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 4, April 2017

Liveness Detection of Fingerprint, Face, Iris Using Convolutional Networks And Local Binary Patterns

Anita Babu [1], Dimple Elizabeth Baby [2], Dr.Vince Paul[3]

M. Tech Student, Dept. of Computer Engineering, Sahrdaya College of Engg.&Tech., Kodakara, Kerala, India[1]

Assistant Professor, Dept. of Computer Engineering, Sahrdaya College of Engg.&Tech., Kodakara, Kerala, India[2]

Associate Professor, Dept. of Computer Engineering, Sahrdaya College of Engg.&Tech., Kodakara, Kerala, India[3]

ABSTRACT: Biometric systems are growingly used for authentication purposes in various security applications. Despite the increase in usage of biometric based systems, these are quiet susceptible to sophisticated spoofing attacks. To improve the level of security, it is necessary to augment the reliable liveness detection tools as software modules along with the existing authentication systems. This paper targets the countermeasures for the biometric spoofing attacks and also suggests technical measures for implementing the biometric liveness detection systems. In order to overcome the shortcomings of already existing liveness detection tools, in this work we propose two different feature extraction techniques for software-based liveness detection: Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier. Dataset Augmentation was used to increase classifier's performance and a variety of preprocessing operations were tested, such as frequency filtering, contrast equalization, and region of interest filtering.

KEYWORDS: : Liveness; Convolutional networks; Local binary patterns; Dataset augmentation; Support vector machines

I. INTRODUCTION

Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. Biometric systems are increasingly used for authentication in various security applications. Biometric based systems offer simplicity of use and reliability. This can avoid problems of systems based on the use of passwords, which can be forgotten, transferred or stolen. Despite the increases in usage of biometrics ,there are several real threats to biometric authentication systems .Biometrics have their own inherent weakness that can potentially compromises the security of a system. Biometric characteristics are not at all private. Fingerprint, face, iris are the frequently used traits in the present authentication systems. For example, we leave fingerprints everywhere we go; it is possible to fool a fingerprint-based system by reproducing the biometric pattern on simple molds made of materials such as silicone, Play-Doh, clay or gelatin. Likewise, iris-based systems can be attacked with fake irises printed on paper or on wearable plastic lenses while face-based systems can be fooled with sophisticated 3D masks (easily bought online once a few photos of the subject are provided) or, again, with faces printed on paper. Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. All these points to the necessity of biometric liveness detection. Inorder to improve the security of a biometric system, it is necessary to embed the liveness detection component to the authentication System.

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

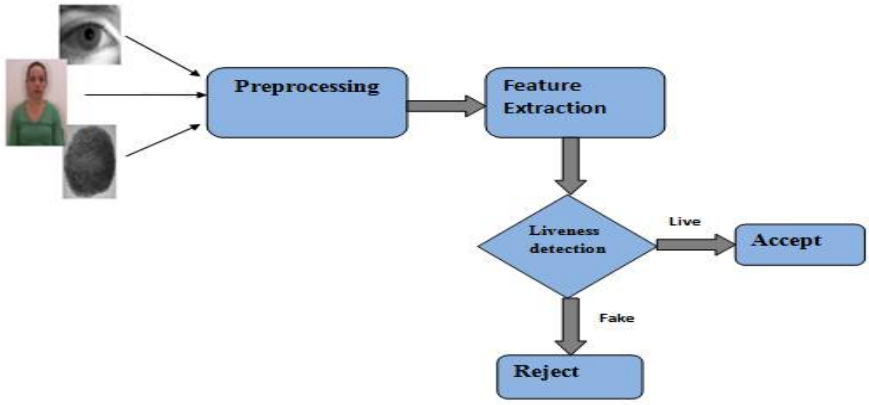
Vol. 6, Issue 4, April 2017

Fig.1 Typical examples of real and fake fingerprint images

Section II describes related works. Section III explains the methodology. Section IV presents experimental results. Finally, Section V presents conclusion.

II. RELATED WORK

A large number of methods have been proposed in recent years to detect spoofing . Some of them rely on the detection of vitality signs at the acquisition stage. Hence they require additional hardware embedded in the sensor which verifies vitality by measuring particular intrinsic properties of a living trait, such as temperature, odor, sweat, blood pressure, or reflection properties of the eye , sometimes also in response to specific stimuli . By combining multiple sources of information, this approach turns out to be more resilient to specific attacks, providing a very good reliability. However, it is a relatively expensive and rigid solution, potentially vulnerable to attacks not considered at design time. On the contrary, software-based methods, based on signal-processing techniques, are certainly more appealing, for their reduced cost and invasiveness, and their higher flexibility. They try to detect liveness by analyzing synthetic image features that are peculiar of vital biometric traits and not easily reproduced on fakes. Liveness detection methods are generally classified into two types : (i) Softwarebased techniques, in this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the trait itself); (ii) Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye)[1]. liveness detection techniques, which use different physiological properties to differentiate between real and fake character. Once the biometric trait has been acquired a feature extraction process followed by a classification step labels the image as fake or live.



.

Fig.2 Overview of liveness detection system

The majority of techniques follow the paradigm shown in Fig.2, differing mainly in the type of features extracted. Liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [7]:

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 4, April 2017

- non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user;
- user friendly, people should not be reluctant to use it;
- fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time;
- low cost, a wide use cannot be expected if the cost is excessively high;
- Performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

III. METHODOLOGY

Biometrics already form an important part of current and emerging authentication systems. Biometrics systems aim to verify the identity of an individual from their behavioural and/or biological characteristics. Despite their many advantages, biometric systems, like any other security application, are vulnerable to a range of attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. The aim of this work is to provide an efficient liveness detection of fingerprint, face, iris using convolutional networks and local binary patterns. In order to overcome the shortcomings of already existing liveness detection tools, in this work we propose two different feature extraction techniques for software-based liveness detection: Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier.

A. Models

Table I discusses the models used in this study. All the models used dataset augmentation. Fig. 3 shows the architecture of the models. For CNN-VGG and CNN-Alexnet, the architecture is the same as described in [12] ,instead of the last 1000-unitsoftmax layer it uses a 2-unit softmax layer , so the network can result in the 2 class output (if the image is real or fake).

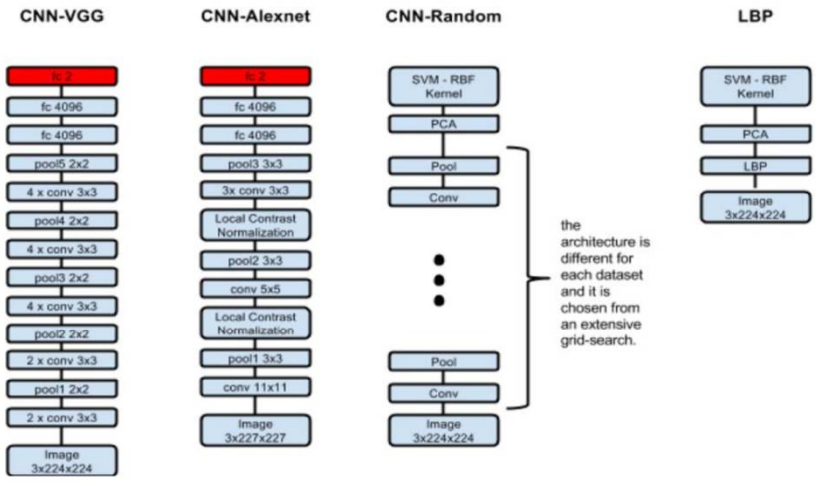


Fig.3 Illustration of the models[12]

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 4, April 2017

CNN-VGG,CNN-Alexnet,CNN-Random are the models used in this study,LBP is the local texture descriptor used to extract the features of fingerprint, fac

TABLE 1. Summary Of The Models

Model Name	Pipeline	Description
CNN-VGG[12]	16 Convolutional Layers + 3 Fully Connected Layers	Pre-trained model and finetuned using liveness detection datasets
CNN-Alexnet[12]	8 Convolutional Layers + 3 Fully Connected Layers	Pre-trained model and finetuned using liveness detection datasets
CNN-Random[12]	CNN-Random + PCA + SVM	Features are extracted using Convolutinal Networks.The feature vector is reduced using PCA and then fed into a SVM classifier with (gaussian)RBF Kernel
LBP[12]	LBP + PCA + SVM	Feature sare extracted using LBP .The feature vector is reduced using PCA and then fed into a SVM classifier with (gaussian)RBF Kernel

B. Convolutional Neural Networks

In this work, we used convolutional neural networks (cnns) for fingerprint, face, iris liveness detection. An alternating layers of convolution and local pooling (i.e., subsampling) forms this type of networks. The basic aim of a convolutional networks is to classify the objects. In our study ,we use convolutional neural networks (cnns) for extracting patterns found within local regions of the inputted images such as fingerprint, face, iris images. From the selected features,the system can discriminate between the real and fake sample. We compared three different models of convolutional networks .CNN-Random, CNN-Alexnet, CNN-VGG are those models. The algorithm used to train CNN-Alexnet and CNN-VGG is the Stochastic Gradient Descent (SGD). Fig. 4 illustrates the different layers feed-forward convolutional network.

C. Local Binary Patterns

Local Binary Patterns (LBP) are a local feature descriptor .This descriptor performed well in computer vision applications, including texture classification and segmentation, image retrieval. In this work it is used as a baseline method for liveness detection. During the feature extraction process, LBP method forms the feature vector of the fingerprint, face, iris images. And this feature descriptor is converted to the normalized histogram of the LBP images. In this study, the histogram of the LBP image was further reduced using PCA, and a SVM with RBF kernel is used as the classifier. Finally it distinguishes the fake from the genuine one.

D. Dataset Augmentation

Dataset Augmentation technique ,artificially creating slightly modified samples from the original ones. It makes the classifier more robust against small variations Dataset augmentation improves the accuracy of the liveness detection system.

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 4, April 2017

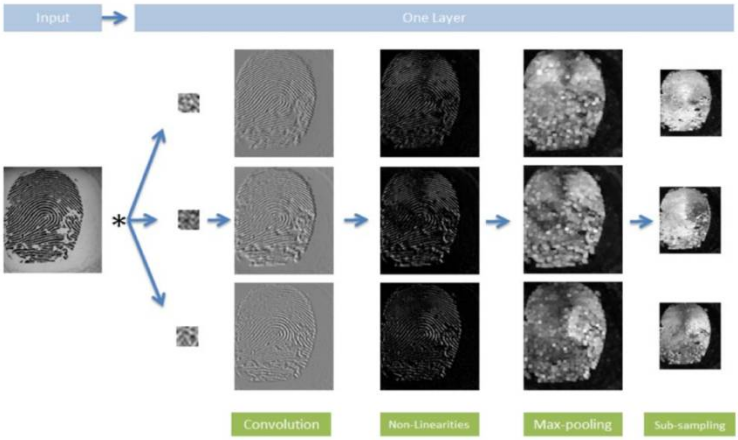


Fig.4 illustrates the convolutional network[12]

IV. EXPERIMENTAL RESULTS

A. Datasets

The datasets provided by the Liveness Detection Competition (LivDet) in the years of 2009 , 2011 , and 2013 are used in this study. In all datasets, the real/fake fingerprint ratio is 1/1 and they are equally distributed between training and testing sets. CASIA Face Anti-Spoofing Database is used for the face liveness detection .ATVS-FFp DB is used for the fingerprint liveness detection. CASIA iris image database v4 is used for the iris liveness detection. Datasets from the BITs was used to train the whole liveness detection system. Datasets are used for training as well as testing

B. Performance Metrics

The classification results were produced by the liveness detection system is evaluated by the Average Classification Error (ACE), which is the standard metric for evaluation in LivDet competitions. It is defined as
ACE = (SFPR+SFNR)/2. where SFPR (Spoof False Positive Rate) is the percentage of misclassified live samples and SFNR (Spoof False Negative Rate) is the percentage of misclassified fake samples.

C. Implementation Details

Python is used to implement the whole algorithms. Build-in functions from Numpy, Scipy, Scikit-Image and Scikit-Learn packages are also used in implementation. Python is used to do the whole project with utilization of opencv 2.4.9 .preprocessing of the inputted images ,feature extraction using LBP and various CNN models, classification using SVM are the different modules of the work. SVM classification is done with the utilization of sklearn pacakage. Dataset augmentation demonstrated to play an important role to increase accuracy and it is simple to implement.

D. Results

The following are the screenshots of the developed system. the system works accurately and it clearly distinguishes the real biometric from the spoofed one.Fig.5 shows the front page of liveness detection system, from this page it is directed to finerprint, face, iris type liveness detection.Fig.6 shows the training of the developed system.

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 4, April 2017

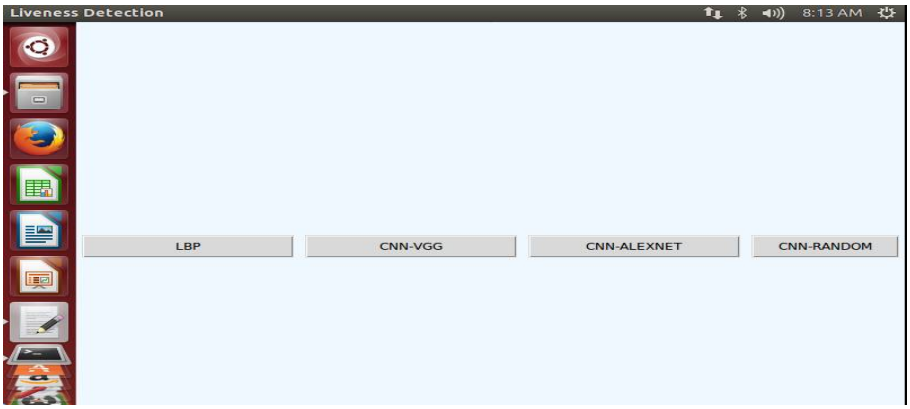


Fig.5 Livess detection system

Fig.5 shows the front page of liveness detection system, from this page it is directed to finerprint, face, iris type liveness detection.

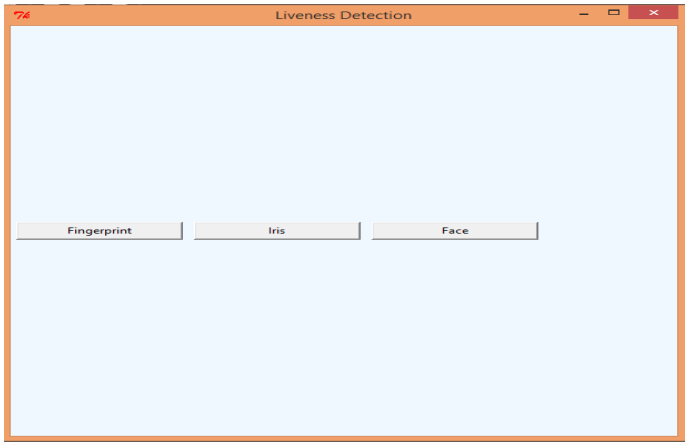
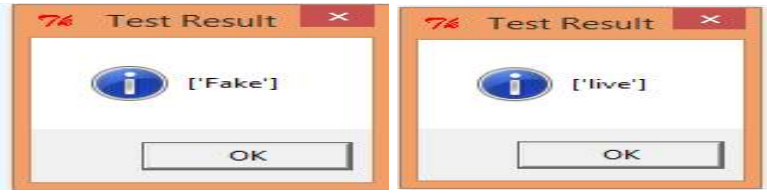


Fig.6 Biometric samples

Fig.6 shows the biometric sample selction page,choose the trait to find the liveness detection



(a) (b)

Fig. 7 (a) Recognizing fake trait (b) Recognizing live trait

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 4, April 2017

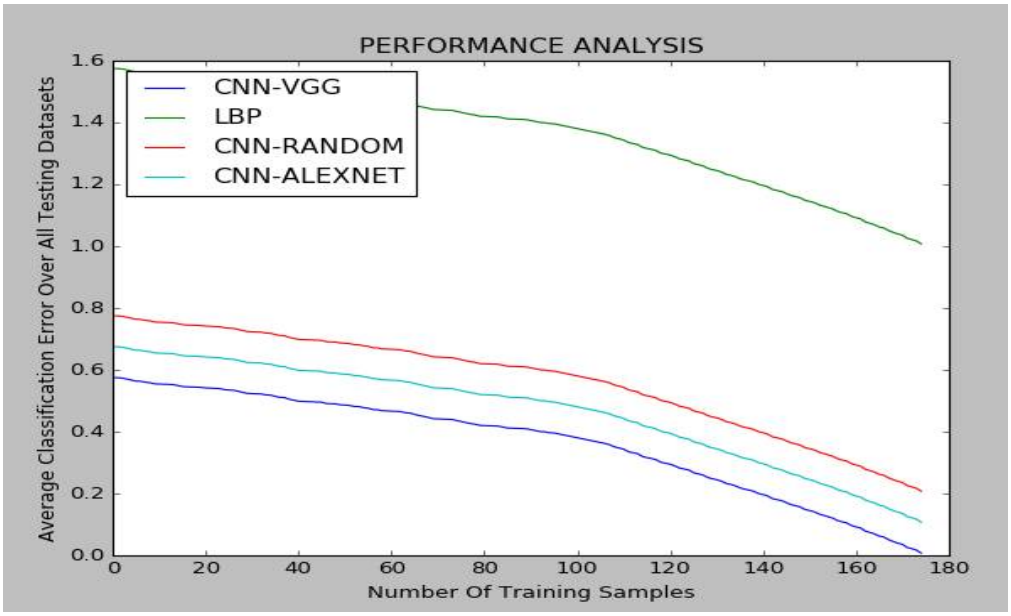


Fig. 8 Performance Analysis

Fig 8 shows the performance graph of various liveness detection system,and it is shows that the Cnn based systems are more accurate in liveness detection compared with the LBP based techniques.CNN-VGG showe low classification error compared to other models.

V. CONCLUSION

Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. .All the main techniques and functions in this liveness detection area are included in this paper. As shown in this paper, there are several different methods and techniques working against current presentation attack scenarios efficiently. Here it must be mentioned that none of these techniques provide an entire protection to biometric systems. Especially, the detection of video attacks is a particular challenge. As a consequence, a combination of different liveness detection techniques is strongly recommended. Moreover, there are several other detection techniques that should be used for detecting presentation attacks and protecting against manipulations of biometric systems to increase the overall security .A very good performing liveness detection system is not only capable of operating under different biometric systems (multibiometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). Inorder to overcome the shortcomings of already existing liveness detection tools,in this work we propose two different feature extraction techniques for software-based liveness detection: Convolutional Networks and Local Binary Patterns. Both techniques were used in conjunction with a Support Vector Machine (SVM) classifier.

REFERENCES

1. Maximilian Krieg,Nils Rogmann," Liveness Detection in Biometrics", BIOSIG international conference, November 2015.
2. P. D. Lapsley, J. A. Lee, D. F. Pare, Jr., and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," U.S. Patent 5737439, Apr. 7, 1998.

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 4, April 2017

3. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 360–373, Sep. 2006.
4. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in Advances in Biometrics. Heidelberg, Germany: Springer, 2005, pp. 265–272.
5. Y. N. Singh and S. K. Singh, "Vitality detection from biometrics: State-of-the-art," in Proc. World Congr. Inf. Commun. Technol., Dec. 2011, pp. 106–111.
6. Diogo Caetano Garcia,Ricardo L. de Queiroz, " Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015.
7. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, Feb. 2014.
8. Di Wen, Hu Han,Anil K. Jain, "Face Spoof Detection With Image Distortion Analysis", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015
9. David Menotti, Giovani Chiachia, Allan Pinto, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015.
10. Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, Fabio Roli" Fingerprint liveness detection using Binarized Statistical Image Features",IEEE 6 th International conference, Oct 2013.
11. Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva," An Investigation of Local Descriptors for Biometric Spoofing Detection", IEEE transactions on information forensics and security, vol. 10, no. 4, April 2015
12. 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