Democratic and Popular Republic of Algeria

Ministry of Higher Education and Scientific Research

University of Kasdi Merbah, Ouargla

Faculty of New Information and Communication Technologies

Department of Electronic and Telecommunication

Detect Spoofing Using Convolutional Neural Network

Memory in order to obtain a:

ACADEMIC MASTER

Domain: Science and technology

Field: Electronic

Specialty: Electronic of Embedded Systems

Presented by:

BOUBLAL Hamza
SADAOUI Radouane
MOULAY OMAR Abderrahmane

Jury Members

President	CHAA Mourad	MCA - Ouargla University
Supervisor	BENLAMOUDI Azeddine	MCB - Ouargla University
Examiner	BENARABI Bilal	MCB - Ouargla University

Academic Year: 2019 – 2020

Democratic and Popular Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Kasdi Merbah, Ouargla
Faculty of New Technologies of Information and Communication (FNTIC)
Department of electronics and telecommunications

Detect Spoofing Using Convolutional Neural Network

MOULAY OMAR Abderrahmane
SADAOUI Redouane
BOUBLAL Hamza

Thesis to obtain the Master Degree in

Electronics of embedded systems

Supervisors: Dr. Azeddine BENLAMOUDI
Dr. khaled BEN SID

September 2020

Dedication

Dedicate this modest work to:

To my gracious parents
To my dear brothers
To the whole family of " Moulay Omar "
To all my relatives and friends
To every science student
For all who use science for happiness and the prosperity of humanity
Finally, I dedicate this modest work to all those I love and appreciate

Moulay Omar Abderrahmane

Dedication

Dedicate this modest work to:

My beloved parents.
My father"AMAR", who has the greatest merit for the support and guidance and who taught me the value of hard work.
To my brother and sisters.
To every family SADAOUI.
To my supervisor Azeddine Benlamoudi.
To all my friends and loved ones.
To all my teachers and everyone who taught me, and to every student of knowledge.

Sadaoui Redouane

Dedication

Dedicate this modest work to:
To My MOTHER a stronger and gentle soul who taught me to trust Allah, believe in hard work and that so much could be done with little.
To My FATHER for learning and honest living for us and for supporting and encouraging me to believe in myself.
To My WIFE and the mother of my children(YOUNES and ISRA), a companion of struggle and passion.
To My BROTHERS and My SISTERS those who stood and encouraging me and always support me in my life.
To every family BOUBLAL.
To my dearest friends, and my thanks go out to my teachers and friends who stood with me during this long journey of success.

BOUBLAL HAMZA

Acknowledgments

*First and foremost, praise to the **almighty ALLAH** for helping us to complete this project. Thanks to all the people who made it possible for students like us, special thanks to our graduation project supervisors **Dr. Azeddine BENLAMOUDI** for the efforts he did to provide us with all useful information and making the path clear for us to implement all the education periods in real time project design and analysis and for their patience and guidance throughout the semester, and for their continuous encouragement and support. Also, fully thanks to **Dr. Khaled BEN SID** for helping us. Special thanks to **Dr. Houssem Eddin DEGHA** and **Dr. Younes TAMISSA** for his time in order to help us in our project.*

Moreover, it is our duty to thank all the 2^{nd} year Master Electronics of embedded systems students. In addition, we would like to express our appreciation to our families for their support. At last, we would like to thank all the people who helped us, supported, and encouraged us to successfully finish our project.

Abstract

Although some progress has been achieved in the field of computer vision research is confirming the identity of the user, such as face recognition, fingerprints, and iris. It has been shown that face recognition techniques are vulnerable to spoofing attack, spoofing a face recognition system is easy to perform: all that is needed is a simple photograph of the user.

In this study, we dealt with the use of a convolutional neural network in terms of its structure and how it works in processing images to differentiate between real and fake faces, It is considered a solution to many computer vision problems in artificial intelligence such as image processing. We will process the image data in three stages : 1) Face alignment and preprocessing 2) feature extraction 3) Classification. The purpose of face alignment is to define the face in the photo, correct the shape of the face, and trim the area of interest, data extraction and classification are also done via the convolutional neural network which is used to distinguish between real and fake faces.

Finally, we mention the results obtained using the database (CASIA), as the experimental results were improved by increasing the number of epochs, also, the considered approach is suitable for real-time application.

Keywords

Computer Vision, Image Processing, Artificial Intelligence, Face Recognition, Spoof Attack, Convolutional Neural Network.

Résumé

Bien que certains progrès aient été réalisés dans le domaine de la recherche en vision par ordinateur pour confirmer l'identité de l'utilisateur, comme la reconnaissance faciale, les empreintes digitales et l'iris. Il a été démontré que les techniques de reconnaissance faciale sont vulnérables aux attaques par usurpation d'identité, l'usurpation d'un système de reconnaissance faciale est facile à réaliser: il suffit d'une simple photographie de l'utilisateur.

Dans cette étude, nous avons traité de l'utilisation d'un réseau de neurones convolutifs en termes de sa structure et de son fonctionnement dans le traitement des images pour différencier les visages réels et faux.Il est considéré comme une solution à de nombreux problèmes de vision par ordinateur en intelligence artificielle tels que l'image en traitement. Nous traiterons les données d'image en trois étapes: 1) Prétraitement et alignement des visages. 2) Extraction de caractéristiques 3) Classification. Le but de l'alignement du visage est de corriger la forme du visage et de rogner la zone d'intérêt, l'extraction et la classification des données se font également via le réseau neuronal convolutif qui sert à distinguer le réel du faux visages.

Enfin, nous mentionnons les résultats obtenus à l'aide de la base de données (CASIA), comme les résultats expérimentaux ont été améliorés en augmentant le nombre d'époques, également, l'approche considérée est adaptée à une application en temps réel.

Mote Clé

Vision Par Ordinateur, Traitement d'image, Intelligence Artificielle, Reconnaissance de Visage, Attaques par Usurpation d'identité, Réseau Neuronal Convolutif.

الملخص:

على الرغم من تحقق بعض التقدم في مجال بحوث الرؤية الحاسوبية في التأكد من هوية المستخدم مثل تمييز الوجوه وبصمات الأصابع وبصمة العين، الا ان تقنيات التعرف على الوجه لازالت عرضة للهجوم بانتحال الشخصية ،حيث يعد انتحال نظام التعرف على الوجه أمرا سهلا كل ماهو مطلوب صورة للمستخدم .

في هذه الدراسة تطرقنا لاستخدام الشبكة العصبية التلافيفية من حيث بنيتها وطريقة عملها في معالجة الصور للتفريق بين الوجوه الحقيقية والمزيفة ، اذ تعتبر حلا للكثير من مشاكل الرؤية الحاسوبية في الذكاء الاصطناعي مثل معالجة الصور، سنقوم بمعالجة بيانات الصور عبر مراحل ثلاث ١) محاذاة الوجه والمعالجة المسبقة ٢) استخراج البيانات ٣) التصنيف. الغرض من محاذاة الوجه هو تحديد الوجه في الصورة وتصحيح شكل الوجه وقص المنطقة المهتم بها ، كما يتم استخراج البيانات والتصنيف عبر الشبكة العصبية التلافيفية التي تستخدم للتمييز بين الوجوه الحقيقية والمزيفة.

اخيرا نذكر النتائج التي تم الحصول عليها باستخدام قاعدة البيانات $(CASIA)$ حيث كانت النتائج التجريبية تتحسن بزيادة عدد الحقب .كما ان النهج المدروس مناسب للتطبيق في الوقت الفعلي

الكلمات الدلالية:

الرؤية الحاسوبية، التعرف على الوجه ، الذكاء الاصطناعي ، معالجة الصور، هجمات الانتحال، الشبكة العصبية التلافيفية .

Contents

List of Figures

List of Tables

Acronyms

AI	Artificial Intelligent
ANN	Artificial Neural Network
CIR	Complementary Infrared
CNN	Convolutional Neural Network
CPU	Central Processing Unit
DNA	DeoxyriboNucleic Acid
DMD	Dynamic Mode Decomposition
DSIFT	Dense Scale Invariant Feature Transform
ELLR	Extended LikeLihood Ratio
FAR	False Acceptance Rate
FRS	Face Recognition System
IDA	Image Distortion Analysis
IQA	Image Quality Assessment
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HOOF	Histogram of Oriented Optical Flow
HSV	Hue, Saturation, and Value
LBP-TOP	Local Binary Patterns on Three Orthogonal Planes
LBPV	Local Binary Patterns Variance
LBP	Local Binary Patterns
LDA	Linear Discriminant Analysis

LED Light Emitting Diode

LLR LikeLihood Ratio

MBSIF-TOP Multiscale Binarized Statistical Image Features on Three Orthogonal Planes

MLPQ-TOP Multiscale Local Phase Quantization on Three Orthogonal Planes

NIR Near Infrared

POS Point Of Sale

PS Pictorial Structure

RBF Kernel Radial Basis Function Kernel

ReLU Rectified Linear Unit

RGB Red-Green-Blue

ROI Region Of Interest

SVM Support Vector Machine

YCbCr Luminance; Chroma Blue; Chroma Red

General Introduction

The general public needs to take security measures against the corrupting threat, and because biometrics in this security industry is the fastest-growing sector. One of the common technology is facial recognition methods, fingerprint recognition, handwriting authentication, hand geometry, retinal scanner, and iris scanner. One advancement that has been developed in recent years is for ease of use and experience with facial recognition technologies relative to other approaches, and it was extended to multiple defense systems. But, generally speaking, facial-recognition algorithms are unable to separate 'real' facial from 'not live' face which is a major security problem. It is a simple way facial expressions such as portrait portraits will circumvent facial recognition systems. To prevent such spoofing, a secure system requires the liveness detection.

Some examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions, or boarding a commercial flight. The main task of a security system is the verification of an individual's identity. The primary reason for this is to prevent impostors from accessing protected resources. General techniques for security purposes are passwords or ID cards mechanisms, but these techniques of identity can easily be lost, hampered, or maybe stolen thereby undermine the intended security. With the help of the physical and biological properties of human beings, a biometric system can offer more security for a security system.

In recent years, liveness identification has been a very important field of study in the fingerprint recognition and iris recognition communities. But methods are very minimal for coping with this issue in face recognition. Liveness is the process of differentiating the space of the trait between living and non-living. Imposters may seek to incorporate a great deal of spoofed bio-

metrics into the scheme. The efficiency of a biometric device would increase with the assistance of liveness detection. It is an essential and challenging problem that determines the secrecy of biometric system protection against spoofing. The normal methods of attacking in face recognition can be divided into many groups. The classification is based on what verification proof is given to the face verification system, such as a stolen photograph, stolen face pictures, recorded video, 3D face models with blinking and lip moving capabilities, 3D face models with different expressions, and so on. The anti-spoof problem should be solved well before facial recognition systems can be applied widely in our daily lives.

Figure 1: Example of face spoofing.

The issues about safety and privacy arise from users, so what happens if my biometric data is compromised? I can always change the password, but can I change the real face with some other method such as an image to hack the system? or how effective is this technique? or Can this algorithm achieve this precision?

In our project ***Detectionn Spoofing Using Convolutional Neural Network (CNN)***, we focused on two main aspects, the theoretical side and the practical side. On the theoretical side, it is divided into two chapters: First,we started in the **Chapter 1**, we studied a comprehensive theory about the overview of Biometric Spoofing. Then the **Chapter 2**, is an in-depth study of spoofing attacks in face recognition and methodology in face anti-spoofing. Next in the **Chapter 3**, we talked to the CNN system and what it consists of? and why we use this system and how important it's, also proper architecture to achieve the effective and security system.

After that in the **chapter 4**, we used the program software (Python) and it's packages (OpenCV, Tensorflow, Keras, numpy...), and we talked about the experiments and the results that we got. Finally, in conclusion, we have talked about the final result of our experiment. Then we have talked about the effectivity of this system and the technique using. We have talked also about future works.

1

Overview Of Biometric Spoofing

1.1 Introduction

The need for reliable user authentication techniques has grown in the face of rising safety concerns and accelerated networking, connectivity, and usability developments. Biometrics, defined as the science of identifying an individual on the basis of his or her legitimate method of identity determination. Biometric authentication or simply biometrics refers to the identification of an individual based on the physiological and behavioral characteristics such as the face, fingerprints, hand geometry, iris, keystroke, signature, voice, etc. Biometric systems offer a number of benefits over traditional authentication schemes.

They are inherently more reliable than password-based authentication as biometric characteristics can not be lost or forgotten; biometric characteristics are difficult to copy, share and distribute; and they require the person to be present at the time and place of authentification (See Figure 1.1). Thus, an authentication scheme based on biometrics is a powerful alternative to traditional authentication schemes [3].

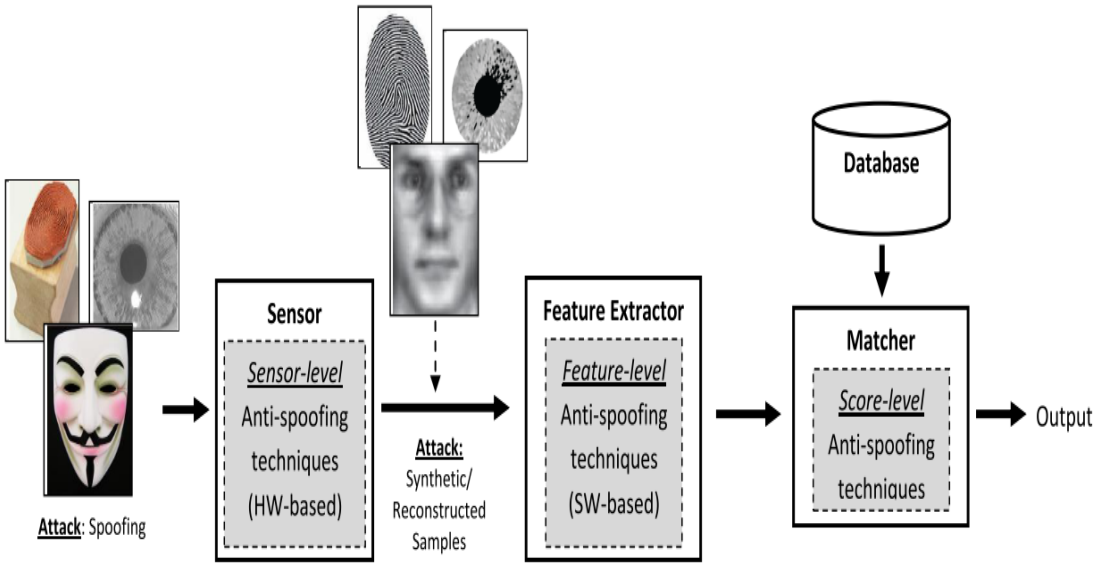


Figure 1.1: General diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated (sensor-level, feature-level, and score-level). Also displayed are the two different types of attacks for which anti-spoofing techniques may offer protection: spoofing and attacks carried out with synthetic or reconstructed samples [1]

1.2 Biometrics in General

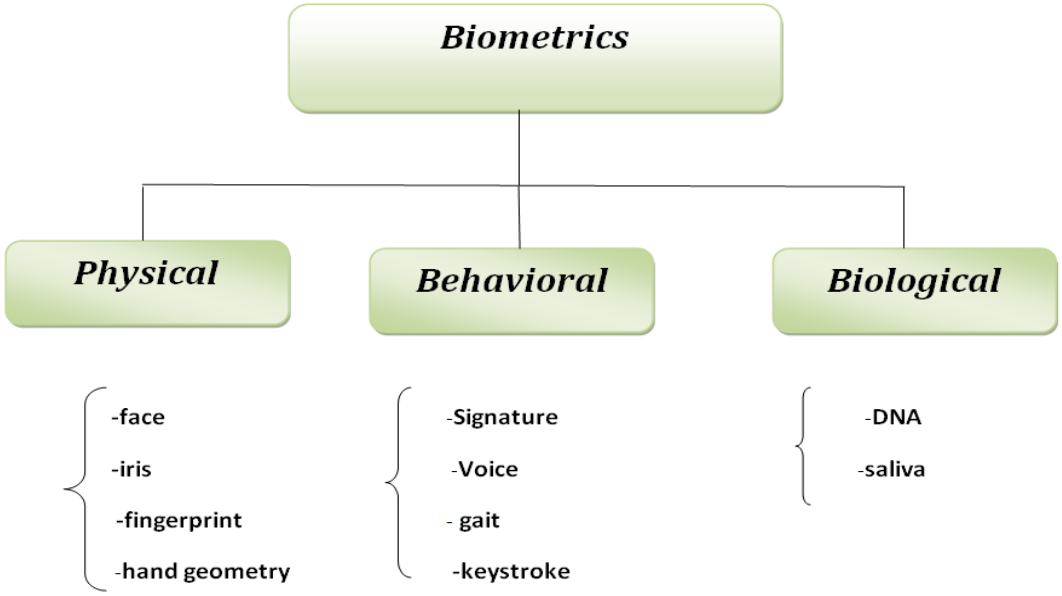


Figure 1.2: Biometrics types.

Biometrics is best described as a system of personal identity verification, meaning your personal identity is verified using individual and unique physical characteristics such as fingerprints, hand geometry, voice, eyes, handwriting, or facial recognition (See Figure 1.2). While this form of device is not commonly seen in most industries, biometrics has been around for some time it is most likely to be used in operations where there is a higher degree of protection in place, such as departments for research and development, military control centers, and buildings or departments which contain top-secret operations.

If your company is using biometrics, you need to provide in your appraisal analysis of the system's infrastructure, procedures, and organizational effectiveness. These programs have been shown to malfunction to the degree that they can allow access when that person has no clearance, or they can refuse access even though the individual who demands access has the correct credentials levels in the authorisation. Each when a failure happens, protection should log the failure and any remedial measures that they have taken [21].

Biometrics is the use of physiological or behavioral or biological characteristics to determine or verify identity. Several aspects of this definition require elaboration. All biometric

identifier scan be divided into three big groups: Physiological, Behavioral, and biological.

1.2.1 Physiological analysis

The subsections below introduce a brief overview of mostly used physiological characteristics for the automatic recognition of individuals.

1.2.1.A Fingerprints

Biometric authentication systems based on fingerprints became one of the most common and effective authentication techniques for the identification and verification processes of one's identity [22–24].

Among other biometric security methods. This method of biometric authentication was established based on the natural truth which indicates that each person has unique fingerprints of his / her hand which distinguish him/her from others. In addition, each person has a different fingerprint. Although when two identical twins have a resemblance in their visible characteristics, they still have completely different prints on the fingers of each one [24] Figure 1.3 shows a sample of a human fingerprint.

Figure 1.3: Sample of human fingerprint. [2]

1.2.1.B Iris

Iris is the circular colored component which is in the middle of the eye. The peculiarity of the iris pattern offers an important individual recognition scheme. It has a specific network

of tissues that are visibly recognized based on the biological composition of the iris. An individual's iris, however, forms during the first year of life when the iris properties can not be genetically ngineer (See Figure 1.4) [22, 23] .

Figure 1.4: Iris recognition system [2].

1.2.1.C Face

The facial features played a major role in people's identification for a long time. It was a common method of biometric identification, based on the face of each person [22–24]. Computers have contributed to the automatic identification of individuals, using the obvious facial characteristics that led to the Face Recognition System (FRS) becoming widely popular. A lot of commercial software is designed to do the real recognition of human facial features (See Figure 1.5).

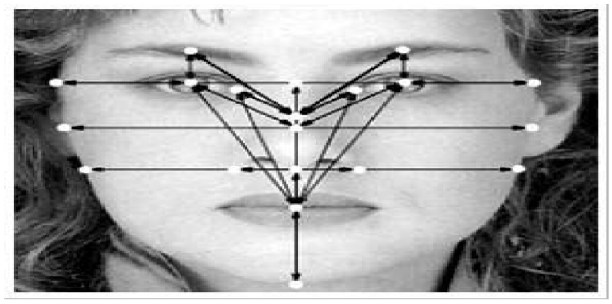


Figure 1.5: Automatic face recognition system [2].

1.2.1.D Hand Geometry

Hand geometry is the use of geometric shape of the hand for recognition purposes. The method is based on the fact that the shape of the hand of one person differs from the shape of

the hand of another person and does not change after certain age [25]. But it is not unique (See Figure 1.6).

Figure 1.6: Example of hand scanning system [3].

1.2.2 Biological analysis

There are several aspects of the present invention relating to a device for the acquisition of biological information, a method for the acquisition of biological information, and a device for biometrics which uses biological information. Biometrics have been implemented to authenticate an approved person, using biological details such as DeoxyriboNucleic Acid (DNA) and saliva [26].

1.2.2.A DNA

Not long ago, Russia's show business was full of rumors that one of Russia's famous singers has two fathers, and every father tried his best to influence the son. Special services have been produced and the situation addressed but only one item has been of concern to the public: Who was the singer's real father? And the singer was confused. The singer and both his father plans to take the DNA test in one of the programs [3] (See Figure 1.7).

Figure 1.7: Example of DNA scanning [3].

1.2.2.B Saliva

Saliva as a diagnostic fluid has significant biochemical and logistical advantages when compared to blood. Bio-chemically, saliva is a clear liquid with an average protein concentration of 1.5 to 2.0 mg/ml. As a consequence of this low protein concentration, it was once assumed that this was a major drawback for using saliva as a diagnostic fluid; however, current ultrasensitive analyte detection techniques have eliminated this barrier. Saliva specimen preparation is simple involving centrifugation prior to storage and the addition of a cocktail of protease inhibitors to reduce protein degradation for long-term storage (See Figure 1.8) [27].

Figure 1.8: Example of saliva [4]

1.2.3 Behavioral analysis

Behavioral biometrics is the area of research relating to the identification of unusual characteristics that are detected and measured in human behaviors. The concept contrasts with physical biometrics, including inherent human attributes such as fingerprints or patterns of iris. Methods of behavioral biometric authentication include keystroke analyses, gait analysis, speech ID,

features of mouse use, signature analysis, and cognitive biometrics. Behavioral biometrics are used in financial institutions, businesses, government facilities, and retail point of sale Point Of Sale (POS) as well as an increasing number of other environments for secure authentication.

1.2.3.A Voice

Voice [3] is unique as are many other characteristics used for biometric methods. Like gait style, analyzing the voice, and identifying the person takes a fairly little time. Voice is presented as a numerical sound model in biometrics or "voiceprint" (See Figure 1.9).

Figure 1.9: Example of voice [5]

1.2.3.B Keystroke

The keystroke [3] is the action of the human means to suggest that on a certain basis the recognition takes place, the various humans have the different techniques of pressing keys (See Figure 1.10).

Figure 1.10: Example of Keystroke [6].

1.2.3.C Signature scanning

Another biometric activity is a signature that allows the data to be extracted by that particular person's signature (See Figure 1.11).

Figure 1.11: Example of signature [7]

1.2.3.D Gait

Gait [28] biometrics tracks phase patterns by video analysis, and then converts the mapped data into a mathematical equation. This form of biometric is unobtrusive, making it perfect for large surveillance of crowds as it can identify people from afar fast (See Figure 1.12).

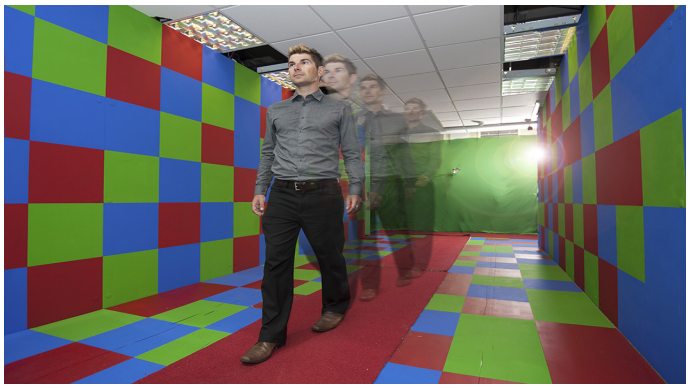


Figure 1.12: Example of Gait [8].

1.3 Definition of biometric spoof

Biometric spoofing is a method of fooling a biometric identification management system in which an artificial object (such as a fingerprint mold made of silicon) is presented to a biometric

scanner imitating the unique biological properties of a person that the system is designed to measure so that the system can not distinguish the artifact from the actual biological target [29].

One growing concern is biometric spoofing. Everywhere in our day-to-day lives, we leave fingerprints, so the chance of someone lifting and copying them is real. At present, it's only academics who do spoofing and copying for testing purposes and it's not a mainstream activity, but it could be soon as more corporations and governments around the world embrace biometrics. For management of identification [30]. Many people want to identify as coded biometric physiological features but they aren't. Our faces and irises are visible to each and every one of us.

May record sounds. Fingerprints and DNA are left wherever we go and it has been proven that these are real threats to be repeated for biometric spoofing schemes [31].

1.4 Definition of biometric anti-spoofing

Despite some ongoing efforts and initiatives to create a consistent and structured vulnerability-related nomenclature, a general agreement on the appropriate vocabulary to be used in each case has not yet been achieved by the biometric community [32–34]. Given the absence of The present article will adopt a closed description of specialized literature in which biometric spoofing is widely understood as being capable of fooling a biometric system into identifying an illegitimate individual as a real one by displaying a fake fabricated version to the sensor.

External biometric feature (i.e., artifact). Such attacks often referred to as direct attacks [10], fall within the broader category of "presentation attacks," described in the current draft $ISO/IEC30107$ specification as "presentation of an item or human feature to the biometric capture subsystem in a manner that could conflict with the biometric system's intended policy" [32]. Such a larger range of attacks often entails introducing human features (not only digital artifacts) such as dead fingers to the acquisition system, mutilated characteristics, actually forced living traits, or a different living feature Such as dead fingers, mutilated traits, real coerced living traits or other living traits (i.e., zero-effort impostor attempts to exploit the False Acceptance Rate (FAR), biometric systems) [33]. Spoofing is therefore the use of an artifi-

cial trait to impersonate a different user or to create a new genuine identity. Typically several scenarios are designed for spoofing attacks depending on the type of biometric system being considered [35].

1. Verification system: in the most common case, spoofing is performed at the time of authentication by presenting a fake physical copy of the genuine user feature to the sensor. Such an artifact is obtained and compared to the true user's enrolled actual example.

2. Closed-set authentication method/identification system: spoofing can also be done at the registration point by creating a new artifact identity (not actually imitating any actual user trait) which may be used later by various users to enter the device.

3. Open-set recognition system: this is usually a situation where a new identity is produced using a spoofing tool to prevent being placed on a watch list (e.g. acquiring a VISA to enter a country illegally) [29].

1.5 Conclusion

A possible area of research has been to protect vital and sensitive networks from being improperly accessed by impostors. Biometric security-based authentication gained significant attention for its accuracy, reliability, universality, and durability, etc. This chapter provided an overview of the most commonly used biometric authentication strategies and we have focused on physiological and biological and behavioral methods of biometric protection, we also addressed us to know biometric spoof and biometric anti-spoofing. The next chapter presents a review of the most important methods for detecting face liveness. Then is discussed noting the benefits and drawbacks of multiple approaches to detecting face anti-spoofing.

2

Spoofing attacks in face recognition

Contents

2.1 Introduction

Although great advances have been made in the face against spoofing over the last decade, the techniques of face spoofing have also evolved and become increasingly sophisticated. Inevitably, many of the current anti-spoofing facial methods are still vulnerable to spoofing, including numerous commercial devices that appear to have a degree of embedded face spoof detection. A coherent face spoofing and anti-spoofing survey [36] clearly indicates that face spoofing is still a huge challenge for existing face recognition systems. Namely, the identification of face spoofing attacks needs several problems to be discussed.

Automated face recognition systems have been implemented in numerous implementations over the past decade because of the rich features of the face that provide a clear biometric cue.

Face spoof attack is a method through which a malicious individual may masquerade a face recognition device as a licensed customer and thereby unlawful access and benefits [37]. Often known as ”direct attack” or ”presentation attack,” facial spoofing attack. Face spoofing also poses a big problem for businesses offering facial biometric identity detection solutions [38].

It is worth mentioning that face spoofing does not require advanced technical skills, thereby increasing the number of potential attackers. In addition, facial images captured from spoofing attacks can look very similar to images captured from real ones, making it very hard to detect face spoofing attacks.

2.2 State of the art in face anti-spoofing

The pioneering studies on biometric vulnerabilities stressed the need to develop effective protection schemes against face spoofing attacks. A number of facial anti-spoofing or animation detection methods have been proposed over the last two decades. The published facial anti-spoofing techniques can be widely grouped into two categories (Hardware based techniques and Softwar based techniques) [20].

2.2.1 Hardware based techniques

Several hardware-based facial vivacity detection techniques were developed based on imaging technologies. Many applications in this area use light spectrum beyond the visible range (e.g., 3D depth [39], complimentary infrared Complementary Infrared (CIR), or near-infrared Near Infrared (NIR) images [40]) to compare reflectance detail on actual faces and spoofing materials. To this end, a particular system of Light Emitting Diode (LED) and photo-diodes is used at two different wavelengths. Recently, authors in [37] performed a face-anti-spoofing thermal imaging analysis by gathering large thermal face images database for actual and spoofed access attempts.

Multimodal biometric devices are also widely thought to be automatic anti-spoofing strategies. To this end, Chatty et al. [41] merged face and voice and studied the association between the action of the lips and the speech being made. In fact, the machine used an anti-spoofing microphone and a voice analyzer. On the whole, though hardware-based solutions tend to provide better results.

2.2.2 Software based techniques

To detect the spoof attacks, software-based techniques use the basic Red-Green-Blue (RGB) images. These approaches can be categorized into strategies that are static and dynamic dependent.

The static-based techniques are applied to a single image, while video sequences are applied to the dynamic-based techniques. Below we give respectively the latest work on both static and dynamic techniques.

The most popular methods of differentiating between the actual faces and the artificial ones are based on inspection of the texture. Counter-measures in texture analysis take advantage of texture patterns that may appear unusual when analyzing the image details. Examples of visible texture patterns are perception errors or blur in the overall shot. In [42], they defined a print-attack detection approach by leveraging the variations in the 2-D Fourier spectra by comparing the client face hard copies and actual accesses.

The approach performs well with specimens of the assaulted identification down-sampled

but is likely to struggle with images of higher quality. Li *et al.* [42] observed print attacks by leveraging variations in hard-copies in faces and actual accesses in the 2-D Fourier spectra. The system performs well in down-sampled object attacks but is likely to fail in samples of higher quality. *et al.* [43] used a linear Support Vector Machine (SVM) classifier to evaluate the micro-textures to detect spoof attacks.

In [44,45], the authors used the Local Binary Patterns (LBP) as a descriptor for spoof attack detection. In [46], the authors have used another version of the LBP descriptor, Local Binary Patterns Variance (LBPV), which was used to discriminate between the true and the false aspects. Image Distortion Analysis (IDA). Four distinct characteristics were used to represent the facial images: specular reflection, blurriness, chromatic moments, and a variety of colors.

These features will capture the variations between the real and the fake images without recording the user-identity details. Patel *et al.* [47] Examined the effect on the performance of the LBP and Dense Scale Invariant Feature Transform (DSIFT) by the different channels of the RGB color spaces (R, G, B, and Gray Scale) and the different facial regions methods DSIFT dependent. Their studies show that the best results are obtained by removing the material from the red channel.

Boulkenafet *et al.* [48] Suggested a face anti-spoofing approach based on an analysis of the color texture. Having represented the RGB images in two color spaces: Hue, Saturation, and Value (HSV) and Luminance; Chroma Blue; Chroma Red (YCbCr), used the LBP descriptor to isolate the texture characteristics from each wave and then merged these characteristics to discriminate between real and fake faces.

Galbally *et al.* [49] Proposed an Image Quality Assessment (IQA) using 14 quality measures to distinguish between the real and the fake faces. In [50] the same authors evaluated 25 different quality measures, which were also used for fingerprint and iris anti-spoofing. Some approaches such as [51, 52] have recently used detailed details from the user to improve the efficiency of facial anti-spoofing methods based on the texture. Biggio *et al.* [53] Tackled the issue of biometric spoof attacks by using two face and fingerprint versions. Various score-fusion rules were checked, such as Sum, Product, and Weighted sum by Linear Discriminant Analysis (LDA), LikeLihood Ratio (LLR), and Expanded Extended LikeLihood Ratio (ELLR).

Analysis of motion one is interested in detecting clues produced when two-dimensional counterfeits are introduced to the input camera system [44, 54, 55], e.g. images or video clips. *et al.* [56] used a simplistic optical flow analysis followed by a heuristic classifier to determine the trajectories of selected parts of the face from a short sequence of images. A method [57] was developed by the same writers to combine these scores with liveness properties such as eye-blinks or mouth motions. Bao *et al.* [58] suggested a method for detecting attacks on planar media using an estimate of the optical flow-dependent motion.

Using kernel discriminant analysis fusion, Arashloo *et al.* [59] merged two spatial-temporal descriptors Multiscale Binarized Statistical Image Features on Three Orthogonal Planes (MBSIF-TOP) and Multiscale Local Phase Quantization on Three Orthogonal Planes (MLPQ-TOP). Pereira *et al.* [60] also experimented with the complex texture of Local Binary Patterns on Three Orthogonal Planes (LBP-TOP) based on to distinguish between the real and the fake human. The last method showed better performance than the simple LBP methods proposed in [44–46].

The reason for LBP-TOP gives good results is that temporal information plays an important role in the anti-spoofing of the face. Pinto *et al.* [61] have suggested a temporal and spectral based approach Knowledge that uses the time-spectral features as low-level descriptors and the visual codebook definition to identify descriptors of mid-level features. Tirunagari *et al.* [62] suggested a Dynamic Mode Decomposition (DMD) algorithm capture the visual dynamics when LBP captures the complex patterns.

Bharadwaj *et al.* [63] took the Eulerian motion Magnification to emphasize signs of motion. It was observed that extracting Histogram of Oriented Optical Flow (HOOF) from the enhanced video provides an enhanced result about the state-of-the-art performance in the Replay-Attack database. Auch Komulainen *et al.* [64] used a fusion Enhancing recognition efficiency between the motion and the texture properties.

Kollreider Komulainen *et al.* [64] suggested innovative techniques to avoid sophisticated spoofing attempts by observing only the action of the mouth, such as replayed images. Detection of liveliness attempts to catch signs of life from consumer photographs by examining random gestures that can not be observed in Photographs such as eye blinks which can occur in humans once every 2-4 seconds [65, 66]. Pan *et al.* [67] used the fact that humans blink once every (2-4

s) and suggested an anti-spoofing strategy based on the wink of an eye.

Garcia *et al.* [68] suggested the identification of face spoofing by looking for Moiré patterns because of the optical grid overlap. Their detection is based on Frequency Domain peak detection. They used the grouping using SVM with the Radial Basis Function Kernel (RBF Kernel). They carried out their studies on the applications Replay Attack Corpus and Moiré.

Other facial anti-spoofing techniques are based on 3D modal textures, such as [69, 70]. The attacker uses a mask in a 3D modal to spoof the system because the use of wrinkles would be a great assistant in detecting the attack.

In [69], they presented a study that addresses the problem of spoofing by analyzing the feasibility of performing low-cost attacks with self-manufactured products 3D printed models to the 2.5D and 3D facial recognition systems. Erdogmus and Marcel [70] examined the spoofing potential of the subject-specific 3D facial masks for different recognition systems and addressed the problem of detection of this more complex type of attack. Also, the authors performed experiments on two different databases.

Recently, in the face of anti-spoofing, deep learning techniques have been used, in particular with the CNN. For example, authors in [71] concentrated on two general-purpose approaches using coevolutionary networks to create image-based anti-spoofing systems. With three biometric modalities, iris, face, and fingerprint, their systems struggle with numerous attack types. The first approach involves studying sufficient coevolutionary network architectures for each area, while the second approach focuses on studying the network's weights by back-propagation.

Below, we present all previous work in face antispoofing techniques, but we focus only on those that are thematically closer to our objectives and contributions (see Table 2.1).

Table 2.1: A summary of published methods on face spoof detection [20]

Athors	Methods	Data-bases	years
Kollreider *et al.* [72]	Motion	MIT–CMU YALE Recaptured	2007
Biggio *et al.* [53]	Multimodal	LivDet11 Photo Attack Personal Photo Attack Print Attack	2011
Chingovska *et al.* [45]	Texture	REPLAY ATTACK CASIA FAS NUAA photograph imposter	2012
Määttä *et al.* [44]	Texture	Yale Recaptured PRINT ATTACK	2012
Erdogmus & and Marcel [70]	3D	Morpho 3D Mask Attack	2013
Yang *et al.* [73]	Texture	NUAA photograph imposter CASIA FAS PRINT ATTACK	2013
Galbally & Marcel [49]	Image Quality Assessment	CASIA FAS REPLAY ATTACK	2014
Bharadwaj *et al.* [63]	Motion	PRINT ATTACK REPLAY ATTACK CASIA FAS	2014
Pereira *et al.* [60]	Motion	REPLAY ATTACK CASIA FAS	2014
Menotti *et al.* [71]	Deep Learning	Warsaw, Biosec & MobBIOfake Replay-Attack & 3DMAD Biometrika, CrossMatch, Italdata & Swipe	2015
Garcia & Queiroz [68]	Moiré-Pattern	Replay Attack Moiré	2015
Yang *et al.* [51]	Person-Specific	CASIA FAS REPLAY ATTACK	2015
Chingovska & Anjos [52]	Person-Specific	REPLAY ATTACK	2015
Wen *et al.* [74]	Motion	REPLAY ATTACK CASIA FAS MSU MFS	2015
Pinto *et al.* [61]	Motion	CASIA FAS REPLAY ATTACK UVAD 3DMAD	2015
Tirunagari *et al.* [62]	Motion	PRINT ATTACK REPLAY ATTACK CASIA FAS	2015
Arashloo & Kittler [59]	Texture	REPLAY ATTACK CASIA FAS	2015
Boulkenafet *et al.* [48]	Colour Texture	NUAA photograph imposter CASIA FAS REPLAY ATTACK	2015
Patel *et al.* [47]	Colour Texture	REPLAY ATTACK CASIA FAS MSU MFS	2015
Galbally and Satta [69]	3D	3DFS-DB EURECOM MASK-ATTACK DB IDIAP MASK-ATTACK DB	2016
Zhao *et al.* [75]	Dynamic Texture	CASIA FAS	2017
Gan *et al.* [76]	3D CNN	REPLAY ATTACK CASIA FAS	2017
Tang *et al.* [77]	Fusing multiple deep features	CASIA FASD REPLAY-MOBILE OULU-NPU	2018
Xiaoguang and Zhang *et al.* [78]	CNN-LSTM	REPLAY ATTACK MSU-MFSD	2019
Nagpal *et al.* [79]	A performance evaluation of CNN	MSU-MFSD	2019

2.3 Face Spoofing Databases

The first public dataset for the study of face recognition anti-spoofing appeared in 2010, the facial anti-spoofing directions explored in this memory are based largely on five publicly available databases [20]: NUAA Photo Imposter Database, Replay-Attack Database, CASIA Face Anti-Spoofing Database, MSU Mobile Face Spoofing Database, and OULU-NPU Face PAD Database. In our work, we used only the CASIA Face Anti-Spoofing Database.

2.3.1 CASIA Face Anti-Spoofing Database

CASIA Face Anti-spoofing Database (CASIA-FASD) [80] overcomes some of the main disadvantages of the NUAA database. For example, the number of clients is as many as 50, and the samples are in a video format. Furthermore, it provides a larger diversity of spoofing attacks, of which there are as many as 3 types: warped print, perforated print, and video attacks. The overall diversity of the database is augmented by using 3 different recording devices for the samples: an old web-camera recording low-quality samples with resolution 640×480, a new web-camera recording normal-quality samples with a resolution of 640×680, and a high-resolution camera recording high-quality samples with a resolution of 1280×720. The database is recorded in adverse conditions, and the majority of attacks are close-up.

The total number of samples in the database is 600 (150 real accesses and 450 attacks). The eye regions were cut off in order to create photographic masks and eye blinking was simulated either by the attacker or by sliding another piece of paper behind the resulting cut photo. The video attacks were executed using an iPad with a screen resolution of 1024×768. Altogether the database consists of 600 video clips and the identities are divided into subject-disjoint subsets for training and testing (240 and 360, respectively).

Since the main purpose of the database is to investigate the possible effects of different fake face types and imaging qualities, the test protocol consists of seven scenarios in which particular train and test samples are to be used. The quality test considers the three imaging qualities separately, low (1), normal (2), and high quality (3), and evaluates the overall spoof detection performance under a variety of attacks at the given imaging quality. Similarly, the

fake face test assesses how robust the anti-spoofing measure is too specific fake face attacks, warped photo (4), cut photo (5), and video attacks (6), regardless of the imaging quality. In the overall test (7), all data is used to give a more general evaluation. Examples of the different scenarios in the database can be seen in Figure 2.1.

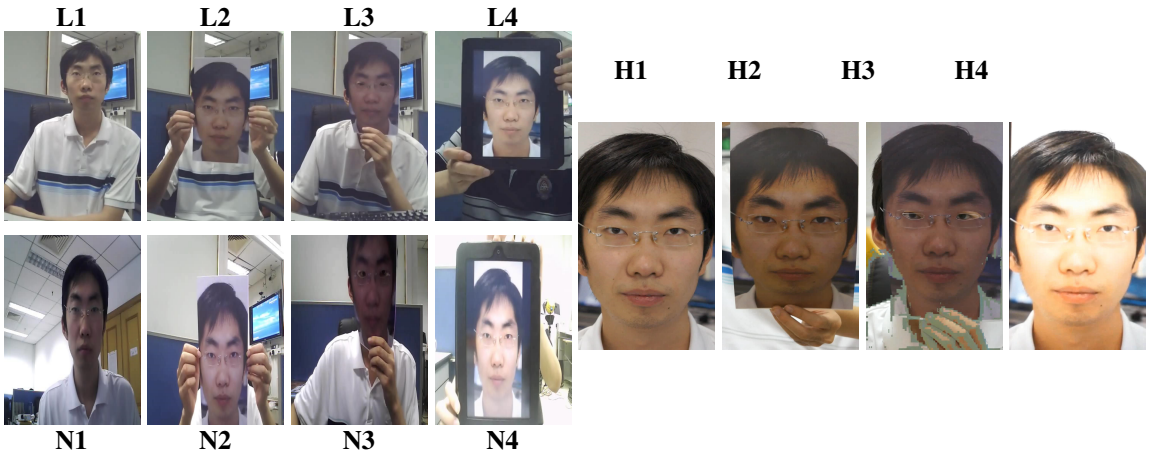


Figure 2.1: Samples from the CASIA face anti-spoofing database. L, N and H for Low, Normal and High quality, respectively. 1, 2, 3 and 4 for real face, warped photo, cut photo and video attacks, respectively.

2.4 Methodology in face anti-spoofing

The use of the face authentication system has become more common in recent years compared to other types of protection, such as fingerprint [81] and the iris system [82]. The fingerprint is fading with age, requiring clean hands and taking more time to scan of iris. This preliminary study helped us get an insight into the issue of face spoofing and countermeasures. Anti-spoofing faces can be divided into three main components: face preprocessing, extraction of features, collection and classification of features [83–87].

2.4.1 Face preprocessing

Facial processing is an important part of facial recognition because the face is most common for people to know each other. But the last one is easily affected by the light condition and facial expression changing and other reasons [88]. So before extracting features we can preprocess

face images to improve the face recognition rate. We explain how we use preprocessing step by step which are: face detection, eye localization, and face normalization.

2.4.1.A Face Detection

The dace detection task is easily done from the perspective of the human visual tasks but when it comes in the view of the computer it is a little bit difficult. An image is given in which the faces are detected leaving the illumination, pose variation, and lighting factors [9]. The faces of the people have been detected as shown in Figure 2.2.

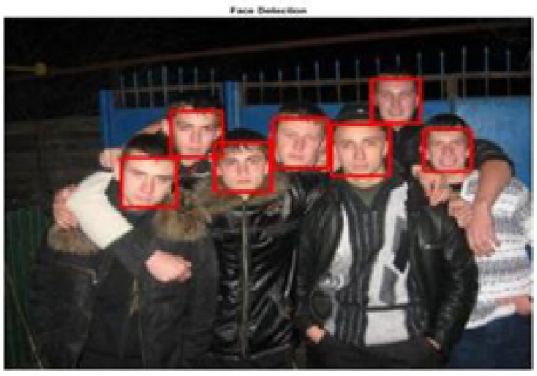


Figure 2.2: Example of face detection [9]

.

2.4.1.B Eyes localization

Detection of the position of the eyes in the face is crucial for the creation of many applications such as facial recognition, facial expression, face anti-spoofing, age estimation, and gender classification, etc. Our goal is to localize the eyes precisely rather than describe the whole face object using facial features. So, a Pictorial Structure PS model which focuses more on the points that count is more appropriate. The difference between eye detection and eye localization is that the last one is given a more accurate prediction of the eye positions than the first one as shown in Figure 2.3.

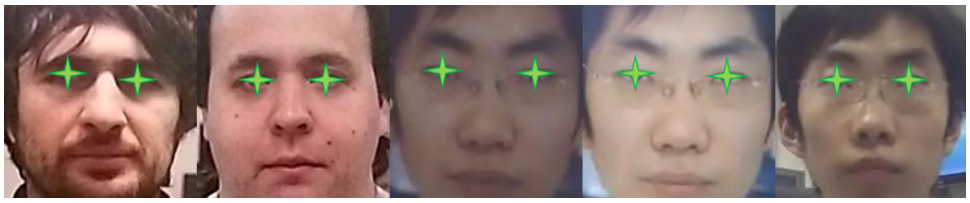
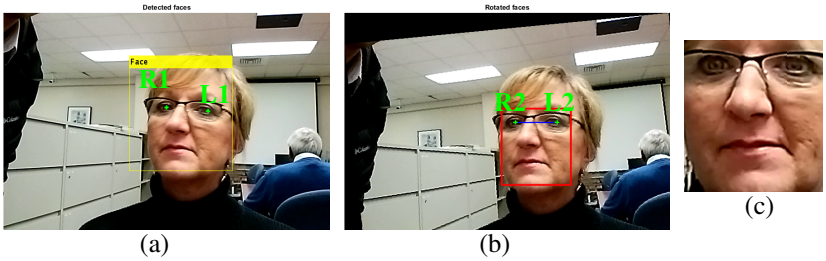


Figure 2.3: Example eye localization by PS algorithm [10].

2.4.1.C Face normalization

We have to normalize the face after face detection and eye localization. In face normalization, we rotate and crop the face depending on the eye coordinate (See Figure 2.4). Obtained through the eye localization algorithm [89]. In Figure 2.5 and equations below we attempt to illustrate how to rotate and crop the face using the eye coordinates. Then, we resize the ROI after rotating and cropping the face ROI.



(a) (b) (c)

Figure 2.4: Example of face alignment. a) face & eyes detection b) pose correction c) face ROI [10].

$$L1_x = (L_x \times (m/100) + bbox(1), L_y \times (m/100) + bbox(2))$$
$$R1_x = (R_x \times (m/100) + bbox(1), R_y \times (m/100) + bbox(2)) \tag{2.1}$$

$$\theta = tan^{-1}(\frac{R1_y - L1_y}{R1_x - L1_x}) \tag{2.2}$$

$$
\begin{aligned}
L2_x &= C_x + (L1_x - C_x).cos(\theta) - (L1_y - C_y).sin(\theta) \\
L2_y &= C_y + (L1_x - C_x).sin(\theta) + (L1_y - C_y).cos(\theta) \\
R2_x &= C_x + (R1_x - C_x).cos(\theta) - (R1_y - C_y).sin(\theta) \\
R2_y &= C_y + (R1_x - C_x).sin(\theta) + (R1_y - C_y).cos(\theta)
\end{aligned}
\tag{2.3}
$$

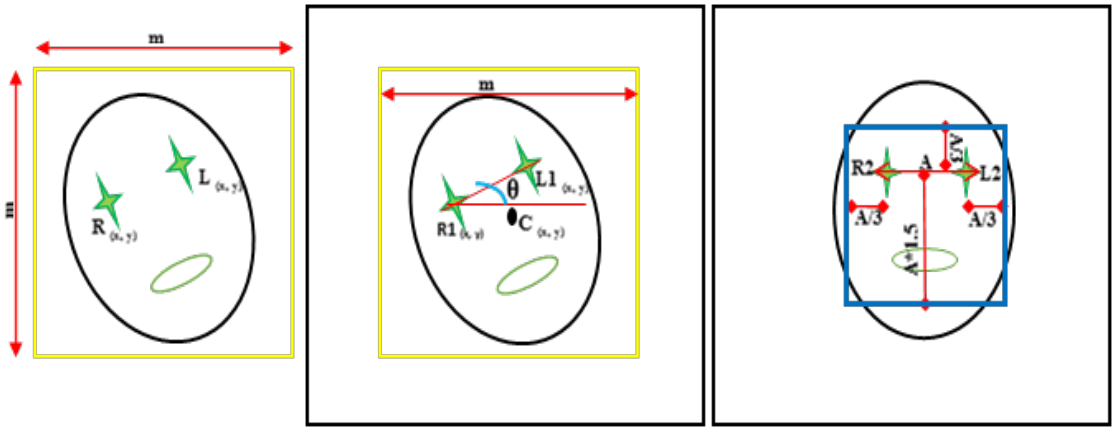


Figure 2.5: Detail of rotate & crop of face [10].

2.4.2 Feature extraction

The extraction of features is a method of reduction of dimensionality by which the initial collection of raw data is reduced to more manageable classes. A characteristic of these large data sets is a large number of variables that require a lot of computing resources to process. Extraction of the function is the term for methods selecting and/or combining variables into features, effectively reducing the amount of data to be processed, while also representing the original data set correctly and completely [90].

2.4.2.A Convolutional Neural Network

Computer vision is evolving rapidly day-by-day. Its one of the reason is deep learning. When we talk about computer vision, a term convolutional neural network [11] (abbreviated as

CNN) comes in our mind because CNN is heavily used here. Examples of CNN in computer vision are face recognition, image classification, etc. It is similar to the basic neural network. CNN also have a learnable parameter like neural network i.e, weights, biases, etc.

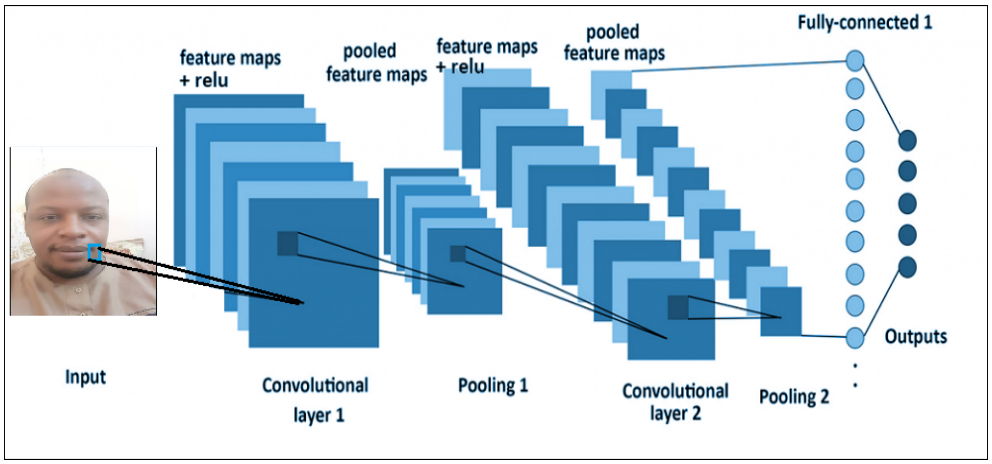


Figure 2.6: convolutional neural network [11]

2.4.3 Classification

Image classification is the process of labeling images according to predefined categories. The process of image classification is based on supervised learning. An image classification model is fed a set of images within a specific category. Based on this set, the algorithm learns which class the test images belong to, and can then predict the correct class of future image inputs, and can even measure how accurate the predictions are [91]. We will create an image classifier of our own that can distinguish whether a given pic is of a real or fake face or something else depending upon your fed data. To achieve our goal, we will use one of the famous machine learning algorithms out there which are used for image classification .

2.5 Conclusion

In this chapter, we begin with a brief overview and reference to general biometrics and face anti-spoofing recognition that is discussed in two sections as face spoofing and facial anti-spoofing. Next, we showed the state of the art. Since the variations due to facial changes are

discussed in this study, we provided an in-depth overview of these variations for the current state. Then we gave a brief description of the publicly available face spoofing databases, differing in data format, number of clients and samples, protocol, types of attacks. In the next chapter, we will study the CNN in image processing to obtain better results in combating spoofing attacks.

3

Convolutional Neural Network

Contents

3.1 Introduction

In recent times, with the rise of the Artificial Neural Network (ANN), the field of machine learning has taken a dramatic twist. These biologically inspired computational models in common machine learning tasks can exceed the performance of previous forms of artificial intelligence by far. One of the most impressive architectural forms of ANN is that of the CNN. The last one is primarily used to solve difficult image-driven pattern recognition tasks and offer a simplified way of getting started with ANNs with their precise yet simple architecture [92]. A CNN is a deep neural network class that is widely used in computer vision. The building blocks of the network are repeatedly altered during the training process so that the network achieves optimal performance and classifies images and objects as accurately as possible (See Figure 3.1).

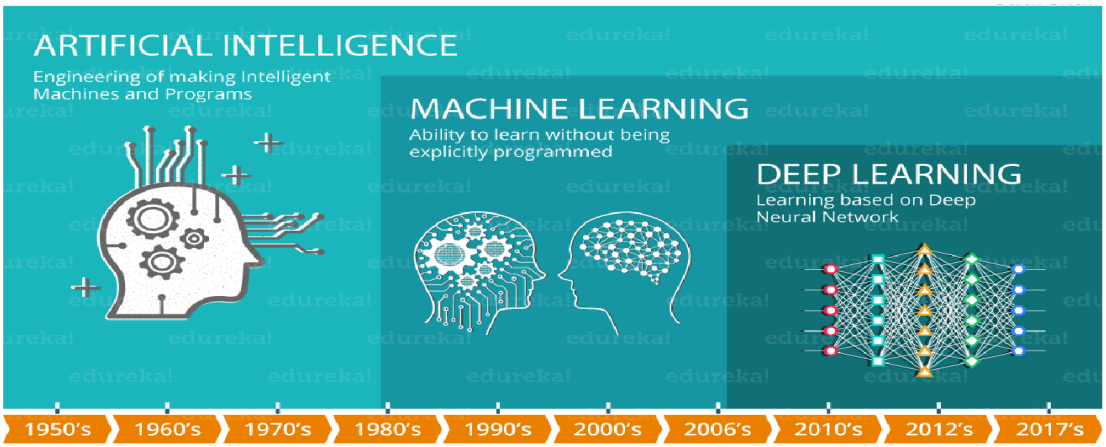


Figure 3.1: AI Technologies Timeline [12].

3.2 Architecture

One of the techniques used to do image classification and image recognition in neural networks is CNN. It is designed with multiple layers of arrays to process the data. This type of neural network is used in applications such as imaging or face recognition. The key distinction between CNN and other neural networks is that CNN functions as a two-dimensional sequence of data. It acts directly on the images instead of relying on the retrieval of features as most

neural networks do (See Figure 3.2).

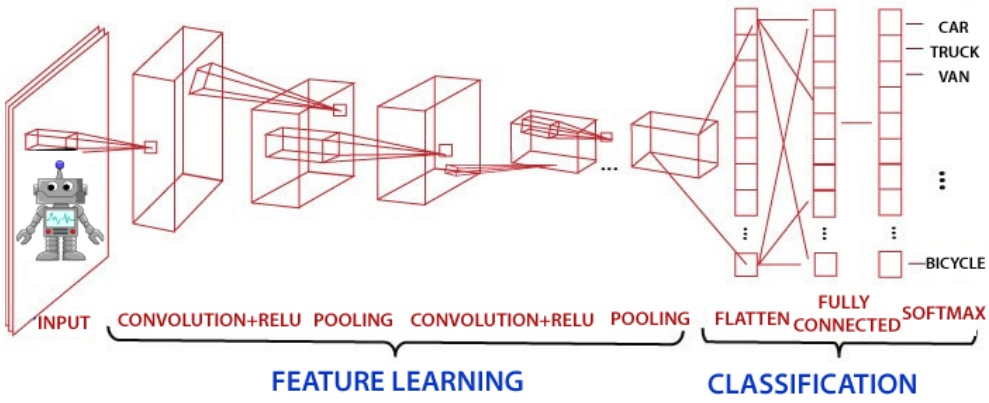


Figure 3.2: Convolutional Neural Network [13]

3.3 Layers

As we described above, the CNN is a series of layers, and every layer of a CNN transforms one volume of activations to another through a differentiable function. To create CNN architectures, we must use three major types of layers: Convolutional Layer, Pooling Layer, and Fully-Connected Layer.

3.3.1 Convolution Layer

The convolution layer [14] is the first layer where features are derived from an input image. The convolutional layer maintains the relation between pixels by learning image features using a small square of input data. It is a mathematical operation that involves two inputs such as a matrix of images and a kernel or filter (See Figure 3.3).

- The dimension of the image matrix is $h \times w \times d$.
- The dimension of the filter is $fh \times fw \times wd$.
- The dimension of the output is $(h - fh + 1) \times w(w - fw + 1) \times 1$.

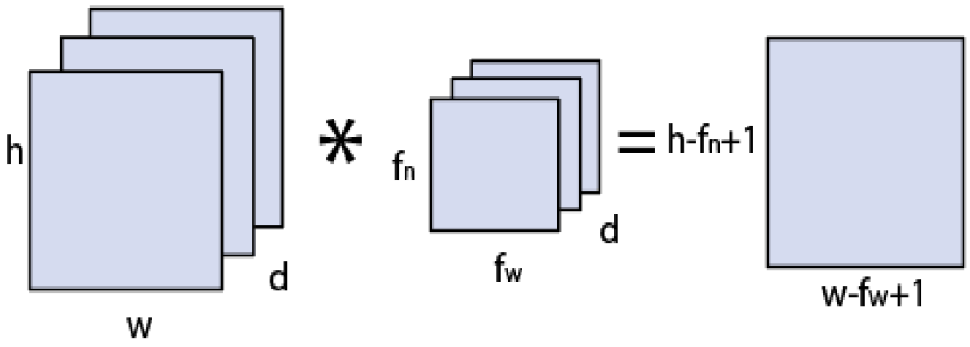


Figure 3.3: Image matrix multiplies Kernel or filter matrix [14]

Let's start with consideration a (5×5) image whose pixel values are 0, 1, and filter matrix (3×3) as :

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \tag{3.1}$$

The convolution of (5×5) image matrix multiplies with (3×3) filter matrix is called "Features Map" and show as an output (See Figure 3.4).

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 3 & 4 \\ 2 & 4 & 3 \\ 2 & 3 & 4 \end{bmatrix}$$

Figure 3.4: Convolved feature [14]

Convolution of an image with different filters can perform an operation such as blur, sharpen, and edge detection by applying filters.

Strides [14]: Is the number of pixels moving over the matrix for inputs. If the step is equal to 1, we shift the filters to 1 pixel at a time and likewise, if the step is equal to 2, then we shift the filters to 2 pixels at a time. The figure below indicates convolution will function with a stride of 2 (See Figure 3.5).

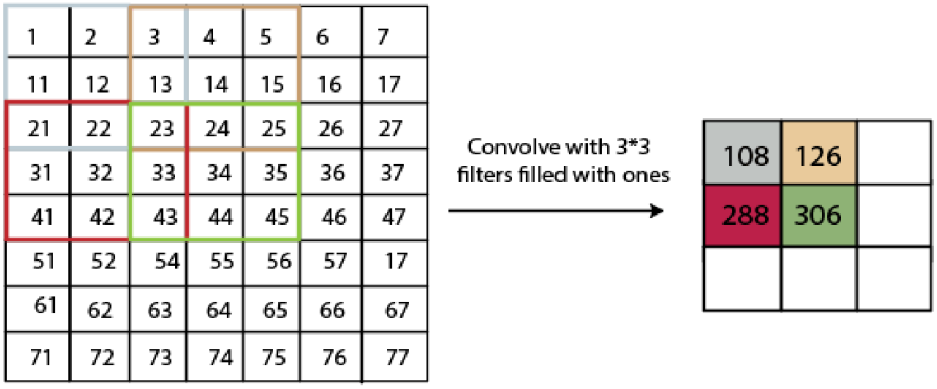


Figure 3.5: strides [14]

Padding [93]: Plays a crucial role in building a convolutional neural network. If the image gets shrinking and we take a neural network with 100's of layers on it, it will give us a small picture after filtering at the top. If we take a three-by-three filter on top of a gray-scale image, then what will happen. the information on the borders of images is not preserved as well as the information in the middle. Padding is simply a process of adding layers of zeros to our input images so as to avoid the problems mentioned above (See Figure 3.6).

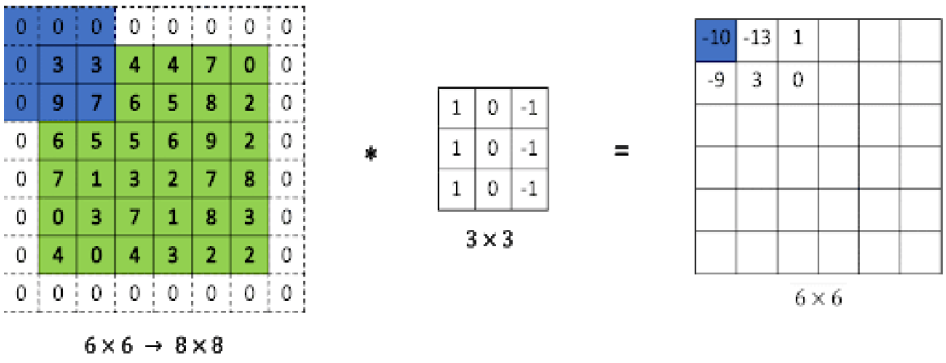


Figure 3.6: padding [15]

Activation Function: Is a node which is positioned between Neural Networks at the end of

or in between. They're helping to decide whether or not the neuron would fire. "On the input signal, the activation function is the nonlinear transformation we do. This transformed output is then forwarded as input to the next layer of neurons" [16].

Rectified Linear Unit (ReLU) function is nowadays the most frequently used activation mechanism in neural networks. One of the greatest advantages ReLU has over other activation mechanisms is that it doesn't simultaneously stimulate all neurons. From the image for the ReLU function (See Figure 3.7), we will find that it converts all negative inputs to zero and that the neuron is not activated. This makes it very effective in terms of computation since few neurons are stimulated every time. In the positive zone, it doesn't saturate. In practice, ReLU converges six times faster than the activation functions of tanh and sigmoid.

Some drawback ReLU offers is that in the negative region it is saturated, meaning that at that region the gradient is zero. With the gradient equal to zero, not all weights will be modified during backpropagation, we use Leaky ReLU to solve this. Also, ReLU functions are not zero-centric. This means that it will have to take a zig-zag path that could be longer for it to get to its optimum point (See Figure 3.7).

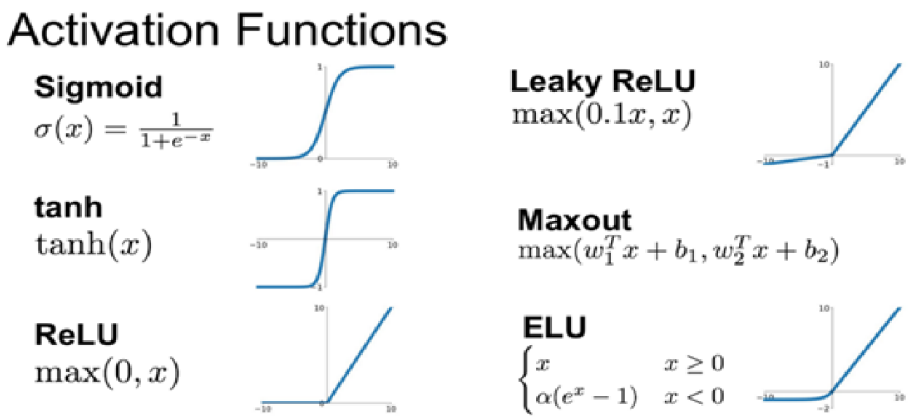


Figure 3.7: Analytics Vidhya [16]

3.3.2 Pooling Layer

Pooling layer [13] plays an essential part in image preprocessing. The pooling layer reduces parameter numbers when the images are too large. Pooling involves "downscaling" the

image from previous layers. Shrinking an image can be related to reducing the pixel density. Spatial pooling is also known as downsampling or subsampling, which decreases each map's dimensionality but preserves the important details. Spatial pooling forms occur as follows:

There are three types of pooling operations: Max, Min, and Average.

Max Pooling: Is a method of sampled discretization. Its main purpose is to downscale an input representation, reduce its dimensionality, and allow the assumption to be made about the features contained in the sub-region binned. Max pooling is performed using a max filter to extend the initial representation to non-overlapping sub-regions (See Figure 3.8 and 3.9).

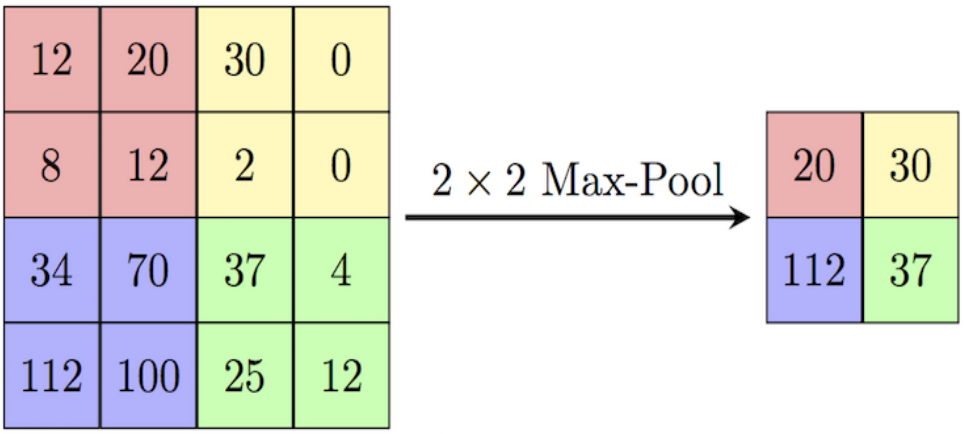


Figure 3.8: max pooling [17].

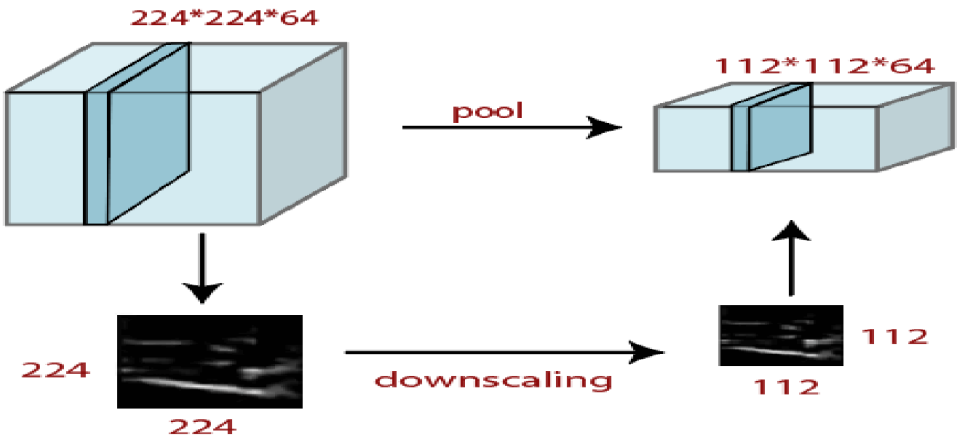


Figure 3.9: max pooling [17]

3.3.3 Flattening layer

To transform the output of the convolutional portion of the CNN into a 1D feature vector after completing the previous two steps, this operation is called flattening [18]. It gets the output of the convolutional layers, flattening all its structure to create a single long feature vector to use for final classification by the dense layer. The reason we're doing this is that later we'll need to incorporate this data into an artificial neural network (See Figure 3.10).

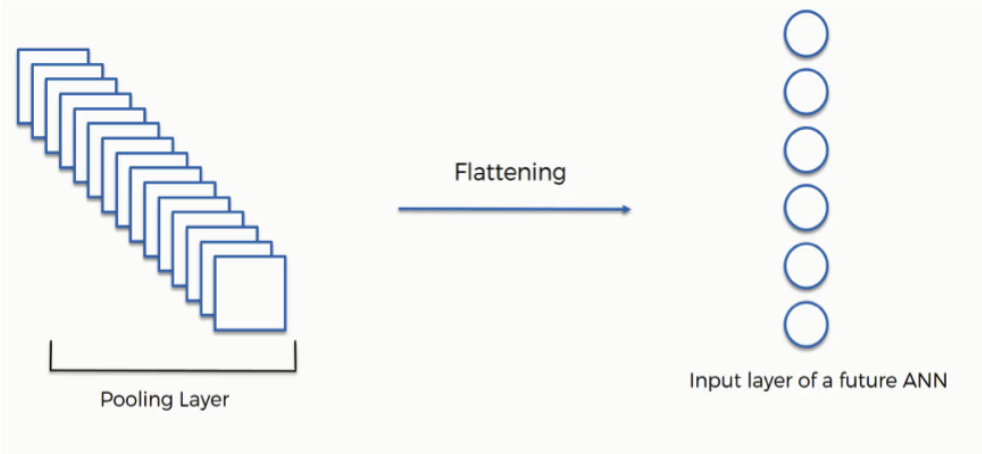


Figure 3.10: The feature maps that convert to a long feature vector [18].

3.3.4 Fully Connected Layer

The fully connected layer is a layer in which the data from the other layers is flattened into and sent into a vector. It converts output by the network into the desired number of groups (See Figure 3.11). The function map matrix will be translated to the vector in the diagram above, such as $(x_1, x_2, x_3..., x_n)$ utilize completely connected layers. We will combine features to create any model and apply activation functions like softmax or sigmoid and other to classify the outputs as a face real or fake, car, dog, truck, etc.

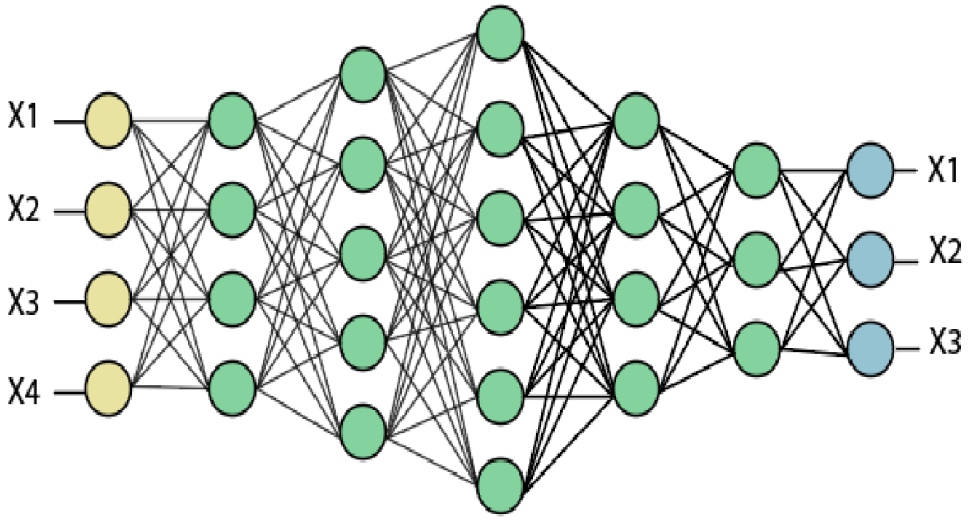


Figure 3.11: fully connected layer [13]

.

3.3.4.A Softmax Classification

The fully Connected Layer output is then passed through the function softmax, the Softmax function [94] takes an arbitrary real-valued score vector and squashes it to a value vector between zero and one that adds up to one (See Figure 3.12).

Figure 3.12: soft max [19]

3.3.4.B Sigmoid Classification

A sigmoid function is a type of activation function, and more specifically defined as a squashing function. Squashing functions limit the output to a range between 0 and 1, making these functions useful in the prediction of probabilities [95].

There are different CNNs architectures available that were essential to building algorithms that which power and shall power AI as a whole in the near future. Some of those were listed below: ***(LeNet, AlexNet, ZFNet, GoogLeNet, and VGGNet)***.

3.4 Conclusion

After this study CNN, we concluded the CNN is very important using deep learning networks in applications such as computer vision and natural language processing as it can mitigate the error rate significantly and hence improve network performances. By analyzing this chapter, one can gain a better understanding of why CNN is employed in numerous applications and facilitates in several machine learning fields. So, we have chosen CNN to study face spoofing to give the best result in our application we will present this result in the next chapter.

4

Experimental Results and Discussion

Contents

4.1 Introduction

We reviewed several conceptual cases presented on facial biometrics in this chapter, the case studies are focused on several popular facial anti-spoofing systems and state-of-the-art. The objective is to demonstrate the benefits of the anti-spoofing systems in producing more accurate facial biometrics.

In this research, we are studying two forms of face spoofing: a true user's photograph and video. We present an anti-spoofing approach for the first form of attack based on a holistic representation of the face region, via a comprehensive collection of low-level feature descriptors, capable of capturing the differences between live and spoof images. For the second attack, we conduct a noise analysis created by the recaptured video in order to differentiate between the two groups.

Anti-Spoofing is a technique that can prevent an attack on facial impersonation. For example, an attacker may use a legal user's photo to "fool" the facial recognition system. It is therefore important to use anti-plagiarism technologies to improve device security, as this subject is well studied using the convolutional neural network. Finally, use CNN to present our experimental and result frameworks for face anti-spoofing.

4.2 Effectiveness of face alignment

Face alignment [96] can be done as a method of transforming various sets of points from input images (into one coordinate system). This coordinate system can be called an output coordinate system and defined as our stationary reference frame. Our task is to rotate, convert, and synchronize all input coordinates with output coordinates. We can add three simple affine transformations for that purpose: rotation, translation, and scaling. We used python with OpenCV in our experiments to convert facial features from the input coordinate systems into the output coordinate system (See Figure 4.1). We may use many different approaches to do face-alignment. We want to use a basic one A tool that only focuses on areas around the eyes.

This method consists of steps such as (Algorithm. 1) below :

Algorithm 1: face alignment

- A image

Predicted face **for** each image **do**
- Detecting faces and eyes in the image
- Calculating the center of detected eyes
- Drawing a line between the center of two eyes
- Drawing the horizontal line between two eyes
- Calculating length of 3 edges of the triangle
- Calculating the angle
- Rotating image by a calculated angle
- Scaling the image;

end

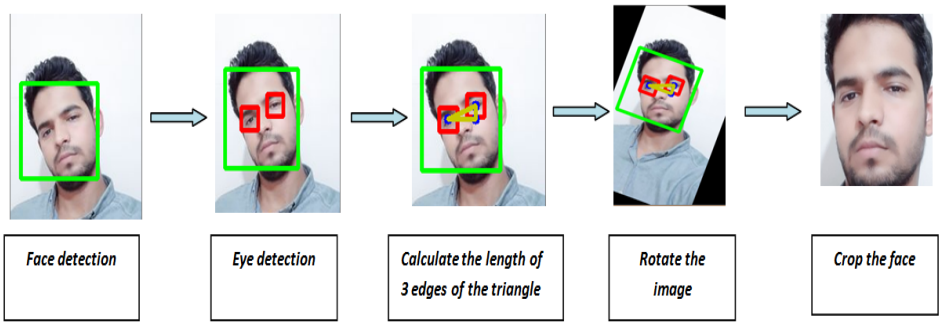


Figure 4.1: face alignment with OpenCV

4.3 Description of the work environment

Python is appealing to many developers as it's easy to learn. Python code is understandable by humans, which makes it easier to build models for machine learning. Additionally, Python offers a concise and readable code. While complex algorithms and versatile workflows stand

behind machine learning and Artificial Intelligent (AI), Python's simplicity allows developers to write reliable systems, and also for its ease of importing its libraries, and we used in writing our program the anaconda environment for ease of working in it.

4.3.1 Python

Python [97] is one of the most commonly used programming languages by data scientists and machine learning engineers. Although there has been no universal study on the prevalence of machine learning algorithms with Python in machine learning, and it is an object-oriented, high-level programming language with dynamic semantics. It's high-level built-in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, It is widely used in machine learning.

4.3.2 Anaconda

Anaconda [98] individual edition is the world's most popular Python distribution platform with over 20 million users worldwide. You can trust in our long-term commitment to supporting the Anaconda open-source ecosystem, the platform of choice for Python data science. Virtual Environment is used to create a container or isolated environment where the Python-related dependencies are installed for a specific project. One can work with many different versions of Python with its various packages. Data scientists tend to use Anaconda distribution, which comes with many useful pre-installed packages, which are easy to install and manage.

Anaconda Navigator is a desktop graphical user interface (Graphical User Interface (GUI)) included in Anaconda distribution that allows you to launch applications and easily manage conda packages, environments, It is available for Windows, macOS, and Linux. The following applications are available by default in Navigator: ***JupyterLab, Jupyter Notebook, Spyder, PyCharm, VSCode,Glueviz, Orange 3 App, RStudio.***

And we created our project using ***Jupyter Notebook*** [99] is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. Uses include data cleaning and transformation, numerical simulation, statistical modeling, data visualization, machine learning, and more.

4.4 Architecture of keras

We will explain the content of this project for how the CNN architecture is building using ***Keras*** as shown in Figure 4.2, the input is fed to the network of stacked Conv, Pool, and Dense layers. The output of a sigmoid layer indicating whether there is a real or fake face. We will explain in the detail below.

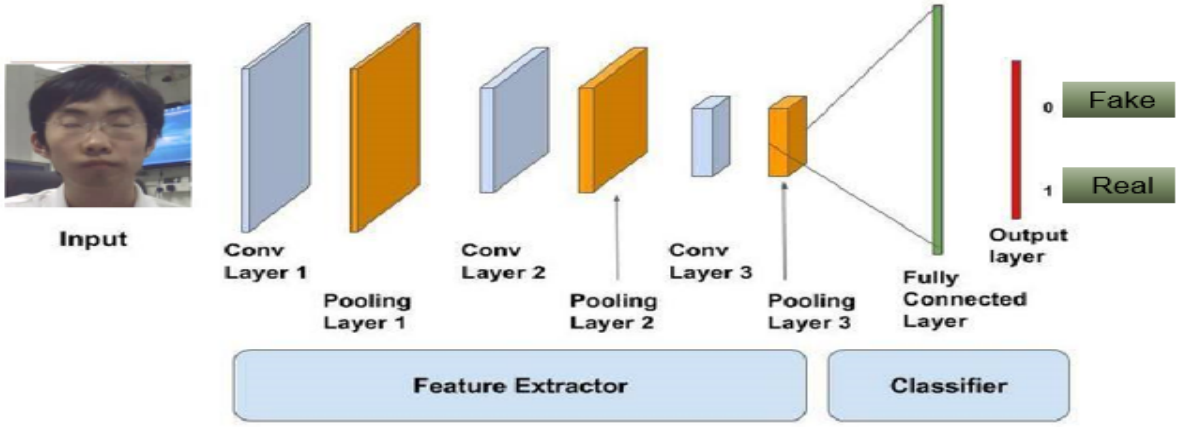


Figure 4.2: CNN model architecture in keras

4.4.1 Tools And Libraries

We begin implementation by importing the most important the following libraries [100]:

- **TensorFlow:** An open-source platform for the implementation, training, and deployment of machine learning models.
- **Keras:** An open-source library used for the implementation of neural network architectures that run on both Central Processing Unit (CPU)s and Graphics Processing Unit (GPU)s.
- **Matplotlib:** A visualization python tool used for illustrating interactive charts and images.

- **NumPy:** Is a package designed for high-level and complex mathematical functions, particularly linear algebra. It is commonly used for machine learning projects like image processing.

- **OpenCV:** Is a cross-platform library using which we can develop real-time computer vision applications. It mainly focuses on image processing, video capture, and analysis including features like face detection and object detection.

4.4.2 Preparing Dataset

Images in the training dataset had differing sizes, therefore images had to be resized before being used as input to the model. The CASIA Face Anti-Spoofing Database contains 25,000 images, each with dimensions 100×100 pixel. The content of the images within the dataset is sampled from 2 classes real or fake (see Figure 4.3).

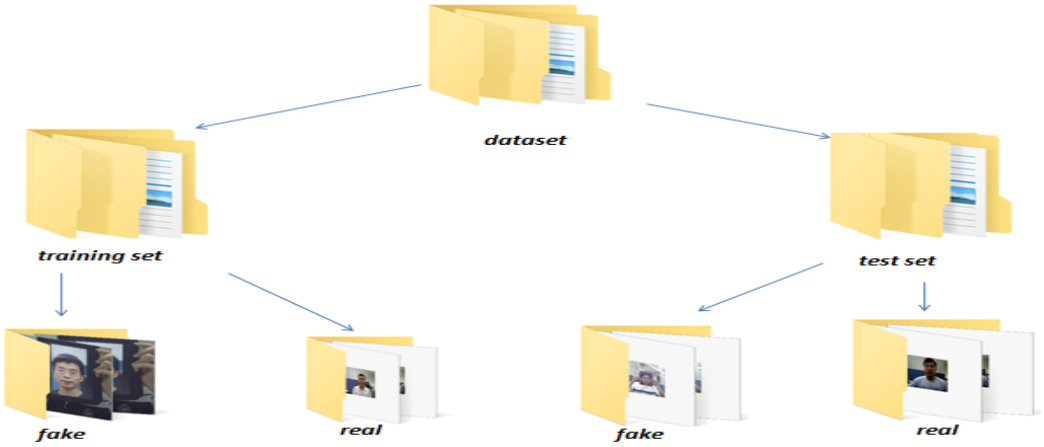


Figure 4.3: Split data

4.4.3 Initialising The Convolutional Neural Network

A CNN uses filters on the raw pixel of an image to learn details patterns compare to a global pattern with a traditional neural net. To construct a CNN, you need to define:

1. Using the feature ”Conv2D” [101] we added a convolution layer. The Conv2D function takes 4 arguments, the first is the number of filters i.e. 32 here, the second argument is the

shape of each filter here i.e. 3×3, the third is the input form and the image type (RGB or Black and White) of each image i.e. the input image our CNN would take is 100×100 resolution and The fourth statement is the activation function we want to use, here Relu' represents the function of the rectifier.

2. We start by taking our classifier object and adding the pooling layer [102]. We take a (2×2) matrix we'll have minimum pixel loss and get a precise region where the feature is located. This program focuses more on the implementation aspect. We only reduced the model's complexity without reducing its performance.

3. We've used the flatten function to perform flattening, we no need to add any special parameters, Keras will understand that the "classifier" object is already holding pooled image pixels and they need to be flattened.

4. After that, we need to build a fully connected layer and link the collection of nodes we have after the flattening step to that layer, these nodes will serve as an input layer for those fully connected layers. As this layer would be present between the input layer and the output layer, a hidden layer may be referred to here.

5. Dense is the function to add a fully connected layer [103], 'units' is where we determine the number of nodes that should be present in this hidden layer, these units meaning will usually be between the number of input nodes and the output nodes but the art of finding the most appropriate number of nodes can only be accomplished by experimental trials. Though using a power of 2 is common practice. And the activation function would be a function of the rectifier.

6. Now it's time to initialize our output layer, which should contain only one node, that the final layer contains only one node, and we will be using a sigmoid activation function for the final layer.

7. It's time to fit our CNN to the image dataset, But before we do that, we are going to pre-process the images to prevent over-fitting. Overfitting is when you get a great training

accuracy and very poor test accuracy due to the overfitting of nodes from one layer to another.

8. Therefore, before we fit our images into the neural network, we need to perform certain image increases on them, which is effectively synthesizing the training data. We will use Keras. Preprocessing library to do the synthesizing portion and prepare the training set as well as the test collection of images present in a properly organized directory, where the name of the directory is used as the mark of all the images present in it.

9. After the building our CNN model, it's time to compile it. Optimizer: parameter is to choose the stochastic gradient descent algorithm. Loss: parameter is to choose the loss function. Finally, the metrics: parameter is to choose the performance metric.

10. Epoch is a single step in training a neural network; in other words, when a neural network is trained on every training samples only in one pass we say that one epoch is finished. So the training process should consist of more than one epochs. In our case, we trained the network in different epochs of 40,100,200, to choose the best training result.

This table explain the parte of training result of our project (See Figure 4.4).

```
Epoch 1/200
31/31 [==============================] - 87s 3s/step - loss: 0.8239 - accuracy: 0.5878 - val_loss: 0.5
911 - val_accuracy: 0.7708
Epoch 2/200
31/31 [==============================] - 16s 512ms/step - loss: 0.4146 - accuracy: 0.8368 - val_loss:
0.3409 - val_accuracy: 0.9115
Epoch 3/200
31/31 [==============================] - 16s 502ms/step - loss: 0.2184 - accuracy: 0.9050 - val_loss:
0.2565 - val_accuracy: 0.8542
Epoch 4/200
31/31 [==============================] - 15s 499ms/step - loss: 0.0977 - accuracy: 0.9773 - val_loss:
0.2328 - val_accuracy: 0.9323
Epoch 5/200
31/31 [==============================] - 16s 505ms/step - loss: 0.0594 - accuracy: 0.9855 - val_loss:
0.4022 - val_accuracy: 0.8229
Epoch 6/200
31/31 [==============================] - 16s 510ms/step - loss: 0.0557 - accuracy: 0.9839 - val_loss:
0.2078 - val accuracy: 0.8698
```

Figure 4.4: training result

4.5 Experimental results

After training our model we got a 98% accuracy and a 2% loss ratio. Note below the graphs showing accuracy and loss ratio in terms of three different epochs 40,100 and 200.

As we see in Figure 4.5 when we used (epoch = 40), where accuracy (right) and loss (left) graph for CNN models. The training process was early stopped because of no improvement over a preset period of time.

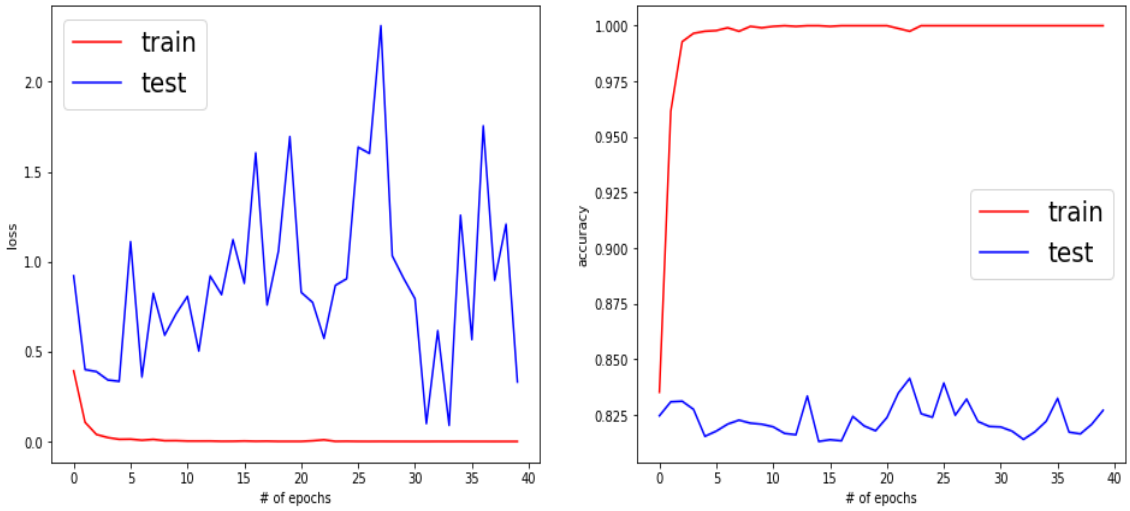


Figure 4.5: Graphic curve showing accuracy and loss for training and testing

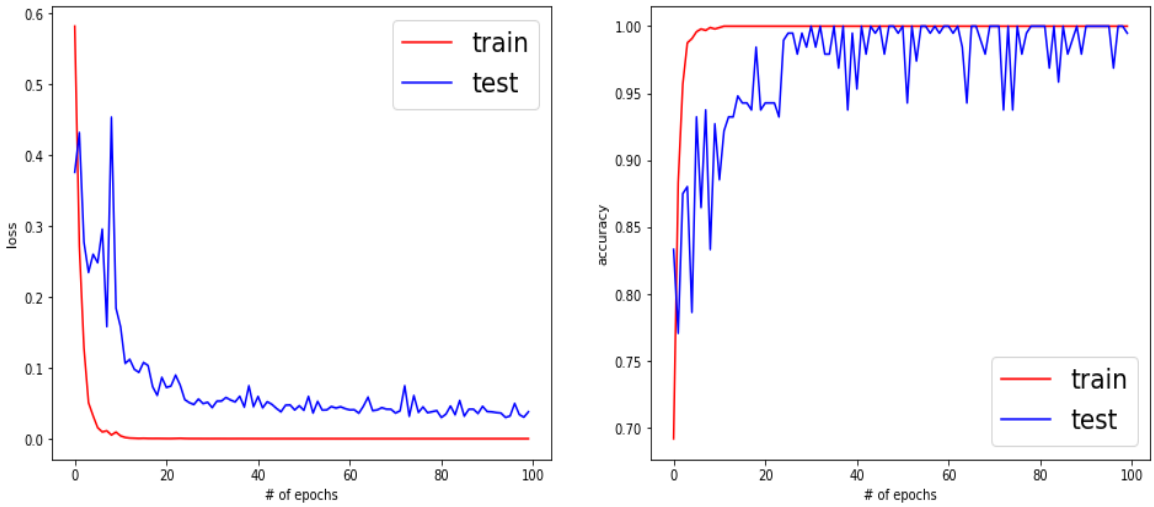


Figure 4.6: Graphic curve showing accuracy and loss for training and testing

As we see in Figure 4.6. when we used (epoch=100), where accuracy (right) and loss (left) there is an improvement curve for CNN models.

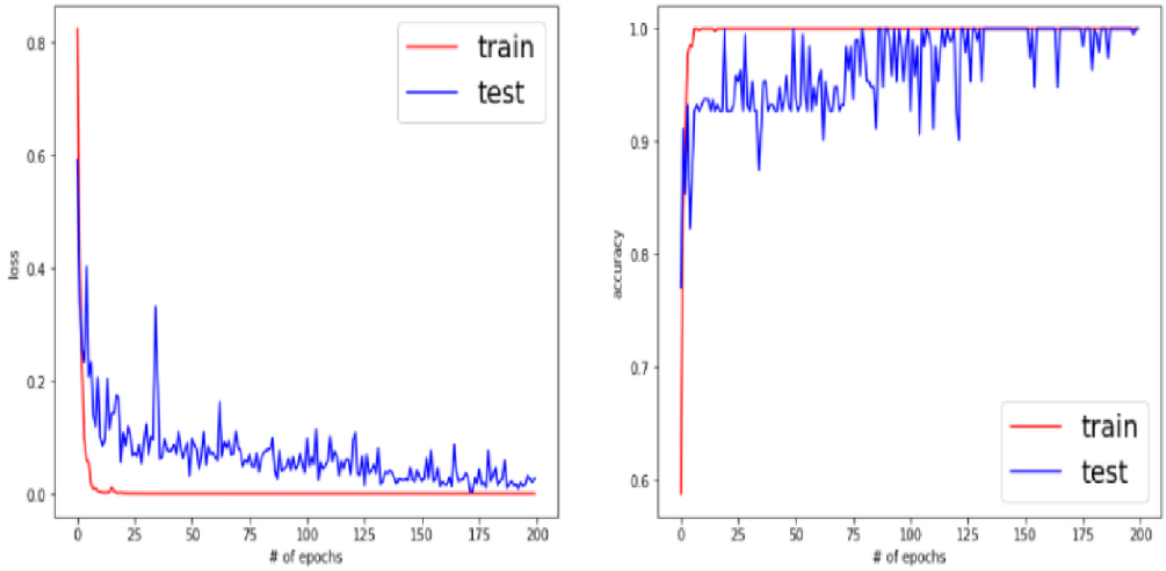


Figure 4.7: Graphic curve showing accuracy and loss for training and testing

As we see in Figure 4.7 when we used (epoch =200).

- The plot of training loss decreases to a point of stability, the plot of test loss decreases to a point of stability.
- The plot of training accuracy growing to a point of stability, the plot of test accuracy growing to a point of stability.

4.5.1 Role Of Epochs

One epoch is when an entire dataset is passed forward and backward through the neural network only once. So, the one epoch leads to underfitting of the curve in the graph. However, there is no right answer to this question. The answer is different for different datasets but you can say that the numbers of epochs are related to how diverse your data. As the number of epochs increases, more times the weight is changed in the neural network and the curve goes from **underfitting** to **optimal** to **overfitting** curve.

The test image holds the image that needs to be tested on the CNN. Once we have the test image, we will prepare the image to be sent into the model by converting its resolution to 100×100. Then we are using the predict method on our classifier object to get the prediction. As the prediction will be in a binary form, we will be receiving either a 1 or 0, which will represent a real face or a fake face respectively (See Figure 4.8, 4.9).

Now, we will do a test on our program, then we will take pictures on the database and the internet, as well as personal photos to test it to make sure this result is accurate.

- First test:

Both images are out of the dataset to surly that these images are real and to effectively our program.

Note: left image obtained on our files, right image it is for my supervisor.

Figure 4.8: Results for predicting first test

- Second test:

Both images are in of dataset to surly that this images are fake or real .

note: We obtained on the CASIA dataset

Figure 4.9: Results for predicting second test

- Third test:

Since our program was not 100% accurate, a prediction error occurred. Instead of the result is real, it was fake (left image), While the image on the right was real(see Figure 4.10).

Figure 4.10: Results for predicting third test

4.6 Experimental results for real time

In our project that blends CNN and computer vision to uncover actual and fake faces in a real-time environment. The frame of the image captured from the webcam is scrolled over a pretrained model. Here are some of the results we got in distinguishing between real and fake faces.

- First test:

After experimental, the prediction was correct (See Figure 4.11), as a distinction was made between a real face and a fake face on the photo, were used two different sizes of high-quality printed paper Using a kodak 7000 photo printer.

left image (size:$10.5cm \times 14.8cm$), right image (size:$14.8cm \times 21.0cm$).

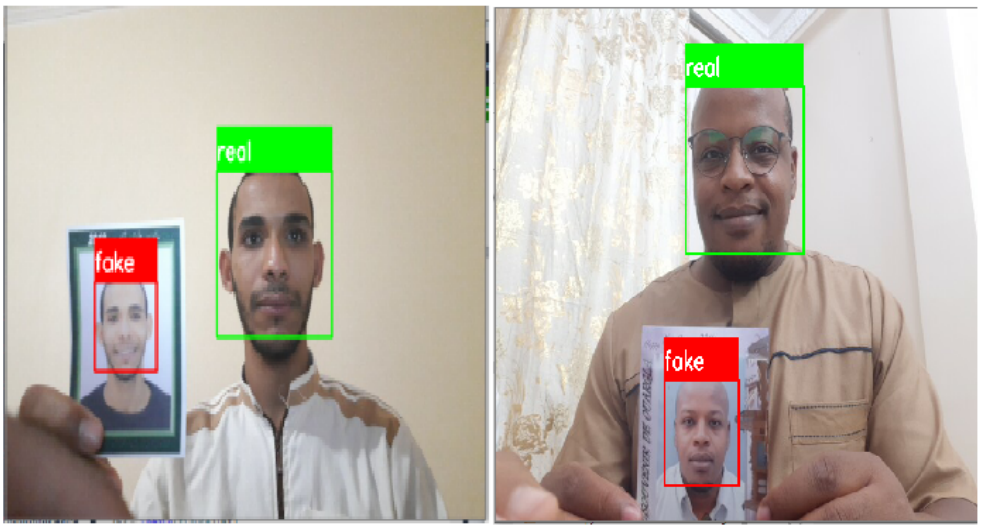


Figure 4.11: Result for real time face detection 01

- Second test:

After experimental, the prediction was correct (See Figure 4.12), as a distinction was made between a real face and a fake face the phone type of Samsung GALAXY A30 with characteristics: Camera 16 Mpx, size($7.4cm \times 15.8cm$).

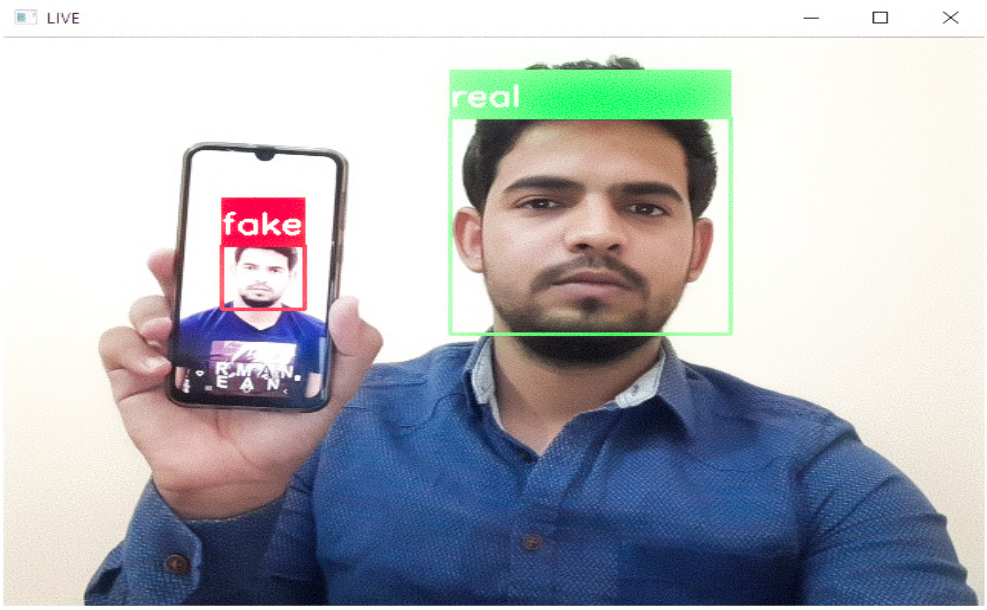


Figure 4.12: Result for real time face detection 02

4.7 Conclusion

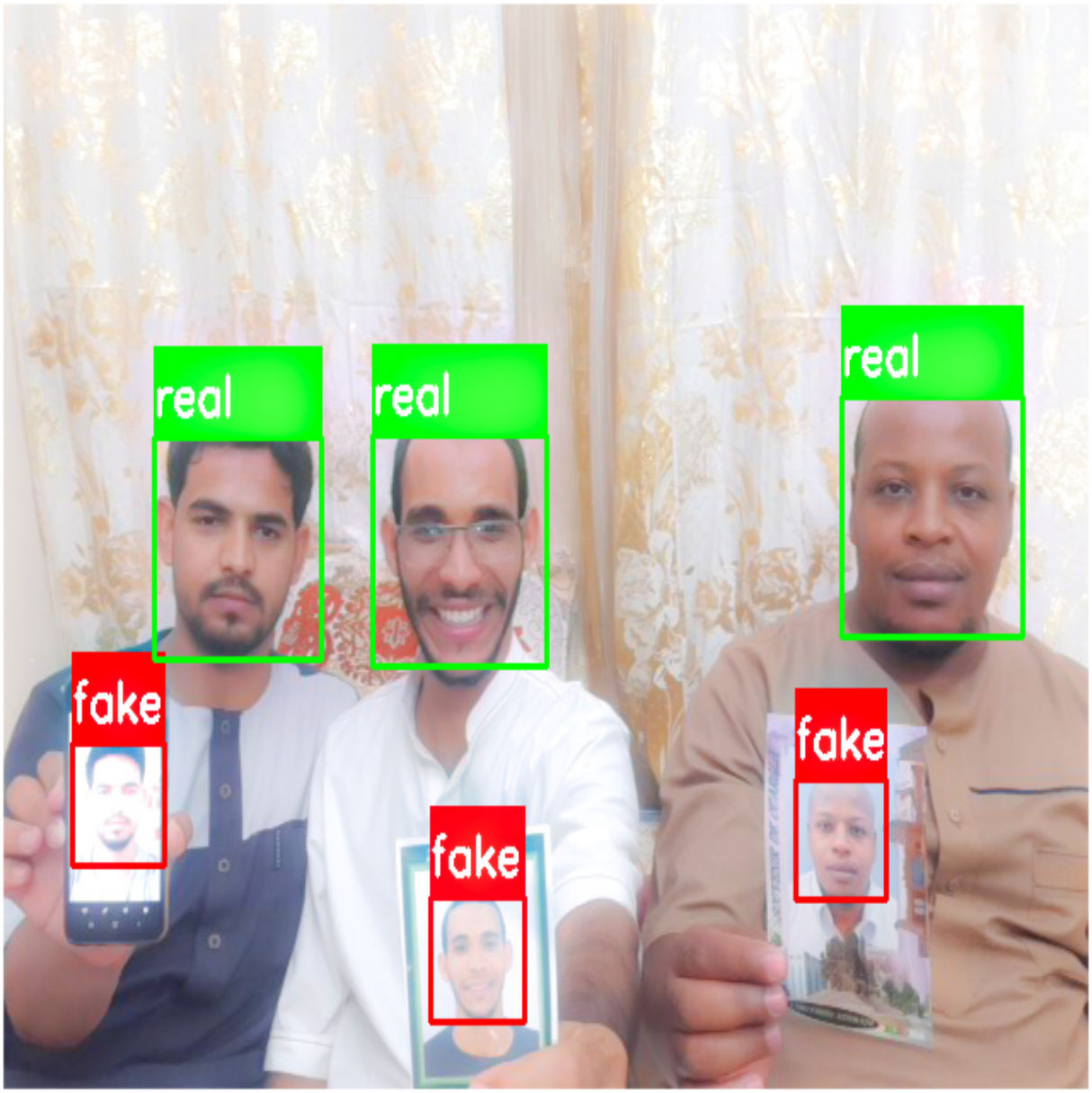
In this chapter, we present our approach to detect facial spoofing. We provided a trial evaluation From CNNs proposed performance. Overall performance was obtained using a different number of training and test images. CNN are achieving the best results so far. Using complex architectures, accuracy is possible rates are around 98%. Despite this result, CNNs cannot function without negative impacts. For the future, we can use more different kinds of categories that would be difficult for the computer to classify and compare more sophisticated classifiers.

General Conclusion

In an increasingly digital world, and although face recognition has been investigated extensively, spoofing attacks persist to be a security challenge for face biometric systems, biometric spoofing is the ability to fool a biometric system into recognizing a fake user as a genuine user by presenting printed photos or replaying recorded videos.

In our project, we provided a comprehensive study about the detection face anti-spoofing technique and we analyzed in-depth about the technology used by using the methodology in face anti-spoofing to make it more accurate, also we used CNN for feature extraction and classifier. We did build CNN architecture for face anti-spoofing applications. i.e. a deep CNN architecture that directly maps the raw input face images to the corresponding output classes. We achieved that The higher the number of epochs, the more accurate the result using build CNN. We also concluded that this study is still not able to obtain an accurate result due to hardware conditions (laptop).So, there are still other challenges, especially with the use of the field of artificial intelligence to make this technology more powerful and accurate than it is by developing new algorithms and other tools.

For future developments, further analysis to build and create new databases for a more inclusive and dynamic creation range should be carried out in the future, also other algorithms more effective.


real
real
real
fake
fake
fake

Bibliography

[1] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 01 2014.

[2] I. M. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages and future development: A review," *International Journal of Scientific & Technology Research*, vol. 4, no. 12, pp. 285–289, 2015.

[3] A. K. Sharma, A. Raghuwanshi, and V. K. Sharma, "Biometric system-a review," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 5, pp. 4616–4619, 2015.

[4] "Dentist's hand taking saliva test from woman's mouth with cotton swab stock photo," https://photostockeditor.com/premium/248268127/dentists-hand-taking-saliva-test-from-womans-mout.

[5] "Think before you speak: voice recognition replacing the password," https://www.information-age.com/think-you-speak-voice-recognition-replacing-password-123461752/, accessed: 1 August ,2016.

[6] "Rhu keystroke dynamics benchmark dataset," https://www.coolestech.com/rhu-keystroke/, accessed: IEEE ICCST ,2014.

[7] "Why use an electronic signature pad?" https://tsgtaxpros.com/software/why-use-an-electronic-signature-pad/.

[8] "Biometrics cybersecurity research gets government cash," https://www.bbc.com/news/technology-20433998, accessed: 22 November, 2012.

[9] K. Vikram and S. Padmavathi, "Facial parts detection using viola jones algorithm," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2017, pp. 1–4.

[10] J. Galbally, "Vulnerabilities and attack protection in security systems based on biometric recognition," Ph.D. dissertation, 01 2009.

[11] "Convolutional neural networka," https://towardsdatascience.com/covolutional-neural-network-cb0883dd6529, accessed: Feb 24, 2019.

[12] "A beginner's guide to understanding convolutional neural networks," https://adeshpande3.github.io/A-Beginner's-Guide-To-Understanding-Convolutional-Neural-Networks/, accessed: July 20, 2016.

[13] "Introduction of convolutional neural network in tensorflow," https://www.javatpoint.com/convolutional-neural-network-in-tensorflow.

[14] "Understanding of convolutional neural network (cnn) — deep learning," https://adeshpande3.github.io/A-Beginner's-Guide-To-Understanding-Convolutional-Neural-Networks/, accessed: March 4 ,2018.

[15] "Cnn padding," http://datahacker.rs/what-is-padding-cnn/, accessed: 01.11.2018.

[16] "Basic overview of convolutional neural network (cnn)," https://medium.com/dataseries/basic-overview-of-convolutional-neural-network-cnn-4fcc7dbb4f17, accessed: Feb 13, 2018.

[17] "Max-pooling / pooling," https://computersciencewiki.org/index.php/Max-pooling_/_Pooling, accessed: 27 February 2018.

[18] "Convolutional neural networks (cnn): Step 3 - flattening," https://www.superdatascience.com/blogs/convolutional-neural-networks-cnn-step-3-flattening, accessed: Aug 18, 2018.

[19] H. Liu, L. Li, and J. Ma, "Rolling bearing fault diagnosis based on stft-deep learning and sound signals," *Shock and Vobration*, vol. 2016, p. 12, 09 2016.

[20] A. Benlamoudi, "Multi-modal and anti-spoofing person identification," PhD dissertation, University of Ouargla, 2018. [Online]. Available: http://dspace.univ-ouargla.dz/jspui/handle/123456789/16532

[21] J. M. White, "Chapter 12 - access control," in *Security Risk Assessment*, J. M. White, Ed. Boston: Butterworth-Heinemann, 2014, pp. 149 – 160. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128002216000126

[22] M. Muniruzzaman, "A survey of biometrics security system," vol. 11, 11 2011.

[23] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2015.

[24] A. N. Kataria, D. M. Adhyaru, A. K. Sharma, and T. H. Zaveri, "A survey of automated biometric authentication techniques," in *2013 Nirma University International Conference on Engineering (NUiCONE)*. IEEE, 2013, pp. 1–6.

[25] S. Trabelsi, D. Samai, A. Meraoumia, K. Bensid, A. Benlamoudi, F. Dornaika, and A. Taleb-Ahmed, "Finger-knuckle-print recognition using deep convolutional neural network," in *020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*. IEEE, 2020, pp. 163–168.

[26] K. Amano and K. Shimizu, "Biological information acquisition device, method for acquiring biological information, and biometrics device," Mar. 27 2012, uS Patent 8,144,938.

[27] C. Streckfus and C. Guajardo-Edwards, *The Use of Salivary as a Biometric Tool to Determine the Presence of Carcinoma of the Breast Among Women*, 06 2011.

[28] "Different types of biometrics," https://www.ibeta.com/different-types-of-biometrics/, accessed: September 9, 2019.

[29] S. A. Schuckers, "Spoofing and anti-spoofing measures," *Information Security technical report*, vol. 7, no. 4, pp. 56–62, 2002.

[30] Z. Boulkenafet, J. Komulainen, Z. Akhtar, A. Benlamoudi, D. Samai, S. Bekhouche, A. Ouafi, A. Taleb-Ahmed, L. Qin, F. Peng, L. Zhang, M. Long, S. Bhilare, V. Kanhangad, E. Vazquez-Fernandez, D. Perez-Cabo, J. J. Moreira-Perez, D. G. alez-Jim enez andS. Bhattacharjee, S.Marcel, S. Volkova, Y. Tang, N. Abe, L. Li, X. Feng, Z. Xia,

F. Dornaika, A. Costa-Pazo, A. Mohammadi, X. Jiang, R. Shao, P. C. Yuen, W. Almeida, F. Andal, R. Padilha, G. Bertocco, W. Dias, J. Wainer, A. Rocha, M. A. Angeloni, G. Folego, A. Godoy, and A. Hadid, "A competition on generalized software-based face presentation attack detection in mobile scenarios," in *International Joint Conference on Biometrics, 2017 IEEE Sixth International Conference on*. IEEE, 2017, pp. 1–9.

[31] "Liveness detection to fight biometric spoofing," https://www.m2sys.com/blog/scanning-and-efficiency/liveness-detection-fight-biometric-spoofing/, accessed: 2018.

[32] C. Busch, "Standards for biometric presentation attack detection," in *Handbook of Biometric Anti-Spoofing*. Springer, 2019, pp. 503–514.

[33] P. Johnson, R. Lazarick, E. Marasco, E. Newton, A. Ross, and S. Schuckers, "Biometric liveness detection: Framework and metrics," in *International biometric performance conference*, vol. 1, 2012.

[34] R. Lazarick, "'spoofs, subversion and suspicion: Terms and concepts," in *Proc. NIST Int. Biometric Perform. Conf.(IBPC)*, 2012.

[35] A. Benlamoudi, K. E. Aiadi, A. Ouafi, D. Samai, and M. Oussalah, "Face antispoofing based on frame difference and multilevel representation," *Journal of Electronic Imaging*, vol. 26, no. 4, p. 043007, 2017. [Online]. Available: http://dx.doi.org/10.1117/1.JEI.26.4.043007

[36] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[37] Z. Boulkenafet, Z. Akhtar, X. Feng, and A. Hadid, "Face anti-spoofing in biometric systems," in *Biometric security and privacy*. Springer, 2017, pp. 299–321.

[38] Z. Akhtar, C. Micheloni, and G. L. Foresti, "Biometric liveness detection: Challenges and research opportunities," *IEEE Security & Privacy*, vol. 13, no. 5, pp. 63–72, 2015.

[39] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3d structure recovered from a single camera," in *2013 International Conference on Biometrics (ICB)*, June 2013, pp. 1–6.

[40] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in *Face and Gesture 2011*, March 2011, pp. 436–441.

[41] D. Navarre, P. Palanque, J.-F. Ladry, and E. Barboni, "Icos: A model-based user interface description technique dedicated to interactive systems addressing usability, reliability and scalability," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 16, no. 4, pp. 1–56, 2009.

[42] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in *Biometric Technology for Human Identification*, vol. 5404. International Society for Optics and Photonics, Aug. 2004, pp. 296–304.

[43] J. Bai, T. T. Ng, X. Gao, and Y. Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*, May 2010, pp. 3425–3428.

[44] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis," *IET Biometrics*, vol. 1, no. 1, pp. 3–10, March 2012.

[45] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, Sept 2012, pp. 1–7.

[46] N. Kose and J. L. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," in *2012 International Conference on Informatics, Electronics Vision (ICIEV)*, May 2012, pp. 1027–1032.

[47] 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)*, May 2015, pp. 98–105.

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

[49] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in *2014 22nd International Conference on Pattern Recognition*, Aug 2014, pp. 1173–1178.

[50] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 710–724, Feb 2014.

[51] J. Yang, Z. Lei, D. Yi, and S. Z. Li, "Person-specific face antispoofing with subject domain adaptation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 797–809, April 2015.

[52] I. Chingovska and A. R. dos Anjos, "On the use of client identity information for face antispoofing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 787–796, April 2015.

[53] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, March 2012.

[54] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *2011 International Joint Conference on Biometrics (IJCB)*, Oct 2011, pp. 1–7.

[55] O. Kähm and N. Damer, "2d face liveness detection: An overview," in *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, Sept 2012, pp. 1–12.

[56] K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating liveness by face images and the structure tensor," in *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, Oct 2005, pp. 75–80.

[57] K. Kollreider, H. Fronthaler, and J. Bigun, "Verifying liveness by multiple experts in face biometrics," in *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, June 2008, pp. 1–6.

[58] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in *2009 International Conference on Image Analysis and Signal Processing*, April 2009, pp. 233–236.

[59] S. R. Arashloo, J. Kittler, and W. Christmas, "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2396–2407, Nov 2015.

[60] T. d. Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikäinen, and S. Marcel, "Face liveness detection using dynamic texture,"

EURASIP Journal on Image and Video Processing, vol. 2014, no. 1, p. 2, Jan 2014. [Online]. Available: https://doi.org/10.1186/1687-5281-2014-2

[61] A. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Face spoofing detection through visual codebooks of spectral temporal cubes," *IEEE Transactions on Image Processing*, vol. 24, no. 12, pp. 4726–4740, Dec 2015.

[62] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, "Detection of face spoofing using visual dynamics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 762–777, April 2015.

[63] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Face anti-spoofing via motion magnification and multifeature videolet aggregation," 2014.

[64] J. Komulainen, A. Hadid, M. Pietikäinen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in *2013 International Conference on Biometrics (ICB)*, June 2013, pp. 1–7.

[65] 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*, Oct 2007, pp. 1–8.

[66] G. Pan, L. Sun, and Z. Wu, *Liveness detection for face recognition*. INTECH Open Access Publisher, 2008.

[67] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image and Vision Computing*, vol. 27, no. 3, pp. 233 – 244, 2009, special Issue on Multimodal Biometrics. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0262885607000893

[68] D. C. Garcia and R. L. de Queiroz, "Face-spoofing 2d-detection based on moiré;-pattern analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 778–786, April 2015.

[69] J. Galbally and R. Satta, "Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models," *IET Biometrics*, vol. 5, no. 2, pp. 83–91, 2016.

[70] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084–1097, July 2014.

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

[72] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in "liveness" assessment," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 548–558, Sept 2007.

[73] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in *2013 International Conference on Biometrics (ICB)*, June 2013, pp. 1–6.

[74] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, April 2015.

[75] X. Zhao, Y. Lin, and J. Heikkilä, "Dynamic texture recognition using volume local binary count patterns with an application to 2d face spoofing detection," *IEEE Transactions on Multimedia*, vol. 20, no. 3, pp. 552–566, 2017.

[76] J. Gan, S. Li, Y. Zhai, and C. Liu, "3d convolutional neural network based on face anti-spoofing," in *2017 2nd international conference on multimedia and image processing (ICMIP)*. IEEE, 2017, pp. 1–5.

[77] Y. Tang, X. Wang, X. Jia, and L. Shen, "Fusing multiple deep features for face anti-spoofing," in *Chinese Conference on Biometric Recognition*. Springer, 2018, pp. 321–330.

[78] X. Tu, H. Zhang, M. Xie, Y. Luo, Y. Zhang, and Z. Ma, "Enhance the motion cues for face anti-spoofing using cnn-lstm architecture," *arXiv preprint arXiv:1901.05635*, 2019.

[79] C. Nagpal and S. R. Dubey, "A performance evaluation of convolutional neural networks for face anti spoofing," in *2019 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2019, pp. 1–8.

[80] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *2012 5th IAPR international conference on Biometrics (ICB)*. IEEE, 2012, pp. 26–31.

[81] S. Thakre, A. Gupta, and S. Sharma, "Secure reliable multimodel biometric fingerprint and face recognition," 01 2017, pp. 1–4.

[82] A. Gangwar and A. Joshi, "Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition," 09 2016.

[83] A. Chergui, S. Ouchtati, J. Sequeira, S. Bekhouche, F. Bougourzi, and A. Benlamoudi, "Discriminant analysis for facial verification using color images," in *Proc. First Int. Conf. Electr. Eng*, 2018.

[84] A. Benlamoudi, D. Samai, A. Ouafi, S. E. Bekhouche, A. Taleb-Ahmed, and A. Hadid, "Face spoofing detection using local binary patterns and fisher score," in *2015 3rd International Conference on Control, Engineering Information Technology (CEIT)*, Algerie, Tlemcen, May 2015, pp. 1–5.

[85] A. Benlamoudi, D. Samai, A. Ouafi, S. Bekhouche, A. Taleb-Ahmed, and A. Hadid, "Face spoofing detection using multi-level local phase quantization (ml-lpq)," in *Proc. of the First Int. Conf. on Automatic Control, Telecommunication and signals (ICATS15)*, Algerie, Annaba, Nov 2015, pp. 1–5.

[86] A. Benlamoudi, F. Bougourzi, M. Zighem, S. Bekhouche, A. Ouafi, and A. Taleb-Ahmed, "Face anti-spoofing combining mllbp and mlbsif," in *10ème Conférence sur le Génie Electrique*, Algerie, Alger, Apr 2017.

[87] S. Bekhouche, A. Ouafi, A. Taleb-Ahmed, A. Hadid, and A. Benlamoudi, "Facial age estimation using bsif and lbp," in *Proceeding of the first International Conference on Electrical Engineering ICEEB'14*, Algerie, Biskra, Dec 2014.

[88] B. Yang and S. Fotios, "Lighting and recognition of emotion conveyed by facial expressions," *Lighting Research & Technology*, vol. 47, no. 8, pp. 964–975, 2015.

[89] X. Tan, F. Song, Z. H. Zhou, and S. Chen, "Enhanced pictorial structures for precise eye localization under incontrolled conditions," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, June 2009, pp. 1621–1628.

[90] "Feature extraction," https://deepai.org/machine-learning-glossary-and-terms/feature-extraction, accessed: april, 2019.

[91] S. Zehani, A. Toumi, A. Benlamoudi, A. Taleb-Ahmed, and M. Mimi, "Features extraction using different histograms for texture classification," in *The eighth International Conference on Image Processing Theory, Tools and Applications (IPTA 2018)*, 2018/11/7.

[92] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv preprint arXiv:1511.08458*, 2015.

[93] "Cnn — introduction to padding," https://www.geeksforgeeks.org/cnn-introduction-to-padding/, accessed: 26-07-2019.

[94] "Beginner's guide to understanding convolutional neural networks," https://medium.com/@junehaoching/beginners-guide-to-understanding-convolutional-neural-networks-5209e5d9f717, accessed: May 10, 2018.

[95] "What is a sigmoid function," https://deepai.org/machine-learning-glossary-and-terms/random-forest, accessed: 09 October,2020.

[96] "Face alignment for face recognition in python within opencv," https://sefiks.com/2020/02/23/face-alignment-for-face-recognition-in-python-within-opencv/, accessed: February 23, 2020.

[97] "What is python? executive summary," https://www.python.org/doc/essays/blurb/.

[98] "data science toolkit," https://www.anaconda.com/products/individual.

[99] "Jupyter notebook," https://jupyter.org/, accessed: Aug 26, 2020.

[100] "Python libraries – python standard library list of important libraries," https://data-flair.training/blogs/python-libraries/, accessed: JUNE 27, 2019.

[101] "Convolutional neural network (cnn)," https://www.tensorflow.org/tutorials/images/cnn, accessed: 10 September,2020.

[102] "How to create a cnn classifier with keras," https://www.machinecurve.com/index.php/2019/09/17/how-to-create-a-cnn-classifier-with-keras/, accessed: 17 September 2019.

[103] "Building powerful image classification models using very little data," https://blog.keras.io/building-powerful-image-classification-models-using-very-little-data.html, accessed: Sun 05 June 2016.