Computer Science Department
Faculty of Computer & Information Sciences
Ain Shams University

Iris liveness Detection Using Intelligent Techniques

Thesis submitted as a partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Sciences.

By

Manar Ramzy Mohamed Dronky

Faculty of Computer and Information Sciences,
Ain Shams University.

Under Supervision of

Prof. Dr. Mohamed I. Roushdy
Professor of Computer Science
Dean of Faculty of Computers & Information Technology,
Future University in Egypt.
Former Dean of Faculty of Computer & Information Sciences,
Ain Shams University.

Dr. Wael Khalifa
Faculty of Computer and Information Sciences,
Ain Shams University.

Acknowledgment

First of all, I would like thank Allah for giving me the strength and knowledge to finish this thesis.

I would like to thank my supervisors Prof. Dr. Mohamed Roushdy and Dr. Wael Khalifa for their support and guidance. I thank them especially for their fast response and helping me to explore new research ideas.

I would like to thank my family, especially my mother. I could not have reached this stage without her faith in me and her continuous support. I also want to thank my friend, Naglaa Fathy, for her unconditional help and advice through this journey.

Most significantly, I wish to thank from the bottom of my heart my husband, Eslam, for all his encouragements, support and helping me in every way possible.

Finally, I would like to thank Dr. Ana F. Sequeira, University of Porto for providing the data used with Clarkson and Mobiofake databases. I would like to acknowledge Clarkson University, USA, University of Porto, Portugal and Chinese Academy of Sciences, China for providing Clarkson, Mobiofake, CASIA-Iris-Syn and CASIA_iris_Fake iris spoofing databases used in this work.

Manar

Abstract

Iris recognition systems have been widely deployed for authentication in many sensitive security areas for its accuracy and consistency. However, as the iris technology evolves, ways to attack it evolve too. Fake iris samples could be used to spoof the iris recognition system. As a result, Iris liveness detection methods have been developed. These methods read the users physiological signs of life to verify if the iris pattern acquired for identification is fake or real.

In this thesis, an extensive review for the previous work done in iris liveness detection is presented. The review has explored in detail the software-based and the hardware-based methods developed for iris liveness detection along with the different attacks detected and databases utilized for performance evaluation.

This thesis also explores the results of BSIF (Binarized statistical image features) descriptor for solving the problem of iris liveness detection to combat presentation attacks. A comprehensive study for the impact of segmentation on iris liveness detection has been carried out. Four public datasets representing printed, plastic, synthetic and contact lens attacks were used for method evaluation in both scenarios segmented and unsegmented eye images. The results have showed that BSIF can efficiently detect plastic and synthetic attacks without segmentation with correct classification rate of 100%. In addition, unsegmented eye images achieved better results in detecting print attack on the tested datasets. Segmentation is still required in the most challenging contact lens attacks.

A new method is proposed using residual images with BSIF to enhance the results of contact lens databases. Three high pass filters were applied separately before feature extraction with BSIF. The results were promising in the unsegmented scenario and the three filters enhanced in the results with 8.6667%, 10% and 18.3333%.

The main contribution is enhancing the accuracy of BSIF on Clarkson dataset from 91.67% to 93.33% in segmented mode using the first filter, in addition to proving that using the whole eye image is better in case of visible-light mobile iris datasets.

This thesis is a comprehensive study that try to evaluate the segmentation step value in iris liveness detection using BSIF descriptor.

List of Publications

A part of the work presented in this thesis has been published in the following publications:

1. Manar R. Dronky, Wael H. Khalifa, Mohamed I. Roushdy, “A Review on Iris Liveness Detection Techniques”; In proceeding of: The Ninth International Conference on Intelligent Computing and Information Systems (ICICIS 2019), Cairo, Egypt, pp 47-58, 2019.
2. Manar R. Dronky, Wael H. Khalifa, Mohamed I. Roushdy, “Impact of segmentation on iris liveness detection”; In proceeding of: The 14th IEEE International Conference on Computer Engineering and Systems (ICCES 2019), Cairo, Egypt, 2019.

Table of Contents

Chapter 1. Introduction 2
1.1 Introduction 2
1.2 Overview 2
1.3 Motivation 4
1.4 Objective 4
1.5 Contribution 4
1.6 Thesis Organization 5
Chapter 2. Biometrics 7
2.1 Biometric Traits 7
2.2 Biometric Systems 7
2.3 Spoofing Attacks 8
2.4 Liveness Detection in biometrics 9
2.5 Accuracy Measurements 10
Chapter 3. Iris Liveness Detection 13
3.1 Introduction 13
3.2 Eye Anatomy 13
3.3 Iris recognition 14
3.4 Attacks 14
3.5 Basic steps 15
3.6 Requirements 16
3.7 Databases 16
3.8 Methods 17
Chapter 4. Literature Review 19
4.1 Hardware based methods 19
4.2 Software based methods 25
Chapter 5. The Proposed Liveness Detection Method 35
5.1 Introduction 35
5.2 Methodology 36
5.3 Enhancing Accuracy Using Residual Filters 43
Chapter 6. Experimental Results 46
6.1 Databases 46
6.2 Evaluation metrics 48
6.3 Results 48
6.4 Comparative Study 56
6.5 Enhancing Accuracy Using Residual Filters 58
Chapter 7. Conclusion & Future Work 63
Appendix A: Code Snippets 66
References 76

List of Figures

Figure 2-1 Examples of biometric traits [8] 7
Figure 2-2 Architecture of Biometric System [9] 8
Figure 2-3 Possible points of attack [10] 9
Figure 2-4 Importance of liveness detection in biometrics [12] 10
Figure 2-5 Illustration of FAR and FRR curves [9] 11
Figure 3-1 Anatomy of the Eye [13] 14
Figure 3-2 A close photo of the Eye [16] 14
Figure 3-3 General diagram for iris recognition steps [17] 14
Figure 3-4 Spoofing attacks on iris-based biometric systems 15
Figure 3-5 Basic steps of iris liveness detection system [23]. 16
Figure 5-1 The objective of the proposed method 36
Figure 5-2 Overview of the implemented method 37
Figure 5-3 BSIF codes with their histograms at filter scales 7x7 and 17 x 17. 37
Figure 5-4 Example of an original image, mask and segmented image [108] 38
Figure 5-5 The eye image is normalized into a scale-invariant [108] 38
Figure 5-6 Results of different BSIF filters for a given image 40
Figure 6-1 Samples from databases used in the experiments. 47
Figure 6-2 Samples from CASIA-Iris-Fake Database 48
Figure 6-3 Accuracy results for the four tested datasets 55
Figure 6-4 Accuracy results for CASIA_iris_Fake Separated Database 55
Figure 6-5 Accuracy results for textured contactlens DB tested using BSIF 55
Figure 6-6 Accuracy results for Clarkson DB for BSIF with the three filters 60
Figure 6-7 Accuracy results for Clarkson DB in unsegmented mode 60

List of Tables

Table 4-1 Summary Of Hardware-Based Methods For Iris Liveness Detection. 23
Table 4-2 Summery Of Software-Based Methods For Iris Liveness Detection..... 30
Table 6-1 Databases used for evaluation in segmented and unsegmented scenarios.46
Table 6-2 Accuracy of CASIA-iris-Synth& CASIA-V1 database..... 49
Table 6-3 Accuracy of Clarkson 2013 database..... 50
Table 6-4 Accuracy of MobioFake database..... 51
Table 6-5 Accuracy of CASIA-Iris-Fake database separated attacks 53
Table 6-6 Summary of top results for DB in segmented and unsegmented modes .. 54
Table 6-7 Summery of the successful mode with each attack 56
Table 6-8 Performance comparison on CASIA-Iris-Syn 57
Table 6-9 Performance comparison on Clarkson 57
Table 6-10 Performance comparison on Mobiofake 57
Table 6-11 Performance comparison on CASIA-Iris-Fake..... 57
Table 6-12 Accuracy of Clarkson 2013 DB using the first residual filter. 58
Table 6-13 Accuracy of Clarkson 2013 DB using the second residual filter..... 59
Table 6-14 Accuracy of Clarkson 2013 DB using Sobel filter 60
Table 6-15 Performance comparison on Clarkson2013 DB after enhancement 61
Table 6-16 Comparison of our proposed method before and after enhancement 61

List of Abbreviations

Acronym	Definition
3D	Three dimensional
2D	Two dimensional
AI	Artificial Intelligence
APCER	Attack Presentation Classification Error Rate
BSIF	Binarized Statistical Image Features
CASIA	Chinese Academy of Sciences Institute of Automation
CCR	Correct Classification Rate
DB	Database
DNA	Deoxyribonucleic acid
ECG	Electrocardiogram
EEG	Electroencephalogram
EER	Equal Error Rate
F	Fake sample
FAR	False Acceptance Rate
FFR	False Fake Rate
FLRR	False Live Rejection Rate
FRR	False Rejection Rate
FSAR	False Spoof Acceptance Rate
GLCM	Gray Level Co-occurrence Matrices
HD	Hamming Distance
IR	Infra-Red
ICA	Independent Component Analysis
L	Live sample
LED	Light-Emitting Diode
LPQ	Local Phase Quantization
LBP	Local Binary Pattern

Acronym	Definition
LDP	Local Derivative Pattern
MATLAB	Matrix Laboratory
ND	Notre Dame
NDCLD	Notre Dame Contact Lens Database
NFOV	Narrow field of view
NIR	Near Infra-Red
PCA	Principal Component Analysis
SIFT	Scale Invariant Feature Transform
SVM	Support Vector Machine
WFOV	Wide field of view

Chapter 1

Introduction

Chapter 1. Introduction

1.1 Introduction

Automatic user identification has become a fundamental requirement nowadays. The user identity must be verified before accessing sensitive areas or secure information. Many methods have been developed based on the assumption that the user has a physical object such as magnetic cards, passports, or keys. Other Methods make use of knowledge the user has such as: passwords or PINs. These methods provide a reasonable level of security. However, they have a lot of disadvantages that make them inapplicable in sensitive areas. Cards could be lost, forgotten, or stolen. Passwords could be forgotten or guessed by an unauthentic user. In fact, all these approaches mostly failed against an obvious problem: any piece of material or knowledge could be fraudulently acquired. Biometrics represents a more natural way of identification. Thus, they have been applied to recognition systems to provide a reliable method for authentication.

The recognition in these systems is done by inspecting a specific feature that the person has rather than information he knows. Biometric identification is relying on unique physiological characteristics (e.g., face, iris, fingerprints, DNA) or behavioral characteristics (e.g., gait, keystroke dynamics, signature). Biometrics is a relatively new technology that have been utilized in many applications such as: border control, criminal investigation, and access to cellphones. Iris is one of the most reliable physiological characteristics that have been used for identification in many areas.

1.2 Overview

In recent years, the continuous studies made in biometric systems enabled them to be used in many security applications. The recognition in these systems is done by inspecting a specific feature that the person has rather than information he knows. These systems have become more reliable than traditional password-based systems where the password can be stolen or forgotten.

On the other hand, biometric systems are prone to spoofing attacks that reduce their level of security. For example, fingerprint-based systems could be spoofed by replicating the biometric pattern on silicone, gelatin, Play-Doh or clay [1] , [2]. Iris-based systems may also be fooled with fake irises like plastic contact lenses or printed iris images [3].

Recently, it has been showed that biometrics spoofing could negatively impact normal people lives after the iris scanner of the smart phone Samsung S8 was spoofed in 2017 with a photo [4] and also in 2018 when the police in U.S.A used the fingerprints of dead suspects to open their iPhones [5].

For more reliable anti-spoofing systems, new researches have been focused on liveness detection techniques that use various physiological signs of life, like eye blinking or changes of facial expressions, to distinguish between real and fake patterns. The main purpose of liveness detection is to assure that the sample presented to sensor is from a live authentic user. Many methods were used for liveness detection such as: ECG, blood pressure or pulse. The feature used to detect the liveness could be the same feature used for biometric recognition or could be a different one. For example, an iris recognition system performing liveness detection may use ECG or the same iris sample acquired from the sensor. Although liveness detection brings a lot of advantages to the system, it also brings further considerations as an additional layer of complexity is added risking the performance of the whole recognition system.

Among the popular biometrics used in various security systems; namely, fingerprint, face, and iris, the latter is considered one of the most accurate. The human iris is a ring-shaped internal organ with rich unique texture and in a relatively well-protected area. No two persons share the exact iris pattern, and even for the exact person, the left and right patterns are different. Iris recognition systems have been widely applied in a lot of airports and sensitive government areas with a high recognition rate up to 99.9% [6]. Hence, researchers pay special attention to iris liveness detection. Many techniques have been developed to detect the liveness of iris patterns. These methods rely on analysis of the iris texture based on image processing algorithms or using a specific hardware that highlighted the unique properties in the human eye.

1.3 Motivation

Currently, iris recognition systems can be found worldwide with outstanding rates of success. While recognition techniques evolve, new methods of spoofing them arise as well, creating an unquestionable need for safer biometric systems in order to detect fraudulent access attempts.

With the advances in printing technology, it is getting easier for unauthorized users to develop high resolution photos and 3D printed objects that could attack the biometric systems even with having the highest recognition rate.

Before starting in the iris recognition process going from segmentation to classification, the system should be able to discover if the biometric sample is real or if it is a fake sample provided from an unauthentic user. A way to achieve that is by test the liveness of the iris sample provided.

Many Methods have been developed to detect the liveness of iris patterns. The challenge now is to verify if a method performs the same way with different attacks or if the characteristics of iris databases influence the accuracy of a liveness detection method.

1.4 Objective

The objective of the thesis is to evaluate the methods used for iris liveness detection with scenarios where different attacks from different datasets are used. Another objective is to study the impact of the segmentation phase in the iris liveness detection system comprehensively for a better application in real life scenarios.

1.5 Contribution

During the development process of the thesis, we gained extensive knowledge about attacks on biometrics, iris recognition and liveness detection algorithms used to detect attacks on iris recognition systems. We conducted experiments using different datasets that represent different attacks.

The contribution of the work can be summarized as follows:

1. Extensive tabular review for iris liveness detection techniques that facilitate the research in this point.
2. Evaluating and analyzing the results of BSIF using databases with the same type of attack (contact lens) tested before in Notre dame DB, in addition to different types of attacks: printed, plastic, synthetic.
3. Using segmented and unsegmented eye images in Near Infrared (NIR) and visible light databases to show if segmentation is required / not required or even it is better to use the whole image in some cases.
4. Proving that segmentation is not required for other attacks rather than contact lens.
5. Proving that using the whole image without segmentation is better than using the iris area in visible light datasets.
6. Proposing a new method using residual filters with BSIF that enhance on the results of contact lens databases.
7. Enhancing the accuracy of BSIF on Clarkson dataset from 91.67% to 93.33% in segmented mode using the first residual filter.

1.6 Thesis Organization

This thesis consists of six chapters:

Chapter 2 describes fundamentals of the biometrics and possible attacks

Chapter 3 explains the basics of iris liveness detection techniques.

Chapter 4 demonstrates literature review about hardware and software methods

Chapter 5 gives a detailed account on the proposed liveness detection method

Chapter 6 shows the experimental results of using the proposed method on datasets

Chapter 7 summarized the conclusion of the research and provides ideas for future work.

Moreover, the thesis contains references, an appendix, and an Arabic abstract.

Chapter 2

Biometrics