Fingerprint Spoof Detector Based on Local Binary Patterns

Chakradhar Reddy Donuri
Graduate Student, Dept of EECS, Wichita State University
Wichita, Kansas, United States of America
email: cxdonuri@shockers.wichita.edu

Abstract - Fake fingers can be easily fabricated using commonly available materials, such as latex, silicone and gelatin, with the fingerprint ridges of an individual engraved on it. These fake fingers can then be used by an adversary to launch a spoof attack by placing them on a fingerprint sensor and claiming the identity of another individual. The success rate of such spoof attacks can be up to 70%. Fingerprint spoof detection algorithms have been proposed as a counter measure against spoof attacks. A fingerprint spoof detector is a pattern classifier that is used to distinguish a live finger from a fake (spoof) one in the context of an automated fingerprint recognition system. Most liveness detectors are learning-based and rely on a set of training images

Aim: To develop a two-class fingerprint spoof detector that uses Local Binary Patterns (LBP) features along with Support Vector Machines (SVM) to distinguish live fingerprints images from spoof samples.

I. INTRODUCTION

Local Binary Patterns (LBP) is a feature extraction method normally used for texture descriptors. The LBP operator assigns a label to every pixel of an image by thresholding the 3x3-neighborhood of each pixel with the center pixel value and considering the result as a binary string, which is then represented as an 8-bit integer. The operator can also be extended to use neighborhoods of different sizes. A rotation invariant LBP version was proposed in which combines equivalent codes into 10 unique codes called uniform coding. After performing the LBP filtering, the normalized histogram is used as the feature vector. The LBP filtered images are equally divided in rectangles and their histograms are concatenated to form a final feature vector. SVM is a supervised machine learning algorithm which can be used for classification or regression problems. It uses a technique called the kernel trick to transform your data and then based on these transformations it finds an optimal boundary between the possible outputs.

II. PROCEDURE

1. Collecting data set for training and testing of live and Fake finger print samples.

2. First, the extraction of Local Binary Patterns (LBP) features from the training image samples and storing them in a list with the corresponding true value as their labels by iterating throughout the training dataset.

3: Now, training the Support Vector Machines (SVM) or in this case the Linear Support Vector Classifier (SVC) to generate a classifier model.

4. Now, obtain the best fit hyperplane that divides or categorizes the data from the trained Linear SVC model.

5. Again, repeat Step 2, but now on the testing image samples and storing the resulting true values in a new list.

6: Predicting the images in the testing dataset and storing them in another list with the corresponding predicted value as their labels by iterating through the testing dataset.

7. Generating the confusion matrix by using the lists obtained from step 5 and Step 6, with the positive and negative labels as “Live” and “Fake” respectively.

8. Calculating the Precision, Recall and Accuracy of the Linear SVC model used for the spoof detection, with the values obtained from the confusion matrix in Step 7.

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = 2 \cdot \frac{precision \cdot recall}{precision + recall}$$

TP = True positive

TN = True negative

FP = False positive

FN = False negative

III. RESULTS

Precision: 0.9027
Recall : 0.8055
Accuracy :0.8510