## A Technical Seminar-I Report on

**FACE BIOMETRIC ANTISPOOFING**

## Submitted in partial fulfillment of the Academic requirements for the award of the Degree of

## Bachelor of Technology

## In

## ELECTRONICS & COMMUNICATION ENGINEERING

## Submitted by

## RASALA SAMITHA (20H51A04A1)

## Under the supervision

## Of

## Dr.A.Pradeep Kumar

## Associate Professor, Department of ECE



|  |
| --- |
|  |
|  |  |

**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited)**

**(Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHALROAD, HYDERABAD - 501401**

**2022-2023**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited)**

**(Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401**

**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**



**CERTIFICATE**

This is to certify that the Technical Seminar-I report entitled **“FACE BIOMETRIC ANTISPOOFING”** is a bonafide work done by **RASALA SAMITHA (20H51A04A1)** of III B. Tech ECE, in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Electronics & Communication Engineering, submitted to the Department of Electronics & Communication Engineering, CMR College of Engineering & Technology, Hyderabad during the Academic Year 2022-2023.

Dr. A. Pradeep Kumar Dr. E.N.V. PURNA CHANDRA RAO

## Assistant Professor, Department of ECE HOD, Department of ECE

## Seminar Supervisor

## 

## 

## ACKNOWLEDGEMENT

I was obliged and grateful to **Dr. E.N.V. PURNA CHANDRA RAO**, HOD, Department of ECE, CMRCET, for his cooperation in all respects during the course.

I would like to thank **Dr. B. LOKESHWARA RAO**, Professor of ECE, Dean Academics CMRCET for his encouragement throughout our course.

I would like to thank Major **Dr. V.A. NARAYANA**,principal CMRCET, for his support in the course of this work.

I would like to thank **Shri Ch. GOPAL REDDY** garu, Secretary & Correspondent of CMRCET, for his cooperation in all respects during the course.

It gives immense pleasure in expressing our deep sense of gratitude to Technical Seminar- I Supervisor **Dr.A.PRADEEP KUMAR**,Associate Professor, Department of ECE, CMRCET, for her valuable suggestions for Technical Seminar-I.

Finally, I would like to thank all teaching & non-teaching staff members of the department, for their cooperation and support throughout the duration of our course.

Ultimately, I own all our success to our beloved parents, whose vision, love and inspiration has made us to reach out for these glories.

**Signature**

**RASALA SAMITHA (20H51A04A1)**

**DECLARATION**

I hereby declare that the results embodied in this Report of Project on **“FACE BIOMETRIC ANTI-SPOOFING”** are from work carried out by using partial fulfillment of the requirements for the award of a B. Tech degree. We have not submitted this report to any other university/institute for the award of any other degree.

**SIGNATURE**

**RASALA SAMITHA (20H51A04A1)**

**DATE:**

**INDEX**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **CONTENTS** | **Page No.** |
|  | **LIST OF FIGURES** | **7** |
|  | **ABSTRACT** | 8 |
| **Chapter 1** | **INTRODUCTION** | 9 |
| 1.1 | OVERVIEW | 10 |
| 1.2 | FACE SPOOFING | 11 |
| **Chapter 2** | **FACIAL RECOGNITION** | 12 |
| 2.1 | TYPES OF ATTACKS | 13-14 |
| 2.1.1 | PRESENTATION ATTACKS | 14-15 |
| 2.1.2 | INDIRECT ATTACKS | 15 |
| 2.2 | ATTACKING METHODS | 15 |
| 2.2.1 | PHOTO ATTACKS | 16 |
| 2.2.2 | VIDEO ATTACKS | 16 |
| 2.2.3 | MASK ATTACKS | 17**-**18 |
| **Chapter 3** | **ANTI-SPOOFING TECHNIQUES** | 19 |
| 3.1 | SENSORS | 20 |
| 3.2 | ALGORITHMS | 21 |
| **Chapter 4** | **ANTI-SPOOFING LEVEL TECHNIQUES** | 22 |
| 4.1 | SENSOR-LEVEL TECHNIQUES | 23-24 |
| 4.2 | FEATURE-LEVEL TECHNIQUES | 24 |
| 4.3 | SCORE LEVEL TECHNIQUES | 24-25 |
| **Chapter 5** | **TECHNIQUES FOR LIVENESS DETECTION** | 26 |
| 5.1 | FACE RECOGNITION | 27 |
| 5.1.1 | PRESENTATION ATTACKS | 27-28 |
| 5.2 | OVERVIEW OF SPOOFING SOLUTIONS | 26-29 |
| 5.3 | PREVENTING PRESENTATION ATTACKS | 29 |
| **Chapter 6** | **CONCLUSION AND REFERENCE** | 30 |
|  | CONCLUSION | 31 |
|  | REFERENCES | 32 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No** | **Figure Name** | **Page No.** |
| 1 | Working process of a basic detector | 11 |
| 2 | Face recognition process | 13 |
| 3 | Attacks in the facial recognition system | 14 |
| 4 | Photo Attack | 16 |
| 5 | Video Attack | 16 |
| 6 | Mask Attack | 17 |
| 7 | Face spoofing attacks | 17 |
| 8 | Face Spoofing Techniques Classification | 18 |
| 9 | Anti-Spoofing Techniques | 23 |
| 10 | Score-Level Techniques | 28 |
| 11 | Measuring efficacy | 28 |

**ABSTRACT**

In an increasingly digital world, protecting confidential information from hackers and unauthorized individuals is becoming more difficult and the need for robust security is paramount. As a result, Biometric spoofing is a growing concern as biometric traits are vulnerable to attacks. Biometric spoofing is the ability to fool a biometric system into recognizing a fake user as a genuine user by means of presenting a synthetic forged version of the original biometric trait to the sensor. Specific countermeasures that allow biometric systems to detect fake artifacts and reject them need to be developed. This paper’s main goal is to provide an overview of different antispoofing techniques used in the now-emerging field of antispoofing with special attention to face modality.

In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in the face and voice recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities, such as fingerprint, face, or iris, to more marginal ones, such as signature or hand. This path of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to spoofing. Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of antispoofing, with special attention to the mature and largely deployed face modality. The work covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the future of this very active field of research. INDEX TERMS Biometrics, security, anti-spoofing, face.

**CHAPTER – I**

# **INTRODUCTION**

## 1.1 OVERVIEW:

Biometrics is the specialized term for body estimations and counts. It alludes to measurements identified with human attributes. Biometrics validation (or sensible confirmation) is utilized as a part of software engineering as a type of recognizable proof and access control. Biometric verification is any method by which a man can be interestingly recognized by assessing at least one recognized organic attribute Fig.1 shows the general block diagram for a biometric system. Interesting identifiers incorporate fingerprints, hand geometry, ear cartilage geometry, retina and iris designs, voice waves, DNA, and face. The most established type of biometric confirmation is fingerprinting. The biometric check has progressed extensively with the appearance of modernized databases and the digitization of simple information, considering the relatively momentary individual distinguishing proof. Iris and retina-design validation techniques are, as of now utilized in some bank-programmed teller machines.

Voice waveform acknowledgment, a strategy for confirmation that has been utilized for a long time with tape accounts in phone wiretaps, is presently being utilized for access to exclusive databanks in looking into offices. Facial recognition innovation has been utilized by law implementation to choose people in vast groups with extensive unwavering quality. Hand geometry is being utilized as a part of the industry to give physical access to structures. Ear cartilage geometry has been utilized to invalidate the personality of people who claim to be somebody else (wholesale fraud). Signature correlation isn't as dependable, independent from anyone else, as the other biometric confirmation techniques however offer an additional layer of check when utilized as a part of conjunction with at least one different strategy[1]. This paper is focused on face biometrics and the various spoofing anti-spoofingfing methods.

Face biometrics is the second largest biometric used, with fingerprint being the first. Hence, it is more open to spoofing attacks or direct (presentation) attacks in which intruders use synthetically produced artifacts or try to mimic the behavior of genuine users, to fraudulently gain access to the biometric system. Certain countermeasures have to be implemented in the form of anti-spoofing methods in order to make biometric verification more secure. An antispoofing technique is normally acknowledged to be any procedure, which can consequently recognize genuine biometric attributes displayed to the sensor from fake biometric characteristics.

## 1.2 FACE SPOOFING

In general, people used to disguise themselves as a different person in order to access their personal data. This is known as spoofing. With the advancement in technology, plastic surgery has become quite popular due to its low cost as well as the speed in which this is carried out, this makes spoofing attacks more difficult to detect. Regardless of the endeavors to create particular algorithms to facial surgery changes, the issue of recognition after surgery is as yet an open challenge for automatic face authentication systems. Some works have also shown that face-based biometric systems may be bypassed using normal makeup [2]. Fig. 2. Shows the various kinds of spoofing attacks that can be carried out in a controlled and adverse scenario.

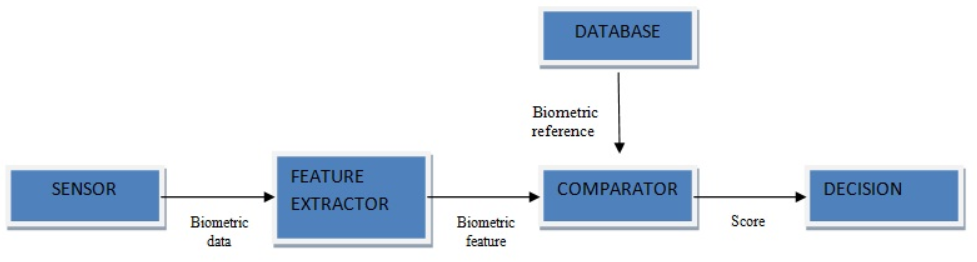


FIG:01: Working process of a basic detector

**CHAPTER – 2**

# **FACIAL RECOGNITION**

## 2.1 TYPES OF ATTACKS

Nowadays, facial recognition is becoming the second most largely deployed biometric authentication method at the world level in terms of market quota right after fingerprints. Each day more and more manufacturers are including face recognition in their products, such as Apple with its Face-ID technology, the banks with the implementation of eKYC solutions for the onboarding process.

Contrary to the main aim of research in face recognition has been given to the improvement of the performance at the verification and identification tasks, the security vulnerabilities of face recognition systems have been much less studied in the past, and only over the recent few years, some attention has been given to detecting different types of attacks consists of detecting whether a biometric trait comes from a living person or it is a fake.

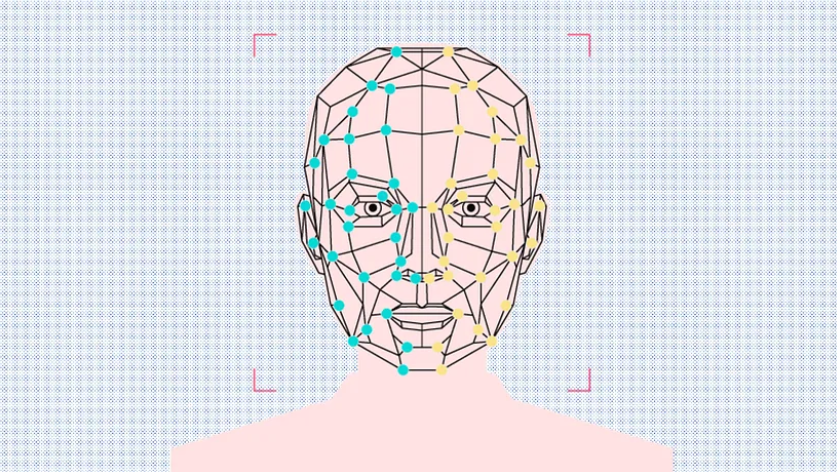


FIG:02: Face recognition process

**Two types of attacks used on the facial recognition system**

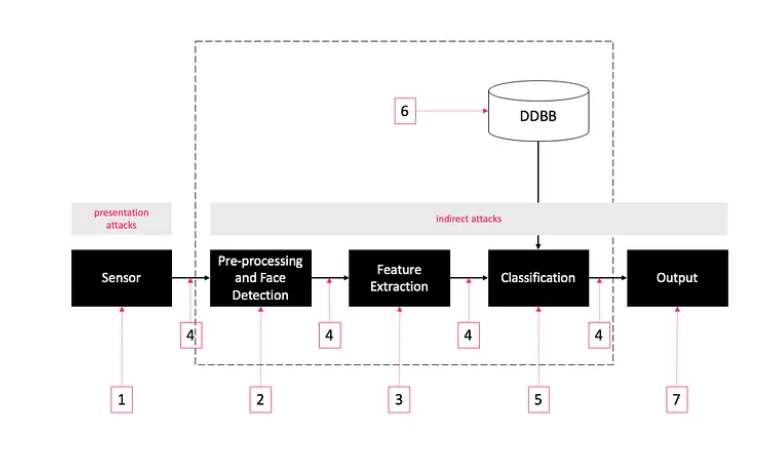
****

FIG:03: Attacks in the facial recognition system

As shown in the figure above, there exist seven modules and points that can be the target of an attack, they are divided into two types: presentation and indirect attack.

## 2.1.1 PRESENTATION ATTACKS

Presentation attacks are performed at sensor level (1), without the need of having access to the interior of the system.

Presentation attacks are related to purely biometric vulnerabilities. In these attacks, intruders use some type of artifact, typically artificial (e.g., a face photo, a mask, a synthetic fingerprint, or a printed iris image), or try to mimic the aspect of genuine users (e.g., gait, signature) to fraudulently access the biometric system.

Because “biometric traits are not secrets”, attackers are aware of this reality that a high amount of biometric data are exposed showing the face, eyes, voice, and behavior of people, so they take advantage of those sources of information to try to circumvent face recognition systems using the following examples.

* Attackers use a photograph of the user to be impersonated.
* They use a video of the user to be impersonated.
* Or hackers can build and use a 3D model of the attacked face, for example, a hyperrealistic mask

We use anti-spoofing techniques to prevent these attacks.

**2.1.2 INDIRECT ATTACKS**

Indirect attacks (2–7) can be performed at the database, that matches, the communication channels, etc. In this type of attack, the attacker needs access to the interior of the system.

Indirect attacks can be prevented by the techniques related to “classical” cybersecurity than to biometrics, so we will don’t discuss them in this post.

**2.2 ATTACKING METHODS**

Without implementing presentation attack detection measures, most state-of-the-art facial biometric systems are vulnerable to simple attacks.

Typically, face recognition systems can be spoofed by presenting to the camera a photograph, a video, or a 3D mask of a targeted person. or use makeup or plastic surgery. However, using photographs and videos is the most common type of attack due to the high exposition of the face and the low cost of high-resolution digital cameras.

**2.2.1 PHOTO ATTACKS :**

The photograph of a genuine user may be taken by the attacker using a digital camera or even retrieved from the internet [3]. Another type of photo attack is the use of photographic masks. These are high-resolution printed photographs where the eyes and mouth have been cut out. Liveness detection can be bypassed as certain facial movements such as blinking of the eye are reproduced.

|  |
| --- |
|  |



FIG:04: Photo Attack

**2.2.2 VIDEO ATTACKS :**

Also known as replay attacks, is a sophisticated version of simple photo spoofs. In this case, the attacker does not use a still image but replays a video of the genuine client using a digital device (e.g., mobile phone, tablet, or laptop) [4], [5].

|  |
| --- |
|  |



FIG:05: Video Attack

**2.2.3 MASK ATTACKS :**

The spoofing artifact is a 3D mask of the genuine client’s face, which makes it difficult to detect impostors. Although the possibility to bypass a biometric system by wearing a mask imitating the face of a different user is an idea that has been circulating for some time [6], these attacks are far less common than the previous two categories due to the increase in cost to reproduce the artifact.

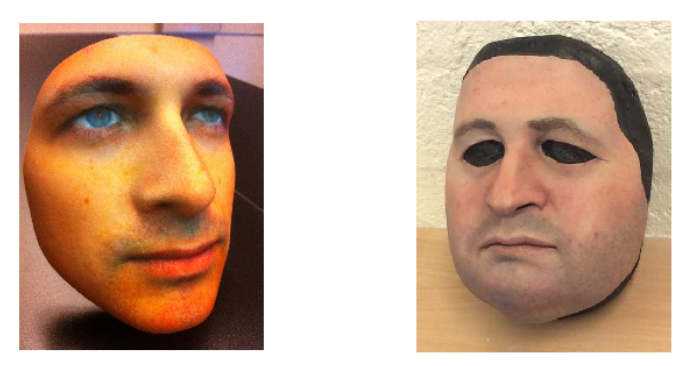
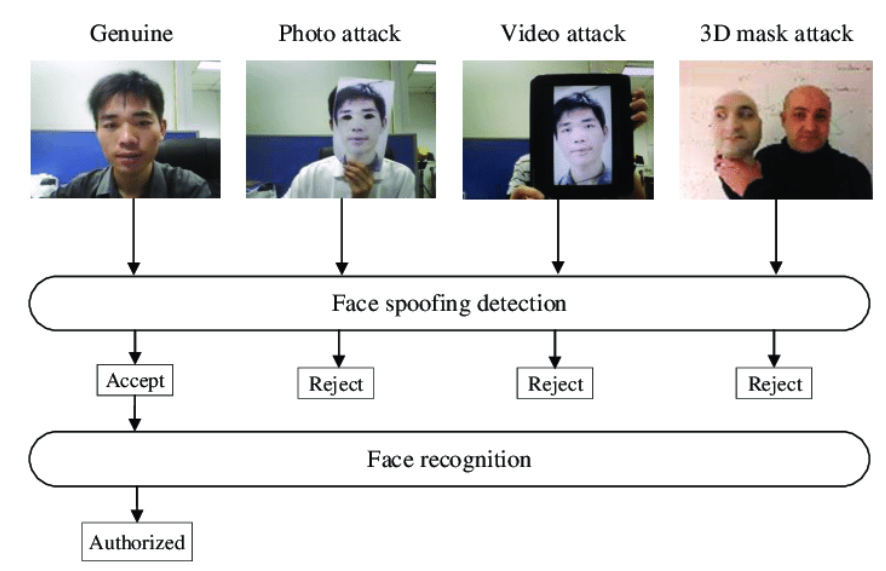


FIG:05: Mask Attack

# **The face spoofing attacks and face spoofing detection task :**



|  |
| --- |
|  |

FIG:06: Face spoofing attacks

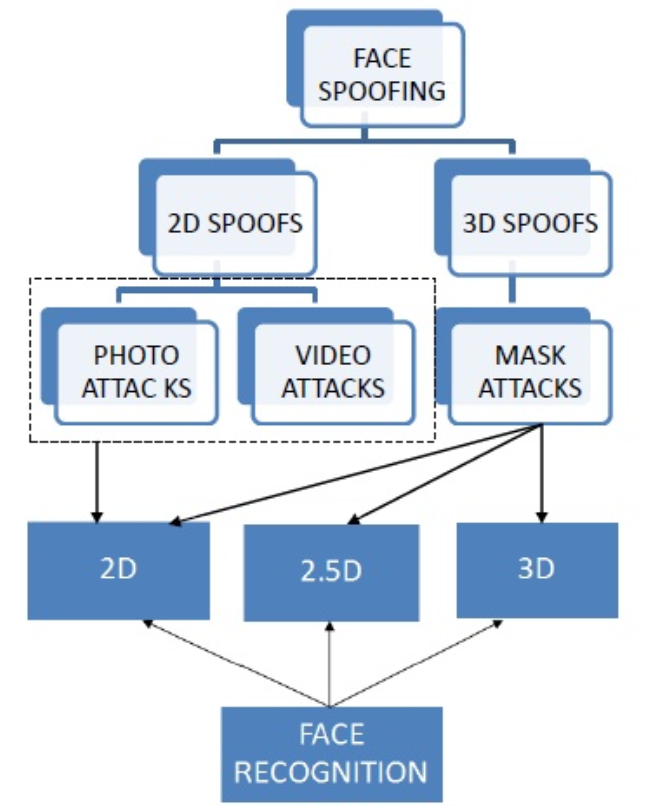
****

FIG. 07: FACE SPOOFING TECHNIQUE CLASSIFICATION

**CHAPTER – 3**

# ANTI-SPOOFING TECHNIQUES

**3: ANTI-SPOOFING TECHNIQUES:**

Because most of the facial recognition system is easy to be attacked by spoofing methods. Therefore, in order to design a secure face recognition system in a real scenario, anti-spoofing techniques should be a top priority from the initial planning of the system.Since face recognition systems try to differentiate between genuine users, not to determine if the biometric sample presented to the sensor is real or a fake. We can do them in four different ways as follows.

**3.1 SENSORS :**

We use available sensors to detect in the signal any pattern characteristic of live traits.

**Dedicated hardware**

With dedicated hardware to detect evidence of liveness such as a 3D camera, but which is not always possible to deploy.

## Challenge-response method

Using a challenge-response method where a presentation attack can be detected by requesting the user to interact with the system in a specific way.

* Smiles
* Facial expressions of sadness or happiness
* Head movements

**3.2 ALGORITHMS :**

Using the following recognition algorithms is intrinsically robust against attacks.

**Specular feature projections:**First, by characterizing the specular feature space corresponding to genuine images and learning the projections of genuine and spoof data on this basis. Nextly the SVM model is trained corresponding to genuine projections, 3D mask projections, and printed photo projections are then used as an anti-spoofing model for detecting impersonations.

**Depth feature fusion:**by deeply studying the importance of facial image color feature information for human face detection, a deep feature fusion network structure is constructed by deep convolutional neural networks ResNet and SENet to effectively train the involved face anti-spoof data.

**Image quality assessment:** the method is based on the combination of image quality measures. This solution compares the original image with an image processed.

**Deep learning**: this method is based on a multi-input architecture that combines a pre-trained CNN model and the local binary patterns descriptor.

**CHAPTER – 4**

# ANTI-SPOOFING LEVEL TECHNIQUES

**4.1: SENSOR-LEVEL TECHNIQUES :**

Otherwise referred to as hardware-based techniques where a specific device is integrated in the biometric sensor which helps to detect specific properties of a living trait. It measures one of three characteristics, namely:

Intrinsic properties of a living body - which could include properties like physical, electrical, spectral or visual properties. Involuntary signals of a living body eg. blood pressure, perspiration, electric heart signal

Responses to external stimuli also referred to as challenge-response methods, require the cooperation from the user as these responses are based on detecting voluntary (behavioural) or involuntary (reflex reactions) to an external signal. Eg. When light is switched on the pupil contracts (reflex), or the head moves following a random path determined by the system (behavioural). Multibiometric anti spoofing is based on the assumption that the blending of various biometrics will decrease the vulnerability to assaults, as, in principle, producing multiple fake characteristics is more difficult than generating an individual fake characteristic. Based on this assumption, multimodal approaches fuse different modalities.

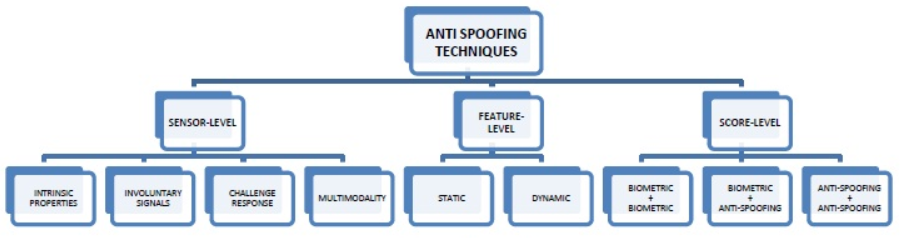


FIG. 08: ANTI-SPOOFING TECHNIQUES

The strategy is using complementary traits for eg. Finger print and finger veins, this strategy requires additional hardware devices, therefore, these techniques may be included in the sensor-level group of anti-spoofing methods. The above assumption of fooling a multibiometric system has already been shown to be untrue as, in many cases, bypassing just one of the unimodal subsystems is enough to gain access to the complete application. Hence, multibiometry by itself does not necessarily guarantee a higher level of protection against spoofing attacks.

**4.2: FEATURE-LEVEL TECHNIQUES :**

Otherwise referred to as software-based techniques, here, the biometric data is acquired with a standard sensor and the distinction between fake and real faces is software based. Under Software based techniques there are two methods for anti spoofing - static and dynamic. Static features may present some degradation in performance but is still preferred over dynamic techniques because it is faster and less intrusive as they require less cooperation from the user. Static anti spoofing methods work on single images while dynamic anti spoofing methods work on video sequence. In feature level technique, multimodality can be implemented. From just one single high resolution image of a face, both face and iris recognition can be performed.

It not only detects spoofing attacks but it also is capable of detecting other types of illegal break-in attempts. For eg. Feature level techniques protects the system against the injection of reconstructed or synthetic samples [9]. The advantages of Feature-level dynamic are - It has high accuracy level. It exploits spatial and temporal features in a video sequence. It is known to be very effective against photo attacks. The disadvantages are – Cannot be used in single image scenario instances. It is comparably slow. Accuracy is lost against video attacks. The advantages of Feature-level static are – It can not only be used with a video sequence but also can be used for single images. Faster when compared to Feature level dynamic technique. It is totally transparent to the user. The disadvantages are – It is based only on image spatial information which reduces the accuracy.

**4.3: SCORE-LEVEL TECHNIQUES :**

It is the most recently introduced anti spoofing technique. This method focuses on the study of bio metric system at score level in order to propose fusion strategies that increase their resistance against spoofing attempts. They are often considered as a supplementary to sensor level and feature level techniques due to their limited performance. The scores to be combined may come from a)two or more unimodal biometric modules b)unimodal biometric modules and anti - spoofing techniques, or c)only results from anti-spoofing modules. The advantages of Sensor-level are – It is highly accurate against all types of spoofing attacks like photo, video and mask.

The disadvantages are – It is generally slower. Higher level of cooperation is required from the user. It is expensive due to the additional hardware that is required to process the biometric traits. The diagram Fig.4. shown below specifies the modules used in biometric system that is the Sensor level, Feature level and Score level. It not only shows the protection offered against spoofing attacks but also shows the protection offered against attacks carried out with synthetic or reconstructed samples.

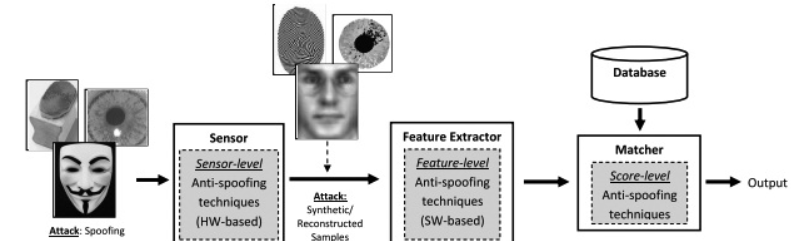


FIG:09:Score-Level Techniques

**CHAPTER – 5**

# TECHNIQUES FOR LIVENESS DETECTION

**5: LIVENESS DETECTION :**

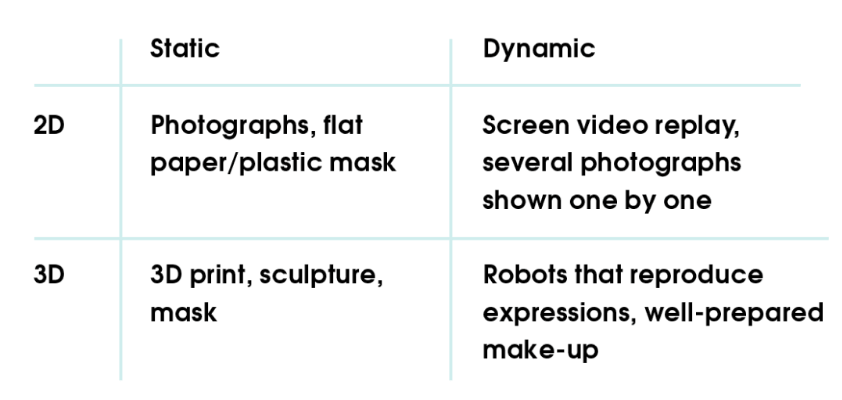
Biometric face recognition technology is a key to security. Finding someone’s photo or video on Facebook or Youtube is easy. These images and videos can be used for ill intent. Face recognition-based biometric authentication systems are vulnerable to attacks via paper photographs, screen replay, or 3D face reconstruction. A security system designed to prevent face spoofing is important. Following is an overview of presentation attacks and anti-spoofing techniques powered by Machine Learning.

**5.1: FACE RECOGNITION :**

Face identification and recognition is a process of comparing data received from the camera to a database of known faces and finding a match. This general face recognition process is flawed. What if someone uses a fake face? Liveness check counters this, distinguishing between a real face and a picture.

**5.1.1: PRESENTATION ATTACKS :**

Attacks on a face recognition system are called Presentation Attacks, or PA. These attacks can be sorted into the following categories:

****

Of course, as technologies evolve, so do presentation attacks.

3D spoofing is not a big problem yet. 2D spoofing is more widespread. This puts the onus on detecting and preventing presentation attacks. The requirements are precise. The product must:

* combat 2D attacks, static or dynamic
* use images, not videos
* work without user interaction

The objective: achieve maximum accuracy in minimum time while also providing a user-friendly experience. A model meeting these requirements would be easy to integrate with existing face recognition systems.

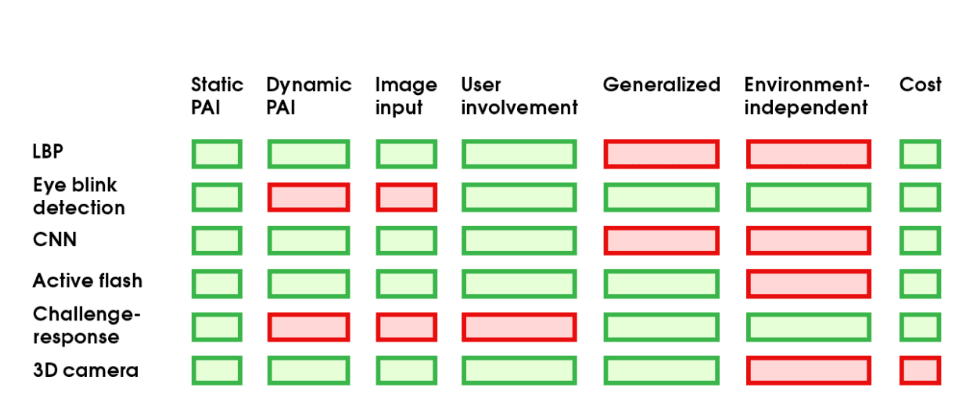
**5.2: OVERVIEW OF SPOOFING SOLUTIONS :** 

FIG:10:Score-Level Techniques

Liveness detection approaches can be combined. Challenge-response and LBP is one example. The first approach uses movements to determine face liveness. The second ensures these movements are not shown on a flat screen. Light reflection and challenge-response can be combined, showing whether a face appears on a flat surface and whether it’s a static mask or 3D print.

**Measuring efficacy: Metrics**

The accuracy of an anti-spoofing system can and should be measured.

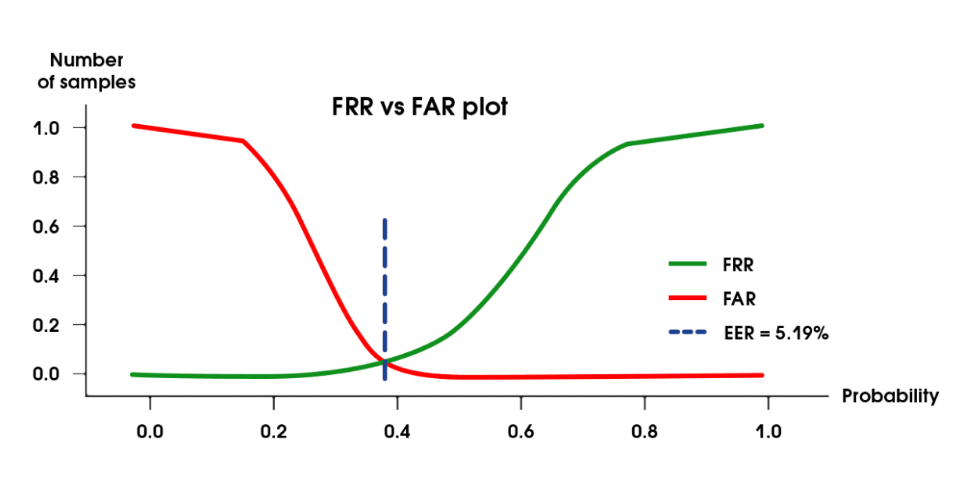


FIG:11:Measuring efficacy

False Acceptance Rate (FAR) and False Rejection Rate (FRR), which are common for biometric verification, are also used for face anti-spoofing. Task specifics define the metrics used to interpret errors. If the objective is to catch every attack, FAR should be minimized. If a user-friendly experience has higher priority, FRR becomes more important. If we visualize probabilities in the following way we will see that 2 curves intersect at a certain point.

This point is Equal Error Rate and it helps to select the best threshold value for decision making. Depending upon the security requirements, we can move threshold value left or right giving an advantage to FAR or FRR. In our case smooth user experience was more important so we adjusted the threshold value in order to minimize FRR.

**5.3: PREVENTING PRESENTATION ATTACKS :**

**Cheaper 3D cameras**

It makes sense to use cheap hardware, if it can provide depth information, to get the safest and most reliable PAD system. A significant amount of recent research is based on datasets collected with the help of 3D cameras.

**Anomaly detection**

In each PAD approach mentioned above, the task was considered a two-class classification. Some propose that anomaly detection is better suited to anti-spoofing, making the network more generalized. All genuine samples have the same nature in common. Attack samples differ but are diverse and rarely combined into a single class.

**Metric learning techniques**

Metric learning techniques are applied to achieve better generalization by minimizing the variance in feature distributions. Variance can be caused by domain or identity specifics. Presentation attack instruments are considered as domains in this case. For example, print and screen replay attacks form separate distributions in the feature space. When the model faces new, unseen devices used for making an attack, there will be a new domain distribution and thus feature separation might lead to misclassifications. This problem can be solved by using distance-based metrics to help change the network training process to reduce separation between distributions.

**CHAPTER – 6**

# **CONCLUSION AND REFERENCE**

**CONCLUSION**

In the anti spoofing techniques, the sensor level presents a higher fake detection rate, whilst feature level techniques are less expensive, less intrusive and more user friendly, since their implementation is hidden from the user. The score level protection technique presents a much lower performance when compared to the sensor level and feature level protection measures. Hence, they are designed only as a support to the sensor level and feature level techniques. Although significant amount of work has been carried out in the field of biometric antispoofing, the level of hacking methodologies have also evolved becoming more sophisticated. As a result, there are still improvements to be made to the current anti spoofing techniques that can challenge the evolving direct attacks in order to make the system more secure.

**REFERENCES**

[1] Javier Galbally, Ssebastien Marcel, (Member, IEEE), and Julian Fierrez.-‘Biometric Antispoofing Methods: A Survey inFace Recognition’.

[2] A. Dantcheva, C. Chen, and A. Ross, ‘‘Can facial cosmetics affect the matching accuracy of face recognition systems?’’ in Proc. IEEE 5th Int. Conf.

Biometrics, Theory, Appl. Syst. (BTAS), Sep. 2013, pp. 391–398.

[3] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, ‘‘Understanding OSN-based facial disclosure against face authentication systems,’’ in Proc. ACM Asia

Symp. Inf., Comput. Commun. Security (ASIACCS), 2014, pp. 413–424.

[4] I. Chingovska, A. Anjos, and S. Marcel, ‘‘On the effectiveness of local binary patterns in face anti-spoofing,’’ in Proc. IEEE Int. Conf. Biometrics Special

Interest Group (BIOSIG), Sep. 2012, pp. 1–7.

[5] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, ‘‘A face antispoofing database with diverse attacks,’’ in Proc. IAPR Int. Conf. Biometrics (ICB),

Mar./Apr. 2012, pp. 26–31.

[6] Y. Kim, J. Na, S. Yoon, and J. Yi, ‘‘Masked fake face detection using radiance measurements,’’ J. Opt. Soc. Amer., vol. 26, no. 4, pp. 760–766, Apr.

2009.

[7] E. Marasco, ‘‘Secure multibiometric systems,’’ Ph.D. dissertation, Dept. Inf. Sistemistica, Univ. Naples Federico II, Naples, Italy, 2010.

[8] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, ‘‘Evaluation of serial and parallel multibiometric systems under spoofing attacks,’’ in Proc. IEEE 5th

Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS), Sep. 2012, pp. 283–288.

[9] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, ‘‘Fingerprint image reconstruction from standard templates,’’ IEEE Trans. Pattern Anal. Mach. Intell.,

vol. 29, no. 9, pp. 1489–1503, Sep. 2007.