

Iris Anti-Spoofing Using Image Quality Measures

Hussaini Habib

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Engineering

Eastern Mediterranean University
January 2019
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Assoc. Prof. Dr. Ali Hakan Ulusoy
Acting Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Computer Engineering.

Prof. Dr. Hadi Işık Aybay
Chair, Department of Computer
Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Computer Engineering.

Assoc. Prof. Dr. Önsen Toygar
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Duygu Çelik Ertuğrul

2. Assoc. Prof. Dr. Önsen Toygar

3. Asst. Prof. Dr. Mehtap Köse Ulukök

ABSTRACT

Spoof detection is a critical issue for the recognition of iris because it reduces the risk of forging iris recognition systems. The most relevant iris spoofing attacks reported in previous studies follows one of the three trends: photo attacks, contact-lens attacks or artificial-eye attacks. Spoofing attacks have prompted the biometric research community to learn more about the threat posed by these kinds of attacks on iris, fingerprint and face biometric systems.

In this thesis, various Image Quality Assessment techniques to detect fake and real iris images presented to biometric systems were used. In this context, full reference image quality assessment measures such as Error Sensitivity Measures, Structural Similarity Measures and Information Theoretic Measures are implemented to distinguish fake and real iris images.

Full-reference Image Quality Measures are also concatenated using feature-level fusion strategy. We propose to fuse twenty one full-reference image quality measures for iris anti-spoofing against print-attacks, contact-lens attacks and artificial-eye attacks.

In order to evaluate the performance of the proposed iris anti-spoofing method using feature-level fusion of Image Quality Assessment techniques, two publicly available databases, namely CASIA and IIITD, were used. A comparative analysis of the performance of these Image Quality Assessment metrics is performed towards the completion of the thesis on various iris spoofing datasets of the aforementioned iris spoofing databases.

Keywords: Spoof Detection, Iris recognition, Photo Attack, Contact Lens Attack,
Image Quality Assessment.

ÖZ

İris tanıma sistemlerinde, saldırı tespiti kritik bir konudur, çünkü bu işlem sistemin güvenilirliğini kaybetme riskini azaltır. Literatürde bahsedilen en belirgin iris yanıltma saldırısı; fotoğraf saldırısı, kontak lens saldırısı ve yapay göz saldırısı olarak üç çeşit olarak belirlenmiştir. İris, paramakizi ve yüz biyometri sistemlerine yapılan yanıltma saldırıları, biyometri alanında çalışma yapan araştırmacıları bu yöndeki tehditler üzerinde çalışmaya yöneltmiştir.

Bu tezde, biyometrik sistemler için kullanılan gerçek ve sahte iris görüntülerinin tespiti için birçok Görüntü Kalitesi Değerlendirme tekniği kullanılmıştır. Bu bağlamda, Hata Hassasiyeti Ölçümü, Yapısal Benzerlik Ölçümü, Kuramsal Bilgi Ölçümü gibi kaynağa bağlı Görüntü Kalitesi Değerlendirme teknikleri, sahte ve gerçek iris görüntülerinin ayırt edilmesi için uygulanmıştır.

Görüntü Kalitesi Değerlendirme teknikleri ayrıca öznitelik-seviyesi kaynaşımı ile birleştirilerek yeni bir yöntem önerilmiştir. Önerilen yöntemde, yirmi bir Görüntü Kalitesi Değerlendirme tekniği birleştirilip, yazdırma saldırısı, kontak lens saldırısı ve yapay göz saldırısına karşı yanıltma karşıtı bir yöntem geliştirilmiştir.

Öznitelik-seviyesi kaynaşımı kullanarak Görüntü Kalitesi Değerlendirme tekniklerini birleştiren önerilen iris yanıltma karşıtı yöntemin performansı, CASIA ve IIITD iris veritabanları kullanılarak yapılmıştır. Görüntü Kalitesi Değerlendirme tekniklerinin karşılaştırmalı performans analizi, belirtilen iris veritabanlarının çeşitli veri kümeleri üzerinde yapılmış ve tezin sonunda sunulmuştur.

Anahtar Kelimeler: Saldırı Tespiti, İris Tanıma, Fotoğraf Saldırısı, Kontak Lens Saldırısı, Görüntü Kalitesi Değerlendirme.

DEDICATION

I dedicate this research work to my lovely parents, siblings and friends who in one way or the other contribute towards the successful completion of this work.

ACKNOWLEDGEMENT

All praise is due to Almighty Allah who from the beginning guided me to complete this research work successfully. Also, my family for their prayers, support and encouragement they have always shown me towards my educational career.

My appreciation goes to my supervisor, Assoc. Prof. Dr. Önsen Toygar, for her immeasurable attention and supervision throughout the cause of this work.

TABLE OF CONTENTS

ABSTRACT.....	iii
ÖZ.....	v
DEDICATION.....	vii
ACKNOWLEDGEMENT.....	viii
LIST OF TABLES.....	xiii
LIST OF FIGURES.....	xiv
LIST OF ABBREVIATIONS.....	xv
1 INTRODUCTION.....	1
1.1 General Overview.....	1
1.2 Biometric Recognition System.....	1
1.3 The Authentication Modes of a Biometric-based System.....	3
1.3.1 The Enrollment Mode.....	4
1.3.2 The Authentication Mode.....	4
1.4 Problem Statement.....	5
1.5 Objective of Research Work.....	5
2 LITERATURE REVIEW.....	6
2.1 Review of FR-IQA.....	6
3 IRIS SPOOFING.....	12
3.1 Spoofing.....	12
3.1.1 Photo Attacks.....	13
3.1.2 Contact Lens Attacks.....	14
3.1.3 Artificial Eye Attacks.....	15
3.2 Anti-Spoofing Techniques.....	16

3.2.1 Iris Anti-Spoofing Techniques	16
3.2.1.1 Sensor-level Anti-Spoofing Techniques	16
3.2.1.2 Feature-Level Anti-Spoofing Techniques.....	17
3.2.1.3 Score-Level Anti-Spoofing Techniques.....	18
4 IMAGE QUALITY ASSESSMENT (IQA)	19
4.1 Error Sensitivity Measures	21
4.1.1 Pixel Difference Measures	21
4.1.2 Correlation-based Measures.....	21
4.1.3 Edge-based Measures.....	21
4.1.4 Spectral Distance Measures.	22
4.1.5 Gradient-based Measures.	22
4.2 Structural Similarity Measures	22
4.3 Information Theoretic Measures.....	23
4.4 FR-IQA and Their Mathematical Representation.....	23
4.4.1 Mean Squared Error (MSE)	23
4.4.2 Peak Signal to Noise Ratio (PSNR).....	24
4.4.3 Signal to Noise Ratio (SNR).....	24
4.4.4 Structural Content (SC).....	24
4.4.5 Maximum Difference (MD).....	24
4.4.6 Averaged Difference (AD).....	25
4.4.7 Normalized Absolute Error (NAE)	25
4.4.8 R-Averaged Maximum Difference (RAMD).....	25
4.4.9 Laplacian Mean Squared Error (LMSE)	25
4.4.10 Normalized Cross Correlation (NXC)	26
4.4.11 Mean Angle Similarity (MAS).....	26

4.4.12 Mean Angle Magnitude Similarity (MAMS).....	26
4.4.13 Total Edge Difference (TED).....	27
4.4.14 Total Corner Difference (TCD).....	27
4.4.15 Spectral Magnitude Error (SME).....	27
4.4.16 Spectral Phase Error (SPE).....	27
4.4.17 Gradient Magnitude Error (GME).....	28
4.4.18 Gradient Phase Error (GPE).....	28
4.4.19 Structural Similarity Index Measure (SSIM).....	28
4.4.20 Visual Information Fidelity (VIF).....	29
4.4.21 Reduced Reference Entropic Difference (RRED).....	29
5 PROPOSED METHOD.....	30
5.1 Feature Extraction.....	31
5.2 Feature-Level Fusion (FLF).....	31
5.3 Matching.....	32
5.4 Classification.....	33
6 EXPERIMENTS AND RESULTS.....	34
6.1 Experimental Setup.....	34
6.2 Databases used for the experiment.....	34
6.2.1 Casia Iris V1.....	34
6.2.2 CASIA-Iris-Syn.....	35
6.2.3 IIITD Combined Spoofing Database.....	36
6.2.3.1 IIITD-CLI Database.....	36
6.2.3.2 IIITD-IIS Database.....	36
6.3 Experimental Results.....	37
7 CONCLUSION.....	49

REFERENCES 51

LIST OF TABLES

Table 1: Summary of Literature Review on Image Quality Assessment	11
Table 2: Summary of Databases used in the experiment.....	37
Table 3: Attack with Synthetic Samples Using CASIA Iris V1 & Iris –Syn.....	38
Table 4: Print Attack using Cogent Dataset.....	40
Table 5: Scan Attack using Cogent dataset.....	41
Table 6: Colored Contact Lens Attack using CLI Cogent Dataset.....	42
Table 7: Transparent Contact Lens Attack using CLI Cogent Dataset	43
Table 8: Print Attack using Vista IIS Dataset.....	44
Table 9: Scan Attack using IIS Vista Dataset.....	45
Table 10: Colored Contact Lens Attack using CLI Vista Dataset.....	46
Table 11: Transparent Contact Lens Attack using CLI Vista Dataset.....	47
Table 12: Summary of Iris Spoofing Attacks and Results	48

LIST OF FIGURES

Figure 1: Diagram of a Biometric System.....	12
Figure 2: Real Iris Images and Their Fake Counterparts using Photo Attacks.....	14
Figure 3: Real Iris Images and Their Fake Counterparts using Contact Lens Attacks.....	15
Figure 4: Real Iris Images and Their Fake Counterparts using Iris Synthetic Attack.....	15
Figure 5: 21 Full Reference IQA Techniques	20
Figure 6: Block Diagram of Proposed Method.....	31
Figure 7: Iris Camera used for Capturing CASIA-IrisV1.....	35
Figure 8: First Session and Second Session Typical Iris Image That may be found in the Database.....	35

LIST OF ABBREVIATIONS

AD	Average Difference
CASIA	Chinese Academy of Sciences Institute
CLI	Contact Lens Iris
CSD	Combined Spoofing Database
DFT	Discrete Fourier Transformation
DLF	Decision Level Fusion
DOG	Difference of Gaussians
FFR	False Fake Rate
FGR	False Genuine Rate
FLF	Feature level Fusion
FR	Full Reference
GME	Gradient Magnitude Error
GPE	Gradient Phase Error
HOG	Histogram of Oriented Gradients
HVS	Human Visual System
ICA	Independent Component Analysis
IITD	Indraprastha Institute of Information
IQA	Image Quality Assessment
IQM	Image Quality Metric
ISD	Iris Spoof Database
LBP	Local Binary Pattern
LDA	Linear Discriminant Analysis
LMSE	Laplacian Mean Square Error

MAMS	Mean Angle Magnitude Similarity
MAS	Mean Angle Similarity
MD	Maximum Difference
MSE	Mean Square Error
NAE	Normalized Absolute Error
NR	No Reference
NXC	Normalized Cross Correlation of Automation
PNSR	Peak Signal to Noise Ratio
QDA	Quadratic Discriminant Analysis
RAMD	R-Averaged Maximum Difference
RR	Reduced Reference
RRED	Reduced Reference Entropy Distortion
SC	Structural Content
SFF	Sparse Fidelity Feature
SME	Spectral Magnitude Difference
SNR	Signal to Noise Ratio
SPE	Spectral Phase Error
SSIM	Structural Similarity Index Measure
SVD	Singular Values Decomposition
TCD	Total Corner Difference
	Technology Delhi
TED	Total Edge Difference
VIF	Visual Information Fidelity

Chapter 1

INTRODUCTION

1.1 General Overview

Traditionally, the use of identity cards, password and PINs to create an invulnerable and reliable environment has been in practice for years. Today, due to the growing situation of illegal and terrorism acts and the improved use of electronic commerce, more efficient and invulnerable biometrics systems are urgently needed in confirming the behavioral or physical traits possessed by a person because these traits are permanent to the person and cannot be forgotten or lost just as the way a person forgets his/her password in a normal system [1]. The systems that use these functions include personal computer systems, reliable internet banking system, digital cellphones and building access control. An individual could be identified primarily based on 'who he/she is' as an alternative to (what the individual has) or (what he/she knows) when using the biometrics system [1].

1.2 Biometric Recognition System

The biometric recognition system operates by acquiring physiological or behavioral traits of an individual, extracting some specific feature set from the obtained data traits and comparing the feature set against a biometric database. A biometric recognition system can function as an authentication system or recognition system depending on the area of its application [1].

In the verification mode, the system validates the identity of an individual by comparing the acquired biometric traits with the biometric template(s) stored in the biometric system database. In such a system, a person who wishes to be recognized claims an identity, usually via personal trait possessed by the individual, and the system conducts a comparison to determine whether or not the biometric data belongs to the person. Identity verification is typically used for positive recognition where multiple people are prevented from using the same identity [2].

In verification mode, the system validates an individual identity by searching for a match through the database template corresponding to all users. Therefore, the system employs a one-to-many comparison to authenticate an individual's identity (or fails if the subject is not registered in the system database) without the subject claiming an identity.

In a biometric system application, the motive to capture an intruder dominates the difficulty of examining a wide range of falsely accused individuals, but false rejection is minimal. Most civil applications, such as ATM access, computer login, require optimal false acceptance and false rejection. Face and voice can be considered an apparent choice for the identification system (police and surveillance applications) because of its non-intrusive acquisition, even for non-cooperative subjects, without one's knowledge, whereas fingerprint and palm-printing can be considered better for the verification system (access control and e-commerce applications) because of their higher stability and uniqueness.

Access to a protected facility or information can only be granted to genuine users with a well-structured biometric system. The system evaluates the specific physical and

behavioral characteristics of an individual extracted and interpreted by computers using certain devices. The fact that users must carry or take identification data into account is also convenient. In many countries, increasingly biometric applications are used in daily life mainly driven by bio-passports. Nevertheless parties must still take a critical security problem into consideration, despite a stimulating and rapidly developing market: the vulnerability to attack, in other words the system seeks to subvert and bypass.

Traditional biometric techniques, like face or fingerprint recognition, have been proved vulnerable to one of the biggest and most negative threats to personal information-identity fraud. Spoofing, also referred to as a display attack, is a direct sensor attack beyond the digital limits of the system. Digital safety mechanisms cannot therefore be used for this purpose. An intruder tries to spoof a biometric system by making a fake biometric pattern and presenting the biometric sensor as a legitimate user. Anti-spoofing means ways in which an intruder has access to the bio-metric system, and prevents it from doing so. Complementary to anti-spoofing modules, commercial biometric authentication products would put high risk to personal safety [1].

1.3 The Authentication Modes of a Biometric-based System

Biometric identification systems are the most effective ones because they do not recognize the physical media, but the unique physical characteristics of a human. Access and data protection systems, based on such technologies, are not only the most reliable but also the most user-friendly nowadays.

1.3.1 The Enrollment mode

In enrollment mode, the biometric data of a user is captured and stored in a database using a biometric reader. The stored template data is marked with a personal identity such as name and identity number in order to facilitate authentication [4].

1.3.2 The Authentication mode

Authentication mode involves capturing the biometric trait of a person and using it by the biometric system to recognize who the person is or validate the individual's claimed identity. While identification process of analyzing the biometric information stored in templates that correspond to all users in the database, verification includes evaluation with only those templates that matched the claimed identity [4]. There are therefore two different problems with their own inherent complexities, identification and verification. There are four key features of a simple biometric system:

- 1) Sensor module: Captures a person's biometric information. An example is a fingerprint that is captured by a fingerprint sensor.
- 2) Feature extraction module: Captures information and processes the information to extract some specific characteristic values.
- 3) Matching Module: Compares the extracted characteristic values to those in the template by generating a matching score.
- 4) Decision-making module: Uses the generated matching score in the matching module to make decision either to accept or reject the identity claimed by the user. False Fake Rate (FFR) and False Genuine Rate (FGR) are reported to determine a biometric system's overall performance.

1.4 Problem Statement

Spoof detection is an essential issue for the recognition of iris because it decreases the chance of forging iris recognition systems. Spoofing attacks have prompted the biometric community to make more research on the vulnerabilities of fraudulent actions regarding to iris, fingerprint, face and multimodal approaches. In order to carry out a fraudulent attack, the impostor applies some kind of synthetically developed artifact (e.g., rubber finger, face mask or printed iris image) to gain fraudulent access to the biometric system.

1.5 Objective of Research Work

The objective of this research work is to develop a system that further enhances the protection of the biometric recognition system using image quality assessment. The system should be easy to use, fast and non-intrusive. In this research work, a new anti-spoofing protection system is suggested, which employs the combination of a complete full reference image quality evaluation to detect genuine and impostor iris images in iris recognition systems. The system can work under various biometric systems with excellent performance and also for various spoofing schemes; it also offers an excellent level of security for particular non-spoofing attacks.

Chapter 2

LITERATURE REVIEW

Literature indicates that many researchers in previous years have helped to improve the measurement of image quality. Articles published in journals, lectures and publications are referred to for literature surveys. In order to understand their consequences and the possibility of extending it, the literature based solely on all the parameters is analyzing in the non-reference color image quality assessment. Researchers can categorize the models in three main categories. They are Full Reference Image Quality Assessment (Error Sensitivity Measures, Structural Similarity and Information Theoretic Measures), Reduced Reference Image Quality Assessment (RR-IQA) metrics and No-Reference Image Quality Assessment (Distortion Specific Measures, Training Based Measures and Natural Scene Statistics Measures). Literature indicates that these quality assessment models are also divided into two classes in each course as image-quality measures for gray images and exceptional color image measures [5].

2.1 Review of FR-IQA

The improvement of IQA model research started with Full Reference (FR) image quality measurements. Image quality metrics have traditionally been used for image fidelity measures such as the Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) [6]. Although they are simple, they are positive [7]. The study signifies that the majority of FR-IQA measurements are based mainly on structural similarity.

Wang et al. [7] suggested a method that utilizes structural similarity as an alternative inspiring principle in the design of image quality measures. Structural Similarity Index (SSIM) was developed to demonstrate an idea of structural similarity and to measure the variation between a reference and the degraded image. The metric has a much better result than traditional image fidelity measures in image databases with different distortions.

Wang et al. [8] proposed a new method of image quality assessment established on structural similarity of multiple scales. When linking the various viewing and image resolution requirements, the proposed approach provides more strength than the usual single-scale strategy. They utilized a way used to calibrate parameters for the relative importance of scales in the image synthesis. The test results show that the technique works well with the SSIM single-scale version and with modern image quality metrics.

Liao and Chen [9] suggested enhanced Double Scale Edge Structure Similarity (MDSSIM) based IQA algorithm. The proposed algorithm takes the information in the Structural Information of the image edge adequately into account and incorporates the edge structure distortion metric in the IQA.

Chang et al. [10] suggested a new full reference IQA based on Sparse Fidelity Feature (SFF). The method uses a sparse correlation coefficient, which is captured by a feature detector trained by the Independent Component Analysis (ICA) algorithm on samples of natural images to obtain the sparse image codes. The sparse correlation coefficient is calculated to record the relationship between the output sets acquired in the receptive field from a sparse single cell model. The results of the proposed method show that SFF works better in matching subjective ratings than the leading IQM.

In order to foretell distortions in a large number of noise sources, Shnayderman et al. [11, 12] proposed a new method to measure image quality on the basis of a Singular Value Decomposition (SVD), multidimensional image quality or scalar measurement. Therefore, they are employed to determine the variation between images. The original and test images have been divided into blocks and each block is equipped with a SVD. They employed the method for determining the error value between the small blocks of the two images and combining the error scores to predict the picture quality. The error values are calculated between the corresponding image blocks, and the image quality is predicted with the integration of error scores.

Narwaria and Lin [13] suggested a method that uses SVD-based machine learning to evaluate visual quality. They used SVD to obtain image features and then used machine learning to combine features that are effective in predicting image quality. They also proposed machine learning to pool features because they are more systematic and data driven. The result shows that the method proposed exceeds the schemes available.

Wang et al. [14] suggested an effective evaluation technique based on a quaternion description of color image structural information. The color picture has a local variance and luminance layer calculated and three imaginary parts of the quaternion encoded in the RGB channel. To calculate the amount of structural similarity, they used the angle formed by the single vectors of the two quaternion matrices.

Narwaria et al. [15] suggested a new IQA algorithm that uses phase and magnitude of the Discrete Fourier Transformation. The proposed technique considers variations in the sensitivity of the human eye to different frequency components. They used a linear

regression technique to merge the acquired value in phase and magnitude changes. The proposed algorithm uses scalability to minimize the amount of reference data. The proposed method is much better than most current complete references, according to experimental results.

Farmanbar and Toygar [16] proposed a new protection approach for fusion methods based on texture and IQA metrics. In this study, the characteristics of the given image are extracted using Difference of Gaussians (DOG), Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG). To minimize the scope of the extracted feature vector, Linear Discriminant Analysis (LDA) and Principal Component Analysis were used. In addition, 7 comprehensive reference image quality measures have been implemented to evaluate image quality. The experiment was performed using the three publicly available spoof databases and the results show a significant improvement in the classification error rate over existing systems.

Pravallika and Prasad [17] proposed a software-based biometric detection technique to detect fake biometric trait. Multiple biometric systems can employ this method to detect variations in spoof attacks. This software-based spoof detection method uses image quality assessment, as the fake image acquired in a spoof attack is of different quality than the genuine sample captured using the normal process designed for the sensor. The method proposed merged iris, face and palm-print images to obtain a single image. Image quality measures are calculated for the fused images and in decision making (i.e. real or fake) the Support Vector Machine (SVM) classifier was used.

Galbally and Marcel [18] proposed a new method of protection using 14 full reference IQMs. These IQMs are extracted from an image and fused using the Linear Discriminative Analysis classifier to discover authentic and impersonator access attempts. The results obtained in that research reveal that the analysis of legit facial samples contains important information to discriminate effectively against impostor images.

Wei et al. [19] suggested three measures to discover impostor iris with printed color contact lens using texture analysis. They proposed a method to define the visual primitives of iris textures using the measurement of sharpness in the edges of the iris, Iris-Texton and some attributes based on co-existing matrix characteristics. The results show the effectiveness of the proposed method.

Wang et al. [20] proposed a method of IQA based on HVS structural similarity (HSSIM). In addition, the proposed measure is based on the frequency and special characteristics of HVS. The results obtained show that this method has better performance than PSNR and SSIM for badly blurred images.

Toprak and Toygar [21] proposed a novel method which employs fusion of full-reference and no-reference IQM's to detect real and fake ear biometric images. The method focused on print attacks scheme, and achieves better results against feature-level fusion method on AMI and UBEAR ear databases.

Table 1 demonstrates a summary of the literature review on image quality assessment for different biometric traits. Additionally, the table presents various research studies with details of the systems and performances obtained in different metrics.

Table 1: Summary of Literature Review on Image Quality Assessment

Reference	Number of images	Algorithm		FFR	FGR	HTER	Recognition Rate
[7]	175 JPEG and 169 JPEG2000	SSIM		N/A	N/A	N/A	96%
[8]	60 images	MSSIM		N/A	N/A	N/A	96%
[9]	401 distorted images	(MDESSIM)		N/A	N/A	N/A	80%
[10]	3,806 images	Sparse Feature Fidelity (SFF)		N/A	N/A	N/A	92%
[11]	30 images	Singular Value Decomposition		N/A	N/A	N/A	99%
[12]	5 images	Singular Value Decomposition Gray scale		N/A	N/A	N/A	92%
[13]	4042 test images and two for video with a total of 228	Singular Value Decomposition		N/A	N/A	N/A	70%
[14]	1 original image and 5 distorted image	Quaternion description for the structural information of color image		N/A	N/A	N/A	N/A
[15]	A total of 3832 distorted images and 228 distorted videos).	Fourier Transform		N/A	N/A	N/A	90% for Q-phase (4) and Q-phase (5)
[16]	700 images	Texture-based methods	LBP	60	35.7	47.8	N/A
	DOG		56.2	61.4	58.8		
	HOG		40	43.7	41.8		
[17]	Fusion of iris, face and palmprint images	SVM	Iris	0.11	2.2	1.15	N/A
	Face		1.1	2.2	1.65		
	Palmprint		9.2	10.1	9.65		
[18]	50 different subjects	14 full reference IQMs		17.9	12.5	15.2	N/A
[19]	DB1 320, DB2 960	Texture Analysis (iris edge sharpness)		2.5	1.87	2.2	N/A
[20]	633 images	HVS-based Structural Similarity		N/A	N/A	N/A	92% on Gaussian blurred image , 93% on all images
[21]	200 images	Decision-level fusion	UBEAR DB	9.00	22.00	15.50	N/A
			AMI DB	11.00	6.00	8.50	

Chapter 3

IRIS SPOOFING

3.1 Spoofing

Biometric systems are widely used technologies in order to verify or identify the living individual based on physiological or behavioral characteristics. Biometric sensors or camera are used in biometric recognition systems to acquire biometric images. The quality of the acquired image is enhanced for further analysis, then the most important features for recognizing the identity of the user is extracted from the acquired biometric image using feature extraction technique. Prior to the deployment of the biometric systems, there exists database template comprising of image features stored in the database to be used in the comparison of biometric images recently acquired for decision making [1]. Figure 1 demonstrates the general diagram of a biometric system.

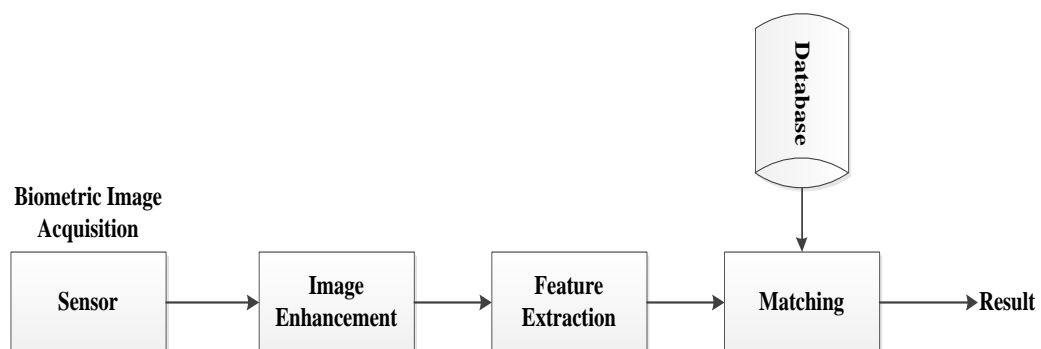


Figure 1: Diagram of a Biometric system

The vulnerability of biometric systems attracts fraudulent attacks by means of the above mentioned processes. Especially, the intruders can easily use the sensor module

as a way to fool the biometric system. With this, fake biometric image can be presented to the sensor. Spoofing is a technique of fooling the biometric system by using a fake biometric trait. Spoof detection is a way of distinguishing a real biometric trait from the fake biometric trait.

There exist many types of intruders who may attempt to spoof a biometric system for many reasons. Firstly, an individual may hide his/her identity to enter another country by using artificial mask, contact lens or fingerprint. Secondly, an intruder is an individual who wants to gain access to another individual's account by imitating his/her biometric trait. Thirdly, a person who uses artificial biometrics to be enrolled in a biometric system can share the identity with another person so that multiple people can have access to the system through a common biometric feature. In sensitive security applications, iris recognition has gained popularity. Various strategies may be used to attack and detect the iris. Facilitative attacks centered on the sensor, data transmission phase, the level of image processing, the phase for pattern recognition, the level or decision of a database can be initiated [22-23].

Spoofing attacks can damage the iris identity checking system effectively by tempering the results. The vulnerability of iris detection systems in high-level safety scenarios has prevented their deployment. Therefore, intelligent self-protection strategies are far from necessary to discover and protect possible attacks on iris systems. The main types of iris spoofing attacks are explained in the following subsections.

3.1.1 Photo Attacks

Photo attacks were the initial attacks to be reported in the literature and continue to gain popularity because of their outstanding ease and, in many cases, their high

achievement rate. Photo attacks are achieved by presenting an image of the real iris to the biometric sensor [24, 25]. The image is usually printed on a paper sheet (e.g. print-attacks). Another common possibility is to display the image on a digital device like a tablet or smart phone (digital-photo-attacks). Figure 2 shows real images and their fake counterparts.

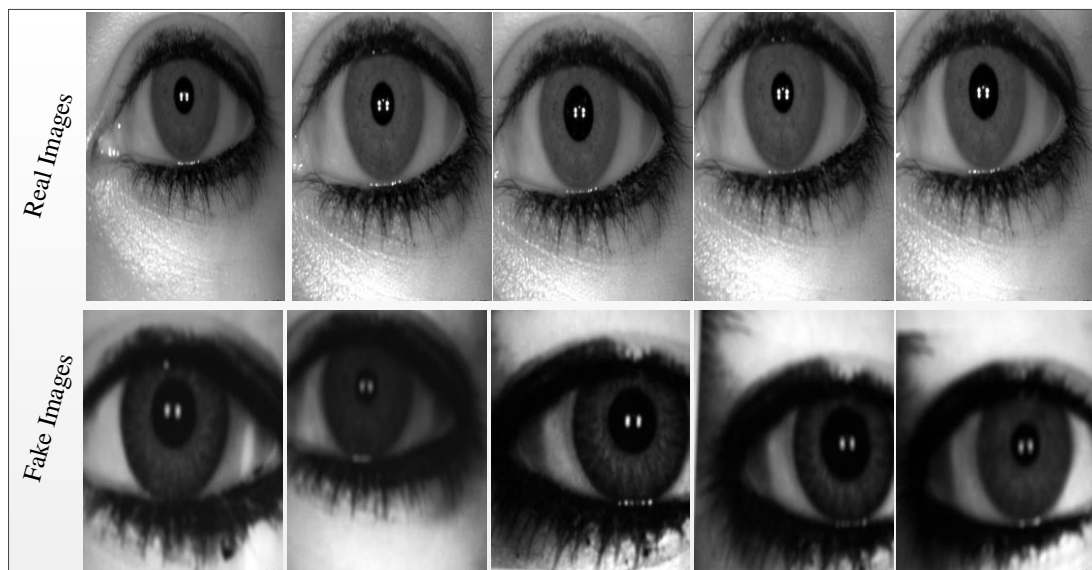


Figure 2: Real iris images and their fake counterparts using photo attacks.

3.1.2 Contact Lens Attacks

Contact lens attacks are carried out with the help of contact lenses. The attacker prints the sample of a genuine iris image onto a contact lens which is used during the entire biometric system attack. Such attacks are very hard to discover even with the help of human operators and will become a major task for automatic protection methods, as all contextual and auxiliary iris information corresponds to the living eye information [19, 26]. Figure 3 shows iris images with contact lens and without contact lens.

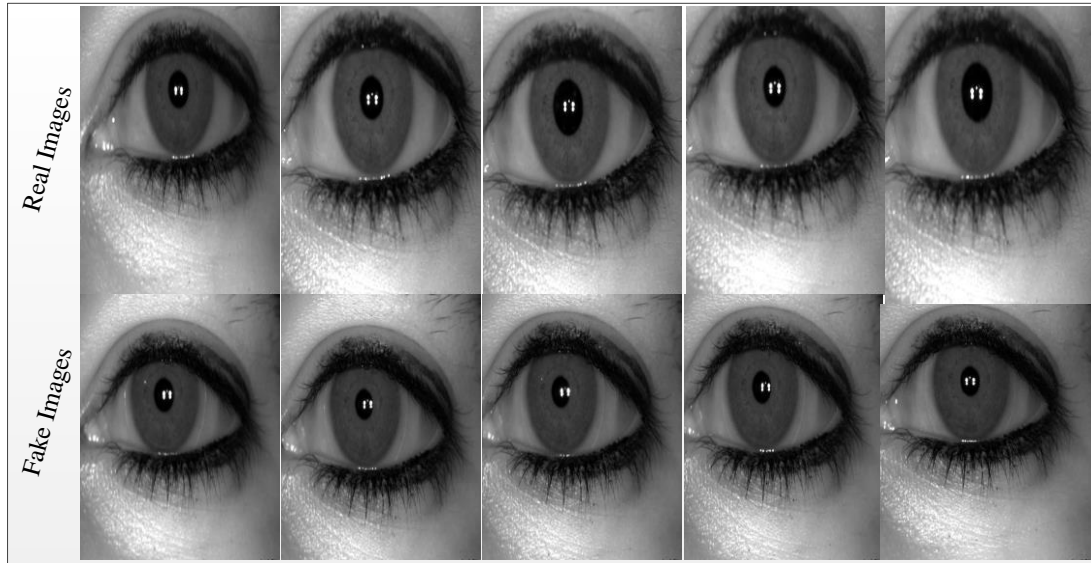


Figure 3: Real iris images and their fake counterparts using contact lens attacks

3.1.3 Artificial Eye Attacks

Artificial eye attacks are uncommon compared to the aforementioned attack types. An artificial eye attack has gained attention and has been systematically studied [26, 27]. Anti-spoofing techniques based on the analysis of the depth properties of the eye are more vulnerable to deception by using such replicas. Figure 4 shows real iris images and synthetic iris images.

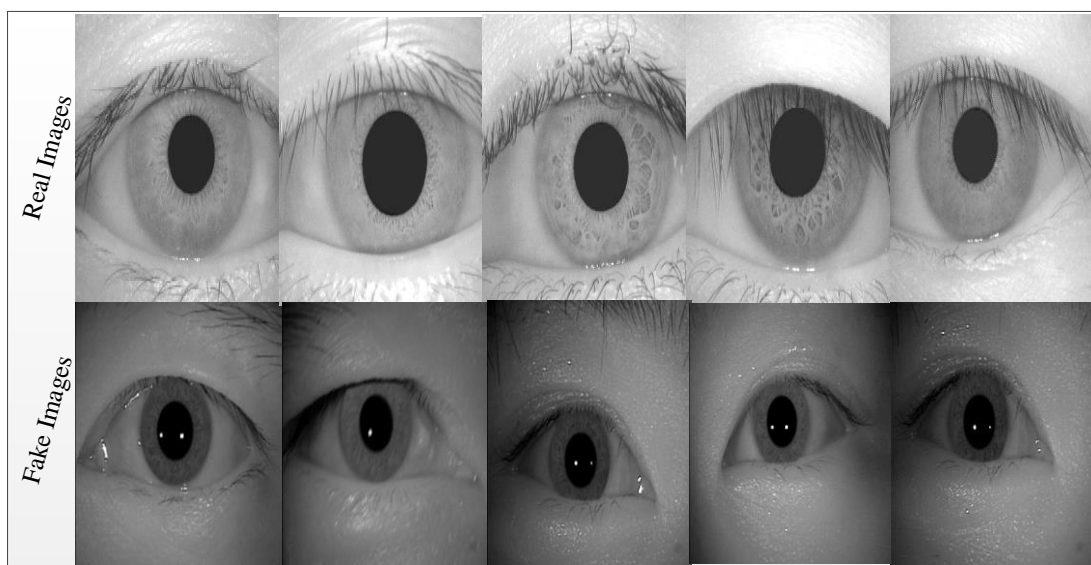


Figure 4: Real iris images and their fake counterparts using iris synthetic attack

3.2 Anti-Spoofing Techniques

Anti-spoofing techniques are automated techniques used to differentiate between genuine biometric features presented to the sensor and fake biometric or synthetically generated artifacts emulating the real feature [1]. Anti-spoofing techniques should meet certain requirements. Firstly, it must be non-invasive that means it should not harm the users of the biometric system or require too much contact with the user. Secondly, it needs to be user friendly. Thirdly, the method is required to be fast in order not to keep the user waiting. The technique also needs to be of low cost to be employed.

3.2.1 Iris Anti-Spoofing Techniques

Iris anti-spoofing techniques are designed to counteract physical spoofing attacks launched against iris recognition systems. Such attacks are directed at the sensor level and try gain access to the system by presenting a physical artifact to the acquisition device. The main iris anti-spoofing techniques are explained in the following subsections.

3.2.1.1 Sensor-level Anti-Spoofing Techniques

Sensor-level anti-spoofing techniques are techniques based on hardware. In these techniques, some hardware devices are added to the sensor to measure or identify certain specific characteristics of a living biometric trait (e.g. eye properties, blood pressure and fingerprint sweat). This helps to decide whether or not the biometric trait is alive.

Daugman [28] has gained fame for his pioneering and very successful early research works in the field of biometrics. Daugman is considered to be the father of automatic iris recognition; he presented some of the first iris biometric anti-spoofing

countermeasures using sensor-level anti-spoofing techniques [28]. According to his previous work, Daugman examined different fields of iris recognition and suggested certain eye-specific features that were used as hardware countermeasures to prevent direct iris biometric attacks. Another feasible group of anti-spoofing techniques highlighted in [2] are mechanisms related to behavioral eye features, such as the hippos or the person's reaction to an unexpected lighting event. Although there is no experimental validation of the above measures, he only gave individual examples as valid proof of the concept, his proposal laid the foundation for many of the sensor-based iris anti-spoofing schemes that were developed later in the literature.

3.2.1.2 Feature-Level Anti-Spoofing Techniques

Feature-level anti-spoofing techniques are software-based techniques. Features that are used to detect fake biometric trait are extracted from raw biometric image. These techniques are usually integrated in feature extraction. The light that enters the eye can mainly be reflected from the retina in the light source, which can be captured via an ordinary sensor without additional hardware, as long as the angle of the light source, the eye and the digital camera is less than 2.5 degrees. Though such anti-spoofing techniques would be very efficient for regular print attacks or even artificial eye attacks, their performance in contact lenses would be at least below question.

Automated feature-level technology has been developed by Pacut & Czajka [29] to analyze synthetic frequencies in printed iris images. In the same way, the wavelet transform, which comes with an SVM classifier, was also used for the detection of photo attacks in order to extract discriminatory aspects from the iris frequency spectrum.

3.2.1.3 Score-Level Anti-Spoofing Techniques

Most multimodal biometric recognition systems merge data at the score level because of the strong trade-off between ease of data integration and better information content. In addition, it is a quite simple way to combine scores extracted by different comparators (matchers). Score-level fusion is therefore the preferred technique for the fusion of biometric data and uses techniques that increase biometric system resistance to spoofing attacks.

Chapter 4

IMAGE QUALITY ASSESSMENT (IQA)

The quality variations between genuine and counterfeit samples include luminance and color levels, amount of data found in genuine and counterfeit images, sharpness level, local artifacts, structural or common appearance. For example, images of iris obtained from printed paper can be plausibly blurred or out of focus because of trembling [30]. In addition, this falsified image apparently lacks some of the properties of natural images when an artificial image is specifically infused into the communications line before the feature extractor. That is why the technique proposed gives another anti-spoofing technique that is not common but found recently in protection scenarios.

Three factors that support the reason for the use of Image Quality Assessment features for liveliness detection within the current state-of-the-art are as follows:

- Image quality assessment was success and was carried out in previous studies for image manipulation steganalysis in the digital forensic field. To a certain extent, a few spoofing attacks, especially those involving the capture of an iris image shown in a 2D device, such as spoofing attacks with printed iris images, could be seen as a type of image manipulation that can be effectively recognized by using different quality features.
- In addition to previous studies in the field of forensic research, there are different characteristics measuring characteristic quality properties that have

already been used for liveness detection in iris applications. A unique quality measure shows different sensitivities to image artifacts and distortions. For example, measures such as the mean squared error respond more to additive noise, while others, such as the spectral phase error, are more sensitive to blur; while gradient-related features react to distortions around edges and textures. Therefore, using a wide range of IQMs using complementary image quality properties, it should be possible to detect the aforementioned quality variations between real and fake samples expected to be found in several attack attempts. The above observations made us to believe that the hypothesis of “differences in quality” is sound and that measures in the quality of images may be successful in biometrics protection tasks.

- Human observers very often refer to the “different appearance” real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

Figure 4 shows a summary of full-reference IQA techniques.

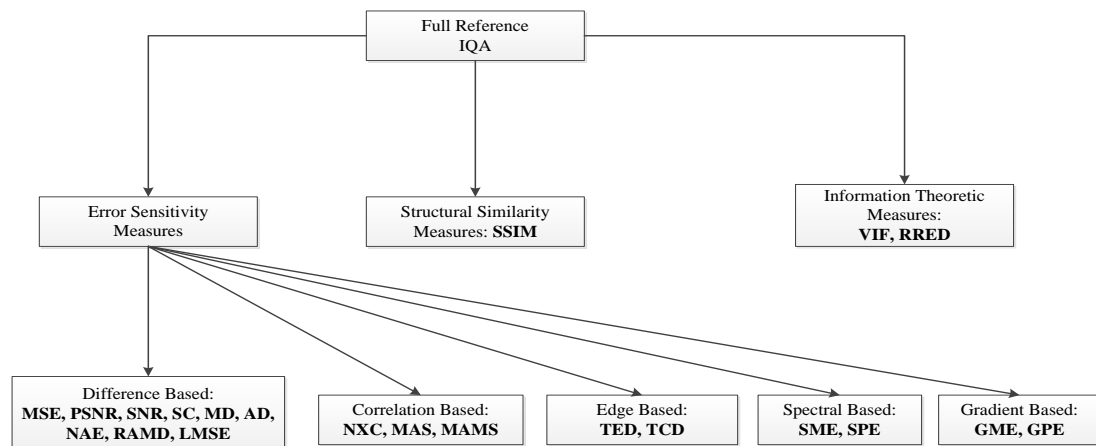


Figure 5: Full Reference IQA Techniques

Full reference IQM techniques are mainly divided into three categories as sensitivity measures, pixel difference measures and edge based measures. These techniques are reviewed in the following subsections.

4.1 Error Sensitivity Measures

Conventional perceptual image quality assessment approaches are based on measuring the errors (i.e. signal differences) between distorted and reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features. Although their potentials as signal fidelity measures are somewhat controversial, they are probably the most common method of IQA because they utilize many psychophysical features of the human visual system. Conventional approaches are also easy to calculate and usually have very poor computational complexity.

4.1.1 Pixel Difference Measures

Pixel difference features calculate the distortion in the pixel distinctions between two images. The examples of these measures are MSE, PSNR, and SNR, NAE, SC, RAMD, AD, MD, LMSE.

4.1.2 Correlation-based Measures

Correlation function can be used to determine the similarity between two images. A variation of correlation-based measures can be obtained by taking into account the statistics of the angles between the pixel vectors of the original and the distorted images. These features include MAS, MAMS and NXC.

4.1.3 Edge-based Measures

Edges and corners are some of the most informative parts of the image that play an important role in the human visual system and in many computer vision algorithms, including quality assessment applications. Since the structural distortion of an image is closely linked to its edge degradation, we have examined two edge-related quality

measures: TED and TCD. To accomplish both features, Sobel operator is used to build the binary edge maps of the original and distorted image and the Harris corner detector to calculate the number of corners found in the original and distorted image, respectively [30].

4.1.4 Spectral Distance Measures

The Fourier transform is another traditional image processing tool used in image quality evaluation. Spectral characteristics related to IQ that are considered in this thesis are SME and SPE.

4.1.5 Gradient-based Measures

Gradients contain essential visual information for quality evaluation. A gradient change reflects several distortions that can affect an image. Structural and contrast changes in an image can therefore be captured correctly with this information. The biometric protection system implemented in this thesis includes two simple gradient-based features namely GME and GPE.

4.2 Structural Similarity Measures

While the above mentioned picture quality metrics based on error sensitivity are very convenient and widely used, they present many problems shown by its dissimilarities (in several cases) to subjective quality measurement systems based on human quality scoring system. In this situation, the hypotheses that the human visual system is well adapted for extracting structural information from the field of viewing are used to suggest a recent model for the assessment of image quality based on structural similarity. Thus distortions in an image which arise as a result of light variations (contrast or changes in brightness) should be treated differently from structural distortions. The SSIM has the easiest formulation and a wide range of practical

applications have become popular. The SSIM is included in the 21-feature parameterization due to its very attractive properties.

4.3 Information Theoretic Measures

In the context of information theory, the issue of quality assessment can also be understood as an information fidelity issue (rather than a signal reliability problem). The approach is based primarily on the idea that an image source transmits a recipient by means of a medium which reduces the amount of information it can receive and causes distortions. The objective is to compare the visual quality of the test image with the quantities of information that is shared between the test and the reference signals or the information. The image quality measures based mainly on fidelity to information benefit from the connection (sometimes imprecise) between image statistics and quality vision. In this work, two of these theoretical measures of information are taken into account namely VIF and RRED.

4.4 FR-IQA and Their Mathematical Representation

The following subsections demonstrate the mathematical representations of full reference image quality assessment techniques used in this thesis.

4.4.1 Mean Squared Error (MSE)

The MSE is perhaps the most used, simplest, and oldest measure of image quality. Mean Squared Error measures the average squared difference that exists between the estimated values and what is estimated. It is computed by [30] as follows:

$$\text{MSE} = (I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (I_{ij} - \hat{I}_{ij})^2 \quad (4.1)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.2 Peak Signal to Noise Ratio (PSNR)

The PSNR indicates the maximum difference between an original signal and its noise-affected version. PSNR is often expressed on the logarithmic decibel scale. It's given [30] as follows:

$$\text{PSNR}(I, \hat{I}) = 10 \log \left(\frac{\max(I)^2}{\text{MSE}(I, \hat{I})} \right) \quad (4.2)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image.

4.4.3 Signal to Noise Ratio (SNR)

SNR is a measure of how the signal is 'clean,' i.e. free from distorting artifacts that affect its comprehensibility. It is a ratio of S / N , where S and N are some measure of the "energy" or power of signal (S) and noise (N). So, if the noise energy is very low, S / N is very high and vice versa. It is given [30] as follows:

$$\text{SNR} = (I, \hat{I}) = 10 \log \left(\frac{\sum_{i=1}^N \sum_{j=1}^M (I_{i,j})^2}{N \cdot M \cdot \text{MSE}(I, \hat{I})} \right) \quad (4.3)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.4 Structural Content (SC)

SC is a metric that computes the sum of all squares between the authentic image and distorted image. It is given [30] as follows:

$$\text{SC} = (I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{i,j})^2}{\sum_{i=1}^N \sum_{j=1}^M (\hat{I}_{i,j})^2} \quad (4.4)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.5 Maximum Difference (MD)

MD is the maximum of the error signal (difference between the reference signal and test image). It is computed in [30] as

$$\text{MD}(I, \hat{I}) = \max |I_{i,j} - \hat{I}_{i,j}| \quad (4.5)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image.

4.4.6. Average Difference (AD)

Average difference is the average difference between the reference signal and test image. It is given in [30] as

$$AD = (I, \hat{I}) = 1/NM \sum_{i=1}^N \sum_{j=1}^M (I_{i,j} - \hat{I}_{ij}) \quad (4.6)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.7 Normalized Absolute Error (NAE)

NAE is the ratio of sums of the absolute reference image to the absolute sum of the original image. NAE can be computed by using the equation below as in [30],

$$NAE = (I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M |I_{i,j} - \hat{I}_{ij}|}{\sum_{i=1}^N \sum_{j=1}^M |I_{i,j}|} \quad (4.7)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.8 R-Averaged Maximum Difference (RAMD)

In order to calculate the average maximum difference, the maximum number value is summed up and divided by R . It is computed in [30] as

$$RAMD (I, \hat{I}, R) = \frac{1}{R} \sum_{r=1}^R \max_r |I_{i,j} - \hat{I}_{ij}| \quad (4.8)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image and R is numbers of value.

4.4.9 Laplacian Mean Squared Error (LMSE)

LMSE calculates the ratio between the square of differences between these two values and the sum of the original image value. It computed in [30] as

$$\text{LMSE}(I, \hat{I}) = \frac{\sum_{i=1}^{N-1} \sum_{j=2}^{M-1} (h(I_{i,j}) - h(\hat{I}_{i,j}))^2}{\sum_{i=1}^{N-1} \sum_{j=2}^{M-1} h(I_{i,j})^2} \quad (4.9)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns and h is a laplacian operator.

4.4.10 Normalized Cross Correlation (NXC)

Brightness of the image and template for image-processing application can differ because of exposure and lighting conditions, the images can be normalized at first. This is usually done at every step by deducting the mean and dividing by the standard deviation. It is given in [30] as

$$\text{NXC}(I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{i,j} - \hat{I}_{i,j})}{\sum_{i=1}^N \sum_{j=1}^M (I_{i,j})^2} \quad (4.10)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.11 Mean Angle Similarity (MAS)

The MAS measures how the mean angle between the original photo and the reference image are similar. It is computed in [30] as

$$\text{MAS}(I, \hat{I}) = 1 - 1/NM \sum_{i=1}^N \sum_{j=1}^M (\alpha_{i,j}) \quad (4.11)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.12 Mean Angle Magnitude Similarity (MAMS)

The MAMS computes the similarity of the mean angle between the authentic image and the distorted image. It can be computed as in [30] as follows:

$$\text{MAMS}(I, \hat{I}) = 1/NM \sum_{i=1}^N \sum_{j=1}^M \left(1 - [1 - \alpha_{i,j}] \left[1 - \frac{||I_{i,j} - \hat{I}_{i,j}||}{255} \right] \right) \quad (4.12)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.13 Total Edge Difference (TED)

The TED computes the ratio between the variations of total number of edges between the two images to the total number of pixels. It is given by [30] as follows:

$$\text{TED}(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M | |I_{E_{ij}} - \hat{I}_{E_{ij}}| | \quad (4.13)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows and M is number of columns.

4.4.14 Total Corner Difference (TCD)

TCD calculates the ratio between total number of corners in the two images and the total pixel quantity. It is computed in [30] as follows:

$$\text{TCD}(I, \hat{I}) = \frac{||N_{cr} - N_{cap_{cr}}||}{\max(N_{cr}, N_{cap_{cr}})} \quad (4.14)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns, N number of corners found in I and \check{N} number of corners found in \hat{I} .

4.4.15 Spectral Magnitude Error (SME)

The SME determines the variations between the Fourier transform of the original image to the Fourier transform of the distorted image then is averaged by the total number of pixels. It is computed by [30] as follows:

$$\text{SME}(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (|F_{ij}| - |\hat{F}_{ij}|)^2 \quad (4.15)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns, F is Fourier transform of I and \hat{F} is Fourier transform of \hat{I} .

4.4.16 Spectral Phase Error (SPE)

The SPE measures the variations between the angles of the original image transformed by Fourier and the angle of the reference image transformed by Fourier and then it is calculated by total pixel numbers. The calculation is as in [30]:

$$\text{SPE}(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M |\arg(F_{i,j}) - \arg(F_{\text{cap}_{i,j}})|^2 \quad (4.16)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns, F is Fourier transform of I and \hat{F} is Fourier transform of \hat{I} .

4.4.17 Gradient Magnitude Error (GME)

The GME computes the variations between the gradient of original image to the gradient of reference image that is averaged by total number of pixels. It is computed in [30] as

$$\text{GME}(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (|G_{i,j}| - |G_{\text{cap}_{i,j}}|)^2 \quad (4.17)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns, G is gradient map of I and \hat{G} is gradient map of \hat{I} .

4.4.18 Gradient Phase Error (GPE)

The GPE calculates the difference between the angles of gradient of the original image and the angle of gradient of the reference image by the average number of pixels. It is computed in [30] as

$$\text{GPE}(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M |\arg(G_{i,j}) - \arg(G_{\text{cap}_{i,j}})|^2 \quad (4.18)$$

where I is the reference image of size $(N \times M)$, \hat{I} is the smoothed version of the reference image, N is number of rows, M is number of columns, G is gradient map of I and \hat{G} is gradient map of \hat{I} .

4.4.19 Structural Similarity Index Measure (SSIM)

The SSIM measures the differences in perception between two similar images. SSIM can be obtained by comparing local patterns of normalized pixel intensities for luminance and contrast. It is given in [30] as

$$\text{SSIM}(I, \hat{I}) = \frac{(2 \mu_I \mu_{\hat{I}} + C_1)(2 \sigma_{I\hat{I}} + C_2)}{(\mu_I^2 + \mu_{\hat{I}}^2 + C_1)(\sigma_I^2 + \sigma_{\hat{I}}^2 + C_2)} \quad (4.19)$$

where I is the reference image of size $(N \times M)$ and \hat{I} is the smoothed version of the reference image.

4.4.20 Visual Information Fidelity (VIF)

The VIF metric is predicated on the notion that human visual imaging constitutes all natural scenes with the same statistic features, it is computed in [30] as

$$\text{VIF} = \frac{\sum_{j \in \text{subbands}} I(C \rightarrow^{N,j}, F \rightarrow^{N,j} | S^{N,j})}{\sum_{j \in \text{subbands}} \hat{I}(C \rightarrow^{N,j}, F \rightarrow^{N,j} | S^{N,j})} \quad (4.20)$$

where C random field (RF) from a subband in the reference signal, F represents a stationary additive white Gaussian noise random field (RF) and S is an random field (RF) of positive scalars.

4.4.21 Reduced Reference Entropic Difference (RRED)

The RRED calculates the average variation between scaled local entropies of reference wavelet coefficients and projected distributed distorted images, it is computed by

$$\text{RRED}_k^{M_k} = \frac{1}{L_k} \sum_{m=1}^{M_k} |\gamma_{mk}^r h(C_{mk}^r | S_{mk} = s_{mk}) - \gamma_{mk}^d h(D_{mk}^d | T_{mk} = t_{mk})| \quad (4.21)$$

where L_k is the size (number of coefficients) of the subband k , M_k is non-overlapping blocks, S_{mk} is a scalar random variable, T_{mk} is the scalar premultiplier random variable as in the reference image .

Chapter 5

PROPOSED METHOD

The proposed method is an iris anti-spoofing approach using image quality assessment. Figure 5 shows the iris anti-spoofing method system diagram using measurements of image quality.

The inputs of the proposed method are I and \hat{I} which are both gray-scale representations of the original test image and filtered test images. In order to apply FR-IQA, the input test image of iris biometric is filtered by using Gaussian kernel filtering with value of 0.5 and size 3x3. Furthermore, 21 FR IQMs are employed in order to measure the quality variations between reference image (I) and filtered image (\hat{I}). Each of the IQM of an iris biometric image is stored in a vector and using feature-level fusion, the extracted full referenced IQM's feature vectors are fused together into a single vector. Nearest Neighbor classifier is then applied in the matching part of the system to make a decision if the iris biometric image is considered as real or fake. Fig 5 shows a block diagram of the proposed method.

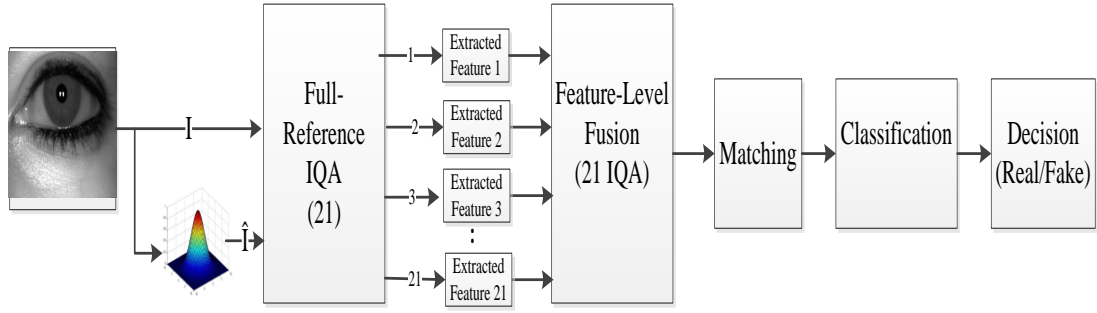


Figure 6: Block diagram of the proposed method.

5.1 Feature Extraction

The input iris gray-scale image I of size $N \times M$ is filtered with a low-pass Gaussian kernel to obtain a smoothed version \hat{I} . The quality between both reference and smoothed images (I and \hat{I}) is computed based on the 21 full reference image quality metrics. The quality loss caused by Gaussian filtering is assumed to differentiate between real and fake biometric samples. This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. Each of the extracted feature metrics is then stored in a feature vector which are then forwarded to the next stage of the proposed method.

5.2 Feature-Level Fusion (FLF)

Biometric recognition has developed immensely for safety protection and personal identity recognition because of the benefits of stability and reliability. Resource protection from an unauthorized person posed a major threat to the owner. The biometric system combines a number of biometrics to improve safety and accuracy, which is why it is capable of effectively addressing the non-universality problem of human traits. In such situations, it may not be effective due to these inherent problems to improve the performance of individual matches. A variety of these setbacks can be alleviated by multi-biometric systems, which show the same identity. These systems

help improve overall performance in order to prevent the application of a single biometric indicator. Concatenating of a couple of biometric features provide beneficial information in contrast to the one acquired using unimodal biometric attribute.

Feature-level fusion combines the feature vectors of individual vectors into one functional vector. The primary benefit of FLF is to discover related feature values that are created by totally different algorithms of biometric system and to identify some outstanding features that enhance recognition performance and consistency. Extracting feature set needs the use of dimensionality reduction techniques and, hence, FLF assumes that a large wide variety of training data is available. Fused feature sets are also expected to reside in a suitable vector space to enable an appropriate matching approach to be applied when feature sets are consolidated [20]. Twenty one full-reference image quality metrics are obtained from the previous stage. The feature vectors are concatenated into a single feature vector using feature level fusion, the single concatenated feature vector is then used in the matching stage.

5.3 Matching

Without taking into consideration the distributions from which the training samples are obtained, the Nearest Neighbor classifier continuously achieves high performance under various techniques of statistical patterns controlled. Usually, the nearest neighbor needs both legitimate and false case training. By determining the distance from the nearest case of training, a new sample is categorized; the sign at that point determines the sample classification. By taking the nearest k points and allocating the majority mark, the Nearest Neighbor classifier extends this concept. In order to break ties (typically 1, 3, or 5), the choice of the value of k is common. Larger k-values

minimize noises within the training data set and k is often selected by cross-validation [31].

Due to the validation (input test set), n dimensional n characteristic pattern vector can be calculated using the samples of training and classified to the minimum distance type. The training examples include vectors with a class label described. In the closest neighbor classification training stage, the vectors are stored and class labels are assigned to training examples. In this classification step, k is a user-defined constant, and an un-labelled vector (a query or test point) is classified by assigning the label which is often frequent among the K training samples that are near to that query point. Euclidean distance is usually used as the continuous variable distance metric.

Nearest Neighbor classifier is applied on the concatenated feature vector obtained from the feature-level fusion phase. After applying Nearest Neighbor classifier, iris image is then classified as real or fake.

5.4 Classification

Nearest Neighbor classifier is used in classifying the iris image as original or fake. An iris image is classified by the number of votes of its neighbors. Then the iris image is assigned to the most resembling one among its nearest neighbors.

Chapter 6

EXPERIMENTS AND RESULTS

Iris anti-spoofing experiments are carried out using different datasets and same experimental setup that are explained in the following sections.

6.1 Experimental Setup

In order to evaluate the performance of the proposed method “Iris Anti-Spoofing Using Image Quality Assessment”, Matlab version R2017a environment is used. Datasets from two publicly available databases are used to perform (1) print attack, (2) scan attack and (3) contact lens attack scenario. The datasets from each of the databases are divided into train and test set. At first, Gaussian filter is applied on the reference iris image in order to obtain the smoothed version of the image. Secondly, the image quality metrics features of the iris images are computed as each of the image quality metrics is obtained separately and then concatenated using feature level fusion. Thirdly, classification is carried out on the concatenated feature vector.

6.2 Databases Used for the Experiment

The details related to the iris spoofing databases used in the experiments are given below.

6.2.1 Casia Iris V1

CASIA V1.0 (CASIA-IrisV1) is a database of iris images obtained from CASIA.

The iris database consists of 756 real sample images of 108 users. Seven iris samples are acquired in two different sessions for each user. The acquisition of the iris images was carried out with an iris camera which is developed by CASIA as shown in Figure

7. The camera captures iris images in BMP format and grey-scale with 320x280 dimensions. A total of seven images are captured with three of them in first session and four in the second session. In this experiment, 101 subjects with their 5 iris images (3 from the first session and 2 from second session), which makes it a total of 505 genuine iris samples are used for the scenario of attack using synthetic samples.

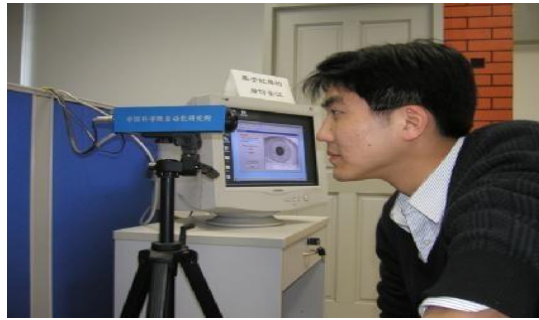


Figure 7: Iris camera used for capturing CASIA-IrisV1

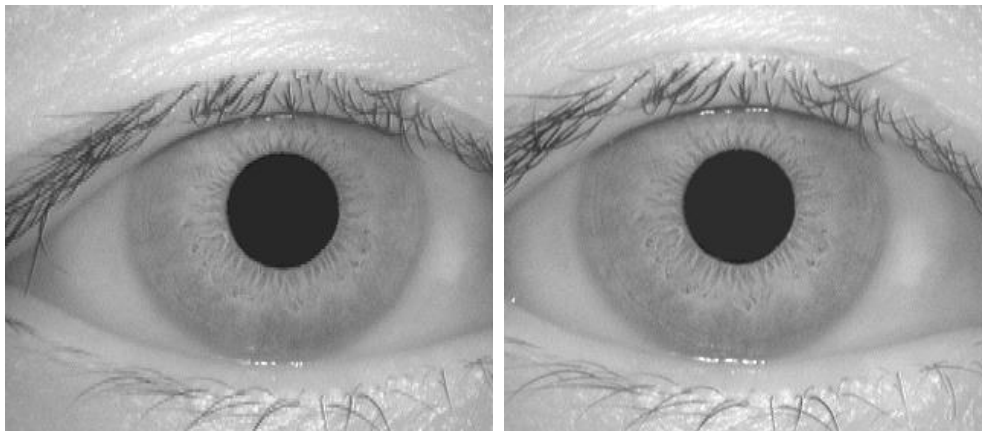


Figure 8: First session and second session typical real iris image that may be found in the database.

6.2.2 CASIA-Iris-Syn

This database is obtained from CASIA. CASIA-Iris-Syn database contains 1,000 classes of iris samples which comprises of 10,000 synthesized iris images. The iris textures of these images are automatically synthesized using Markov Random Fields using a dataset of CASIA- IrisV1 [32]. The artificial iris images become more realistic because the regions of the ring are unified into the authentic iris images [32]. In the

experiments, 101 subjects with their 5 iris images, which makes it 505 in total are used from Casia-Iris-Syn to evaluate attack with synthetic samples.

6.2.3 IIITD Combined Spoofing Database

IIITD Combined Spoofing Database (CSD) is obtained from the Indraprastha Institute of Information Technology Delhi (IIITD). The database consists of iris images obtained from several spoofing databases available to the public for the purpose of research. IIITD (CSD) consists of Contact Lens Iris (CLI) database and Iris Spoofing database (IIS) [33].

6.2.3.1 IIITD-CLI Database

IIITD CLI database comprises of a total number of 6570 images of 101 subjects. Iris images are acquired from both eyes (left and right), and as a result, 202 iris classes exist in the database. CLI database comprises of iris images without lens (with title Normal CLI), transparent lens (with title Transparent CLI), and colored textured lens (with title Color CLI) [18]. Cogent and Vista sensors are used to capture IIITD iris images.

In the experiments, for normal CLI, transparent CLI and Colored CLI, we used 101 subjects with 5 iris images (3 from left and 2 from right), which makes it 505 fake iris images that are randomly selected from IIITD-CLI. The size of the iris images is 640x480 pixels [32].

6.2.3.2 IIITD-IIS Database

For the preparation of the IIS database, 12 iris images per subject (right and left irises with different types of lenses) were selected from the CLI database and then high-resolution printouts were taken using the HP Color LaserJet 2025 printer. Print attack is carried out using optical flatbed scanning (Cogent CIS 202) and optical scanner. In

the print capture attack, the iris dataset is the printout of iris images captured by iris scanners.

A pair of authentic data sets is used for each scheme. Data sets are divided into a train set and test set for training the classifier and the performance evaluation of the proposed method. Train set of each of the dataset contains 255 real images and 255 corresponding fake images, which makes it 510 iris images in total. The test set of each of the dataset contains 250 real images and corresponding 250 fake iris images, which makes it 500 iris images in total [33]. A summary of databases used in the experiments is given in Table 2.

Table 2: Summary of Databases used in the experiment

Dataset	Number of train images	Number of test images
CASIA Iris V1	255 real images 255 fake images	250 real images 250 fake images
IIITD-CLI Database	255 real images 255 fake images	250 real images 250 fake images
IIITD-IIS Database	255 real images 255 fake images	250 real images 250 fake images

6.3 Experimental Results

In the experiments, the results are shown in tables below in terms of False Fake Rate, which states the rate of real irises that are termed as fake and False Genuine Rate, which states the rate of fake irises that are been categorized as authentic. HTER is also obtained by $(FFR+FGR)/2$. Based on the results, obtained decisions cannot be made based on each IQM, because the result of one IQM may not give the best result for every database. Due to this reason Feature-Level Fusion (FLF) and Decision-Level Fusion (DLF) methods are used in order to make a decision according to the extracted full reference IQMs. In Decision-Level Fusion method, after matching using the

Nearest Neighbor Classifier, decisions of either real or fake are made according to each IQM. Majority Voting is performed to make the final decision.

In Feature-Level Fusion method, 21 full reference feature vectors' IQMs are merged into a single feature vector and then decision is made based on the single feature vector.

Table 3 shows the experimental results of Iris Biometric attack with Synthetic samples on CASIA V1 dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 3: Attack with synthetic samples using Casia Iris V1 & Iris -Syn

#	IQM	CASIA Iris V1 & CASIA Iris-Syn		
		FFR	FGR	HTER
1	MSE	0.0	0.0	0.0
2	PSNR	0.0	0.4	0.2
3	SNR	0.0	0.8	0.4
4	SC	0.0	0.2	0.1
5	MD	0.0	3.0	1.5
6	AD	0.0	0.0	0.0
7	NAE	0.0	0.6	0.3
8	LMSE	0.0	0.0	0.0
9	NXC	0.0	12.8	6.4
10	TCD	0.0	0.4	0.2
11	TED	0.4	2.2	1.3
12	SME	0.0	0.0	0.0
13	SPE	3.6	6.2	4.9
14	GME	5.4	1.2	3.3
15	GPE	1.2	2.4	1.8
16	SSIM	0.0	1.8	0.9
17	VIF	0.0	0.4	0.2
18	RRED	0.0	0.0	0.0
19	MAS	0.0	0.0	0.0
20	MAMS	0.0	0.0	0.0
21	RAMD	0.0	1.6	0.8
	DLF	0.0	0.4	0.2
	FLF	0.0	0.0	0.0

The result shown in Table 3 shows that, feature-level fusion method achieves better performance result compared to the decision-level fusion method of 21 full referenced IQMs. The decision-level fusion method obtained an HTER of 0.2% on CASIA iris dataset. However, feature-level fusion method demonstrates a HTER of 0.0% on CASIA iris dataset. This shows that feature-level fusion method outshines decision level fusion on CASIA iris dataset based on Iris synthetic attack scenario.

Table 4 shows the experimental results of Iris Biometric attack with print attack on Indraprastha Institute of Information Technology Delhi (IIITD) IIS Cogent dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 4: Print attack using Cogent dataset

		IIITD IIS COGENT dataset (Print Attack)		
#	IQM	FFR	FGR	HTER
1	MSE	25.2	12.4	18.8
2	PSNR	25.2	12.6	18.9
3	SNR	10.6	23.0	16.8
4	SC	17.8	24.4	21.1
5	MD	5.8	20.4	13.1
6	AD	13.0	24.0	18.5
7	NAE	8.2	12.8	10.5
8	LMSE	16.4	11.6	14.0
9	NXC	1.4	3.2	2.3
10	TCD	13.0	25.8	19.4
11	TED	0.2	2.4	1.3
12	SME	13.6	12.6	13.1
13	SPE	6.0	22.6	14.3
14	GME	0.6	1.2	0.9
15	GPE	0.6	2.8	1.7
16	SSIM	6.4	11.6	9.0
17	VIF	0.2	1.2	0.7
18	RRED	2.6	18.2	10.4
19	MAS	31.2	24.8	28.0
20	MAMS	14.2	18.6	16.4
21	RAMD	2.6	28.6	15.6
	DLF	0.6	2.2	1.4
	FLF	0.2	1.2	0.7

The results achieved by FLF and DLF on Cogent dataset based on Print attack scenario are shown in Table 4 above. Feature-Level Fusion method have the lowest HTER with 0.7% compared to Decision-Level Fusion method which has HTER of 1.4%. This shows that feature-level fusion method performs better than decision-level fusion method in print attack scenario on cogent dataset.

Table 5 shows the experimental results of Iris Biometric attack with scan attack on Indraprastha Institute of Information Technology Delhi (IIITD) IIS Cogent dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 5: Scan attack using cogent dataset

#	IQM	IIITD-IIS Cogent dataset (Scan Attack)		
		FFR	FGR	HTER
1	MSE	5.4	11.0	8.2
2	PSNR	5.4	11.0	8.2
3	SNR	17.2	1.6	9.4
4	SC	9.0	1.0	5.0
5	MD	0.2	0.0	0.1
6	AD	27.0	20.6	23.8
7	NAE	21.8	6.2	14.0
8	LMSE	8.2	11.0	9.6
9	NXC	0.8	1.2	1.0
10	TCD	9.0	1.2	5.1
11	TED	1.0	1.4	1.2
12	SME	18.6	29.8	24.2
13	SPE	9.0	30.8	19.9
14	GME	0.4	6.8	3.6
15	GPE	7.6	24.4	16.0
16	SSIM	3.8	15.8	9.8
17	VIF	7.6	21.8	14.7
18	RRED	14.2	9.6	11.9
19	MAS	0.0	0.0	0.0
20	MAMS	4.2	12.8	8.5
21	RAMD	14.2	10.6	12.4
	DLF	1.0	0.6	0.8
	FLF	0.0	0.0	0.0

Results obtained in Table 5 show that feature-level fusion method performs better than decision-level fusion method on IIITD IIS Cogent dataset in order to evaluate scan attack scenario. Feature-level fusion method obtained a HTER of 0.0% while decision-level fusion method obtained 0.8% HTER.

Table 6 shows the experimental results of Iris Biometric attack with Colored Contact lens attack on Indraprastha Institute of Information Technology Delhi (IIITD) Contact Lens Iris (CLI) Cogent dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 6: Colored Contact lens attack using CLI cogent dataset

#	IQM	IIITD-CLI Cogent dataset		
		FFR	FGR	HTER
1	MSE	16.4	21.4	18.9
2	PSNR	16.2	26.2	21.2
3	SNR	30.2	19.0	24.6
4	SC	24.4	19.0	21.7
5	MD	10.0	39.2	24.6
6	AD	26.2	30.4	28.3
7	NAE	26.4	23.8	25.1
8	LMSE	24.6	25.6	25.1
9	NXC	25.2	22.0	23.6
10	TCD	24.2	20.6	22.4
11	TED	31.4	18.2	24.8
12	SME	21.0	28.2	24.6
13	SPE	25.4	21.0	23.2
14	GME	7.0	42.8	24.9
15	GPE	21.2	23.4	22.3
16	SSIM	23.4	20.6	22.0
17	VIF	23.6	23.2	23.4
18	RRED	23.6	23.0	23.3
19	MAS	17.6	21.8	19.7
20	MAMS	29.8	25.6	27.7
21	RAMD	21.2	18.6	19.9
	DLF	17.8	23.8	20.8
	FLF	19.4	25.6	22.5

The results shown in Table 6 above show that decision-level fusion method performs better with minimum HTER of 20.8% compared to feature-level fusion method which has HTER of 22.5% on IIITD CLI cogent dataset based on colored contact lens attack scenario.

Table 7 shows the experimental results of Iris Biometric attack with Transparent Contact lens attack on Indraprastha Institute of Information Technology Delhi (IIITD) Contact Lens Iris (CLI) Cogent dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 7: Transparent Contact Lens attack using CLI cogent dataset

		IIITD-CLI COGENT dataset		
#	IQM	FFR	FGR	HTER
1	MSE	28.4	29.4	28.9
2	PSNR	27.6	29.2	28.4
3	SNR	30.2	28.2	29.2
4	SC	24.4	24.8	24.6
5	MD	11.2	14.4	12.8
6	AD	25.6	26.4	26.0
7	NAE	27.0	18.8	22.9
8	LMSE	21.6	25.2	23.4
9	NXC	26.4	27.8	27.1
10	TCD	29.2	31.0	30.1
11	TED	26.2	26.0	26.1
12	SME	18.8	13.0	15.9
13	SPE	20.4	16.4	18.4
14	GME	1.4	1.2	1.3
15	GPE	25.8	25.4	25.6
16	SSIM	23.2	26.4	24.8
17	VIF	25.4	23.0	24.2
18	RRED	36.0	31.6	33.8
19	MAS	27.4	22.0	24.7
20	MAMS	28.2	28.0	28.1
21	RAMD	26.0	25.2	25.6
	DLF	21.4	29.0	25.2
	FLF	28.0	28.8	28.4

The result shown in Table 7 above shows that decision-level fusion method performs better with minimum HTER of 25.2% compared to feature-level fusion method which has HTER of 28.4% on IIITD CLI cogent dataset based on transparent contact lens attack.

Table 8 shows the experimental results of Iris Biometric attack with print attack on Indraprastha Institute of Information Technology Delhi (IIITD) IIS Vista dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 8: Print Attack using Vista IIS dataset

#	IQM	IIITD-IIS VISTA dataset		
		FFR	FGR	HTER
1	MSE	2.4	1.2	1.8
2	PSNR	2.6	1.0	1.8
3	SNR	13.8	10.0	11.9
4	SC	21.0	17.6	19.3
5	MD	0.2	0.0	0.1
6	AD	0.8	0.6	0.7
7	NAE	8.8	12.0	10.4
8	LMSE	0.4	0.4	0.4
9	NXC	1.0	3.6	2.3
10	TCD	20.8	14.8	17.8
11	TED	0.4	0.6	0.5
12	SME	17.2	11.6	14.4
13	SPE	1.0	0.2	0.6
14	GME	1.0	5.2	3.1
15	GPE	0.8	4.2	2.5
16	SSIM	15.0	3.8	9.4
17	VIF	15.8	3.8	9.8
18	RRED	4.4	2.6	3.5
19	MAS	1.4	5.0	3.2
20	MAMS	0.4	0.2	0.3
21	RAMD	3.6	9.2	6.4
	DLF	0.6	0.4	0.5
	FLF	0.2	0.0	0.1

The results achieved by FLF and DLF on IIITD-IIS Vista dataset based on print attack scenario are shown in Table 8 above. FLF has the minimum HTER of 0.1% compared to decision-level fusion method which has HTER of 0.5%. This shows that feature-level fusion method performs better than decision-level fusion method in print attack scenario on IIITD-IIS Vista dataset.

Table 9 shows the experimental results of Iris Biometric attack with scan attack on Indraprastha Institute of Information Technology Delhi (IIITD) IIS Vista dataset. Also,

False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 9: Scan Attack using IIS vista dataset

#	IQM	IIITD-IIS VISTA dataset		
		FFR	FGR	HTER
1	MSE	0.2	0.8	0.5
2	PSNR	0.2	0.4	0.3
3	SNR	0.6	4.0	2.3
4	SC	1.8	4.8	3.3
5	MD	6.2	16	11.1
6	AD	3.0	2.4	2.7
7	NAE	0.6	2.0	1.3
8	LMSE	1.4	1.0	1.2
9	NXC	3.0	3.2	3.1
10	TCD	1.6	5.2	3.4
11	TED	0.2	0.0	0.1
12	SME	11.2	16.8	14
13	SPE	3.4	2.0	2.7
14	GME	0.2	2.4	1.3
15	GPE	8.2	5.8	7.0
16	SSIM	0.2	1.4	0.8
17	VIF	3.0	7.2	5.1
18	RRED	0.2	0.8	0.5
19	MAS	0.4	1.0	0.7
20	MAMS	0.2	0.8	0.5
21	RAMD	1.2	1.8	1.5
	DLF	0.2	0.4	0.3
	FLF	0.2	0.0	0.1

Results obtained in Table 9 show that feature-level fusion method performs better than decision-level fusion method on IIITD-IIS Vista dataset in order to evaluate scan attack scenario. Feature-level fusion method obtained a HTER of 0.1% while decision-level fusion method obtained HTER of 0.3%.

Table 10 shows the experimental results of Iris Biometric attack with Colored Contact lens attack on Indraprastha Institute of Information Technology Delhi Contact Lens Iris Vista dataset. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

Table 10: Colored contact lens attack using CLI vista dataset

		IIITD-CLI VISTA dataset		
#	IQM	FFR	FGR	HTER
1	MSE	23.4	23.8	23.6
2	PSNR	23.2	24.0	23.6
3	SNR	20.2	25.0	22.6
4	SC	27.6	21.2	24.4
5	MD	8.6	40.0	24.3
6	AD	24.2	22.0	23.1
7	NAE	18.2	28.6	23.4
8	LMSE	24.0	21.4	22.7
9	NXC	27.6	21.8	24.7
10	TCD	28.2	20.8	24.5
11	TED	23.4	17.2	20.3
12	SME	21.8	27.8	24.8
13	SPE	22.4	22.4	22.4
14	GME	4.2	45.0	24.6
15	GPE	27.8	22.2	25.0
16	SSIM	25.4	22.4	23.9
17	VIF	27.6	19.8	23.7
18	RRED	22.8	16.8	19.8
19	MAS	22.8	16.2	19.5
20	MAMS	27.2	25.0	26.1
21	RAMD	25.6	23.4	24.5
	DLF	22.4	16.2	19.3
	FLF	17.2	22.8	20.0

The result shown in Table 10 above shows that decision-level fusion method performs better with HTER of 19.3% compared to feature-level fusion method which has HTER of 20.0% on IIITD-CLI VISTA dataset based on colored contact lens attack.

Table 11 shows the experimental results of Iris Biometric attack with Transparent Contact lens attack on Indraprastha Institute of Information Technology Delhi Contact Lens Iris Vista. Also, False Fake Rate, False Genuine Rate and Half Total Error Rate are all computed for each IQM.

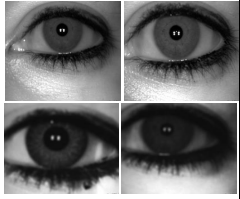
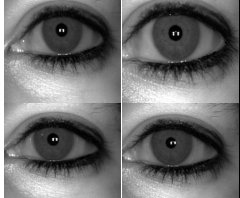

Table 11: Transparent Contact Lens attack using CLI Vista Dataset

#	IQM	IIITD-CLI VISTA dataset		
		FFR	FGR	HTER
1	MSE	25.2	20.8	23.0
2	PSNR	26.6	21.2	23.9
3	SNR	21.8	26.8	24.3
4	SC	25.4	25.0	25.2
5	MD	10.4	40.0	25.2
6	AD	24.2	20.4	22.3
7	NAE	17.8	31.4	24.6
8	LMSE	25.6	19.0	22.3
9	NXC	24.2	28.6	26.4
10	TCD	27.2	25.0	26.1
11	TED	24.2	22.6	23.4
12	SME	20.8	29.0	24.9
13	SPE	23.0	24.6	23.8
14	GME	9.8	39.0	24.4
15	GPE	24.8	28.2	26.5
16	SSIM	27.6	23.8	25.7
17	VIF	27.0	20.6	23.8
18	RRED	22.0	25.8	23.9
19	MAS	24.8	26.2	25.5
20	MAMS	25.2	25.4	25.3
21	RAMD	21.8	28.2	25.0
	DLF	21.6	25.2	23.4
	FLF	20.0	28.6	24.3

The result shown in Table 11 above shows that decision level fusion method performs better with minimum HTER of 23.4% compared to feature-level fusion method which has HTER of 24.3% on IIITD-CLI Vista dataset based on transparent contact lens attack.

A summary of experimental results for three types of spoofing attacks are shown in Table 12. The results are demonstrated in terms of False Fake Rate, False Genuine Rate and Half Total Error Rate for both Decision-level fusion and Feature-level fusion approaches.

Table 12: Summary of iris spoofing attacks and results

Types of attacks	Real and Fake Iris Images	Experimental Result					
		DLF			FLF		
		FFR	FGR	HTER	FFR	FGR	HTER
Print Attacks		0.6	2.2	1.4	0.2	1.2	0.7
Contact lens		17.8	23.8	20.8	19.4	25.6	22.5
Artificial Eye		0.0	0.4	0.2	0.0	0.0	0.0

In conclusion, feature-level fusion performs better in print and scan attack scenarios, while decision level fusion performs better in Contact lens attack scenarios.

Chapter 7

CONCLUSION

In today`s technological era, efficient, fast, robust and invulnerable biometric systems are needed in order to secure personal information or physical property. Most commonly, intruders in traditional access control systems have taken the advantage of a fundamental vulnerability. Biometric authentication systems have been able to overcome the majority of traditional security systems` weaknesses/vulnerabilities and have become increasingly significant in recent years. The task of securing vital and sensitive data or information is becoming difficult and has gained popularity in biometric research field. Iris spoof detection is a vital issue in biometric research field for the recognition of iris because it reduces the chance of forging an iris recognition system.

In this thesis, full reference Image Quality Assessment techniques are used in order to detect genuine and imposter iris images presented to an iris biometric system since real and impostor iris image quality characteristics are different. Image Quality Assessment (IQA) is used as an iris anti-spoofing technique against different biometric attacks (e.g. spoofing and attack with synthetic samples). Methods based on feature-level fusion and decision-level fusion are used in this context on full reference Image Quality Measures (IQM`s) extracted from an iris image. On the basis of two iris databases, the proposed method has been evaluated. Feature-level fusion performs better on synthetic

attack, print attack and scan attack scenario while decision-level fusion works better on contact lens attack scenario.

As a future work, an improved iris anti-spoofing technique will be studied using no-reference image quality measures. The combination of different types of quality measures will be searched for iris anti-spoofing. Additionally, texture based or deep learning techniques can be involved further to build an enhanced iris anti-spoofing system.

REFERENCES

- [1] Bodade, R. M., & Talbar, S. N. (2014). *Iris analysis for biometric recognition systems*. Springer.

- [2] Tiwari, S., & Singh, S. K. (2013). Information Security Governance Using Biometrics. In *IT Security Governance Innovations: Theory and Research* (pp. 191-224). IGI Global.

- [3] Mellado, D. (Ed.). (2012). *IT Security Governance Innovations: Theory and Research: Theory and Research*. IGI Global.

- [4] Sui, Y., Zou, X., & Du, E. Y. (2011, July). Biometrics-based authentication: A new approach. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on* (pp. 1-6). IEEE.

- [5] Patil, S., & Sheelvant, S. (2015). Survey on image quality assessment techniques. *Int. J. Sci. Res*, 4(7), 1756-1759.

- [6] Galbally, J., & Gomez-Barrero, M. (2016, March). A review of iris anti-spoofing. In *Biometrics and Forensics (IWBF), 2016 4th International Workshop on* (pp. 1-6). IEEE.

- [7] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4), 600-612.
- [8] Wang, Z., Simoncelli, E. P., & Bovik, A. C. (2003, November). Multiscale structural similarity for image quality assessment. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003* (Vol. 2, pp. 1398-1402). IEEE.
- [9] Liao, B., & Chen, Y. (2007, September). An image quality assessment algorithm based on dual-scale edge structure similarity. In *Innovative Computing, Information and Control, 2007. ICICIC'07. Second International Conference on* (pp. 56-56). IEEE.
- [10] Chang, H. W., Yang, H., Gan, Y., & Wang, M. H. (2013). Sparse feature fidelity for perceptual image quality assessment. *IEEE Trans. Image Processing*, 22(10), 4007-4018.
- [11] Shnayderman, A., Gusev, A., & Eskicioglu, A. M. (2003, December). Multidimensional image quality measure using singular value decomposition. In *Image Quality and System Performance* (Vol. 5294, pp. 82-93). International Society for Optics and Photonics.

- [12] Shnayderman, A., Gusev, A., & Eskicioglu, A. M. (2006). An SVD-based grayscale image quality measure for local and global assessment. *IEEE transactions on Image Processing*, 15(2), 422-429.
- [13] Narwaria, M., & Lin, W. (2012). SVD-based quality metric for image and video using machine learning. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 42(2), 347-364.
- [14] Wang, Y., Liu, W., & Wang, Y. (2008, May). Color image quality assessment based on quaternion singular value decomposition. In *Image and Signal Processing, 2008. CISP'08. Congress on* (Vol. 3, pp. 433-439). IEEE.
- [15] Narwaria, M., Lin, W., McLoughlin, I. V., Emmanuel, S., & Chia, L. T. (2012). Fourier transform-based scalable image quality measure. *IEEE Transactions on Image Processing*, 21(8), 3364-3377.
- [16] Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on face and palmprint biometrics. *Signal, Image and Video Processing*, 11(7), 1253-1260.
- [17] Pravallika, P., & Prasad, K. S. (2016, August). SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print. In *Inventive Computation Technologies (ICICT), International Conference on* (Vol. 1, pp. 1-6). IEEE.

- [18] Galbally, J., & Marcel, S. (2014). Face anti-spoofing based on general image quality assessment. In *Pattern Recognition (ICPR), 2014 22nd International Conference on* (pp. 1173-1178). IEEE.
- [19] Wei, Z., Qiu, X., Sun, Z., & Tan, T. (2008). Counterfeit iris detection based on texture analysis. In *ICPR* (No. s 1, pp. 1340-1343).
- [20] Wang, B., Wang, Z., Liao, Y., & Lin, X. (2008). HVS-based structural similarity for image quality assessment. In *Signal Processing, 2008. ICSP 2008. 9th International Conference on* (pp. 1194-1197). IEEE.
- [21] Toprak, I., & Toygar O. (2018). Fusion of Full- Reference and No-Reference Anti-Spoofing Techniques for Ear Biometrics under Print Attacks. *International conference on advanced technologies*. pp1-5
- [22] Ruiz-Albacete, V., Tome-Gonzalez, P., Alonso-Fernandez, F., Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2008). Direct attacks using fake images in iris verification. In *European Workshop on Biometrics and Identity Management* (pp. 181-190). Springer, Berlin, Heidelberg.
- [23] Schuckers, S. A. (2002). Spoofing and anti-spoofing measures. *Information Security technical report*, 7(4), 56-62.
- [24] Raghavendra, R., & Busch, C. (2014). Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of light field

- camera. In *Biometrics (IJCB), 2014 IEEE International Joint Conference on* (pp. 1-8). IEEE.
- [25] Ruiz-Albacete, V., Tome-Gonzalez, P., Alonso-Fernandez, F., Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2008). Direct attacks using fake images in iris verification. In *European Workshop on Biometrics and Identity Management* (pp. 181-190). Springer, Berlin, Heidelberg.
- [26] Zhang, H., Sun, Z., Tan, T., & Wang, J. (2011). Learning hierarchical visual codebook for iris liveness detection. In *International Joint Conference on Biometrics* (Vol. 1).
- [27] Chen, R., Lin, X., & Ding, T. (2012). Liveness detection for iris recognition using multispectral images. *Pattern Recognition Letters*, 33(12), 1513-1519.
- [28] Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE transactions on pattern analysis and machine intelligence*, 15(11), 1148-1161.
- [29] Pacut, A., & Czajka, A. (2006). Aliveness detection for iris biometrics. In *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*(pp. 122-129). IEEE.

- [30] Galbally, J., Marcel, S., & Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE transactions on image processing*, 23(2), 710-724.
- [31] Bhaskar, P. V., & Rao, S. R. Emotional Telugu Speech Signals Classification Based On K-NN Classifier.
- [32] Makthal, S., & Ross, A. (2005, September). Synthesis of iris images using Markov random fields. In *Signal Processing Conference, 2005 13th European* (pp. 1-4). IEEE.
- [33] Gupta, P., Behera, S., Vatsa, M., & Singh, R. (2014, August). On iris spoofing using print attack. In *Pattern recognition (ICPR), 2014 22nd international conference on* (pp. 1681-1686). IEEE.