ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

A Novel Approach for Fingerprint Liveness Detection Using Multi Features

Meda Sanjeeva Naga Abhinay[1], S.Aruna M.Tech[2]

M.Tech Student DECS, Dept. of ECE, Shri Shirdi Sai Institute of Science & Engineering, Affiliated to JNTUA, India[1]

Associate Professor, Dept. of ECE, Shri Shirdi Sai Institute of Science & Engineering, Affiliated to JNTUA, India[2]

Abstract: Fingerprints are good basis for individual identification by biometric authentication. Password based authentication systems are less secure than that of the fingerprint authentication where fingerprints and Iris are unique for every Individual. With the emerging use of biometric authentication systems in the past years, spoof fingerprint detection has become increasingly important. In this work, a static software approach is developed. This new method is suggested to unite low-level gradient features from speeded-up robust features, pyramid conservatory of the histograms of oriented gradient and texture features from Gabor wavelet by employing dynamic score level integration. These features are extracted from a single fingerprint image to resolve the problems faced in dynamic software methods, which needs user collaboration as well as longer computational time. An investigational study done on LivDet 2011 data generated an average equal error rate (EER) of 3.86% over four databases.

KEYWORDS*:* Fingerprint liveness, low level features, Gaborfilters.

I. INTRODUCTION

Biometrics authentication system refers to the identity identification based on their physiological and behavioural characteristics. Therefore, biometric recognition systems are commonly used for authentication in various security applications.The ability of fingerprint authentication system to discriminate whether the fingerprint samples presented are really from a live finger tip or spoofed one, which is called liveness detection. In order to prevent spoofing, many kinds of detection methods have been proposed in recent years. The advantage of using biometrics for authentication purpose comes from the unique features of each individual. Iris and fingerprints are unique for every human. Fingerprints are most generally used for numerous security systems due to the high-level accuracy and users convenience. Nowadays, such fingerprints are used to a key application, e.g., payment, on mobile devices by the small size of fingerprint sensors. Even though the high-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. To address this drawback, early studies have explored spatial characteristics of ridges and valleys within the fingerprint. Fingerprint liveness detection has been an active research topic over the last several years. It has been proven that it is possible to spoof. As illustrated in Fig. 1, we observe that it is very difficult to visually differentiate between live and fake fingerprints.The possibility to spoof a fingerprint based authentication system creates the need to develop a method which can distinguish between live and fake fingerprint images. Both hardware and software based approaches can be used to solve this problem.However, hardware based approaches require additional devices to measure finger temperature, odor, pulse, oxiometry etc. In addition, hardware based approaches are typically costlier due to the additional sensors required.

II. RELATED WORK

1) B. Tan and S. Schuckers, “Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise,”
Biometric fingerprint scanners are positioned to provide improved security in a great span of applications from government to private. However, one highly publicized vulnerability is that it is possible to spoof a variety of fingerprint scanners using artificial fingers made from Play-Doh, gelatin and silicone molds. Therefore, it is necessary

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

to offer protection for fingerprint systems against these threats. In this paper, an anti-spoofing detection method is proposed which is based on ridge signal and valley noise analysis, to quantify perspiration patterns along ridges in live subjects and noise patterns along valleys in spoofs. The signals representing gray level patterns along ridges and valleys are explored in spatial, frequency and wavelet domains. Based on these features, separation (live/spoof) is performed using standard pattern classification tools including classification trees and neural networks. We test this method on a larger dataset than previously considered which contains 644 live fingerprints (81 subjects with 2 fingers for an average of 4 sessions) and 570 spoof fingerprints (made from Play-Doh, gelatin and silicone molds in multiple sessions) collected from the Identix fingerprint scanner. Results show that the performance can reach 99.1% correct classification overall. The proposed anti-spoofing method is purely software based and integration of this method can provide protection for fingerprint scanners against gelatin, Play-Doh and silicone spoof fingers.
2) D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Fingerprint liveness detection based on weber local image descriptor,”
In this paper, we investigate the use of a local discriminative feature space for fingerprint liveness detection. In particular, we rely on the Weber Local Descriptor (WLD), which is a powerful and robust descriptor recently proposed for texture classification. Inspired by Weber's law, it consists of two components, differential excitation and orientation, evaluated for each pixel of the image. Joint histograms of these components are then processed to build the discriminative features used to train a linear kernel SVM classifier. Experimental results with different databases and different sensors show WLD to perform favorably compared to the state-of-the-art methods in fingerprint liveness detection. In addition, by combining WLD with LPQ (Local Phase Quantization) results further improve significantly.
3) G. L. Marcialis*et al.*, “First international fingerprint liveness detection competition—LivDet 2009,”
Fingerprint recognition systems are vulnerable to artificial spoof fingerprint attacks, like molds made of silicone, gelatin or Play-Doh. "Liveness detection", which is to detect vitality information from the biometric signature itself, has been proposed to defeat these kinds of spoof attacks. The goal for the LivDet 2009 competition is to compare different methodologies for software-based fingerprint liveness detection with a common experimental protocol and large dataset of spoof and live images. This competition is open to all academic and industrial institutions which have a solution for software-based fingerprint vitality detection problem. Four submissions resulted in successful completion: Dermalog, ATVS, and two anonymous participants (one industrial and one academic). Each participant submitted an algorithm as a Win32 console application. The performance was evaluated for three datasets, from three different optical scanners, each with over 1500 images of "fake" and over 1500 images of "live" fingerprints. The best results were from the algorithm submitted by Dermalog with a performance of 2.7% FRR and 2.8% FAR for the Identix (L-1) dataset. The competition goal is to become a reference event for academic and industrial research in software-based fingerprint liveness detection and to raise the visibility of this important research area in order to decrease risk of fingerprint systems to spoof attacks.
4) H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, “Speeded-up robust features (SURF),”
This article presents a novel scale- and rotation-invariant detector and descriptor, coined SURF (Speeded-Up Robust Features). SURF approximates or even outperforms previously proposed schemes with respect to repeatability, distinctiveness, and robustness, yet can be computed and compared much faster.
This is achieved by relying on integral images for image convolutions; by building on the strengths of the leading existing detectors and descriptors (specifically, using a Hessian matrix-based measure for the detector, and a distribution-based descriptor); and by simplifying these methods to the essential. This leads to a combination of novel detection, description, and matching steps.
The paper encompasses a detailed description of the detector and descriptor and then explores the effects of the most important parameters. We conclude the article with SURF’s application to two challenging, yet converse goals: camera calibration as a special case of image registration, and object recognition. Our experiments underline SURF’s usefulness in a broad range of topics in computer vision.

III.EXISTING SYSTEM

In existing system, a user is only required to place his/her finger on the sensor for a short duration in an undedicated way for a single image capture. Most of the works in fingerprint liveness detection use a single feature based approach. A single feature set from a single classifier is insufficient to perform similarly over different databases which are recorded using different fingerprint sensors. This is because different sensors capture information differently.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

In addition, various materials such as gelatin based fake fingerprint may not produce similar features as compared to other materials such as latex, play-doh or wood-glue. This is because fake fingerprints exhibit different intensity gradient and ridge shape due to the thickness of material used.

IV. PROPOSED SYSTEM

In this paper, we propose a method to overcome the limitations faced in the static software based approaches where a single feature set fails to perform equally over different fingerprint sensors and materials.
Our methodology extracts low level textural and gradient information for fingerprint liveness detection from a single image. We propose the use of SURF features in combination with PHOG to obtain gradient features that discriminate well between fake and live fingerprint images. SURF features have a concise descriptor length which is compact and takes less computational time as compared to LBP. In addition, SURF is also invariant to scale and image rotation.
PHOG feature descriptor extracts intensity gradient and edge directions to describe the shape and appearance in an image. The PHOG extractor is also invariant to geometric and photometric transformation. Thus, combination of SURF and PHOG enables our method to perform similarly over various sensors and materials.
In order to obtain textural features, we propose the use of Gabor wavelets as they have optimal localization properties in both the frequency and spatial domain. They extract discriminative ridge feature maps and have performed well in discriminating between live and fake fingerprint images.

V. SYSTEM ARCHITECTURE

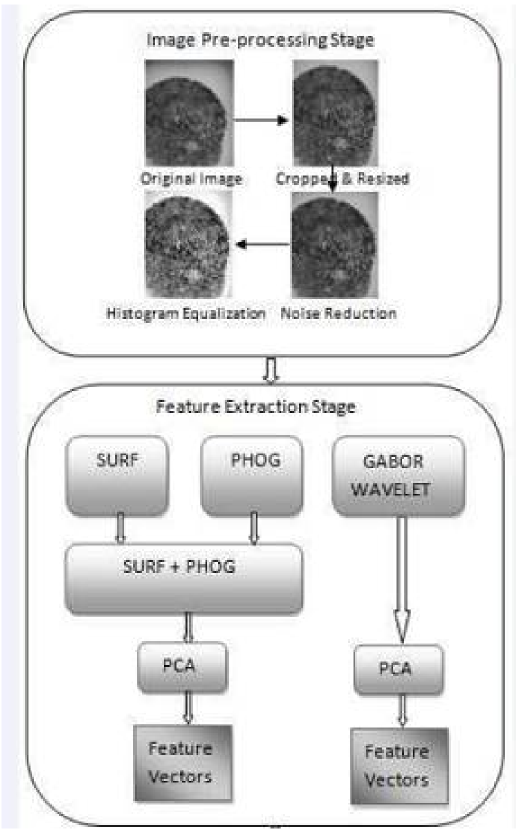


Fig 1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

VI. IMPLEMENTATION

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 SVM and Random Forest. RF and SVM classifier is applied over the features and the classification is done.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

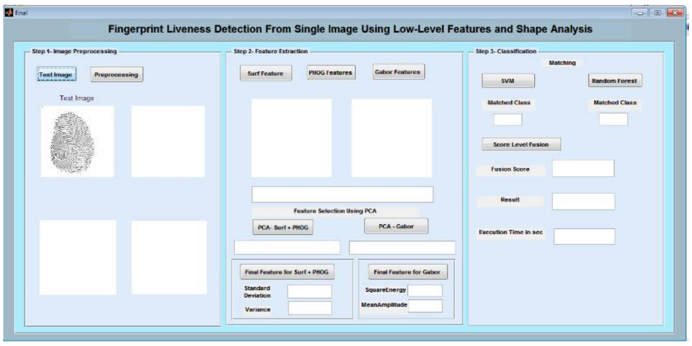
International Journal of Innovative Research in Computer and Communication Engineering

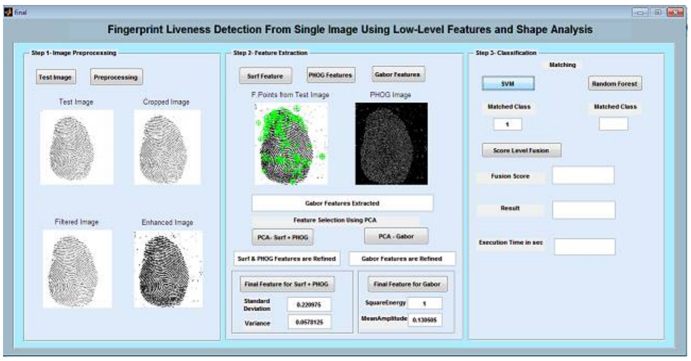
(A High Impact Factor, Monthly, Peer Reviewed Journal)

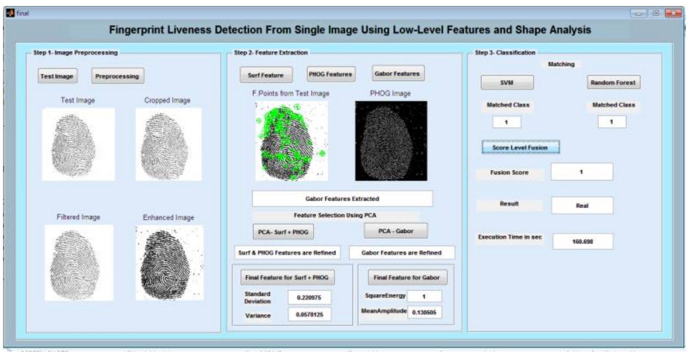
Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

VII. SIMULATION RESULTS







ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

VIII. CONCLUSION

I 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. The proposed method scored consistently low EER over all the six sensors which were not observed in the state of the art methods.

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. Institutionenförsystemteknik, 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.