Attacks and Mitigation Techniques for Iris-based Authentication Systems

Laeticia Etienne and Hossain Shahriar
Department of Information Technology
Kennesaw State University, USA
letienne3@students.kennesaw.edu
hshahria@kennesaw.edu

***Abstract*— Authentication is a key step for accessing resources and services. Currently, there are several ways of performing authentication such as text-based passwords and graphical images. These methods can be circumvented to bypass authentication system. Biometric signatures have been gaining popularity for user authentication. In this paper, we examine various attacks on iris-based authentication system followed by some common examples of mitigation techniques.**

Keywords—Iris; Authentication system; Classification.

I. INTRODUCTION

Authentication is a key step for accessing resources and services [1]. Currently, there are several ways of performing authentication such as text-based passwords and graphical images. However, these methods can be circumvented to bypass authentication system. Biometric signatures have been gaining popularity for user authentication. One common biometric-based authentication approach is iris pattern recognition [2]. In an iris-based authentication system, iris images are captured from users, and features are extracted to be matched at a later stage for authentication.

Iris is unique for each individual. It has distinct textures and patterns that can be used for authentication. Iris-based authentication can overcome the limitations of traditional password-based authentication systems that are vulnerable to brute force and dictionary-based attacks. However, iris-based authentication systems are vulnerable to several attack types such as Media Based Facial Forgery [3]. In this paper, we examine various attacks on iris-based authentication system followed by some common examples of mitigation techniques.

II. ATTACK TYPES AND MITIGATION APPROACHES

Media based Forgery and Spoofing are the most common kind of attacks in iris-based authentication system. Similarly, we find replay attack against iris is common [13]. Those kind of attack method can be detected as liveness detection. Liveness detection allows system to validate the authentication process of valid user by real biometric identifiers. Below we define a number of attack types.

a) Media based forgery: Media based forgery is one of the common intrusion method to deceive any biometric based authentication or processing system. Intruder can present printed images or frames of images of authenticated user and slip out of liveness detection to get authenticated user's access in the system. For finger print authentication system, attackers can use authenticated user's printed finger print in polymer plastic to authenticated access in the system.

b) Spoofing: Spoofing is a method of biometric liveness attack against identification system where a dummy artificial object of a user is presented by an intruder to the system to imitate the identification feature which the process is designed to check so that it can allow authentication to attacker. It is similar to use the cloned biometric part of any authenticated user and apply a biometric part to get access in the system. Spoofing is mostly used by most attackers in biometric authentication attack. In context of our topic we can do face spoofing attack by using printed iris image or any cosmetic contact lens. These kind of attacks can be crucial and alarming points for system authentication and cause a serious damage to system.

c) Fake Iris: Iris recognition system uses data stored in the system that are merely bits of code in binary form. Reverse engineering is possible to obtain the actual image of the iris. Genetic algorithm can be used to make different attempts using synthetic iris to be recognizable to iris detection. It takes about 100 to 200 iterations to produce a similar iris image that is stored in iris recognition system.

d) Presentation attacks: The presentation of biometric spoof is called presentation attack. Biometric spoof could be some image, video instead of a live person; or fake silicon or gelatin fingerprints or fake synthetic iris instead of real eye. Recognition system should be equipped with liveliness detection systems. It detects whether the presentation is alive or a spoof.

We compare existing iris-based authentication systems, sources of data and attack types they can defend against in Table 1. Comparison of existing solutions that address iris-based authentication system, and attacks on them are shown in Table I.

III. CONCLUSION

In this paper, we described various attacks on iris-based authentication system and classified some existing approaches. The classification shows not all authentication system capable

of defending all types of known attacks. It is worth of looking to improve current approaches and combining multiple approaches.

Table I. Comparison of biometric-based authentication system

Work	Approach	Biometric source	Attack type
Li et al. [3]	Inertial Sensor Based	Face	Facial Forgery
Pacut et al. [4]	Liveness Detection based on frequency of Iris	Iris	Spoofing
Ratha et al. [5]	Splitting of data	Fingerprint/ Iris/ Face	Spoofing
Andreas et al. [6]	Camera Photo Response Non Uniformity (PRNU) Fingerprint	Iris	Forgery & Spoofing
Kathikeyan et al. [7]	Electroencephalogram	Iris	Direct attacks and spoofing
Puhan et al. [19]	Liveness detection based on texture dissimilarity of Iris for contact lens	Iris	Contact lens Spoofing
Komogortsev et al. [8]	Oculomotor plant characteristics	Eye	Attack on mechanical replica of eye
Adam et al. [9]	Liveness detection based on amplitude spectrum	Iris	Spoofing & fake image
Rohit et al. [10]	Feature and Shape Analysis	Fingerprint	Spoofing
Karunya et al. [11]	Image Quality Assessment	Fingerprint and Iris	Spoofing & Fake image
Yuming et al. [12]	Shearlet-based feature descriptors	Face	Spoofing & Media based forgery
Karunya et al. [11]	Liveness detection	Fingerprint, Face and iris	Spoofing & image based forgery
Thavalengal [14]	Liveness detection based on multi spectral information	Iris	Presentation attacks
Huang et al. [15]	Pupil constriction	Iris	Media based forgery & cosmetic contact lens
Kanematsu et al. [16]	Liveness detection based on variation of brightness	Iris	Fake iris
Mhatre et al. [17]	Feature Extraction and Encryption Using Bio-Chaotic Algorithm (BCA)	Iris	Image feature encryption

REFERENCES

[1] M. Boatwright, & X. Luo, "What do we know about biometrics authentication?" In *Proceedings of the 4th Annual Conference on Information security curriculum development*, September 2007.

[2] S. Sheela & P. Vijaya, "Iris recognition methods-survey," *International Journal of Computer Applications*, 3(5), pp. 19-25, 2010.

[3] Li, Y., Li, Y., Yan, Q., Kong, H., & Deng, R. H. (2015, October). Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1558-1569).

[4] Pacut, A., & Czajka, A. (2006, October). Aliveness detection for iris biometrics. In Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology (pp. 122-129).

[5] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634.

[6] Andres Uhl, Yevonne Holler, Iris sensor Authentication using Camera PRNU Fingerprints. Proc. of 5th IARP International Conference on Biometric (ICB), 2012.

[7] Kathikeyan, T., & Sabarigiri, B. (2012, February). Countermeasures against iris spoofing and liveness detection using electroencephalogram (eeg). In 2012 International Conference on Computing, Communication and Applications (pp. 1-5).

[8] Komogortsev, O. V., & Karpov, A. (2013, June). Liveness detection via oculomotor plant characteristics: Attack of mechanical replicas. In 2013 International Conference on Biometrics (ICB) (pp. 1-8).

[9] Czajka, A. (2013, August). Database of iris printouts and its application: Development of liveness detection method for iris recognition. In Methods and Models in Automation and Robotics (MMAR), 2013 18th International Conference on (pp. 28-33).

[10] Dubey, R. K., Goh, J., & Thing, V. L. (2016). Fingerprint Liveness Detection From Single Image Using Low-Level Features and Shape Analysis. IEEE Transactions on Information Forensics and Security, 11(7), 1461-1475.

[11] Karunya, R., & Kumaresan, S. (2015, January). A study of liveness detection in fingerprint and iris recognition systems using image quality assessment. In Proc. of International Conference on Advanced Computing and Communication Systems, 2015 (pp. 1-5).

[12] Li, Y., Po, L. M., Xu, X., Feng, L., & Yuan, F. (2016, March). Face liveness detection and recognition using shearlet based feature descriptors. In 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 874-877).

[13] Menotti, D., Chiachia, G., Pinto, A., Schwartz, W. R., Pedrini, H., Falcao, A. X., & Rocha, A. (2015). Deep representations for iris, face, and fingerprint spoofing detection. IEEE Transactions on Information Forensics and Security, 10(4), pp. 864-879.

[14] Thavalengal, S., Nedelcu, T., Bigioi, P., & Corcoran, P. (2016). Iris liveness detection for next generation smartphones. IEEE Transactions on Consumer, Vol. 62, Issue 2, pp. 95-102.

[15] 15. Huang, X., Ti, C., Hou, Q. Z., Tokuta, A., & Yang, R. (2013, January). An experimental study of pupil constriction for liveness detection. Proc. of IEEE Workshop on Applications of Computer Vision (WACV), 2013, pp. 252-258.

[16] Kanematsu, M., Takano, H., & Nakamura, K. (2007, September). Highly reliable liveness detection method for iris recognition. In Society of Instrument and Control Engineers of JapanSICE, 2007 Annual Conference, pp. 361-364.

[17] Mhatre, R. M., & Bhardwaj, D. (2015, December). Classifying Iris Image Based on Feature Extraction and Encryption Using Bio-Chaotic Algorithm (BCA). In 2015 International Conference on Computational Intelligence and Communication Networks (CICN), pp. 1068-1073. IEEE.