IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

Master Face Attacks on Face Recognition Systems

Mr. Pradeep Nayak[1], Darshan S[2], Yashvardhan SG[3], Sudeep K[4], Finny Paul[5]
Assistant Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
Alvas's Institute of Engineering and Technology, Mijar, Moodbidre, Karnataka, India

Abstract: *Due to its simplicity, face authentication is currently more frequently used than authentication using a personal identification number or an unlock pattern, especially on mobile devices. This has made it a seductive target for attackers who use a demonstration assault. Traditional presentation attacks employ the victim's face or victim footage. The existence of master faces—faces that match numerous enrolled templates in face recognition systems—has been demonstrated in earlier research, and their presence increases the effectiveness of presentation attacks. In this article, we present the results of a thorough investigation of latent variable evolution (LVE), a technique frequently employed to produce master faces. To determine the characteristics of master faces, an LVE algorithm was used in a variety of settings and with many databases and/or face recognition systems.*

Keywords: Master face, wolf attack, face recognition system, latent variable evolution

REFERENCES

[1]. "The Goode Intelligence Biometric Survey 2021." Goode Intelligence. Apr. 2021. [Online]. Available:https://www.goodeintelligence.com/ report/the-goode-intelligence-biometric-survey-2021/
[2]. S. Bhattacharjee, A. Mohammadi, A. Anjos, and S. Marcel, "Recent advances in face presentation attack detection," in Handbook of Biometric Anti-Spoofing. Cham, Switzerland: Springer, 2019, pp. 207–228.
[3]. P. Bontrager, W. Lin, J. Togelius, and S. Risi, "Deep interactive evolution," in Proc. Int. Conf. Comput. Intell. Music Sound Art Des., 2018, pp. 267–282.
[4]. H. H. Nguyen, J. Yamagishi, I. Echizen, and S. Marcel, "Generating master faces for use in performing wolf attacks on face recognition systems," in Proc. IJCB, 2020, pp. 1–10.
[5]. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," IEEE Access, vol. 7, pp. 23012–23026, 2019.
[6]. P. Bontrager, A. Roy, J. Togelius, N. Memon, and A. Ross, "DeepMasterPrints: Generating MasterPrints for dictionary attacks via latent variable evolution," in Proc. BTAS, 2018, pp. 1–9.
[7]. M. Une, A. Otsuka, and H. Imai, "Wolf attack probability: A new security measure in biometric authentication systems," in Proc. ICB, 2007, pp. 396–406.
[8]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. CVPR, 2019, pp. 4690–4699.
[9]. D. P. Kingma and M. Welling, "Auto-encoding variational bayes," in Proc. ICLR, 2014.
[10]. I. Goodfellow et al., "Generative adversarial nets," in Proc. NIPS, 2014, pp. 2672–2680.