Vibration-Aided Picture-Based Authentication System and Methods

US Patent 12,393,663

Dr. Faisal S. Alsubaei (University of Jeddah) and Dr. Abdullah Eid Abuhussein (St. Cloud State University, USA)

Introduction

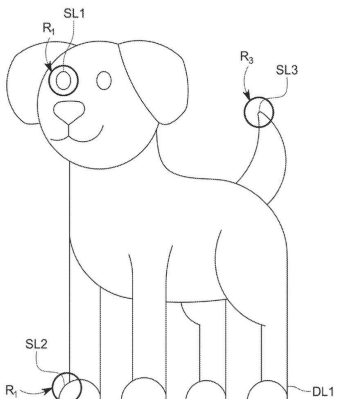
Traditional authentication methods such as text passwords and standard graphical passwords are vulnerable to shoulder-surfing attacks, especially in public environments. Many graphical authentication schemes also impose high cognitive load and perform poorly on small screens.
This project introduces a vibration-aided picture-based authentication system that enhances security by embedding covert haptic cues into the authentication process, making visual observation attacks ineffective.

Objectives

- Design a shoulder-surfing-resistant authentication mechanism for mobile devices.
- Integrate covert vibration cues into picture-based authentication.
- Randomize authentication challenges per session to prevent pattern learning.
- Ensure usability on commodity smartphones without auxiliary hardware.

Methods

The system uses a **client–server authentication approach** based on picture passwords enhanced with covert vibration cues. During registration, users select an image, define ordered secret touch points, choose deceiving points, and map vibration patterns to decoy taps. During login, the server generates a randomized sequence combining secret and deceiving points. The device vibrates only for deceiving points, while secret points are entered silently. Authentication is verified based on tap location and duration, and challenges are regenerated on failure.



SL = Secret Location
DL = "Deceiving Location
R = the Region around a secret location

Results and Discussion

Security Performance
- Strong resistance to shoulder-surfing attacks
- Observers could not distinguish secret taps from decoy taps
- Covert vibration cues successfully hid real password inputs

Usability Results
- High login success rate when vibration cues were followed correctly
- Smooth operation on small touchscreen devices
- No additional hardware required

Randomization Effect
- Decoy locations and vibration patterns changed every session
- Reduced hotspot formation and pattern learning
- Improved protection against repeated observation

Observed Limitations
- Errors mainly caused by incorrect tap duration
- Tight spatial tolerance increased user mistakes
- Indicates the need for device-specific calibration

Discussion Summary
- Tactile cues provide an effective non-visual authentication channel
- A balance between security and usability is essential

Conclusion

This project successfully designed and implemented a **vibration-aided picture-based authentication system** that mitigates shoulder-surfing without requiring auxiliary hardware. By shifting security cues from the visual channel to the tactile channel, the system conceals password patterns from observers while maintaining usability on commodity smartphones.
The solution enhances security through per-session randomization, covert haptic signaling, and flexible configuration of tap regions and durations. Despite limitations related to device vibration reliability and threshold calibration, the approach proves practical, scalable, and suitable for real-world mobile authentication scenarios.

References

1. F. S. Alsubaei and A. E. Abuhussein, *Vibration-Aided Picture-Based Authentication System and Method*, U.S. Patent 12,393,663 B1, Aug. 19, 2025.
2. G. E. Blonder, *Graphical Password*, U.S. Patent 5,559,961 A, Sep. 24, 1996.
3. A. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," 1998.
4. I. Jermyn et al., "The Design and Analysis of Graphical Passwords," *USENIX Security Symposium*, 1999.
5. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," 2000.
6. W. Luo et al., "Feel Vibration: Challenge-Response Mobile Authentication with Covert Channel," *ICCT*, 2020.

Acknowledgements

The inventor thanks the Ministry of Education and the University of Jeddah for their technical and financial Support.