN framework are evaluated with respect to their similarity with real iris images. For this purpose, different quality score metrics are computed for both real and generated iris images. The quality metrics can evaluate factors such as sharpness of generated images, shape and concentricity of pupil and iris etc.

[1] https://www.tensorflow.org

3.2.1 Experimental Protocol

The objective of this experiment is to determine the quality of the synthetically generated iris images and compare the quality score distribution with real iris images. Using the combined training set described above, 8,905 real iris images are selected. This is followed by generating an equal number of synthetic iris images using the proposed iDCGAN framework. Bharadwaj et al. [63] described that the quality of iris images can be categorized into image-based and biometric modality based quality measures. Using VeriEye, several image specific and biometric modality specific quality scores are computed. These quality score metrics are described in ISO/IEC 29794-6 standards [64]. The following quality score metrics are employed for analysis purposes:

- Pupil boundary circularity: This parameter represents the circularity of the iris-pupil boundary. It is calculated as

$$\left(2 * \sqrt{\pi \times \text{pupil area}}\ \right) / \,(\text{pupil perimeter})$$

- Pupil contrast: The contrast value at the boundary of iris and pupil is an important parameter for successful iris segmentation. It is computed as the mean of differences in grayscale values at left and right end of iris-pupil boundary.

- Pupil-iris ratio: This quality measure signifies the amount of dilation or constriction in the pupil.

- Pupil concentricity: This parameter measures the corresponding concentricity between the iris and the pupil. It is calculated as follows where X and Y represent the coordinates of the iris and pupil.

$$\sqrt{(X_{pupil} - X_{iris})^2 + (Y_{pupil} - Y_{iris})^2}/IrisRadius$$

- Sharpness: The sharpness of the image parameter is examined to understand the magnitude of defocus in the input iris image. This is calculated using Daugman's focus score [65].

- Overall quality: The overall quality score of the iris image represents the comprehensive biometric quality of the presented iris sample. We have utilized output quality score generated from VeriEye.

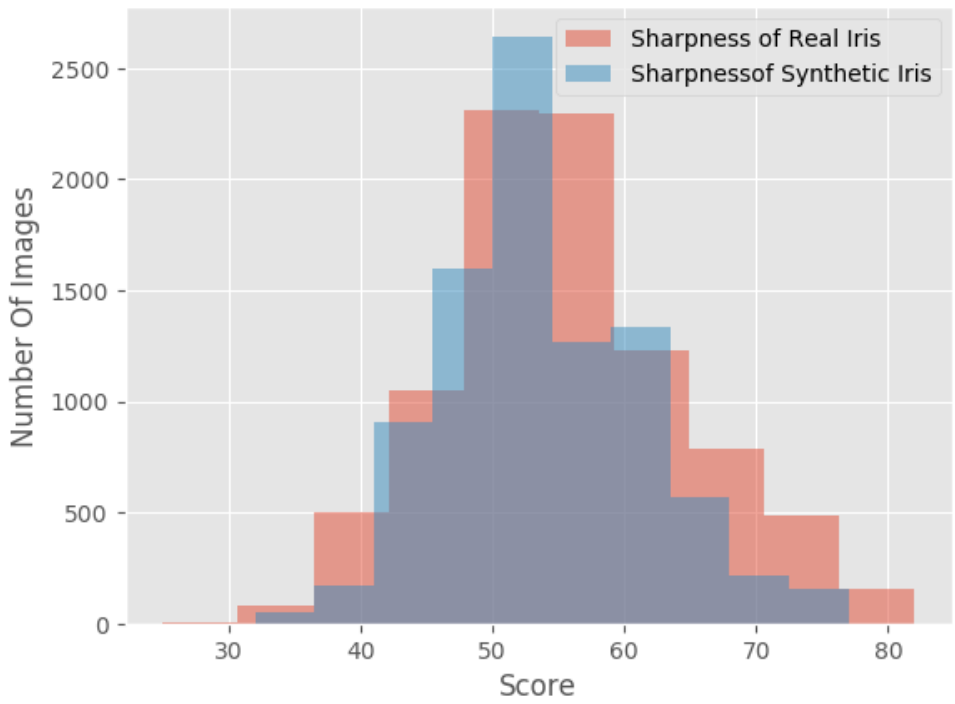

Figure 3.4: Sharpness Metric for Real Iris vs generated Synthetic Iris

3.2.2 Results and Analysis

Figure 3.4, 3.5, 3.6, 3.7, 3.8 and 3.9 showcases the distributions of the above mentioned quality parameters pertaining to real iris images and synthetically generated iris images. We observe that the quality measurements of the synthetically generated images follow similar trends to the real iris images. The analysis of the quality metrics can be categorized as follows:

Image based Quality: The sharpness score is an image based quality metric. It is observed from Fig 3.4 that there is a significant overlap between the histograms of sharpness observed in real iris images and synthetically generated iris images. The χ^2 distance between the sharpness quality histograms is 1.07 which is relatively low[2]. Similarly, pupil contrast parameter represents contrast difference in a specific region of interest in the image. The χ^2 distance between the pupil contrast histogram is 4.02. It can be observed that the pupil contrast of synthetically generated images is skewed on the higher side as compared to the pupil contrast of real iris images. Thus, larger number of synthetically generated iris images using the proposed iDCGAN framework have higher pupil contrast score as compared to real iris images.

Biometric based Quality: The pupil-iris ratio, pupil boundary circularity, and

[2]Lower χ^2 distance values signify very close match.

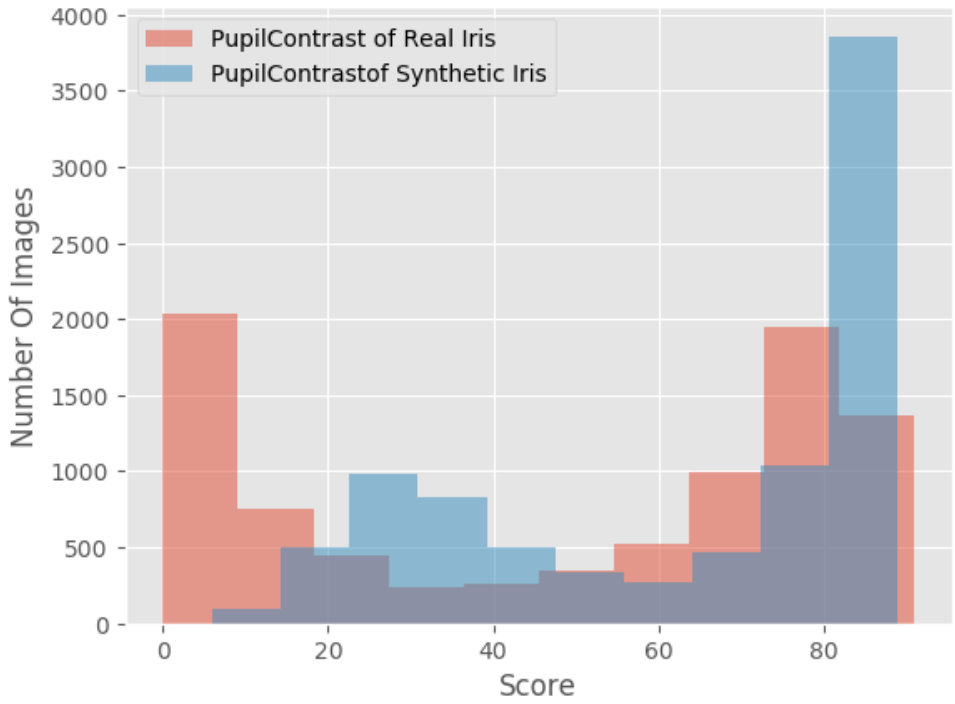

Figure 3.5: Pupil Contrast Metric for Real Iris vs generated Synthetic Iris

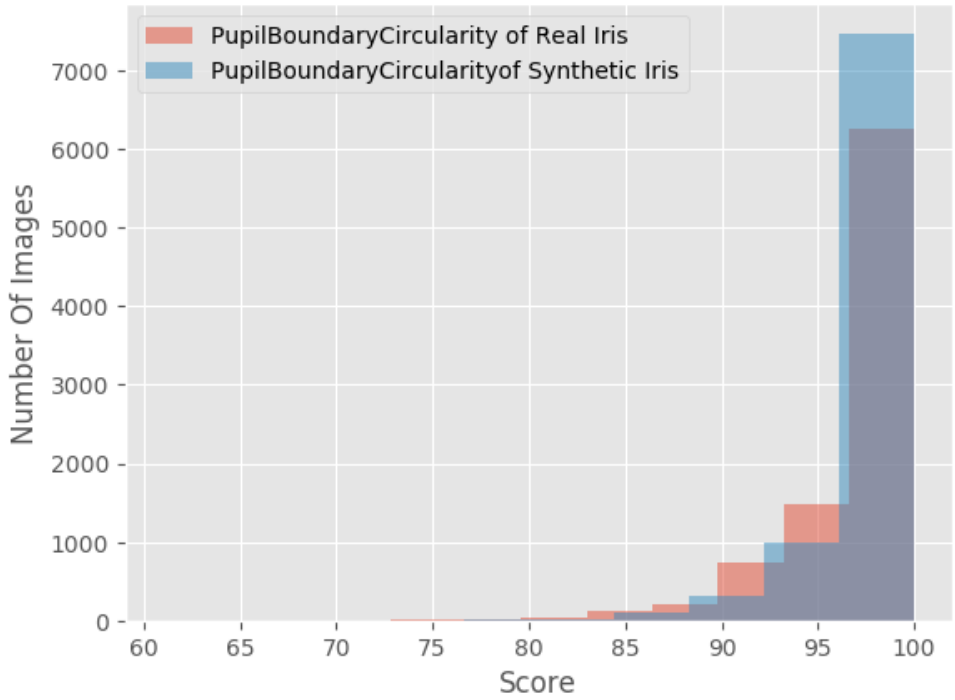

Figure 3.6: Pupil Boundary Circularity Metric for Real Iris vs generated Synthetic Iris

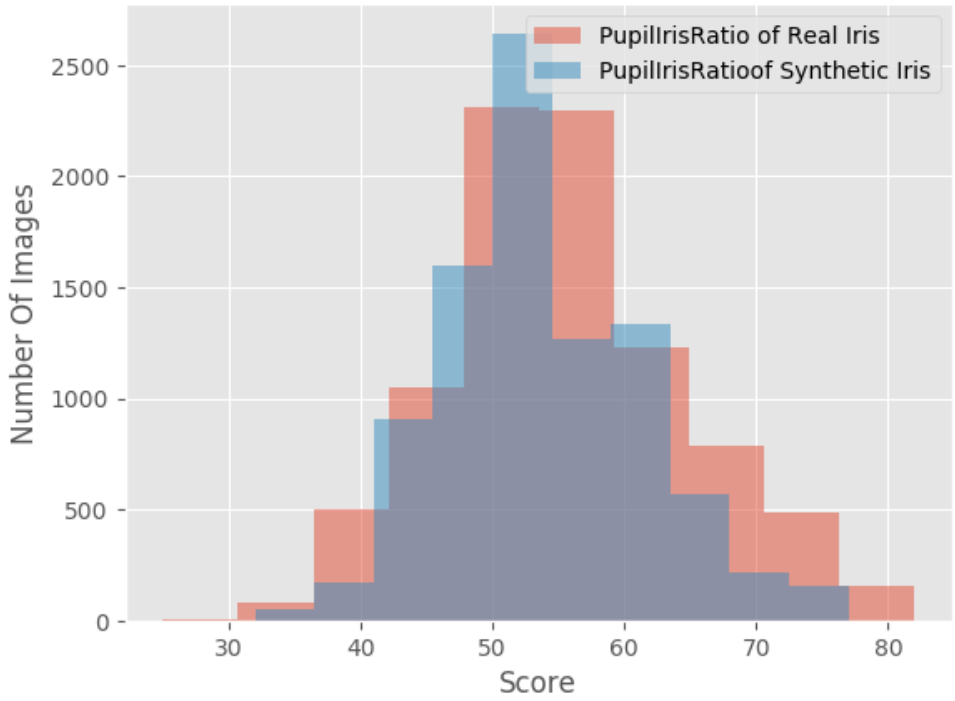

Figure 3.7: Pupil Iris Ratio Metric for Real Iris vs generated Synthetic Iris

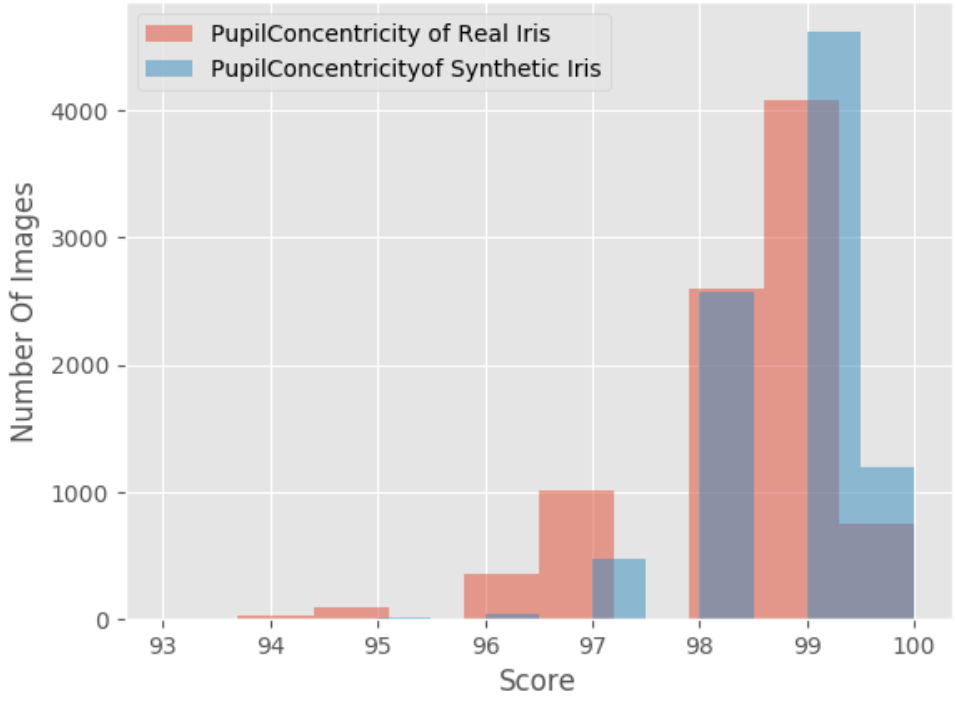

Figure 3.8: Pupil Concentricity Metric for Real Iris vs generated Synthetic Iris

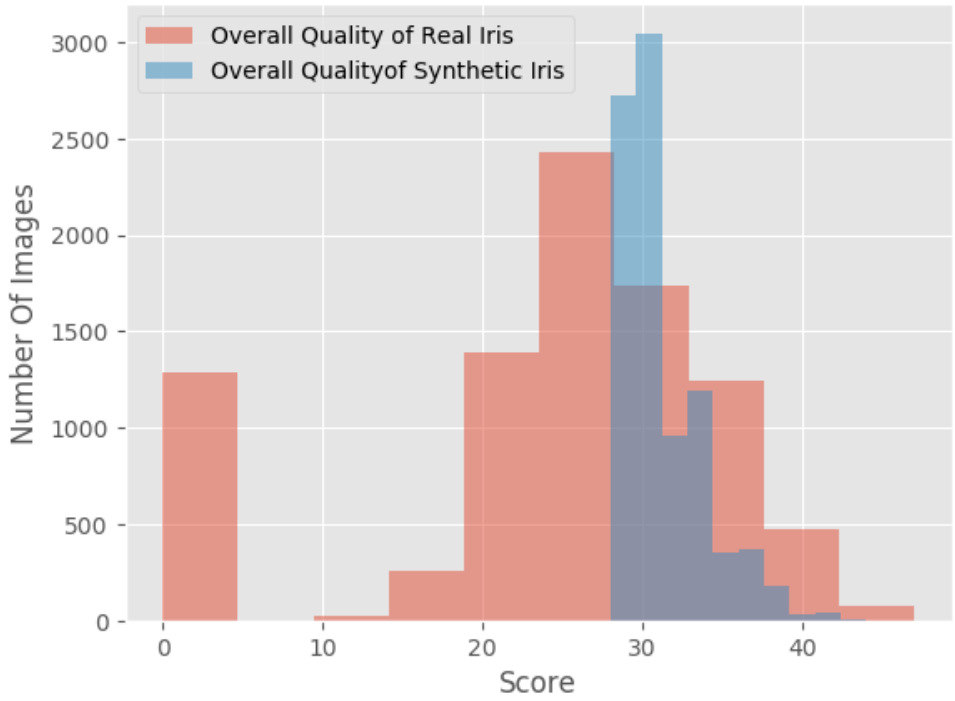

Figure 3.9: Overall Quality Metric for Real Iris vs generated Synthetic Iris

pupil concentricity are measures of the iris biometric modality. We observe that there is a significant overlap between the distribution of pupil-iris ratio, pupil concentricity and pupil boundary which is also confirmed by the χ^2 distance of 1.07, 0.04 and 0.34, respectively.

Overall Quality: The quality of the synthetically generated iris images is skewed on the higher side and is different from the quality of the real iris images in the combined training set. The generator network in the proposed iDCGAN framework is trained to discard iris images that are not of good quality. Therefore, it has generated high quality synthetic images.

The comparative analysis of these quality score metrics indicates that the synthetically generated iris images very closely resemble the real iris images.

3.3 Synthetic Iris as Presentation Attack

The objective of the proposed iDCGAN framework is to generate iris images which appear *real*. Due to the realistic appearance of these synthetic iris images, they can be used as an attack on any iris recognition system. In this experiment, we utilize VeriEye [66] to examine if a commercial iris recognition matches these synthetic images to real

iris images. The results of this experiment are utilized to establish that the output images from the proposed iDCGAN framework can act as an iris presentation attack.

3.3.1 Experimental Setup

The goal of this experiment is to compute iris recognition scores between gallery and probe sets to evaluate the impact of synthetically generated iris as presentation attacks. For this iris recognition experiment, real genuine, real impostor, and synthetic impostor pairs are created using 8,905 real iris images and 8,905 synthetic iris images. The match scores obtained by matching these pairs are analyzed and the results are presented below.

3.3.2 Results and Analysis

These real genuine and synthetic impostor scores are analyzed to observe the impact of synthetically generated iris images on the performance of VeriEye. Upon minimizing the synthetic iris false accept to 0%, we observe that 15.2% of real iris genuine scores are misclassified as impostors. On the other hand, minimizing the real iris false reject to 0% leads to synthetic false accept rate of 67.66%. This showcases that the

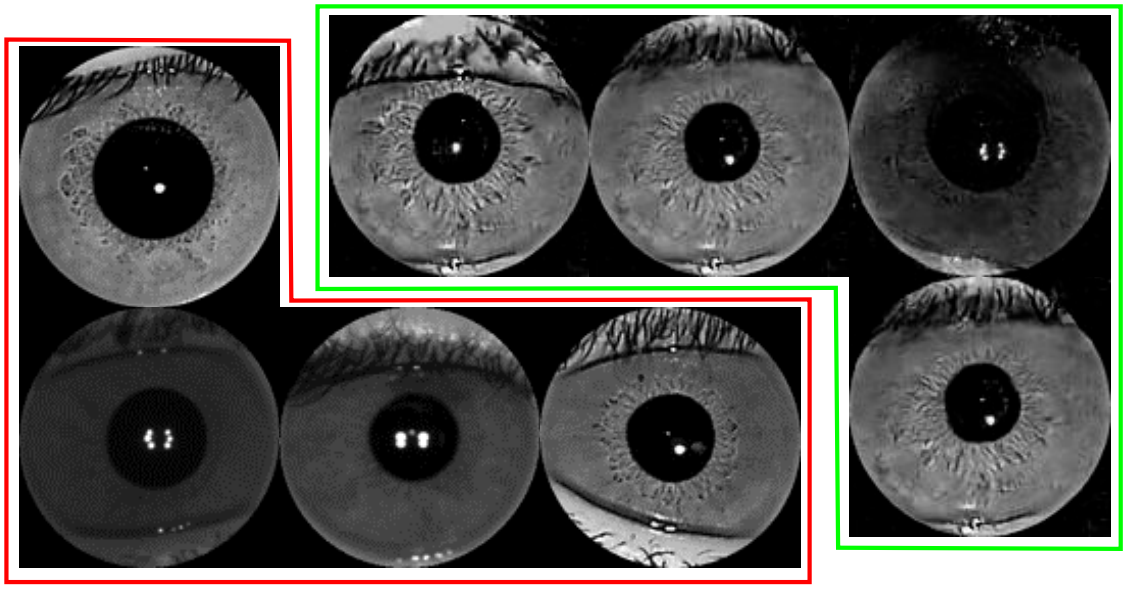

Figure 3.10: Marked real iris and synthetically generated iris images using the proposed iDCGAN framework. Iris images inside the red border are real iris images and the remaining iris images inside the green border are synthetically generated images.

synthetically generated images adversely affect iris recognition and can pass through the recognition system based on the chosen permissible error threshold.

Interestingly, we observe that all the synthetically generated iris images are encoded by VeriEye and templates are created for every image. A denial of service attack can easily be executed on an iris recognition system by sending such synthetically generated iris images as input. These results validate that the realistic-looking synthetically-generated iris outputs from the proposed iDCGAN framework can be potentially used for iris presentation attack. Figure 3.10 showcases the visual similarity between real iris and synthetically generated iris images.

3.4 Summary

In this chapter, iDCGAN framework is proposed which incorporates iris domain-specific knowledge in the form of quality metric to generate high-quality iris images. It is observed that the distributions of quality parameters described for a biometric sample for the synthetically generated iris images are similar to that of real iris images, thus, establishing the similarity between real and synthetically generated images. We also demonstrate the probability of a successful presentation attack by utilizing these synthetically generated iris images. This thesis highlights the need to develop accurate iris presentation attack detection algorithms that can adapt to newer types of attacks such as synthetic iris image attacks.

Chapter 4

Detection of Iris Presentation Attacks using DESIST

In the literature, researchers have focused on one particular type of iris presentation attack and have developed different algorithms to address it [67, 43, 41]. However, in real-world scenarios, iris recognition systems should be able to handle and detect all types of presentation attacks. The key motivation of this chapter is to simulate this real-world iris presentation attack scenario for which, we assess print attacks, synthetic iris images, and contact lenses comprehensively. Additionally, as shown in Chapter 3, synthetically generated iris images can be used to attack iris recognition systems and thus, need to be detected successfully.

The major contributions of this chapter are:

- Combining different types of iris presentation attacks in an attempt to simulate real world scenarios,
- Proposing a novel framework utilizing structural and textural features to detect such multiple complex presentation attacks, and
- Evaluating the proposed framework on synthetically generated iris images.

In the subsequent sections, we explain the proposed framework followed by the databases used in this chapter, experimental protocol, and the results obtained.

4.1 Proposed Detection Framework for Iris Presentation Attack

Figure 4.1 shows the proposed **DE**tection of iri**S** spoof**I**ng using **S**tructural and **T**extural feature (DESIST) framework for detecting spoofed iris images. The proposed framework involves two components: structural decomposition of images to analyze local regions of the images and a textural analysis to observe the changes in contrast to the input iris image. We describe both the parts in detail below.

4.1.1 Structural Decomposition of Images using Zernike Moments

Zernike moments (ZMs) are known for their invariance across scale, rotation, and translation; and have been successfully applied in iris segmentation [68] and iris recognition at a distance [69]. The motivation behind extracting these Zernike moments is to capture the changes in the shape between a *spoofed* and a *normal* iris image. ZMs of an image are defined over an orthogonal set of polynomials and involve computation of the radial polynomial $R_{n,m}$. Zernike basis functions can be calculated after the polynomial is computed and projection of the input image over these basis functions is determined. The radial polynomial R is defined as:

$$R_n^m(\rho) = \sum_{i=0}^{\frac{n-|m|}{2}} \frac{(-1)^i \rho^{n-2i}(n-i)!}{i!\left(\frac{n+|m|}{2}-i\right)!\left(\frac{n-|m|}{2}-i\right)!} \tag{4.1}$$

where, ρ is the distance between the center of the image and a corresponding point (x, y) on the image, n is called the order of the polynomial and m are the repetitions such that $\mid m \mid < \ n$ and $\mid n - m \mid$ is even. Zernike basis function can be directly computed in the Cartesian coordinate space as defined below:

$$Z_{n,m}(x, y) = R_n^m(\rho_{x,y}) e^{-jm\theta_{x,y}} \tag{4.2}$$

where $N \times N$ is the size of the image,

$$\rho_{x,y} = \frac{1}{N} \times \sqrt{(2x - N + 1)^2 + (N - 1 - 2y)^2} \tag{4.3}$$

and

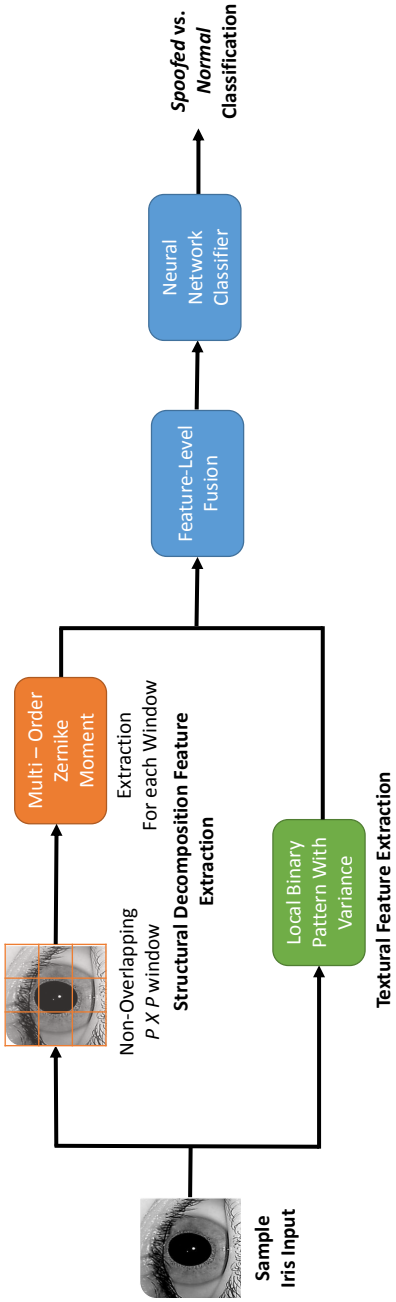

Figure 4.1: Proposed structural and textural feature based iris presentation attack detection (DESIST) framework for detecting spoofed iris images.

$$\theta_{x,y} = tan^{-1}\left(\frac{N-1-2y}{2x-N+1}\right) \tag{4.4}$$

Given an iris image I, dense Zernike moments are calculated for a given pair of (n, m) across non-overlapping windows of size $P \times P$. Multiple pairs of (n, m) are selected to compute the amplitude of multi-order Zernike moments. This will help in enhancing the representation of the input iris image.

4.1.2 Textural Analysis using LBPV Descriptor

Through earlier studies [24, 23], it is known that spoofed iris attacks such as contact lens iris images, printed iris images have variations in texture with respect to the regular iris images. Therefore, the motivation behind utilizing texture techniques is to identify the changed texture of the spoofed iris image. For this purpose, Local Binary Pattern Variance (LBPV) descriptor [70] is utilized. LBPV descriptor accounts for the contrast in the input images by adaptively weighing the LBP vectors by their variance of the region. It is also more robust to illumination variation which is useful as the acquired iris images may have different illumination sources. Thus, LBPV descriptor is calculated for the input iris image and provided to the classifier.

4.1.3 Feature Fusion and Classification

Multi-order Zernike and LBPV features provide complementary information regarding the input iris image. Therefore, feature-level fusion is performed by concatenating them. The concatenated (fused) feature vector is then used as input for an artificial neural network (ANN) to determine whether the iris is spoofed or not. A three-layer ANN is trained with H hidden nodes and scaled conjugate gradient algorithm is utilized for back-propagation.

4.2 Experimental Results

4.2.1 Combined Spoofing Database

Different types of iris presentation attack databases are available in the research community. We collected images from multiple publicly available iris presentation attack databases and formed a combined spoofing database (CSD)[1]. In this chapter,

[1]The database can be downloaded from: http://iab-rubric.org/resources.html

Table 4.1: Details of Combined Spoofing Database (CSD) and its constituents utilized in this study.

Database	**No. of Subjects**	**Type of Iris Images**	**No. of *Spoofed* Samples**	**No. of *Normal* Samples**
IIIT-Delhi CLI [23]	101	Normal, Soft Contact Lens, Textured Contact Lens	4420	1063
IIITD IIS [24]	101	Print+Scan and Print+Capture of IIIT-Delhi CLI	4848	0
SDB [37]	1000	Synthetically Generated	2100	0
IIT Delhi Iris [71]	224	Normal	0	2240
MID	547	Normal	0	6022
CSD	1872	All Combined and Normal	11368	9325

the following databases are utilized to simulate the real-world scenario of a variety of iris presentation attacks for iris recognition systems:

- IIIT-Delhi Contact Lens Iris (CLI) Database [23]: It contains images pertaining to 101 subjects. For each subject, images are captured without lens, with transparent (soft) lens, and with cosmetic lens (textured) using two different iris sensors.

- IIITD Iris Spoofing (IIS) Database [24]: IIIT-Delhi CLI database is utilized to create the IIS database. Cogent CIS 202 dual eye iris scanner and HP flatbed optical scanner are used to create print attack scenarios. In the print+capture attack, input to iris scanners are the printed iris images whereas in the print+scan attack, printed iris images are scanned using a flatbed scanner.

- Synthetic Database (SDB) [37]: The database by Galbally et al. is generated using Markov Random Field and various iris features to create images of 1000 subjects.

- IIT Delhi Iris Database [71]: This database contains normal (non-spoofed) iris images of 224 subjects. The database has been included in the study to represent the *normal* class.

- Multi-sensor Iris Database (MID): In order to build representations of the *normal* class, iris images of 547 subjects are collected and included in the combined database.

Table 4.1 summarizes the characteristics of combined spoofing database (CSD) and its constituent databases used in this study.

4.2.2 Experimental Setup

To evaluate the performance of the proposed DESIST framework, images from the combined spoofing database (CSD) are resized to a common size of 256×256 pixels. Following the protocol described in [23], two folds are created for each database where 50% of the subjects are assigned to fold one and the remaining 50% of the subjects are assigned to the other fold. Using these unseen training and testing folds, five times random two fold cross-validation is performed.

Multi-order local Zernike moments are computed from non-overlapping windows of size $P \times P$ of the images. The amplitude of the Zernike moments is computed for order of the Zernike moments (n) = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10) and corresponding repetition number of Zernike moment (m) = (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0). LBPV features are also computed for the whole iris image and feature-level fusion is performed using the Zernike and LBVP features. These features are used for the final classification of the input image as *spoofed* or *normal*. A three layer neural network is trained using fused features for two-class classification. Along with the proposed algorithm, we have evaluated the performance of several existing descriptors as well.

4.2.3 Results and Analysis

Receiver Operating Characteristics (ROC) curves shown in Figure 4.2 and Tables 4.2 and 4.3 summarize the results. Key observations of the experiments are:

Average classification accuracy (along with standard deviation), across cross validations trials, of whether the given iris image is *normal* or *spoofed* is shown in Table 4.2. The proposed DESIST framework yields average classification accuracy of **82.20**%. This highlights the challenging nature of the problem that arises while dealing with a medley of iris presentation attacks.

The parameters are tuned empirically for computing Zernike moments and learning the artificial neural network model. For calculation of Zernike moments, non-overlapping patch sizes of 4×4, 8×8, and 16×16 are tested and patch size of 8×8

yields the highest classification accuracy. For training the artificial neural network, parameter testing is performed to compute the optimum number of hidden nodes (H). By experimental analysis, 170 hidden nodes are chosen.

For comparison purposes, classification accuracies obtained by m-BSIF [45], wLBP [35], and LUCID [12] are also reported in Table 4.2. The proposed DESIST framework yields the highest accuracy of **82.20**% as compared to wLBP, m-BSIF, and LUCID. Figure 4.2 shows the ROC curves for the top three performing algorithms: proposed DESIST framework, LUCID, and m-BSIF. The Equal Error Rates (EERs) are 17.86%, 20.68%, and 27.02% for proposed DESIST framework, LUCID, and m-BSIF, respectively.

Further analysis is performed on the performance of the proposed framework. The proposed DESIST framework correctly classifies 81.44% of *normal* iris images (true

Table 4.2: Average detection accuracy (%) for iris presentation attack detection using different classification algorithms.

Classification Algorithm	**Mean Classification Accuracy (Std Dev)(%)**
wLBP [35]	59.85 (5.01)
m-BSIF [45]	63.86 (3.61)
LUCID [12]	73.21 (3.97)
Multi-Order Zernike Moments + ANN	76.22 (5.15)
LBPV + ANN	78.45 (5.49)
Proposed DESIST Framework	**82.20 (1.29)**

Table 4.3: Average detection accuracy (%) for iris presentation attack detection on different databases separately using proposed DESIST framework and LUCID [12]. Note that training is performed on the train set of CSD and for the test set, results pertaining to individual spoof attacks are reported.

Database	**Spoofing Type**	**Proposed DESIST Framework**	**LUCID [12]**
IIIT-Delhi CLI [23]	Contact Lens	54.34	54.88
IIITD IIS [24]	Print+Scan, Print+Capture	98.67	95.16
SDB [37]	Synthetic Iris	98.10	84.95
IIT Delhi Iris [71]	Normal	98.57	97.41
MID	Normal	88.55	84.96

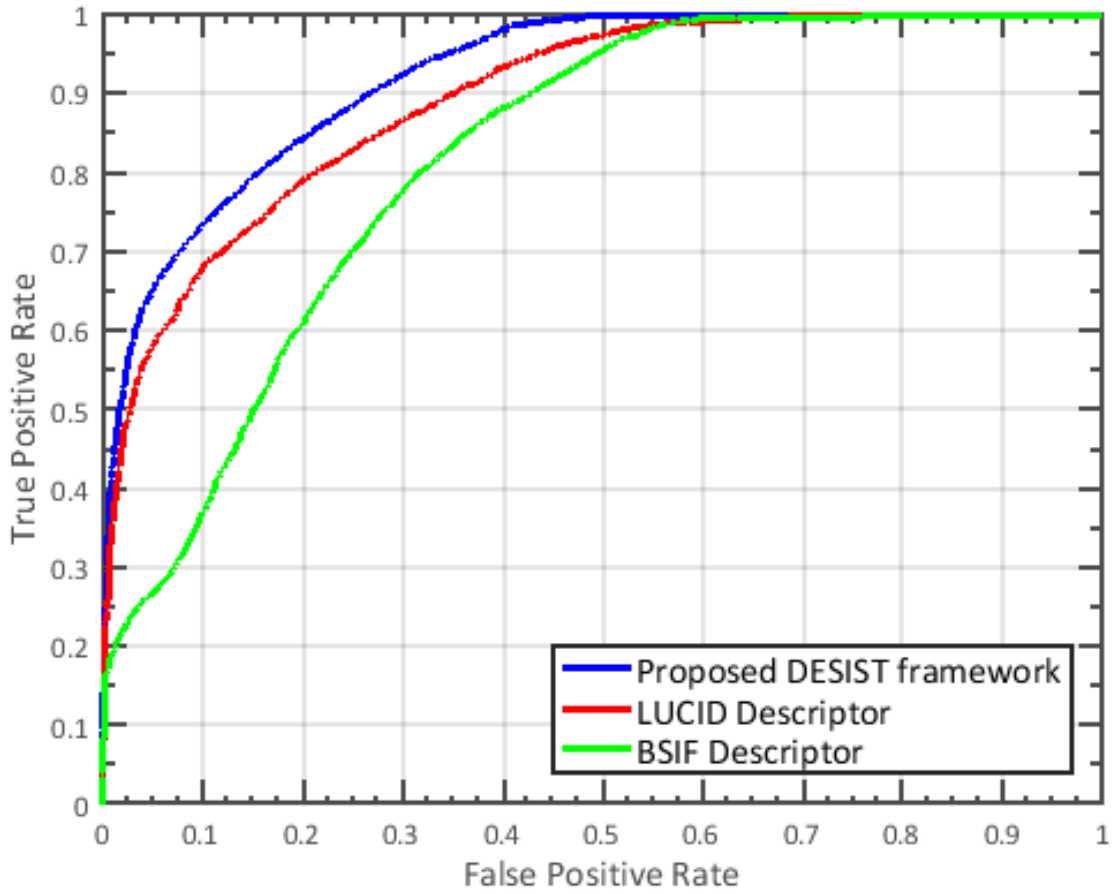

Figure 4.2: ROC curves showing the performance of top three anti-spoofing algorithms.

positive rate) whereas 82.92% of *spoofed* images are correctly labeled (true negative rate). Figure 4.3 shows sample images from *normal* and *spoofed* classes which are correctly and incorrectly classified by the proposed DESIST framework.

The proposed DESIST framework utilizes feature-level fusion of multi-order Zernike moments and LBPV computed on the input iris image. For comparative analysis, the performance of multi-order Zernike moments with ANN, and LBPV with ANN are reported separately. On its own, multi-order Zernike moments with ANN yields an accuracy of 76.22%, while LBPV with ANN yields an accuracy of 78.45%. These results demonstrate that by applying feature-level fusion, there is an improvement in the performance.

Table 4.3 shows the results obtained by analyzing the classification accuracy of input iris images based on the type of presentation attack. Images from IIIT-Delhi CLI database [23] show the lowest classification accuracy of 54.34%. It is observed

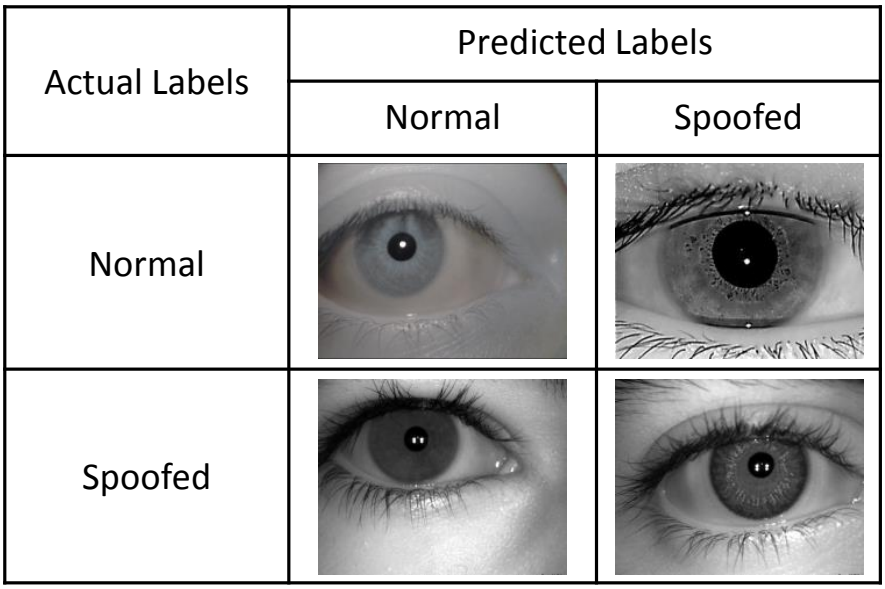

Figure 4.3: Sample iris images from *normal* and *spoofed* classes which are correctly and incorrectly classified by the proposed DESIST framework.

that 44.36% of normal, 58.58% of transparent (soft), and 59.93% of textured (cosmetic lens) are correctly detected. On IIITD IIS database [24], the proposed DESIST framework correctly detects 98.67% images. In this database, 99.67% of print+scan spoofed images and 97.60% of print+capture spoofed images are correctly classified as *spoofed*. For SDB, IIT Delhi Iris, and MID databases correct classification accuracy of 98.10%, 98.57%, and 88.55% is achieved by the DESIST framework.

In [23], the reported results show 64.14% accuracy on normal, 61.63% on transparent contact lens, and 94.74% on textured contact lens. Further, Gupta et al. [24] have shown 100% classification accuracy in detecting print+scan attacks on IIITD IIS database. it is worth mentioning that these reported results pertain to a single spoofing attempt. However, in our case, the training model is learned from multiple attacks and therefore, direct comparison of results is not feasible.

To compare the performance of the proposed DESIST framework with other approaches, database-wise performance of LUCID [12] is also reported in Table 4.3. It is observed that similar to DESIST, LUCID shows lower accuracies on IIIT-D CLI database. This highlights the challenging nature of the CSD database. For IIITD IIS, SDB, IIT Delhi Iris, and MID, LUCID yields classification accuracy of 95.16%, 84.95%, 97.41%, and 84.96%, respectively.

Evaluation on LivDet-Iris 2013: The proposed DESIST framework is also

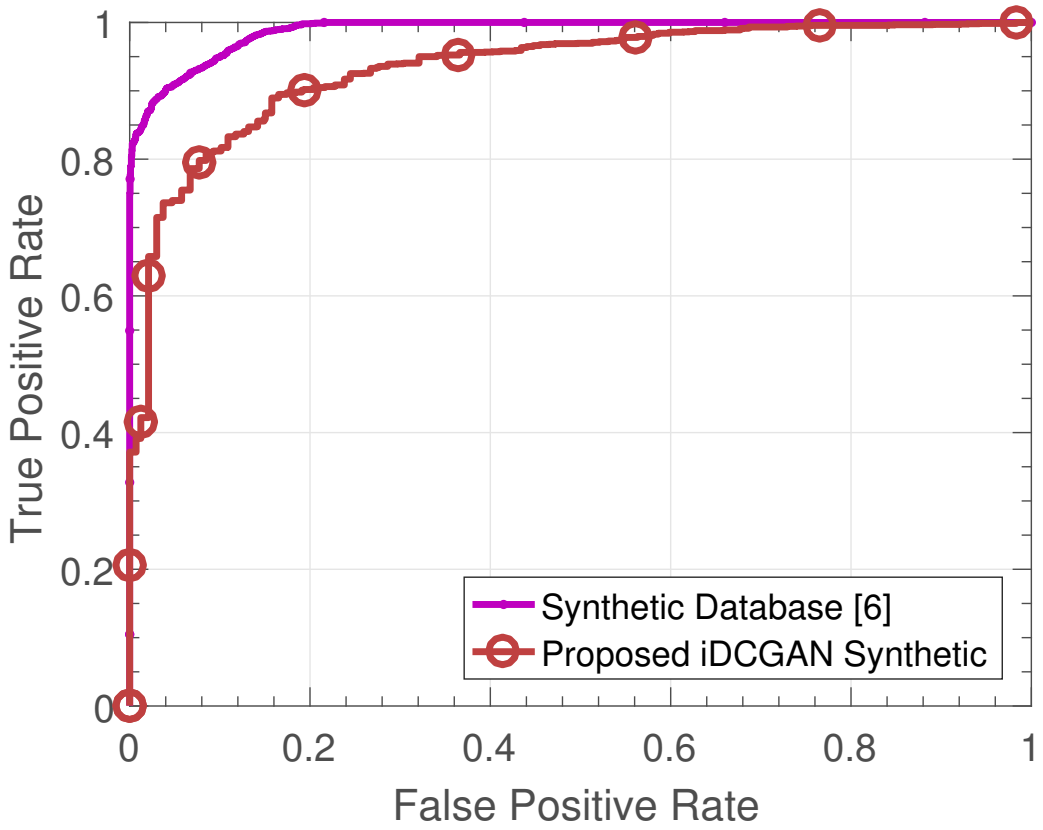

Figure 4.4: Performance of presentation attack detection using DESIST on images from the Synthetic DataBase [2] and the proposed iDCGAN synthetic images.

evaluated on Warsaw and Clarkson subsets of LivDet-Iris 2013 competition [72]. The provided training and testing images are utilized for the comparison. Using the DESIST framework, total classification accuracy of 92.08% is observed on the Warsaw subset and 79.59% on the Clarkson subset. The average classification accuracy for the two databases combined is 87.03%. Using the proposed DESIST framework, the true positive rate obtained is 97.19% and 70.73% for Warsaw and Clarkson subsets, respectively. The proposed DESIST framework outperforms the participating algorithms in the competition by achieving the lowest average false positive rate of 11.56% on the two datasets averaged. On the other hand, the achieved true negative rate is 87.11% and 84.55% for Warsaw and Clarkson subsets, respectively.

4.3 Iris PAD on iDCGAN Generated Iris Images

The key results of Chapter 3 illustrate that the synthetically generated iris images from the proposed iDCGAN framework can be effectively deployed in iris presentation

attacks. Hence, it is important to develop accurate iris presentation attack detection (PAD) algorithms which can distinguish such synthetic iris images from real iris images. In this section, we showcase the results of DESIST [39] framework, which has been shown to outperform other algorithms on the combined spoofing dataset, on these iris images.

4.3.1 Experimental Protocol

In this experiment, we analyze the performance of DESIST PAD algorithm for detecting synthetically generated iris images. To showcase that the synthetically generated iris images using the proposed iDCGAN framework are stronger adversary as compared to existing synthetic iris images, we utilize SDB [2]. SDB comprises 2,100 synthetic iris images. An equal number of real iris images and iris images that are synthetically generated from the iDCGAN approach are utilized for experimental evaluation. In this experiment, five-fold cross-validation is performed with unseen training and testing samples. Multi-order Zernike moments and local binary pattern with variance (LBPV) features are extracted to provide input to the DESIST framework for classifying iris images as real or synthetic using a neural network as the classifier.

4.3.2 Results

The results of the presentation attack detection using DESIST are presented in Figure 4.4. Iris PAD accuracy on the synthetically generated iris images using the proposed iDCGAN framework is 85.95% with equal error rate (EER) of 14.19%. PAD performance of DESIST on SDB is 92.17% with an EER of 7.09%. We observe that EER by DESIST on SDB is approximately 2 times higher than the EER obtained with iDCGAN generated images. As discussed in Chapter 3, the iris image quality scores of the realistic appearing synthetically generated samples are closer to the real-world samples and hence, it is difficult for the DESIST model to discriminate between the samples of the real iris and presentation attack iris classes.

4.4 Summary

In the literature of iris presentation attack detection, researchers have typically focused on a particular type of iris spoofing attack and have presented solutions to

address them. However, in real-world scenarios, iris recognition systems have to handle any type of presentation attack. In this chapter, we present a real-world scenario, where a medley of spoofed iris images can be presented at the acquisition step. We have utilized a combined database containing spoofed iris images belonging to contact lens, print-capture, print-scan, and synthetic iris images. We propose DESIST, a framework to detect spoofed iris images across real-world attack scenarios. The framework learns local structural changes by projecting the original image in the Zernike moment space. Multi-order dense Zernike features are computed across the input iris image. We also learn textural information through Local Binary Patterns with Variance that accounts for contrast information. A feature level fusion of these complementary features is presented and finally, a neural network classifier is trained to detect spoofed iris images and normal images. The proposed DESIST framework detects spoofed iris images with a classification accuracy of 82.20% when applied to a combined iris spoofing database of *normal* and *spoofed* iris images and outperforms other comparative algorithms. Additionally, we showcase the performance of DESIST on the synthetic iris images generated by iDCGAN framework and observe that these synthetic images are difficult to detect as compared to the previously generated synthetic iris images.

Chapter 5

Conclusion and Future Work

5.1 Conclusion and Future Work

Similar to other biometric modalities, iris recognition systems are also vulnerable to presentation attacks (commonly known as spoofing) that attempt to conceal or impersonate identity. Examples of typical iris presentation attacks are printed iris images, textured contact lenses, and synthetic creation of iris images. In the era of improving deep learning algorithms, we present a novel iDCGAN framework to generate synthetic iris images. The framework utilizes generative adversarial networks alongside iris quality measures to synthesize realistic iris images. The generated images are compared and shown to have similar or better iris quality measures as compared to real iris images that were used to train the framework. Finally, we showcase the efficacy of these images as presentation attacks and observe that these images end up being enrolled by a commercial iris recognition software. In this thesis, we also focus on detecting a medley of iris presentation attacks and present a unified framework for detecting such attacks. We propose a novel structural and textural feature based iris spoofing detection framework (DESIST). Multi-order dense Zernike moments are calculated across the iris image which encode variations in the structure of the iris image. Local Binary Pattern with Variance (LBPV) is utilized for representing textural changes in a spoofed iris image. The highest classification accuracy of 82.20% is observed by the proposed framework for detecting presentation attack on a combined iris spoofing database. We also showcase the performance of this framework on the iDCGAN generated images and observe that current iris presentation detection algorithms need to be improved to detect such attacks.

The increasing interest in iris recognition, particularly in mobile devices, has made

it highly vulnerable to presentation attacks and has renewed interest in developing sophisticated presentation attack detection algorithms. Generative algorithms continue to improve with new generative adversarial algorithms coming up such as BEGAN [6], BIG-GAN [73], and other generative algorithms such as Wasserstein Autoencoders [74]. These algorithms can be utilized in conjunction with iris quality measures to generate realistic iris images at a higher resolution. Novel deep learning based presentation attack detection algorithms should be trained for better performance. One of the issues currently why such algorithms are difficult to train, is lack of large-scale iris presentation attack databases. Thus, the creation of such databases is another area that researchers should focus on.

Bibliography

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[2] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512 – 1525, 2013.

[3] M. Ferrara, R. Cappelli, and D. Maltoni, "On the feasibility of creating double-identity fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 892–900, 2017.

[4] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," *arXiv preprint arXiv:1511.06434*, 2015.

[5] Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, and J. Choo, "Stargan: Unified generative adversarial networks for multi-domain image-to-image translation," *arXiv preprint*, vol. 1711, 2017.

[6] D. Berthelot, T. Schumm, and L. Metz, "Began: boundary equilibrium generative adversarial networks," *arXiv preprint arXiv:1703.10717*, 2017.

[7] T. Karras, T. Aila, S. Laine, and J. Lehtinen, "Progressive growing of gans for improved quality, stability, and variation," *arXiv preprint arXiv:1710.10196*, 2017.

[8] A. Lefohn, B. Budge, P. Shirley, R. Caruso, and E. Reinhard, "An ocularist's approach to human iris synthesis," *IEEE Computer Graphics and Applications*, vol. 23, no. 6, pp. 70–75, 2003.

[9] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *IEEE International Conference on Image Processing*, 2006, pp. 317–320.

[10] L. Cardoso, A. Barbosa, F. Silva, A. M. G. Pinheiro, and H. Proença, "Iris biometrics: Synthesis of degraded ocular images," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1115–1125, 2013.

[11] Z. Wei, T. Tan, and Z. Sun, "Synthesis of large realistic iris databases using patch-based sampling," in *International Conference on Pattern Recognition*, 2008, pp. 1–4.

[12] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "Mobio_livdet: Mobile biometric liveness detection," in *Conference on Advanced Video and Signal Based Surveillance*, 2014, pp. 187–192.

[13] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[14] D. Bobeldyk and A. Ross, "Predicting eye color from near infrared iris images," in *IEEE International Conference on Biometrics*, 2018, pp. 104–110.

[15] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[16] J. Daugman, "How iris recognition works," *Proceedings of the IEEE*, vol. 14, no. 1, pp. 21–30, 2000.

[17] S. Marcel, M. S. Nixon, and S. Z. Li, *Handbook of Biometric Anti-Spoofing*. Springer, 2014.

[18] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 105–110.

[19] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in *IEEE International Conference on Biometrics: Theory, Applications and Systems*, 2013, pp. 1–6.

[20] I. Manjani, S. Tariyal, M. Vatsa, R. Singh, and A. Majumdar, "Detecting silicone mask-based presentation attack via deep dictionary learning," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1713–1723, 2017.

[21] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, and S. Schuckcrs, "Livdet 2013 fingerprint liveness detection competition 2013," in *IEEE International Conference on Biometrics*, 2013, pp. 1–6.

[22] N. Kohli, D. Yadav, M. Vatsa, and R. Singh, "Revisiting iris recognition with color cosmetic contact lenses," in *International Conference on Biometrics*, 2013, pp. 1–7.

[23] D. Yadav, N. Kohli, J. Doyle, R. Singh, M. Vatsa, and K. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 851–862, 2014.

[24] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On iris spoofing using print attack," in *Proceedings of International Conference on Pattern Recognition*, 2014, pp. 1681–1686.

[25] J. Cui, Y. Wang, J. Huang, T. Tan, and Z. Sun, "An iris image synthesis method based on PCA and super-resolution," in *International Conference on Pattern Recognition*, 2004, pp. 471–474.

[26] R. Cappelli, A. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprint-image generation," in *International Conference on Pattern Recognition*, 2000, pp. 471–474.

[27] A. Roy, N. Memon, and A. Ross, "Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2013–2025, 2017.

[28] J. Zuo, N. A. Schmid, and X. Chen, "On generation and analysis of synthetic iris images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 77–90, 2007.

[29] Q. Zhao, A. K. Jain, N. G. Paulter, and M. Taylor, "Fingerprint image synthesis based on statistical feature models," in *IEEE International Conference on Biometrics: Theory, Applications and Systems*, 2012, pp. 23–30.

[30] P. Johnson, F. Hua, and S. Schuckers, "Texture modeling for synthetic fingerprint generation," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 154–159.

[31] A. Lanitis, C. J. Taylor, and T. F. Cootes, "Toward automatic simulation of aging effects on face images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 4, pp. 442–455, 2002.

[32] J. Suo, F. Min, S. Zhu, S. Shan, and X. Chen, "A multi-resolution dynamic model for face aging simulation," in *IEEE Conference on Computer Vision and Pattern Recognition*, 2007, pp. 1–8.

[33] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in *European Workshop on Biometrics and Identity Management*. Springer, 2008, pp. 181–190.

[34] K. W. Bowyer and J. S. Doyle, "Cosmetic contact lenses and iris recognition spoofing," *Computer*, vol. 47, no. 5, pp. 96–98, 2014.

[35] H. Zhang, Z. Sun, and T. Tan, "Contact lens detection based on weighted LBP," in *International Conference on Pattern Recognition*, 2010, pp. 4279–4282.

[36] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 385–395, 2011.

[37] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[38] Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, pp. 1120–1133, 2014.

[39] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Detecting medley of iris spoofing attacks using DESIST," in *IEEE International Conference on Biometrics Theory, Applications and Systems*, 2016, pp. 1–6.

[40] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "An investigation of local descriptors for biometric spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 849–863, 2015.

[41] P. Silva, E. Luz, R. Baeta, D. Menotti, H. Pedrini, and A. X. Falcao, "An approach to iris contact lens detection based on deep image representations," in *Conference on Graphics, Patterns and Images*, 2015, pp. 157–164.

[42] O. V. Komogortsev, A. Karpov, and 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, 2015.

[43] D. Menotti, G. Chiachia, A. Pinto, W. Robson Schwartz, H. Pedrini, A. Xavier Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 864–879, 2015.

[44] J. S. Doyle and K. W. Bowyer, "Robust detection of textured contact lenses in iris recognition using BSIF," *IEEE Access*, vol. 3, pp. 1672–1683, 2015.

[45] R. Raghavendra and C. Busch, "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 703–715, 2015.

[46] Y. Hu, K. Sirlantzis, and G. Howells, "Iris liveness detection using regional features," *Pattern Recognition Letters*, vol. 82, pp. 242–250, 2016.

[47] D. Yadav, N. Kohli, S. Yadav, M. Vatsa, R. Singh, and A. Noore, "Iris Presentation Attack via Textured Contact Lens in Unconstrained Environment," in *IEEE Winter Conference on Applications of Computer Vision*, 2018, pp. 503–511.

[48] A. Kuehlkamp, A. Pinto, A. Rocha, K. W. Bowyer, and A. Czajka, "Ensemble of multi-view learning classifiers for cross-domain iris presentation attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1419–1431, June 2019.

[49] K. B. Raja, R. Raghavendra, and C. Busch, "Color Adaptive Quantized Patterns for Presentation Attack Detection in Ocular Biometric Systems," in *ACM International Conference on Security of Information and Networks*, 2016, pp. 9–15.

[50] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems*, 2014, pp. 2672–2680.

[51] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," in *International Conference on Learning Representations*, no. 2014, 2013, pp. 1–14.

[52] M. Mirza and S. Osindero, "Conditional generative adversarial nets," *CoRR*, vol. abs/1411.1784, 2014.

[53] E. L. Denton, S. Chintala, R. Fergus *et al.*, "Deep generative image models using a Laplacian pyramid of adversarial networks," in *Advances in Neural Information Processing Systems*, 2015, pp. 1486–1494.

[54] X. Chen, Y. Duan, R. Houthooft, J. Schulman, I. Sutskever, and P. Abbeel, "InfoGAN: Interpretable representation learning by information maximizing generative adversarial nets," in *Advances in Neural Information Processing Systems*, 2016, pp. 2172–2180.

[55] R. Yeh, C. Chen, T. Lim, M. Hasegawa-Johnson, and M. N. Do, "Semantic image inpainting with perceptual and contextual losses," *CoRR*, vol. abs/1607.07539, 2016.

[56] X. Wang and A. Gupta, "Generative image modeling using style and structure adversarial networks," in *European Conference on Computer Vision*, 2016, pp. 318–335.

[57] C. Ledig, L. Theis, F. Huszar, J. Caballero, A. P. Aitken, A. Tejani, J. Totz, Z. Wang, and W. Shi, "Photo-realistic single image super-resolution using a generative adversarial network," *CoRR*, vol. abs/1609.04802, 2016.

[58] A. Shrivastava, T. Pfister, O. Tuzel, J. Susskind, W. Wang, and R. Webb, "Learning from simulated and unsupervised images through adversarial training," in *IEEE Conference on Computer Vision and Pattern Recognition*, 2017, pp. 1–10.

[59] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," *CoRR*, vol. abs/1511.06434, 2015.

[60] N. D. Kalka, J. Zuo, N. A. Schmid, and B. Cukic, "Image quality assessment for iris biometric," in *Defense and Security Symposium*. International Society for Optics and Photonics, 2006, pp. 62 020D–62 020D.

[61] M. Vatsa, R. Singh, and A. Noore, "Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 38, no. 4, pp. 1021–1035, 2008.

[62] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern Recognition*, vol. 43, no. 3, pp. 1016 – 1026, 2010.

[63] S. Bharadwaj, M. Vatsa, and R. Singh, "Biometric quality: a review of fingerprint, iris, and face," *EURASIP Journal on Image and Video Processing*, vol. 2014, no. 1, p. 34, 2014.

[64] "Information Technology - Biometric Sample Quality."

[65] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[66] VeriEye, "Iris recognition software," http://www.neurotechnology.com/verieye.html.

[67] N. Evans, S. Z. Li, S. Marcel, and A. Ross, "Guest editorial: Special issue on biometric spoofing and countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 699–702, 2015.

[68] C.-W. Tan and A. Kumar, "Automated segmentation of iris images using visible wavelength face images," in *Computer Vision and Pattern Recognition Workshops*, 2011, pp. 9–14.

[69] ——, "Accurate iris recognition at a distance using stabilized iris encoding and zernike moments phase features," *IEEE Transactions on Image Processing*, vol. 23, no. 9, pp. 3962–3974, 2014.

[70] Z. Guo, L. Zhang, and D. Zhang, "Rotation invariant texture classification using LBP variance (LBPV) with global matching," *Pattern recognition*, vol. 43, no. 3, pp. 706–719, 2010.

[71] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[72] D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, and S. Schuckers, "Livdet-iris 2013-iris liveness detection competition 2013," in *IEEE International Joint Conference on Biometrics*, 2014, pp. 1–8.

[73] A. Brock, J. Donahue, and K. Simonyan, "Large scale GAN training for high fidelity natural image synthesis," *CoRR*, vol. abs/1809.11096, 2018.

[74] I. Tolstikhin, O. Bousquet, S. Gelly, and B. Schoelkopf, "Wasserstein auto-encoders," *arXiv preprint arXiv:1711.01558*, 2017.