Vulnerability Assessment in the Use of Biometrics in Unsupervised Environments

by

Anas Hussein Ahmad Husseis

A dissertation submitted by in partial fulfillment of the requirements for the degree of Doctor of Philosophy in

Electrical Engineering, Electronics and Automation

Universidad Carlos III de Madrid

Advisor(s):

Raúl Sánchez Reíllo

Judith Liu Jiménez

Tutor:

Raúl Sánchez Reíllo

January 2021

This is for you, Dad.

Acknowledgements

The state-of-the-art languages do not have the capacity to put my gratitude into a form of written speech for those who supported me to achieving this thesis. Nevertheless, I still feel the necessity of not skipping this page.

In the first place, I would like to thank my advisors Raul and Judith for all the support they provided through my journey in GUTI. I am very proud for being a research fellow with these great advisors and I hope I will be good enough to make them proud of me in the future.

I would also like to thank my family for standing with me from the beginning. For being there supporting, listening, and giving good vibes all the time.

Infinite thanks to my colleagues (gutitos) and my friends all around the world for the continuous encouragement and enthusiasm. I would specifically mention my Japanese friends Ichigo, L, and Goku for being there all the time.
Finally, I would take the opportunity to thank myself for being patient and hard worker, for believing in me, and for the constant reminders that this thesis will be finely finished.

Published and submitted content

Journal papers:

- Anas Husseis, Judith Liu-Jimenez, Ines Goicoechea-Telleria, Raul Sanchez-Reillo, "Dynamic Fingerprint Statistics: Application in Presentation Attack Detection" in IEEE Access, 2018.
    - Published
    - Role: experimental planning, collecting data, performing the experiment, reporting results, and writing the paper.
    - Wholly included in Thesis. Chapter 4.
    - URL: https://ieeexplore.ieee.org/abstract/document/9097282
- Anas Husseis, Judith Liu-Jimenez, Raul Sanchez-Reillo, "Fingerprint Presentation Attack Detection Utilizing Spatio-Temporal Feature".
    - Submitted to Sensors (under review)
    - Role: performing the experiment, reporting results, and writing the paper.
    - Wholly included in Thesis. Chapter 5.
- Anas Husseis, Judith Liu-Jimenez, Raul Sanchez-Reillo, "The Impact of Pressure on the Fingerprint Impression: Presentation Attack Detection Scheme".
    - Submitted to Sensors (under review)
    - Role: performing the experiment, reporting results, and writing the paper.
    - Wholly included in Thesis. Chapter 6.

Conference papers:

- Anas Husseis, Judith Liu-Jimenez, Ines Goicoechea-Telleria, Raul Sanchez-Reillo, "A survey in presentation attack and presentation attack detection" in in IEEE International Carnahan Conference on Security Technology (ICCST), 2019.
    - Published
    - Role: conducting the study and writing the paper.
    - Wholly included in Thesis. Chapter 2.
    - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
    - The material from this source included int his thesis is not singled out with typographic means and references
    - URL: https://ieeexplore.ieee.org/abstract/document/8888436

- R Blanco Gonzalo, Barbara Corsetti, Ines Goicoechea-Telleria, Anas Husseis, Judith Liu-Jimenez, Raul Sanchez-Reillo, Teodors Eglitis, Elakkiya Ellavarason, Richard Guest, Chiara Lunerti, M Azimi, J Khiarak, Salatiel Ezennaya-Gomez, N Whiskerd, R Kuzu, E Okoh, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach" in IEEE International Carnahan Conference on Security Technology (ICCST), 2018.
    - Published
    - Role: participating in the experiment as an attacker and reporting partial results of the complete experiment.

- Partially included in Thesis. Annex I.
- The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
- The material from this source included int his thesis is not singled out with typographic means and references
- URL: https://ieeexplore.ieee.org/abstract/document/8585726

Other research merits

- I. Goicoechea-Telleria, A. Garcia-peral, A. Husseis, and R. Sanchez-reillo, “Presentation Attack Detection Evaluation on Mobile Devices: Simplest Approach for Capturing and Lifting a Latent Fingerprint,” in International Carnahan Conference on Security Technology (ICCST), 2018.
- Ines Goicoechea-Telleria, Kiyoshi Kiyokawa, Anas Husseis, Judith Liu-Jimenez, Raul Sanchez-Reillo, “Fingerprint Presentation Attack Detection: Multispectral imaging with a narrow-band camera using Bag of Features,” in International Carnahan Conference on Security Technology (ICCST), 2019.

Abstract

In the last few decades, we have witnessed a large-scale deployment of biometric systems in different life applications replacing the traditional recognition methods such as passwords and tokens. We approached a time where we use biometric systems in our daily life. On a personal scale, the authentication to our electronic devices (smartphones, tablets, laptops, etc.) utilizes biometric characteristics to provide access permission. Moreover, we access our bank accounts, perform various types of payments and transactions using the biometric sensors integrated into our devices. On the other hand, different organizations, companies, and institutions use biometric-based solutions for access control. On the national scale, police authorities and border control measures use biometric recognition devices for individual identification and verification purposes.

Therefore, biometric systems are relied upon to provide a secured recognition where only the genuine user can be recognized as being himself. Moreover, the biometric system should ensure that an individual cannot be identified as someone else. In the literature, there are a surprising number of experiments that show the possibility of stealing someone's biometric characteristics and use it to create an artificial biometric trait that can be used by an attacker to claim the identity of the genuine user. There were also real cases of people who successfully fooled the biometric recognition system in airports and smartphones [1]–[3]. That urges the necessity to investigate the potential threats and propose countermeasures that ensure high levels of security and user convenience.

Consequently, performing security evaluations is vital to identify: (1) the security flaws in biometric systems, (2) the possible threats that may target the defined flaws, and (3) measurements that describe the technical competence of the biometric system security. Identifying the system vulnerabilities leads to proposing adequate security solutions that assist in achieving higher integrity.

This thesis aims to investigate the vulnerability of fingerprint modality to presentation attacks in unsupervised environments, then implement mechanisms to detect those attacks and avoid the misuse of the system. To achieve these objectives, the thesis is carried out in the following three phases.

In the first phase, the generic biometric system scheme is studied by analyzing the vulnerable points with special attention to the vulnerability to presentation attacks. The study reviews the literature in presentation attack and the corresponding solutions, i.e. presentation attack detection mechanisms, for six biometric modalities: fingerprint, face, iris, vascular, handwritten signature, and voice. Moreover, it provides a new taxonomy for presentation attack detection mechanisms. The proposed taxonomy helps to comprehend the issue of presentation attacks and how the literature tried to address it. The taxonomy

represents a starting point to initialize new investigations that propose novel presentation attack detection mechanisms.

In the second phase, an evaluation methodology is developed from two sources: (1) the ISO/IEC 30107 standard, and (2) the Common Evaluation Methodology by the Common Criteria. The developed methodology characterizes two main aspects of the presentation attack detection mechanism: (1) the resistance of the mechanism to presentation attacks, and (2) the corresponding threat of the studied attack. The first part is conducted by showing the mechanism's technical capabilities and how it influences the security and ease-of-use of the biometric system. The second part is done by performing a vulnerability assessment considering all the factors that affect the attack potential. Finally, a data collection is carried out, including 7128 fingerprint videos of bona fide and attack presentation. The data is collected using two sensing technologies, two presentation scenarios, and considering seven attack species. The database is used to develop dynamic presentation attack detection mechanisms that exploit the fingerprint spatio-temporal features.

In the final phase, a set of novel presentation attack detection mechanisms is developed exploiting the dynamic features caused by the natural fingerprint phenomena such as perspiration and elasticity. The evaluation results show an efficient capability to detect attacks where, in some configurations, the mechanisms are capable of eliminating some attack species and mitigating the rest of the species while keeping the user convenience at a high level.

Resumen

En las últimas décadas, hemos asistido a un despliegue a gran escala de los sistemas biométricos en diferentes aplicaciones de la vida cotidiana, sustituyendo a los métodos de reconocimiento tradicionales, como las contraseñas y los tokens. Actualmente los sistemas biométricos ya forman parte de nuestra vida cotidiana: es habitual emplear estos sistemas para que nos proporcionen acceso a nuestros dispositivos electrónicos (teléfonos inteligentes, tabletas, ordenadores portátiles, etc.) usando nuestras características biométricas. Además, accedemos a nuestras cuentas bancarias, realizamos diversos tipos de pagos y transacciones utilizando los sensores biométricos integrados en nuestros dispositivos. Por otra parte, diferentes organizaciones, empresas e instituciones utilizan soluciones basadas en la biometría para el control de acceso. A escala nacional, las autoridades policiales y de control fronterizo utilizan dispositivos de reconocimiento biométrico con fines de identificación y verificación individual.

Por lo tanto, en todas estas aplicaciones se confía en que los sistemas biométricos proporcionen un reconocimiento seguro en el que solo el usuario genuino pueda ser reconocido como tal. Además, el sistema biométrico debe garantizar que un individuo no pueda ser identificado como otra persona. En el estado del arte, hay un número sorprendente de experimentos que muestran la posibilidad de robar las características biométricas de alguien, y utilizarlas para crear un rasgo biométrico artificial que puede ser utilizado por un atacante con el fin de reclamar la identidad del usuario genuino. También se han dado casos reales de personas que lograron engañar al sistema de reconocimiento biométrico en aeropuertos y teléfonos inteligentes [1]–[3]. Esto hace que sea necesario investigar estas posibles amenazas y proponer contramedidas que garanticen altos niveles de seguridad y comodidad para el usuario.

En consecuencia, es vital la realización de evaluaciones de seguridad para identificar (1) los fallos de seguridad de los sistemas biométricos, (2) las posibles amenazas que pueden explotar estos fallos, y (3) las medidas que aumentan la seguridad del sistema biométrico reduciendo estas amenazas. La identificación de las vulnerabilidades del sistema lleva a proponer soluciones de seguridad adecuadas que ayuden a conseguir una mayor integridad.

Esta tesis tiene como objetivo investigar la vulnerabilidad en los sistemas de modalidad de huella dactilar a los ataques de presentación en entornos no supervisados, para luego implementar mecanismos que permitan detectar dichos ataques y evitar el mal uso del sistema. Para lograr estos objetivos, la tesis se desarrolla en las siguientes tres fases.

En la primera fase, se estudia el esquema del sistema biométrico genérico analizando sus puntos vulnerables con especial atención a los ataques de presentación. El estudio revisa la literatura sobre ataques de presentación y las soluciones correspondientes, es decir, los mecanismos de detección de ataques de presentación, para seis modalidades biométricas:

huella dactilar, rostro, iris, vascular, firma manuscrita y voz. Además, se proporciona una nueva taxonomía para los mecanismos de detección de ataques de presentación. La taxonomía propuesta ayuda a comprender el problema de los ataques de presentación y la forma en que la literatura ha tratado de abordarlo. Esta taxonomía presenta un punto de partida para iniciar nuevas investigaciones que propongan novedosos mecanismos de detección de ataques de presentación.

En la segunda fase, se desarrolla una metodología de evaluación a partir de dos fuentes: (1) la norma ISO/IEC 30107, y (2) Common Evaluation Methodology por el Common Criteria. La metodología desarrollada considera dos aspectos importantes del mecanismo de detección de ataques de presentación (1) la resistencia del mecanismo a los ataques de presentación, y (2) la correspondiente amenaza del ataque estudiado. Para el primer punto, se han de señalar las capacidades técnicas del mecanismo y cómo influyen en la seguridad y la facilidad de uso del sistema biométrico. Para el segundo aspecto se debe llevar a cabo una evaluación de la vulnerabilidad, teniendo en cuenta todos los factores que afectan al potencial de ataque. Por último, siguiendo esta metodología, se lleva a cabo una recogida de datos que incluye 7128 vídeos de huellas dactilares genuinas y de presentación de ataques. Los datos se recogen utilizando dos tecnologías de sensor, dos escenarios de presentación y considerando siete tipos de instrumentos de ataque. La base de datos se utiliza para desarrollar y evaluar mecanismos dinámicos de detección de ataques de presentación que explotan las características espacio-temporales de las huellas dactilares.

En la fase final, se desarrolla un conjunto de mecanismos novedosos de detección de ataques de presentación que explotan las características dinámicas causadas por los fenómenos naturales de las huellas dactilares, como la transpiración y la elasticidad. Los resultados de la evaluación muestran una capacidad eficiente de detección de ataques en la que, en algunas configuraciones, los mecanismos son capaces de eliminar completamente algunos tipos de instrumentos de ataque y mitigar el resto de los tipos manteniendo la comodidad del usuario en un nivel alto.

Table of Contents

List of figures

List of Tables

Chapter 1. Introduction

The rapid technological development has influenced our daily life allowing us to perform personal, administrative, and job-related tasks electronically. Nonetheless, the electronic services (e.g. governmental, banking, data storage) require a high level of security to ensure that the person who performs the e-operation is authorized to do so. For that reason, biometric systems have been replacing the conventional recognition solutions such as passwords and tokens, achieving high acceptability and overcoming some disadvantages such as forgetting passwords and stealing cards [4], [5].

Theoretically, biometric solutions provide sustained and secured recognition since biometric traits are assumed to be unique, collectible, convenient, long term, universal, and acceptable [6]. Despite all these attractive features, it has been proved that most of the human biometric characteristics can be captured by an attacker and used to create a duplicate (e.g. facial mask, silicon fingerprint, face image) with the objective of claiming someone's identity [7].

The threat of biometric identity theft has been gaining much attention since a large proportion of the biometric solutions is utilized in unsupervised devices; e.g. smartphones, laptops, smart-cards, etc. The level of human supervision is a crucial element when speaking about biometric security. For example, biometric data acquisition at police stations is typically carried out with the supervision of a human operator, which diminishes the opportunities of attack. Contrarily, the attacker in unsupervised environments would exploit the absence of human supervision so that he can perform different types of attacks without restrictions.

Consequently, the biometric system should determine two questions: (1) does the presented biometric characteristic match with the one that belongs to the claimed identity? (2) is the presented biometric characteristic a bona fide, i.e. genuine, or an attack? In other words, in addition to the biometric recognition functionality, which already answers the first question, there should be automatic countermeasures within the biometric system that provide an explicit decision about the nature of the presented biometric trait so that the second question is determined.

Attacking biometric systems using manipulated biometric characteristics belongs to the group of physical attacks that take place at the biometric sensor. These attacks are standardized as Presentation Attacks (PAs) [8]. On the other hand, the automatic mechanisms that verify the authenticity of the presented trait to the biometric sensor are standardized as Presentation Attack Detection (PAD) mechanisms.

Despite the intensive research in the field of biometric security, the problem of PAs is still open to researchers seeking to achieve a deeper understanding of the issue and to propose

efficient solutions that detect those attacks. Accordingly, this thesis investigates the vulnerability of biometric systems to PAs in different modalities and picks up the fingerprint modality aiming to propose a set of software solutions that mitigate the risk of PAs. Moreover, the thesis associates the proposed solutions with the corresponding level of threat through an evaluation methodology that puts together the vulnerability assessment and the performance of presentation attack detection mechanisms. First, the vulnerability assessment is carried out following the Common Evaluation Methodology (CEM) [9], by the Common Criteria, determining the existence of exploitable vulnerabilities in the system and defining the threat of attacks by analyzing the different factors that influence the attack potential. Secondly, the performance of the proposed PAD mechanisms is evaluated following the standards ISO/IEC 30107 1-3 [8], [10], [11]. The combination of these two parts provides a clear representation of the resistance of PAD to a certain level of threat.

This chapter seeks to provide a comprehensive overview of the biometric systems' security and the potential vulnerabilities in the biometric recognition scheme. The issue of PA is discussed by analyzing basic definitions and expounding why biometric systems are vulnerable to PAs. Finally, the organization of the document is presented providing the main contributions in the thesis.

1. 1. BACKGROUND ON PRESENTATION ATTACKS

In 2011, a young Asian man had successfully deceived the border control authorities in Hong Kong-China. He boarded a flight heading to Vancouver-Canada using a silicone face and neck mask that gave him the appearance of an old man [2], shown in Figure 1.1. The airlines' security staff noticed that the old man appeared to have young-looking hands. Then, during the flight, the man went to the toilet to remove the mask and returned to his place causing more suspicions. The cabin crew directly reported the case to the Canada Border Services Agency (CBSA) where the traveler was escorted off the plane by Border Services Officers on landing. In 2013, the biometrics hacking team of the Chaos Computer Club had successfully bypassed the fingerprint security of iPhone 5s using every day means [12]. The group demonstrated that a photograph of the user’s fingerprint, taken from a glass surface is enough to create an artificial fingerprint that is capable of unlocking the mobile device. More recently, in 2017, a group of researchers from Bkav demonstrated that the facial recognition of the iPhone X can be fooled using a 3-D printed mask for a cost of 150$ [3]. These observations indicate that biometric recognition systems have security shortcomings. That raises the alarm on the usage and deployment of biometric based solutions and imposes the necessity of considering security flaws such as the vulnerability to presentation attacks.

Figure 1.1. The plane traveler boarded up with a silicone face and neck veil that gave him the look of an elderly person [2].

Based on those real cases, the following question arises: "why biometric systems are vulnerable to presentation attacks when they are claimed to be more secured than conventional recognition techniques?". A simple way to answer this question may start from the following definitions, given in the standard ISO/IEC 2382-37:2017 Information technology – Vocabulary [11]:

- **biometric characteristics:** *biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition*.
- **biometric recognition:** *automated recognition of individuals based on their biometric characteristics*.

From these definitions, we conclude that biometric systems require only distinguishing and repeatable human characteristics to perform the recognition process. If those characteristics were captured and used to create a duplicate artefact, and then the artefact was presented at the biometric sensor, there would be a chance that the biometric system will recognize the artefact as the genuine biometric characteristic, thus the system's security is compromised. The success potential of this type of attack depends on several physical and logical factors, subsequently, the attack potential must be analyzed and calculated to show the resistance of biometric systems to PAs; further details about vulnerability analysis are provided in Chapter 3.

1. 2. WHAT IS PRESENTATION ATTACK DETECTION?

We can define PAD as the process of determining the authenticity of biometric presentations by extracting discriminative features, i.e PAD features, from the acquired biometric data. The initial matters that need to be considered are "*what are these features?*" and "*why are they expected to distinguish malicious presentations?*". As soon as the PAD features are defined, the PAD mechanism is implemented in a fashion that examines the

captured biometric presentation using the defined features, then determines whether it is a bona fide or attack presentation.

The attributes from both bona fide and attack presentations can be exploited to define the PAD features. Genuine biometric characteristics have natural physical and behavioural attributes which can be captured and analyzed for the purpose of attack detection, for example, the human face has its 3-D geometry, skin characteristics, and voluntary and involuntary reactions. On the other hand, analyzing known attacks leads to define attributes that assess the determination of PAs, for example, photo attacks on face recognition systems have a 2-D geometry and might contain distortion due to the image/video encoding in the printing or display device.

The objective of PAD mechanisms is to explicitly declare a decision to accept or reject the performed presentations, moreover, PAD mechanisms should satisfy the following requirements during its operation [13]:

1) Accuracy: the PAD mechanism should demonstrate high accuracy of detecting malicious presentations. It is equally important that the PAD mechanism demonstrates a low false rejection rate of bona fide subjects.
2) Non-invasive: the detection procedure should not involve any harmful or excessive contact with the user.
3) User friendly: users should not be hesitant to collaborate to perform the process.
4) Fast: current biometric authentication processes require a real-time operation, and the use of the PAD mechanism should not interfere with the intended authentication process.
5) Low cost: the cost is an essential factor in deploying PAD solutions. High-cost solutions might not be adopted by technology manufacturers.

1. 3. THE OBJECTIVE OF THE THESIS

This thesis is devoted to providing an overview of the PA and PAD in different biometric modalities and take the research further to study the fingerprint modality providing various PAD mechanisms that mitigate the risk of fingerprint PAs considering different sensing technologies. The ultimate goal is to achieve high accuracy for the proposed PAD mechanisms keeping the user-convenience at a high level.

Fingerprint modality was selected because it is one of the most deployed technologies in the biometric market. The fingerprint sensor market size is projected to grow from USD 3.5 billion in 2019 to USD 7.1 billion by 2024 [14]. The modality had demonstrated efficient performance and high user acceptance, for that reason, it has been integrated into many supervised and unsupervised recognition solutions. On the other hand, fingerprints are known to leave traces at touched surfaces providing a potential ground for attackers to exploit the biometric system's vulnerability to PAs and initiate an attack.

To achieve these objectives, the thesis conducts the following phases:

Reviewing and analysing the recent investigation in the domain of PA and PAD and revisit the existing taxonomies providing suggestions and necessary modifications, keeping in mind the current investigations and directions of development.

Combining the vulnerability assessment and the PAD performance evaluation in one evaluation methodology that has the capacity to demonstrate the technical capabilities of the proposed PAD mechanisms and provides vulnerability analysis of the corresponding threat.

Planning, implementing, and conducting dynamic data collection with the objective of acquiring fingerprint videos from (i) bona fide users, and (2) attacks using different attack species.

Implementation, development, and evaluation of PAD mechanisms.

1. 4. THESIS ORGANIZATION

This dissertation is divided into seven chapters. The first chapter has provided an overview of the thesis topic, the importance of the study, and the intended research direction. The rest of the dissertation is presented as follows (Figure 1.2):

Chapter 2: In this chapter, a brief overview of biometric security is given. The vulnerabilities of biometric systems are explained by showing the different points of attacks on the generic biometric scheme. The chapter tightens the focus on the vulnerability of presentation attacks. Then, the state of the art of presentation attack and presentation attack detection is provided for six biometric modalities, specifically: fingerprint, face, iris, vascular, handwritten signature, and voice. A new taxonomy of presentation attack and presentation attack detection is proposed to categorize the prospect attacks and proposed PAD mechanisms.

Chapter 3: This chapter provides the evaluation methodology that had been followed during the experimental part of this thesis. The methodology includes techniques and measures that characterize valid and comparable evaluations for the proposed PAD mechanisms. Moreover, the evaluation methodology details the data collection and analyzes the attack potential for the collected attacks.

Chapter 4: The first PAD mechanism is proposed in this chapter. In this experiment, the fingerprint video is investigated as a sequence of dependent frames. It was noticed that the visual appearance of the videos shows differences in the development of global features such as intensity, contrast, randomness, etc. Consequently, the method extracts eight global features from each frame and concatenates the features of all the frames in the video, and uses them as the PAD features to classify the presentation to “attack” or “bona fide”.

Chapter 5: As the previous mechanism concatenates 2-D features from the video frames, this experiment investigates the fingerprint presentation (i.e. fingerprint video) as a 3-D signal. In this chapter, various video descriptors are utilized to extract the spatio-temporal features and utilize them as PAD features. The proposed features show significant improvement over the results obtained in Chapter 4. Moreover, the obtained accuracy shows improvement to the State-of-the-Art dynamic mechanisms.

Chapter 6: The last experiment focuses on analyzing the influence of fingerprint pressure on the dynamic features that had been studied in chapters 4 and 5. The study shows that once the capture-subject adds pressure during the fingerprint presentation, the dynamic features provide more accurate and stable performance.

Chapter 7: Finally, this last chapter draws the main conclusions of this thesis and provides future directions of development in this domain.

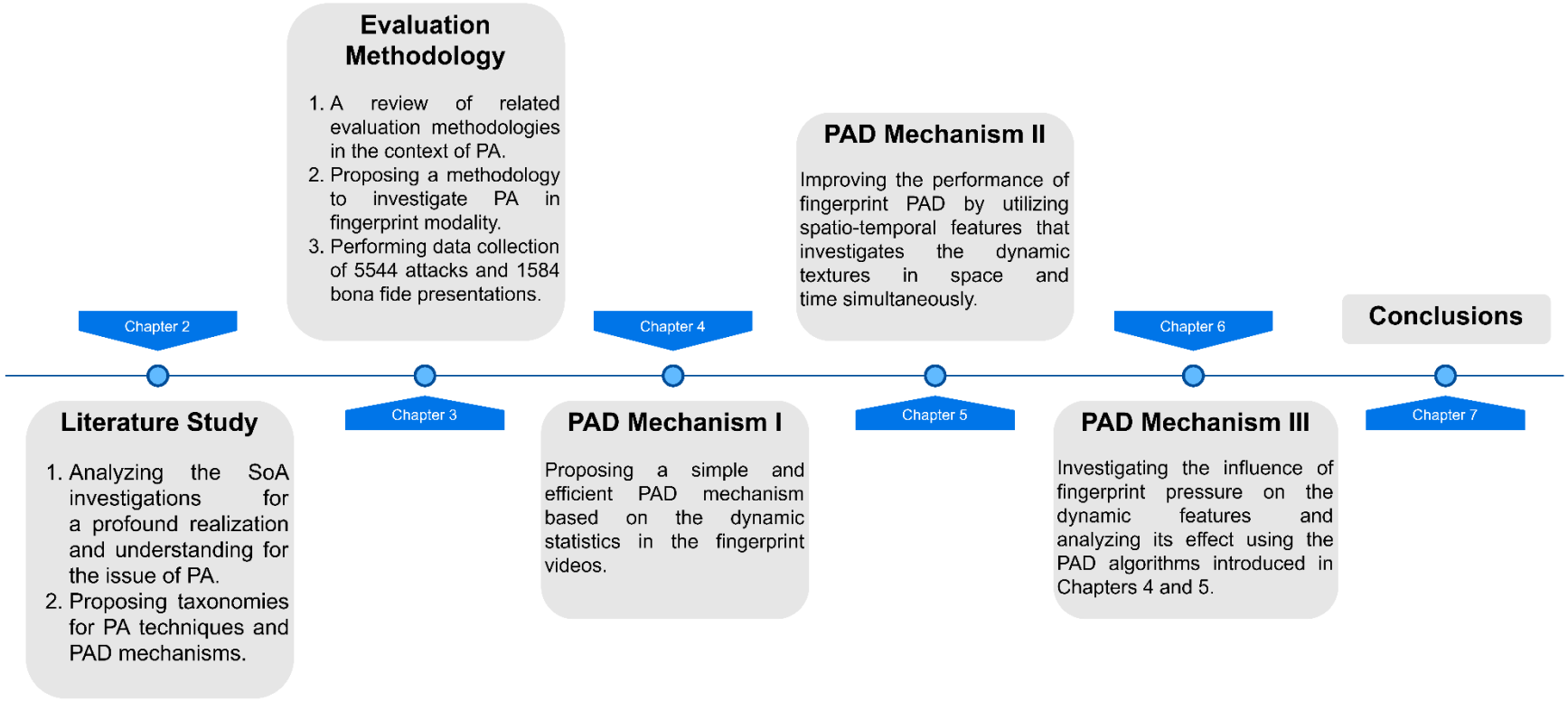


Figure 1.2. The main contributions of the thesis and the corresponding organization in this document.

Chapter 2. A Survey in Presentation Attack and Presentation Attack Detection

Despite the accuracy of biometric systems, there exist many vulnerabilities that can be exploited by attackers seeking to manipulate the final decision of the biometric recognition process [15]. The existence of those vulnerabilities hampers the system's security, therefore, performing a vulnerability analysis that shows the system's resistance to prospective attacks is indispensable. Studying the known vulnerabilities specifies approximate guidance for the system security considering certain scale/s of threat.

Given that the focus of this thesis is on presentation attack and presentation attack detection, this chapter seeks to review the vulnerable points in the biometric system, then to conduct a literature review on presentation attack and presentation attack detection considering different biometric modalities. To achieve these objectives, this chapter is organized as follows: Section 1 Introduces the security of biometric systems and explains the points of attack on the generic biometric system. Section 2 proposes taxonomies for presentation attacks and presentation attack detection mechanisms. Section 3 and Section 4 provide a literature study on PA and PAD considering six biometric modalities. Finally, Section 5 concludes the key findings of this chapter.

2. 1. INTRODUCTION TO BIOMETRIC SECURITY

There are two main categories of attacks that endeavor to reverse the biometric recognition decision: (1) the presentation of manipulated biometric characteristics to the biometric sensor, i.e. presentation attack, also known as direct or spoofing attack; and (2) manipulating the electronic and/or digital process in the biometric system, i.e. indirect attacks. The second category can be further analyzed by showing the internal components of the biometric system and points of attacks, as shown in Figure 2.1; the figure is illustrated in the operational environment whereas the system can be used either in identification or verification mode.

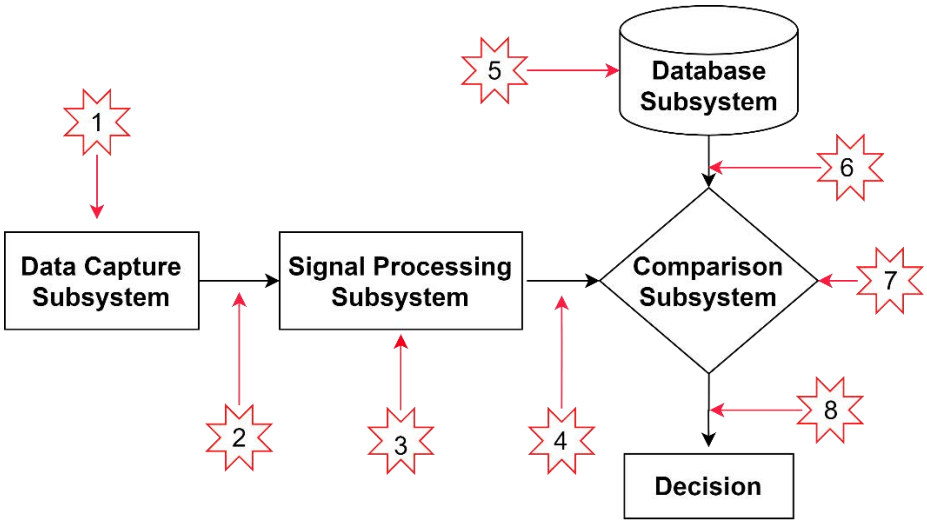


Figure 2.1. The generic biometric scheme in the subsystem level and the points of attacks [8].

2. 1. 1. Presentation Attack

Attack presentations are performed at the physical level of the recognition environment, from Figure 2.1 (attack point 1), by two types of attackers: biometric concealer, where the attacker purposes to avoid being recognized as a known capture subject to the system, or biometric imposter, where the attacker intends to claim someone's else identity using a Presentation Attack Instrument (PAI) [8].

The biometric concealer endeavors to conceal his/her biometric characteristics rather than demonstrating the characteristics of a known capture subject, examples include utilizing artefact, through camouflage, or modification of the genuine biometric characteristics.

On the other hand, there are two fashions to perform imposter attacks. First, the imposter selects the targeted capture subject, creates duplicate biometric characteristics, and claims the targeted individual's identity. Second, the imposter uses a manipulated biometric characteristics intending to be recognized as any person enrolled in the system.

2. 1. 2. Indirect Attacks

As follows from Figure 2.1, it's observed that indirect attacks target either the communication channels between the biometric subsystems or the internal components of those subsystems. Nonetheless, the attacker needs access to the internal processes in order to carry out attacks at points 2-8. This subsection discusses indirect attacks with the corresponding vulnerability points.

Communication Channels

The different subsystems within the biometric system are connected through multiple communication channels, points 2, 4, 6, and 8, which transmit the signal/s from one subsystem to the next. In this group of attacks, the attacker seeks to modify the transmitted signal with the

objective of manipulating the recognition decision. Thus, biometric systems are designed in a fashion that secures the data during transmission to avoid potential attacks.

Biometric Subsystems

The biometric system includes a sequence of subsystems that perform the different tasks of biometric recognition (Figure 2.1). These subsystems can be targeted by the attacker seeking to manipulate the recognition process as follows:

a) **Data Capture Subsystem:** Besides the presentation attack, the biometric sensor, point 1, is subject to indirect attacks. The acquisition device can be replaced by another one that transmits a duplicate biometric sample such as a replay attack. Therefore, the biometric system is expected to include countermeasures that identify any attempt to interfere with the physical sensor.
b) **Signal Processing Subsystem:** The captured biometric sampled is handled at the first level at this subsystem, point 3. The executed processes depend on the implementation of the biometric system and may include: quality check, segmentation, noise removal, signal enhancement, and feature extraction. The attacker attempts to exploit this vulnerability by modifying the digital process seeking to bypass the system's security. For instance, the feature extractor might be replaced to perform a hell climbing attack.
c) **Comparison Subsystem:** The matching process compares the captured sample with a stored template in the database. If the attacker was able to compromise the matching process such that the matching score is modified, he can be recognized by the system as being the claimed identity.
d) **Database Subsystem:** the database contains the data of all enrolled individuals. Once the database is compromised, the attacker can add, modify, and remove data and then perform several types of attacks.
e) **Administrative Management** The administration of biometric systems is a vital element that ensures biometric security. The integrity of the authorized administrator/s on controlling: the decision thresholds, the quality check criteria, and the enrollment process, reflects the integrity of the overall system.

2. 2. PRESENTATION ATTACK AND PRESENTATION ATTACK DETECTION TAXONOMIES

Each biometric system utilizes a specific physiological and/or behavioral characteristic for the recognition process. Additionally, each biometric modality has different types of sensors that vary with other technologies in terms of data acquisition methods. This variety inquires the attacker to perform the presentation attack using a specific Presentation Attack Instrument (PAI) species that is adjusted to the target biometric system. The different PAI species may come from different sources and provide distinct capabilities even for the same biometric modality. For instance, image

and video attacks on face recognition systems show different dynamic characteristics when presented to the same sensor.

On the other hand, the research on presentation attack detection has been quite extensive in recent years. There had been hundreds of proposals for automatic countermeasures that reduce the risk of attack presentations. Some of these proposals were based on modifying the design of the biometric sensor while others focus on modifying the recognition process by additional examination for the acquired biometric sample.

In order to organize the investigations in this line of research, different taxonomies had been proposed in the literature to classify the different categories of presentation attack and presentation attack detection mechanisms. First, hardware/software classification [16] sorts the PAD mechanisms by implying the necessity of modifying the hardware design of the biometric sensor, (b) dynamic/static classification [17] clarifies whether the temporal biometric information is needed for a PAD mechanism.

The next subsections propose general taxonomies for presentation attack and presentation attack detection.

2. 2. 1. Presentation attack taxonomy

In general, capturing biometric traits is categorized based on the cooperation of the bone fide subject [11] (Figure 2.2). Cooperative PAs are carried out with full cooperation of the bona fide subject regardless of the intention of the attack, while non-cooperative PAs are performed assuming that the target bona fide is unaware of the attack or the attack is performed against his/her well. Non-cooperative attacks are often rather sophisticated because of the need for special expertise and adequate hardware/software tools, moreover, the targeted biometric modality plays an important role to determine the ease of the process. For instance, latent fingerprints, which are left on surfaces due to the fingerprint moistness, can be developed and captured by an expert using specific tools then used to create an artificial fingerprint. On the contrary, the vascular pattern needs to be captured directly from the bona fide subject using an infrared imaging capture device, as the pattern is not exposed either leaves traces.

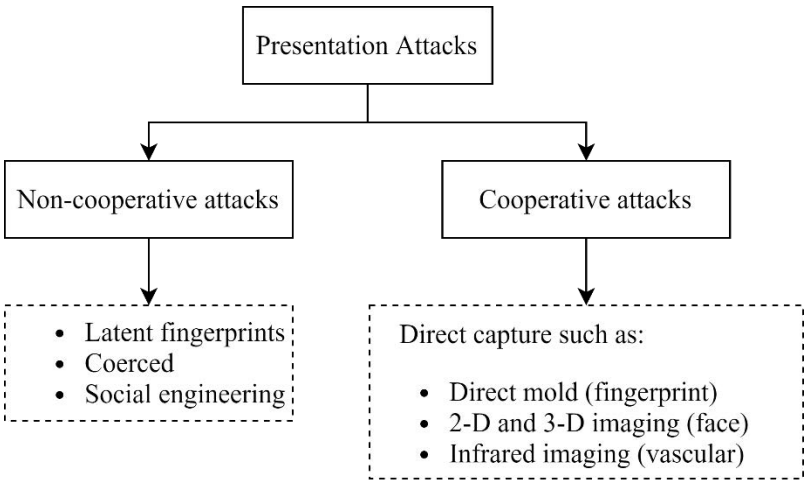


Figure 2.2. Types of PAs based on the cooperation of the bona fide user.

On the other hand, perceiving the intended meaning of performing a presentation is critical in analyzing presentation attacks. Two main classes are established for presentation attack based on the user intention. Each class consists of different subclasses of attacks, taking into account the attack type (see Figure 2.3).

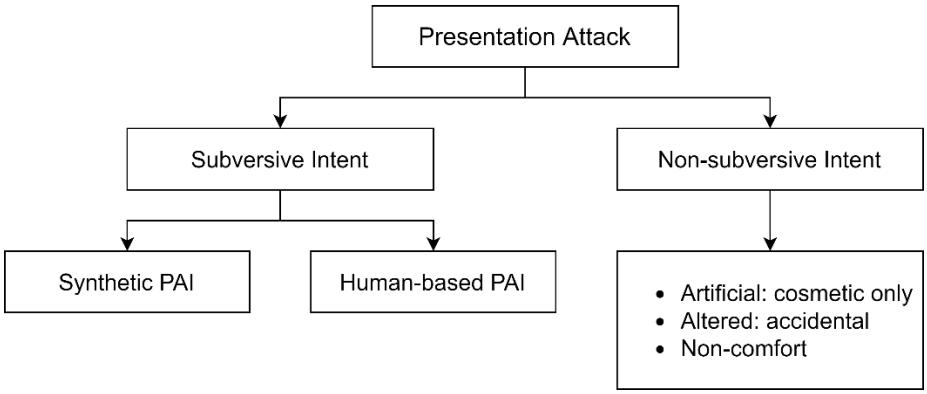


Figure 2.3. Presentation attack taxonomy (inspired by [8]).

2.2.1.1 Attacks with non-subversive intent

In this case, the subject performs a biometric presentation that may interfere with the final decision of the recognition system. Basically, no malicious intent is considered from the subject's standpoint. For example, using artificial products for cosmetic purposes, such as cosmetic contact lenses, may lead to suspicious detection. Furthermore, the genuine biometric trait might be altered because of accidental changes like burns or scars. Unlimited to these cases, non-conformant presentations (e.g. non-attentive, poorly trained, and careless users) are considered non-subversive; no malicious goal is assumed.

2.2.1.2 Attacks with subversive intent

This category assumes that malicious purpose is intended by the attacker. The presented instrument could be synthesized or human-based, and yet it could be created with the cooperation of the genuine user. The proposed taxonomy details subversive attacks into subclasses based on the attack type.

1) Synthetic PAI: Synthesizing a PAI might be simple such as wearing sunglasses or sophisticated like producing a 3D facial mask. Generally speaking, PAI can be organized from two different perspectives:

First, does PAI contain full or partial biometric information? Depending on attack type we may define the following types:

- Fully synthesized (complete) artefacts are created such that PAIs have identical features as real biometric traits. For instance, 3D masks and artificial eyes provide a 3D presentation that could bypass the system's countermeasures;
- partial samples are those samples that contain partial discriminative features and used later by a claim or evade an identity. For example, textured contact lens attack is a potential attack due to the fact that it has a 3D shape of the eye when it's being used by the attacker, furthermore, the correspondent eye behaves naturally.

Second, can PAI provide the dynamic information of real biometrics? The artefact may have dynamic changes or not, the attacker makes a decision based on the attack type and ToE:

- Static artefact provides information of time instant for a biometric trait. Image attack on face or iris systems is a static attack;
- Dynamic artefact provides dynamic temporal information during the presentation. For instance, a video attack provides dynamic information that may succeed in the attack.

Previous classes result in four generic types of PAIs: (1) static complete instrument, (2) static partial instrument, (3) dynamic partial instrument, and (4) dynamic complete instrument. Examples of these classes are provided in Table 2.1.

2) Human-based PAI: instead of synthesizing a PAI, attackers may present live, dead, altered, or imitated samples. One way to present a live sample occurs when coercing the genuine user to present his biometric sample to the sensor. Similarly, dead body parts (i.e. cadaver or severed parts) could be employed to overcome the biometric system, dead fingers are studied in [18]. Moreover, alterations on the attacker biometric trait are considered as a potential change that brings out different characteristics that result in a suspicious presentation (e.g. damaged on purpose, burns, plastic surgeries).

Behavioral biometrics are also attainable, whereas attackers collect as much information as possible about the trait and try to imitate it at the biometric sensor. The dynamic handwritten signature is a significant example where the attacker aims to forge the graphical form of the signature while applying similar features such as speed, pressure, and orientation [19]–[21].

Table 2.1. Presentation attack instruments.

PAI source	PAI Type	Examples
Human-based	Live sample	Zero-effort attempt, (under coercion, drugged, unconscious) genuine.
	Dead body part	Pulled eye, severed hand or finger, cadaver part.
	Altered	Body part amputation, plastic surgeries, fingerprints switching.
	Behavioral	Forging handwritten signature, mimicking voice, gait imitation.
Synthetic	static complete	Printed image, display image, full head casting, artificial eye, static handwritten signature.
	static partial	Glasses, scarf, partial face image.
	dynamic partial	Cosmetic makeup, textured eye lenses, facial hair, dirty fingerprints.
	dynamic complete	Video attack, voice record, wearable 3D masks, forging a dynamic handwritten signature.

Consequently, we can conclude that biometric vulnerability to attack presentations is interpreted by stating that biometric systems are not yet as perfect as they should be. In addition to the distinguishable and time-invariant features, biometric systems should inspect additional discriminative features that confirm that the presented biometric characteristic at the data capture subsystem belongs to the bona fide user.

2. 2. 2. Presentation attack detection taxonomy

Due to the vast amount of literature on PAD, different taxonomies have been proposed to organize the conducted investigations by identifying useful and meaningful classes [13], [17], [22], as shown in Figure 2.4. Those taxonomies facilitate research and discovery in the field of PAD driving improved detection mechanisms and novel methods, moreover, manifest the potential directions to develop robust and accurate PAD mechanisms. It is noticed that those classifications focus on the required tools to develop the mechanism, i.e. hardware and software tools, and at a secondary level discuss the proposed features/methods that are necessary for the implementation of the PAD scheme. In other words, the taxonomy in Figure 2.4 can be interpreted as the following three steps:

1. Defining the required PAD features.
2. Inspecting whether the defined features can be acquired by the SoA sensors or need a modification/addition on the hardware modules.
3. Determining the specifications of the acquisition and/or processing in order to carry out the PAD examination.

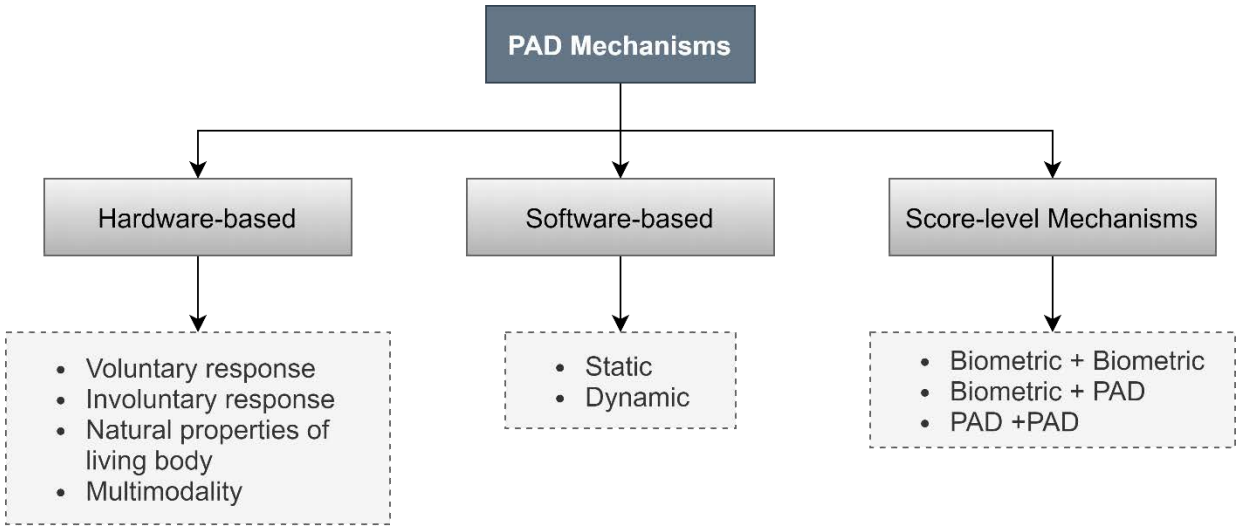


Figure 2.4. State of the art taxonomy of PAD mechanisms [13].

State of the art classifications categorize PAD methods into three main classes based on the necessary tools to detect the attacks [13]: (1) Hardware methods, where extra hardware components are embedded in the biometric sensor. (2) Software methods, where additional processes take place in order to analyze the acquired data, which support the decision process to mitigate presentation attacks. (3) Score level methods, mainly, the process is performed in the matcher to analyze the information that comes from biometric sensors, PAD mechanisms or a combination of both.

It is noticed from the classification in Figure 2.4 that the PAD categories describe the used tools and acquisition methods to classify the PAD mechanisms. However, it does not provide information about the exploited PAD features which are the basis of the final decision to accept or reject a presentation. For that reason, we propose a PAD taxonomy that classifies the PAD mechanisms based on the investigated PAD attributes which are assumed to bring out discriminative features and lead to rejecting attack presentations (Figure 2.5).

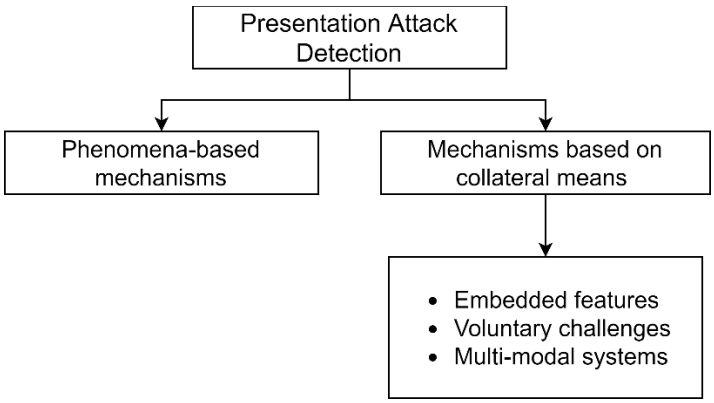


Figure 2.5. Presentation attack detection Taxonomy.

The following subsections expose these two categories with examples for each.

2.2.2.1 Within sample phenomena

In addition to the unique discriminative pattern of a natural biometric trait, manifest and latent spatio-temporal information can be extracted. Case in point, the human face has a unique 3D geometry that has specific characteristics and capable of responding to environmental conditions; unconscious responses like eye blinking. This definition of face extends the meaning for face biometric trait. Therefore, a PAD mechanism can be implemented based on that unique 3-D geometry to detect 2-D attacks (images and videos). Furthermore, vein pattern is recognized by blood flow in the vein network, in this case, the dynamic acquisition might be utilized to prove the trait liveness.

In this class, the PAD features are caused by the genuine biometric trait and they can be captured through modifying the acquisition and processing methods or by utilizing additional hardware.

2.2.2.2 Collateral means

This group focuses on the acquired biometric sample to be a source of extra information, which could be exploited to classify bona fide and attack presentations. Collateral information is not necessarily provided in natural presentations, other types of collateral means might be included in voluntary challenge response and multimode composition.

- Embedded features: in this class, the PAD features are caused by elements other than the biometric trait; e.g. caused by the PAI or the behaviour of the attacker. Thus, the acquired presentations are expected to contain additional means that assess the process of detecting attacks. For instance, distortion analysis, texture analysis, and quality measures are popular and widely investigated tools in this type of PAD mechanism.
- Voluntary challenge response: Humans are capable to respond to voluntary requests like mouth and eye movement [23], where the PAD mechanism analysis the response to eliminate potential attacks.
- Multimodal biometrics: different combinations of biometric modalities are proposed in the literature, proposing enhancement in the overall security of the biometric system [24]–[26]. The system acquires different traits and combines mechanism results to take a decision that verifies or rejects the presentation.

Literature exposes more research on software solutions compared to those studies on hardware solutions. Software solutions are proposed on testing datasets of biometric sensors without any need to modify the original design of the sensor, which means no additional cost on the overall system. Moreover, software solutions assist the deployed commercial devices that use biometric recognition systems.

The next two sections explore presentation attacks and correspondent solutions that aim to eliminate or mitigate those attacks.

2. 3. STATE OF THE ART IN PRESENTATION ATTACK

The vulnerability of biometric systems to presentation attacks has gained outstanding interest from the researchers as shown in the abundant and various explorations in this research scope. This section reviews the literature of presentation attacks on six biometric modalities (iris, fingerprint, face, vascular, handwritten signature, and voice) and connects the defined attacks with the taxonomy in Section 2.

2. 3. 1. Iris recognition

Iris recognition system may use visible-light [27]–[29] or near-infrared (NIR) illumination to acquire the iris sample. Systems that operate on visible light illumination had shown a major obstacle to localizing the pupil [30], especially, for eyes with a high concentration of melanin. This is explained by the significant capability of melanin to absorb light. Currently, because of the high accuracy of NIR systems, all commercial sensors work on NIR illumination [31], [32].

Identifying the sensing technology directs the attacker to choose a PAI that may succeed in the intended PA. Two comprehensive surveys [32], [33] have been proposed to cover potential attacks on the iris recognition system. Table 2.2 summarizes known attacks and connect them with the proposed taxonomy in Figure 2.3:

Table 2.2. Presentation attack on iris recognition systems.

PAI type		PAI	REFERENCES
Synthetic	**Static complete**	Printed image	[34]–[36]
		Prosthetic Eye	[33], [37]–[41]
		Display image	[42]–[52]
	Dynamic Complete	Display video	
		Textured contact lens	(imposter)
	Dynamic Partial	Textured contact lens (cosmetic)	[53], [54] (concealer)
Human-based	**Non-Conformant Use**	Eye movement and rotation	[55]
		Actual eye affected by drugs	[56], [57]
	Cadavers	Cadaver eye	[58]–[60]
	Coercion	Presentation under coercion	-

2. 3. 2. Fingerprint recognition

In the literature, there are many studies that have been carried out to prove the feasibility of creating an artificial fingerprint from latent fingermarks [34], [61]–[64]. Recent investigation has demonstrated an imaging technique that revealed fingermarks on difficult substrates, an exceptional level of detail has been obtained after over 26 days of deposition [65].

Biometric society is aware of this threat, and currently, many researchers are conducting presentation attack experiments to estimate the risk of such attacks. Often, those studies are performed with the cooperation of subjects, where a mold of fingermarks is taken directly from the real finger [61]–[64], [66]–[72].

Various reviews of the literature on fingerprint presentation attacks have been carried out in [17], [73], [74], to investigate the system's vulnerabilities and classify corresponding threats and countermeasures. Table 2.3 lists the investigated attack types, and it is followed by key observations.

Table 2.3. Presentation attack on fingerprint.

PAI type		PAI
Synthetic	**Static complete**	Printed image
		Fingerprint reactivation
	Dynamic Complete	Artefacts
		Latent fingerprint
	Dynamic Partial	
Human-based	**Non-Conformant Use**	Side of a finger, presenting different finger (e.g. index instead of thumb)
	Cadavers	dead fingerprint
	Altered	Altered fingerprint
	Coercion	Bona fide presentation under coercion

2. 3. 3. Face recognition

Face recognition encounters diverse presentation attacks designed to manipulate the biometric system's decision. Similar to previous modalities, attacking face recognition starts with identifying the target sensor, i.e. 2D or 3D acquisition system. In fact, the human face has a unique 3D geometry and capable of performing physical movements and emotional expressions. Moreover, a man has unconscious facial responses for external events such as eye blinking.

Face recognition security occupies high attention since it has been deployed in many areas such as passport check and video surveillance. Surveys [16], [75], and book chapters [73] have been published to update the threats and solutions for face recognition systems. Table 2.4 classifies potential attacks based on Figure 2.3.

Table 2.4. Presentation attack on face recognition systems.

PAI type		PAI	REFERENCES
Synthetic	**Static partial**	Facial accessories	[76], [77], [78]
	Static complete	full head casting, static mask	
		Printed image	
		Display image	[79]–[82]
	Dynamic Complete	Display video	
		Wearable mask	[83]–[85]
	Dynamic Partial	Artificial and natural facial hair	[78], [86]
Human-based	**Non-Conformant Use**	facial expressions	[87]
	Altered	Plastic surgery, facial makeup	[88], [89], [90], [91]
	Live	Identical twin	[92], [93]
	Coercion	Presentation under coercion	-

2. 3. 4. Vascular recognition

In the 9th GBDe Summit, a study about the security of the embedded black-box system was demonstrated [94], vein biometric systems were investigated, and the possibility of creating artificial traits was discussed as well. This work pointed out the need for further studies and evaluations to understand the deficiencies of vascular biometric systems.

Investigations have started with cooperative attacks, where researchers started performing PAs with the genuine user's cooperation. That is to test the system vulnerability against PAIs. As far as proposed in the literature, the only presentation attack performed on vascular biometric sensors is photo attack [95]–[97].

2. 3. 5. Handwritten signature forgery

Handwritten signature forgery is a behavioral attack that is performed by a forger (i.e. human based), aiming to produce an identical graphical signature and temporal features like speed and pressure. Forging handwritten signatures is influenced by two main factors: the complexity of the signature [98] and proficiency of the imposter [99].

A difficulty index has been proposed in [100] to evaluate a genuine signature vulnerability to imposter's attacks. In fact, the proposed "difficulty index" is completely independent of the quality of the forged sample which is produced by an imposter, and it contributes to measuring the challenge of imitating the genuine signature.

Imposters are classified in literature, depending on their knowledge and ability to forge a signature, into three main types [101]: (a) Random (Simple) forgery: imposter uses the victim name in order to generate a signature without any knowledge about the genuine signature; (b) causal forgery: the forger in this class has observed the genuine signature for a while then an imitation is performed based on the graphical memories of the imposter; (c) skilled forgery: imitating the signature is performed by a professional who has prior knowledge about the genuine sample, and typically trains many times before performing the attack.

2. 3. 6. Automatic speaker recognition

Speech is generally influenced by complex biological, social, and regional factors. Aging, stress, colds, etc. are typical causes of voice variation which bring out more challenges for Automatic Speaker Verification (ASV) algorithms [102], [103]. In case of considering those cases as attacks, they would fit under alternated presentations with no malicious intent.

Literature exposes presentation attacks on ASV as shown in Table 2.5. These attacks are supposed to be performed with malicious intent; i.e. according to Figure 2.5, they are considered as subversive attacks with dynamic PAIs.

Table 2.5. Presentation attack on speaker recognition systems.

PAI type		PAI	REFERENCES
Synthetic	Dynamic Complete	Replay attack	[105]–[110]
		Speech synthesis	[111]–[115]
		Voice conversion	[116]–[123]
Human	Alternations	Voice changes	[102], [103]
	Behavioural	Impersonation	[124]–[127]

2. 4. STATE OF THE ART IN PRESENTATION ATTACK DETECTION

As stated in the previous section, many investigations are being undertaken in order to study presentation attacks seeking to propose detection mechanisms to eliminate or mitigate those attacks. There is a vast amount of literature on presentation attack and presentation attack detection evaluations, which we introduce in this section and link those investigations to the proposed taxonomy.

The following subsections present a literature review about the proposed PAD mechanisms and link them to the proposed taxonomy in Figure 2.5.

2. 4. 1. Mechanisms based on natural biometric phenomena

The PAD mechanisms in this class are basically developed to investigate the influence of the natural biometric phenomena on the acquired presentation. In other words, the PAD mechanism defines additional distinguishing characteristics in the genuine biometric traits seeking to determine whether the presentation is consistent or not with the human characteristics, consequently, reject malicious presentations. For example, the perspiration of fingerprint provides unique dynamic patterns when analyzing the presentation as a sequence of successive frames, deeper details, and analysis for the fingerprint modality are provided in the next chapters.

Table 2.6 lists the proposed PAD mechanisms that consider natural phenomena as distinguishing basis to address the issue of PA.

Table 2.6. PAD mechanisms based on natural characteristics.

Modality	Method	Reference	Hardware\Software
Iris	Dynamic eye response	[36], [39], [107]–[114]	Both
	3D geometry analysis	[36], [107], [115], [116],	HW
Fingerprint	Perspiration analysis	[119]–[123]	SW
	Pores detection	[120]	SW
	Fingerprint coarseness	[121]	SW
Face	Behavioral analysis	[114]–[119]	SW
	3D geometry analysis	[129]–[131]	HW
Vascular	Blood features	[125] [126]	SW
	Motion magnification	[127]	SW
Handwritten signature	Dynamic signature analysis	[20], [21], [128]–[130]	HW

2. 4. 2. Mechanisms based on collateral means

As stated in Section 2, this category includes the mechanisms that exploit secondary information that distinguishes genuine presentations from attacks. The next subsections explain the three sub-classes of this category.

2.4.2.1 Embedded features

This type of feature refers to the secondary attributes that can be exploited in the biometric presentation to distinguish attacks. For example, the quality analysis focuses on the quality of the acquired biometric sample and it assumes that attack instruments provide a different quality than that provided by genuine presentations. Moreover, when texture analysis is used as the PAD features, the algorithms assume in the first place that the texture of attacks differs from the texture of genuine traits then using a data-driven model the algorithm classifies the input presentation as a bona fide or attack presentation.

Table 2.7 shows the different methods which have been investigated in the literature for the different modalities.

Table 2.7. PAD mechanisms based on collateral means.

Modality	Method	Reference	Hardware\Software
Iris	Quality measures	[131]	SW
	Texture analysis	[132], [133] [134]–[138] [107], [139]–[141] [53], [54], [140], [142], [143] [55] [144]	SW
	Light reflection	[145]	SW
	Multi-spectral analysis	[146]–[151]	HW
Fingerprint	Distortion analysis	[152]–[154]	SW
	Quality measures	[155]–[158] [159]–[167]	SW
	Statistical approaches	[168] [169]	SW
	Power spectrum analysis	[170], [171]	SW
	Local phase quantization	[172]–[174]	SW
	Optical coherence tomography	[175], [176]	HW
Face	Facial texture analysis	[177]–[180]	SW
	Quality measures	[139], [181]–[183]	SW
	Context base analysis	[184], [185]	SW
	Statistical approaches	[79], [186], [187]	SW
	Spectral approaches	[124], [188]–[192]	SW
	Light polarization	[193]	HW
Vascular	Texture analysis	[194], [195]	SW
Voice	Voice analysis	[196] [197] [198] [199] [200] [201]–[205] [206]	SW

2.4.2.2 Voluntary challenge response

The biometric system's user is capable of performing simple actions while performing a biometric presentation. Eye and mouth movements, face rotation, or any other conscious response will be classified under this subclass [23], [113], [207], [208].

2.4.2.3 Multimodal systems

Independent biometric modalities might be combined in one biometric system such that different acquisition subsystems are employed to capture the user biometric data [209]. Theoretically, multimodal systems are supposed to provide a high level of security[24]–[26], but nevertheless, various investigations show that a multimodal system is vulnerable to presentation attack [210]–[212].

2. 5. CONCLUSIONS

Many factors impact the generation of efficient artefacts that can defeat the recognition system. The general taxonomy of presentation attacks is proposed in a way that helps to recognize any potential attack. Firstly, the intention of the user (genuine or attacker) is essential. Subversive intents mean to defeat and end up with a successful imposter or concealer try. On the other hand, non-subversive intents are still considered as suspicious presentations, while users are behaving

normally by wearing commercial products for cosmetic purposes, facing accidents which cause problems in engaging with a system, or need more knowledge about the use of these systems.

Considering two major types of modalities: physiological and behavioral modalities, generating artefacts can take different directions. Presentation attacks are performed by creating a spoofing trait that contains static or dynamic information, depending on the recognition system topology, such that the PAI provides an identical pattern to the genuine sample. Additionally, the attacker here focuses on the biometric sensor specifications, the required hardware and software tools, and PAIs creation methodology.

At the same time, behavioral modalities demand the attacker has particular experience for each sample, this involves training on each target sample to get a high-quality spoof. Moreover, the dynamic information should be considered while applying the attack.

As presented in section 3, all modalities have been defeated by presentation attacks. Consequently, the reliability of biometrics as recognition systems is lower. Statistically speaking, evaluation measures of biometric systems security are degraded while considering presentation attacks. Therefore, countermeasures have been developed and embedded in the system to boost the resistance of the system against spoofing attacks.

Literature exposes massive research on PAD mechanisms which have been reclassified in this paper. A novel PAD taxonomy is proposed in Section 2 to categorize the state of the art anti-spoofing methods. The base criteria we adopted to establish the taxonomy is the type of information used in the PAD mechanism. The first class consists of the methods which analyze the natural features of the trait; i.e. features produced because of natural phenomena or any information from within the sample. The second class covers the rest of the solutions which detect collateral information adding extra hardware or software to the system.

PAD hardware based methods require modifications on the sensor in the biometric system, meaning that cooperation from the manufacturers is expected to deploy this type of solution. Meanwhile, the rest of the solutions are proposed following testing of datasets on a biometric sensor without any need to modify the original design of the sensor, which means no additional cost on the overall system. This explains the relatively low quantity of hardware-based solutions compared to software-based solutions.

Chapter 3. Presentation Attack Detection: Evaluation Methodology

Performance evaluation of a PAD mechanism is essential to characterize its technical capabilities such as security and ease-of-use. Although all PAD mechanisms have the same objective, different configuration methods can be implemented to integrate the PAD subsystem in the biometric system. Hence, adequate evaluation methodologies are vital to achieving valid and comparable PAD evaluations. For that reason, different methodologies, such as the standard ISO/IEC 30107 *Information technology - Biometric presentation attack detection* [8], [10], [11], [213] and *Common Methodology for Information Technology Security Evaluation (CEM)* [9] by the Common Criteria, were proposed in the literature providing frameworks and techniques that can be used to assess the performance of PAD mechanisms.

Essentially, PAD evaluation determines the technical competence of a PAD mechanism considering specific attack potential. Therefore, the evaluation should provide enough details and analysis about the assumed attack potential, showing that the obtained technical competence corresponds to the supposed level of threat. In this chapter, we adopt the vulnerability analysis method and the calculation of attack potential following the recommendations of the CEM [9]. On the other hand, the evaluation of PAD technical competence is performed based on the standard ISO/IEC 30107-Part 3: *Testing and reporting* [11]. Figure 3.1 illustrates the corresponding reference at each part of the proposed methodology.

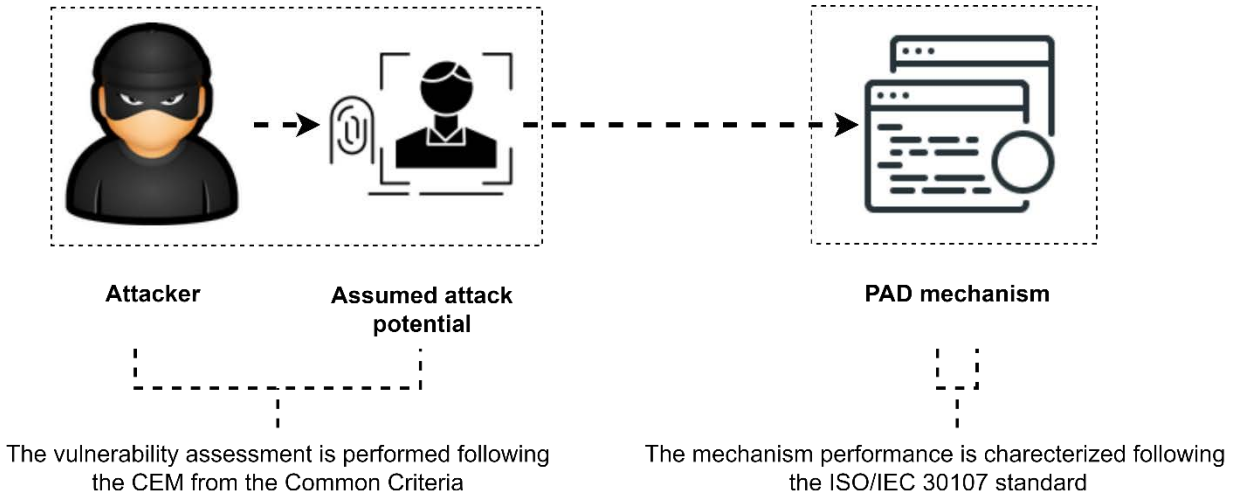


Figure 3.1. The use of existing standards in the proposed methodology.

Most of the current public PAD datasets, such as LivDet databases [214], do not characterize PAs considering the factors influencing the attack potential. For instance, the level of knowledge and expertise of an attacker/s is expected to affect the result from the PAD mechanism [215]. Having

this factor undescribed questions the confidence of the proposed solutions when considering different datasets with significant differences in the attack characteristics.

In this thesis, the evaluation of the proposed PAD mechanisms is not carried out immediately after the data acquisition but offline at a later time. This chapter provides the required framework to perform the evaluations, details the data collection process, and provides a vulnerability assessment for the Target of Evaluation (ToE).

This chapter is primarily concerned with PAD evaluations for fingerprint modality following the directions of the aforementioned methodologies with the following objectives:

- Define the main technical terms;
- explain the PAD evaluation levels;
- performing a vulnerability assessment to determine the existence and exploitability of weaknesses or flaws in the fingerprint recognition system;
- assessing the security of the PAD mechanism by examining its capability to correctly identify presentation attacks;
- evaluating the influence of the PAD mechanism on the biometric system's ease-of-use through analysing the prospect of rejecting bona fide presentations;
- determining the testing plan; and,
- describe the data collection.

The rest of this chapter is organized into two main sections. The first section introduces the theoretical framework for the evaluation by explaining the levels of evaluation, the vulnerability assessment method, and the details of PAD performance evaluation. The second section presents the test plan and the data collection, then performs a vulnerability assessment on the introduced database following the provided framework in Section 1.

3. 1. THEORETICAL FRAMEWORK OF EVALUATION

3. 1. 1. Terminology

The standard ISO/IEC 30107 defines a set of terms to describe the evaluation of PAD mechanisms. In the experiments of this thesis, these terms are used to report the results. The related and most used terms are defined as follows:

- Biometric representation: a presentation of biometric sample or biometric feature set to the biometric sensor. It could be a bona fide or attack presentation.
- Bona fide: analogous to normal or routine, when referring to a bona fide presentation.
- Presentation Attack Instrument (PAI): class of presentation attack instruments created using a common production method. Many studies use the term ‘‘spoof’’, which informally refers to PAI.
- PAI species: class of presentation attack instruments created using a standard production method and based on different biometric characteristics.
- Attack type: element and characteristic of a presentation attack.

- Item Under Test IUT: an implementation that is the object of a test assertion or test case. The equivalent term in the Common Criteria is Target of Evaluation (ToE).
- Attack potential: a measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources, and motivation.
- Attack Presentation Classification Error Rate (APCER): the proportion of attack presentations incorrectly classified as bona fide presentations;
- Bona Fide Presentation Classification Error Rate (BPCER): the proportion of bona fide presentations incorrectly classified as presentation attacks;
- Correct Classification Rate (CCR): The percentage of presentations Correctly Classified; (not defined in the standards, but used in previous studies as a measure of classifier's accuracy)
- Spoofing and anti-spoofing: informal vocabularies which are used in literature instead of presentation attack, and presentation attack detection.

3. 1. 2. Levels of Evaluation

The biometric system is a combination of multiple subsystems that work jointly to provide the final recognition score/decision including the PAD result. Thus, PAD evaluations shall completely describe the ToE, i.e. system or subsystem that is the subject of evaluation, including the details of PAD implementation and the evaluator's attributes.
The standard ISO/IEC 30107-3 categorizes the ToE into the following classes:

I. **PAD subsystem** is the hardware or/and software implementation of a PAD mechanism that provides a score/decision which determines whether a presentation is bona fide or attack.

II. **Data capture subsystem** is the hardware or/and software segment where all presentations take place. The capture process may include quality and PAD checks before acquiring or rejecting a presentation. The evaluator would have access to the capture decision and might obtain further details depending on the acquisition tool provided by the manufacturer. This category of ToE can be evaluated individually to assess the resistance of the biometric system to acquire certain PAI species or by combining it with the PAD subsystem evaluations.

III. **Full biometric system** comprises the complete recognition process starting with data acquisition and ending with the final recognition score/decision. This class of evaluation includes the bias of data capture, matching, and PAD subsystems and should provide statistical measures for the complete system's performance.

All the experiments in this thesis are evaluated considering the PAD subsystem evaluation to keep the focus of evaluation on the proposed mechanisms.

3. 1. 3. Vulnerability Assessment Method

Vulnerability assessment refers to the process of determining exploitable vulnerabilities introduced in the development or operation of ToE [216]. This determination depends on investigating the evaluation evidence and exploring publicly available tools by the evaluator and is assisted by evaluator infiltration testing [9]. In addition to the vulnerability analysis,

vulnerability assessment analyzes the attack potential by exploring different factors that affect the potential of attacks.

3.1.3.1 Vulnerability analysis

The objective of vulnerability analysis is to determine the exploitability of development and operational vulnerabilities of the ToE. In the context of presentation attacks, development vulnerabilities refer to the ToE flaws that were introduced during its development, e.g. unknown presentation attacks. Operational vulnerabilities refer to the flaws and weaknesses of a PAD mechanism.

Vulnerability analysis is conducted through three steps: (1) identifying potential vulnerability, (2) identifying potential attacks, and (3) penetrating testing to demonstrate if the identified potential vulnerabilities are exploitable in the ToE. Note that penetrating testing might lead to identifying new vulnerabilities and/or attacks. Thus, these steps are performed as one vulnerability analysis task.

During the vulnerability analysis of fingerprint sensors, the evaluator seeks to define various PAI species that can be detected and captured by the sensors, this process is defined as the identification phase. Then, the evaluator achieves the attack on another instance using the techniques and analysis defined in the identification phase. Figure 3.2 illustrates the process of analyzing the determined vulnerability as one task.

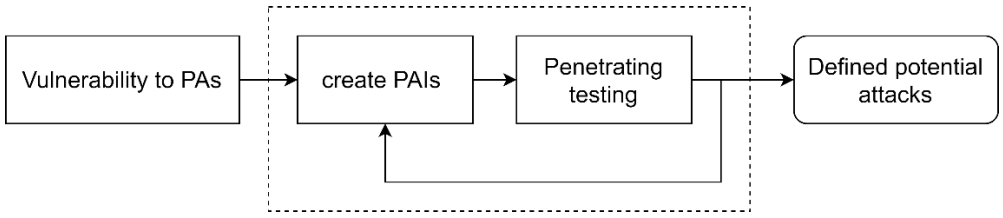


Figure 3.2. Steps of data capture vulnerability analysis.

3.1.3.2 Attack potential

Attack potential is defined as a function of motivation, expertise, and resources. Accordingly, the attack potential corresponds to the required effort to exploit a vulnerability in the ToE through creating an attack and prove that it allows the attacker to violate the security functional requirements.

Attack potential is carried out as a sub-activity during the vulnerability assessment in order to ascertain if the ToE is impervious to attacks under a given attack potential of an attacker. Once a potential vulnerability is reported to be exploitable in a ToE, the evaluator should confirm that it is exploitable taking into account all of the environmental aspects, including the undertaken attack potential. To determine specific attack potential, the following factors should be taken into account:

1. Elapsed time
   Refers to the required time to identify a potential vulnerability, develop an attack, and to sustain the required effort to apply the attack at the TOE. In order to calculate the consumed time in identifying or exploiting a vulnerability the following measures are used: a day = 8 hours; a week = 40 hours; and a month =180 hours.
2. Specialist expertise
   Refers to the level of conventional knowledge on the basic principles, sensor type or attack techniques. There are four levels of attacker expertise:
   a) Layman is unknowledgeable compared to proficient or expert attackers, with no specific expertise;
   b) Proficient is familiar with the security conduct of the biometric system;
   c) Expert is familiar with the biometric algorithms, protocols, sensors, structure, principles and concepts of biometric security, PAD methods, conventional attack types, tack methods, etc.
   d) Multiple-experts level is considered when more than one expert are involved to carry out the attack.
3. Knowledge of the ToE.
   Refers to specific expertise in relation to the biometric PAD solutions. The knowledge is classified in four categories: public information, restricted information, sensitive information, and critical information.
4. The window of opportunity.
   This factor highly depends on the level of supervision over the operation of biometric recognition. In unsupervised environments, the attacker has unlimited access to the ToE and has the opportunity to apply attacks without restrictions.
5. Required hardware and/or software tools.
   Refers to the equipment that is needed to identify and exploit an attack. The following classification is to be used:
   a) Standard equipment is equipment that is available to the attacker and can be obtained from local or online stores.
   b) Specialized equipment isn't promptly accessible to the attacker, however could be procured without excessive effort.
   c) Bespoke equipment isn't promptly accessible to the public as it may need to be specially created, or on the grounds that the equipment is particular to such an extent that its distribution is controlled, potentially even restricted. Instead, the equipment might be very pricey.
   d) Multiple Bespoke level corresponds to the attacks that require different types of bespoke at distinct steps of an attack.

Considering these factors, the attack potential can be calculated by summing the values of all factors as shown in Table 3.1.

Table 3.1. Attack potential calculation [216].

Factor	Value		Factor	Value
Elapsed Time			**Knowledge of TOE**	
<= one day	0		Public	0
<= one week	1		Restricted	3
<= two weeks	2		Sensitive	7
<= one month	4		Critical	11
<= two months	7		**Window of Opportunity**	
<= three months	10		Unnecessary / unlimited access	0
<= four months	13		Easy	1
<= five months	15		Moderate	4
<= six months	17		Difficult	10
> six months	19		None	
Expertise			**Equipment**	
Layman	0		Standard	0
Proficient	3		Specialized	4
Expert	6		Bespoke	7
Multiple experts	8		Multiple bespoke	9

Finally, the obtained attack potential value is used to define the resistance of the ToE to the identified attacks. Figure 3.3 and Table 3.2 shows the steps of the process.

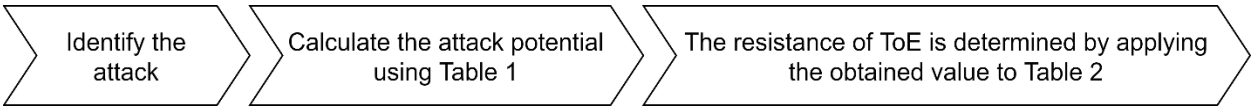


Figure 3.3. Determining the resistance of a ToE to an identified attack.

Table 3.2. Rating of vulnerabilities and TOE resistance.

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:
0-9	Basic	No rating
10-13	Enhanced-basic	Basic
14-19	Moderate	Enhanced-basic
20-24	High	Moderate
=>25	Beyond high	High

3. 1. 4. PAD Technical Competence

As provided in the standard ISO/IEC 30107 *part 3: Testing and reporting*, the goal of PAD subsystem evaluations is to determine the PAD mechanism's ability to correctly classify attacks and bona fide presentations. Nonetheless, PAD subsystems are subject to classification errors, i.e. false positive and false negative. The conducted evaluation should report sufficient description which characterizes the influence of those error rates on the security and ease-of-use attributes of the biometric systems.

3.1.4.1 Security

The security of PAD subsystem is impaired by the false negatives where attack presentations are misclassified as bona fide presentations. Thus, the security of a PAD subsystem is characterized by the metric APCER (Attack Presentation Classification Error Rate) which represents the proportion of misclassified attack as bona fide presentations.

APCER can be analyzed in two manners:

I. Total APCER ($APCER_{Total}$) is used to measure the PAD subsystem security when different PAI species are used to evaluate the system. In this case, all attacks are labelled as an attack. This metric does not demonstrate the strengths and weaknesses of the different PAI species. $APCER_{Total}$ is calculated by:

$$APCER_{Total} = \frac{1}{N} \sum_{i=1}^{N} Res_i \quad 3.1$$

where, N is the total number of attack presentations and Res_i is 1 if the attack i^{th} presentation is classified as bona fide and 0 otherwise.

II. APCER for a given PAI ($APCER_{PAI}$) is used to analyze the strength of a certain PAI species and is calculated by:

$$APCER_{PAI} = \frac{1}{N_{PAI}} \sum_{i=1}^{N_{PAI}} Res_i \quad 3.2$$

where, N_{PAI} is the total number of attack presentations for the given PAI, and Res_i is 1 if the attack i^{th} presentation is classified as bona fide and 0 otherwise.

Along with the APCER measures, the evaluator should report the following details:

- the number of independent capture subjects who participated in the experiment by allowing the attacker to use their biometric characteristics to perform PAs;
- the number of biometric sources given by each capture subject stating the number of taken biometric characteristics;
- the required level of cooperation from the capture subject to collect the biometric source;
- the used PAI species;
- the total number of attack presentations;
- the total number of attack presentations for each PAI species; and,
- the number of attack attempts per each PAI.

3.1.4.2 Ease-of-Use

The PAD subsystem evaluation should report approximate guidance to illustrate the influence of PAD mechanism on the system's ease-of-use. False-positive errors caused by the PAD subsystem have a negative effect on the user experience where bona fide presentations are incorrectly classified as attacks. The proportion of those misclassified bona fide presentation, i.e. BPCER (Bona fide Presentation Classification Error Rate) is calculated by:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_{BF}} \quad 3.3$$

where N_{BF} is the total number of bona fide presentations and Res_i is 1 if the i[th] presentation is classified as attack and 0 otherwise.
In a similar manner with APCER reporting, the BPCER testing should refer to:

- the number of independent capture subjects who donated their biometric characteristics;
- the corresponding biometric traits for each capture subject;
- the total number of bona fide presentations; and
- if more than one visit was needed, the evaluation should specify the duration between the visits and report any differences in the acquisition environment.

3.1.4.3 PAD Subsystem Accuracy: Security vs. Ease-of-Use

There are a wide variety of techniques to report the PAD subsystem accuracy. The choice of reporting PAD accuracy is crucial to provide comparable results that would help to contrast one mechanism with another or to make a comparison with the SoA investigations. The following subsections explain the used techniques in the context of this thesis.

3.1.4.3.1 Reporting BPCER at Fixed APCER Value

The PAD subsystem accuracy can be determined in a single figure as BPCER at a fixed APCER. This allows determining the ease-of-use measures at certain levels of security making the comparison between different mechanisms more evident and accurate. For example, BPCER can be computed when APCER=5% and then reported as BPCER20. The opposite is also valid where APCER can be calculated at fixed levels of BPCER.

3.1.4.3.2 Detection Error Tradeoff (DET) Curve

The DET curve [217] is a graphical representation for APCER versus BPCER. This representation describes the trade-off between security and ease-of-use, and helps to define a decision threshold that suits the security/ease-of-use requirements.

3.1.4.3.3 Tradeoff Equal Error Rate (TEER)

The conventional EER measure has been used in the evaluations of biometric systems performance. However, early investigations in PAD were conducted before proposing the PAD evaluation methodologies, and for that reason, many works in the literature reported the PAD subsystem accuracy in terms of EER. To dismiss the confusion between biometric performance

and PAD performance, we define the measure TEER as the point where APCER and BPCER equalize.

The usage of TEER is not recommended since it reports the accuracy of different mechanisms at different levels of security/ ease-of-use. The motivation to report the TEER in this study is to compare the accuracy of the proposed mechanisms with the SoA investigations.

3. 2. THE DATABASE

As stated in Chapter 1, this thesis was undertaken in order to investigate the dynamic fingerprint characteristics as the PAD features. These dynamic characteristics are caused by the behavioural placement of the fingertip on the sensor surface, and the natural characteristics of the presented fingerprint or PAI during a short period of time. However, studying those characteristics requires a database of fingerprint videos.

This section introduces the details of collecting the dynamic fingerprint database that is used to validate the proposed PAD mechanisms in this thesis. The data collection was carried out by modifying the sensors' acquisition mode so that the sensors capture a sequence of frames for the fingerprint presentation instead of capturing a single image.

The following subsections detail the test plan, data collection, and the corresponding vulnerability assessment.

3. 2. 1. Test Plan

For the initiation of PAD testing process, the primary step is to define the test target including the biometric modality, sensing technology, operational scenarios, and the ToE. Afterward, the required data to perform the testing should be determined. With the completion of these steps, the required resources (e.g. participants, hardware, software) are characterized.

3.2.1.1 Test Targets

This thesis investigates the vulnerability of fingerprint modality to direct attacks. The investigation seeks to analyze the biometric system vulnerability at two levels: data capture subsystem and PAD subsystem levels. The data capture subsystem is assumed to be compromised once the evaluator define the successful attack species (Figure 3.2), then the captured data is studied at a later stage to determine the PAD accuracy. The data collection is carried out using optical and thermal sensing technologies seeking to define the influence of each technology on the performance of different PAD mechanisms. The differences between the sensing technologies are presented later within the database characteristics.

As the data collection is carried out prior to the development of the PAD mechanisms, an evaluation of offline PAD mechanisms is performed. The evaluation of PAD mechanisms is

conducted on the level of PAD subsystem, that is to characterize the mechanisms' capabilities and weaknesses against different attack species.

3.2.1.2 What Data Needs to be Collected

A major observation on recent investigations is the focus on developing static PAD algorithms using benchmarks. However, less effort is invested in developing evaluations that are intended to investigate natural fingerprint phenomena. In our opinion, developing PAD mechanisms relies equally on (i) the characteristics of used datasets, and (ii) the detection algorithm. Thus, focusing on both components leads to a more coherent and interpretable evaluation.

Consequently, a dynamic database of bona fide and attack presentations is a necessity. At the time of performing this thesis, there is no publicly available database with the requirements stated above. Therefore, dynamic data collection is conducted covering bona fide presentations and cooperative attacks using different PAI species. The selection of PAI species covers different physical characteristics such as flexibility. Furthermore, the data is collected in two different operational scenarios: (1) performing ordinary fingerprint presentations, (2) performing fingerprint presentations with pressure. The database is characterized in detail in the following section.

3. 2. 2. Data Collection

In this section, we introduce a dynamic database that is intended to extend the SoA investigations on dynamic fingerprint features, also to study the fingerprint's dynamic-reaction to pressure. The database (Table 3.3) is composed of 7128 fingerprint videos, corresponds to bona fide and attack presentations, collected from 66 statistically independent fingerprints of eleven separate capture subjects. The database is divided into two subsets. The first subset consists of dynamic presentations that represent ordinary presentations. In contrast, the second subset is collected with an instructed acquisition, whereas the capture subjects were demanded to apply pressure during the fingerprint presentation.

Table 3.3. Generic description of the database.

Participants	11 capture subjects
Number of fingerprints	66 fingerprints
acquisition scenarios	1. Ordinary presentations 2. Presentations with pressure
Presentation types	1. Bona fide 2. cooperative attacks
Total acquired videos	7128

3.2.2.1 Required Resources

This section defines the required resources as follows:

- Optical and thermal fingerprint sensors. Those sensors were chosen due to the significant differences in the characteristics of acquired data, which will lead to identifying the influence of sensing technology on the PAD mechanisms;
- developing a GUI to interact with the sensors keeping in mind fingerprint video acquisition as a requirement;
- participants to perform bona fide presentations and to provide molds of their fingerprints;
- an attacker to use the collected molds to create PAIs and perform attacks; and,
- materials to create different PAI species.

3.2.2.2 The Database

The proposed dynamic database contains uncompressed fingerprint videos of bona fide and attack presentations. Data acquisition, storage, and management were carried out through a systematic study following the General Data Protection Regulation (GDPR) directive. The experiment was approved by the ethics advisor of AMBER project and the data protection officer at UC3M. Next, an invitation to participate was sent to a group of university students and staff members. Eleven participants volunteered to donate their biometric characteristics and gave written informed consent.

Data were collected from genuine fingerprints and seven PAI species using two commercial fingerprint sensors. Since the sensors do not support a video acquisition mode, a customized acquisition tool, Figure 3.4, is developed using the sensors' SDKs in order to capture the sequence of frames (Video) instead of acquiring a single image. The acquisition tool is implemented to attach the following information to the acquired videos: bona fide tag, attacker tag, presentation type, visit/session, PAI species, finger tag, and attempt. As per the GDPR principles, the labels on the biometric data do not include any biographical data or any part of it.

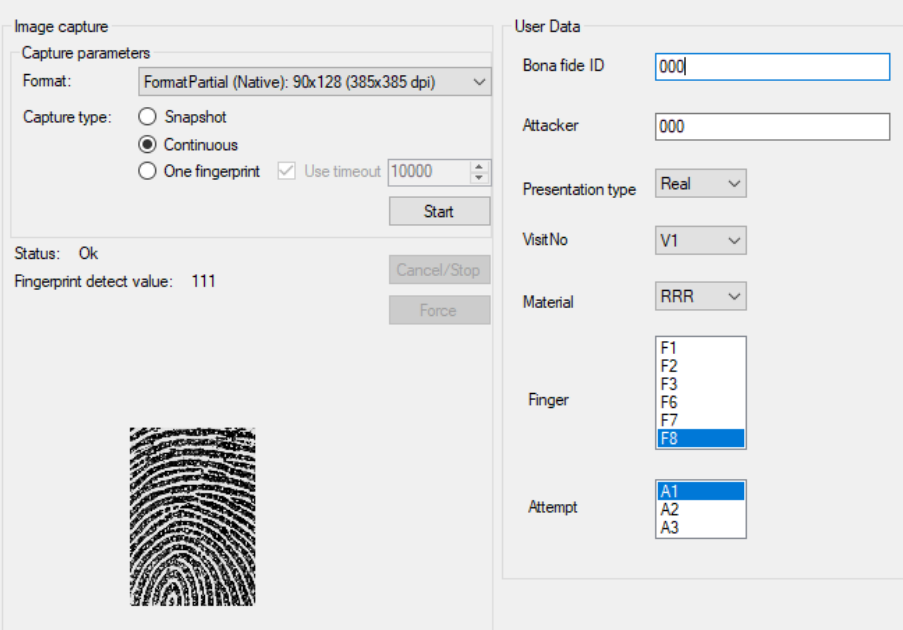


Figure 3.4. GUI implementation to capture fingerprint videos.

The database is illustrated in Figure 3.5 and explained in detail as follow:

Participants

Eleven capture subjects, four females and seven males, have participated in the data collection. Each subject donated his/her biometric samples from 6 fingers: thumb, index, and middle of both hands. With this in mind, we ended up with a total of 66 statistically independent fingerprints.

Scenarios

Initially, the participants were given a brief overview of the typical use cases of fingerprint sensors. They then were asked to present their fingerprints to the sensors, knowing that each sensor acquires the complete placement over its surface as a video. The presentations were collected assuming two different operational scenarios: (1) ordinary presentations and (2) presentations with additional pressure on the sensor's surface.

Sensors

Two sensing technologies with different capabilities are utilized to collect the data. The sensors produce different characteristics for the captured videos due to their distinctions in Table 3.4.

Table 3.4. Comparison of the used sensors in the data collection.

Sensing technology	Resolution	Surface size	Image size	Gray levels	Scan time	Presentation length
Optical	500 ppi	900 x 900 pixels	900 x 900 pixels	256	0.05 second/image	from the moment of detection until finger removal
Thermal	385 ppi	180 x 256 pixels	90 x 128 pixels	256	0.7 second/image	7 frames/presentation

Bona fide visits

Capture subjects were required to fulfill two visits, at least two weeks apart, to donate their fingerprint characteristics. The visits are conducted as illustrated in Table 3.5.

Table 3.5. Summary of the bona fide visits.

Visit	Scenario	Sensor	Fingers	Attempts per finger	Total bona fide presentations
Visit 1	Ordinary	Optical	Both hands (thumb, index,and middle)	3	3 attempts × 6 fingers × 2 sensors × 2 scenarios × 2 visits ×11 subjects = 1584
		Thermal			
	Pressure	Optical			
		Thermal			
Visit 2	Ordinary	Optical			
		Thermal			
	Pressure	Optical			
		Thermal			

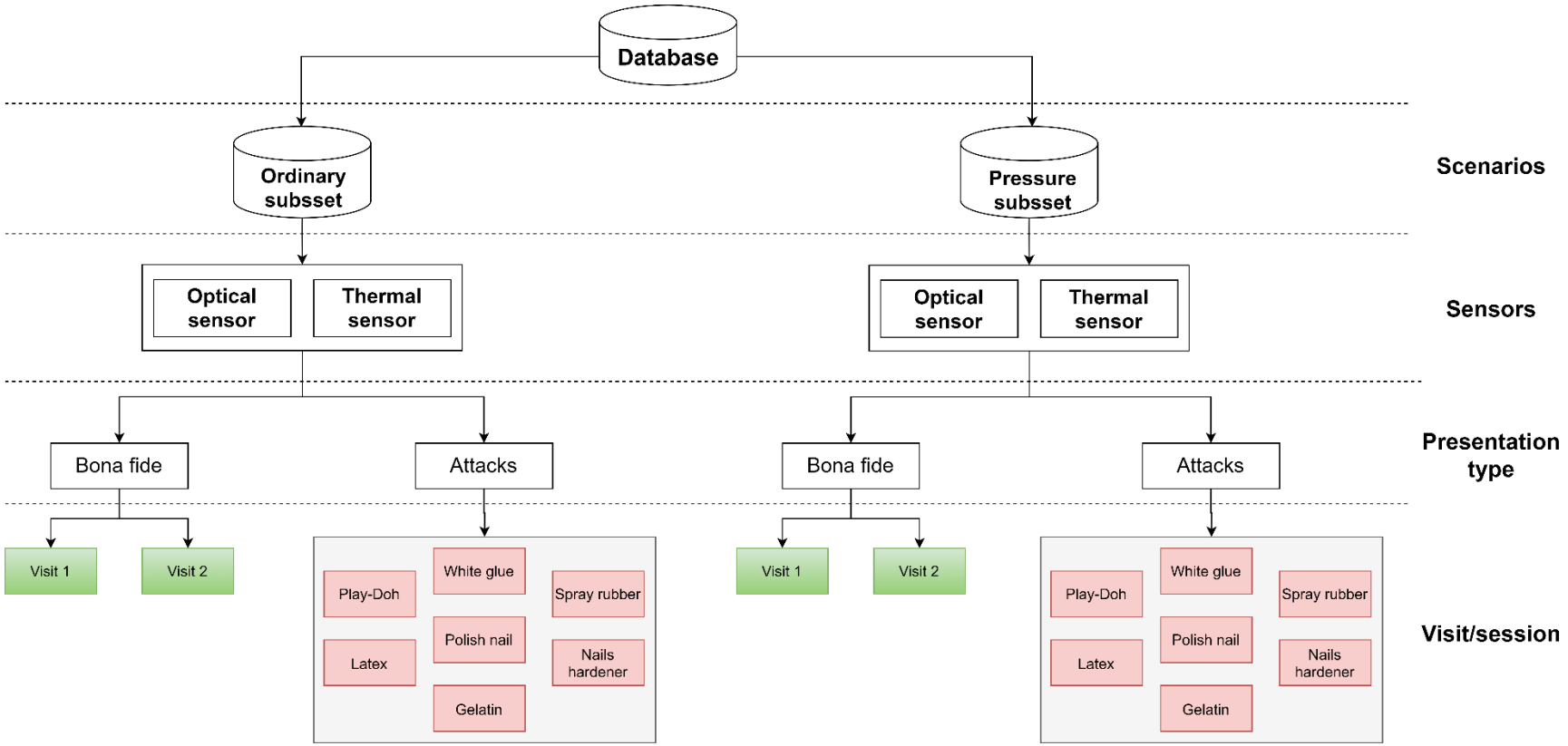


Figure 3.5. Database characteristics.

Attacker

The task of performing PAs is assigned to one attacker. The attacker has extensive knowledge about fingerprint sensors, fingerprint security, and presentation attacks. The attacker has participated in an experiment to attack fingerprint sensors in mobile devices [218]. The details of the experiment are provided in Annex 1. Moreover, the attacker had tested different PAI species on the thermal and optical sensors as training before conducting the formal investigation.

Based on those bases, following the discussion on Section 3.1.3.2, the attacker is classified as an expert.

Attacks

The attacks are conducted in cooperation with the subjects. 3-D silicon molds were collected from the selected 66 fingerprints. Only one mold was collected from each fingerprint. Accordingly, the attacker performed attack presentations using seven PAI species, specifically: Play-Doh, white glue, spray rubber, nail polish, nail hardener, gelatin, and latex. Table 3.6 lists the details of the attacks following the recommendations of ISO/IEC 30107-3.

Table 3.6. Summary of attack sessions.

Molds	66
PAI species	7
Attempts per PAI species	3
PAI series	- For all materials except Play-Doh: 1 PAI per source. Total = 66 PAI × 7 species = 462. - Play-Doh: 1 PAI per attack. Total = 3 attempts × 66 molds × 2 sensors × 2 scenarios = 792.
Total attacks per (scenario, sensor, and species)	198
Total attacks	3 attempts × 6 fingers × 2 sensors × 2 scenarios × 7 species ×11 subjects = 5544

3.2.2.3 Vulnerability Assessment: Fixed Attack Potential

As explained in Chapter 1, the biometric system is proven to be vulnerable to presentation attacks at the sensor level. The evaluator seeks to exploit the vulnerability by defining various PAI species that can be detected and captured by the fingerprint sensors.

Vulnerability Analysis

Following the steps in Section 3.1.3.1, the evaluator defined the vulnerability at the surface of the fingerprint sensor. Then, the potential attacks were defined following two steps: creating testing PAIs from different materials and select the species that can be detected by the sensors.

The process of analyzing the defined vulnerability is illustrated in Figure 3.2.

Attack Potential

The assumed attack potential is characterized in Table 3.7. Following the rating of vulnerabilities and ToE resistance provided by the CC, the required attack potential to exploit the data capture subsystem's vulnerability for the investigated sensors is basic.

Table 3.7. Calculation of attack potential.

Factor	Description	Value
Elapsed Time	Less than one week	1
Expertise	Expert	6
Knowledge of ToE	Public	0
Window of opportunity	Unlimited access	0
Equipment	Standard	0
Total		**7**

The elapsed time is calculated considering the seven PAI species; defined in Figure 3.5. The evaluator reported the effectiveness of all the species to perform successful attacks within seven days. The evaluator gained expertise in previous experiments to attack fingerprint sensors embedded in smartphones [219]. At the moment of performing the attacks, the evaluator had only access to the public information about the ToE. Since the environment is assumed to be unsupervised, the evaluator obtained unlimited access to perform the attacks. Finally, All the used equipment in this experiment were purchased from online shops, local shops, and supermarkets; thus, the equipment is reported as standard.

The following chapters conduct several experiments proposing fingerprint PAD mechanisms. The mechanisms are assessed using the proposed database and evaluation methodology in this chapter.

Chapter 4. Dynamic Fingerprint Statistics: Application in Presentation Attack Detection

Fingerprint is typically perceived as the static pattern of the fingertip's impression. Basically, fingerprint recognition algorithms process the acquired fingerprint image by extracting distinctive features, such as minutia, and compare them to the stored template. In this context, the attacker tries to create a PAI that can make a clear fingerprint impression on the sensor's surface, hence, achieving high similarity score that allows him to access the system. As explained in Chapter 2, different studies attempt to provide static PAD mechanisms based on the extracted features from a single image. Although some of those studies achieved high accuracy, the risk of attack presentations remains high when considering expert attackers who can produce attacks of high quality fingerprint impressions [215].

In addition to the distinct pattern of ridges and valleys, i.e. the static pattern, genuine fingerprints comprise natural phenomena like elasticity, perspiration, temperature, etc. These phenomena influence the dynamic signal, i.e. fingerprint video, which is captured during the fingerprint presentation. Therefore, real presentations are expected to differ from attacks when an appropriate set of dynamic features is defined and extracted. The proposed PAD mechanism extracts the variation of first order statistics in the video, i.e. images sequence, of a fingerprint presentation. Different machine learning classifiers are used for the purpose of declaring the presentation type.

The rest of this chapter is organized as follows. Section 1 details the adopted method by explaining the feature extraction and classification processes. Section 2 explains the used data, data preparation, and the evaluation protocol. The experimental results are provided in Section 3. Finally, conclusions are drawn in section 4.

4. 1. RELATED WORK

Existing dynamic PAD mechanisms can be categorized into two main classes: perspiration based and ridge distortion based mechanisms. Perspiration based mechanisms rely on the fact that genuine fingerprints naturally produce moisture from the pores, this moisture diffuses during the interaction with the sensor surface resulting in a darker image as time goes by. On the other hand, ridge distortion mechanisms base on the claim that bona fide and attack presentations produce significantly different distortions under certain presentation circumstances such as pressure [6]. Table 4.1 conducts a PAD performance analysis for literature researches on both categories and shows the used sensors and attack species.

Table 4.1. Performance of state of the art dynamic PAD mechanisms.

PAD mechanism	Dynamic Analysis	Technique	PAI species	Sensor	Error rates
Antonelli [152]	Distortion	Optical Flow	Gelatin, RTV silicon, white glue, latex	Optical	EER = 11.24%
Zhang [154]	Distortion	Thin-Plate Spline	Silicon	Optical	EER = 4.5%
Jia [153]	Distortion	Statistics	Gelatin	Capacitive	EER = 4.78%
Derakhshani [222]	Persperation	Fourier	Play-Doh, Cadaver	Capacitive	EER = 11.11%
Parthasaradhi [223]	Persperation	Statistics; Fourier	Play-Doh, Cadaver	Capacitive	APCER= 5% - 20%, BPCER= 6.77% - 20%
				Optical	APCER= 4.6%-14.3, BPCER= 0% - 26.9%
				Electro-Optical	APCER= 0%-19%, BPCER= 6.9% - 38.5%
Abhyankar [119]	Persperation	Wavelet	Play-Doh, Cadaver, gummy	Optical, electro-optical, capasitive	EER = 13.85%
Plesh [224]	Persperation	Color analysis	Play-Doh, ecoflex, gelatin, dragonskin, ModelMagic, SillyPutty, wood glue, latex, printed paper, transparent film	Optical	APCER= 0.2%, BPCER= 13.8% - 18.35%

4. 1. 1. DISTORTION'S DYNAMIC ANALYSIS

Preliminary work in fingerprint plastic distortion was carried out in the early 2000s to cope with non-linear deformations of dynamic fingerprint acquisitions [220]. Then, a systematic study on skin distortion was conducted demonstrating that genuine fingerprints produce higher distortion when compared to fake fingerprints [221]. The used dataset was collected using an optical sensor (high frame rate), with user instructions on how to present the fingerprint with rotation and pressure. For each presentation, the method computes the optical flow, Distortion map and distortion code consecutively, afterward compares the distortion codes to detect attacks.

In [154] the authors analyzed the fingerprint deformation and modeled the distortion of genuine fingerprints and attacks using a thin plate spline (TPS). The tested dataset was collected as following: fingerprint presentation is performed by presenting the finger to the sensor then pressure should be applied in different directions. The authors underline that attack instruments are more rigid when compared to the genuine fingerprint's elasticity, thus the deformation of attacks is lower when the same presentation conditions apply. Under those circumstances, the minutia movement represents the global distortion, and a sequence of paired minutia before and after distortion is used to calculate the parameters of the TPS model. The bending energy vector of the TLS model is utilized to distinguish bona fide and attack presentations.

Skin elasticity was analyzed under the assumption that the sequence of genuine fingerprint contains an increasing size of the fingerprint pattern and a higher intensity [153]. The evaluation was reported using a dynamic dataset that was collected by a high frame rate capacitive sensor, while only a gelatin attack was performed. Based on those specifications, the mechanism extracts (a) the correlation coefficient of the fingerprint area and the signal intensity, and (b) the standard deviation of the fingerprint area extension in x and y axes. Finally, Fisher linear discriminant analysis is used to classify bona fide and attack presentations.

4. 1. 2. PERSPIRATION'S DYNAMIC ANALYSIS

Perspiration is a natural distinctive phenomenon in human skin that is affected by physical, psychological and environmental factors. When a fingerprint contacts any surface, the finger's sweat glands start releasing moisture that diffuses along the ridges in time. Therefore, it had been suggested that a fingerprint dynamic acquisition is capable of detecting the consequence of perspiration, by analyzing the sequence of fingerprint images.

Initial work was undertaken to study the perspiration pattern in genuine fingerprints [222]. A dataset of genuine, cadaver and artificial fingerprints was collected via a capacitive scanner to evaluate the proposed algorithm. Two successive images, five seconds apart, were used to extract: (a) four dynamic features that describe the general swing, i.e. local maximum minus local minimum, and (b) a static feature that represent the energy for the first image. It was observed that the swing is generally higher in genuine fingerprints when compared to the attacks, furthermore, the energy of the first image is significantly high in genuine fingerprints in comparison with the attacks. Finally, classification is done using a back propagation neural network. The experiment was extended to cover electro-optical and optical sensors, furthermore, to address the extreme cases of dry and moisturized fingerprints [223].

Another proposition was to isolate the changing energy of the perspiration pattern and use the energy distribution of changing coefficients to classify bona fide presentations from attacks [119]. A dataset of genuine, cadaver and artificial fingerprints were collected by capacitive, electro-optical and optical sensors. At each presentation two images, two seconds apart, were captured. The authors reported the contributions of this work over their previous work in [222], to be: Using a larger dataset, the algorithm requires only 2 seconds between the two successive frames instead of 5 seconds, and the algorithm is integrated with the verifinger SDK [225].

A more recent mechanism has proposed to utilize a color dynamic acquisition in order to analyze the dynamics of bona fide and attack presentations; ten different materials used for producing PAIs [224]. The algorithm analyzes two images, 0.625 second apart, by extracting five dynamic and 2 static features sets. The dynamic features were defined to represent intensity variation, displacement, perspiration, foreground and background analysis. Finally, a deep neural network is used to classify the presentation.

4. 2. FINGERPRINT DYNAMIC STATISTICS

This section focuses on analyzing the complete interaction between the fingerprint and the sensor surface rather than analyzing a single fingerprint image. The study is performed by analyzing the fingerprint presentation as a sequence of frames, wherein each frame is characterized by its global features. The fingerprint presentation is then described by the variation of the global features in its frames. Finally, the obtained description is prepared and utilized to train and test different machine learning classification models, as shown in Figure 4.1. The obtained models are examined in the results section showing the technical capabilities of the proposed PAD mechanism.

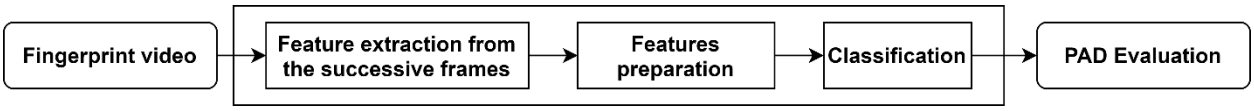


Figure 4.1. The proposed PAD scheme.

4. 2. 1. FEATURE EXTRACTOR

The selected features in the PAD feature extractor are the dynamic *mean, entropy, standard deviation, median, energy, skewness, kurtosis, and coefficient of variation*. The following formula is used to extract the features from each presentation (Figure 4.2):

$$(F_n)_{n=1}^{L}, \qquad F_n = features(n), \qquad n \in [1,2,\dots,L] \tag{4.1}$$

Where, $(F_n)_{n=1}^{L}$ is the features vector which describes *L* successive frames, *n* is the image number in the sequence, and *L* presents the last image. "*features"* is a vector of 8 elements, whereas each element corresponds to one of the measures in equations (2-9).

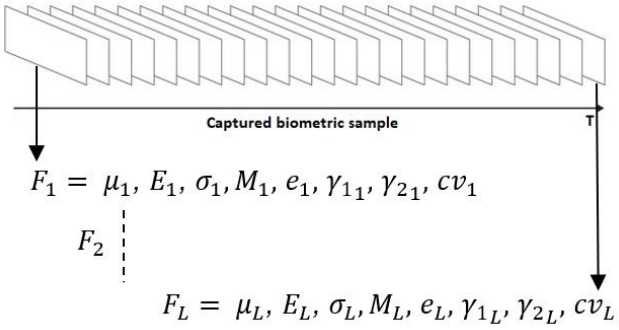


Figure 4.2. Dynamic video statistics.

- Mean

$$\mu = \frac{1}{N}\sum_{n=0}^{N-1} H(n) \tag{4.2}$$

- Entropy

$$E = -\sum_{n=0}^{N-1} H(n)\ log\, H(n) \quad (4.3)$$

- Standard deviation

$$\sigma = \sum_{n=0}^{N} (n-\mu)^2\, H(n) \quad (4.4)$$

- Median

$$M = arg\, \min_{a} \sum_{n} H(n)\, |n-a| \quad (4.5)$$

- Energy

$$e = \sum_{n=0}^{N-1} H(n)^2 \quad (4.6)$$

- Skewness

$$\gamma_1 = \frac{1}{\sigma^3} \sum_{n=0}^{N} (n-\mu)^3\, H(n) \quad (4.7)$$

- Kurtosis

$$\gamma_2 = \frac{1}{\sigma^4} \sum_{n=0}^{N} (n-\mu)^4\, H(n) \quad (4.8)$$

- Coefficient of variation

$$cv = \frac{\sigma}{\mu} \quad (4.9)$$

Where *H(n)* is the frame's histogram and *N* is the number of histogram bins.

4. 2. 2. CLASSIFICATION

Choosing the machine learning algorithm for the classification model is not straight forward and depends on many factors such as type of data, accuracy, classification algorithm complexity, etc. As a result, different classification algorithms are tested to determine the method with the best generalizability. The following classifiers are investigated in this chapter: (a) Linear Discriminant Analysis, (b) Support Vector Machine (second degree polynomial kernel SVM), and (c) Ensemble Learning method (RUSBoosted trees). These classifiers were selected after examining seven

machine learning algorithms with different configuration modes, as shown in Table 4.2. The selection process was basically conducted based on the algorithms' performance. The table shows the classification performance based on the optimal threshold that was obtained by each algorithm considering 50% partitioning for training and testing. The PAD subsystems evaluation is determined in the results section showing the DET curves and different partitioning sizes for a wider comparison.

Table 4.2. Classification accuracy of different machine learning methods.

Machine learning algorithm	Configuration	Accuracy	
		Optical	Thermal
Tree	Fine tree	80.0%	84.9%
	Medium tree	83.5%	84.5%
	Coarse tree	83.3%	82.9%
Discriminant Analysis	**Linear discriminant**	**84.0%**	**89.5%**
	Quadratic discriminant	77.8%	88.2%
Logistic regression	Logistic regression	79.3%	88.8%
Naive bayes	Gaussian naive bayes	56.3%	77.3%
	Kernel naive bayes	78.2%	81.2%
SVM	Linear SVM	87.5%	88.0%
	Quadratic SVM	**91.5%**	**91.1%**
	Fine gaussian SVM	79.0%	88.2%
	Medium gaussian SVM	90.6%	87.1%
	Coarse gaussian SVM	77.9%	78.3%
KNN	Fine KNN	80.8%	87.8%
	Medium KNN	85.4%	87.1%
	Coarse KNN	80.1%	82.2%
	Cosine KNN	85.9%	87.0%
	Cubic KNN	85.2%	86.2%
	Weighted KNN	86.9%	89.0%
Ensemble	**RUSBoosted trees**	**83.8%**	**85.6%**

4. 3. EXPERIMENT SETUP

To evaluate the proposed PAD mechanism, the portion of ordinary presentations in the introduced database (Chapter 3) is used. This portion includes bona and attack presentations that were acquired by different sensing technologies allowing us to analyze the impact of attack species and

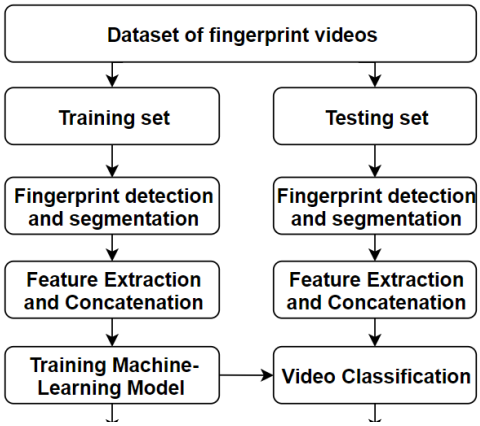


Figure 4.3. Presentation attack detection subsystem.

technologies on the PAD subsystem accuracy. Figure 4.3 demonstrates the scheme of attack detection subsystem.

4. 3. 1. SENSORS

Within the framework of this experiment, this subsection summarizes the differences between the data acquired by each sensor. The frame rate difference, caused by scanning time, results in two different acquisition methods. Fixed-length videos were captured by the thermal sensor (7 frames per presentation), while in the case of the optical sensor, the dynamic acquisition starts when the finger contacts the sensor and stops when the finger is removed, which results in different lengths of interaction between subjects and the sensor.

4. 3. 2. DATA BASE

In order to validate the proposed mechanism, the first scenario, i.e. ordinary dynamic presentations, from Chapter 3 is used.

4. 3. 3. FINGERPRINT DETECTION AND VIDEO SEGMENTATION

Fingerprint detection is carried out in the software acquisition tool using the SDKs implementations for both sensors. Therefore, empty frames before or after the fingerprint placement are taken away.

Segmentation is executed differently in each sensor subset due to the different sensor sizes. (a) Thermal sensor data is segmented during the acquisition such that only the central area (90×128 pixels) is captured. Partial capture has been performed as per the sensor instructions to reduce the frame acquisition time from 1 second to 0.7 second. (b) Optical sensor data segmentation is implemented to consider the sensor's surface area where the fingerprint interaction had taken place. Figure 4.4 and Figure 4.5 demonstrate samples from both sensors for bona fide and attack presentations.

Figure 4.4. Optical sensor captures. For reasons of space, this figure shows partial examples of bona fide and attack presentations (The average number of frames/presentation is 25).

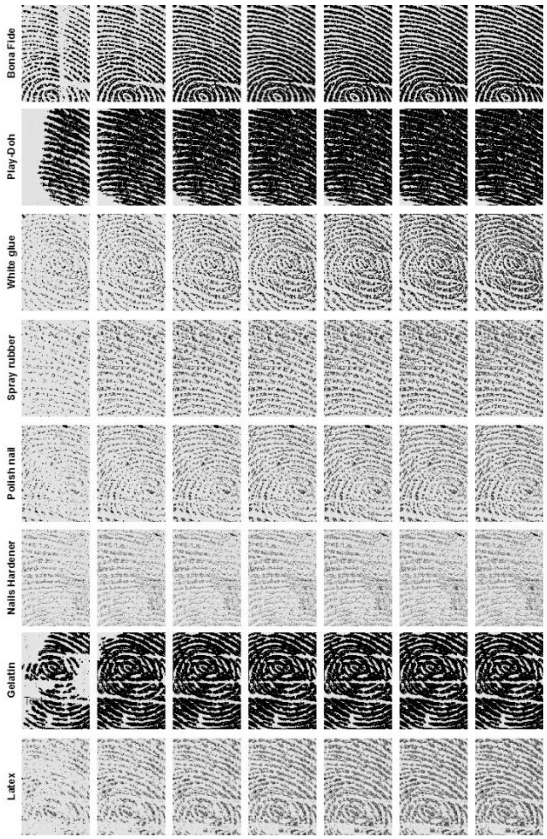


Figure 4.5. Thermal sensor captures. (Each row shows a presentation type in successive frames of a video).

4. 3. 4. FEATURE EXTRACTION AND CONCATENATION

As demonstrated in the previous section, feature extraction is performed on the segmented dataset, consequently, $8\times L$ feature dimensions represent each fingerprint presentation. Since L is fixed to 7 frames for the thermal sensor subset, then the corresponding dimensionality is fixed to 56 for all presentations. Contrariwise, presentations in the optical sensor subset differ in length (i.e. L differ in the various presentations), resulting in $8\times L$ feature dimension per presentation.

Standard machine learning algorithms do not cope with the variation of dimensionality in different samples; thus, it is necessary to transform the dimensionality of the features for all presentations so that they fit into the learning model. The following steps are followed to transform features into a fixed dimensionality size trying to preserve the behavior of the feature using linear interpolation\decimation:

First, feature extraction is executed for every presentation. Second, the number of frames per presentation is averaged across all presentations and it is found to be roughly 25 frames. Third, presentations that have less, or more than 25 frames were subject to interpolate, decimate the dimensionality of the features into $8\times 25 points$. Linear interpolation/ decimation is performed as demonstrated in Figure 4.6 and Figure 4.7. Finally, all features are concatenated such as each presentation is presented by 200 dimensions.

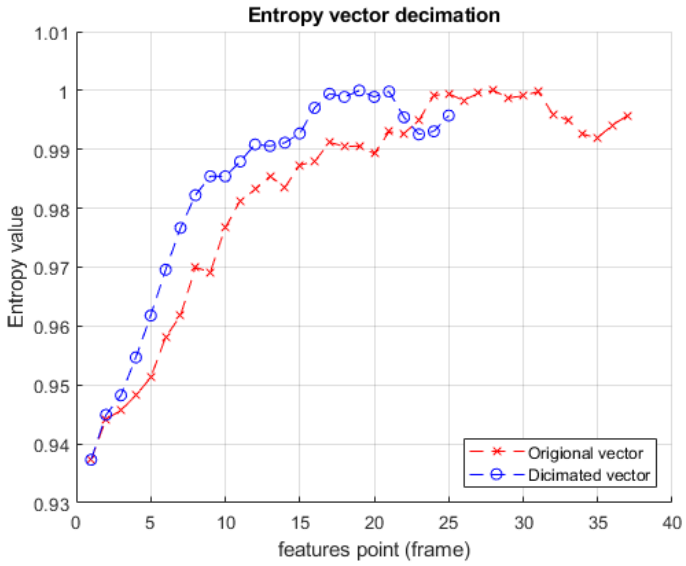


Figure 4.6. Decimating normalized entropy of a 37 frames bona fide presentation (the presentation's length is approximately 2 seconds).

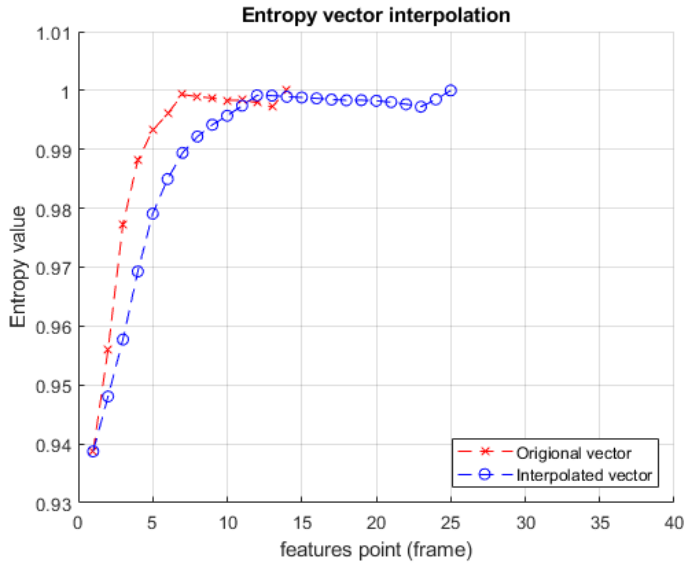


Figure 4.7. Interpolating normalized entropy of a 14 frames bona fide presentation (the presentation's length is approximately 1 second).

4. 3. 5. PAD EVALUATION PROTOCOL

In order to evaluate the proposed mechanism on the collected dataset, each sensor's data is studied apart. We believe that for each commercial fingerprint sensor there must be an independent trained PAD model, given that each sensor captures different images' signal type, noise\s, and resolution. Equally important, for preserving all the details of the captured videos, the preprocessing before extracting PAD features has not been taken into account. For example, noise removal, contrast enhancement, and image filtering algorithms of the original image, which represent the interaction between a fingerprint\PAI and the sensor, may result in a loss of discriminative features.

In the context of this chapter, the PAD subsystem evaluation measures the ability of a PAD model to correctly determine whether a fingerprint video comes from a genuine user or an attack. The evaluation is conducted following the provided framework in Chapter 3.

The evaluator has defined the non-response as no appearance of a fingerprint in successive frames of a bona fide or attack presentation. Despite that, all presentations were successfully captured by the sensors and, consequently, non-response error rates are reported to be 0.

4. 4. PAD EVALUATION RESULTS

The proposed PAD subsystem evaluation is characterized by positive and negative error rates, $APCER_{total}$ and BPCER, as defined in Chapter 3. Both metrics have been calculated for three classification algorithms, each sensor apart. For reliable results, only testing data is used to conduct the evaluation, i.e. training data is merely used to train the models. For more robust accuracy estimation, k-fold cross validation is performed using 2, 3, 5 and 10 folds by the classification algorithms as demonstrated in Figure 4.8 and Figure 4.9. Moreover, Table 4.3 and Table 4.4 report

BPCER values at a fixed $APCER_{total}$ =0.05 and when the equal error occurs i.e. when $APCER_{total}$ =BPCER.

The figures are revealing in several ways. First, classification methods show a difference in the performances. Linear discriminant analysis and SVM methods show high contrast between a low $APCER_{total}$ and a relatively high BPCER, while in the ensemble learning method the contrast between $APCER_{total}$ and BPCER is less notable. Secondly, the number of folds does not influence the methods' performance significantly. For instance, 2 and 10 folds (consecutively 50% and 10% of the dataset) represent different sizes of the testing set, but surprisingly, the error rates are nearly the same. This might be caused by the small size of the dataset. Thirdly, the PAD mechanism shows a resemblance between the performances when considering different sensing technologies.

From Figure 4.8-a and Figure 4.9-a, we observe that at the tradeoff equal error rate, our method achieves 89% accuracy for the thermal sensor and 88.3% for the optical sensors. These results validate our underlying supposition about the statistical differences between attacks and genuine fingerprints in the dynamic scenario.

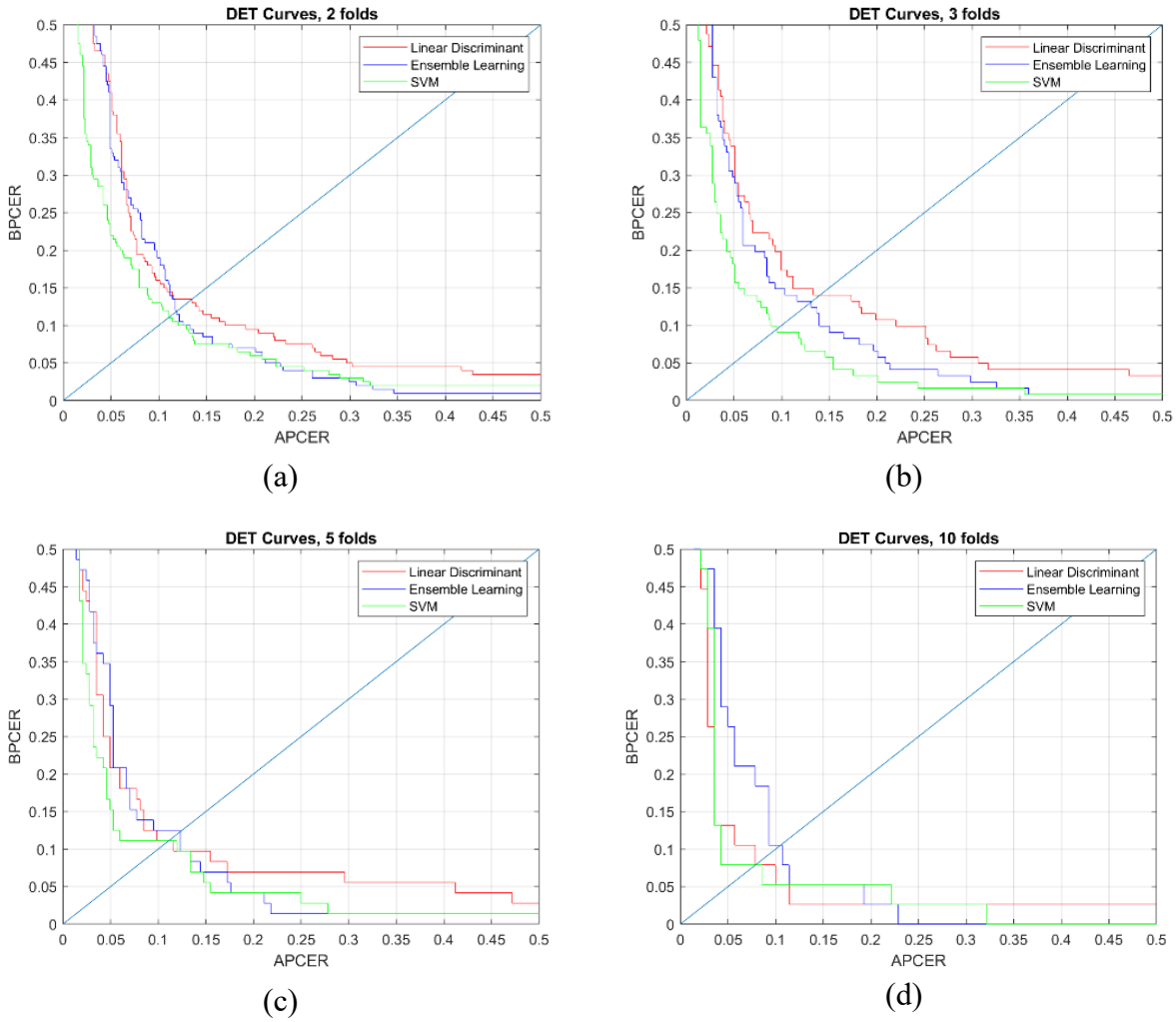


Figure 4.8. DET Curves for PAD subsystem performance under different classification methods and partitioning (Thermal sensor).

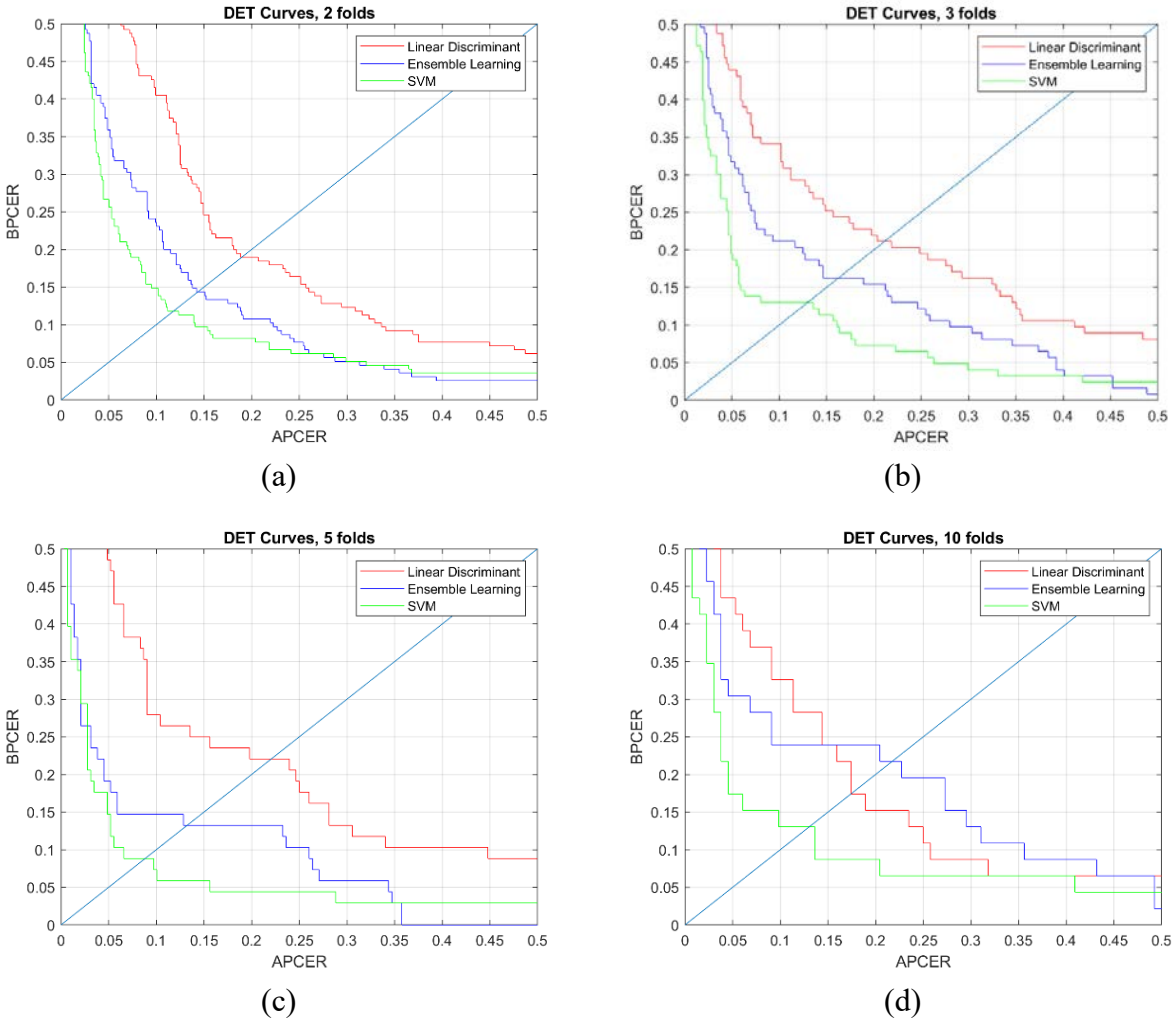


Figure 4.9. DET Curves for PAD subsystem performance under different classification methods and partitioning (Optical sensor).

Table 4.3. Classification Performance: BPCER at fixed APCER (Thermal sensor).

Classifier	Number of folds	BPCER% @APCER=5%	(APCER=BPCER)%
LI	2	41	13.46
	3	33.8	14.5
	5	20.8	11.1
	10	50	19.3
EN	2	33.5	11.87
	3	29.7	13.1
	5	29.1	12.3
	10	47.3	19.3
SVM	2	22	11
	3	18.1	9.5
	5	15.2	11.1
	10	23.6	10.5

Table 4.4. Classification Performance: BPCER at fixed APCER (Optical sensor).

Classifier	Number of folds	BPCER% @APCER=5%	Equal error rate (APCER=BPCER)%
LI	2	57.9	18.9
	3	43.9	21.1
	5	48.5	22
	10	43.4	17.4
EN	2	35.9	14.3
	3	31.7	16.2
	5	19.1	13.2
	10	30.4	21.7
SVM	2	26.6	11.7
	3	19.5	13
	5	14.7	8.8
	10	17.3	13

The next section analyzes and interprets the obtained results where attack potential is studied for each PAI specie individually. Further analysis has been performed in section 4. 4. 2 aiming to enhance the PAD subsystem performance through dimensionality reduction using sequential feature selection.

4. 4. 1. ATTACKS STRENGTH

Different attack types are expected to have different attack potentials, a PAD mechanism may not succeed to distinguish specific attack types, while performs more successfully with other types [11]. As an illustration, Figure 4.10 and Figure 4.11 analyzes the misclassified predictions of the three classification methods in the case of 2-folds cross-validation, considering seven PAI species and multi-class classification scheme.

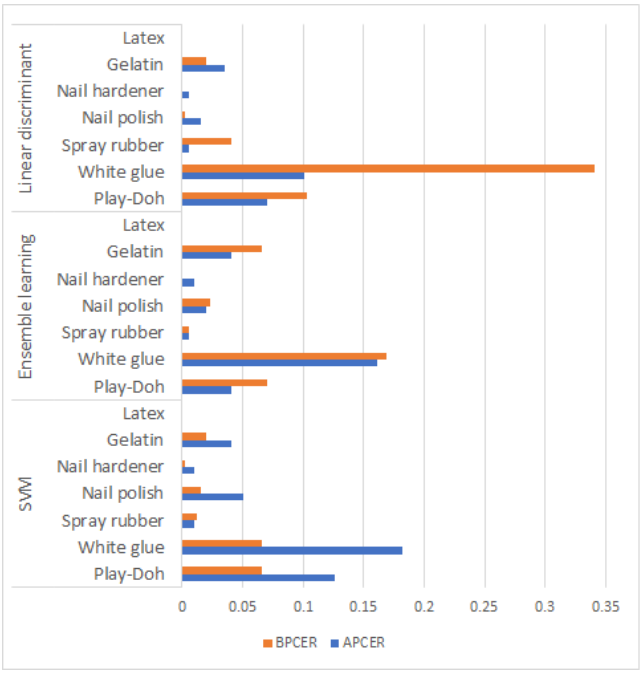


Figure 4.10. PAD subsystem performance considering $APCER_{PAIS}$, $BPCER_{PAIS}$, and 50% training and testing cross validation (Thermal sensor).

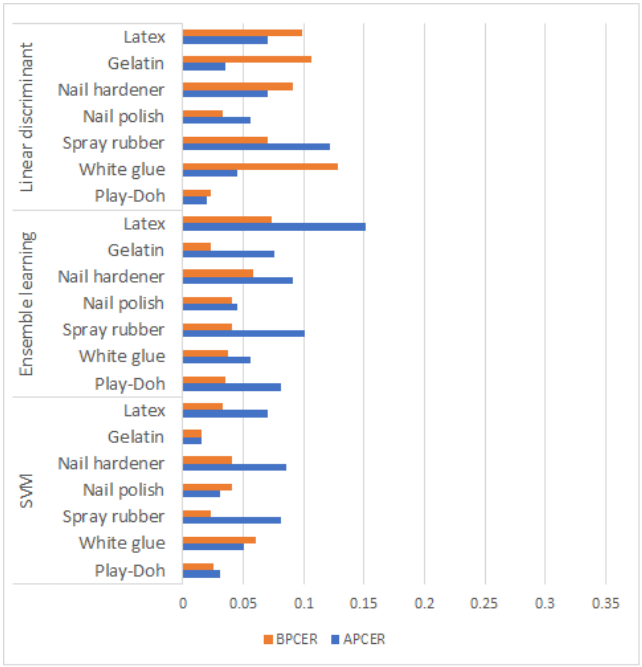


Figure 4.11. PAD subsystem performance considering $APCER_{PAIS}$, $BPCER_{PAIS}$, and 50% training and testing cross validation (Optical sensor).

Broadly speaking, we found values for APCER and BPCER of the thermal subset to be lower than 5% for all attack types excluding Play-Doh and White Glue attacks. This lends support to the fact that different attack types have different potentials. On the contrary, the PAD mechanism shows a

form of consistency for the different attacks when considering the optical sensor subset, APCER and BPCER are 5% ± 3 for all attacks in the SVM model.

Since all attacks are performed by the same attacker, fingerprint sources (i.e. 3D molds), and attack methodology, we suggest that the attack potential of the different species varies due to the characteristics of each PAI species; nonetheless, introducing another attacker might produce different results.

4. 4. 2. SEQUENTIAL FEATURE SELECTION

Sequential feature selection method is used to eliminate the features that increase the prediction error. The algorithm starts by choosing one feature and calculate the corresponding prediction error. Then the rest of features are tested one by one, and only those features which reduce the error are added to the model.

Contrary to expectations, the overall performance of the tested models is decreased compared to classification results without dimensionality reduction. Figure 4.12 and Figure 4.13 demonstrate the PAD subsystem performance using 2, 3, 5, 10 folds cross validation, while Figure 4.14 and Figure 4.15 compare DET curves of feature selection for each classifier considering 2 folds cross validation.

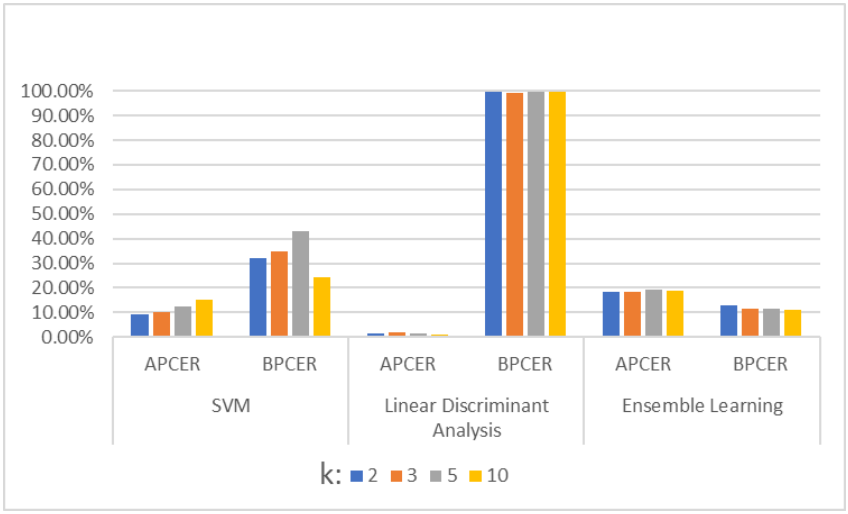


Figure 4.12. PAD subsystem performance after applying sequential feature selection (Thermal sensor).

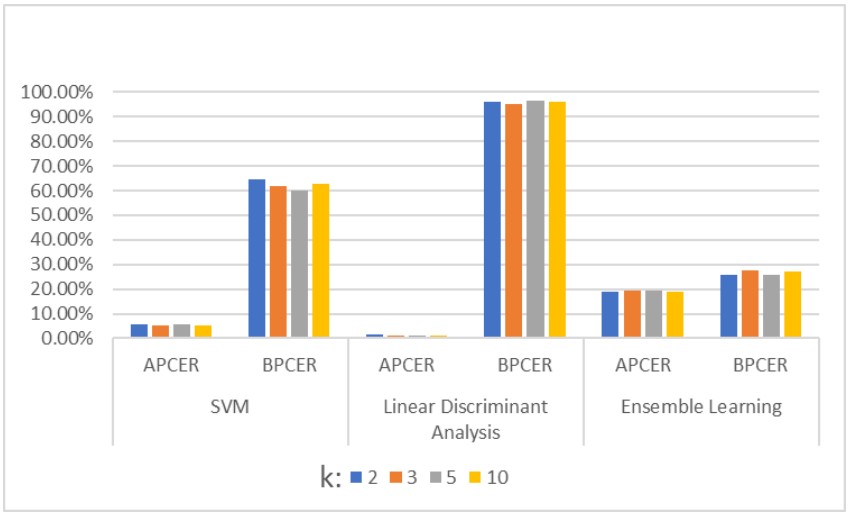


Figure 4.13. PAD subsystem performance after applying sequential feature selection (Thermal sensor).

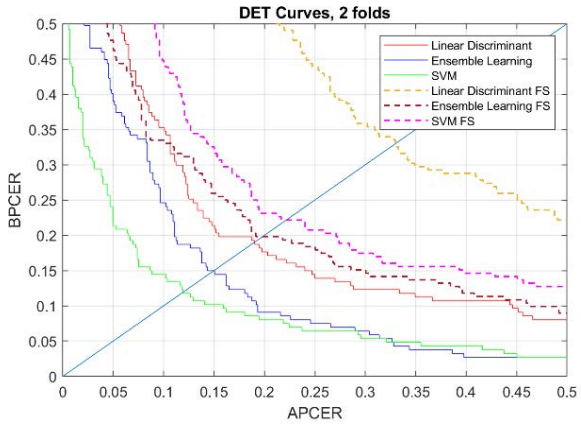


Figure 4.14. PAD subsystem performance with and without Feature Selection (Thermal sensor).

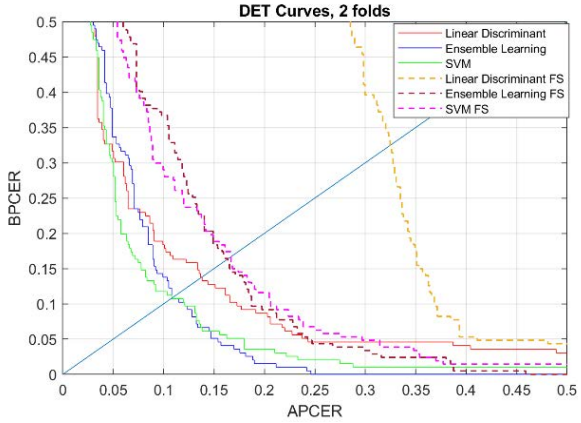


Figure 4.15. PAD subsystem performance with and without Feature Selection (Optical sensor).

Table 4.5 and Table 4.6 report the PAD performance after feature selection by showing BPCER at fixed APCER and the equal error rate.

Table 4.5. Classification performance: BPCER at fixed APCER (thermal sensor).

Classifier	BPCER% @APCER=5%	Equal error rate (APCER=BPCER)%
LI	95.6	32.4
EN	57.9	16.3
SVM	52.1	16.6

Table 4.6. Classification performance: BPCER at fixed APCER (optical sensor).

Classifier	BPCER% @APCER=5%	Equal error rate (APCER=BPCER)%
LI	73.1	32.9
EN	47.6	19.8
SVM	65.5	22.17

Even though feature selection reduces the computational cost of the overall PAD system, it decreases the PAD performance, thus feature selection is not considered in our method.

4. 4. 3. COMPARISON WITH SoA METHODS

Comparing our method with the state-of-the-art methods is not as straightforward as comparing the two sensors in our experiment. We recommend considering the following factors before comparing those results with the PAD mechanisms in Table 4.7: (i) experiment's protocol, (ii) database characteristics, and (iii) evaluation methodology.

Table 4.7. Comparison of the SoA mechanisms.

PAD mechanism	Sensor	APCER	BPCER	TEER
Antonelli 2006 [152]	Optical	NA	NA	11.24%
Zhang 2007 [154]	Optical	NA	NA	4.5%
Jia 2007 [153]	Capacitive	NA	NA	4.78%
Derakhshani 2003 [222]	Capacitive	NA	NA	11.11%
Parthasaradhi 2005 [223]	Capacitive	5% - 20%	6.77% - 20%	NA
	Optical	4.6%-14.3	0% - 26.9%	NA
	Electro-Optical	0%-19%	6.9% - 38.5%	NA
Abhyankar 2009 [119]	Optical, electro-optical, and capacitive	NA	NA	13.85%
Plesh 2019 [224]	Optical	0.2%	13.8% - 18.35%	NA
Proposed	Optical	5%	26.6%	11.7%
	Thermal	5%	11%	22%

4. 5. CONCLUSION

Our work has led us to the conclusion that genuine fingerprint is a rich source of information, rather than only a graphical static pattern. Having an accurate and deep understanding of fingerprint phenomena, e.g. skin elasticity, temperature, perspiration, etc. is a key for PAD solutions' development. The findings of the studies on dynamic fingerprint features support the fact that genuine fingerprints produce unique dynamic patterns.

The proposed PAD method explores the variation of eight global measures e.g. intensity (mean), contrast (std), randomness (entropy), during fingerprint presentations. Those features are concatenated to form a description of the fingerprint pattern's formation. To verify whether the description is sufficiently discriminative, different classification algorithms are tested; SVM, LDA, and ensemble learning. The evaluation is conducted using a dynamic dataset that was collected using thermal and optical sensors, 66 genuine fingerprints, and 7 PAI species.

Considering SVM classification and 50% partitioning for training and testing, we note comparable PAD performance for both sensors. Error rates are $APCER_{total}$ = BPCER= 11% for the thermal subset and $APCER_{total}$ = BPCER= 11.7% for the optical subset. Even though error rates show a resemblance for both sensors, we have shown that each PAI species has a certain attack potential. To put it differently, dominant attacks that increase error rates in the thermal subset are Play-Doh and white glue attacks, while different attack species have roughly homogeneous error rates in the optical subset.

Dimensionality reduction method has been tested seeking to enhance the PAD subsystem performance, but results were unsatisfactory compared to the original results.

The most important limitation of this investigation is the small size of the dataset, which consists of 11 independent subjects 6 fingers each. Moreover, the proposed mechanism has a limitation in distinguishing specific materials for the thermal sensor. Nevertheless, we believe our methodology could be a starting point for developing more sophisticated mechanisms.

To further our research, we intend to acquire data from new subjects, as well as investigating more sophisticated features in order to enhance the performance of the PAD subsystem.

Chapter 5. Fingerprint Presentation Attack Detection Utilizing Spatio-Temporal Features

In the previous chapter, the experiment was conducted by analyzing the fingerprint as a sequence of dependent frames. The dynamic features were extracted from the video frames in the spatial domain, then the variation of those spatial features was used to describe each fingerprint video. The results of the experiment had shown that concatenating features from the spatial domain provides a certain level of accuracy as provided by the PAD mechanism's error rates.

In order to improve the PAD accuracy, this chapter proposes to investigate the fingerprint videos as 3-D signals. That is to say, instead of concatenating 2-D features from the video frames, the proposed algorithm analyzes the 3-D patterns in the fingerprint video by consolidating the spatial and temporal information. For that reason, five state-of-the-art dynamic texture descriptors (spatio-temporal feature extractors) are used for the PAD feature extraction and then evaluated after an SVM classification. The spatio-temporal features provide significant improvement compared to the obtained results in the previous section and the SoA works in the dynamic fingerprint PAD.

The rest of this chapter is structured as follows. Section 1 presents a brief overview of the dynamic texture applications in the biometrics discipline. In the second section, we describe the framework of the proposed PAD subsystem. The experiment is characterized in Section 3. Section 4 reports and discusses the experimental results. Finally, we the conclusions are drawn in section 5.

5. 1. DYNAMIC TEXTURE: APPLICATIONS IN BIOMETRICS

Dynamic textures are textures with motion [226]. Ideally, a dynamic texture descriptor consolidates 2-D textures in a scene with temporal variations, meaning that information of space and time are obtained simultaneously. There is a vast amount of literature on dynamic texture recognition with application to biometric recognition and analysis, this section highlights the most related works in this domain.

In their seminal paper of 2007 [227], Zhao and Pietikäinen proposed a simple approach to extract dynamic textures using Volume Local Binary Patterns (VLBP) and Local Binary Patterns from Three Orthogonal Planes (LBP-TOP). The method had been proposed with application to facial expression recognition and reported over 95% accuracy. Moreover, a recent study on spontaneous facial micro-expression recognition suggested a deep learning model based on spatial and temporal streams and reported 63.53%-74.05% accuracy [228].

In 2018, an experiment had been carried out on the applications of the VLBP in face PAD [229]. The authors had evaluated their PAD mechanism considering printed and replay attacks (video attacks). The PAD mechanism had successfully eliminated all printed attacks with 100% accuracy and mitigated replay attacks with 97.38% accuracy.

Additionally, various dynamic descriptors were suggested to categorize human actions. Solmaz et al. [230] extended the GIST descriptor into GIST3D and evaluated the method on different datasets, the authors obtained 92% accuracy for classifying 6 action categories. Further, the authors in [231] suggested utilizing the binarized statistical image feature (BSIF) to extract the dynamic features from 3-D salient patches and reported 93.43% accuracy for classifying low-quality videos.

5. 2. PROPOSED PRESENTATION ATTACK DETECTION SUBSYSTEM

The proposed PAD subsystem is designed in a fashion that leverages the dynamic information provided during the fingerprint presentation (Figure 5.1). Thus, the proposed feature extraction approach suggests exploiting the spatio-temporal features to achieve a robust description that characterizes the complete interaction between the fingerprint and the sensor's surface. Toward this end, we propose three modes to investigate fingerprint dynamics in frequency and time domains. Five feature extractors are therefore selected to achieve a description that discriminates genuine from attack presentations. By feeding the extracted features into a pre-trained classifier, the PAD subsystem finally decides whether the input video is a bona fide or attack presentation. The following subsections expound the processing modes, feature extractors, and classification method.

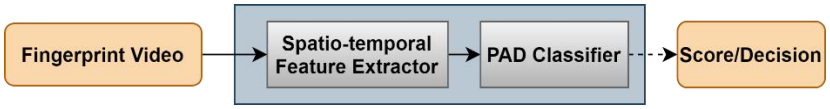


Figure 5.1. Dynamic PAD Subsystem Scheme.

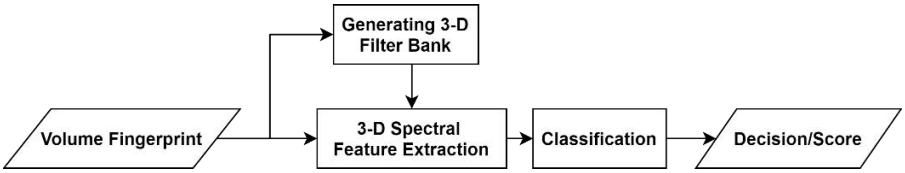
5. 2. 1. FEATURE EXTRACTION MODES

In order to investigate different aspects of fingerprint dynamics, three feature extraction modes are elaborated in this subsection. The first mode investigates dynamic fingerprint features in the frequency domain whereas a 3-D filter bank is utilized to extract spectral features in a diverse range of scales and orientations. As the video's frequency components effectively represent the static fingerprint pattern and the temporal variations, it is expected that the differences between natural skin and attack species produce frequency components in different planes. Hence, this mode captures the spatio-temporal information by filtering the video frequency spectrum in different orientations and center frequencies.

The second mode samples the fingerprint video on space-time domain into small 3-D patches, extracts the spatio-temporal features from those samples, and provides the description as the frequency distribution of the extracted features. This mode has two main interesting features, primarily, it has the capacity to define local features in a stack of XY patches so that any anomalous formation in the fingerprint video is detected. Secondly, it provides the possibility of processing the 3-D patches in space-time and/or frequency domains.

The third mode resembles the second mode, a small brick is added after the sampling to decompose the 3-D patches into the Three Orthogonal Planes (TOP) XY, XT, and YT planes. Over the advantages of the second mode, the third mode had proved significantly reduced complexity for the adopted feature extractor while preserving a high accuracy [227].

Figure 5.2 illustrates these modes and Figure 5.3 shows an example of a fingerprint video and its sampling into 3-D patches and TOPs.



(a) Spectral feature extraction using a 3-D filter bank.

(b) Feature extraction from 3-D Patches.

(c) Feature extraction from 3-D Patches decomposed into three orthogonal planes.

Figure 5.2. Proposed PAD scheme in different modes.

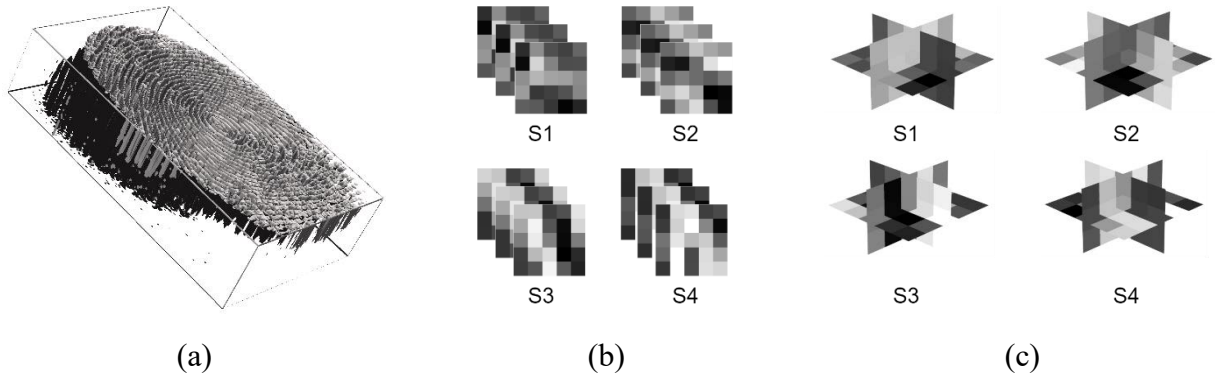


Figure 5.3. Illustration of 3-D sampling and decomposition: (a) fingerprint video (b) 3-D patches sized (5x5x3) (c) patches in b decomposed into XY, XT, and YT planes.

5. 2. 2. FEATURE EXTRACTORS

The feature extractors were selected in order to be in accordance with the proposed modes, moreover, to analyze the features in spatio-temporal and spectral domains. Table 5.1 summarizes the proposed scenarios with the corresponding dynamic feature extractors and the following subsections reviews these algorithms.

Table 5.1. The used feature extraction (FE) algorithms.

FE algorithm	FE Mode	Domain of FE	Source of features	Reference
GIST 3-D	Mode 1	spatio-temporal frequency domain	Sub-volumes in the frequency domain	[230]
Volume Local Binary Patterns	Mode 2	spatio-temporal domain	3-D Patches	[229]
Local Binay Patterns from Three Orthogonal Planes	Mode 3	spatio-temporal domain	Patches of TOPs	[229]
Volume Local Phase Quantization	Mode 2	spatio-temporal frequency domain	3-D Patches	[232]
Local Phase Quantization from Three Orthogonal Planes	Mode 3	spatio-temporal frequency domain	Patches of TOPs	[232]

5.2.2.1 GIST 3-D Descriptor

GIST 3-D is a global spatio-temporal descriptor that had been proposed for video classification problems. The method integrates the motion information and the scene structure in one feature vector without applying background subtraction or salient point detection at the input video, achieving performance better than SoA dynamic descriptors.

In our experiment, the GIST3-D works as follows: first, the frequency spectrum of the complete fingerprint video is achieved by applying 3-D Discrete Fourier Transform; as computed by equation 5.1.

$$F(f_x, f_y, f_t) = \frac{1}{MNT} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{t=0}^{T-1} f(x, y, t)\ e^{-j2\pi(\frac{xf_x}{M}+\frac{yf_y}{N}+\frac{tf_t}{T})} \quad 5.1$$

Then, a bank of narrow band 3-D Gabor filters $G(fr, \theta, \phi)$ is generated and each 3-D filter $Gi(f_x, f_y, f_t)$ is applied to the frequency spectrum as given by equation 5.2. The filter bank is composed by 3-D filters with different orientations and scales, which allows capturing the components at various intervals of the video's frequency spectrum.

$$\Gamma_i(f_x, f_y, f_t) = F(f_x, f_y, f_t)[G_i(f_x, f_y, f_t)] \quad 5.2$$

After taking the inverse 3-D DFT as in equation 5.3 for each filter in the bank, the output volume is quantized in fixed sub-volumes and the sum of each sub-volume is taken, thus, a feature vector is obtained to represent the video description.

$$H_i(x, y, t) = \sum_{f_x=0}^{M-1} \sum_{f_y=0}^{N-1} \sum_{f_t=0}^{T-1} \Gamma_i(f_x, f_y, f_t)\ e^{j2\pi(\frac{xf_x}{M}+\frac{yf_y}{N}+\frac{tf_t}{T})} \quad 5.3$$

5.2.2.2 Volume Local Binary Patterns

The basic Local Binary Patterns method was extended to VLBP in order to describe the dynamic texture in a sequence of successive images [227]. The algorithm starts by sampling the gray level volume input into small 3D samples considering a certain number of local neighbors (P), time interval (L), and radius (R) in x-y plane, then every neighbor pixel in the 3D sample is given a

binary value based on a comparison with the center pixel of the sample. Finally, each binary value is multiplied by a corresponding weight and all results are summed to form the sample's $VLBP_{L,P,R}$ code; equation 5.4. The distribution of the codes is used to compose the dynamic texture feature vector.

$$VLBP_{L,P,R} = \sum_{p=0}^{3P+1} s(g_p - g_c)\ 2^p \qquad 5.4$$

where g_p and g_c correspond to the gray values of the central pixel and neighbors in the 3-D sample.

The authors in [227] proposed two additional modes for the method: (1) rotation-invariant VLBP mode ($VLBP^{ri}_{L,P,R}$) which is based on the assumption that volume data rotates only around *t*-axis, (2) uniform VLBP mode ($VLBP^{u2}_{L,P,R}$), where the VLBP histogram consists of uniform patterns (i.e. patterns contain at most 2 bitwise transitions between 0 and1) and sums up all non-uniform patterns in 1 bin.

5.2.2.3 Volume Local Phase Quantizer

The VLPQ method [232] is an extension to the local phase quantization which was originally proposed as an image descriptor [173]. VLPQ essentially encodes local Fourier transform's phase information at low-frequency points. The method consists of three steps: (1) local Fourier transform is applied, using Short Term Fourier Transform (STFT), over MxMxN neighborhood N_x centered at each pixel position x using 1-D convolutions for each dimension, (2) the dimensionality of the achieved data is reduced using Principal Component Analysis (PCA), and (3) a scalar quantization is applied to produce an integer value. The histogram of the binary codewords is computed to form the $VLPQ_{M,N}$ feature vector.

5.2.2.4 Local Binary Patterns from Three Orthogonal Planes

Although VLBP method is interesting, it suffers from two major issues. First, initializing the algorithm with a large number of neighbors *P* results in a very large number of patterns in the VLBP feature vector, limiting the method's applicability. Second, choosing a time radius *L* larger than 1 excludes the frames with a time variance less than *L*.

To address these issues, VLBP-$TOP_{L,P,R}$ method had been proposed in [227] to concatenate the local binary patterns on the three orthogonal planes: XY-LBP, XT-LBP, and YT-LBP. With this approach, spatial patterns are obtained from XY plane and space-time transitions information is attained from XT and YT planes. As a result, the number of patterns on the feature vector is significantly reduced from 2^{3P+2} to $3 \cdot 2^P$ which allows considering a large number of neighbors with reduced computational cost, moreover, including neighbor pixels from frames with a time variance less than *L*, when *L* is larger than 1.

5.2.2.5 Local Phase Quantizer from Three Orthogonal Planes

LPQ-TOP$_{Rx,Ry,Rz}$ is implemented by calculating LPQ histograms from three orthogonal planes similar to LBP-TOP. The histograms are normalized and concatenated to form the LPQ-TOP descriptor [232].

5. 2. 3. PAD Classification

Through our experiment, we have tested different classification algorithms, specifically: Classification Trees, Discriminant Analysis, Naive Bayes, Nearest Neighbors, SVM Classification, and Classification Ensembles. SVM classification has been chosen due to its highest accuracy as shown in Table 5.2, while the other classification methods are not considered in this Chapter. Moreover, we have examined the impact of changing the SVM kernel whereas a second polynomial kernel demonstrated the best accuracy. A binary classification scheme has been utilized to evaluate the PAD subsystem performance and to assess the influence of specific PAI species on system security and usability.

The results in Table 5.2 are produced using one feature extractor, i.e. VLPQ, for showing the machine learning methods accuracy and to justify the selection of the quadratic SVM algorithm. the results for the other feature extractors provide the same result which is the selection of the SVM model.

Table 5.2. PAD classification accuracy for the dynamic features. The VLPQ features were used to produce these results considering 50% training and 50% testing partitioning.

Machine learning algorithm	Configuration	Accuracy	
		Optical	Thermal
Tree	Fine tree	88.8%	83.3%
	Medium tree	88.9%	84.0%
	Coarse tree	82.7%	82.6%
Discriminant Analysis	Linear discriminant	84.8%	78.6%
Logistic regression	Logistic regression	84.3%	77.4%
Naive bayes	Gaussian naive bayes	69.8%	74.1%
	Kernel naive bayes	76.4%	81.4%
SVM	Linear SVM	96.0%	92.1%
	Quadratic SVM	**97.6%**	**95.5%**
	Fine gaussian SVM	77.6%	77.8%
	Medium gaussian SVM	96.5%	92.5%
	Coarse gaussian SVM	85.6%	83.8%
KNN	Fine KNN	96.0%	89.8%
	Medium KNN	91.1%	87.4%
	Coarse KNN	78.7%	80.8%
	Cosine KNN	91.2%	87.8%
	Cubic KNN	90.9%	86.4%
	Weighted KNN	93.8%	88.9%
Ensemble	RUSBoosted trees	92.9%	89.6%

5. 3. EXPERIMENT

To evaluate the performance of the proposed PAD subsystem, we use the dynamic dataset presented in [233]. In the initial stage of the experiment, a volume segmentation is applied to the database. This sets the input fingerprint videos to the feature extraction step. At this point, we utilize the scheme in Figure 5.2 to extract the features and train the SVM model. As soon as these steps have been carried out, the testing process is performed, and the PAD subsystem accuracy is assessed.

5. 3. 1. DATABASE

In this chapter, the first portion of the database, which represent ordinary dynamic presentation, is used. The same portion was used in the experiment of Chapter 4.

5. 3. 2. VOLUME SEGMENTATION

To neglect the influence of empty background on the extracted features, we apply 3-D segmentation to the dataset so that the features are extracted only from the part of the sensor's surface where the presentation was applied.

1) Segmentation of thermal subset

The thermal sensor's SDK provides a capturing mode that acquires only the central region of the sensor sized 90×128 pixels. Thus, the acquired sequence is already segmented as a stack of 7 frames sized 90×128 Figure 5.4.

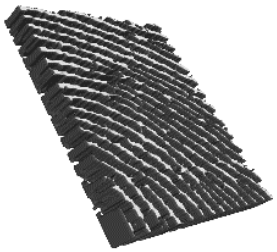
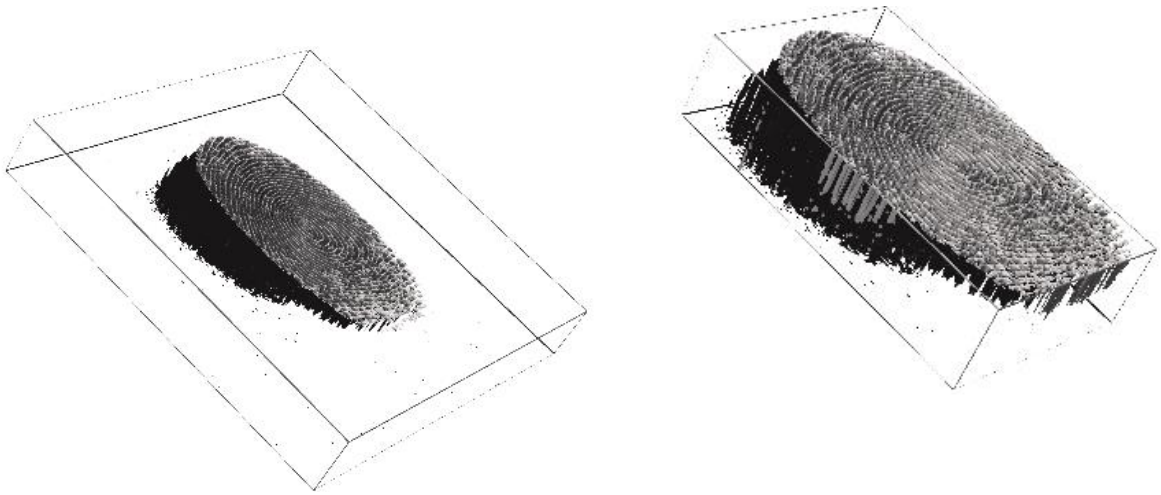


Figure 5.4. Segmented fingerprint video.

2) Segmentation of optical subset

Since our study analyzes the formation of fingerprints, we have implemented a simple volume segmentation tool that creates the boundaries of the entire Interaction between a fingerprint and the sensor. Then, we have applied the segmentation to the entire subset of the optical sensor before feature extraction; an example is shown in Figure 5.5 (a) and (b).



(a) (b)

Figure 5.5. Demonstration of a volume segmentation for a presentation of 29 images, before and after segmentation sized 375x400 and 234x145 respectively. The figures do not reflect the real scale of the fingerprint.

5. 3. 3. EXPERIMENTAL PROTOCOL

Each sensor subset is evaluated independently due to the differences in the sensors' technology, image size, resolution, noise, and capturing rate which produce different video characteristics. For a robust accuracy estimation, we have set a holdout validation scheme where the database is divided into training (55%) and testing (45%) sets. The database division into training/testing is randomized by independent subjects, meaning that presentations of each independent subject is either used for training or testing.

The PAD evaluation is carried out following the proposed methodology in Chapter 3. The results are discussed in the next section.

5. 4. RESULTS AND DISCUSSION

In this section, we assess the accuracy of the proposed PAD scheme and analyze the influence of selecting the feature extractor on the PAD subsystem efficiency.

5. 4. 1. Impact of PAD Subsystem Mode and Feature Extraction Method

The first set of analyses examined the impact of (i) the size of 3-D samples used in the processing mode, and (ii) selecting rotation invariant or uniform features, on the feature extractor performance. Figure 5.6 and Figure 5.7 show DET curves for VLBP, LBP-TOP, VLPQ, and LPQ-TOP with the corresponding sampling parameters. The figures confirm that 3-D spectral features (i.e. VLPQ and LPQ-TOP) performs better at smaller sampling size, and the accuracy degrades considerably when comparing the smallest and largest sampling size. An exception is noticed for

the LPQ-TOP when executed on the optical sensor. On the other hand, 3-D spatio-temporal features (i.e. VLBP and LBP-TOP) have not revealed a general correlation between sampling size and accuracy. However, it is evident that rotation invariant and uniform features do not necessarily improve the accuracy in most of the cases, but nonetheless no significant degradation has taken place after considering those features.

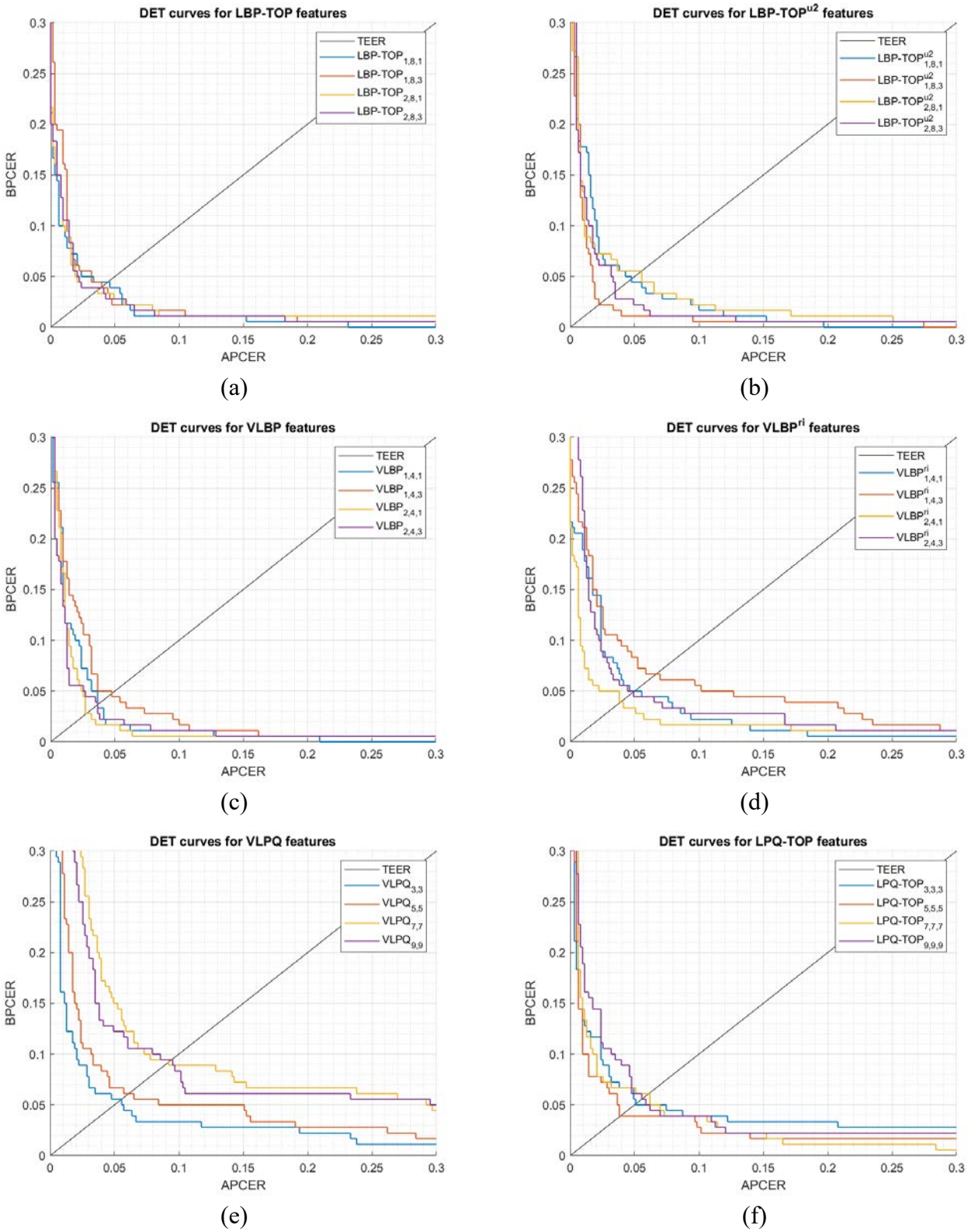


Figure 5.6. DET curves comparison of the proposed feature extraction algorithms using different parameters (optical sensor).

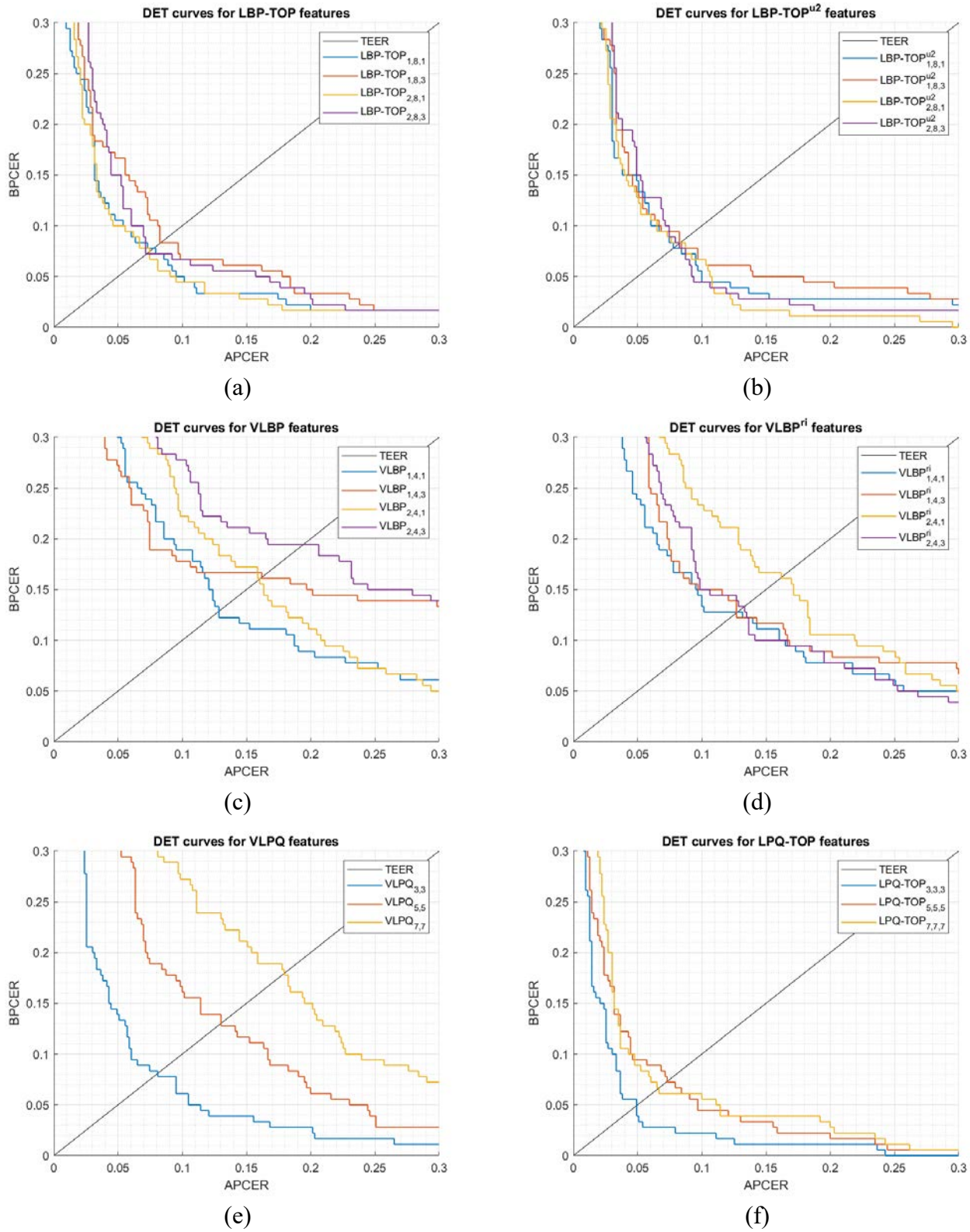


Figure 5.7. DET curves comparison of the proposed feature extraction algorithms using different parameters (thermal sensor).

Table 5.3 and Table 5.4 detail the results categorized by the feature extraction method. We have selected multiple thresholds: (i) TEER, (ii) APCER= 5%, and (iii) APCER= 2.5% to evaluate the methods at different security levels. The tables reveal the total number of the misclassified bona fide/attack presentations at each threshold. It is worthwhile noting that testing data, which corresponds to 5 independent subjects, consists of 630 attack and 180 bona fide presentations.

Table 5.3. PAD performance of optical sensor.

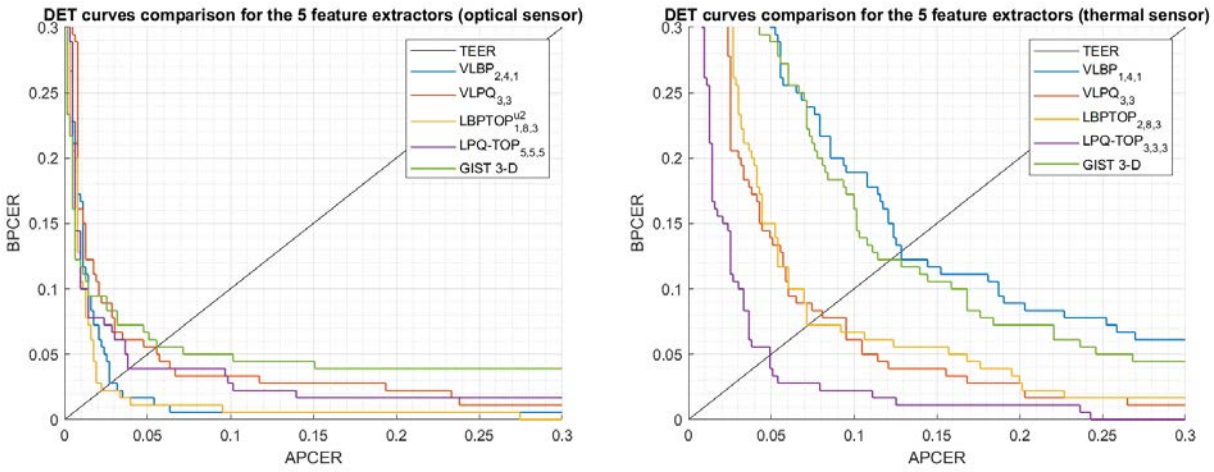
Descriptor	TEER			at APCER = 5%			at APCER = 2.5%		
	TEER	Successful attacks	Rejected B-F	BPCER20	Successful attacks	Rejected B-F	BPCER	Successful attacks	Rejected B-F
$VLPQ_{3,3}$	**5.56%**	**35**	**10**	**5.56%**	31	**10**	**8.89%**	16	**16**
$VLPQ_{5,5}$	6.11%	39	11	6.67%		12	11.11%		20
$VLPQ_{7,7}$	9.21%	58	17	15.00%		27	29.44%		53
$VLPQ_{9,9}$	9.44%	60	17	12.22%		22	25.00%		45
$LPQ\text{-}TOP_{3,3,3}$	5.08%	32	9	5.56%	31	10	9.44%	16	17
$LPQ\text{-}TOP_{5,5,5}$	**3.89%**	**25**	**7**	**3.89%**		7	**7.22%**		**13**
$LPQ\text{-}TOP_{7,7,7}$	6.11%	39	11	6.67%		12	7.78%		14
$LPQ\text{-}TOP_{9,9,9}$	5.56%	35	10	6.11%		11	11.11%		20
GIST 3-D	**5.56%**	**35**	**10**	**6.67%**	31	**12**	**9.44%**	16	**17**
$VLBP_{1,4,1}$	3.65%	23	7	1.67%	31	3	7.22%	16	13
$VLBP_{1,4,3}$	4.76%	30	9	4.44%		8	11.67%		21
$VLBP_{2,4,1}$	**2.78%**	**18**	**5**	**1.67%**		**3**	**5.00%**		**9**
$VLBP_{2,4,3}$	3.65%	23	7	2.22%		4	5.56%		10
$VLBP^{ri}_{1,4,1}$	5.00%	32	9	5.00%	31	9	8.89%	16	16
$VLBP^{ri}_{1,4,3}$	6.67%	42	12	8.33%		15	13.33%		24
$VLBP^{ri}_{2,4,1}$	3.89%	25	7	3.33%		6	5.00%		9
$VLBP^{ri}_{2,4,3}$	4.92%	31	9	4.44%		8	8.89%		16
$LBP\text{-}TOP_{1,8,1}$	4.44%	28	8	3.89%	31	7	5.00%	16	9
$LBP\text{-}TOP_{1,8,3}$	3.97%	25	7	2.22%		4	5.56%		10
$LBP\text{-}TOP_{2,8,1}$	3.65%	23	7	2.78%		5	3.89%		7
$LBP\text{-}TOP_{2,8,3}$	3.89%	25	7	2.78%		5	3.89%		7
$LBP\text{-}TOP^{u2}_{1,8,1}$	4.76%	30	9	4.44%	31	8	7.22%	16	13
$LBP\text{-}TOP^{u2}_{1,8,3}$	**2.22%**	**14**	**4**	**1.11%**		**2**	**2.22%**		**4**
$LBP\text{-}TOP^{u2}_{2,8,1}$	5.56%	35	10	5.56%		10	7.22%		13
$LBP\text{-}TOP^{u2}_{2,8,3}$	3.49%	22	6	2.22%		4	6.11%		11

Table 5.4. PAD performance of thermal sensor.

Descriptor	at TEER			at APCER = 5%			at APCER =2.5%		
	TEER	Successful attacks	Rejected B-F	BPCER20	Successful attacks	Rejected B-F	BPCER	Successful attacks	Rejected B-F
$VLPQ_{3,3}$	**8.10%**	**51**	**15**	**13.89%**	31	**25**	**27.78%**	16	**50**
$VLPQ_{5,5}$	13.02%	82	23	31.67%		57	46.11%		83
$VLPQ_{7,7}$	17.94%	113	32	46.67%		84	65.00%		117
$LPQ\text{-}TOP_{3,3,3}$	**4.92%**	**31**	**9**	**3.89%**	31	**7**	**14.44%**	16	**26**
$LPQ\text{-}TOP_{5,5,5}$	7.30%	46	13	9.44%		17	17.78%		32
$LPQ\text{-}TOP_{7,7,7}$	6.67%	42	12	8.89%		16	22.78%		41
GIST 3-D	**12.22%**	**77**	**22**	**28.89%**	31	**52**	**46.67%**	16	**84**
$VLBP_{1,4,1}$	12.86%	81	23	30.00%	31	54	51.67%	16	93
$VLBP_{1,4,3}$	16.19%	102	29	27.22%		49	48.33%		87
$VLBP_{2,4,1}$	16.03%	101	29	37.22%		67	61.11%		110
$VLBP_{2,4,3}$	19.44%	123	35	43.89%		79	57.78%		104
$VLBP^{ri}_{1,4,1}$	12.78%	81	23	**23.89%**	31	**43**	**41.11%**	16	**74**
$VLBP^{ri}_{1,4,3}$	**12.70%**	**80**	**23**	37.22%		67	72.22%		130
$VLBP^{ri}_{2,4,1}$	16.19%	102	29	33.33%		60	53.89%		97
$VLBP^{ri}_{2,4,3}$	13.33%	84	24	35.56%		64	56.67%		102
$LBP\text{-}TOP_{1,8,1}$	7.78%	49	14	10.56%	31	19	**23.33%**	16	**42**
$LBP\text{-}TOP_{1,8,3}$	8.33%	53	15	16.67%		30	24.44%		44
$LBP\text{-}TOP_{2,8,1}$	7.46%	47	13	10.00%		18	20.00%		36
$LBP\text{-}TOP_{2,8,3}$	**7.22%**	**46**	**13**	15.00%		27	36.11%		65
$LBP\text{-}TOP^{u2}_{1,8,1}$	7.78%	49	14	14.44%	31	26	28.33%	16	51
$LBP\text{-}TOP^{u2}_{1,8,3}$	8.33%	53	15	13.33%		24	28.33%		51
$LBP\text{-}TOP^{u2}_{2,8,1}$	8.33%	53	15	**12.78%**		**23**	29.44%		53
$LBP\text{-}TOP^{u2}_{2,8,3}$	8.25%	52	15	15.00%		27	37.22%		67

We then carry out a performance comparison between the five dynamic feature extraction methods (Figure 5.8) by selecting the methods' best parameters from Table 5.3 and Table 5.4. Note that those parameters had been chosen empirically, thus they might not be optimal for the suggested feature extractors in the context of our experiment.

The most striking result to emerge from Figure 5.8 is the achievement of significantly low TEERs, where the system security remains high (low APCER) with low bona fide rejects (low BPCER), that is to say, these results offer powerful evidence for the fact that a genuine fingerprint provides sufficiently discriminative dynamic information that distinguishes it from attacks.



(a) Optical sensor (b) Thermal sensor

Figure 5.8. DET curves comparison of the proposed PAD subsystem using five feature extractors.

5. 4. 2. Impact of Sensing Technology

We next investigate the robustness of the proposed PAD subsystem when different fingerprint sensing technologies are used, explicitly, we compare the PAD accuracy for the thermal and optical sensors (Figure 5.8) in terms of TEER. We observe from Table 5.5 that the accuracy of the PAD subsystem for the optical sensor has best results over the thermal sensor. The distinction appears to be well substantiated by the higher frame rate, image size, and resolution in the optical sensor which allows to precisely capture the fingerprint/PAI formation; i.e. spatio-temporal information. Moreover, each presentation in the thermal sensor is captured over roughly 5 seconds while in the optical sensor, a presentation can be captured in 0.5 second including 10 successive frames.

Table 5.5. BPCER20 comparison between the optical and thermal sensors.

Sensor\FE	**VLPQ**		**LPQ-TOP**		**GIST 3-D**	**VLBP**		**LBP-TOP**	
Optical	$VLPQ_{3x3}$	5.5%	$LPQ\text{-}TOP_{5x5x5}$	3.8%	6.6%	$VLBP_{2x4x1}$	1.6%	$LBP\text{-}TOP^{u2}_{1x8x3}$	2.2%
Thermal	$VLPQ_{3x3}$	13.8%	$LPQ\text{-}TOP_{3x3x3}$	3.8%	28.8%	$VLBP_{1x4x1}$	30.0%	$LBP\text{-}TOP_{2x8x3}$	15.0%
Difference	8.3%		0.00%		22.2%	28.33%		12.78%	

5. 4. 3. Impact of Attack species

This section expounds the results from Section 5. 4. 1 seeking to point out the attack potential for each PAI species. The classification results are shown considering the SVM classification decision in Table 5.6 and Table 5.7.

Table 5.6. Attacks strength considering different PAI species (optical sensor).

	SVM error rates		APCER_PAI						
	APCER	**BPCER**	**Play-Doh**	**White glue**	**Spray rubber**	**Polish nail**	**Nails hardener**	**Gelatin**	**Latex**
$VLBP_{2,4,1}$	1.75%	7.78%	**0.00%**	1.11%	1.11%	**0.00%**	8.89%	**0.00%**	1.11%
$LBP\text{-}TOP^{u2}_{1,8,3}$	1.59%	6.67%	3.33%	1.11%	**0.00%**	1.11%	1.11%	2.22%	2.22%
$VLPQ_{3,3}$	3.33%	6.67%	5.56%	**0.00%**	3.33%	1.11%	8.89%	4.44%	**0.00%**
$LPQ\text{-}TOP_{5,5,5}$	2.38%	11.67%	3.33%	3.33%	**0.00%**	**0.00%**	3.33%	4.44%	2.22%
GIST 3D	1.43%	10.56%	4.44%	1.11%	2.22%	1.11%	**0.00%**	1.11%	**0.00%**

Table 5.7. Attacks strength considering different PAI species (thermal sensor).

	SVM error rates		APCER_PAI						
	APCER	**BPCER**	**Play-Doh**	**White glue**	**Spray rubber**	**Polish nail**	**Nails hardener**	**Gelatin**	**Latex**
$VLBP_{1,4,1}$	1.59%	56.11%	**0.00%**	10.00%	1.11%	**0.00%**	**0.00%**	**0.00%**	**0.00%**
$LBP\text{-}TOP_{2,8,3}$	4.44%	16.67%	1.11%	21.11%	6.67%	2.22%	**0.00%**	**0.00%**	**0.00%**
$VLPQ_{3,3}$	3.33%	18.33%	2.22%	15.56%	1.11%	1.11%	**0.00%**	3.33%	**0.00%**
$LPQ\text{-}TOP_{3,3,3}$	2.70%	11.11%	**0.00%**	8.89%	4.44%	2.22%	**0.00%**	3.33%	**0.00%**
GIST 3D	4.76%	29.44%	8.89%	24.44%	**0.00%**	**0.00%**	**0.00%**	**0.00%**	**0.00%**

As expected, the tables prove that different attack species have different attack potential considering a target sensor/PAD method. The PAD subsystem has been capable of eliminating some of the attack species and mitigate the rest of the species. Even though the overall performance for the optical sensor has been proven to be higher than the thermal sensor, a comparison between Table 5.6 and Table 5.7 demonstrates that the thermal sensor is notably vulnerable to white glue attacks but resistant to the rest of the attack species. On the other hand, the optical sensor shows either relatively low or 0% APCER for all attack species.

5. 4. 4. Accuracy Comparison with SoA mechanisms

To conduct a comparison between different PAD mechanisms, we emphasize the importance of considering the differences between experimental protocols, used databases, and evaluation methodologies. These factors refer to a certain attack potential to specific database/technology and evaluated using defined metrics.

In Chapter 3, these factors were characterized to a considerable extent in order to allow the reader to compare our proposed PAD mechanism with SoA mechanisms. Table 5.8 compares the performance of the proposed mechanism in this chapter with the related works that were explained in Chapter 4. We note that our results for both sensing technologies demonstrate significant improvement to the SoA methods.

Table 5.8. Comparison with SoA mechanisms.

PAD mechanism	Sensor	APCER	BPCER	TEER
Antonelli 2006 [152]	Optical	NA	NA	11.24%
Zhang 2007 [154]	Optical	NA	NA	4.50%
Jia 2007 [153]	Capacitive	NA	NA	4.78%
Derakhshani 2003 [222]	Capacitive	NA	NA	11.11%
Parthasaradhi 2005 [223]	Capacitive	5% - 20%	6.77% - 20%	NA
	Optical	4.6%-14.3	0% - 26.9%	NA
	Electro-Optical	0%-19%	6.9% - 38.5%	NA
Abhyankar 2009 [119]	Optical, electro-optical, and capacitive	NA	NA	13.85%
Plesh 2019 [224]	Optical	0.20%	13.8% - 18.35%	NA
Dynamic statistics (Chapter 4)	Optical	5%	26.60%	11.70%
	Thermal	5%	11%	22%
Dynamic Texture	**Optical**	**5%**	**1.11%**	**2.22%**
	Thermal	**5%**	**3.89%**	**4.92%**

5. 4. 5. Time Performance

Finally, we assess the computational cost of the selected feature extractors. The evaluation is conducted using the MATLAB source codes provided by the authors of the dynamic descriptors and the Statistics and Machine Learning Toolbox – MATLAB [234]. The used machine is a Dell XPS/15/9560 at 2.80 GHz CPU, 16 GB RAM, and Windows 10 Pro 64-bit operating system. The codes had not been optimized for our use case and executed to verify the PAD mechanism efficiency rather than the computational complexity, nevertheless, the analyses in this section give an insight into our experimental work.

We separately evaluate the feature extraction time for optical and thermal sensors in Table 5.9 and Figure 5.9.

Table 5.9. Average FE time for the thermal sensor.

FE method	GIST3D	VLBP	LBPTOP	VLPQ	LPQTOP
bins of FE histogram	34816	16384	768	1024	768
FE time (in seconds)	0.995	0.406	0.590	0.124	0.267

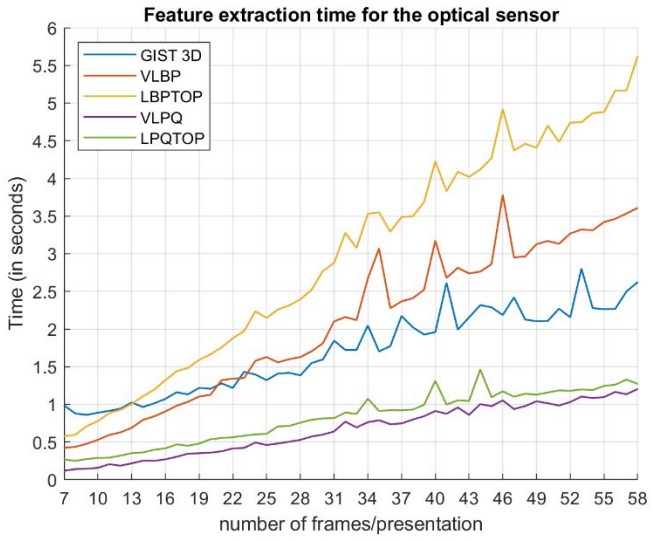


Figure 5.9. Average FE time for the optical sensor.

From Table 5.9 and Figure 5.9, we observe that computation time in 3-D frequency domain is significantly lower than that in 3-D spatial domain. Moreover, Figure 5.9 shows the influence of the presentation length, i.e. the number of frames per presentation, on computation time.

5. 5. CONCLUSIONS

In this chapter, we present a novel fingerprint PAD approach in the dynamic scenario. We propose three modes to investigate the spatio-temporal and spectral features in fingerprint videos. We utilize five dynamic feature extractors to leverage the fingerprint features in space and time, then a binary SVM is used for classifying bona fide and attack presentations.

The significance of the proposed approach is integrating the effect of natural fingerprint phenomena from the acquired video using dynamic descriptors, for instance, the intensity variation caused by the perspiration and pressure, and the ridge/valley pattern's formation caused by the 3-D form and elasticity of genuine fingerprints. Moreover, the approach has the capacity to detect anomalous patterns caused by the various PAI species, consequently, enhance the PAD subsystem's accuracy.

The local spatio-temporal features were extracted using VLBP and LBP-TOP. On the other hand, spectral features were explored locally using VLPQ and LPQ-TOP, and globally using GIST 3-D. These feature extractors are evaluated for thermal and optical sensors showing an advantage for the latter due to its acquisition characteristics.

The experiment points out the importance of studying each sensing technology apart by comparing (i) the accuracy of the different feature extractors, and (ii) the potential of the attack species on the two sensors. The best accuracy is obtained by LBP-TOP for the optical sensor with 1.11 BPCER20, and by LPQ-TOP for the thermal sensor with 3.89 BPCER20.

These results would seem to suggest that our approach has an excellent capability of eliminating/mitigating PAs in different sensing technologies. Further, a comparison with SoA mechanisms shows that our method provides competitive error rates. However, given the small number of participants in the database, caution must be taken.

Finally, it is noticed that feature extraction time is high when processing longer videos. However, these results were obtained in testing environment where the used software was implemented to validate the algorithms regardless the processing time. The processing time can be enhanced by utilizing adequate environment with optimized codes.

Chapter 6. The Impact of Pressure on Dynamic Fingerprint Features

6. 1. INTRODUCTION

As explained in earlier chapters, the fundamental research question in the development of novel PAD mechanisms concerns the distinct features that segregate genuine from malicious biometric traits. In other words, a robust PAD mechanism contributes to defining discriminative features from genuine and malicious traits for the purpose of eliminating those malicious attacks. Additional to answering "What are the distinct features?", the defined features are relied upon to reveal reliable interpretability which answers "Why those features are considered as distinguishing?".

In order to define the PAD features, let us revisit the elements (i.e. physical, behavioural, and logical) of the biometric presentation in the typical use case. The biometric presentation is performed by a *subject* who *interacts* voluntarily or involuntarily with a *biometric system* under a certain level of *supervision* and *instructions*. Any of these elements can be exploited for the purpose of collecting and analyzing additional information (i.e. PAD features) other than what is intended to be collected for biometric recognition.

Most of the current investigations in fingerprint PAD solutions focus on the differences between different types of presentations, i.e. bona fide and attacks, through static images. On the other hand, a few studies had been conducted to investigate the presentation itself considering different presentation scenarios. In this chapter, we propose a fingerprint PAD subsystem that exploits two of the presentation's elements: (1) presentation instruction, and (2) a software implementation that investigate the presented fingerprint/attack considering the provided instruction; as illustrated in Figure 6.1.

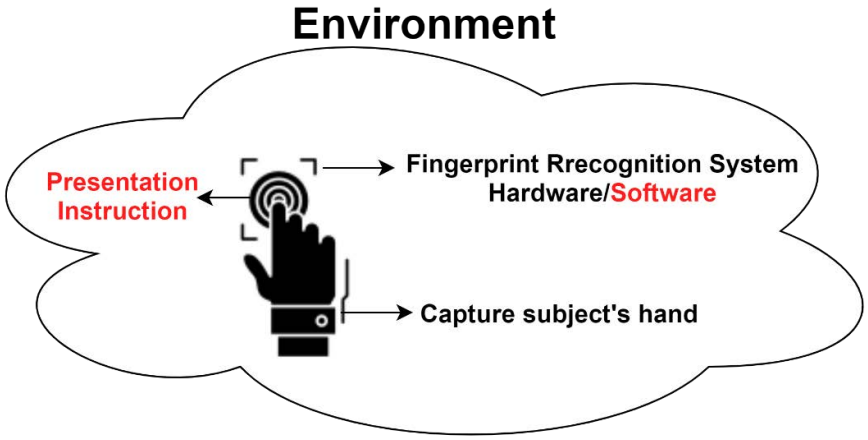


Figure 6.1. Elements of the fingerprint presentation in the typical use scenario.

I. Presentation instruction:

Presentation instructions, which might be referred to as *challenge-response* in the context of PAD, are used to trigger the biometric trait aiming to obtain a unique reaction pattern/s that, ideally, cannot be achieved by attacks. In this chapter, we investigate the influence of pressure on the fingerprint ridge/valley pattern by instructing the subjects to perform additional pressure during the fingerprint placement on the sensor's surface. The acquired presentation corresponds to the complete interaction between the finger and the sensor and is eventually captured as an uncompressed video. With this intention, different PAI species are selected to investigate their dynamic features under the defined instructions. Different attack species have been chosen to show different physical characteristics such as elasticity. The selected species includes very elastic material (e.g. gelatin and Play-Doh) and very rigid materials (e.g. white glue and nail polish) so that the dynamic variation and distortion are analyzed in both cases.

II. Software PAD subsystem:

After introducing additional information to the acquired fingerprint videos, a software PAD subsystem is required to extract decisive and interpretable features that validate the experiment's assumption and succeed in the task of attack detection. The proposed PAD algorithms in this chapter explore (a) the development of ridge/valley pattern in the captured video through examining the pattern's statistical variations in the consequent frames, (b) the dynamic texture in fingerprint videos so that the spatial fingerprint pattern is consolidated with the temporal changes, as shown in our previous work in fingerprint dynamics (Chapter 5). By exploiting these features, the PAD subsystem presents a countermeasure with certain efficiency as reported in the results.

The remaining of this chapter is organized as follows. Section 2 puts together the state-of-the-art investigations about dynamic fingerprint distortion and its application in PA. In Section 3, the proposed PAD subsystem is presented. Section 4 outlines the experimental protocols and report the experimental results. Finally, conclusions are drawn in Section 5.

6. 2. RELATED WORK

The clarity of a fingerprint image has a significant influence on the fingerprint matcher's performance. According to the NIST report on fingerprint image quality [235], fingerprint images that have clear and distinct ridges and valleys can positively affect the performance of an automatic fingerprint recognition system. However, multiple behavioural and/or physical factors, such as inadequate fingerprint presentation and skin conditions, may cause the acquired image to be less likely clear and distinct. In [236] the author discussed six attributes that characterize a good ridge quality, namely (1) sufficiently wide dynamic range, (2) even density distribution, (3) linearity, (4) no black or white saturation, (5) no significant blur or smudge, and (6) sufficient separation between ridges and valleys.

As stated above, an inadequate presentation may affect one or more of the six attributes, resulting in a challenge for the matching subsystem. This effect could be interpreted as a result of a fingerprint's inherent phenomenon. For instance, considering the internal bone position and skin elasticity, applying additional pressure during the fingerprint placement often cause linear and nonlinear distortions in the resulting ridge and valley pattern [237]. That can be perceived in the acquired image by thicker ridges, ridge flow distortion, black saturation, and less clarity. Additional examples of inadequate presentation include but are not limited to lack of usage knowledge/experience and intentional malicious behavior for the purpose of evading recognition.

Different attempts were conducted aiming to improve the robustness of fingerprint matching techniques considering inadequate presentations. Initial investigations such as [238] rely on the assumption that elastic distortion is a local issue, consequently, measuring local similarity between a distorted image and a fingerprint template would lead to better matching accuracy compared to measuring global similarity. The authors of [238] derived class by class matching networks using a neural classification network and the peak, width, and area components of the local Fourier transform achieving 90.9% matching accuracy.

In [239], the authors suggest that controlling the applied force during fingerprint placement at the sensor's surface leads to avoid distortion in the first place. The proposed method required: (1) an additional sensor that measures the force being applied at the sensor, and (2) adjusting the pressure level by examining cooperative and good quality images.

As mentioned by Cappelli [220], those aforementioned investigations tended to relax the definition of similarity aiming to consider small elastic deformations, but they had not attempted to model fingerprint distortion. For that reason, Cappelli et al. had carried out their experiment to cope with non-linear deformations of dynamic fingerprint acquisitions and proposed a fingerprint distortion function that is suitable for developing distortion-tolerant fingerprint matching algorithms.

A more recent investigation [240] proposes a fingerprint rectification system that estimates the center and the direction of the fingerprint, then it detects the distorted fingerprint, discovers the distorted pattern, and applies image transformation. Although this method proved a significant enhancement in the speed, the authors revealed some limitations related to the accuracy of pose estimation.

Initial studies in fingerprint PAD using the dynamic distortion followed the conclusions of [220]. A systematic study on skin distortion was conducted to analyze the distortion caused by the elasticity of human skin [221]. Based on the research observations, the experiment initially suggests that genuine fingerprints and PAIs cause different distortions since artificial fingerprints are more rigid, consequently cause lower distortion compared to genuine fingerprints. In their paper, the authors argue that even when a high elastic PAI specie is used to attack the system, it is very difficult to precisely emulate the distortion of genuine fingerprints since the behavior is identified with the manner in which the outside skin is anchored to the underlying derma and impacted by the position and state of the finger bone. In order to validate those assumptions, a dynamic dataset was collected using an optical sensor (high frame rate), with user instructions on

presenting the fingerprint with rotation and pressure. The evaluation included presentations from bona fide capture subjects and five PAI species (Table 6.1). For each presentation, the method computes the optical flow, Distortion map, and distortion code consecutively afterward compares the distortion codes to detect attacks.

Different from the latter technique, Zhang et al. used a Thin-Plate Spline (TSP) model to globally characterize fingerprint distortion and utilize this model to detect malicious presentations performed by PAI species [154]. The experiment relied on the same assumptions in [220] which state that genuine fingerprints produce a unique distortion pattern that is very difficult to be emulated by attack presentations. A different database was collected to assess the method including genuine fingerprint and silicon attack presentations. The database was collected under controlled presentation instructions where the fingerprint/PAI is placed on the sensor's surface, then pressure is applied in different directions. Under those conditions, the minutia movement represents the global distortion, and a sequence of paired minutia before and after distortion is used to calculate the parameters of the TPS model. The bending energy vector of the TPS model is utilized to distinguish bona fide from attack presentations.

Further analysis of fingerprint elasticity was performed by Jia et al. [153], analyzing the variations in the fingerprint area, intensity, and standard deviation. The variations in area and intensity were justified by the applied pressure and skin's moistness. The experiment had shown that genuine fingerprints have an increased size and intensity in the sequence while artifacts demonstrate a random fluctuation in intensity with increasing size for the area. On the other hand, the standard deviation feature characterizes the skin extension in x and y directions within the deformation process of the fingerprint pattern. The evaluation was reported using a dynamic dataset that was collected by a high frame rate capacitive sensor, while only a gelatin attack was performed. Fisher linear discriminant analysis is used to classify bona fide and attack presentations.

Table 6.1 shows a PAD comparison for the aforementioned methods by highlighting the methods' accuracy, sensing technologies, and used PAI species.

Table 6.1. Dynamic PAD mechanisms based on fingerprint deformation analysis.

Author	Technique	PAI species	Sensing technology	TEER (%)
Antonelli et al. [152]	Optical Flow	Gelatin, RTV silicon, white glue, and latex	Optical	11.24
Zhang et al. [154]	Thin-Plate Spline	Silicon	Optical	4.5
Jia et al. [153]	First Order Statistics	Gelatin	Capacitive	4.78

There is still considerable ambiguity with regard to the generalizability of some of the previous conclusions. First, dynamic fingerprint patterns comprise all of the natural phenomena of genuine fingerprints and not only an individual characteristic such as elasticity. Second, Experiments in [153], [154] were conducted using one PAI species, so conclusions are limited to those attacks and might not apply for other PAI species. Finally, even though the different PAI species have demonstrated different behaviors, other factors such as attacking tools and attacker's level of

expertise must be taken into account to completely characterize the interaction over the sensor's surface.

6. 3. PROPOSED METHOD

In this section, we demonstrate a fingerprint PAD mechanism that is particularly designed to investigate the dynamic distortion of fingerprint patterns under additional pressure during the presentation. The method relies on the fact that adding extra pressure during a genuine fingerprint presentation produces certain distortion which differs from that produced by various attack species.

In this scenario, where the solution is driven by the acquired data, the PAD solution is segmented into two folds (i) instructed data acquisition: the participants are given sufficient information about the style of performing a presentation by adding pressure while placing the fingertip at the sensor's surface, (ii) software algorithm/s used in the PAD subsystem to extract sufficiently discriminative features that classify bona fide and attack presentations.

The details of data acquisition were explained earlier in Section 3. 2, however, the next subsection demonstrates the software portion of the proposed PAD subsystem.

6. 3. 1. PAD SUBSYSTEM

In the context of this experiment, we investigate two feature extraction schemes, the first concerns the global variations in the fingerprint pattern while the second utilizes spatio-temporal descriptors to extract local and global features from space-time and spectral domains. After that, different machine learning algorithms are tested to select the classification algorithm with the highest accuracy. The PAD subsystem accuracy is characterized by the classifier's capability of correctly classifying bona fide and attack presentations. Although the subsystem may provide a significant capability of detecting some attack species, it may provide a medium or high portion of misclassified attacks from other species. Thus, a detailed analysis of the impact of different attack species on the PAD subsystem performance is shown in the results section.

6.3.1.1 FEATURE EXTRACTION APROACHES

6.3.1.1.1 DISTORTION-BASED FEATURES

This feature extractor analyzes the impact of pressure on the fingerprint ridge/valley dynamic-pattern considering both bona fide and attack presentations. Initially, several trials had been performed to visualize the development of the fingerprint/attack pattern and how additional pressure impact the pattern dynamics.

Consequently, assuming that each fingerprint presentation is a sequence of n frames $(F_i)_{i=1}^{n}$, i.e. $\{F_1, F_2,\ldots,F_n\}$, the following observations are perceived:

- In bona fide presentations, the image intensity is consistently increased as i increases. Specifically, once the pressure is performed the image intensity starts to increase very

rapidly resulting in a darker pattern, Figure 6.2 (a). Although pressure causes the rapid increment in the image intensity, it is equally important considering the other fingerprint's phenomena such as perspiration and elasticity;

- each PAI species shows a specific behavior during the PAI placement at the sensor. Therefore, each specie demonstrates a different reaction to the pressure depending on the PAI characteristics which are implied by the preparation recipe and used material/s Figure 6.2 (b-h);
- a slight shift takes place in the central region of the fingerprint pattern of genuine users after pressure, Figure 6.3 (a). Considering elastic and rigid PAI species, Figure 6.3 (b-c) demonstrate how the ridges/valley shift might be extreme in the gelatin presentation whilst excessively unnoticed in the polish nail attack;
- as successive frames in the fingerprint presentation represent the development of ridge/valley pattern, it is subjectively noticed that the similarity between the successive frames of bona fide presentations slightly varies when pressure is performed. On the contrary, using elastic materials such as Play-Doh and gelatin, the fingerprint pattern vanishes or degrades after applying pressure Figure 6.2 (b-g). On the other hand, rigid material such as white glue and polish nails, are likely to demonstrate consistent pattern while *i* increases, and contrary to bona fide and elastic materials, pressure may enhance the visual pattern in those attacks Figure 6.2 (c-e);
- despite the fact that attacks may imitate the fingerprint pattern at later frames in the presentation, it is noticed that the early frames show an anomalous development in the ridges/valley pattern Figure 6.2 (c-d,g-h); and,
- contrary to the latter observation, the size, ridges continuity, and contour's shape of bona fide presentations are developed homogeneously Figure 6.2 (a).

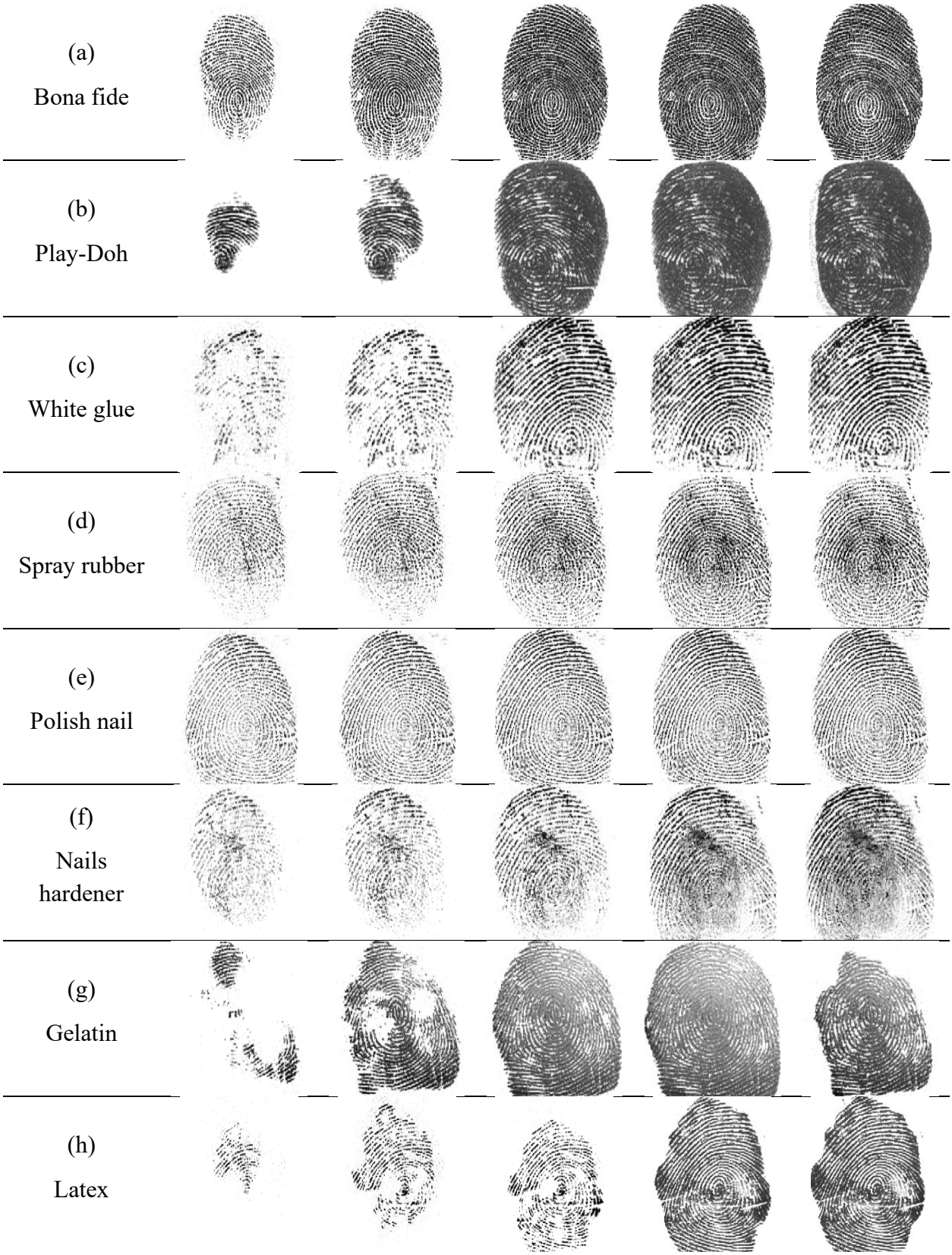


Figure 6.2. The influence of pressure in genuine and attack presentations. Frames are taken to demonstrate the variations at the beginning, mid, end of the presentation (left to right).

(a) Bona fide (b) Gelatin (c) Nail polish

Figure 6.3. The impact of pressure on the pattern shape. Each sub-image demonstrates two frames taken from a video and matched. Colors are: initial frame in green, later frame in magenta, and matching pattern in black.

Based on the hybrid subjective-objective observations and analysis, we propose an analysis scheme which investigates the development of fingerprint pattern during the placement on the sensor's surface.

Assume that fingerprint presentation is a sequence $(F_i)_{i=1}^{n}$, of n frames. The following steps are carried out (illustrated in Figure 6.4):

a. Select a reference frame F_r from the premier captured frames such that it includes the fingerprint pattern before applying pressure and provides an adequate extent for the comparison with the other frames in the sequence. To address these requirements, the image dimensions are experimentally determined to be above 75×75 pixels.
b. Segment the fingerprint pattern in all of the frames by isolating the background.
c. In a loop from i= 1:n, find the mutual area between F_i and F_r, and conduct a global comparison between the two frames in the mutual area. For instance, considering the structural similarity index SSIM as a comparison function, the feature vector that represents the sequence is $(SSIM_m)_{m=1}^{n-1}$. Figure 6.5 demonstrates the structural similarity feature vector for each presentation class. The SSIM values are computed based on the previous steps.
d. Extract the dynamic first order statistics from the input video to boost the video description. This step is carried out as shown in Chapter 4.
e. If required, apply interpolation and/or decimation to prepare the features to the machine learning model, shown in Chapter 4.
f. Create the output feature vector by concatenating the extracted features in the previous steps.

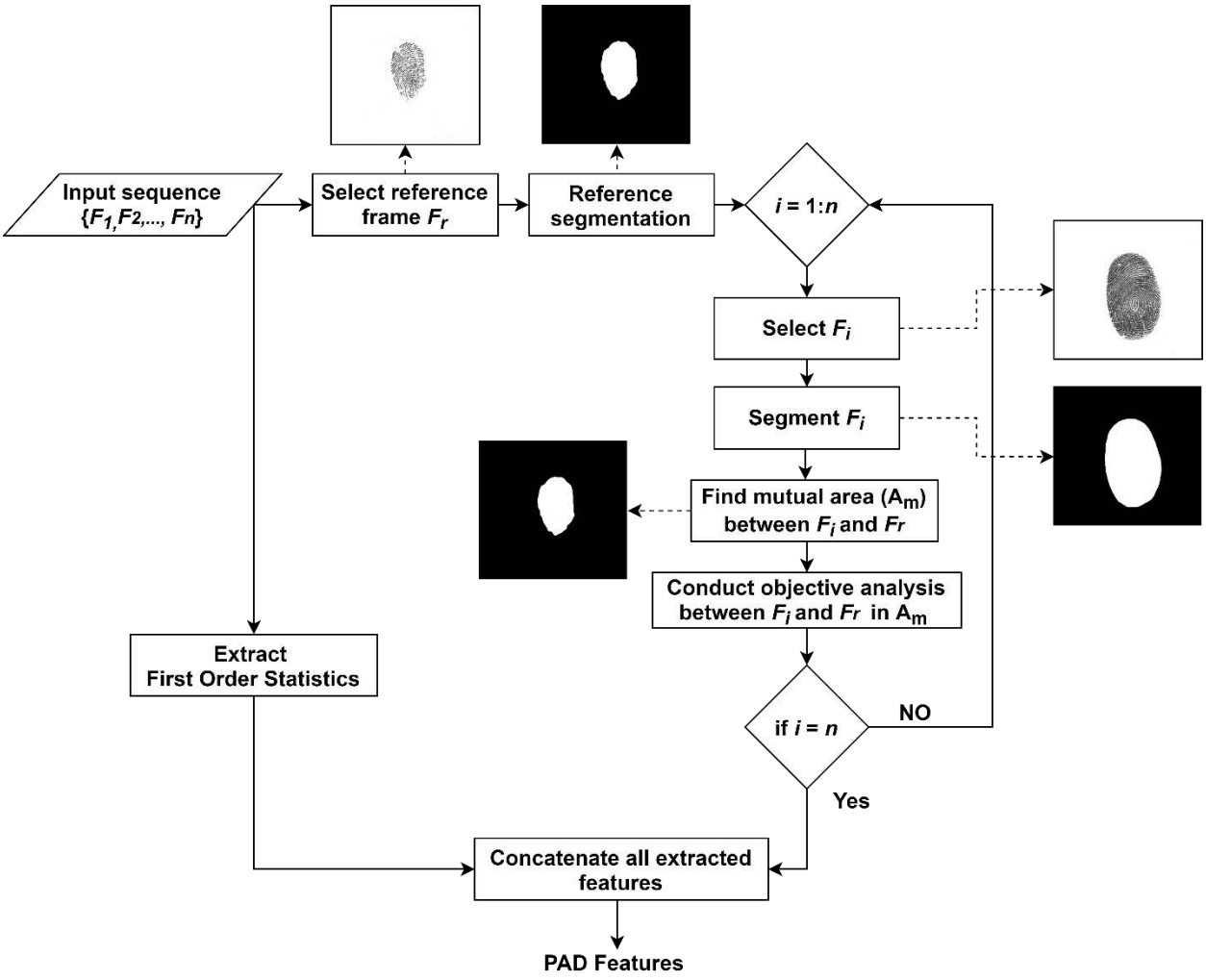


Figure 6.4. Objective analysis scheme for dynamic fingerprint distortion.

This scheme is inspired by the works in image distortion analysis where different methods had been proposed in the image processing literature to measure the statistical differences between a reference image and a distorted image [241], [242]. The proposed objective analysis is designed to represent the statistical variation in the dynamic fingerprint pattern as follows:

Let X be a reference image (i.e. F_r) and Y be an image from the same fingerprint presentation (i.e. F_i), then

1. Peak Signal to Noise Ratio ($PSNR$) measures the peak error between two images.

$$PSNR = 10\ log_{10}\left(\frac{R^2}{MSE}\right), \qquad 6.1$$

where R is the maximum fluctuation in the input image data type and MSE is calculated by:

$$MSE = \frac{\sum_{M,N}[X(m,n) - Y(m,n)]^2}{M \times N} \quad 6.2$$

2. Correlation coefficient (r) is a statistical measure that represents the relationship between two images.

$$r = \frac{\sum_m \sum_n (X_{mn} - \overline{X})(Y_{mn} - \overline{Y})}{\sqrt{(\sum_m \sum_n (X_{mn} - \overline{X})^2)(\sum_m \sum_n (Y_{mn} - \overline{Y})^2)}} \quad 6.3$$

3. Structural Similarity Index ($SSIM$) is a full reference perceptual metric that quantifies quality degradation between a reference and processed image. In the fingerprint sequence, image degradation is caused by the applied pressure during a presentation.
SSIM between images X and Y is calculated as follow:

$$SSIM(X,Y) = [l(X,Y)]^{\alpha} \cdot [c(X,Y)]^{\beta} \cdot [s(X,Y)]^{\gamma} \quad 6.4$$

where,

$$l(X,Y) = \frac{2\mu_X\mu_Y + C_1}{\mu_X^2 + \mu_Y^2 + C_1}, \quad 6.5$$

$$c(X,Y) = \frac{2\sigma_X\sigma_Y + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2}, \quad 6.6$$

$$s(X,Y) = \frac{\sigma_{XY} + C_3}{\sigma_X\sigma_Y + C_3} \quad 6.7$$

where μ_X, μ_Y are local means, σ_X, σ_Y are standard deviation, and σ_{XY} is the cross-covariance for the images.

4. Mutual Information is a measure of mutual dependence between two Images $X; Y$ equation 6.8. Explicitly, it quantifies the information obtained about one Image by observing another Image.

$$I(X;Y) = \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} P(x,y) \log \frac{P_{XY}(x,y)}{P_X(x)\, P_Y(y)} \quad 6.8$$

Where $P_{XY}(x,y)$ is the joint probability distribution, and $P_X(x)$,$P_Y(y)$ are the marginal distributions.

Finally, the defined four features (i.e. PSNR, r, SSIM, and I) in addition to the eight statistics introduced in [233], are combined to form the final PAD features. This mechanism is evaluated later to examine PAD classification performance.

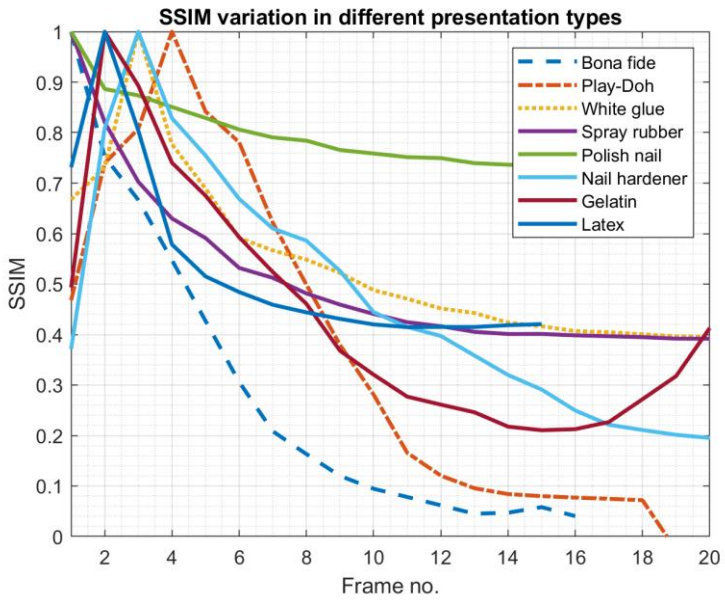


Figure 6.5. Illustration of $(SSIM_m)_{m=1}^{n-1}$ for a bona fide and 7 attack presentations. The presentations are acquired using the optical sensor.

6.3.1.1.2 SPATIO-TEMPORAL FEATURES

In our previous work (Chapter 5), dynamic texture has shown a high capacity to provide discriminative descriptions for dynamic fingerprint presentations. This section revisits the used feature extraction methods, namely: VLBP, LBP-TOP, VLPQ, LPQ-TOP, and GIST 3-D, and utilizes them as PAD feature extractors considering the database which includes the pressure scenario.

The previous conclusions state that those methods are capable of detecting the dynamic features of genuine fingerprints and the abnormal variations of attacks when fingerprint videos are investigated. Therefore, the dynamic pattern's variation caused by pressure is expected to provide additional discriminative features that improve the overall accuracy of the PAD subsystem.

6.3.1.2 CLASSIFICATION

Different classification methods were examined in a pre-experiment step to define the most efficient classifier. Specifically, we tested the following machine learning techniques (as explained in the Chapters 4 and 5): Classification Trees, Naive Bayes, Discriminant Analysis, SVM Classification, Nearest Neighbors, and Classification Ensembles. SVM classification has been chosen for our experiments due to its highest accuracy, while the other classifiers are not considered in the results part. Moreover, the impact of changing the SVM kernel was examined whereas the second-degree polynomial kernel demonstrated the best accuracy. A binary classification scheme is used to evaluate the PAD subsystem performance and to assess the influence of specific PAI species on system security and ease of use.

6. 4. EXPERIMENTAL RESULTS

This section aims to verify the validity of the proposed PAD mechanisms, knowing that the only difference between the proposed techniques is the feature extraction approach, as shown in Section 3.1.1. In the following subsections, the distortion-based and spatio-temporal features are analyzed through a set of experiments that illustrate the effectiveness of each approach. Accordingly, Section 4.1 explains the experimental protocols and highlights the used database/s at each experiment. Subsequently, the following five experiments were carried out to examine and assess the PAD mechanisms:

- *Experiment I* studies the fingerprint distortion-based features according to the defined method in section 6.3.1.1.1, taking into account the portion of the database with pressure;
- *Experiment II* investigates the spatio-temporal features as explained in section 6.3.1.1.2, considering the same database used in Experiment I;
- *Experiment III* carries out a PAD subsystem comparison when considering ordinary presentations and presentations with additional pressure;
- *Experiment IV* highlights the influence of sensing technology on the PAD mechanism; and,
- *Experiment V* demonstrates a comparison to the related works.

6. 4. 1. Experimental Protocols

In order to carry out the proposed experiments, the following protocols are provided to ensure obtaining reliable and comparable results.

1) Protocol I

The purpose of this protocol is to evaluate the proposed PAD mechanisms in section 6.3.1.1 by conducting Experiments I and II. We thus utilize the database in Section 3. 2, which was collected to investigate the influence of pressure on bona fide and attack presentations, to validate the proposed PAD mechanisms. In all of the corresponding experiments, each sensor's data is studied individually because of the differences between the acquired data, i.e frame rate, image size, resolution, noise, etc. Then sensors' data are divided into 55% training set and 45% testing set, as shown in Figure 6.6. The division is performed by randomizing capture subjects such that all the presentations (bona fide and attacks) of an independent capture subject are either in the training or testing data. The randomization of partitioning is performed to ensure that the machine learning model has never seen presentations that correspond to the tested capture subjects in the training phase. Finally, the PAD subsystem is evaluated through performing the PAD feature extraction, training/testing the PAD classifier, and assessing the obtained results following the evaluation methodology.

2) Protocol II

The aim of the second protocol is to compare the PAD performance of the proposed mechanisms in the scenarios of ordinary presentations and presentations with pressure. The comparison is performed in two phases:

(i) Accuracy comparison: we apply the steps of protocol I to the database in Section 3. 2 which includes ordinary fingerprint presentations, then we compare the results to those obtained in Experiments I-II

(ii) Generalizability comparison: in order to test the mechanisms' generalizability, we perform 'leave-one-out' cross-validation to the machine learning model. The cross-validation is performed for each sensor individually for the reason mentioned in protocol I. Then each sensor's data is split into *k* folds, where *k* represents the number of individual capture subjects. The learning algorithm is performed *k* times by taking one capture subject as a testing set and all other capture subjects as a training set, Figure 6.7. At each testing phase, the PAD subsystem is evaluated, and results are reported. Once the cross-validation is done, results are demonstrated.

Table 6.2 summarizes the proposed experiments, the corresponding protocol and database, and the experiment objective. The results of the first two experiments show a higher accuracy for the spatio-temporal feature extractors, thus the rest of the experiments are conducted considering those features. Additionally, experiments IV-V are conducted by exploiting the results from experiments I-III and previous results in Chapter 5.

Table 6.2. Summary of the proposed experiments.

Experiment	Feature extraction technique/s	Protocol	Database	Validation strategy	Objective
I	Distortion-based features	Protocol I	Pressure	Hold-out validation	Examine the PAD scheme in Figure 6.4
II	VLBP, LBP-TOP, VLPQ, LPQ-TOP, and GIST 3-D	Protocol I	Pressure	Hold-out validation	Examine the PAD accuracy using Spatio-temporal feature extractors
III		Protocol II	Ordinary + Pressure	Cross-validation	Compare the PAD accuracy considering pressure and ordinary scenarios
IV		Protocol I	Pressure	Hold-out validation	Examine the impact of sensors
V		Protocol I	Pressure	Hold-out validation	Comparison with SoA

(a) Training set

(b) Testing set

Figure 6.6. Data partitioning in Protocol I.

(a) Training set

(b) Testing set

Figure 6.7. Data partitioning in leave-one-out cross-validation.

6. 4. 2. Experiment I: Dynamic Fingerprint Pattern Analysis

In this subsection, we apply the pressure database to the scheme in Figure 6.4 in order to extract the distortion-based PAD features. After that, we carry out Protocol I for the extracted features and utilize a binary SVM model to classify presentations. The results are reported based on the evaluation methodology in Section 3. 1.

The PAD subsystem performance is illustrated in Figure 6.8 as a comparison between the obtained DET curves for the optical and thermal sensors. Moreover, Table 6.3 assesses the PAD subsystem performance as a measure of BPCER at different values of APCER. Since binary classification is applied, APCER in Figure 6.8 and Table 6.3 implicitly refers to the proportion of all attack species which were misclassified as bone fide presentations. Further analysis is performed to the obtained results to demonstrate the influence of PAI species on the PAD performance (Table 6.4).

Although the PAD accuracy for the optical sensor is significantly higher than the thermal sensor at low APCER values. The DET curves converge and equalize at TEER = 11%, after that, the mechanism's accuracy shows a slight advantage for the thermal sensor. Additionally, Table 6.4 breaks down the total APCER demonstrating the mechanism's capability of detecting attacks considering the different technologies; the results are reported at fixed $APCER_{Total} = 5\%$. Although the mechanism generally performs better for the optical sensor, all attack species succeeded with the least $APCER_{PAI} = 2.22\%$ for white glue and gelatin attacks. On the other hand, attacks with spray rubber, nails hardener, and latex were rejected by the PAD mechanism for the thermal sensor reporting $APCER_{PAI} = 0\%$ for these species. Nevertheless, white glue species has achieved APCER 25.56% for the thermal sensor and 2.22% for the optical sensor.

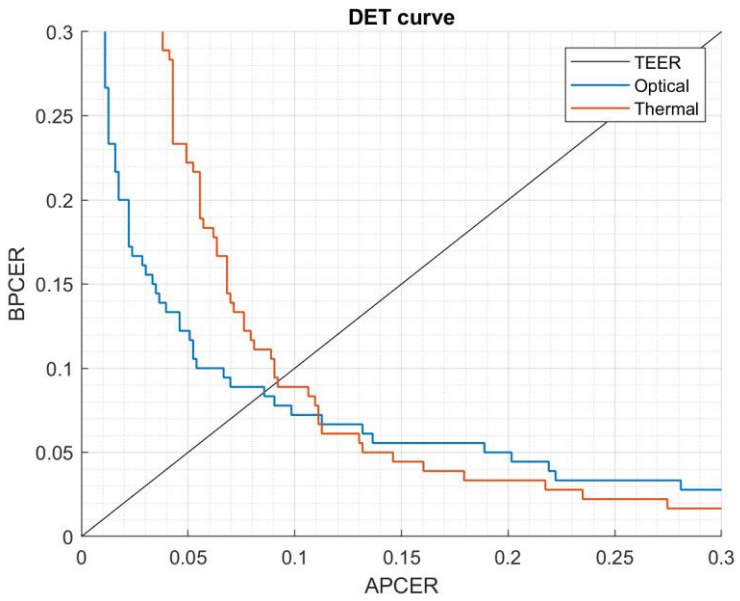


Figure 6.8. PAD subsystem DET curves using the distortion features.

Table 6.3. PAD subsystem accuracy as BPCER at different APCER values.

Sensor	BPCER% @		
	APCER = 5%	**APCER = 2.5%**	**TEER**
Optical	12.22%	16.67%	8.57%
Thermal	22.22%	46.11%	9.21%

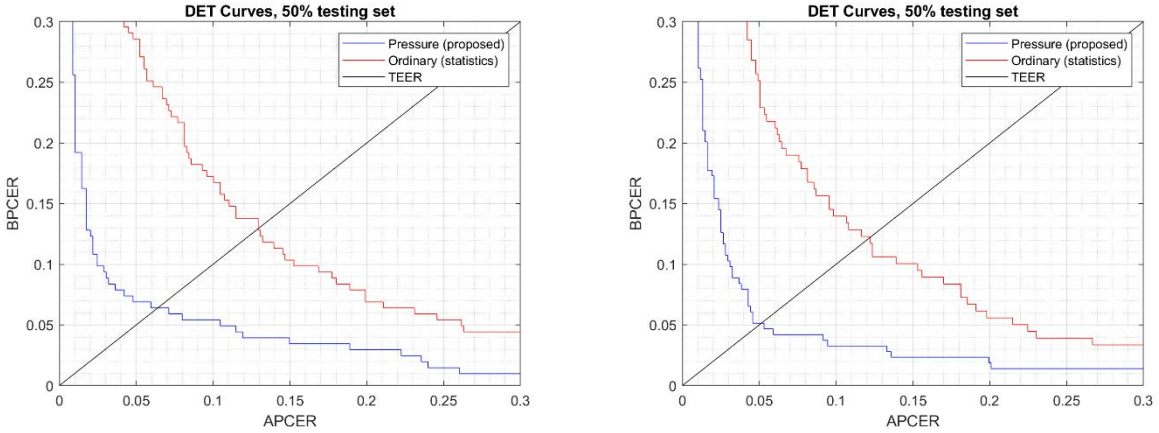
Table 6.4. Analyzing 5% APCERtotal into $APCER_{PAI}$.

Sensor	$APCER_{PAI}$ (%)						
	Play-Doh	**White glue**	**Spray rubber**	**Polish nail**	**Nails hardener**	**Gelatin**	**Latex**
Optical	3.33%	2.22%	7.78%	3.33%	7.78%	2.22%	6.67%
Thermal	5.56%	25.56%	**0.00%**	1.11%	**0.00%**	2.22%	**0.00%**

These results are obtained through a data partitioning protocol that differs from the experimental protocol used in Chapter 4. In this experiment, the partitioning is randomized by the capture subjects while in Chapter 4 it was k-folds cross-validation, therefore, a direct comparison will not be coherent. In order to compare the presented algorithm with that proposed in Chapter 4, we apply cross-validation data partitioning to the pressure dataset then we train an SVM model in the same fashion presented in Chapter 4; results are shown in Figure 6.9.

Two main observations are perceived from Figure 6.9. First, the proposed algorithm in this chapter provides a significant accuracy improvement compared to the results of the dynamic statistics using ordinary presentations; illustrated by the DET curves. Secondly, it is noticed that the same algorithm and the same data provide different results when applying different partitioning protocols. It is evident that partitioning the database considering each fingerprint video as an

independent observation (Figure 6.9) provides higher accuracy than considering the partitioning by randomizing the capture subjects (shown in Figure 6.8).



(a) Optical sensor (b) Thermal sensor

Figure 6.9. DET curves comparison between the proposed algorithm (presentation with pressure) and the dynamic statistics (ordinary presentation).

6. 4. 3. Experiment II: Fingerprint Dynamic Texture

This experiment aims to investigate the dynamic fingerprint texture, specifically caused by pressure, as PAD features. The experiment is conducted through the following steps:

- Apply protocol I to manage the data division;
- utilize the dynamic texture methods which were explored in Chapter 5 as the PAD feature extractors;
- utilize a binary SVM classification model with a second-degree polynomial kernel, as the PAD classifier;
- perform PAD subsystem evaluation, as demonstrated in Chapter 3, considering all PAD feature extraction methods.

The classification accuracy of the proposed PAD mechanism, using all feature extractors and different parameters, is reported as BPCER at APCER=5% and APCER = 2.5% in Figure 6.10. Moreover, The PAD testing scores are expressed as functions of the decision threshold, i.e. DET curves, considering all feature extraction algorithms in Figure 6.11 and Figure 6.12.

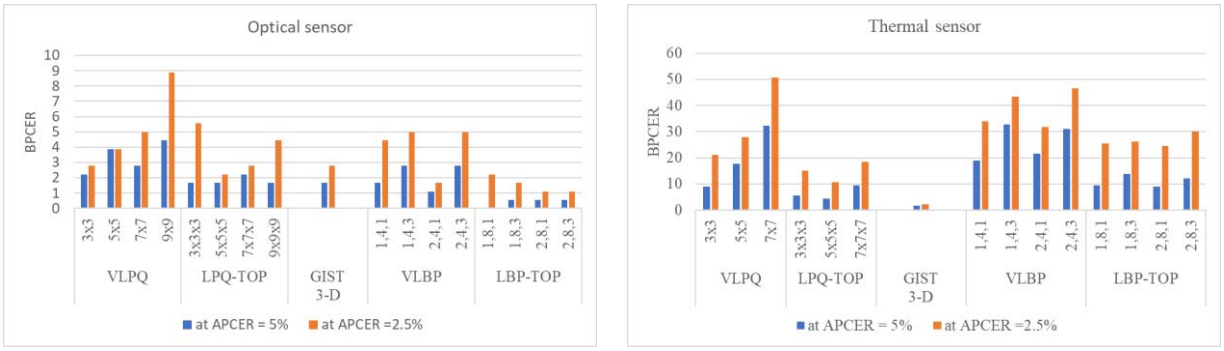
The most desirable result to emerge from the figures is achieving low values for the pair (APCER|BPCER). For instance, at 5% APCER, BPCER values are 0% for the optical sensor using LBP-TOP$_{1,8,1}$, and 1.66% for the thermal sensor using GIST 3-D. While at 2.5% APCER, BPCER values are: 1.11% for the optical sensor using LBP-TOP$_{2,8,1}$ and 2.22% for the thermal sensor using GIST 3-D.

In order to examine the PAD subsystem capability of detecting different PAI species, APCER$_{PAI}$ for the seven attack species is reported at APCER$_{total}$ = 5% in Table 6.5 and Table 6.6. In other

words, the tables list the distribution of 5% $APCER_{total}$ on the seven PAI species. It is interesting to note that despite the similarity in DET curves, the $APCER_{PAI}$ distribution might differ notably. For example, considering the optical sensor, the spray rubber species has an APCER = 2.22% when $VLPQ_{3x3}$ is utilized, however, APCER raises to 18.89% using $VLPQ_{9x9}$.

The $APCER_{PAI}$ distribution confirms a significant difference in the PAD subsystem vulnerability to the different attack species. Meaning that the PAD subsystem, at a certain threshold, might have the capacity of eliminating some PAI species as shown in Table 6.5 and Table 6.6, nevertheless, the results demonstrate its vulnerability to other species.

These results significantly vary from the previous results reported in Experiment I. For both sensing technologies, PAD using spatio-temporal features had been able to obtain BPCER values lower than 2.5% at APCER = 2.5%. This implies that both security and ease of use aspects have been achieved without the need to compromise one over the other, as the case in the distortion based features. These differences can be accounted for by the fact that spatio-temporal feature extractors utilize local features from 3-D samples, whereas distortion based features are designed in a fashion that extracts global image features. Consequently, the following experiments further investigate the effectiveness and generalizability of spatio-temporal features.



(a) (b)

Figure 6.10. BPCER (%) results for the five feature extractors. The scale of y- axis is adjusted for each figure for better visualization to the obtained error rates.

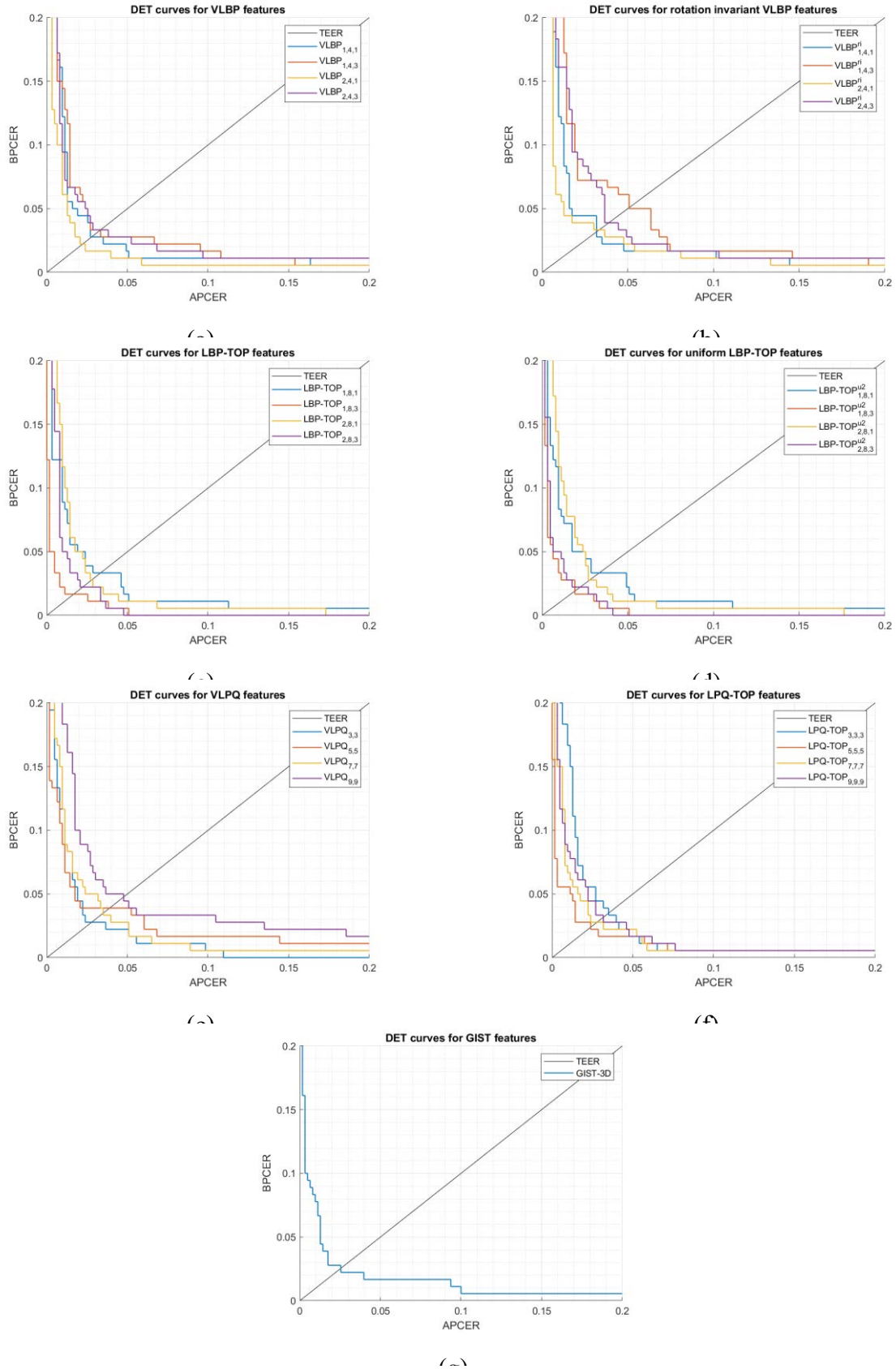


Figure 6.11. DET curves for the five feature extractors (optical sensor).

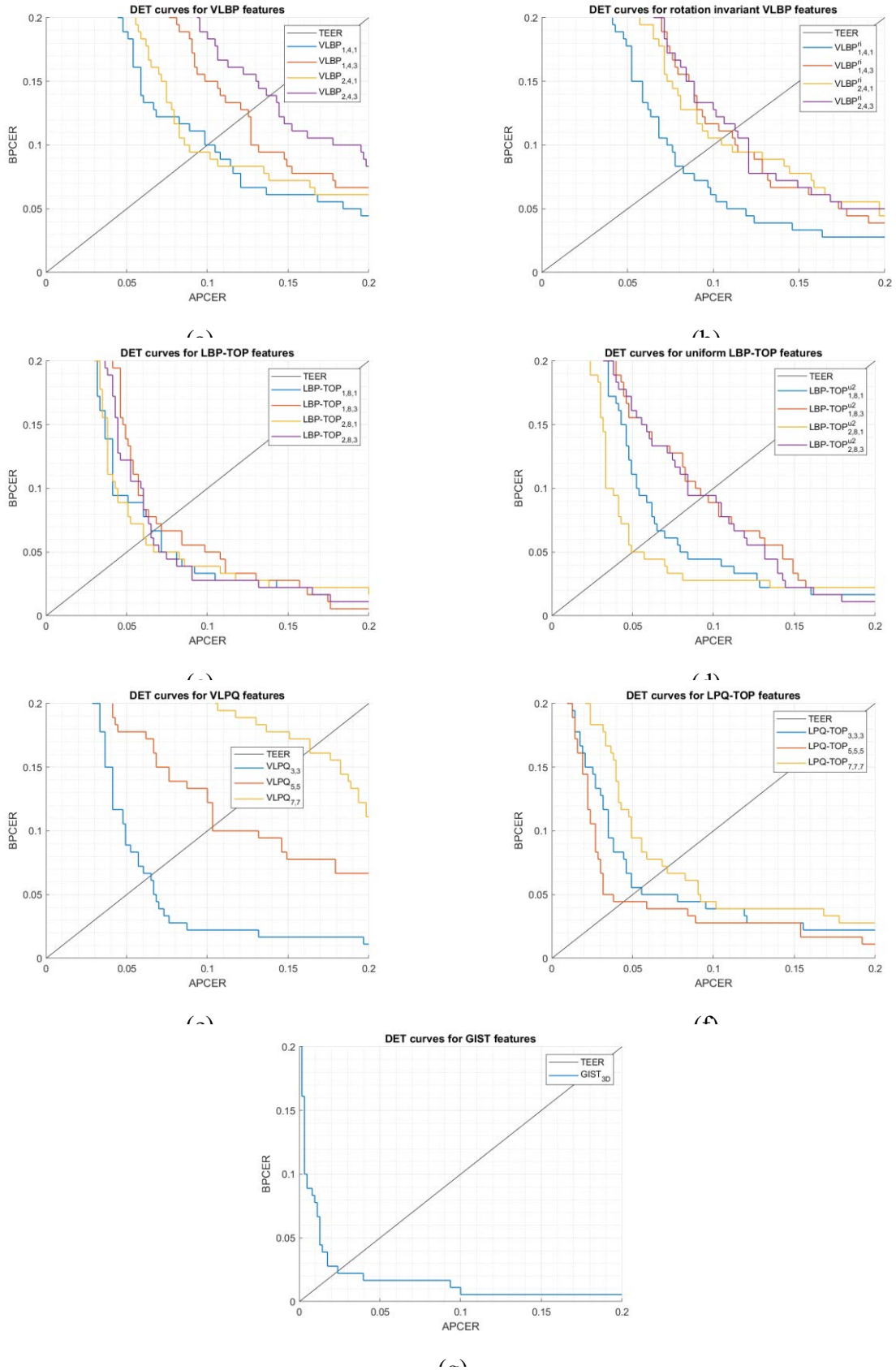


Figure 6.12. DET curves for the five feature extractors (thermal sensor).

Table 6.5. $APCER_{PAI}$ for the optical sensor.

Feature extractor	$APCER_{PAI}$ (%)						
	Play-Doh	White glue	Spray rubber	Polish nail	Nails hardener	Gelatin	Latex
$VLPQ_{3x3}$	1.11	5.56	2.22	2.22	3.33	5.56	13.33
$VLPQ_{5x5}$	3.33	6.67	5.56	2.22	3.33	4.44	7.78
$VLPQ_{7x7}$	3.33	3.33	12.22	1.11	**0.00**	3.33	10.00
$VLPQ_{9x9}$	2.22	**0.00**	18.89	**0.00**	**0.00**	4.44	7.78
$LPQ\text{-}TOP_{3x3x3}$	2.22	7.78	3.33	2.22	2.22	5.56	10.00
$LPQ\text{-}TOP_{5x5x5}$	2.22	5.56	6.67	1.11	6.67	3.33	7.78
$LPQ\text{-}TOP_{7x7x7}$	2.22	7.78	6.67	1.11	3.33	4.44	7.78
$LPQ\text{-}TOP_{9x9x9}$	2.22	10.00	5.56	0.00	1.11	4.44	10.00
GIST 3-D	3.33	5.56	6.67	1.11	**0.00**	4.44	12.22
$VLBP_{1,4,1}$	3.33	5.56	5.56	3.33	10.00	6.67	**0.00**
$VLBP_{1,4,3}$	**0.00**	4.44	2.22	4.44	20.00	2.22	**0.00**
$VLBP_{2,4,1}$	6.67	2.22	2.22	2.22	7.78	8.89	3.33
$VLBP_{2,4,3}$	1.11	4.44	2.22	1.11	13.33	10.00	1.11
$VLBP^{ri}_{1,4,1}$	2.22	6.67	5.56	4.44	12.22	1.11	1.11
$VLBP^{ri}_{1,4,3}$	**0.00**	6.67	3.33	3.33	15.56	3.33	1.11
$VLBP^{ri}_{2,4,1}$	4.44	4.44	4.44	3.33	8.89	3.33	4.44
$VLBP^{ri}_{2,4,3}$	2.22	4.44	3.33	3.33	12.22	6.67	2.22
$LBP\text{-}TOP_{1,8,1}$	6.67	4.44	3.33	2.22	4.44	10.00	2.22
$LBP\text{-}TOP_{1,8,3}$	4.44	7.78	8.89	2.22	5.56	3.33	1.11
$LBP\text{-}TOP_{2,8,1}$	4.44	5.56	4.44	1.11	4.44	8.89	4.44
$LBP\text{-}TOP_{2,8,3}$	5.56	7.78	2.22	4.44	6.67	3.33	3.33
$LBP\text{-}TOP^{u2}_{1,8,1}$	5.56	4.44	4.44	2.22	4.44	6.67	6.67
$LBP\text{-}TOP^{u2}_{1,8,3}$	6.67	5.56	4.44	4.44	6.67	3.33	2.22
$LBP\text{-}TOP^{u2}_{2,8,1}$	5.56	4.44	2.22	2.22	5.56	7.78	5.56
$LBP\text{-}TOP^{u2}_{2,8,3}$	3.33	6.67	2.22	6.67	7.78	6.67	**0.00**

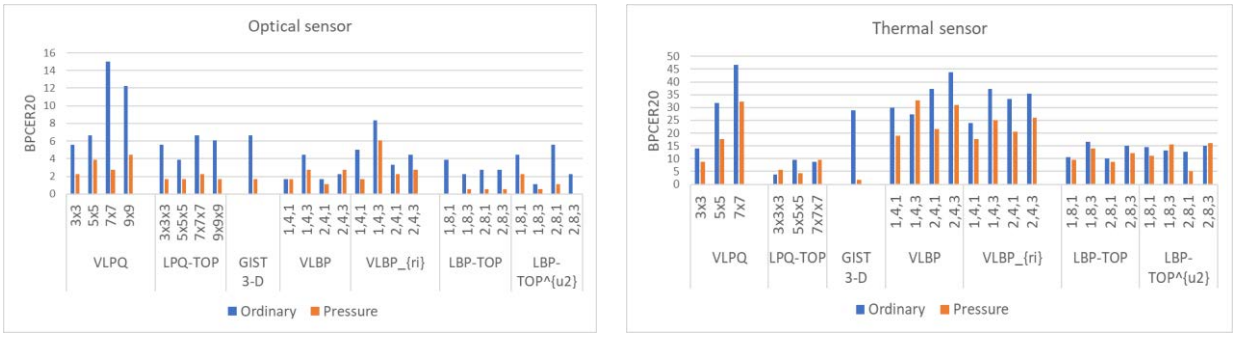
Table 6.6. $APCER_{PAI}$ for the thermal sensor.

Feature extractor	$APCER_{PAI}$ (%)						
	PlayDoh	White glue	Spray rubber	Polish nail	Nails hardener	Gelatin	Latex
$VLPQ_{3x3}$	1.11	32.22	**0.00**	1.11	**0.00**	**0.00**	**0.00**
$VLPQ_{5x5}$	2.22	26.67	**0.00**	1.11	**0.00**	2.22	1.11
$VLPQ_{7x7}$	4.44	7.78	1.11	2.22	3.33	3.33	12.22
$LPQ\text{-}TOP_{3x3x3}$	1.11	28.89	4.44	**0.00**	**0.00**	**0.00**	**0.00**
$LPQ\text{-}TOP_{5x5x5}$	2.22	25.56	2.22	**0.00**	**0.00**	**0.00**	3.33
$LPQ\text{-}TOP_{7x7x7}$	2.22	20.00	2.22	2.22	**0.00**	**0.00**	7.78
GIST 3-D	3.33	5.56	6.67	1.11	**0.00**	4.44	12.22
$VLBP_{1,4,1}$	5.56	27.78	**0.00**	**0.00**	**0.00**	**0.00**	1.11
$VLBP_{1,4,3}$	1.11	28.89	2.22	1.11	**0.00**	**0.00**	1.11
$VLBP_{2,4,1}$	3.33	30.00	**0.00**	**0.00**	**0.00**	1.11	**0.00**
$VLBP_{2,4,3}$	1.11	25.56	4.44	1.11	1.11	**0.00**	1.11
$VLBP^{ri}_{1,4,1}$	3.33	26.67	3.33	**0.00**	**0.00**	**0.00**	1.11
$VLBP^{ri}_{1,4,3}$	1.11	22.22	10.00	**0.00**	**0.00**	**0.00**	1.11
$VLBP^{ri}_{2,4,1}$	3.33	28.89	2.22	**0.00**	**0.00**	**0.00**	**0.00**
$VLBP^{ri}_{2,4,3}$	1.11	21.11	8.89	1.11	**0.00**	**0.00**	2.22
$LBP\text{-}TOP_{1,8,1}$	2.22	28.89	2.22	**0.00**	**0.00**	**0.00**	**0.00**
$LBP\text{-}TOP_{1,8,3}$	1.11	30.00	2.22	**0.00**	**0.00**	**0.00**	1.11
$LBP\text{-}TOP_{2,8,1}$	3.33	26.67	2.22	**0.00**	**0.00**	**0.00**	1.11
$LBP\text{-}TOP_{2,8,3}$	1.11	26.67	4.44	**0.00**	**0.00**	**0.00**	1.11
$LBP\text{-}TOP^{u2}_{1,8,1}$	1.11	31.11	1.11	**0.00**	1.11	**0.00**	**0.00**
$LBP\text{-}TOP^{u2}_{1,8,3}$	2.22	27.78	1.11	**0.00**	1.11	**0.00**	2.22
$LBP\text{-}TOP^{u2}_{2,8,1}$	2.22	31.11	**0.00**	**0.00**	1.11	**0.00**	**0.00**
$LBP\text{-}TOP^{u2}_{2,8,3}$	3.33	24.44	1.11	2.22	**0.00**	1.11	2.22

6. 4. 4. Experiment III: The Influence of Pressure on the PAD Subsystem Accuracy

1) PAD Subsystem Accuracy: Pressure Versus Ordinary Presentations

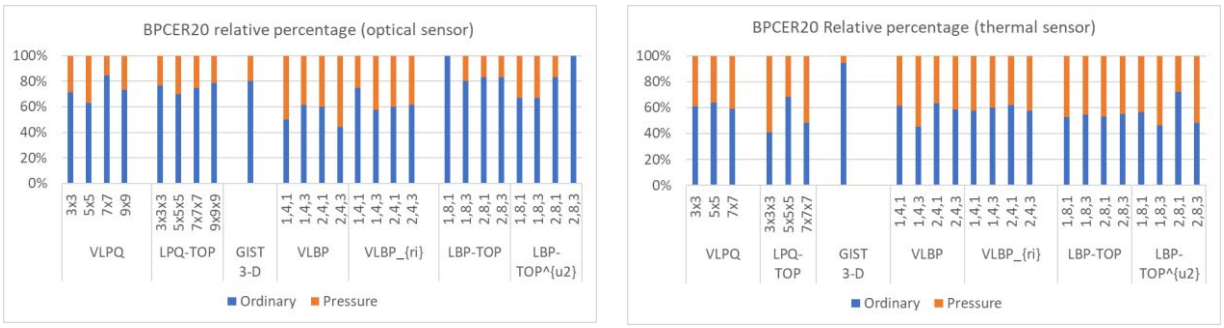
In order to identify the influence of pressure on the PAD subsystem accuracy, BPCER20 is used to compare the PAD subsystem accuracy considering the scenarios of ordinary presentations and presentations with pressure. The error rates, reported in Chapter 5 for ordinary presentation and in the previous experiment for presentations with pressure, are shown in Figure 6.13 to compare the PAD subsystem accuracy for both scenarios.



(a) (b)

Figure 6.13. Scenario comparison for the proposed PAD subsystem considering the 5 feature extractors.

Figure 6.14 illustrates the relative BPCER20 percentage of pressure and ordinary scenarios taking into account the sensing technology and feature extraction method.

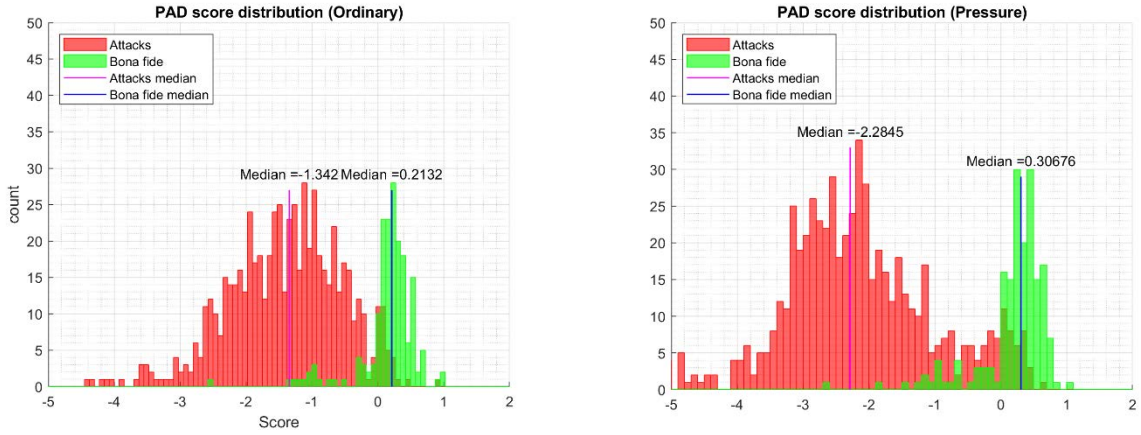


(a) (b)

Figure 6.14. Relative comparison for the proposed PAD subsystem considering the 5 feature extractors.

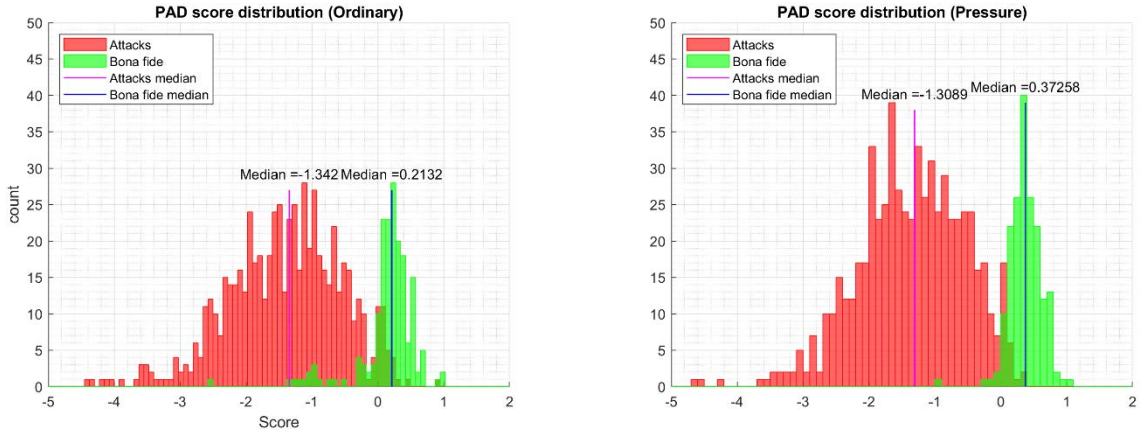
The majority of tests in Figure 6.13 and Figure 6.14 reveal that additional finger pressure during the presentation results in a reduction in BPCER20. This reduction could be significantly large as noticed when examining the PAD subsystem using GIST 3-D descriptor, where the BPCER was reduced over 80% for both sensors. On the other hand, a few tests in the figure show an advantage for ordinary presentations. Those scenarios are further investigated in the next subsection.

The most intriguing observation to emerge from Figure 6.13 and Figure 6.14 is the significant accuracy enhancement when using $VLPQ_{7\times7}$ for the optical sensor and GIST 3-D for the thermal sensor. Thus, Figure 6.15 and Figure 6.16 demonstrate the score distributions for bona fide and attack presentations considering both cases. The influence of pressure can be simply noticed by comparing the median values for attacks, and the median values for bona fide. Considering the optical sensor, the median of attacks dropped from -1.34 to -2.28 and the median of bona fide increased from 0.21 to 0.30. On the other hand, the thermal sensor does not show a noticeable change in the median of attacks but the median of bona fide increased from 0.21 to 0.37. Another interpretation can be seen by the decreased misclassified presentations when pressure is considered.



(a) Ordinary presentations database (b) Pressure presentations database

Figure 6.15. : PAD scores distribution for the optical sensor using $VLPQ_{7\times7}$ features.



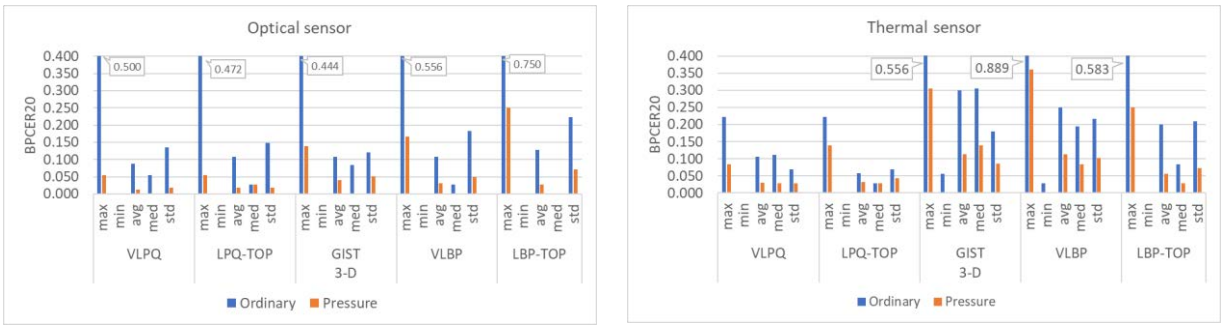
(a) Ordinary presentations database (b) Pressure presentations database

Figure 6.16. PAD scores distribution for the thermal sensor using GIST 3-D features.

2) PAD Subsystem Generalizability: Pressure Versus Ordinary Presentations

To assess the PAD subsystem generalizability, the second part of Protocol II is applied. Accordingly, leave-one-out cross-validation model is applied for each scenario considering all feature extractors. considering the data division in Figure 6.7, each combination between a scenario and feature extraction method is evaluated 11 times; once for each fold. To describe each cross-validation model from 11 testing sets, let us assume that $(BPCER20_i)_{i=1}^{11}$ is the sequence of error rates, where i is the fold number. The vector $BPCER20_i$ is analyzed by showing: (i) minimum, (ii) maximum, (iii) mean, (iv) median, and (v) standard deviation values.

Figure 6.17 highlights the differences between those statistics by showing BPCER20 for the best (i.e. min. BPCER20) and worst (i.e. max. BPCER20) testing folds, and how the BPCER20 is distributed with respect to the average value using the median value. Moreover, the stability of a model is implied by the standard deviation values. In other words, a low average with low disparity confirms higher generalizability for the tested model.



(a) (b)

Figure 6.17. The influence of pressure on the PAD subsystem efficiency. Unshown bars refer to the value 0.

As can be seen from Figure 6.17, the differences between the max BPCER20 values are remarkable when comparing the pressure and ordinary scenarios. The best improvement is achieved considering VLPQ for the optical sensor, where BPCER20 is reduced from 50% to approximately 5%, i.e. BPCER20 is 10 times less for the pressure scenario. In addition, the average, median, and standard deviation values are reduced for all feature extractors for the pressure scenario. This implies a lower range of disparity at a lower average value for BPCER20.

The findings of this experiment emphasize the validity of the proposed model when it is compared to ordinary dynamic presentations. Primarily, significant enhancement in the PAD subsystem accuracy was obtained using the same sensors, feature extractors, and evaluation methodology. Furthermore, the proposed model illustrated lower error rate variance when each independent captured subject was tested individually, demonstrated in Figure 6.17.

The observed enhancement in the accuracy, shown in Figure 6.15 and Figure 6.16, is in line with the initial assumption which claims that fingerprint pressure produces more distinctive dynamic features that allow differentiating bona fide from attack presentations. On the other hand, the

stability of the PAD model, which was confirmed by the leave-one-out cross validation, could be interpreted as being a result of obtaining more generic features that are less dependent on certain differences between capture subjects.

6. 4. 5. Experiment IV: The Influence of Sensing Technology

This experiment points out the influence of the tested sensing technologies on the proposed PAD subsystem efficiency. The comparison focuses on two main aspects:

I. The overall PAD mechanism accuracy is determined using BPCER at fixed APCER values. Hence, the most effective feature extractors are selected, then the sensors are compared using BPCER20, Figure 6.18, and Figure 6.19.

II. The mechanism's capability of eliminating specific PAI species. The comparison is carried out by determining the number of eliminated PAI species considering the different sensors and feature extractors, Figure 6.20.

The comparison here is not as straightforward as it seems. Even though the optical sensor is demonstrating a higher accuracy in part of the DET curves, the PAD mechanism has shown the vulnerability to all attack species, and in its best case, the PAD mechanism rejected two species. On the other hand, utilizing the PAD mechanism at the thermal sensor had proven a higher capability to reject more attack species, where four PAI species were rejected using VLBP, LBP-TOP, VLPQ, and LPQ-TOP features.

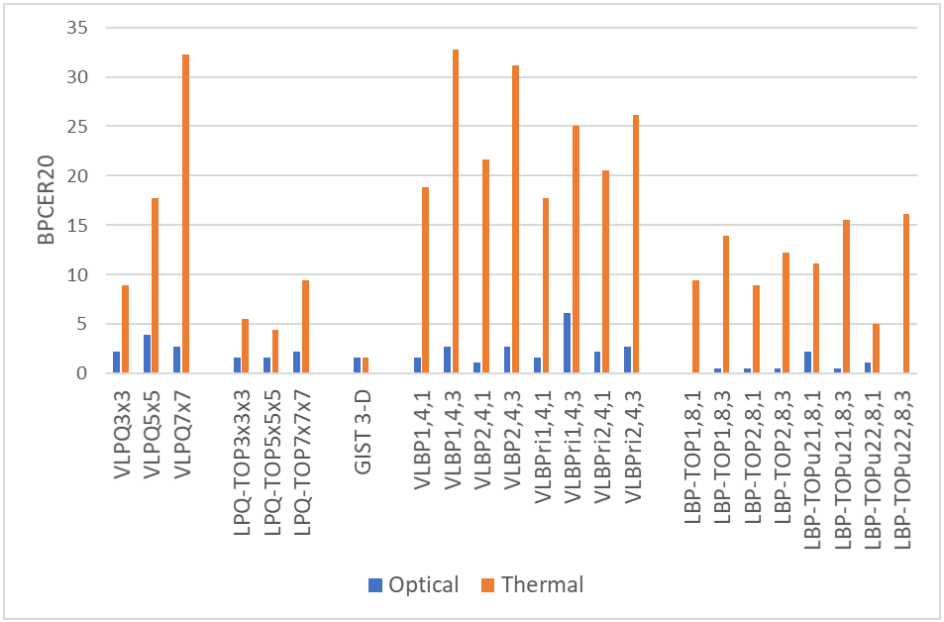


Figure 6.18. PAD accuracy for the two sensors in terms of BPCER20.

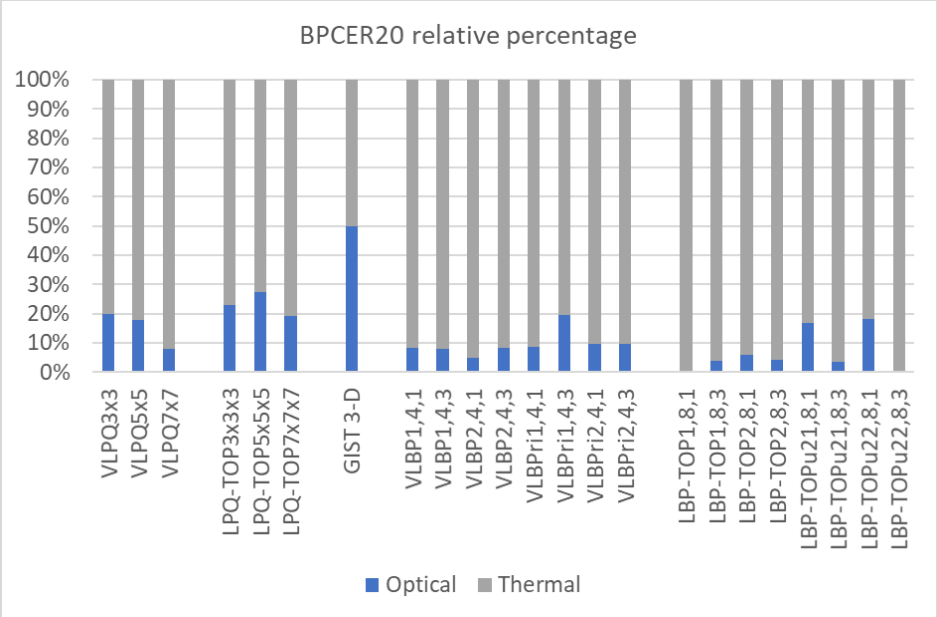


Figure 6.19. Relative comparison between the PAD accuracy using optical and thermal technologies in terms of BPCER20.

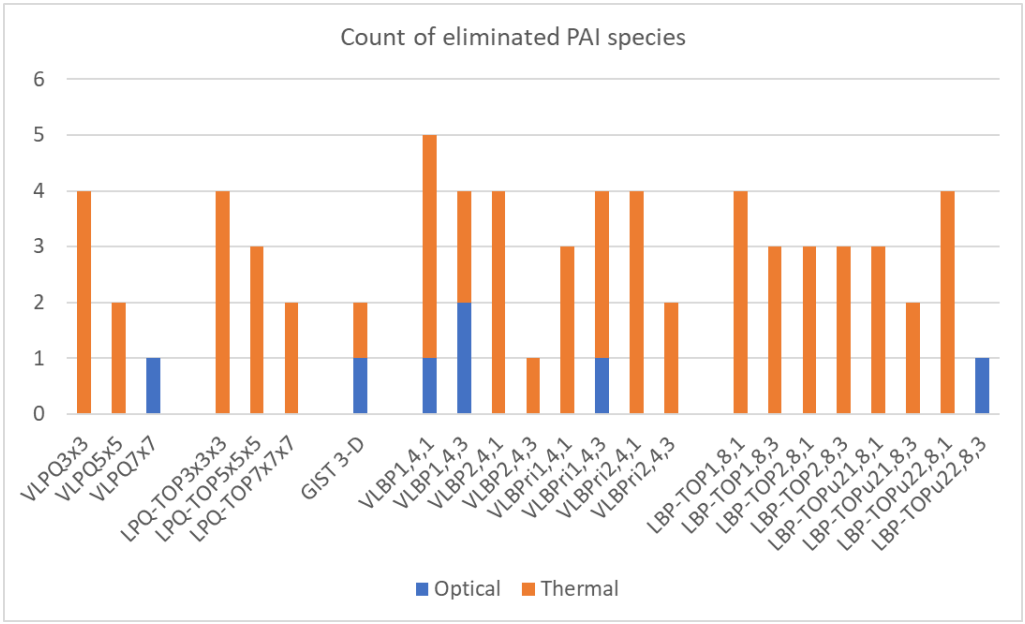


Figure 6.20. PAD mechanisms capability of eliminating PAI species.

6. 4. 6. Experiment V: Comparison with SoA Mechanisms

Literature studies had aimed to evidence the assumption that under certain presentation instruction, genuine fingerprints produce unique variation and/or distortion patterns that assist the process of detecting attacks. The aforementioned assumption counts on the natural structure of the human finger and its phenomena such as elasticity, internal bone position, etc. Moreover, previous studies had attempted to define some characteristics of different PAI species. For instance, Antonelli et.

al [221] had studied five PAI species and concluded that artificial artefacts are more rigid than genuine fingerprints. Thus, the produced distortion while rotating and pressuring the finger during a presentation is higher for genuine users.

This experiment compares the proposed PAD subsystem with those mechanisms discussed in Section 6. 2. All related works had been reported using TEER, thus the results are compared in Table 6.7 using TEER. These results are discussed in the next section.

Table 6.7. Comparison with SoA mechanisms.

Method	Sensing technology	TEER (%)	PAI species
Antonelli et al.	Optical	11.24	Gelatin, RTV silicon, white glue, and latex
Zhang et al.	Optical	4.5	Silicon
Jia et al.	Capacitive	4.78	Gelatin
Proposed	Optical	1.67	Play-Doh, white glue, spray rubber, polish nail, nails hardener, gelatin, latex
	Thermal	2.38	

We find that the obtained results are significantly improved compared to the SoA results, even though a wider set of attack species were used in our experiments. Due to the limited data provided in the SoA studies, further details cannot be reported.

6. 5. CONCLUSIONS

In this chapter, we examined the influence of pressure in fingerprint presentations and utilized this influence for the purpose of PAD. We studied the dynamic characteristics of genuine and attack presentations through a subjective and objective analysis. Based on those analyses on genuine fingerprints and seven PAI species, we concluded that the reaction to pressure in fingerprint patterns depends on the characteristics of the presented trait, genuine or attack. Bona fide presentations had shown a consistent variation in the pattern which is highlighted by a homogeneous degradation in the structural similarity in the consequent frames. On the other hand, elastic species (e.g. Play-Doh and gelatin) had shown an extreme variation in the pattern, sometimes the pattern vanishes and a dark region is obtained after pressure. Differently, rigid species (e.g. polish nail and white glue) had shown that pressure might improve the fingerprint pattern and result in high contrast between the ridges and valleys.

Fingerprint dynamic features were investigated using different dynamic texture descriptors. The utilized feature extractors had demonstrated a significant capability to detect presentation attacks and low false reject rates at the same time. Statistically speaking, when the PAD subsystem is evaluated at 2.5% APCER, i.e. 16 successful attacks out of 630 attacks, BPCER values are 1.11% for the optical sensor, i.e. 2 rejected bona fide presentations out of 180 total, and 2.22% for the thermal sensor, i.e. 4 rejected bona fide presentations out of 180 total.

The obtained results were compared to the ordinary dynamic presentations. The analysis confirms that additional pressure significantly improves the PAD performance in terms of accuracy and

generalizability. Moreover, the proposed method has illustrated high accuracy for the different sensing technologies and our results had discussed the pros and cons of each sensor.

This study contributes to the SoA investigation with a deeper understanding of the fingerprint dynamic features and the dynamic characteristics of different attack species.

Future work should concentrate on studying larger datasets that include a larger number of independent capture subjects. Moreover, the selection of participant/PAI species should include a wide spectrum of skin/materials categories, that is to include very dry skin to very sweaty skin for bona fide and different features for PAIs. From another perspective, the attacker's expertise should be taken into account for conducting a larger-scale evaluation. Meaning that multiple attackers with different capabilities should participate to produce PAs. Finally, we suggest studying fingerprint-specific dynamic features such as contours development and region of interest variations.

Chapter 7. Conclusions and Future Work

7. 1. SUMMARY AND CONCLUSIONS

Over the past few decades, the biometric community has been investigating the security of biometric recognition technologies by identifying the biometric system vulnerabilities, studying potential threats, and proposing countermeasures seeking to overcome the possible threats. The presentation attack issue has obtained significant attention, specifically for those applications that operate in unsupervised environments. All studies in this field of research emphasize the importance of developing presentation attack detection mechanisms that ensure the biometric systems' integrity.

Accordingly, this thesis investigates the vulnerability of biometric systems to presentation attacks with a focus on the fingerprint recognition system considering unsupervised environments. The investigation was initiated by revisiting the state-of-the-art investigations in presentation attack and presentation attack detection (Chapter 2). We taxonomized presentation attacks based on 3 essential factors: (1) the cooperation with the bona fide user, (2) the intention of the attacker, and (3) the nature of the attack species. Subsequently, the presentation attack detection mechanisms were taxonomized based on the intended PAD features. The proposed taxonomies provided a deeper understanding of the issue of presentation attacks, and the development of presentation attack detection evaluations. Existing taxonomies focus on the used tools to build the PAD mechanism, e.g. hardware/software or static/dynamic mechanisms which does not imply the targeted PAD features. On the other hand, the proposed taxonomy classifies the PAD mechanisms with emphasis on the PAD features and the basis of distinguishing attacks from genuine biometric presentations.

In Chapter 3, an evaluation methodology was developed by combining: (1) the PAD performance from the ISO/IEC 30107 standard, and (2) PAD vulnerability assessment from the Common Evaluation Methodology by the Common Criteria. The developed methodology provides comparable and accurate methods that characterize the technical capabilities of the PAD solutions considering specific attack potential. The main contribution of the methodology is the vulnerability assessment of presentation attacks considering all the factors that influence the attack potential. With that in mind, we end up knowing the PAD resistance to a known level of threat.

The attack potential relates exponentially with the attacker expertise and the latter can be improved by practicing. For example, the attacker in this thesis started the first practical experiment with an objective of unlocking smartphones using PAIs; explained in Annex I. As had been the first attacking experience, the attacker reported that success rate increases with practice, and he reported 90% success rate after 12 hours of practicing. After that, the attacker practiced to prepare PAIs using different species targeting different fingerprint sensors. During this training process the

attacker used thermal and optical sensing technologies to observe the differences between attacks and genuine patterns, and to prepare for the collecting data phase.

Subsequently, the data collection was carried out considering fingerprint modality, two scenarios (ordinary and pressure), and dynamic acquisition. The data was collected from 66 fingerprints taken from eleven capture subjects. 3-D molds were collected as well to create the PAIs later. The captured fingerprint videos for genuine presentations had demonstrated a consistent and uniform visual development for the ridge/valley pattern. That is due to the natural phenomena of the genuine fingerprint trait such as 3-D shape, elasticity, and perspiration. On the other hand, seven PAI species were used to perform attack presentations, namely: Play-Doh, white gle, spray rubber, nail hardener, polish nails, gelatin, and latex. The selected species provided distinct physical characteristics where some materials (e.g. gelatin) are very elastic while others (e.g. white glue) were rigid. That causes variance on the produced dynamic fingerprint patterns of the attacks. In general, the videos of attack presentations had shown irregularities and inhomogeneous development for the fingerprint pattern. These differences had been the basis for the proposed algorithms in the subsequent chapters.

The dynamic database provides a great benefit to study the fingerprint as a 3-D signal. Instead of studying the 2-D pattern, fingerprint videos show the development of the fingerprint pattern in space and time which provides significant amount of information that can be utilized to distinguish genuine presentations from attacks.

The first experiment (Chapter 4) had used the variation of global features in the fingerprint video frames as PAD features. These PAD features imply the global fingerprint characteristics (contrast, intensity, randomness, etc.) at each frame providing a feature vector that describes the fingerprint dynamics in the video. The PAD mechanism had achieved comparable performance considering thermal and optical technologies where BPCER20 was 18.1% for the thermal sensor and 19.5% for the optical sensor. Although the performance show similarity between the two sensors, the resistance of each sensor to the different PAI species varies. The optical sensor shows close rates in $APCER_{PAI}$ for the seven species, while the thermal sensor shows lower higher rates in $APCER_{PAI}$ for Play-Doh and white glue attacks. The attempt of improving the results using sequential feature selection had not provided an improvement to the results, contrarily, error rates were increased significantly. Even though the defined features were global and simple, the results had shown that they can be considered to mitigate the risk of attack presentations taking into account the corresponding error rates. Moreover, the proposed algorithm utilizes image statistics, thus, it does not require high computational cost and can be processed in real time.

The second experiment (Chapter 5) improved the performance of the PAD mechanism by consolidating the information from the space and time in the fingerprint video. The 5 dynamic feature extractors (i.e. VLBP, LBP-TOP, VLPQ, LPQ-TOP, and GIST 3-D) had shown significant improvement compared to the mechanism in Chapter 4, moreover, the results provided an improvement to the state-of-the-art investigations (BPCER 20 is 1.11% for the optical sensor and 3.89% for the thermal sensor). The most significant improvement achieved by this method is

achieving high level of security (low APCER) keeping high performance for the ease-of-use at (low BPCER). Additionally, the results of both sensing technologies were competitive compared to the state-of-the-art mechanisms. The mechanism was able to either mitigate or eliminate all the attack species for both sensors except the white glue attack for the thermal sensor where the $APCER_{PAI}$ was noticeably higher. The major flaw of the mechanism was the computational time. The evaluation was performed with an objective to validate the concept ignoring the computational time. However, the computation time is expected to be improved by utilizing optimized codes.

The last experiment (Chapter 6) focused on analyzing the dynamic fingerprint features when pressure is applied during the presentation. Applying pressure during the placement of the fingerprint causes slight movement in the ridges of the fingerprint pattern of genuine fingerprints. On the other hand, applying pressure when a PAI is placed at the sensor surface would produce a reaction that depends on the physical characteristics of the used materials. The study had shown that the differences between genuine and attack presentations can be visually noticed, thus using dynamic descriptors would efficiently characterize those differences. Therefore, the experiment used the feature extractors from Chapter 5 and involved an improvement to the proposed method in Chapter 4. In this scenario, the PAD performance provided two advantages over the method in Chapter 5. First, a significant improvement on the PAD accuracy. The mechanism shows a high capability to mitigate all the PAI species to low $APCER_{PAI}$ rate with the exception of white glue attacks for the thermal sensor. Secondly, the PAD features demonstrated less dependency on the training set, thus the PAD mechanism had shown more stable performance when applying leave-one-out cross-validation, achieving higher generalizability compared to ordinary presentations. The BPCER20 was reported as 0% for the optical sensor and 1.66% for the thermal sensor.

The proposed solutions had shown a better understanding of the attacks and the natural phenomena of biometric traits leads to stable and accurate solutions. This was shown by the sequence of our experiment. We first investigated the variation of global features, then the temporal information was integrated with the spatial domain achieving higher accuracy. Finally, we exploited the nature of genuine fingerprint and achieved the highest PAD accuracy and stability. The proposed methods provide a ground for future investigations and propose to exploit the dynamics of fingerprint as the basis for the PAD features.

7. 2. FUTURE WORK

Following the obtained results in this thesis, it is recommended that further research should be undertaken in the following areas:

1. Although the obtained results in Chapter 4 and Chapter 5 are promising, they should be validated by a larger dataset in order to provide a high level of confidence. Rules such as Rule of 3 and Rule of 30, might be utilized to obtain certain level of confidence about the achieved performance.

2. We observed through the experiments that fingerprint perspiration is capable of producing significant distortion when considering the class of subjects who have very moisture skin. On the other hand, the subjects with dry skin might demonstrate dynamic fingerprint behaviour similar to the rigid PAIs. Those observations were not systematically reported in this thesis due to the lack of data that supports those claims, therefore, further studies should analyse the fingerprint patterns for the users with extreme conditions (dry, perspiratory, skin diseases, etc.).
3. At the moment of finishing this thesis, there are no investigations or public datasets that are collected with different attack potentials. It is recommended to initiate data collections of presentation attacks with multiple groups of attackers that represent different attack potentials. That allows identifying the resistance of the proposed PAD mechanisms at different levels of risk.
4. The dynamic feature extractors can be customized to investigate specific fingerprint dynamics by focusing on particular regions in the fingerprint video. For instance, the development of a genuine fingerprint's contour starts as a small ellipse that enlarges while the fingerprint is placed on the sensor. When analyzing attacks, the contour does not develop homogenously where it contains irregularities and sharp edges.
5. In terms of biometric recognition, the different fingerprints of the same capture subject are statistically independent. It is interesting to investigate whither the PAD features of the different fingers of the same subject are also statistically independent. There expected to be specific correlation between the subject's fingerprints since we are talking about the same physical characteristics.
6. The framework of dynamic features can be applied to other biometric modalities such as Iris recognition systems. For example, the eye's pupil naturally responds to the variations of lighting conditions (pupil dilation), and the eye makes slight movements when adjusting the eye in front of the sensor. The dynamic descriptors used in this thesis are expected to efficiently characterize these dynamics as PAD features.

Finally, we believe that the proposed mechanisms in this thesis makes a step forward to achieving more secured recognition process, however, research should continue pursuing the perfection of system's confidentiality, integrity, and availability.

Bibliography

[1] "Amsterdam airport's facial ID fooled by simple photo," *Biometric Technol. Today*, vol. 2020, no. 1, pp. 11–12, Jan. 2020.

[2] "Man boards plane disguised as old man then arrested on arrival in Canada | Daily Mail Online." [Online]. Available: https://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html. [Accessed: 02-Nov-2020].

[3] "How Bkav tricked iPhone X's Face ID with a mask - YouTube." [Online]. Available: https://www.youtube.com/watch?v=i4YQRLQVixM&feature=emb_logo. [Accessed: 02-Nov-2020].

[4] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[5] R. Blanco-Gonzalo, R. Sanchez-Reillo, J. Liu-Jimenez, and C. Sanchez-Redondo, "How to assess user interaction effects in Biometric performance," in *2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017*, 2017.

[6] J. Nelson, "Biometrics Characteristics," in *Effective Physical Security*, Elsevier Inc., 2013, pp. 255–256.

[7] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of biometric anti-spoofing : presentation attack detection*. .

[8] "ISO/IEC 30107-1:2016 - Information technology -- Biometric presentation attack detection -- Part 1: Framework." .

[9] "Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Standard, Common Criteria, Sep. 2012." Common Criteria.

[10] "ISO/IEC 30107-2:2017 - Information technology -- Biometric presentation attack detection -- Part 2: Data formats." .

[11] "ISO/IEC 30107-3:2017 - Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting." .

[12] "CCC | Chaos Computer Club breaks Apple TouchID." [Online]. Available: https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid. [Accessed: 02-Nov-2020].

[13] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[14] "Fingerprint Sensor Market | Size, Trends, Share, Industry Analysis and Market Forecast to 2024 | MarketsandMarkets™." [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/fingerprint-sensors-market-169519533.html. [Accessed: 24-Nov-2020].

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

[16] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face

Recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[17] E. Marasco and A. Ross, "A Survey on Antispoofing Schemes for Fingerprint Recognition Systems," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–36, Nov. 2014.

[18] P. Sengottuvelan and A. Wahi, "Analysis of Living and Dead Finger Impression Identification for Biometric Application," in *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, 2007, pp. 466–470.

[19] R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, "Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries," in *2015 International Carnahan Conference on Security Technology (ICCST)*, 2015, pp. 373–378.

[20] R. Sanchez-Reillo, H. C. Quiros-Sandoval, I. Goicoechea-Telleria, and W. Ponce-Hernandez, "Improving Presentation Attack Detection in Dynamic Handwritten Signature Biometrics," *IEEE Access*, vol. 5, pp. 20463–20469, 2017.

[21] R. Sanchez-Reillo, J. Liu-Jimenez, R. Blanco-Gonzalo, and O. Miguel-Hurtado, "Performance evaluation of handwritten signature recognition in mobile environments," *IET Biometrics*, vol. 3, no. 3, pp. 139–146, Sep. 2014.

[22] M. S. Nixon, *Handbook of Biometric Anti-Spoofing*, no. April. Cham, Switzerland: Springer, 2019.

[23] A. K. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," in *2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014)*, 2014, pp. 592–597.

[24] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," *J. Vis. Lang. Comput.*, vol. 20, no. 3, pp. 169–179, Jun. 2009.

[25] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness of multi-modal biometric verification systems under realistic spoofing attacks," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–6.

[26] Y. Wang, T. Tan, and A. K. Jain, "Combining Face and Iris Biometrics for Identity Verification."

[27] "MobBIO: A Multimodal Database Captured with a Portable Handheld Device," in *Proceedings of the 9th International Conference on Computer Vision Theory and Applications*, 2014, pp. 133–139.

[28] "SOCIA Lab. - Soft Computing and Image Analysis Group. 2004. Noisy Visible Wavelength Iris Image Databases (UBIRIS). (2004)." [Online]. Available: http://iris.di.ubi.pt/.

[29] M. Trokielewicz and E. Bartuzi, "Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images."

[30] "Biometric personal identification system based on iris analysis," Jul. 1991.

[31] G. W. Quinn, P. Grother, J. Matey, W. L. Ross, and W. Copan, "NISTIR 8207 IREX IX Part One Performance of Iris Recognition Algorithms NISTIR 8207 IREX IX Part One

Performance of Iris Recognition Algorithms Executive Summary," 2018.

[32] A. Czajka and K. W. Bowyer, "Presentation Attack Detection for Iris Recognition," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–35, Jul. 2018.

[33] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," in *2016 4th International Conference on Biometrics and Forensics (IWBF)*, 2016, pp. 1–6.

[34] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body check: biometric access protection devices and their programs put to the test," *C'T Magazine*, vol. 11, p. 114, 2002.

[35] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct Attacks Using Fake Images in Iris Verification," Springer, Berlin, Heidelberg, 2008, pp. 181–190.

[36] A. Pacut and A. Czajka, "Aliveness Detection for IRIS Biometrics," in *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, 2006, pp. 122–129.

[37] A. Czajka, "Pupil Dynamics for Iris Liveness Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 726–735, Apr. 2015.

[38] A. Czajka, "Iris Liveness Detection by Modeling Dynamic Pupil Features," Springer, London, 2016, pp. 439–467.

[39] I. Rigas and O. V. Komogortsev, "Eye movement-driven defense against iris print-attacks," *Pattern Recognit. Lett.*, vol. 68, pp. 316–326, Dec. 2015.

[40] C.-H. Teng *et al.*, "Liveness Detection: Iris," in *Encyclopedia of Biometrics*, Boston, MA: Springer US, 2009, pp. 931–938.

[41] J. Zuo, N. A. Schmid, and X. Chen, "On Generation and Analysis of Synthetic Iris Images," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 1, pp. 77–90, Mar. 2007.

[42] W. S.-A. Fathy and H. S. Ali, "Entropy with Local Binary Patterns for Efficient Iris Liveness Detection," *Wirel. Pers. Commun.*, pp. 1–14, Dec. 2017.

[43] L. He, H. Li, F. Liu, N. Liu, Z. Sun, and Z. He, "Multi-patch convolution neural network for iris liveness detection," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–7.

[44] J. Connell, N. Ratha, J. Gentile, and R. Bolle, "Fake iris detection using structured light," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 8692–8696.

[45] X. He, Y. Lu, and P. Shi, "A New Fake Iris Detection Method," Springer, Berlin, Heidelberg, 2009, pp. 1132–1139.

[46] X. Huang, C. Ti, Q. Hou, A. Tokuta, and R. Yang, "An experimental study of pupil constriction for liveness detection," in *2013 IEEE Workshop on Applications of Computer Vision (WACV)*, 2013, pp. 252–258.

[47] M. Kumar and N. B. Puhan, "Iris liveness detection using texture segmentation," in *2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*, 2015, pp. 1–4.

[48] M. De Marsico, D. Riccio, and H. Wechsler, “Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols,” *Pattern Recognit. Lett.*, vol. 57, pp. 17–23, May 2015.

[49] A. F. Sequeira, J. Murari, and J. S. Cardoso, “Iris liveness detection methods in the mobile biometrics scenario,” in *2014 International Joint Conference on Neural Networks (IJCNN)*, 2014, pp. 3002–3008.

[50] A. F. Sequeira, S. Thavalengal, J. Ferryman, P. Corcoran, and J. S. Cardoso, “A realistic evaluation of iris presentation attack detection,” in *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, 2016, pp. 660–664.

[51] Y. N. Singh and S. K. Singh, “Vitality detection from biometrics: State-of-the-art,” in *2011 World Congress on Information and Communication Technologies*, 2011, pp. 106–111.

[52] Z. Sun and T. Tan, “Iris Anti-spoofing,” Springer, London, 2014, pp. 103–123.

[53] J. DAUGMAN, “DEMODULATION BY COMPLEX-VALUED WAVELETS FOR STOCHASTIC PATTERN RECOGNITION,” *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 01, no. 01, pp. 1–17, Mar. 2003.

[54] J. S. Doyle, P. J. Flynn, and K. W. Bowyer, “Automated classification of contact lens type in iris images,” in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–6.

[55] A. Czajka, K. W. Bowyer, M. Krumdick, and R. G. VidalMata, “Recognition of Image-Orientation-Based Iris Spoofing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 9, pp. 2184–2196, Sep. 2017.

[56] A. N. Al-Raisi and A. M. Al-Khouri, “Iris recognition and the challenge of homeland and border control security in UAE,” *Telemat. Informatics*, vol. 25, no. 2, pp. 117–132, May 2008.

[57] I. Tomeo-Reyes, A. Ross, and V. Chandran, “Investigating the impact of drug induced pupil dilation on automated iris recognition,” in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–8.

[58] A. Sansola, “Postmortem iris recognition and its application in human identification,” 2015.

[59] M. Trokielewicz, A. Czajka, and P. Maciejewicz, “Human iris recognition in post-mortem subjects: Study and database,” in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2016, pp. 1–6.

[60] M. Trokielewicz, A. Czajka, and P. Maciejewicz, “Post-mortem human iris recognition,” in *2016 International Conference on Biometrics (ICB)*, 2016, pp. 1–6.

[61] T. Matsumoto, “Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis,” Springer, Berlin, Heidelberg, 2002, pp. 574–575.

[62] T. Putte and J. Keuning, “Biometrical Fingerprint Recognition: Don’t get your Fingers Burned,” in *Smart Card Research and Advanced Applications*, Boston, MA: Springer US, 2000, pp. 289–303.

[63] M. Espinoza, C. Champod, and P. Margot, “Vulnerabilities of fingerprint reader to fake fingerprints attacks,” *Forensic Sci. Int.*, vol. 204, no. 1–3, pp. 41–49, Jan. 2011.

[64] T. Chugh, K. Cao, and A. K. Jain, “Fingerprint Spoof Buster: Use of Minutiae-Centered

Patches," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2190–2202, Sep. 2018.

[65] T. D. Thandauthapani, A. J. Reeve, A. S. Long, I. J. Turner, and J. S. Sharp, "Exposing latent fingermarks on problematic metal surfaces using time of flight secondary ion mass spectroscopy," *Sci. Justice*, vol. 58, no. 6, pp. 405–414, Nov. 2018.

[66] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, "Analysis of the attack potential in low cost spoofing of fingerprints," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1–6.

[67] C. Barral and A. Tria, "Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin," Springer, Berlin, Heidelberg, 2009, pp. 57–69.

[68] S. A. . Schuckers, "Spoofing and Anti-Spoofing Measures," *Inf. Secur. Tech. Rep.*, vol. 7, no. 4, pp. 56–62, Dec. 2002.

[69] M. Sandstrom, "Liveness Detection in Fingerprint Recognition Systems," 2004.

[70] S. J. Elliott, S. K. Modi, L. Maccarone, M. R. Young, C. Jin, and H. Kim, "Image Quality and Minutiae Count Comparison for Genuine and Artificial Fingerprints," in *2007 41st Annual IEEE International Carnahan Conference on Security Technology*, 2007, pp. 30–36.

[71] J. Blommé, "Evaluation of biometric security systems against artificial fingers," 2003.

[72] J. Spurny, M. Doleel, O. Kanich, M. Drahansky, and K. Shinoda, "New Materials for Spoofing Touch-Based Fingerprint Scanners," in *2015 International Conference on Computer Application Technologies*, 2015, pp. 207–211.

[73] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of biometric anti-spoofing : presentation attack detection*. .

[74] C. Busch and C. Sousedik, "Presentation attack detection methods for fingerprint recognition systems: a survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[75] R. Ramachandra and C. Busch, "Presentation Attack Detection Methods for Face Recognition Systems," *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–37, Mar. 2017.

[76] R. Min, A. Hadid, and J.-L. Dugelay, "Improving the recognition of faces occluded by facial accessories," in *Face and Gesture 2011*, 2011, pp. 442–447.

[77] H. Liu, H. Duan, H. Cui, and Y. Yin, "Face recognition using training data with artificial occlusions," in *2016 Visual Communications and Image Processing (VCIP)*, 2016, pp. 1–4.

[78] M. Singh, R. Singh, M. Vatsa, N. Ratha, and R. Chellappa, "Recognizing Disguised Faces in the Wild," Nov. 2018.

[79] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–7.

[80] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 555–563.

[81] R. Tronci *et al.*, “Fusion of multiple clues for photo-attack detection in face recognition systems,” in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–6.

[82] K. Patel, H. Han, A. K. Jain, and G. Ott, “Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks,” in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 98–105.

[83] N. Kose and J.-L. Dugelay, “On the vulnerability of face recognition systems to spoofing mask attacks,” in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 2357–2361.

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

[85] N. Erdogmus and S. Marcel, “Spoofing Face Recognition With 3D Masks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[86] T. I. Dhamecha, R. Singh, M. Vatsa, and A. Kumar, “Recognizing Disguised Faces: Human and Machine Evaluation,” *PLoS One*, vol. 9, no. 7, p. e99212, Jul. 2014.

[87] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, “Eigenfaces vs. Fisherfaces: recognition using class specific linear projection,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 711–720, Jul. 1997.

[88] R. Singh, M. Vatsa, and A. Noore, “Effect of plastic surgery on face recognition: A preliminary study,” in *2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2009, pp. 72–77.

[89] A. S. O. Ali, V. Sagayan, A. Malik, and A. Aziz, “Proposed face recognition system after plastic surgery,” *IET Comput. Vis.*, vol. 10, no. 5, pp. 344–350, Aug. 2016.

[90] Z. Zheng and C. Kambhamettu, “Multi-level Feature Learning for Face Recognition under Makeup Changes,” in *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, 2017, pp. 918–923.

[91] Z. Zheng and G. Guo, “A joint optimization scheme to combine different levels of features for face recognition with makeup changes,” in *2016 IEEE International Conference on Image Processing (ICIP)*, 2016, pp. 3001–3005.

[92] A. Afaneh, F. Noroozi, and Ö. Toygar, “Recognition of identical twins using fusion of various facial feature extractors,” *EURASIP J. Image Video Process.*, vol. 2017, no. 1, p. 81, Dec. 2017.

[93] P. J. Phillips *et al.*, “Distinguishing identical twins by face recognition,” in *Face and Gesture 2011*, 2011, pp. 185–192.

[94] “gbd-e.org.” [Online]. Available: http://gbd-e.org/?domain=gbd-e.org?reqp=1&qaspoofip=163.117.174.163&reqp=1&reqr=. [Accessed: 14-Jun-2018].

[95] “VERA Palmvein Database.” [Online]. Available: https://www.idiap.ch/dataset/vera-palmvein. [Accessed: 14-Jun-2018].

[96] P. Tome and S. Marcel, “On the Vulnerability of Palm Vein Recognition to Spoofing Attacks.”

[97] P. Tome, M. Vanoni, and S. Marcel, “On the Vulnerability of Finger Vein Recognition to Spoofing.”

[98] J.-J. Brault and R. Plamondon, “A complexity measure of handwritten curves: modeling of dynamic signature forgery,” *IEEE Trans. Syst. Man. Cybern.*, vol. 23, no. 2, pp. 400–413, 1993.

[99] L. Ballard, D. Lopresti, and F. Monrose, “Forgery Quality and Its Implications for Behavioral Biometric Security,” *IEEE Trans. Syst. Man Cybern. Part B*, vol. 37, no. 5, pp. 1107–1118, Oct. 2007.

[100] J.-J. Brault and R. Plamondon, “How to detect problematic signers for automatic signature verification,” in *Proceedings. International Carnahan Conference on Security Technology*, pp. 127–132.

[101] G. Pirlo, “Algorithms for Signature Verification,” in *Fundamentals in Handwriting Recognition*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 435–454.

[102] E. Zetterholm, “Same speaker – different voices A study of one impersonator and some of his different imitations.”

[103] E. Zetterholm, K. P. H. Sullivan, and J. Van Doorn, “THE IMPACT OF SEMANTIC EXPECTATION ON THE ACCEPTANCE OF A VOICE IMITATION.”

[104] B. Gillett and S. King, “Transforming F0 Contours.”

[105] Chung-Hsien Wu, Chi-Chun Hsia, Te-Hsien Liu, and Jhing-Fa Wang, “Voice conversion using duration-embedded bi-HMMs for expressive speech synthesis,” *IEEE Trans. Audio, Speech Lang. Process.*, vol. 14, no. 4, pp. 1109–1116, Jul. 2006.

[106] E. E. Helander and J. Nurminen, “A Novel Method for Prosody Prediction in Voice Conversion,” in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP ’07*, 2007, pp. IV-509-IV–512.

[107] A. Czajka, “Making iris recognition more reliable and spoof resistant,” *SPIE Newsroom*, 2007.

[108] A. CZAJKA, A. PACUT, and M. CHOCHOWSKI, “METHOD OF EYE ALIVENESS TESTING AND DEVICE FOR EYE ALIVENESS TESTING,” Mar. 2008.

[109] F. M. Villalbos-Castaldi and E. Suaste-Gomez, “In the use of the spontaneous pupillary oscillations as a new biometric trait,” in *2nd International Workshop on Biometrics and Forensics*, 2014, pp. 1–6.

[110] N. K. Shaydyuk and T. Cleland, “Biometric identification via retina scanning with liveness detection using speckle contrast imaging,” in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, 2016, pp. 1–5.

[111] I. Rigas and O. V. Komogortsev, “Gaze estimation as a framework for iris liveness detection,” in *IEEE International Joint Conference on Biometrics*, 2014, pp. 1–8.

[112] K. B. Raja, R. Raghavendra, and C. Busch, “Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2048–2056, Oct. 2015.

[113] O. V. Komogortsev, A. Karpov, and C. D. Holland, “Attack of Mechanical Replicas:

Liveness Detection With Eye Movements," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 716–725, Apr. 2015.

[114] O. V. Komogortsev and A. Karpov, "Liveness detection via oculomotor plant characteristics: Attack of mechanical replicas," in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–8.

[115] E. C. Lee and K. R. Park, "Fake iris detection based on 3D structure of iris pattern," *Int. J. Imaging Syst. Technol.*, vol. 20, no. 2, pp. 162–166, May 2010.

[116] E. C. Lee, K. R. Park, and J. Kim, "Fake Iris Detection by Using Purkinje Image," Springer, Berlin, Heidelberg, 2005, pp. 397–403.

[117] Bozhao Tan and S. Schuckers, "Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, pp. 26–26.

[118] B. DeCann, B. Tan, and S. Schuckers, "A Novel Region Based Liveness Detection Approach for Fingerprint Scanners," Springer, Berlin, Heidelberg, 2009, pp. 627–636.

[119] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recognit.*, vol. 42, no. 3, pp. 452–464, Mar. 2009.

[120] S. Memon, N. Manivannan, and W. Balachandran, "Active pore detection for liveness in fingerprint identification system," in *2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers*, 2011, pp. 619–622.

[121] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," *Electron. Lett.*, vol. 41, no. 20, p. 1112, 2005.

[122] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," in *2007 IEEE 11th International Conference on Computer Vision*, 2007, pp. 1–8.

[123] Wei Bao, Hong Li, Nan Li, and Wei Jiang, "A liveness detection method for face recognition based on optical flow field," in *2009 International Conference on Image Analysis and Signal Processing*, 2009, pp. 233–236.

[124] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," Springer, Berlin, Heidelberg, 2010, pp. 504–517.

[125] B. Qin, J. Pan, G. Cao, and G. Du, "The Anti-spoofing Study of Vein Identification System," in *2009 International Conference on Computational Intelligence and Security*, 2009, pp. 357–360.

[126] J. Lee *et al.*, "A finger-vein imaging and liveness detection for identity authentication using 2-axis MEMS scanner," in *2016 International Conference on Optical MEMS and Nanophotonics (OMN)*, 2016, pp. 1–2.

[127] R. Raghavendra, M. Avinash, S. Marcel, and C. Busch, "Finger vein liveness detection using motion magnification," in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2015, pp. 1–7.

[128] S. J. Elliott, "Development of a biometric testing protocol for dynamic signature

verification," in *7th International Conference on Control, Automation, Robotics and Vision, 2002. ICARCV 2002.*, vol. 2, pp. 782–787.

[129] M. Vatsa, R. Singh, P. Mitra, and A. Noore, "Signature Verification Using Static and Dynamic Features," Springer, Berlin, Heidelberg, 2004, pp. 350–355.

[130] R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, "Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries," in *2015 International Carnahan Conference on Security Technology (ICCST)*, 2015, pp. 373–378.

[131] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *2012 5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 271–276.

[132] H. Zhang, Z. Sun, T. Tan, and J. Wang, "Learning Hierarchical Visual Codebook for Iris Liveness Detection."

[133] Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris Image Classification Based on Hierarchical Visual Codebook," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1120–1133, Jun. 2014.

[134] Z. Akhtar, C. Michelon, and G. L. Foresti, "Liveness detection for biometric authentication in mobile applications," in *2014 International Carnahan Conference on Security Technology (ICCST)*, 2014, pp. 1–6.

[135] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "MoBio_LivDet: Mobile biometric liveness detection," in *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 2014, pp. 187–192.

[136] F. Alonso-Fernandez and J. Bigun, "Exploting periocular and RGB information in fake iris detection," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1354–1359.

[137] A. Das, U. Pal, M. A. Ferrer, and M. Blumenstein, "A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics," *Pattern Recognit. Lett.*, vol. 82, pp. 232–241, Oct. 2016.

[138] D. Gragnaniello, C. Sansone, and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," *Pattern Recognit. Lett.*, vol. 57, pp. 81–87, May 2015.

[139] A. P. S. Bhogal, D. Sollinger, P. Trung, and A. Uhl, "Non-reference image quality assessment for biometric presentation attack detection," in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6.

[140] C. Chen and A. Ross, "A Multi-task Convolutional Neural Network for Joint Iris Detection and Presentation Attack Detection," in *2018 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, 2018, pp. 44–51.

[141] A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," in *2013 18th International Conference on Methods & Models in Automation & Robotics (MMAR)*, 2013, pp. 28–33.

[142] J. S. Doyle and K. W. Bowyer, "Robust Detection of Textured Contact Lenses in Iris

Recognition Using BSIF," *IEEE Access*, vol. 3, pp. 1672–1683, 2015.

[143] J. S. Doyle, K. W. Bowyer, and P. J. Flynn, "Variation in accuracy of textured contact lens detection based on sensor and lens pattern," in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2013, pp. 1–7.

[144] D. Yadav, N. Kohli, M. Vatsa, R. Singh, and A. Noore, "Unconstrained visible spectrum iris with textured contact lens variations: Database and benchmarking," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 574–580.

[145] *J. Daugman, Biometrics. Personal Identification in a Networked Society, chapter Recognizing Persons by their Iris Patterns, pp. 103–121, Kluwer Academic Publishers, 1999. .*

[146] S. J. Lee, K. R. Park, and J. Kim, "Robust Fake Iris Detection Based on Variation of the Reflectance Ratio Between the IRIS and the Sclera," in *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, 2006, pp. 1–6.

[147] J. H. Park and M. G. Kang, "Iris Recognition Against Counterfeit Attack Using Gradient Based Fusion of Multi-spectral Images," Springer, Berlin, Heidelberg, 2005, pp. 150–156.

[148] J. H. Park and M.-G. Kang, "Multispectral iris authentication system against counterfeit attack using gradient-based image fusion," *Opt. Eng.*, vol. 46, no. 11, p. 117003, Nov. 2007.

[149] R. Chen, X. Lin, and T. Ding, "Liveness detection for iris recognition using multispectral images," *Pattern Recognit. Lett.*, vol. 33, no. 12, pp. 1513–1519, Sep. 2012.

[150] S.-H. Hsieh, Y.-H. Li, W. Wang, and C.-H. Tien, "A Novel Anti-Spoofing Solution for Iris Recognition Toward Cosmetic Contact Lens Attack Using Spectral ICA Analysis," *Sensors*, vol. 18, no. 3, p. 795, Mar. 2018.

[151] S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, "Iris liveness detection for next generation smartphones," *IEEE Trans. Consum. Electron.*, vol. 62, no. 2, pp. 95–102, May 2016.

[152] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 3, pp. 360–373, Sep. 2006.

[153] J. Jia, L. Cai, K. Zhang, and D. Chen, "A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis," in *Advances in Biometrics*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 309–318.

[154] Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake Finger Detection Based on Thin-Plate Spline Distortion Model," in *Advances in Biometrics*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 742–749.

[155] Eyung Lim, Xudong Jiang, and Weiyun Yau, "Fingerprint quality and validity analysis," in *Proceedings. International Conference on Image Processing*, vol. 1, pp. I-469-I–472.

[156] Y. Chen, S. C. Dass, and A. K. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance," Springer, Berlin, Heidelberg, 2005, pp. 160–170.

[157] Tai Pang Chen, Xudong Jiang, and Wei Yun Yau, "Fingerprint image quality analysis," in *2004 International Conference on Image Processing, 2004. ICIP '04.*, vol. 2, pp. 1253–

1256.

[158] Lin Hong, Yifei Wan, and A. Jain, “Fingerprint image enhancement: algorithm and performance evaluation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777–789, 1998.

[159] B. Sankur, B. Sankur, and K. Sayood, “Statistical evaluation of image quality measures,” *J. Electron. Imaging*, vol. 11, no. 2, p. 206, Apr. 2002.

[160] Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” *Electron. Lett.*, vol. 44, no. 13, p. 800, 2008.

[161] Susu Yao, Weisi Lin, EePing Ong, and Zhongkang Lu, “Contrast signal-to-noise ratio for image quality assessment,” in *IEEE International Conference on Image Processing 2005*, 2005, pp. I–397.

[162] A. M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” *IEEE Trans. Commun.*, vol. 43, no. 12, pp. 2959–2965, 1995.

[163] M. G. Martini, C. T. E. R. Hewage, and B. Villarini, “Image quality assessment based on edge preservation,” *Signal Process. Image Commun.*, vol. 27, no. 8, pp. 875–882, Sep. 2012.

[164] N. B. Nill and B. Bouzas, “Objective image quality measure derived from digital image power spectra,” *Opt. Eng.*, vol. 31, no. 4, p. 813, 1992.

[165] Anmin Liu, Weisi Lin, and M. Narwaria, “Image Quality Assessment Based on Gradient Similarity,” *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 1500–1512, Apr. 2012.

[166] R. Soundararajan and A. C. Bovik, “RRED Indices: Reduced Reference Entropic Differencing for Image Quality Assessment.”

[167] X. Zhu and P. Milanfar, “A NO-REFERENCE SHARPNESS METRIC SENSITIVE TO BLUR AND NOISE.”

[168] A. Abhyankar and S. Schuckers, “Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques,” in *2006 International Conference on Image Processing*, 2006, pp. 321–324.

[169] S. B. Nikam and S. Agarwal, “Curvelet-based fingerprint anti-spoofing,” *Signal, Image Video Process.*, vol. 4, no. 1, pp. 75–87, Mar. 2010.

[170] P. Coli, G. L. Marcialis, and F. Roli, “Power spectrum-based fingerprint vitality detection,” in *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, 2007, pp. 169–173.

[171] C. Jin, H. Kim, and S. Elliott, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” in *Information Security and Cryptology - ICISC 2007*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 168–179.

[172] V. Ojansivu, E. Rahtu, and J. Heikkila, “Rotation invariant local phase quantization for blur insensitive texture analysis,” in *2008 19th International Conference on Pattern Recognition*, 2008, pp. 1–4.

[173] V. Ojansivu and J. Heikkilä, “Blur Insensitive Texture Classification Using Local Phase Quantization,” Springer, Berlin, Heidelberg, 2008, pp. 236–243.

[174] J. G. Martins, L. S. Oliveira, and R. Sabourin, “Combining textural descriptors for forest species recognition,” in *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*, 2012, pp. 1483–1488.

[175] Y. Cheng and K. V. Larin, “Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis,” *Appl. Opt.*, vol. 45, no. 36, p. 9238, Dec. 2006.

[176] S. Chang, Y. Cheng, K. V. Larin, Y. Mao, S. Sherif, and C. Flueraru, “Optical coherence tomography used for security and fingerprint-sensing applications,” *IET Image Process.*, vol. 2, no. 1, p. 48, 2008.

[177] A. Z. A. Aziz, H. Wei, and J. Ferryman, “Face anti-spoofing countermeasure: Efficient 2D materials classification using polarization imaging,” in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6.

[178] L. Li, P. L. Correia, and A. Hadid, “Face recognition under spoofing attacks: countermeasures and research directions,” *IET Biometrics*, vol. 7, no. 1, pp. 3–14, Jan. 2018.

[179] T. Ahonen, A. Hadid, and M. Pietikainen, “Face Description with Local Binary Patterns: Application to Face Recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[180] G. B. de Souza, D. F. da Silva Santos, R. G. Pires, A. N. Marana, and J. P. Papa, “Deep Texture Features for Robust Face Spoofing Detection,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 64, no. 12, pp. 1397–1401, Dec. 2017.

[181] E. Fourati, W. Elloumi, and A. Chetouani, “Face anti-spoofing with image quality assessment,” in *2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART)*, 2017, pp. 1–4.

[182] H. Li, S. Wang, and A. C. Kot, “Face spoofing detection with image quality regression,” in *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 2016, pp. 1–6.

[183] C.-H. Yeh and H.-H. Chang, “Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis,” in *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2018, pp. 49–56.

[184] G. Pan, L. Sun, Z. Wu, and Y. Wang, “Monocular camera-based face liveness detection by combining eyeblink and scene context,” *Telecommun. Syst.*, vol. 47, no. 3–4, pp. 215–225, Aug. 2011.

[185] J. Komulainen, A. Hadid, and M. Pietikainen, “Context based face anti-spoofing,” in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2013, pp. 1–8.

[186] W. R. Schwartz, A. Rocha, and H. Pedrini, “Face spoofing detection through partial least squares and low-level descriptors,” in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–8.

[187] R. Tronci *et al.*, “Fusion of multiple clues for photo-attack detection in face recognition systems,” in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–6.

[188] J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live Face Detection Based on the Analysis of

Fourier Spectra."

[189] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in *2011 18th IEEE International Conference on Image Processing*, 2011, pp. 3557–3560.

[190] Di Wen, Hu Han, and A. K. Jain, "Face Spoof Detection With Image Distortion Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 746–761, Apr. 2015.

[191] R. T. Tan and K. Ikeuchi, "Separating reflection components of textured surfaces using a single image," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 2, pp. 178–193, Feb. 2005.

[192] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in *2015 IEEE International Conference on Image Processing (ICIP)*, 2015, pp. 2636–2640.

[193] E. M. Rudd, M. Gunther, and T. E. Boult, "PARAPH: Presentation Attack Rejection by Analyzing Polarization Hypotheses," in *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2016, pp. 171–178.

[194] R. Raghavendra and C. Busch, "Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study," in *2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, 2015, pp. 628–632.

[195] P. Tome *et al.*, "The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks," in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 513–518.

[196] L. Stoll and G. Doddington, "Hunting for Wolves in Speaker Recognition."

[197] W. Shang and M. Stevenson, "Score normalization in playback attack detection," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010, pp. 1678–1681.

[198] J. Villalba and E. Lleida, "Preventing replay attacks on speaker verification systems," in *2011 Carnahan Conference on Security Technology*, 2011, pp. 1–8.

[199] A. Paul, R. K. Das, R. Sinha, and S. R. M. Prasanna, "Countermeasure to handle replay attacks in practical speaker verification systems," in *2016 International Conference on Signal Processing and Communications (SPCOM)*, 2016, pp. 1–5.

[200] C. H. E. E. (ELECO), 2017 10th, and undefined 2017, "Features and classifiers for replay spoofing attack detection," *ieeexplore.ieee.org*.

[201] P. L. De Leon, I. Hernaez, I. Saratxaga, M. Pucher, and J. Yamagishi, "Detection of synthetic speech for the problem of imposture," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 4844–4847.

[202] Z. Wu, E. S. Chng, and H. Li, "Detecting Converted Speech and Natural Speech for anti-Spoofing Attack in Speaker Recognition."

[203] Z. Wu, X. Xiao, E. S. Chng, and H. Li, "Synthetic speech detection using temporal modulation feature," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 7234–7238.

[204] F. Alegre, A. Amehraye, and N. Evans, "Spoofing countermeasures to protect automatic

speaker verification from voice conversion," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 3068–3072.

[205] M. J. Correia, A. Abad, and I. Trancoso, "Preventing converted speech spoofing attacks in speaker verification," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1320–1325.

[206] Z. Wu *et al.*, "ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge," *IEEE J. Sel. Top. Signal Process.*, vol. 11, no. 4, pp. 588–604, Jun. 2017.

[207] W.-Y. Yau, H.-L. Tran, and E.-K. Teoh, "Fake finger detection using an electrotactile display system," in *2008 10th International Conference on Control, Automation, Robotics and Vision*, 2008, pp. 962–966.

[208] I. Rigas and O. V. Komogortsev, "Eye movement-driven defense against iris print-attacks," *Pattern Recognit. Lett.*, vol. 68, pp. 316–326, Dec. 2015.

[209] A. A. (Arun A. Ross, A. K. Jain, and K. Nandakumar, *Handbook of Multibiometrics*. .

[210] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks."

[211] P. A. Johnson, B. Tan, and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in *2010 IEEE International Workshop on Information Forensics and Security*, 2010, pp. 1–5.

[212] R. N. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2010, pp. 1–5.

[213] "ISO - ISO/IEC 30107-4:2020 - Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices." [Online]. Available: https://www.iso.org/standard/75301.html. [Accessed: 14-Oct-2020].

[214] "LivDet - Liveness Detection Competitions." [Online]. Available: http://livdet.org/registration.php. [Accessed: 15-Dec-2020].

[215] I. Goicoechea Telleria, "Evaluation of presentation attack detection under the context of common criteria," Universidad Carlos III de Madrid, 2019.

[216] "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components," 2009.

[217] A. Martin, A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET curve in assessment of detection task performance," in *Proceedings of the European Conference on Speech Communication and Technology*, 1997, pp. 1895--1898.

[218] R. B. Gonzalo *et al.*, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach," in *2018 International Carnahan Conference on Security Technology (ICCST)*, 2018, pp. 1–5.

[219] R. Blanco Gonzalo *et al.*, "Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach," in *Proceedings - International Carnahan Conference on Security*

Technology, 2018, vol. 2018-October.

[220] R. Cappelli, D. Maio, and D. Maltoni, "Modelling Plastic Distortion in Fingerprint Images," Springer, Berlin, Heidelberg, 2001, pp. 371–378.

[221] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 3, pp. 360–373, Sep. 2006.

[222] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, Feb. 2003.

[223] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices," *IEEE Trans. Syst. Man Cybern. Part C (Applications Rev.*, vol. 35, no. 3, pp. 335–343, Aug. 2005.

[224] R. Plesh *et al.*, "Fingerprint Presentation Attack Detection utilizing Time-Series, Color Fingerprint Captures," in *2019 International Conference on Biometrics, ICB 2019*, 2019.

[225] "VeriFinger fingerprint recognition technology, algorithm and SDK for PC, smartphones and Web." [Online]. Available: http://www.neurotechnology.com/verifinger.html. [Accessed: 25-Mar-2020].

[226] M. Szummer and R. W. Picard, "Temporal texture modeling," in *IEEE International Conference on Image Processing*, 1996, vol. 3, pp. 823–826.

[227] G. Zhao and M. Pietikäinen, "Dynamic texture recognition using local binary patterns with an application to facial expressions," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 6, pp. 915–928, Jun. 2007.

[228] B. Song *et al.*, "Recognizing spontaneous micro-expression using a three-stream convolutional neural network," *IEEE Access*, vol. 7, pp. 184537–184551, 2019.

[229] X. Zhao, Y. Lin, and J. Heikkila, "Dynamic Texture Recognition Using Volume Local Binary Count Patterns with an Application to 2D Face Spoofing Detection," *IEEE Trans. Multimed.*, vol. 20, no. 3, pp. 552–566, Mar. 2018.

[230] B. Solmaz, S. M. Assari, and M. Shah, "Classifying web videos using a global video descriptor," *Mach. Vis. Appl.*, vol. 24, no. 7, pp. 1473–1485, Sep. 2013.

[231] S. Rahman and J. See, "Spatio-temporal mid-level feature bank for action recognition in low quality video," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2016, vol. 2016-May, pp. 1846–1850.

[232] J. Päivärinta, E. Rahtu, and J. Heikkilä, "Volume local phase quantization for blur-insensitive dynamic texture classification," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, vol. 6688 LNCS, pp. 360–369.

[233] A. Husseis, J. Liu-Jimenez, I. Goicoechea-Telleria, and R. Sanchez-Reillo, "Dynamic Fingerprint Statistics: Application in Presentation Attack Detection," *IEEE Access*, vol. 8, pp. 95594–95604, 2020.

[234] "Statistics and Machine Learning Toolbox - MATLAB." [Online]. Available:

https://nl.mathworks.com/products/statistics.html. [Accessed: 08-Jun-2020].

[235] E. Tabassi, C. L. Wilson, and C. I. Watson, “Fingerprint Image Quality,” 2004.

[236] M. Hara, “Thoughts on Fingerprint Image Quality and Its Evaluation Thoughts on Fingerprint Image Quality and Its Evaluation Fingerprint Image Quality and Its Evaluation Fingerprint Image Quality and Its Evaluation,” in *NIST Biometric Quality Workshop II*, 2007.

[237] R. A. Hicklin, “IMPROVING THE RIGOR OF THE LATENT PRINT EXAMINATION PROCESS,” University of Lausanne, 2017.

[238] C. L. Wilson, C. I. Watson, and E. G. Paek, “Effect of resolution and image quality on combined optical and neural network fingerprint matching,” *Pattern Recognit.*, vol. 33, no. 2, pp. 317–331, Feb. 2000.

[239] N. K. Ratha and R. M. Bolle, “Effect of controlled image acquisition on fingerprint matching,” in *Fourteenth International Conference on Pattern Recognition (Cat. No.98EX170)*, 1998, pp. 1659–1661.

[240] S. Gu, J. Feng, J. Lu, and J. Zhou, “Efficient Rectification of Distorted Fingerprints,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 1, pp. 156–169, Jan. 2018.

[241] A. Jain and V. Bhateja, “A full-reference image quality metric for objective evaluation in spatial domain,” in *Proceedings of the 2011 International Conference on Communication and Industrial Application, ICCIA 2011*, 2011.

[242] J. D. Ruikar, A. K. Sinha, and S. Chaudhury, “Structural SIMilarity and correlation based filtering for Image Quality Assessment,” in *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*, 2014, pp. 476–479.

Annex I. Attacking a Smartphone Biometric Fingerprint System

Prior to performing the data collection (presented in Chapter 3), the attacker gained solid knowledge and experience in the subject of fingerprint presentation attacks. In addition to the theoretical knowledge, the attacker participated in an experiment given the task of creating a series of fake fingers in an attempt to unlock a variety of smartphones.

The three key factors in undertaking this study were that:

1. The attacker had no previous practical experience of fingerprint spoofing.
2. Materials used were able to be purchased through outlets such as Amazon or supermarkets. The attacker was able to research methods and materials on-line for a one-week period prior to the study.
3. The experiment was limited a 12-hour development and testing limit.

In the experiment, the smartphones are considered as black boxes that give a binary response to each attack, i.e. accept or reject. Then, the resistance of each smartphone to presentation attacks is evaluated by showing the proportion of successful attacks, as shown in Table I.

Table I. Attempts and successful attacks for each device

Smartphone	Total attacks	Rejected	Successful	Success rate
S01	20	17	3	15.0%
S02	30	9	21	70.0%
S03	52	13	39	75.0%
S04	10	1	9	90.0%
Total	**112**	**40**	**72**	**64.3%**

The attacks were performed using four PAI species. Table II analyses the success rate for each species by showing the proportion of successful attacks for each species.

Table II. Attempts and successful attacks for the used PAI species.

PAI species	Total attacks	Rejected	Successful	Success rate
Algenate	60	20	40	66.7%
White glue + graphite	30	8	22	73.3%
Plastilina	10	9	1	10.0%
Wax + conductive ink	12	3	9	75.0%
Total	**112**	**40**	**72**	**64.3%**

The main observations reported by the attacker are:

1. In the primary stages of the experiment, different presentation attack attempts were carried out and failed. They had not been reported since they were not detected by the sensors.

2. The results reporting started after defining the best PAI species for each smartphone. That is to say, for each smartphone (fingerprint sensor), there are species that work better than others, even if the sensors use the same sensing technology.
3. The attack success rate increases while the attacker keeps practicing. In other words, as the attacker keeps experimenting, his expertise increases, thus the attack potential increases.
4. The last experiment was performed on the device S04 after over 12 hours of practical work. The success rate was 90%.