Fingerprint Liveness Detection using Moment Features

Vijaylaxmi S Patil[1] S A Angadi[2]
[1]Student [2]Head of Dept.
[1,2]Department of Computer Science & Engineering
[1,2]VTU Belagavi, India 590018

Abstract— In this paper, Fingerprint liveness detection technique is proposed using moment features like Zernike moment, central moment and Daubechies wavelet analysis. Now a day's production of fake fingerprints has become more common due to advancement in technology and thus it is necessary to detect the type of fingerprint during the identification of person. Here the datasets are collected from LivDet competition 2011 and 2013. A dataset of 50 spoof and 50 live images was used for experiment. Half of these were divided into training and testing images. A probabilistic neural network is classifier implemented. The proposed method has accuracy of 90%.

Key words: Fingerprint Liveness, Daubechies Wavelet Analysis, Moment Features, Probabilistic Neural Network

I. INTRODUCTION

Identification of person has become more important in recent days. In today's security field authentication using Biometric Systems are getting more interest. Each individual has their own unique features, which can be advantage to biometric systems. There are different biometric schemes like Voice, Face, Iris, Fingerprint etc. But the most emerging scheme is a fingerprint authentication as they do not change over a time and no two fingerprints are identical. Each fingerprint has its own identity. In Password based systems, the passwords can be visually seen and remembered easily. Fingerprints are simple and copying them is also a difficult task. Also they cannot be remembered easily.

The technology is growing day by day and now with this advanced technique one can produce spoof fingerprints and fool the biometric systems. Thus it is necessary for the authentication system to differentiate between the Live Fingerprint and Spoofed Fingerprint.

Now a day in most of the fields they prefer fingerprint security systems, which is easy for attackers. From several years Fingerprint Liveness Detection has become interesting topic in research. Both Software and Hardware methods can be developed to find a solution to this problem.

A. Objective

Fingerprint liveness detection system aims to find the fingerprint type when provided with test fingerprint. Firstly the publicly available dataset containing both live and fake fingerprints is collected, in which half is used for training and the next half for testing or to measure the performance of the system. Next the DWT along with Daubechies wavelet is used to extract features from training dataset, later used to train the PNN classifier. Finally the trained PNN model identifies the fingerprint type under testing phase.

In this paper experiments are carried out on fingerprint images collected from publicly available datasets of LiveDet Competition 2011 and 2013. The training dataset contains 25 live and 25 spoof images and testing data also contains 25 live and 25 spoof images. The accuracy of this data on the system proposed is 90%.

The rest of the paper is organized into four sections. In section II, we review some methods proposed in the field of fingerprint liveness detection. In section III, we describe our proposed method using moment features. In section IV, an extensive experiment is conducted and the results are given. Finally, we draw the conclusion and give future work in section V.

II. RELATED WORK

This section contains the literature in the field of software based fingerprint liveness detection. These methods extract intrinsic properties directly from the fingerprint images which are acquired by the sensor. Recent experiments, reported in the third edition of Fingerprint Liveness Detection competition (LivDet 2013), have clearly shown that fingerprint liveness detection is a very difficult and challenging task.

In one of the method a novel fingerprint liveness descriptor named "BSIF" is described, which, similarly to Local Binary Pattern and Local Phase Quantization-based representations, encodes the local fingerprint texture on a feature vector.

The Pore-based method uses 2 adaptive Gaussian Filters, one to strengthen the pores and valleys and second one to strengthen the only valley of the fingerprint image. Converts these two images to binary and subtract to obtain pore information. Now removes any spurious pores if available. Calculates pore density and depending on threshold density discriminates between the real and fake fingerprint.

One more method using CNN features of random sample patches first performs a segmentation of fingerprint area. Segmented area is rotated in 5º increments in the range -30º to +30º.130 patches are generated from a single image. Locations of patches are determined through normal distributions of segmented areas of the fingerprint image. The extracted patches are learned through CNN. It results in convolution images called feature maps. Patches are labeled. Now for the test image 11 patches are extracted using normal distribution on the segmented image. The trained CNN model is used to decide the label of fingerprint image. A voting strategy is used to decide the label of the fingerprint image. Depending on the number of types of patches the system classifies the input image. For example if the number of fake patches are greater than that of real patches, the test fingerprint image is classified as fake fingerprint.

Later static software approach was proposed to combine low-level gradient features from speeded-up robust features, pyramid extension of the histograms of oriented gradient and texture features from Gabor wavelet using dynamic score level integration. These features were extracted from a single fingerprint image to overcome the

issues faced in dynamic software approaches, which require user cooperation and longer computational time.

The approach using Multi-Scale LPQ and PCA selects a particular image applies a two-dimensional wavelet transform to obtain the same frequency coefficients together. Coefficients four directions are approximation, horizontal, vertical and diagonal are gained. Before constructing feature vectors, normalization is performed to unify data from different sensors. Next features of different co-efficient are extracted to through multi-scale Local Phase Quantity. Principal Component Analysis (PCA) is used to remove redundant information and reduce the dimensionality of feature vector. Finally Support Vector Machine (SVM) is adopted to construct a training model. The optimal dimensionality feature vectors are fed to the trained model (SVM), a two-class classifier. It reports the test fingerprint is real or fake.

These surveys indicate that there is an area where we can improve the method to detect the liveness of fingerprint. The proposed method can be used to avoid the access of unauthorized person or any other intruder .This proposed method takes advantage of various developed methods discussed above. Implements DWT for feature extraction and PNN classifier.

III. PROPOSED METHOD

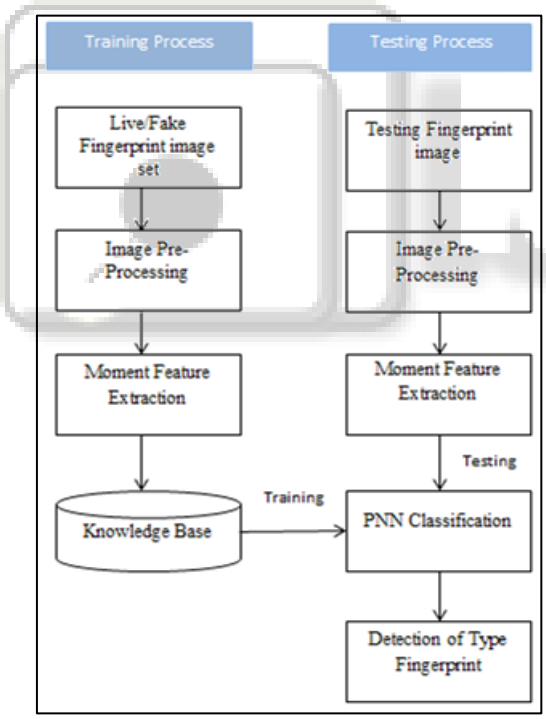


Fig. 1: Block Diagram

A. *Data Acquisition*

In this step we are collecting fingerprint images of both live and fake fingers, instead of capturing them as it is a software based method. In this approach experiments are conducted on publicly available fingerprint datasets from University of Cagliari, Department of Electrical and Electronic Engineering and Clarkson University, Department of Electrical and Computer Engineering.

1) Image Preprocessing

After collecting fingerprint images we pre-process the image by converting the original image into grey scale then to binary image, which is then subjected to background elimination and image, will be displayed to the user. Finally the original image is also subjected to background elimination and is then displayed to the user.

2) Image Enhancement

Image enhancement is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interest in an image. To enhance the image further Histogram equalization (HE) is applied.

Here block diagram depicts two sections those are Training and Testing phases.

3) Region of Interest of Image

Although HE method preserves the input brightness on the output image with a significant contrast enhancement, they may produce images with area that is not useful. To solve this Region of interest is found by finding the center of fingerprint image and all other four ends, using which the image is cropped.

4) Feature Extraction

The Cropped image with region of interest is used to extract the moment features of fingerprint. Daubechies wavelet is used to perform wavelet analysis.

Fig. 2: Wavelet Analysis

5) Training

Once we have the extracted features with us we then make use of Probabilistic neural Network to train the system.

6) Classification

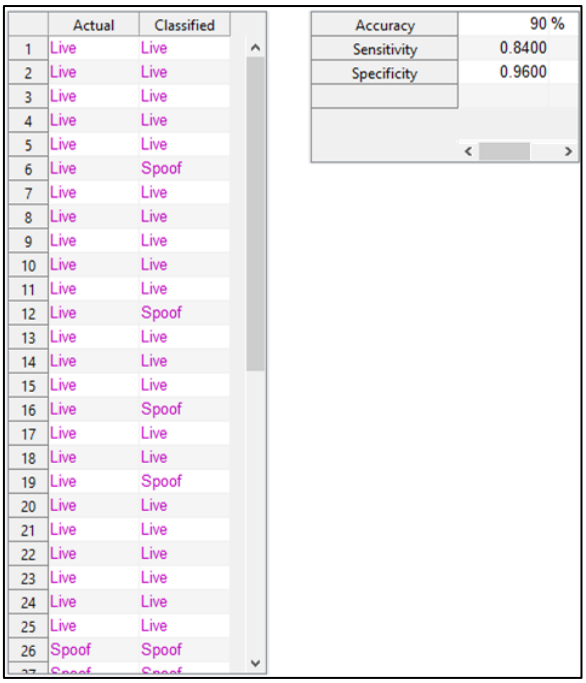
Probabilistic Neural Network is a classification technique used in this method. Here the result will be displayed to the user regarding the type of the Fingerprint.

IV. RESULTS

In this section, we evaluate our method for fingerprint liveness detection. Experiments were carried out on publicly available fingerprint liveness database for LivDet 2011 and 2013 competitions from Clarkson University - University of Cagliari.

The figure 3 depicts the performance of the system implemented. It performs testing on 25 live and 25 spoof images and has accuracy of 90%.

ROC curve is a graphical plot that represents the demonstrative capacity of a parallel classifier framework. It is constructed by plotting of the genuine positive rate (Sensitivity) against the false positive rate (Specificity). The curve generated by proposed method is above 45º diagonal indicating the accuracy of test is good is shown in fig 4.



	Actual	Classified
1	Live	Live
2	Live	Live
3	Live	Live
4	Live	Live
5	Live	Live
6	Live	Spoof
7	Live	Live
8	Live	Live
9	Live	Live
10	Live	Live
11	Live	Live
12	Live	Spoof
13	Live	Live
14	Live	Live
15	Live	Live
16	Live	Spoof
17	Live	Live
18	Live	Live
19	Live	Spoof
20	Live	Live
21	Live	Live
22	Live	Live
23	Live	Live
24	Live	Live
25	Live	Live
26	Spoof	Spoof

Accuracy	90 %
Sensitivity	0.8400
Specificity	0.9600

Fig. 3: Performance Analysis Results

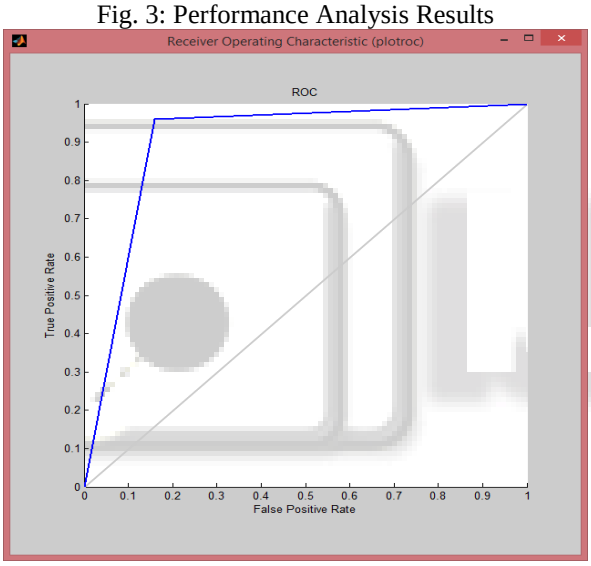


Fig. 4: Receiver Operating Characteristic Curve

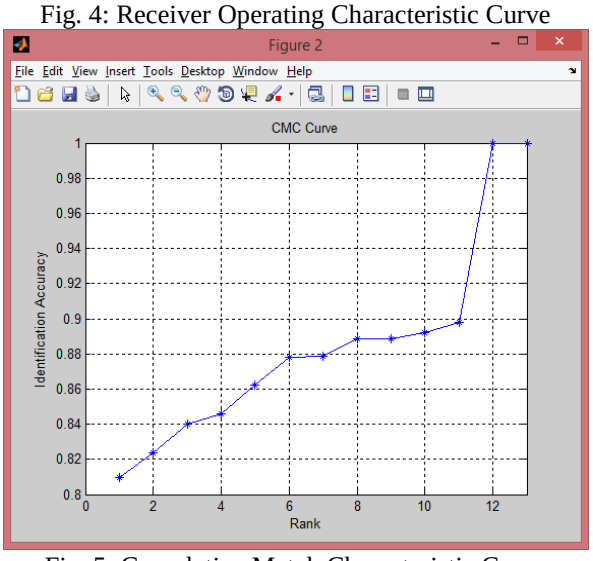


Fig. 5: Cumulative Match Characteristic Curve

CMC is a graph to represent a performance of closed-set identification system. The graph is generated by plotting Identification Accuracy against Rank. The combined match score is whether there is a right outcome inside the principal R sections. R is known as the rank.

For the system proposed the CMC curve analysis results are shown in the below table 1.

Rank	Identification Accuracy
1	0.810
2	0.824
3	0.840
4	0.846
5	0.862
6	0.878
7	0.879
8	0.889
9	0.889
10	0.892
11	0.898
12	1.000
13	1.000

Table 1: CMC curve results

V. Conclusion and Future Work

In this paper the fingerprint liveness detection method is proposed using moment features, which include Zernike moments, Geometric moments. Daubechies wavelet is implemented for wavelet analysis and finally Probabilistic neural network is used for classification of the test fingerprint. Carried out experiments on two most popularly used databases from LivDet competition 2011 and 2013. The proposed method gives a accuracy of 90%.

This method can be improved by including more moment features in order to enhance the performance measure of the system implemented and also determine the type of material used to produce the spoof/fake fingerprint, if the fingerprint under test is classified as spoof fingerprint.

References

[1] A. Jain, "Next generation biometrics," Dept. Comput. Sci.Eng., Michigan State Univ., Lansing, MI, USA, Tech. Rep.,Dec. 2009. [Online]. Available: http://www.cse.msu.edu/rgroups/biometrics/Presentations/Next_generation_biometrics_Korea_Dec2010.pdf.

[2] Fingerprint liveness detection using binarized statistical image features by L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, in Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS), Sep. 2013, pp. 1–6.

[3] M. Sepasian, C. Mares, and W. Balachandran, "Liveness and spoofing in fingerprint identification: Issues and challenges," in Proc. 4th WSEAS Int. Conf. Comput. Eng. Appl. (CEA), 2009, pp. 150 – 158. [Online] http://dl.acm.org/citation.cfm?id=1808102.1808130

[4] M. Sandstrom, "Liveness detection in fingerprint recognition systems," M.S. thesis. Institutionen för system eknik, Linköping, Sweden, Jun.2004. [Online]. Available: http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf.

[5] "Automatic Palmprint Identification based on High Order Zernike Moment" American Journal of Applied Sciences 9 (5): 759-765, 2012 ISSN 1546-9239.

[6] "Fingerprint Liveness Detection From Single Image Using Low-Level Features and Shape Analysis" Rohit Kumar Dubey, Jonathan Goh, and Vrizlynn L. L. Thing

[7] "A new method of fingerprint authentication using 2d wavelets" Avinash Pokhriyal Sushma Lehri Vol. 13 No.2 March, 2010 pp (131 - 138).
[8] "Wavelet Based Fingerprint Authentication System: A Review" An International Journal (ELELIJ) Vol 5, No 1, February 2016

