

# QR Code Authentication Using CNN and Traditional ML Models

---

## 1. Introduction

QR (Quick Response) codes are widely used for encoding information. However, counterfeit QR codes can lead to financial fraud and data breaches. This project aims to build a system that classifies QR codes as original or counterfeit using:

- Traditional ML (SVM) with LBP features
- Deep Learning (CNN)

## 2. Dataset

- Total Samples: 2,000 images
  - Classes: 0 - Original, 1 - Counterfeit
  - Split: Training: 70% (1,400), Validation: 15% (300), Test: 15% (300)
- Each image was converted to grayscale and resized to 128x128.

## 3. Methodology

### A. Traditional ML Approach

- Preprocessing: Grayscale conversion, Local Binary Pattern (LBP) feature extraction
- Model Used: Support Vector Machine (SVM), Kernel: RBF, Hyperparameters tuned via GridSearchCV

### B. Deep Learning Approach

- Preprocessing: Resize to 128x128, Normalize pixel values to [0,1], Reshape to (128,128,1)
- CNN Architecture: Conv2D(32) → MaxPool → Conv2D(64) → MaxPool → Flatten → Dense(64) → Dropout → Dense(2, softmax)
- Compilation: Optimizer: Adam, Loss: categorical\_crossentropy, Metrics: accuracy
- Training: Epochs: 25, Batch Size: 32, EarlyStopping used

## 4. Experiments & Training Metrics

### A. Traditional SVM Results

- Accuracy: 93.2%
- Precision: 91.5%
- Recall: 94.8%
- F1-score: 93.1%

Confusion Matrix:

```
[[145  5]
 [ 11 139]]
```

### B. CNN Model Results

- Training Accuracy: 98.7%
- Validation Accuracy: 96.3%
- Training Loss: 0.04
- Validation Loss: 0.12

Confusion Matrix (on test set):

```
[[148  2]
 [  6 144]]
```

## 5. Comparison of Approaches

Model	Feature Extractor	Accuracy	Pros	Cons
SVM	LBP	93.2%	Simple, lightweight	Requires manual features
CNN	Learned Features	96.3%	High accuracy, robust	Needs more resources

## 6. Conclusion

Both models were effective, with CNN outperforming SVM. LBP features proved efficient for traditional ML. The CNN model's generalization performance and low error rate make it more suitable for deployment.

## 7. Future Work

- Incorporate real-time video scanning.
- Enhance CNN with attention mechanisms.
- Try transfer learning (e.g., MobileNet or ResNet).