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

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".