Fingerprint Liveness Detection by a Testing and Trained Data using Convolutional Neural Network

Vishwas Prakash. R
P.G Student
Department of Master of Computer Application
P.E.S College of Engineering
Mandya, Karnataka, India

Dr. Mohan Kumar H. P
Professor and Head
Department of Master of Computer Application
P.E.S College of Engineering
Mandya, Karnataka, India

***Abstract*— It is understood that fingerprints are synthesized quickly to deceptively classify structures. In this paper we suggest a latest approach integrating for fingerprint as trained data which are stored in the liveliness detection device for identification. In order to fit new fingerprints that want to get to the network, the testing fingerprint ID Application will have a set of sample fingerprints saved. The proposed method uses the fingerprints referring to the trained and test fingerprints use convolution neural networks to render a judgment on liveliness. The proposed methodology shows an accuracy of 90.8 % for classification of data. The dataset are being classified through various algorithm for their precision.**

Keywords—Liveness Detection, Testing-Trained, Convolutional Neural Networks

I. INTRODUCTION

The identification of fingerprints was a secure and easy safety mechanism for different devices like mobile phones and tablets. However, the synthetically reproducible fingerprints are also identified. Fake fingerprints can be replicated from the daily usable materials like glue and clay materials [1], [2]. The recognition method may be manipulated even with raw synthetic fingerprints. An identification system for fingerprints works on the first recorded fingerprints of the sample and often stores (i.e trained fingerprint) several separate press from the similar finger. The machine authorization is given when the fingerprint sample meets the fingerprints stored in fingerprint dataset. These schemes could be overridden when the synthetic finger with the fingerprint fit creates an identification system with the testing fingerprint. An equivalent finishing thumbprint can in principle be collected from a large variety of personal items such as doorbells or metallic frames. Often workers transform their own fingerprints synthetically and swap them with colleagues to allow the program to register for fake participation. A safer fingerprint recognition program is therefore needed to fit fingerprints properly and identify false finger impression. From the recent studies, fraud biometric recognition issue had been differentiated from the recognition framework. Precision of the liveness model is calculated by admitting the dataset (i.e Fingerprint) to be live or fake [1], [2]. The recognition of the fingerprint dataset are the main purpose of spoof detection. The fingerprint sample must be compared to trained dataset if the fingerprint is said to be live, then it should be allowed to enter into the network [12,13]. Therefore, using the trained fingerprints for spoof identification is not only feasible but also rational.

II. LITERATURE REVIEW

H.Y. Jung and Y.S. Heo [3] proposed a new technique for avoidance in the use of synthetical reproducing biometrics by providing a robust framework and introducing it in the network training and detection and also employs squared regression error at the receptive fields by not using the fully connected layer.

Aditya Abhyankar and Stephanie Schuckers [5] introduced a simple cost effective method by measuring liveness of single image which is developed by using multi resolutional texture analysis and orientation maps.

Luca Ghiani [6] et al proposed BSIF and a textural analysis algorithm which was conducted by livedet.org and using of live det 2011 datasets [4].

Yujia Jiang and Xin Liu [7] defined their work by using uniform binary pattern and once the feature is being obtained then it is being trained by SVM classifier by using LivDet 2013 dataset. [4]

Toosi et al. [8] performed an extensive analysis of the different features of liveliness and Investigated the efficiency of various practical fusion methods for fresh components, for instance of binary statistics.

Luca Ghiani [9] et al introduced Picture attributes, equivalent to local binary patterns as well as local phase quantization characterizations, have been presented.

Equally relevant for researchers into fingerprint liveness identification, LivDet.org has held major tournaments with multiple databases since 2009[1][2][4][10][11]. Many events has been found through the exhibition.

Vinod Nair and E. Hinton [10] proposed Restricted Boltzmann techniques have been developed utilizing hidden state from binary stochastics. It can be simplified by substituting each binary unit with a limitless number of copies all of which have having similar loads but gradually also have negative bias. The guidelines for training and estimation of such "Stepped Sigmoid Groups" remain constant.

HO YUB JUNG [11] et al proposed the system can be developed on top of existing capable of identifying liveness to boost performance although substantially increasing its time complexity. The analysis of the LivDet data's demonstrate that the proposed approach for detecting liveliness of fingerprints is capable of achieving state-of-the-art precision [11][4].

III. PROPOSED SYSTEM

In this paper we're introducing a new way to integrate into this proposed framework, by checking the liveness using Feature extraction, Training and Testing.

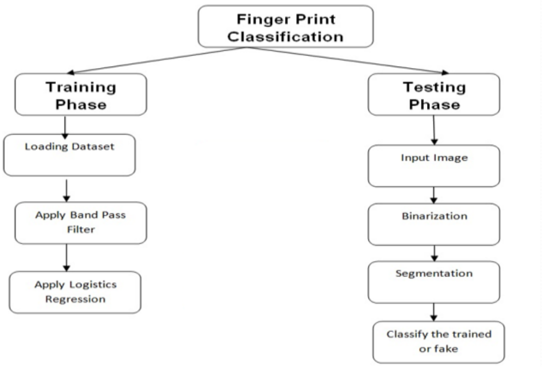

Fig. 1. Architecture of Proposed System.

IV. IMPLEMENTATION AND WORKING

In the previous segment we appear to quote about Development and technological stack connected to fraud Application. We discuss about the deployment in this section and System functioning in real world situation.

A. Convolutional Neural Networks

The proposed solution does not consider the problem of liveness identification as a simple problem of classification. Preferably, we know there would be definite textural characteristics found more at spoof fingerprints, then in the live fingerprint ther're more certain characteristics. We can also see that there would be live fingerprint with much fake attributes, likewise there would be more live attributes in the fake fingerprint. These fingerprints couldn't be identified easily.

B. Feature Extraction

In order to provide the efficiency by not making any changes in the previous model following features have been taken to increase its accuracy. The following features are extracted in fingerprints.

- Gabor Filter
- Ridge Segment
- Ridge Frequency
- Ridge Orientation

C. Training Phase

The training phase consists of mainly 3 functionalities in it. Where this phase is mainly used to store the datasets (i.e fingerprints) and further Band Pass Filter is applied on that fingerprint. For upcoming process these fingerprints are stored for compared. The Logestic regression is applied on it.

```
In [1]: runfile('C:/Users/Vishwas Prakash/project1/main.py', wdir='C:/Users/
Vishwas Prakash/project1')
loading sample image
C:/Users/Vishwas Prakash/project1/main.py:35: DeprecationWarning: `imread`
is deprecated!
`imread` is deprecated in SciPy 1.0.0.
Use ``matplotlib.pyplot.imread`` instead.
  img = scipy.ndimage.imread(img_name);
C:/Users/Vishwas Prakash/project1/main.py:48: DeprecationWarning: `imresize`
is deprecated!
`imresize` is deprecated in SciPy 1.0.0, and will be removed in 1.3.0.
Use Pillow instead: ``numpy.array(Image.fromarray(arr).resize())``.
  img = scipy.misc.imresize(img,(np.int(new_rows),np.int(new_cols)));
```

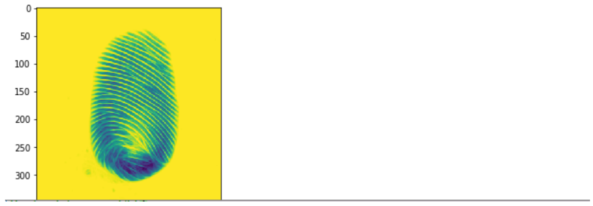

Fig.2. Loading Fingerprint in Training Phase.

D. Testing Phase

The Testing Phase mainly consists of 4 stages in it. The scanned fingerprints are stored in the testing stage. Further it has been passed through the Binarization process where it works in the same way by applying filter on the fingerprint to get the similar quality of the fingerprint which has been taken in the training phase. Finally, the Fingerprints are classified whether it's a fake or the live fingerprint.

	Image	L2CA	...	cD1 std	Class
0	Extract1.bmp	68243.902473499	...	0.0722696155	Live
1	Extract1.png	70777.8630447713	...	0.0194780634	Fake
2	Extract10.bmp	65352.0989406296	...	0.2545692467	Live
3	Extract10.png	72815.4843911259	...	0.014897026	Fake
4	Extract100.bmp	67281.7494343461	...	0.0787343676	Live

Fig.3. Liveness Detection on Testing Phase.

E. Classification

The train score, test score, train timings for each prediction of the fingerprints are verified. The algorithm which are used for the classification process are Random Forest, Gradient Boosting, Decision Tree, K-Nearest Neighbors, Neural Net, Support Vector Machine, Logistic Regression, Ada Boost, Naive Bayes.

classifier	train_score	test_score	train_time
Random Forest	1.000000	0.908388	208.624376
Gradient Boosting Classifier	1.000000	0.901844	508.221632
Decision Tree	1.000000	0.883403	1.058217
Linear SVM	0.880405	0.863772	8.503579
AdaBoost	0.941690	0.852469	164.934628
Nearest Neighbors	0.877628	0.785247	1.273932
Logistic Regression	0.732844	0.755503	1.173910
Naive Bayes	0.663229	0.678168	0.076541
Neural Net	0.701706	0.647234	41.095901

Fig.4. Classification of Fingerprints.

V. CONCLUSION

Fingerprint liveness were measured with the trained data also with the tested data. The liveness of the fingerprint can be checked for those which are registered in fingerprint model. The proposed methodology shows an accuracy of 90.8% for classification of data. Using fingerprint data for both test and trained datasets as a captured function, the introduced method would be increasing in precision of the liveness detection.

REFERENCES

[1] Luca Ghiani, David A Yambay, Valerio Mura, Gian Luca Marcialis, Fabio Roli, and Stephanie A Schuckers. Review of the fingerprint liveness detection (livdet) competition series: 2009 to 2015. Image and Vision Computing, 58:110–128, 2017.

[2] Mura, Valerio, et al. "LivDet 2017 fingerprint liveness detection competition 2017." 2018 International Conference on Biometrics (ICB). IEEE, 2018.

[3] Jung, H. Y., and Y. S. Heo. "Fingerprint liveness map construction using convolutional neural network." Electronics Letters 54.9 (2018): 564-566.

[4] http://livdet.org.

[5] Aditya Abhyankar and Stephanie Schuckers. Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In Proceedings of the International Conference on Image Processing (ICIP), pages 321–324. IEEE, 2006.

[6] Ghiani, Luca, et al. "Fingerprint liveness detection using binarized statistical image features." 2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS). IEEE, 2013.
Jiang, Yujia, and Xin Liu. "Uniform local binary pattern for fingerprint liveness detection in the Gaussian pyramid." Journal of Electrical and Computer Engineering 2018 (2018).

[7] Amirhosein Toosi, Andrea Bottino, Sandro Cumani, Pablo Negri, and Pietro Luca Sottile. Feature fusion for fingerprint liveness detection: A comparative study. IEEE Access, 5:23695–23709, 2017.

[8] Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, and Fabio Roli. Fingerprint liveness detection using binarized statistical image features. In Proceedings of the International Conference on Biometrics: Theory, Applications and Systems (BTAS), pages 1–6. IEEE, 2013.

[9] Ghiani, L., Yambay, D., Mura, V., Tocco, S., Marcialis, G. L., Roli, F., & Schuckcrs, S. (2013, June). Livdet 2013 fingerprint liveness detection competition 2013. In 2013 International Conference on Biometrics (ICB) (pp. 1-6). IEEE.

[10] Nair, Vinod, and Geoffrey E. Hinton. "Rectified linear units improve restricted boltzmann machines." Proceedings of the 27th international conference on machine learning (ICML-10). 2010.

[11] Jung, Ho Yub, Yong Seok Heo, and Soochahn Lee. "Fingerprint Liveness Detection by a Template-Probe Convolutional Neural Network." IEEE Access 7 (2019): 118986-118993.

[12] S. Prabu, V. Balamurugan, and K. Vengatesan, “Design of cognitive image filters for suppression of noise level in medical images,” Measurement, vol. 141, pp. 296-301, 2019.

[13] B.D. Parameshachari, H.T. Panduranga, and S.K. Naveenkumar, “Partial encryption of medical images by dual DNA addition using DNA encoding,” In Proc. of international conference on recent innovations in signal processing and embedded systems (RISE), pp. 310-314, 2017.