International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1797-1801 www.ijaem.net ISSN: 2395-5252

Fingerprint Liveliness Detection Using Image Processing – A Static Software Approach

Sanjeetha.U[1], Beema Jahaan K[2], Mrs.Umamaheswari.B[3], Mrs.Reena.R[4]

[1]Department of Computer Science Engineering, Prince Shri Venkateshwara Padmavathy Engineering College
[21]Department of Computer Science Engineering, Prince Shri Venkateshwara Padmavathy Engineering College
[31]Assisstant Professor,Department of Computer Science Engineering, Prince Shri Venkateshwara Padmavathy Engineering College
[41] Head of Department, Department of Computer Science Engineering, Prince Shri Venkateshwara Padmavathy Engineering College

Submitted: 05-06-2022 Revised: 17-06-2022 Accepted: 20-06-2022

ABSTRACT -Biometrics refers to “metrics related to human traits”. Biometric authentication is used in computer science as a part of identification, to spot individuals in groups that are under supervision. Fingerprint Identification System is the widely and frequently used biometric technique. Apart from other biometric traits like iris, face, palm, etc., fingerprint recognition is preferred due to the distinctive characteristics of fingerprint of every individual. This attribute makes it most dependable and chosen procedure amongst all other mechanisms. The fundamental intention of biometrics is to inevitably identify and distinguish threads in a genuine methodology. Fingerprint-based authentication systems have developed rapidly in the recent years. However, current fingerprint-based biometric systems are vulnerable to spoofing attacks. Moreover, single feature-based static approach does not perform equally over different fingerprint sensors and spoofing materials. We propose 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. We extract these features from a single fingerprint image to overcome the issues faced in dynamic software approaches, which require user cooperation and longer computational time.

KeyWords:biometrics, image processing, matlab, static software, fingerprint, liveliness

I. INTRODUCTION

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. This technology is primarily used for identification and access control, or for identifying people under surveillance. The basic premise of biometrics is that each person can be accurately identified by their unique physical or behavioral characteristics. Fingerprint authentication is a secure and simple security mechanism for various devices such as mobile phones andtablets.However,syntheticallyreproducible fingerprints are also identified. Fake fingerprints can be duplicated fromeveryday materials such as glue andclay materials. The recognition process can also be manipulated using raw synthetic fingerprints. Today, it's not difficult to find detailed instructions or instructions on how to create fake fingerprints. Distinguishing between real and fake fingerprints is called "spoofing detection". Due to the vulnerability, many fingerprint activity detection algorithms have been proposed and fall into two categories: hardware and software. The hardware approach adds specific devices to the sensor to detect properties such as blood pressure and skin

Distortion and smell. The software approach extracts from the fingerprint image the features used to distinguish between real and fake fingerprints.Image processing is a method of converting an image to a digital format and performing some operations on the image to get an expanded image or extract some useful information from it.Due to the vulnerabilities, many fingerprintliveness detection algorithms have been proposed and areclassified into two categories: hardware and software. In thehardware approach, a particular device will be added to thesensor to recognise the properties like blood pressure, skindistortion or odor. In the software approach, features used todiscriminate between real and spoof fingerprints are

extracted from the fingerprint image. In this paper, we have proposed a software based classification using KNN algorithm and Random Forest and a comparison is made with the existing SVM classifier.

II. RELATED WORK

1) LivDet 2013 fingerprint liveness detection competition 2013AUTHORS: L. Ghiani et al

A spoof or fake is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor Liveness detection distinguishes between live and fake biometric traits. Liveness detection is based on the principle that additional information can be garnered above and beyond the data procured by a standard verification system, and this additional data can be used to verify if a biometric measure is authentic. The Fingerprint Liveness Detection Competition (LivDet) goal is to compare both software-based (Part 1) and hardware-based (Part 2) fingerprint liveness detection methodologies and is open to all academic and industrial institutions. Submissions for the third edition were much more than in the previous editions of LivDet demonstrating a growing interest in the area. We had nine participants (with eleven algorithms) for Part 1 and two submissions for Part 2.

2) Fingerprint liveness detection using binarized statistical image features

AUTHORS: L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli

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. Although the number of approaches is large, none of them can be claimed as able to detect liveness of fingerprint traits with an acceptable error rate. In our opinion, in order to investigate at which extent this error can be reduced, novel feature sets must be proposed, and, eventually, integrated with existing ones. In this paper, 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. Experimental results on LivDet 2011 data sets appear to be encouraging and make this descriptor worth of further investigations.

3) Time-series detection of perspiration as a liveness test in fingerprint devices

AUTHORS: S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers

Fingerprint scanners may be susceptible to spoofing using artificial materials, or in the worst case, dismembered fingers. An anti-spoofing method based on liveness detection has been developed for use in fingerprint scanners. This method quantifies a specific temporal perspiration pattern present in fingerprints acquired from live claimants. The enhanced perspiration detection algorithm presented here improves our previous work by including other fingerprint scanner technologies; using a larger, more diverse data set; and a shorter time window. Several classification methods were tested in order to separate live and spoof fingerprint images. The dataset included fingerprint images from 33 live subjects, 33 spoofs created with dental material and Play-Doh, and fourteen cadaver fingers. Each method had a different performance with respect to each scanner and time window. However, all the classifiers achieved approximately 90% classification rate for all scanners, using the reduced time window and the more comprehensive training and test sets.

4) Liveness and spoofing in fingerprint identification: Issues and challenges

AUTHORS: M. Sepasian, C. Mares, and W. Balachandran

The fingerprint liveness detection refers to the inspection of the finger characteristics to ensure whether the input finger is live or artificial. A number of fingerprint identification systems are used widely and implemented at various important places such as border and immigration services. However, it is not declared by the manufacturers of these systems whether liveness detection is actually implemented. Possible measures to detect liveness are only proposed in patents and published literature. There are three major schemes, which are reported in fingerprint liveness literature. These coupled with the additional hardware, software, or combination of fingerprint with other identifications is aimed to verify the liveness in submitted fingerprints. The hardware-based methods use auxiliary sensors to detect the biological and physiological measurements from finger, whereas software-based methods utilize changes in physical properties that take place in early stages of pressing the finger. In this paper, various fingerprint liveness detection methods, which are categorized as voluntary and involuntary, are explored. These categories are based on determining the presence of a user by different responses from either voluntary (e.g. passwords or multiple biometrics) or involuntary (e.g. pulse oximetry or blood pressure) liveness detections. The main objective of this paper is to critically review the voluntary and involuntary fingerprint liveness detection techniques proposed in the literature, and discuss their effectiveness and possible limitations.

5) Fake fingerprint detection by odor analysis
AUTHORS: D. Baldisserra, A. Franco, D. Maio, and D. Maltoni

This work proposes a novel approach to secure fingerprint scanners against the presentation of fake fingerprints. An odor sensor (electronic nose) is used to sample the odor signal and an ad-hoc algorithm allows to discriminate the finger skin odor from that of other materials such as latex, silicone or gelatin, usually employed to forge fake fingerprints. The experimental results confirm the effectiveness of the proposed approach.

III. PROPOSED SYSTEM

There are Various methods that are used for fingerprint liveness Detection. It is very difficult to distinguish a fake fingerprint from a real fingerprint. The convolutional methods lack accuracy. The features extracted are insufficient to performthe test. The existing system is a approach for distinguishing a spoof fingerprint from a real fingerprin which uses LBP feature extraction method along with HOG feature extraction improves the accuracy.Apart from SVM, in this paper the Random Forest method is also used. The system accuracy is checked by performing training and classification using both SVM and Random Forest method. The proposed system shows the comparison of result obtained by SVM with K-NN algorithm. It is observed that Random Forest Method provides more accuracy than using KNN. The Proposed system is evaluated on the datasets provided by LivDet (Liveness Detection) . This work consists of following modules.They are

Image Acquisition:

Image acquisition in image processing can be broadly defined as the action of retrieving an image from some source, usually a hardware-based source, so it can be passed through whatever processes need to occur afterward. Performing image acquisition in image processing is always the first step in the workflow sequence because, without an image, no processing is possible. The image that is acquired is completely unprocessed and is the result of whatever hardware was used to generate it, which can be very important in some fields to have a consistent baseline from which to work.

Preprocessing:The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing.We enhanced the quality of the image by first cropping the fingerprint region in the image and median filtering is then applied on the cropped images without reducing the sharpness of the input image. Finally, histogram equalization is performed to improve the contrast in the image by diversifying the intensity range over the whole cropped image. The output achieved after this stage is an image with a reduced noise and improved definition of the ridge structure.

Feature Extraction:

In fingerprint authentication systems, the image is usually captured from multiple subjects using 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. In our work, we choose to use SURF as it is invariant to illumination, scale and rotation. SURF is also used because of its concise descriptor length. While SURF is invariant to object orientation and scale transformation, it is not invariant to geometric transformations. Hence, in order to compensate the limitations of SURF, PHOG descriptors are used to extract local shape information to obtain more discriminative features. In addition, Gabor wavelet features are also incorporated for texture analysis.

Feature Reduction using PCA:

Excessive features increase computation times and storage memory. Furthermore, they sometimes make classification more complicated, which is called the curse of dimensionality. It is required to reduce the number of features. PCA is an efficient tool to reduce the dimension of a data set consisting of a large number of interrelated variables while retaining most of the variations. It is achieved by transforming the data set to a new set of ordered variables according to their variances or importance.

Classification:The classification process is done over the extracted features. The main novelty here is the adoption of K-Nearest Neighbor and Random Forest. RF and KNN classifier is applied over the features and the classification is done. The following figure shows the work flow of the proposed system.

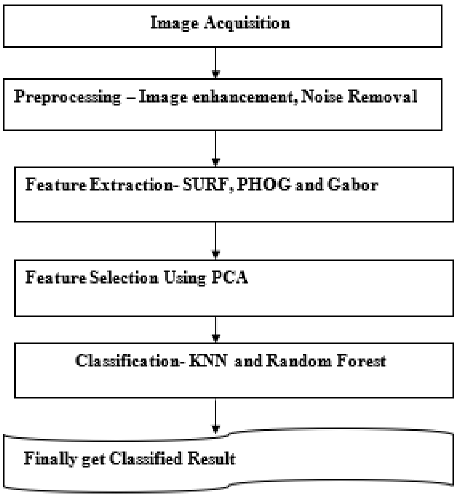


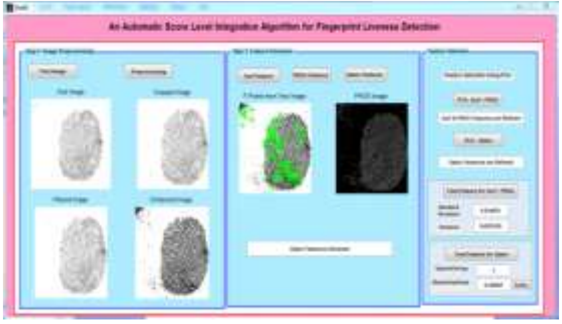
Image Acquisition
Preprocessing – Image enhancement, Noise Removal
Feature Extraction- SURF, PHOG and Gabor
Feature Selection Using PCA
Classification- KNN and Random Forest
Finally get Classified Result

IV. EXPERIMENTAL ANALYSIS AND RESULT

The experimental results of the proposed technique for Fingerprint liveliness detection using k-NN classification is Discussed in this section. A static software approach is created using MATLAB application to implement this technique. This proposed system also shows the comparison between the accuracy of existing SVM classification and our system.

RESULT

The algorithm discussed above is implemented using MatLab2013a. In this proposed work, we basically use a fingerprint image as input. By processing this image, the system produces a result whether it is real or spoof. And in the next module, the accuracy comparison will be shown. The following image is the screenshot of the output.


An Automatic Score Level Integration Algorithm for Fingerprint Liveness Detection

An Automatic Score Level Integration Algorithm for Fingerprint Liveness Detection

ANALYSIS

The analysis of the proposed system is performed on the basis of accuracy. Accuracy is computed by comparing the results obtained with the ground truth images. The graph is given for both the accuracy of existing and proposed system.

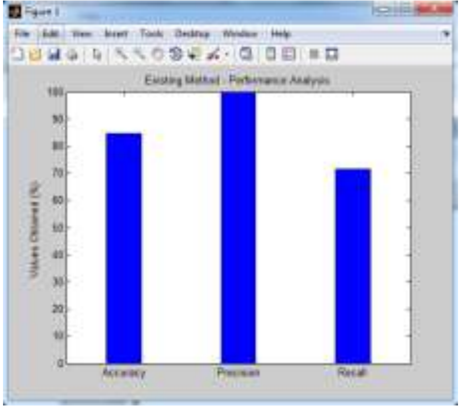


Figure: Performance analysis of existing system

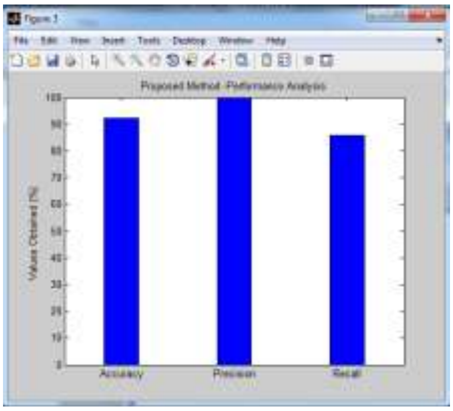


Figure: Performance analysis of Proposed system

V. CONCLUSION

In this paper, we proposed a novel method for fingerprint liveness detection by combining low level features, which includes gradient features from SURF, PHOG, and texture features from Gabor wavelet. In addition, an effective dynamic score level integration module is proposed to combine the result from the two individual classifiers. We carried out experiments on two most popularly used databases from LivDet competition 2011 and 2013. In depth comparison is done with the current state of the art, and the winner of LivDet 2011 and 2013 fingerprint liveness detection competition. ACE rate of 2.27% in comparison to the 12.87% of the 2013 LivDet competition winner is a significant performance gain.

REFERENCES

[1]. L. Ghiani et al., “LivDet 2013 fingerprint liveness detection competition 2013,” in Proc. Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.

[2]. 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.

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

[4]. S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, “Time-series detection of perspiration as a liveness test in fingerprint devices,” IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 35, no. 3, pp. 335–343, Aug. 2005.

[5]. 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]. Available: http://dl.acm.org/citation.cfm?id=1808102.1808130.

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

[7]. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, “Fake fingerprint detection by odor analysis,” in Advances in Biometrics (Lecture Notes in Computer Science), vol. 3832, D. Zhang and A. Jain, Eds. Berlin, Germany: Springer, 2005, pp. 265–272. [Online]. Available:http://dx.doi.org/10.1007/11608288_36.

[8]. P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, “A new antispoofing approach for biometric devices,” IEEE Trans. Biomed. Circuits Syst., vol. 2, no. 4, pp. 328–337, Dec. 2008.

[9]. S. A. C. Schuckers, “Spoofing and anti-spoofing measures,” Inf. Secur. Tech. Rep., vol. 7, no. 4, pp. 56–62, 2002.

[10]. D. Yambay, L. Ghiani, P. Denti, G. Marcialis, F. Roli, and S. Schuckers, “LivDet 2011—Fingerprint liveness detection competition 2011,” in Proc. 5th IAPR Int. Conf. Biometrics (ICB), Mar./Apr. 2012, pp. 208–215.