Exploring Attacks and Mitigation Strategies in Biometric Authentication Systems

Matin Fallahi

April 16, 2024

1 Background

Biometric technology refers to the use of unique physiological or behavioral characteristics to identify individuals. Common forms of biometric data include fingerprints, facial recognition, iris scans, and voice patterns. This technology is widely used for security and authentication purposes, as biometric identifiers are difficult to replicate or steal compared to traditional passwords or identification cards and do not require memorization. Its applications range from unlocking smartphones and laptops to enhancing security at airports and monitoring attendance in workplaces.

Attacks on biometric verification systems pose significant security risks. These attacks can be physical, such as creating fake fingerprints or masks to fool fingerprint and facial recognition systems, or digital, involving the manipulation of biometric data within the system's database. Spoofing attacks, where attackers mimic legitimate user biometrics, and tampering with biometric software to alter authentication outcomes are common strategies. As reliance on biometric technology increases, enhancing the security protocols to defend against these threats is critical.

2 Objective

The objective of this project is to explore the attack surface of biometric systems. We aim to investigate the potential consequences each type of attack could impose on various modalities and identify possible mitigation strategies to prevent these vulnerabilities. Additionally, we will implement several of these attacks and design experiments to compare their effects. This analysis will help in understanding the robustness of biometric systems and contribute to the development of more secure authentication technologies.

3 Related References

- Roberts C. Biometric. Attack Vectors and Defences. Computers & Security. 2007 Feb 1;26(1):14-25.
- Galbally J, McCool C, Fierrez J, Marcel S, Ortega-Garcia J. On the vulnerability of face verification systems to hill-climbing attacks. Pattern Recognition. 2010 Mar 1;43(3):1027-38.
- Wang X, Yan Z, Zhang R, Zhang P. Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications. 2021 Aug 15;188:103080.