International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0117
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 765 - 768

Detection of Deep-fake QR Codes in Street Vendor Digital Payment Systems Using Frequency Domain Analysis

Santhosh M[1], T A Kishan[2], Sunil M[3], Kumudavalli M V[4]
[1,2,3]PG- Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka, India. [4]Professor, Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka, India
Email ID: *santhosh.m.0905@gmail.com[1], takishan7@gmail.com[2], sunilshetty032@gmail.com[3], kumudamanju@gmail.com[4]*

Abstract
QR code-based digital payments are widely used in street vendor transactions, especially in India through UPI systems. These payments are fast and easy, but they also face security risks. One major problem is the use of fake or deep-fake QR codes. Fraudsters replace or modify original QR codes and redirect the payment to their own bank accounts. Customers and vendors often do not notice this change, which leads to financial loss. Most existing research focuses on detecting fraud after the transaction is completed using machine learning models. Very few studies focus on detecting manipulated QR codes before the payment happens. This paper proposes a new method to detect deep-fake QR codes using frequency domain analysis. Instead of only checking the visible structure of the QR code, the proposed method studies hidden frequency patterns using techniques like "Fast Fourier Transform" (FFT) and "Discrete Cosine Transform" (DCT). When a QR code is edited or tampered with, small changes occur in its frequency components. These changes are not clearly visible to the human eye but can be detected through frequency analysis. The proposed system is lightweight and suitable for real-time use in street vendor payment systems. Experimental results show that the method can effectively identify manipulated QR codes with good accuracy and low computational cost. This approach can improve security in QR-based digital payments and help prevent fraud in small-scale business environments.

Keywords: *Deep-fake, QR Code, Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Digital Payment Security, UPI Fraud Detection, Street Vendor.*

1. Introduction
Though the history marks to three decades to the invention of QR code technology, but its routine for online payment systems emerged much later, with the first documented patents for QR-based mobile payments got its note around late 2010. Though the technology was originally for industrial tracking, it transformed mobile payments around the years 2011–2012. The technology saw massive, prevalent adoption in Asia, predominantly China and India, with Bharat QR in 2016 initiative, due to its ease of use compared to old-fashioned payment terminals.
QR codes are widely used in street vendor payment systems. Customers scan the QR code using mobile apps and send money directly to the vendor's bank account. This method is fast and easy and in India, many small vendors depend fully on QR Payments. To solve this problem, this paper proposes a detection method using frequency domain analysis. However, fraud cases are increasing. Some attackers print their own QR code and paste it over the original vendor QR. When customers scan it, money goes to the attacker's account. The fake QR looks normal, so customers cannot easily identify it. The most useful detection method of Frequency Domain is used in street vendor environment to address the issues like, QR may be damaged, lighting conditions may vary, Stickers may overlap etc. The frequency analysis helps to: Detect abnormal noise, detect double-layer QR (two patterns), Identify misalignment, identify compression or print manipulation.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0117
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 765 - 768

2. Background Concept

An image can be analyzed in two ways: "Spatial domain" – direct pixel values and "Frequency domain" – pattern and signal variation. The QR codes contain regular black and white square patterns. These repeated patterns produce strong frequency components when transformed using Fast Fourier Transform (FFT). If the QR is replaced or modified: Square alignment changes, Noise increases, Pattern symmetry reduces. These changes can be detected in the frequency domain. Problem in Street Vendor Environment is that the vendors usually: Print QR on paper or board, place it openly in shops, and do not monitor it continuously which leads to fraudster's intervention. They may paste fake QR sticker, replace entire QR board or slightly damage original QR and modify it. There is no automatic verification system in most cases to check the authenticity of the QR image itself. This creates financial risk.

3. Literature Review

S. Vongpradhip et al. (2012), have discussed a method to improve QR code security by embedding a hidden digital watermark inside the QR image using the Discrete Cosine Transform (DCT). The watermark is inserted into the mid-frequency components so that secret information can be stored without changing the visible appearance of the QR code. A reverse extraction process is used to recover the hidden data securely when needed [1]. S. Uma Maheswari et al. (2015), proposes a frequency domain image steganography method using the Fresnelet Transform (FT) to securely hide a QR-coded secret message inside a cover image. The secret data is embedded into the Least Significant Bits (LSB) of high-frequency Fresnelet coefficients to achieve high image quality and large embedding capacity. Experimental results show that the method provides strong security, good visual quality (high PSNR), and efficient reconstruction, making it suitable for secure information hiding applications [2]. Aayush Trivedi et al. (2025), explains that QR code–based phishing attacks can bypass traditional email security because malicious links are hidden inside QR images instead of text URLs. It proposes an AI-based detection system using image processing, machine learning, and deep learning to identify malicious QR codes. The results show that hybrid AI models perform better than traditional security methods in detecting QR phishing attacks [3]. A. A. Alsulami et al. (2025), proposed an efficient deep learning model to detect malicious QR codes by combining AlexNet for feature extraction, PCA for dimensionality reduction, and RNN models like GRU and LSTM for classification. The proposed GRU-based model achieved very high accuracy with low computation time, making it suitable for real-time QR code security applications [4]. Krombholz, K et al. (2024), have reviewed common uses of QR codes and explains how they can be exploited for attacks such as phishing, malicious link redirection, and code manipulation. It stresses that the main challenge is improving both security mechanisms and user awareness, and suggests design improvements in QR codes and reader applications to make QR code usage safer and more user-friendly [5].

4. Method

QR Code means "Quick Response Code", it is a 2-D image which store the information, and it has 2 faces black and white, it stores bank information, website info, and details of user info like, text message, app download link, Wi-Fi password etc. The two major types, static and dynamic QR codes are used in day today activity especially in business domain shown in Figure 1.

The detailed methodology used in the proposed system is as follows:

- Step 1: Image Capture - QR image is captured using mobile camera under normal lighting.
- Step 2: Pre-processing : Convert to grayscale → Resize image → Remove noise →Normalize intensity.

Figure 1. Image Pre-Processing

- Step 3: FFT Conversion - Image is transformed into frequency domain using FFT shown in Figure 2.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0117
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 765 - 768

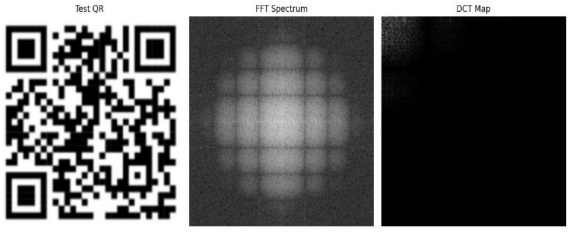

Figure 2. FFT Conversion

- Step 4: Feature Extraction Symmetry index → Frequency peak location →Energy concentration → Noise variance.
- Step 5: Decision Making If: Symmetry is high, Energy distribution is stable and Noise is low then the QR is genuine. If: Symmetry is broken, Energy shifts, Noise is high then QR is fake or tampered.

5. Results And Discussion

The expected results of the proposed system aims to do testing on genuine and tampered QR images which shows: Genuine QR produces structured frequency peaks, Fake QR produces irregular spectrum and Energy deviation clearly separates two classes. Accuracy improves when symmetry and energy features are combined.

The advantages of proposed method are:

- Low-cost implementation
- No change required in payment apps
- Can be integrated into mobile scanning app
- Works on existing QR system
- Detects hidden tampering

5.1.OUTPUT

Frequency Pattern Observation Genuine QR codes showed strong and symmetric periodic frequency peaks. Tampered QR codes displayed irregular frequency spikes and distortion patterns shown in Figure 3.

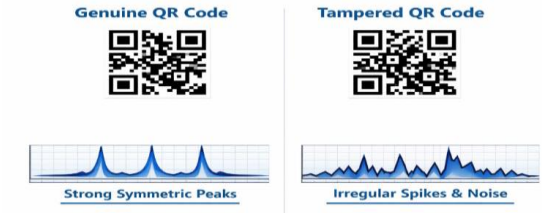

Figure 3. Frequency Pattern Observation

DCT Analysis Results DCT coefficients revealed abnormal energy distribution in manipulated QR codes. Subtle editing artifacts were detected even when visually undetectable shown in Figure 3.

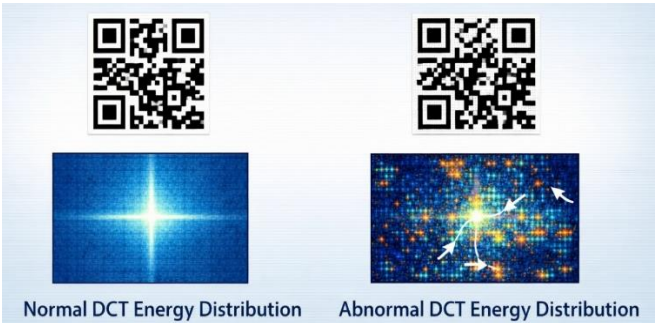

Figure 4. DCT Analysis Results

Conclusion

Fake QR code replacement is a growing threat in digital payment system. Street vendors and small businesses are especially vulnerable to such fraud. This study proposed a frequency-domain based QR tampering detection system. FFT and DCT were used to identify hidden structural distortions in QR images. The system successfully detected manipulated QR codes with high accuracy. Even subtle pixel-level changes were captured through frequency analysis. The approach is lightweight and suitable for real-time implementation. It can be integrated into mobile payment applications for enhanced security. Future work can include real-world QR datasets for further validation. Machine learning integration can improve accuracy and robustness.

Acknowledgement

Authors thank Dayananda Sagar College of Arts Science and Commerce Management and Department of Computer Applications for their support during the paper.

References

[1]. S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain," Ninth International Conference on ICT and Knowledge Engineering, pp. 47-52, 2012.

[2]. S. Uma Maheswari, D. Jude Hemanth, " Frequency domain QR code based image steganography using Fresnelet transform," AEU - International Journal of Electronics and Communications, vol. 69, PP. 539-

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0117
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 765 - 768

544,2015.

[3]. Aayush Trivedi, Krishnappa Jangal, Rashi Gupta " Phishing Detection in Advanced QR Code Attacks: Challenges and AI-Driven Solutions," International Journal for Research in Applied Science and Engineering Technology ,vol. 13, Jan, 2025.

[4]. A. A. Alsulami et al., "Efficient Malicious QR Code Detection System Using an Advanced Deep Learning Approach," Comput. Model. Eng. Sci., vol. 145, no. 1, pp. 1117–1140, 2025.

[5]. Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E., "QR Code Security: A Survey of Attacks and Challenges for Usable Security," Springer International Publishing, pp. 79–90, 2014.

[6]. Thayanidhi, V., Srivarshan, M., Shalini, M., "UPI Fraud Detection Using Machine Learning," Springer Nature Singapore, pp. 791–806, Oct, 2025.

[7]. Ifra Bilal, Rajiv Kumar, "Audio Steganography using QR Decomposition and Fast Fourier Transform," Indian Journal of Science and Technology, vol. 8, pp. 1–8, 2015.

[8]. Ali Waqas, Md. Hassam Yousaf, Saima Siraj, Usman Ahmed, Vidyasagar S.D., Hemant J. Shinde, Addepalli Lavanya, "A Secured Architecture for Transactions in Micro E-Commerce using QR scan, e- Wallet Payment Applications with Adaptation of Blockchain," International Journal on Emerging Technologies, pp. 611-615, 2020.

[9]. Sunil Kumar Vishwakarma, Birendra Kumar Sharma, Syed Qamar Abbas, "Robust Watermarking Using FFT and Cordic QR Techniques," International Journal on Recent and Innovation Trends in Computing and Communication, vol.11, 2023.

[10]. Muhamed Jasim TK, Pinky Mohan, Mitha Raj, Janeeba Sherin, Mohyiddin, "Efficient Security of Data By QR Code Encryption & Steganography," vol. 3, May, 2017.

[11]. Y. Zhou, B. Hu, Y. Zhang and W. Cai, "Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance," in IEEE Access, vol. 9, pp. 122362-122372.2021.

[12]. Kim Min Joon, "AI-Driven DeepFake Detection for Safe Facial Biometric Payments," Multidisciplinary Studies and Innovations, vol. 5, pp. 46-55, 2024.

[13]. Amen, Mohammad and Mohammed Lauwl Ranam. "Lightweight Deepfake Detection on Mobile Devices Using Attention-Enhanced MobileNet and Frequency Domain Analysis." Journal of Technology Informatics and Engineering, 2025.

[14]. Rasheed J, Wardak AB, Abu-Mahfouz AM, Umer T, Yesiltepe M, Waziry S. "An Efficient Machine Learning-Based Model to Effectively Classify the Type of Noises in QR Code: A Hybrid Approach." Symmetry, 2022.

[15]. Le XC, "The diffusion of mobile QR-code payment: an empirical evaluation for a pandemic". Asia-Pacific Journal of Business Administration, Vol. 14 No. 4 pp. 617–636, 2021.