JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FINGERPRINT LIVENESS AND SPOOF DETECTION

SHAIK NASREEN[1] & P. VAISHNAVI RAJEEV[2]

[1]PG Scholar, Department of CSE, B.I.T Institute of Technology, Hindupur, Andhra Pradesh, India.
[2]Assistant Professor, Department of CSE, B.I.T Institute of Technology, Hindupur, Andhra Pradesh, India.

Abstract:

Biometric recognition is nowadays a mature technology with several applications. However, biometric systems based on fingerprint are vulnerable to direct attacks consisting on the presentation of a fake fingerprint to the sensor. This work focuses on fingerprint liveness detection methods as an attempt to overcome that vulnerability. Two methods from the state-of-the-art in iris liveness detection were tested with fingerprint databases containing different kinds of fake samples. One aim of the work was to investigate how these iris techniques would perform with fingerprint fake samples.
The other purpose was to diversify the classification scenario by broaden the classification task from being made within each type of samples to being made in sets mixing the types of fake samples.
.

Keywords: live behavior, Pose prediction, Yawn prediction

1. INTRODUCTION

The basic aim of biometrics is to automatically discriminate subjects in a reliable manner for a target application-based ozone or more signals derived from physical or behavioral traits, such as fingerprint, face, iris, voice, palm, or handwritten sign-nature. Biometric technology presents several advantages over classical security methods based on either information (PIN, Password, etc.) or physical devices (key, card, etc.) .

However, providing to the sensor a fake physical biometric can be an easy way to overtake the systems security. Fingerprints can be easily spoofed from common materials, such as gelatin, silicone, and wood glue. Therefore, a safe fingerprint system must correctly distinguish a spoof from an authentic finger. Different fingerprint liveness detection algorithms have been proposed and they can be broadly divided into two approaches: hardware and software.

In the hardware approach, a specific device is added to the sensor to detect properties of a living trait such as blood pressure, skin distortion ,or odor. In the software approach, which is used in this study, ace traits are detected once the sample has been acquired with standard sensor. The features used to distinguish between real and fakeness are extracted from the image of the fingerprint. There are techniques such as those in which the features used in the classifier are based on specific fingerprint measurements, such as ridge strength, continuity, and clarity. In contrast, some works use general feature extractors such as Weber Local Descriptor (WLD), which is a texture descriptor composed of differential excitation and orientation components. A new local descriptor that uses local amplitude contrast (spatial domain) and phase (frequency domain) to form a bi-dimensional contrast-phase histogram was proposed in.

1.2 OBJECTIVE

The Liveness Detection Competition of years 2009, 2011 and 2013, which comprise almost 50,000 real and fake fingerprints images. We compare four different models: two CNNs pre-trained on natural image sand fine-tuned with the fingerprint images, CNN with random weights, and a classical Local Binary Pattern approach. We show that pre-trained CNNs can yield state-of-the-art results with no need for architecture or hyperparameter selection. Dataset Augmentation is used to increase the classifiers performance, not only for deep architectures but also for shallow ones. We also report good accuracy on very small training sets (400 samples) using these large pre-trained networks. Our best model achieves an overall rate of 97.1% of correctly classified samples - a relative improvement of 16% in test error when compared with the best previously published results.

This model won the first prize in the Fingerprint Liveness Detection Competition (LivDet) 2015 within overall accuracy of 95.5%.

.

2. OVERVIEW OF THE SYSTEM

2.1 Existing System:

Because of the epidemic, teaching in schools is not possible when different video consultation methods were used to educate students. Education is good for students, because it has the power to change society and these students will be the future of the country. Thus, the ITC has contributed to new educational reforms such as introducing various self-sustaining agents in teacher-student interactions. The main idea of study was to determine the influence on students about learning using the visual tools mentioned above. Nowadays situation is like, with the improvement of a portable platform, such as a smart phones and pads, the E-Learning model has been rapidly evolved online and improve learning. There are many students who take these classes lightly and think they cannot be punished, because of their negligence and thus they get low marks.

Thanks to this center parents face problems in keeping students or their children in control.

2.1.1 Disadvantages of Existing System

Some fingerprint recognition techniques use correlation-based methods to directly compare images but most of the fingerprint recognition and classification algorithms employ a feature extraction stage. Also, some pre-processing, segmentation and enhancement steps are often per-formed but accuracy of those methods is less.

2.2 Proposed System

Deep networks designed and trained for the task of object recognition can be used to achieve state-of-the-art accuracy in fingerprint liveness detection. No specific hand-engineered technique for the task of fingerprint liveness detection was used. Thus, we provide another success case of transfer learning for deep learning techniques. Pre-trained Deep networks require less labeled data to achieve good accuracy in a new task.

CNN and SVM algorithms are used to train model and compare accuracy of each model. Better performed model is used for prediction of fingerprint.

2.2.1 Advantages of the Proposed System

This method is used to analyses the important degree of packet vectors to obtainfine-grained features which are more salient for malicious traffic detection.

At the output layer, the features generated by attention mechanism are then imported into a fully connected layer for feature fusion, which obtains the key features that accurately characterize network traffic behaviours.

3. ARCHITECTURE

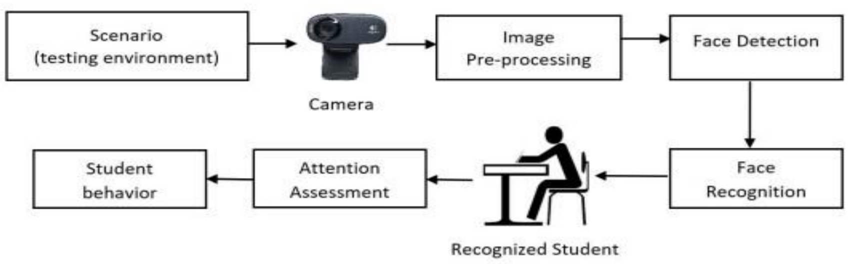


Fig: Architecture diagram

4. SYSTEM DESIGN

Data Collection

The methods were tested in two subsets of the fingerprint datasets made available for the LivDet2013 competition. The images of these datasets were acquired with four different sensors: Biometrical, Crossmatch, Ital-data and Swipe and the fake samples were built using seven different ma-trials: Body Double, Latex, Play-Doh, Wood Glue, Gelatin, Silicon endonasal. For more details on these sets see [2]. The subsets tested for this work were Biometrical and Swipe . This choice was made based on previous results in which Biometrical and Swipe performed better for wLBPand GLCM methods, respectively. Biometrical subsets comprise 2000 real samples and 400 samples for each material. For building the fake samples of Biometrical the materials used were: Ecoflex, Gelatine, Latex, Modasiland Wood Glue. Swipe subsets comprise 2374 real samples and approximately 500 samples for each material. For the fake samples of Swipe, the materials used were Latex, Wood Glue, Body Double and Play- Doh.

Pre-Processing

The feature extraction was performed using the two methods, wLBPand GLCM (see section 2) in the whole image. For the classification task we used Support Vector Machines (SVM), with a polynomial kernel, and for optimizing the parameters a "grid- search" was performed on C and d parameters: the exponential growth of C = 2 N was tested, with N varying from − 1 to 15 and the polynomial degree (d) was tested with the following values { 1 , 2 , 3 , 4 , 5 } . We also used crossvalidation so that the data was divided randomly in 62 . 5% of the samples for training and37 . 5% for testing. Two different classification scenarios were studied: within each material (Method 1) and using a mix of all materials (Method2 -"mixed sets"). In methods 1 and 2, the classification error was obtained by averaging the error in 50 runs and in each run the data was divided randomly in 62. 5% of the samples for training and 37. 5% for testing.

Train-Test Split and Model Fitting

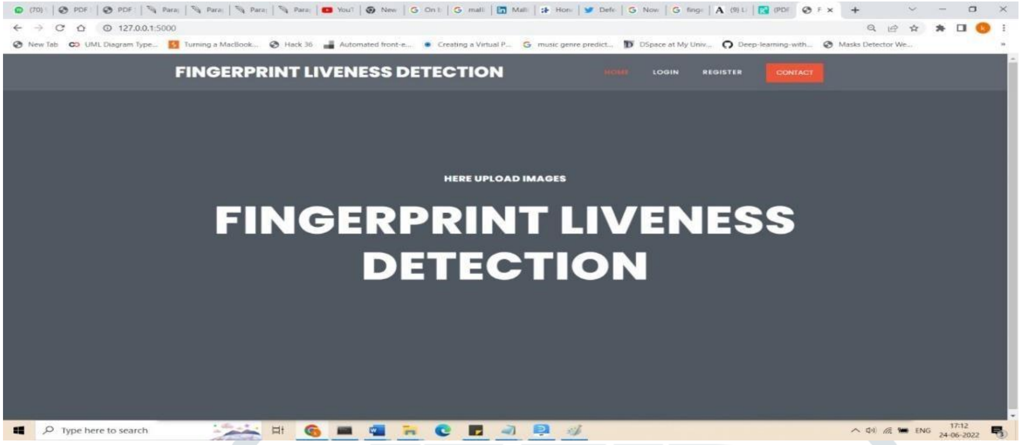
Now, we divide our dataset into training and testing data. Our objective for doing this split is to assess the performance of our model on unseen data and to determine how well our model has generalized on training data. This is followed by a model fitting which is an essential step in the model building process.

Model Evaluation and Predictions

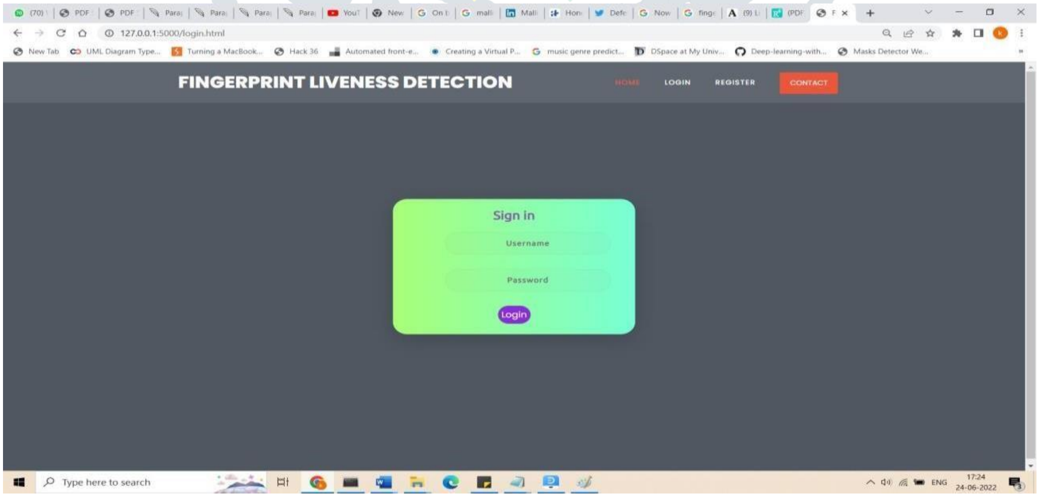
This is the final step, in which we assess how well our model has performed on testing data using certain scoring metrics, I have used 'accuracy score' to evaluate my model. First, we create a model instance, this is followed by fitting the training data on the model using a fit method and then we will use the predict method to make predictions on x_test or the testing data, these predictions will be stored in a variable called y_test_hat. For model evaluation, we will feed the y_test and y_test_hat into the accuracy_score function and store it in a variable called test_accuracy, a variable that will hold the testing accuracy of our model. We followed these steps for a variety of classification algorithm models and obtained corresponding test accuracy scores.

5. RESULTS SCREEN SHOTS

HOME SCREEN



UPLOAD IMAGES



VIEW UPLOADED IMAGES

PREDICTED RESULT

6. CONCLUSION

In this work, two methods for iris liveness detection were applied in fin-reprint images. ComparingourresultswiththeonesfromLivDet2013[2]we may consider our results encouraging of further investigation since income cases the results outperform those. Regarding the two different classification scenarios, we concluded that the results worsened when we go from training and testing within the same fake samples to mixing all the materials (but fixing the sensor). This is not unexpected since the vari-ability in the types of fake samples is expected to increase the difficulty the classification task. This finding leads us to think that the traditional approach we find in the literature is a somehow optimist. As future work we intend to broad this study to more datasets for fingerprint liveness de-taction and possibly compare these methods with state-of-the-art methods in this field.

In this project CNN and SVM algorithms are used to train model and accuracy of each model is predicted and CNN with higher accuracy is used for prediction purpose.

7. REFERENCES

[1] Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega-Garcia. Qual-ity measures in biometric systems. IEEE Security & Privacy, 10(6):52–62,2012.

[2] Luca Ghiani, David Yambay, Valerio Mura, Simona Tocco, Gian Luca Mar-cialis, Fabio Roli, and Stephanie Schuckers. Livdet 2013 fingerprint livenessdetection competition. In Int. Conf. on Biometrics (ICB), pages 1–6, 2013.

[3] R.M. Haralick, K. Shanmugam, and I. Dinstein. Textural features for imageclassification. In IEEE TSMC , volume SMC-3, no. 6, pages 610 – 621, 1973.

[4] David G Lowe. Object recognition from local scale-invariant features. In 7th IEEE Int. Conf. on Comp. Vis., volume 2, pages 1150–1157, 1999.

[5] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. Handbook of fingerprint recognition. Springer, 2009.

[6] Marie Sandström. Liveness detection in fingerprint recognition systems.2004.

[7] Ton Van der Putte and Jeroen Keuning. Biometrical fingerprint recognition:don’t get your fingers burned. In Smart Card Research and Advanced Applications, pages 289–303. Springer, 2000.