ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Fingerprint Liveness Detection using Deep Stacking Network

Akshata Satish Shet[1]

ME Student, Department of Electronics and Telecommunication Engineering, MIT College of Engineering, Kothrud, Pune, India[1]

ABSTRACT:Fingerprints have beenmost generally utilized for diverse security systems because of the high-level accuracy and user's convenience. Since fingerprints begin to be broadly used in the smart mobile phones and tablets for payment as well as security, high-performed algorithms have been explored in the literature. At the same time, such mobile systems are highly required to detect spoofing attacks by fabricated fingerprints with malicious intends. This system implemented by using MATLAB software. In this paper, we used combination Speeded-Up Robust Features (SURF), Histograms of Oriented Gradient (HOG) and texture features from Gabor filter and deep stacking network as a classifier of the system. Nowadays deep learning adapting success in object recognition area for its ability in deep feature extraction and representations. In this study, we performed experiment analysis on the database from livdet2015.

KEYWORDS:fingerprint liveness; Gabor filter; Deep stacking network.

I. INTRODUCTION

Fingerprint liveness detection is the goal to detect a fingerprint image, capture by an electronic device, belongs to an alive fingertip or to be an artificial of it. Biometric systems are an emerging technology that refers to the identity identification based on their physiological and behavioral characteristic. Therefore, biometric recognition systems are commonly used for authentication in various security applications. Biometric technology presents several advantages than traditional security methods based on either some information (PIN, Password, etc.) or physical devices (key, card, etc.) The ability of fingerprint authentication system to determine whether or not the fingerprint samples presented are really from a live fingertip or fake one, which is called liveness detection.To prevent an attack, many different kinds of detection methods have been proposed in recently.

During the previousdecade, the large growth in biometric analysis resulting in the advancement of innovative sensors, novel feature extraction and matching algorithms. Fingerprints are most generally used for numerous security systems because of the high-level accuracy and user's convenience.

Nowadays, such fingerprints are used to a key application, e.g., payment, on mobile devices by the small size of fingerprint sensors. performed recognition methods have been systematically developed, most of them still suffer from spoofing attacks using different materials, e.g. silicone, gelatin, wood glue, etc. [1] Moreover, fingerprints can be easily captured from scanning the stolen device, which are readily employed to penetrate the security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

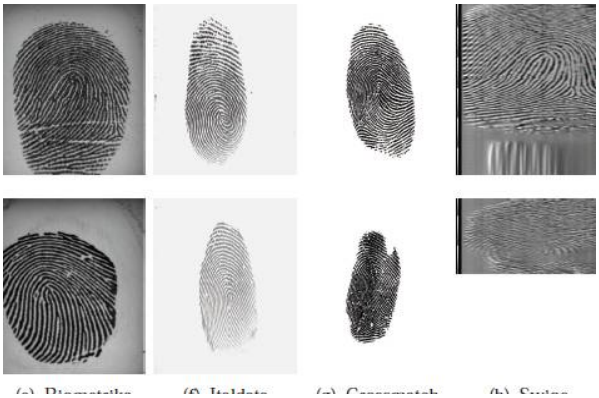

Fig. 1. Example of live (above) and fake (below) fingerprints acquired with 4 sensors.

As illustrated in Fig. 1, we observe that it is very difficult to visually differentiate between live and fake fingerprints. The fingerprint based authentication system creates the need to develop a method which can distinguish between live and fake fingerprint images.

In this paper, to analyse the detection performance we employ dataset from livDet2015 which consist various fake fingerprints generated by silicone, gelatin, and playdoh have been captured from fingerprint sensors.

II. RELATED WORK

In this section, we tend to discuss the literature in the field of software based fingerprint liveness detection. D. Yambay et. al. [2] "Liveness detection", a system used to decide the authentication of a submitted biometric, has been implemented in fingerprint scanners in recent years. The main principle for the LivDet 2013[2] and LivDet 2015[3] competition is to check software-based fingerprint liveness detection strategies as well as fingerprint frameworks which incorporate liveness detection capabilities utilizing a standardized testing protocol and huge quantities of spoof and live fingerprint images. LivDet is the worldwide public competition for programming-based fingerprint liveness recognition and first public assessment of framework based fingerprint liveness recognition.

Rodrigo [4] proposed a method based on convolutional neural networks (CNNs) for fingerprint liveness detection. In this systemexperimental analysis was done on the data sets used in the liveness detection competition of the years 2009, and 2011 which comprises almost 50000 live and fake fingerprints images. The system consist comparison of four different algorithm models: two CNNs pretrained on natural images and fine-tuned with the fingerprint images, CNN with random weights, and a classical local binary pattern approach.

Perspiration-based method: Sweat glands creates moisture, the real live fingerprint images from fingerprint devices will change marginally in a brief span period.. However the obtained spoof ones from sensor devices can not generate moisture. Therefore, analysts discover find the fingerprint vitality through the study of Perspiration.The authors Tan and Schuckers[5] obtain a skeleton of the ridge structure and this skeleton determine extracted ridge signal. The signal is analyzed by using wavelets and classified between the fake and real fingers. In this paper, Tan and Schuckers [6] also analyze the middle ridge signal generate from the centers of the ridges structure of skeleton. On account of the perspiration phenomenon, the middle ridge signal obtained from a real finger is of a periodic nature determined by the periodic occurrence of the active sweat pores. Because of the absence of the sweating process, the middle ridge signals obtained from the fake and do not exhibit this significantly periodic nature.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Sweat pores: The sweat pores are very small circular structures present in the fingerprint ridges of the living fingers that are the endings of internal skin structures called sweat glands.

The sweat glands are responsible for production of sweating fluid. The liveness detection methods based on the analysis of the sweat pores usually expect that such small structures would be very difficult to reproduce with sufficient quality when the fake finger is produced.

III. PROPOSED SYSETEM

In this work, we divide the system into three main sequential blocks:

- Image Pre-processing Stage
- Feature Extraction Stage
- Image Classification Stage

A. *Image pre-processing stage*

This is initial stage of system. A low quality fingerprint image is usually noisy and has low contrasts between valleys and ridges. These effects will happen throughout image acquisition, as result of dry or wet skin. Since the image acquisition stage is not always monitored for accepting only high quality images, fingerprint image enhancement and noise reduction are, therefore, important pre-processing factors in accurately detecting fingerprint liveness.

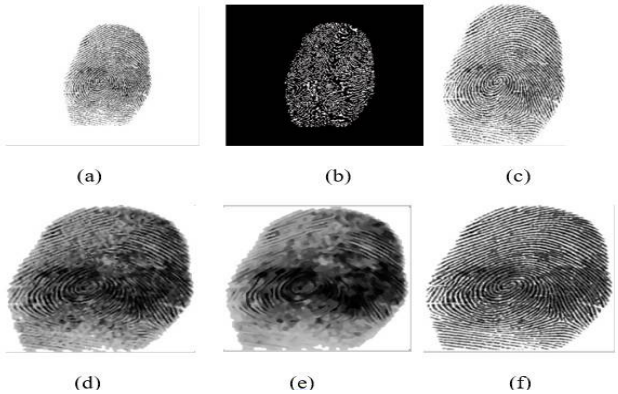

Fig. 3. (a) Original Image (b) Canny Image (c) Cropped Image (d) after median filtering (e) after histogram equalization (f) Resized

Canny edge detector is first applied for the purpose of to detect wide range of edges in the images as shown in fig. 3(b). We can enhanced the quality of the image by cropping the fingerprint region in the image and then performing histogram equalization expand the discernment dataas shown in Fig. 3(e).To remove noise during image acquisition, median filtering is then applied on the cropped images as shown in Fig. 3(d).

B. *Feature Extraction stage:*

In fingerprint security systems, the image is usually captured from different scanners. Therefore, fingerprint images are typically found to be of different scales and rotations. In certain scenarios, the fingerprint images are partially captured due to human errors. In order to obtain features that are invariant to these problems, we use various features that capture properties of live fingerprint images.Fig. 4 shows the block diagram of feature extraction.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

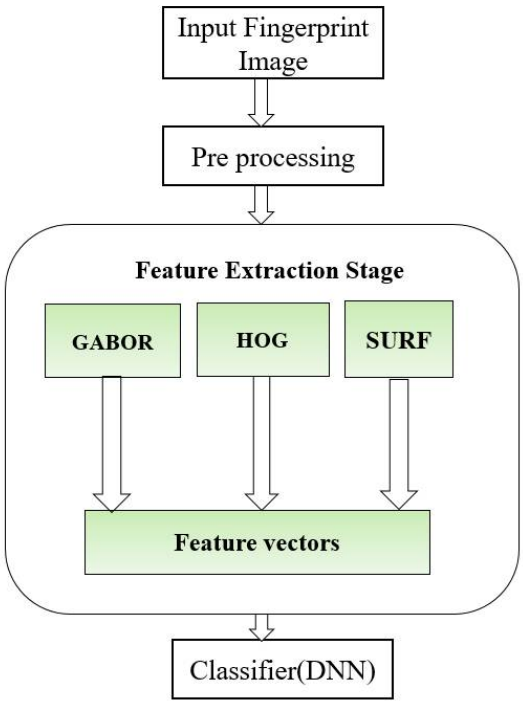

Fig. 3. Block diagram of System

a) SURF

In this paper we choose to use SURF (Speed Up Robust Feature) as it is invariant to illumination, scale and rotation. The detector locates the key points in the image and the descriptor describes the features of the key points to build the feature vectors of the key points. The determinant of the approximate Hessian-matrix uses by SURF on the integral image to locate the key feature points. For the key point descriptor, SURF uses the sum of the Haar wavelet responses to describe the feature of a key point [8]. SURF descriptors have been used to locate and recognize objects, people or faces, to track objects and to extract points of interest.

b) HOG

The histogram of oriented gradients (HOG) is anelement descriptor used in image processing for the purpose of object detection. The histogram of oriented gradients descriptor can be described by the distribution of intensity gradients or edge directions. The technique counts occurrences of gradient orientation in localized portions of an image. This technique is same to that of edge orientation histogramsscale-invariant feature transform descriptors, and shape contexts. The features of the gradient are sustained into the neural network classifiers that give increasingly extra exactness in the classification comparing with other classifiers.

Following steps are to calculate Histogram of gradients.

i. To calculate a HOG descriptor, first calculate the horizontal (x) and vertical (y) gradients then calculate the histogram of gradients. The output of this as shown in following fig.5.This is easily achieved by filtering the image with the [-1 0 1] kernels.

ii. To find magnitude and direction of gradient using the following formula.

$$g = \sqrt{g_x^2 + g_y^2}$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

$$\theta = arctan\frac{g_y}{g_y}$$

iii. Sincedifferent images may have differentcontrast, contrast normalization can be very useful. Normalization is done on the histogram vector within a block. One of the following norms could be used.

$$L1\ norm : f = \frac{v}{\|v\|_1 + e}$$

Fig.5(a) x gradient (b) y gradient

c) Gabor filter

Gabor filter is used to extract features from fingerprint images for texture analysis. Gabor filters have optimal localization properties in both the frequency domain and spatial domain.A Gabor filter is obtained by modulating a sinusoid with a Gaussian. For the case of one dimensional (1D) signals, a 1D sinusoid is modulated with a Gaussian.

Let g(x, y, Θ, ϕ) be the function defining a Gabor filter centered at the origin with Θ as the spatial frequency and ϕas the orientation. We can view Gabor filters as:

$$(x, y, \Theta, \phi) = \exp\left(-\frac{x^2 + y^2}{\sigma^2}\right)\exp(2\Pi\Theta i(x\ cos\ \phi + y \sin\Theta)))$$

It has been shown that, σ the standard deviation of the Gaussian kernel depends upon the spatial frequency to measured. i.e. Θ. In our case σ = 0.65Θ.

C.Classification:

The grouping is separate for real and fake fingerprint. Once the features have been extracted, we continue advance by grouping the images and distinguishing the fingerprint. For this arrangement we have different algorithms but we use deep stacking network as classifier for distinguishing real and fake fingerprint.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

DSN Architecture:

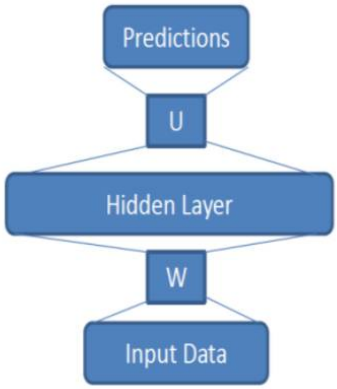

Fig.6. A typical DSN architecture

Basic learning algorithm:

The input feature vector is denoted

$$X = [x_1, \dots x_i, \dots x_N](x_i = [x_{1i}, \dots x_{ji}, \dots x_{Di}]^T)$$

Where *D* is the dimension of each input vector and *N* is the number of the training samples.
Let *L* be the number of hidden units, and *C* be the dimension of the output vector. Then the output of the DSN module is

$$y_i = U^T h_i$$

Where $h_i = \sigma(W^T x_i)$ is the output of hidden layer,
U is the upperweight matrix of dimension LxC
Wis the lower weightmatrix dimension DxL[10]

IV. EXPERIMENTAL RESULTS

IN THIS SECTION, WE DONE EXPERIMENTAL ANALYSIS OF LIVENESS OF FINGERPRINT.

A. DATASETS

Our analyses were completed on openly accessible fingerprint liveness database for LivDet 2015 competitions from Clarkson University - University of Cagliari. For the LivDet 2015 database, four optical sensors, Biometrika, Digital Persona, Greenbit, and Crossmatch were used to collect the fingerprints. The corresponding spoof materials were chosen from body double, latex, PlayDoh, wood glue, gelatine, latex.

B. Result

This system built in MATLAB Software. First created GUI (Graphical User Interface) as shown in figure with input test image.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

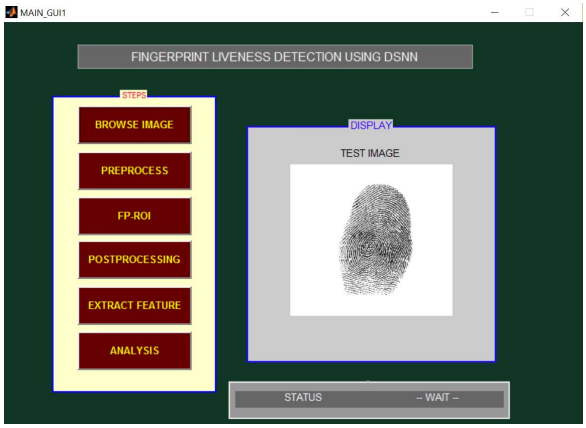

FIG.7. GUI OF THE SYSTEM

AFTER PERFORMING ALL STAGES OF THE SYSTEM WILL CLASSIFY THE FINGERPRINT IMAGE IS REAL OR FAKE.

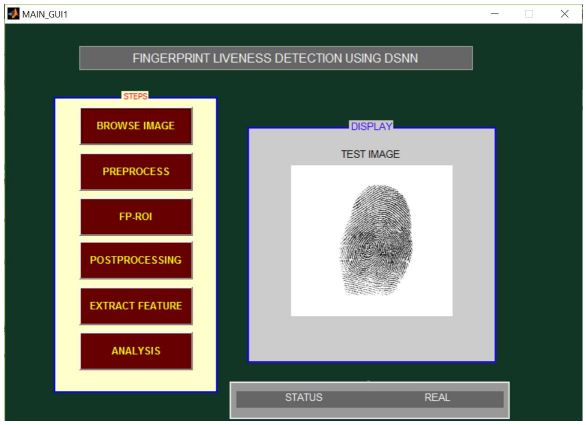

FIG. 8. OUTPUT OF THE SYSTEM

C. Confusion matrix

We have total 2000 sample images with 1500 real n 500 are fake. In the following confusion matrix positive means real fingerprint and negative means fake fingerprint.

N=2000	Positive	Negative
Positive	1470	30
Negative	480	20

In all our experiments, we use AverageClassification Error (ACE) equation and Equal Error Rate (ERR).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

TABLE I : Comparison of ACE with LivDet 2011 competition database

Methods	ACE
WLD+LPQ	7.87
MBLTP	9.77
multiresolution LBP	10.22
Tans method	14.24
Power Spectrum	33
Curvelet Energy	35.87
Our Method	**3**

To determine accuracy we use following equation

$$ACC = \frac{TP + TN}{N}$$

Here TP as true positive value and TN true negative value.

Table II provides the comparison of accuracy with algorithm used in livDet2015 competition.

TABLE II: Comparison of accuracy with algorithm used in livDet2015 competition

Algorithm	Accuracy
Nogueira	95.51
Unina	93.23
jinglian	92.82
anonym	92.51
Titanz	91.21
ohbirkholz	90.64
hectorn	87.32
Our Method	**97.5**

VI.CONCLUSION

In this paper we have tendency to implement unique technique for liveness detection of fingerprint. To keep a decent level of security, reliable spoofing detection tools or device are necessary, preferably implemented as software modules. In this paper we used SURF, Gabor filter and HOG for texture feature and in addition Deep Stacking Network as classifier which have owns advantages to other deep models for its simplicity. We carried out experiments on used databases from LivDet2015. The proposed method scored consistently low EER and high accuracy compare to other used methods.

REFERENCES

[1] Rohit Kumar Dubey,Jonathan Goh,and Vrizlynn L L Thing "Fingerprint liveness detection from single image using Low level feture and shape analysis" IEEE Transactions on, Information Forensics and Security DOI 10.1109/TIFS.2016.

[2] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G.L. Marcialis, F. Roli, and S. Schuckcrs, "Livdet 2013 fingerprint liveness detection competition 2013," in Biometrics (ICB), 2013 International Conference on, June 2013, pp. 1–6.

[3] Valerio Mura, Luca Ghiani, Gian Luca Marcialis, Fabio Roli "LivDet2015 fingerprint liveness detection competition 2015," in Biometrics Theory, Application and System (BTAS),2015 IEEE 7th International Conference on Sept 2015.

[4] Rodrigo Frassetto Nogueira, Roberto de Alencar Lotufo, and Rubens Campos Machado," Fingerprint Liveness Detection Using Convolutional Neural Networks", IEEE transactions on information forensics and security, vol. 11, no. 6, June 2016

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

[5] Tan, B., Schuckers, S.: 'Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing'. Proc. ComputerVision and Pattern Recognition Workshop (CVPRW '06), 2006, pp. 26.

[6] Tan, B., Schuckers, S.: 'Spoofing protection for fingerprint scanner byfusing ridge signal and valley noise', Pattern Recognit., 2010, 43, (8),pp. 2845–2857.

[7] Espinoza, M., Champod, C.: 'Using the number of pores on fingerprint images to detect spoofing attacks'. Proc. Int. Conf. on Hand-Based Biometrics (ICHB), 2011, pp. 1–5.

[8] Herbert Bay , Andreas Ess "Speeded-Up Robust Features (SURF)"Science Direct Computer Vision and Image Understanding 110 (2008) 346–359.

[9] V. Shiv Naga Prasad_University of Maryland "Gabor Filter Visualization"

[10] *Mingyi He, Xiaohui Li, Yifan Zhang,* "Hyperspectral Image Classification Based On Deep Stacking Network"2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS) pages 3286-3289.