Face Anti-spoofing methods

Rinu Anna Varghese
M. Tech Student
Department of Electrical Communication Engineering
Mount Zion College Of Engineering And Technology, Kadammanita

Juby Susan Mathew
M. Tech Student
Department of Electrical Communication Engineering
Mount Zion College Of Engineering And Technology, Kadammanita

Abstract

Biometric spoofing is a method of fooling a biometric identification management system, where an artificial object is presented to the biometric scanner that imitates the unique biological properties of a person which the system is designed to measure, so that the system will not be able to distinguish the artifact from the real biological target. Different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks. Here, we discuss the spoofing and anti spoofing in face biometrics.

Keywords: Spoofing, Anti-spoofing

I. INTRODUCTION

FOR thousands of years, humans have used body characteristics such as face, voice, gait, and so on to recognize each other. Biometrics first came into extensive use for law-enforcement and legal purposes—identification of criminals and illegal aliens, security clearances for employees in sensitive jobs, paternity determinations, forensics, positive identifications of convicts and prisoners, and so on. Today, however, many civilian and private-sector applications are increasingly using biometrics to establish personal recognition. The term comes from the Greek words bios (life) and metrikos (measure). Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the requirements of universality, distinctiveness, permanence, and collectability [1]

According to the International Biometric Group (IBG), face is the second most largely deployed biometric at world level in terms of market quota right after fingerprints[1]. It is also adopted in most official identification documents such as the ICAO-compliant biometric passport or national ID cards. As such, nowadays face is one of the biometric traits with the highest potential impact both from an economic and a social point of view.

In recent years, facial biometric systems have received increased deployment in various applications such as Surveillance, access control and forensic investigations. However, one of the limitations of face recognition system is the high possibility of the system being deceived or spoofed by non-real faces such as photograph, video clips or dummy face.

II. FACE SPOOFING

Facial biometrics spoofing techniques involve placing genuine photographs or dummies, playing video recording etc. in front of the camera. A human photograph represents planar objects with only one static facial expression. However, it lacks the three-dimensional (3D) information and provides less physiological clues than videos3. These limitations of still photographs are often exploited in liveness detection for facial biometrics. However, the challenges in facial detection increase for spoofing attacks that involve the use of video cameras.

The attacks can be classified in to two groups depending on whether the artefacts used are: *i*) 2D surfaces (e.g., photo, video) which are successful against 2D face recognition systems or *ii*) 3D volumes (e.g., masks) which may be used to attack 2D, 2.5D and 3D face recognition technology. Such artefacts have been used to carry out three main types of attacks [1] which present an increasing level of spoofing potential:

A. Photo Attacks:

These fraudulent access attempts are carried out presenting to the recognition system a photograph of the genuine user. The photograph may have been taken by the attacker using a digital camera, or even retrieved from the internet after the user himself uploaded it to one of the very popular online social networks available today. The image can then be printed on a paper (i.e., print attacks, which were the first to be systematically studied in the literature) or may be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital-photo attacks) .A slightly more advanced type of photo-attack that has also been studied is the use of photographic masks. These masks are high resolution printed photographs where eyes and mouth have been cut out. At the time of the attack the impostor is placed behind so that certain face movements such as eye blinking are reproduced .

B. Video Attacks:

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). Such attacks appeared as a further step in the evolution of face spoofing and are more difficult to detect, as not only the face 2D texture is copied but also its dynamics.

C. Mask Attacks:

In these cases the spoofing artefact is a 3D mask of the genuine client's face, increasing the difficulty to find accurate countermeasures against them. Since the complete 3D structure of the face is imitated, the use of depth cues which could be a solution to prevent the previous two types of attacks (carried out with at surfaces), becomes inefficient against this particular threat.

III. FACE ANTI-SPOOFING

In the area of anti-spoofing assessment, as in other biometric related scenarios, two main types of evaluations are possible: (i) algorithm-based, also known as the technology evaluation thought to evaluate liveness detection modules or algorithms, independently of the rest of the system. This type of evaluation is therefore well suited to assess feature-level techniques; (ii) system-based, also known as scenario evaluation, designed to evaluate biometric systems as a whole, including the scanner. Adequate therefore to assess sensor-level schemes where acquisition devices are specific for each system. [1]

The advantage of algorithm-based evaluations is that the same data and protocol may be used to assess all techniques. Furthermore, this benchmark can be made public, so that future software-based methods may be directly compared to the evaluation results. On the other hand, system based evaluations are just restricted to the scope of a given competition, and no further comparison may be established with future systems, as new data would have to be acquired for each specific sensor. That is, due to their intrinsic hardware-based nature, it is not possible to acquire a single distributable database that satisfies the particular hardware acquisition requirements of each different sensor-based approach.

The typical countermeasure to spoofing attacks is liveness detection that aims at detecting physiological signs of life (such as eye blinking, facial expression changes and mouth movements).

In blinking-based liveness detection, an approach proposed by Pan et al [2] is introduced for prevention of photograph spoofing is introduced. It requires no extra hardware except for a generic web camera. Eyeblink sequences often have a complex underlying structure. We formulate blink detection as inference in an undirected conditional graphical framework, and are able to learn a compact and efficient observation and transition potentials from data. For purpose of quick and accurate recognition of the blink behavior, eye closity, an easily-computed discriminative measure derived from the adaptive boosting algorithm, is developed, and then smoothly embedded into the conditional model.

This may work in cases of attacks using photographs, they are generally ineffective when using a video (or simply shaking the photograph before the camera) as a mean of spoofing.

Inspired by image quality assessment, characterization of printing artifacts and by differences in light reflection, An approach for spoofing detection is proposed [3]based on learning the micro-texture patterns that discriminate live face images from fake ones.

A novel approach of liveness detection based on skin elasticity is proposed in [4]. In which a set of face images is captured after asking the user to do some face movement activities. Then correlation coefficient is calculated and images are discriminated using some discriminant analysis. Since this approach is software based, so it will be less cost method for liveness detection.

A method for detecting eyes in sequential input images and then variation of each eye region is calculated and whether the input face is real or not is determined [5]. The basic assumption is that because of blinking and uncontrolled movements of the pupils in human eyes, there should be big shape variations. Liveness detection can also be carried out by the analysis of lip movements and lip reading [5].

A method based on information of the structure and the movement of a face is described [6] by the classification between live and fake faces using Fourier spectra, based on the assumption that high frequency components of photo are less than that of a live face. However, it was sensitive to the lighting effect and vulnerable to spoofing attacks using high quality photographs.

Liveness can also be evaluated by using a technique based on a short sequence of images [7]. The work describes a binary detector that evaluates the trajectories of select parts of the face presented to the input sensor using a simplified optical flow analysis followed by a heuristic classifier. Such a classification scheme achieves an equal-error rate of 0.5% for samples of real accesses extracted from XM2VTS and attacks produced using hard-copies of those data.

A method that differentiates between video sequences showing real persons and their photographs is used in liveness detection. [8]. The optical flow of the face region is calculated using the Farnebäck algorithm. Then the motion information is converted into images and performs the initial data selection. Finally, the Support Vector Machine is applied to distinguish between real faces and photographs. Thus the combination of optical flow estimation and SVM classifier can be used to achieve the task of liveness verification.

One of the key challenges faced nowadays by the rapidly evolving biometric industry is the need for publicly available standard datasets that permit the objective and reproducible evaluation of different aspects related to biometric recognition systems (e.g., performance, security, interoperability or privacy). This is particularly relevant for the assessment of spoofing attacks and their corresponding anti-spoofing protection methodologies. In addition to data acquisition and distribution another key factor for developing the anti-spoofing technology is the organization of competitive evaluations. Such contests give a clear snapshot of systems performance at a given point and help to achieve a better understanding of the different algorithms accuracy. Furthermore, most public datasets are acquired in the framework of such competitions.

IV. CONCLUSION

There are different anti-spoofing methods that have been developed to raise the difficulty level for photo, video and synthesis attacks.Eventhough the outcome of research efforts on anti-spoofing appears to be making a significant progress, but the quest continues towards a more reliable and secure system. Although a great amount of work has been done in the field of spoofing detection, attacking methodologies are also becoming more and more sophisticated. As a consequence, there are still big challenges to be faced in the protection against direct attacks that will hopefully lead in the coming years to a new generation of more secure biometric systems.For blinking and movement of eyes based liveness.

REFERENCES

[1] Javier Galbally, Ssebastien Marcel, (Member, IEEE), and Julian Fierrez.-'Biometric Antispoofing Methods: A Survey inFace Recognition'
[2] Gang Pan, Zhaohui Wu and Lin Sun –'Liveness Detection for Face Recognition'
[3] Jukka Maatta, Abdenour Hadid, Matti Pietik¨ainen- 'Face Spoofing Detection From Single Images Using Micro-Texture Analysis'
[4] Dr. Chander Kant Nitin Sharma- 'Fake Face Detection Based on Skin Elasticity'
[5] Saptarshi Chakraborty and Dhrubajyoti Das- 'An overview of faceliveness detection'
[6] Sajida Parveen,*, Sharifah Mumtazah Syed Ahmad, Marsyita Hanafi1 and Wan Azizun Wan Adnan-' Face anti-spoofing methods'
[7] Abdenour Hadid-'Face Biometrics under Spoofing Attacks:Vulnerabilities, Countermeasures, Open Issues and Research Directions.'
[8] Maciej Smiatacz –'Liveness measurements using optical flow for biometric person authentication'.