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

Georgi Gary Rozenman

Potential competing interests: No potential competing interests to declare.

The paper by Rana Majumdar et al. proposes a novel framework for securing mobile applications using color QR codes, which incorporates asymmetric RSA encryption to enhance security during login processes. The authors have attempted to address the practical implications of QR code security and provide both theoretical and applied perspectives to support their framework. However, the manuscript suffers from several critical issues that need to be addressed before it can be considered for publication.

1. Please review and include the latest advancements in QKD and quantum computing such as:

    1. "Quantum computing: A taxonomy, systematic review and future directions." Software: Practice and Experience 52.1 (2022): 66-114.

2. "The quantum internet: A synergy of quantum information technologies and 6G networks." IET Quantum Communication 4.4 (2023): 147-166.

3. "Quantum cryptography—A simplified undergraduate experiment and simulation." Physics 4.1 (2022): 104-123.

4. "Archives of quantum computing: research progress and challenges." Archives of Computational Methods in Engineering 31.1 (2024): 73-91.

5. "Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges." Nature Communications 15.1 (2024): 2123.

2. **The figures included in the manuscript, particularly Figures 1, 2, and 3, appear overly simplistic and lack originality. The graphical representation does not add substantive value to the text and seems to be generic representations that could potentially be sourced from widely available resources. There is a concerning lack of originality which raises questions about potential plagiarism. I strongly recommend that the authors revise these figures to provide original, clear, and more informative visual representations that genuinely contribute to the understanding of the proposed framework.**

3. The content of the paper, especially the descriptive parts of the QR code technology and its application, closely mirrors general knowledge that can be found in basic tutorials and existing literature without sufficient transformation or unique contribution. The overlap is significant enough to suggest a review of the sources to ensure proper

attribution and to substantiate the claims of original research with more distinct analysis or data.

4. While the paper outlines a framework using color QR codes for enhanced security, it lacks depth in the technical validation of the security features proposed. The security analysis is superficial and does not adequately simulate or discuss potential real-world attack vectors in detail. More rigorous testing and a deeper security analysis are required to validate the claims made about the imperceptibility, integrity, and security of the QR codes developed.

5. The methodology section does not provide enough detail about the experimental setup or the statistical methods used for analyzing the performance of the proposed solution. This lack of detail makes it difficult to assess the robustness of the study and to reproduce the results. A more detailed explanation of the methods and the inclusion of comprehensive experimental results are necessary to substantiate the claims made.

Conclusion:

The paper presents an interesting approach to enhance mobile application security using color QR codes; however, it fails to meet the publication standards in its current form due to concerns over originality, depth of analysis, and methodological rigor. The figures need to be revised to ensure originality and enhance clarity, and a thorough check for potential plagiarism is imperative. Additional experimental details and a more comprehensive security analysis are required to demonstrate the efficacy and innovation of the proposed framework.