Review of: "A Security Framework for the Mobile Application Using Color Barcode"

Guowen Xu[1]

1 Nanyang Technological University

This paper outlines the development of a QR code framework that enhances security through a secret key-secured system, using asymmetric key verification. Specifically, it utilizes SSH and server-based QR codes for website login, with the client-side storing an RSA private key to encrypt information via QR code verification. Unlike traditional methods, the QR codes in this system are two-dimensional images designed for encryption.

Then, mobile devices capture these QR codes and send a cryptographic response to the server for extensive verification. The system supports a color QR code that utilizes cyan, magenta, and yellow channels within the mobile app for encoding, and red, green, and blue channels for capturing the color image. This method embeds the quantized QR code into color images without causing visible distortions, thus maintaining high levels of imperceptibility, integrity, and security. Below are several minor concerns about this paper.

1. In Section 1, when discussing the conversion of 2D images to 1D electronic data, you should add proper citations to validate its feasibility. For instance:

Ni, Tao, Xiaokuan Zhang, and Qingchuan Zhao. "Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel." Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023.

Jiang, Qinhong, et al. "{GlitchHiker}: Uncovering Vulnerabilities of Image Signal Transmission with {IEMI}." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

2. In Section 2, you lack important citations about QR code-related authentications. For example:

An, Zhenlin, et al. "One tag, two codes: Identifying optical barcodes with NFC." Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021.

Pan, Hao, et al. "mqrcode: Secure QR code using nonlinearity of spatial frequency in light." The 25th Annual International Conference on Mobile Computing and Networking. 2019.

You should also discuss other authentication methods that prevent password cracking, such as

Cao, Hangcheng, et al. "HandKey: Knocking-triggered robust vibration signature for keyless unlocking." IEEE Transactions on Mobile Computing 23.1 (2022): 520-534.

Chen, Yongliang, et al. "SwipePass: Acoustic-based second-factor user authentication for smartphones." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 6.3 (2022): 1-25.

Jiang, Hongbo, et al. "SmileAuth: Using dental edge biometrics for user authentication on smartphones." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4.3 (2020): 1-24.

3. Figures should be clearer; please use the PDF format instead of jpg or png. For example, the text in Figure 1 and Figure 2 cannot be recognized.