IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Anti-Spoofing Face Recognition System

Rohaan Farooq[1], Akeel Qasim[2], Arqam Fayaz[3],Mr. Tarun Kumar Chugh[4]
Department of CSE
ITS Engineering College, Greater Noida, UP, India[1,2,3,4]

Abstract: *The use of biometric recognition technologies has become extremely popular recently. Facial recognition systems have grown very popular as webcams are integrated into so many various gadgets (cell phones, tablets, laptops, access doors at some facilities, etc.). As a result, more people try to cheat these systems as they become more popular.*

The facial recognition technology is vulnerable to three different forms of attacks: image-based attack, in which the attacker displays a photo of the face of another user; video-based assault in which the attacker plays a previously captured video of a different user; Attacks based on masks occur when an attacker impersonates a legitimate user to fool a facial recognition system.

In this work, I tackle picture-based and video-based assaults. Hence, I foster a test reaction framework. The thought a methodology is to distinguish where a client can do what framework has moved him to do. Along these lines, we know that the face that is introduced to the camera is alive. The client is expected to watch a moving spot on the screen. The speck begins from the focal point of the screen and goes to the arbitrarily picked side of the screen, so this way client can't present a prerecorded video. As client follows the spot, the framework appraises the course where the client's eyes are moving. For these reasons, I carried out three unique methodologies. The custom brain network that takes as an info projections of three sequential edges of an eye development and orders which the course of the development. In the third approach, I guessed then when the client is watching at collinear focuses on a vertical line, the x directions of the client's student will be roughly something very similar having little difference. A similar applies to y organizes on a flat line. In this way by investigating the change of the directions, we can identify whether an aggressor is not introducing to someone else's Picture.

Keywords: Biometric Recognition Technologies

I. INTRODUCTION

Traditional access control systems involve keys that users are forced to carry about or passwords that they must remember. Biometric recognition has recently replaced this method of identification. Systems for biometric recognition that use a user's fingerprint, iris, voice, face, palm veins, etc. have achieved great success recently.

Furthermore, a source projects that the global market for biometric authentication and identification will surpass 51.98 billion by 2023. The usage of biometric recognition technology for user authentication is now simple and trustworthy. They are preferable to conventional methods of user identification since they cannot be forgotten or misplaced.

Nowadays they are so widely spread (from logging in to laptops, phones to paying your receipt by your face). With such popularity number of people trying to trick the system increase as well. When one user tries to present himself with a false identity and have the intention to get unapproved access is called a spoofing attack.

When one user tries to present himself with a false identity and have the intention to get unapproved access is called a spoofing attack. In order for an active system to recognize a user as being alive, the user must comply with all requests made by the system. They demand a user to interact directly with a system; the passive method, however, does not. It also does not require a user to comprehend how the system operates or what it does. It records and examines involuntary facial motions such blinking, iris movement, and the way light reflects off the surface of the face. In this work, I created an active system that asks the user to keep an eye on a dot as it moves from the screen's center to a randomly selected side. The first two methods for preventing system spoofing examine the If the direction of the user's eye movement matches the direction of the dot, the user is regarded as being alive. The third one calls for the viewer to watch at least two episodes of the dot travelling to the side of the screen, not just one. Then, when the user looks at a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

collinear object, the system analyses the variance of the user's pupil center's x and y coordinates. A user is only regarded to be alive if their value is below a specific threshold.

II. LITERATURE SURVEY

Spoofing attacks approaches

Figure 2.1 shows the typical types of spoofing attack. The unknown user attempts to exhibit someone's face as a printed picture, video clip, or 3D mask.

FIGURE 2.1: Types of spoofing attacks

Picture based-attack

Attackers frequently attempt to alter images so they approximate the 3D shape of a real human face.

Video based -attack

The capabilities of this assault type are identical to those of the previous attack type. Videos can also provide the sensor with a piece of sequential information regarding changes in face features and the dynamic nature of the environment. Which increases the likelihood of an attacker obtaining unauthorized access.

Mask based-attack

This type of attack helps to preserve 3D facial features and environmental
Conditions, it gives an adversary an ability to move eyes, which can additionally, it allows an adversary to move their eyes, which can be useful for getting around challenge-response anti-spoofing systems.

Spoofing detection approaches

There are various techniques for spotting spoofing attempts. Each of them makes use of a different aspect of the target's property. There are four main methods for preventing spoofing.

Texture Analysis

Extracts static characteristics such blurriness, illumination differences, etc. Most systems of this kind just need one image.

Image quality analysis

Assumes that a user's face will be of poorer quality when he performs a spoofing attack (picture- or video-based assaults).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Face liveliness- detection

A strategy based on sequential features. It examines the user's involuntary face, iris, and blinking movements among others to determine how alive they are. Using challenge-response techniques, the system may ask you to take certain actions (such as following a dot with your eyes, turning your head, smiling, etc.), after which it will assess whether you responded appropriately.

Hardware based solution

Using Face ID-like sensors, stereoscopic cameras, or infrared cameras. Cons of this technique include the cost of additional hardware and the difficulty in scaling and integrating it because users' devices (laptops, phones, etc.) cannot utilize hardware-based systems.

Systems can also be categorized based on user interaction. Systems can be divided into active and passive categories based on these criteria.

The active approach asks the user to take an action, like as rotating their head or staring at a stimulus, in order to interact with the system's sensor.

Because they don't require user cooperation, passive anti-spoofing strategies are more user-friendly. They recognize a user's liveness using many indicators, including as blinking, uncontrollable facial movements, how the face reflects light, image texture, and blurriness

Datasets for Anti-spoofing Face Recognition:

Replay Attack Dataset: The Replay-Attack dataset, which comprises video recordings of actual users and various spoofing attacks including printed photos and video replays, was introduced by [4].

CASIA Face Anti-Spoofing Dataset:

[6]Created the CASIA Face Anti-Spoofing Dataset, containing genuine faces and different types of spoofing attacks, including printed photos, masks, and 3D models.

NUAA Imposter Database:

The NUAA Imposter Database was created by [5]and includes real face photographs as well as spoofing techniques including printed photos and makeup masks.

Evaluation Criteria:

The accuracy, false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) evaluation criteria for anti-spoofing face recognition were covered by[6].

Existing solution

As was previously said, there are numerous ways to safeguard your facial recognition system from spoofing assaults. Several options have been put forth in recent decades.

Static models

[6]Work makes the assumption that printed photographs of real people's faces are accurate.

Faces vary from one another in terms of quality and shape. They made use of the power spectrum and the Local Binary Pattern (LBP) to perform frequency and texture studies. Next they employ combined frequency- and texture-based classifiers to spot fake images.

This technique makes use of a picture's chrominance component as opposed to the previous one.

[6]Presented a method that makes use of an image's color gradient. A Roberts cross operator is used by this anti-spoofing technology to separate a color gradient between real and fake faces.

Sharpness and blurriness are used in a model given by [1]. This technique is based on how digital focus works, where a 3D object will have areas that are sharper when it is closer to the camera and areas that are blurrier when it is farther away. They made use of the cheek and the nose on the face. Then, using a threshold, they extracted the gradient magnitude and blurriness level.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Since these methods only require one image, they are typically simple to compute.
Additionally, it is very convenient that these systems do not require the user to interact with the sensor for an extended period of time. On the other hand, they perform poorly when altered lighting, ambient conditions, or image quality occur.

Dynamics Models

The methodology used by [3] is based on examining the characteristics of real-world human behavior. With this method, the users' face is used to extract the coordinates of both eye pupils. They then determine the coordinate variance. If it exceeds a specific it meets a certain threshold, it is recognized as a genuine user; otherwise, a spoofing assault. The challenge-response technique is another method of spotting a spoofing assault.
Since the system is given dynamic features, which are more difficult to forge than static ones that are extracted from photographs, this approach offers better robustness.
Systems of this kind were employed by [2].Users were required to turn their heads in order to look in certain randomly selected directions by the system. The system calculates the user's head attitude using the model's two feature points (the corners of the left eye) and its understanding of the 3D characteristics of a human face. The technology confirmed the user was a real person if the user's head position was accurate.
The [1] provided a method where a gaze tracking system was put into place where users were shown a stimulus and were required to examine it. The system then looked at the frames where the stimulus passed by collinear locations. It is intended that the user's eyes should have similar coordinates on the x-axis while viewing collinear points. The variance of those coordinates is then investigated. In comparison to fake ones, the coordinates of a live user pupil vary less.
In general, challenge-response strategies are more reliable than static-based models because they take advantage of the sequential character of human movement. As a result, they are less sensitive to environmental changes and noise.
I then made the decision to test out several KPs. I recorded the eye movements of nine persons as they looked at the KPs in Figure 3.2(B). The idea was that since a dot travels a greater distance towards the corner of the screen than it does towards the side, the eye movement will be more pronounced and simpler to categories. The first dataset includes 24 participants who examine KPs 3.2(A), and the second dataset includes 9

III. CONCLUSION

In order to improve security measures and reduce the risks brought on by spoofing attacks, the research paper's main goal was to design an anti-spoofing facial recognition system. The research's findings and conclusions address the shortcomings of conventional facial recognition systems in spotting and thwarting spoofing attempts, and they provide a contribution to the field of biometric identification.
It was shown that precise distinction between authentic and spoofed facial photos may be obtained with the deployment of an effective and reliable anti-spoofing algorithm. The system demonstrated better effectiveness in identifying several spoofing methods, such as printed pictures, 3D masks, and deep fake movies, by adding cutting-edge techniques like liveness recognition and user interaction difficulties.
The proposed anti-spoofing facial recognition system, according to the evaluation process's findings, had a high level of accuracy and reliability. It showed the capacity to recognize and reject fake face photos with accuracy, reducing the likelihood of unauthorized access, identity theft, and fraudulent activity.
The effective creation of this anti-spoofing facial recognition system will have wide-ranging effects on practical applications. Businesses in sectors like banking, law enforcement, and secure facilities can gain from heightened security measures that protect sensitive data and guarantee system integrity.
It is crucial to remember that even if the proposed system produced encouraging results, there are still some restrictions and difficulties that must be overcome. It is still difficult to find a variety of reliable faked face image datasets for training and testing. The system needs more study and development to keep performing better and to adapt to new spoofing methods.
In conclusion, this research paper makes a valuable contribution to the field of anti-spoofing face recognition. It highlights the importance of incorporating robust anti-spoofing mechanisms into face recognition systems to ensure the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

authenticity of identity verification. The proposed system demonstrates the potential to enhance security measures and protect against spoofing attacks, ultimately contributing to the advancement of biometric authentication technologies.

ACKNOWLEDGEMENT

I would like to thank everyone who helped me finish my research work on anti-spoofing face recognition and for their contributions. First of all, I would like to thank my supervisor for her invaluable advice, knowledge, and support during the study process.

I also want to express my gratitude to the volunteers who voluntarily offered their time and vital facial data for the research. Their assistance was crucial in getting important outcomes.

In addition, I want to thank the academics and researchers whose earlier work served as the basis for our study. They have made incredibly essential contributions and breakthroughs to the field of anti-spoofing face recognition.

REFERENCES

[1]. Ali,Asad,FarzinDeravi, and SanaulHoque (2012)."Liveness detection using gaze collinearity". IEEE pp.62-65.

[2]. Frischholz, Robert W and Alexander Werner (2003). “Avoiding replay attacks in a face recognition system using head-pose estimation”. In: Analysis and Modeling of Faces and Gestures, 2003. AMFG 2003. IEEE International Workshop on. IEEE, pp. 234–235

[3]. Jee, Hyung-Keun, Sung-Uk Jung, and Jang-HeeYoo (2006). “Liveness detection for embedded face recognition system”. In: International Journal of Biological and Medical Sciences 1.4, pp. 235–238.

[4]. Chingovska, I., et al. (2012). On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. In Proceedings of the IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1-6.

[5]. Tan,X., et al. (2010). Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1-8.

[6]. Zhang, Z., et al. (2012). A Face Anti-Spoofing Scheme Based on Image Distortion Analysis. In Proceedings of the IEEE International Conference on Automatic Face & Gesture Recognition (FG), pp. 1-6.1.Ali, Asad, FarzinDeravi, and SanaulHoque (2012). “Liveness detection using gaze collinearity”.