IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Face Biometric Antispoofing

Minu Correya[1], Dr. Thippeswamy G[2]

M.Tech Student, Department of CSE, BMS IT&M, Bangalore, India[1]

Head of Department, Department of CSE, BMS IT&M, Bangalore, India[2]

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 system to detect fake artefacts and to 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.

Keywords: Biometrics, spoofing, antispoofing, antispoofing techniques.

I. INTRODUCTION

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 recognizing organic attributes. 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. Biometric check has progressed extensively with the appearance of modernized databases and the digitization of simple information, considering 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 look into offices. Facial recognition innovation has been utilized by law implementation to choose people in vast group with extensive unwavering quality. Hand geometry is being utilized as a part of 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, the various spoofing and anti spoofing 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 artefact or try to mimic the behaviour 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 characteristic.

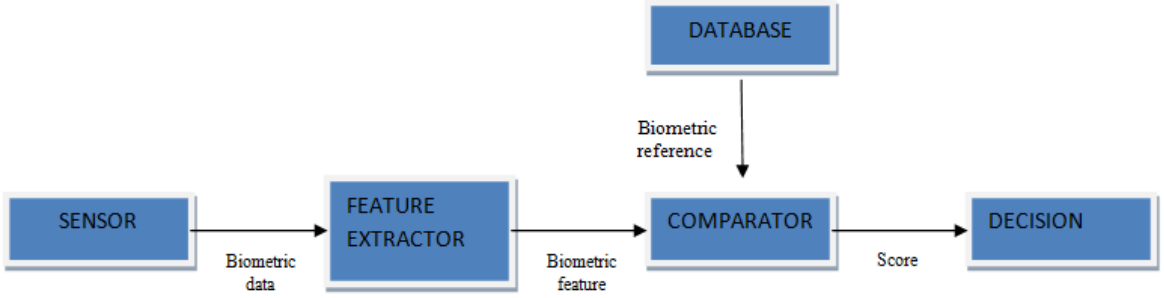

Fig. 1.Biometric system

DOI 10.17148/IJARCCE.2018.7310

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

II. 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 endeavours 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 a normal make-up [2].Fig. 2. Shows the various kinds of spoofing attacks that can be carried out in a controlled and adverse scenario.

A. Three types of spoofing attacks:

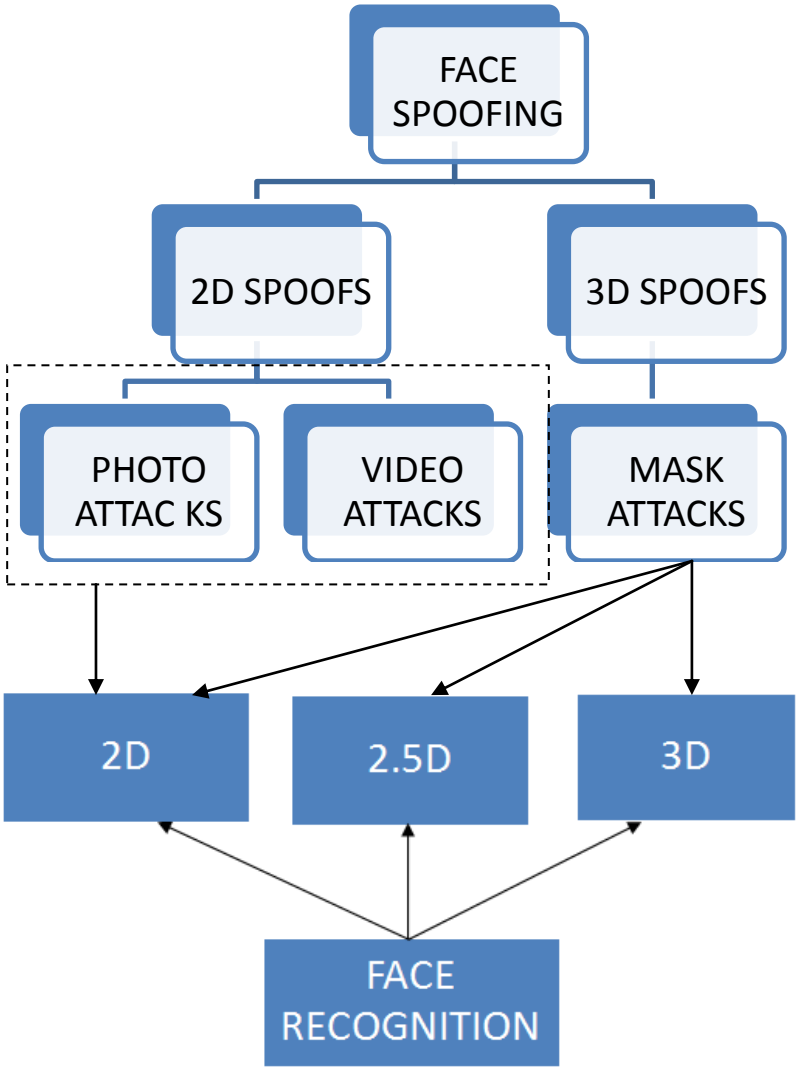

Fig. 2. Face spoofing technique classification

- 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 eyes and mouth have been cut out. Liveness detection can be bypassed as certain facial movements such as blinking of the eye are reproduced.
- Video Attacks. Also known as replay attacks, is a sophisticated version of the 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].
- Mask Attacks. The spoofing artefact 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 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 increase in cost to reproduce the artefact.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

III.ANTI SPOOFING TECHNIQUES

Anti-spoofing techniques as shown in Fig.3., depending on the biometric system module in which they are integrated may be classified into one of three groups:

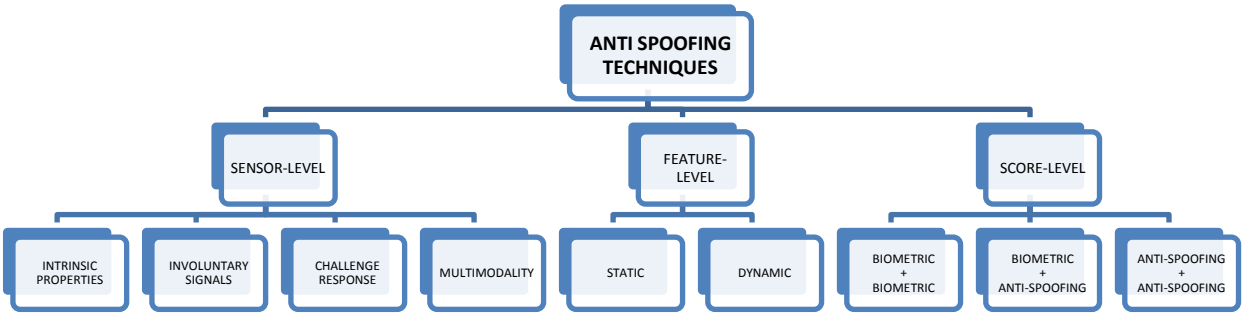

Fig.3. Anti Spoofing Techniques

A. 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 signals
- Responses to external stimuli, also referred to as challenge-response methods, which requires 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[7], 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. 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 [8]. Hence, multibiometry by itself does not necessarily guarantee a higher level of protection against spoofing attacks.

B. 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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

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

C. Score level technique

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 acurate 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.

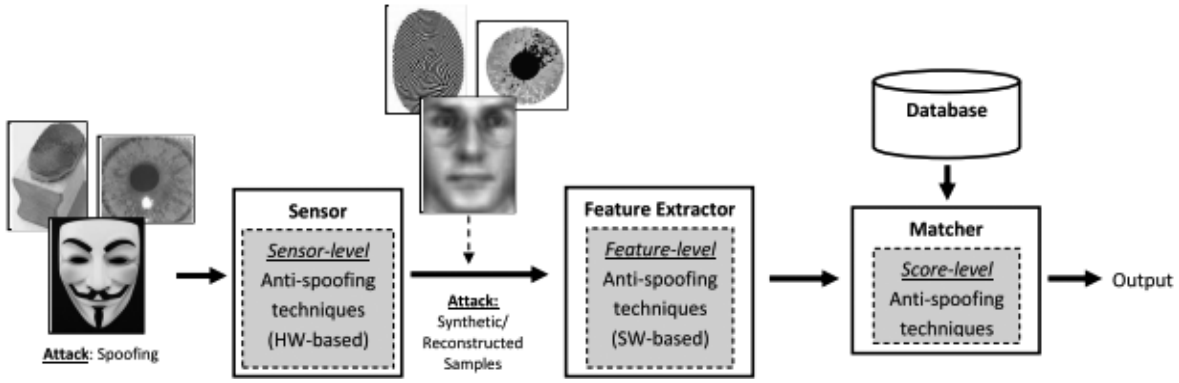

Fig.4.Biometrics system modules specifying three types of Anti Spoofing Techniques

IV. 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.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude for the support and guidance rendered by all the faculty members of Computer Science and Engineering Department, BMS Institute of Technology and Management, Bangalore.

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.