International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Novel Approach for Fingerprint Liveness Detection Using Gradient and Texture Features

P. Shanthi[1], R. Madhumathi[2]

[1]Research Scholar, Department of Computer Science, Sakthi college of Arts and Science For Women, oddanchatram, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science, Sakthi college of Arts and Science For Women, oddanchatram, Tamil Nadu, India

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 paper, we propose a static software approach that combines all sorts of fingerprint features. Initially, we extract the features of the fingerprint image using Gabor wavelet feature process. The extracted features are then aligned with histogram process. Each extracted features are preserved with dynamic score level integration. This dynamic approach consumes higher computational time. It has been experimented on the LivDet 2011 dataset which proves the efficiency of our proposed system. These have shown the classification rate of 9.625% with reduced error rate of 2.27%.

Keywords: Fingerprint liveness, low level features, Gabor filters, texture analysis, Biometric Security.

I. INTRODUCTION

Biometrics is burlier authentication system in the domain of security. Fingerprints are intrinsic to persons and can neither be lost nor stolen which makes it highly truthful and trustworthy. Furthermore, the accessibility of low-cost fingerprint readers united with easy integration capabilities has led to the broad spread use of fingerprint biometrics in a diversity of organizations. An organization can have unlimited benefits by appropriately deploying biometric technology. Today's economy is a developing one and technological progressions have altered the system in which organizations function and conduct businesses. Recent organizations require being adaptive, flexible and responsive to endure in the competitive business surroundings. Fingerprint technology can promote organizations in a diversity of segments e.g. health care, government, retail enterprises, technology organizations, manufacturing industry, libraries, universities etc Employee identification and workforce management becomes faster, exact and more proficient with fingerprint technology [1]. Different magnetic strip cards or passwords, individuals constantly carry their fingerprints with them and they cannot be misplaced or elapsed. Tracking attendance of employees in industrialized organizations checks employee time thievery and diminish deceptive behavior. A biometric system facilitate automated calculation of employee hours therefore sinking paper expenditure and time exhausted in manual settlement of attendance data.

Fingerprint biometrics can give both physical access to company buildings and logical access to internal

resources such as enterprise computers and systems. Governments and private organizations, institutes everywhere in the world are opting biometric technology to contest identity fraud and security breaches, secure confidential data, and reduce costs and to develop overall user understanding. Biometrics is one of the quickly emerging eras in the information technology segment with fingerprint recognition anticipated to stay put the most leading form of biometric technology [2]. Fingerprint liveness detection has been a vigorous research area in excess of the previous several years. It has been confirmed that it is achievable to spoof standard optical and capacitive sensors .The possibility to spoof a fingerprint based authentication system generates the necessity to grow a method which can differentiate between live and fake fingerprint images.

Biometric technology presents numerous advantages over classical security methods based on moreover some information (PIN, Password, etc.) or physical devices e.g. key, card, etc. Though, providing to the sensor a fake physical biometric can be a simple mode to overhaul the system's security. Fingerprints, in particular, can be simply spoofed from ordinary resources, such as gelatin, silicone, and wood glue. Consequently, a protected fingerprint system should discriminate properly a spoof from an authentic finger. Several fingerprint liveness detection algorithms have been developed, and they can be widely divided into two approaches: Hardware and Software approach [3]. In the hardware approach a particular device is added to the sensor sequentially to detect exacting properties of living aspects such as the blood pressure, skin distortion or the odor. In the software approach, which is used in this work, fake characters are detected once the sample has been obtained with a standard sensor. Additionally, hardware based approaches are usually more costly due to the added sensors essential; next to, they need an end user to cooperate with the extra hardware. Alternatively, software based approaches do not utilize extra persistent biometric dimensions. However, these approaches are more demanding as they need the identification of distinguishable features to discriminate between live and fake fingerprint images.

Software based approaches are additionally separated generally into dynamic and static based approaches. Dynamic software based approaches necessitate a minimum of two time series images ensuing in added computational time. So, the hardware approach would be costly but less secure and software approach is complicated to construct an algorithm which can distinguish different features between fake and live fingerprint. Software algorithm is a demanding approach and important method for fingerprint liveness detection. Because of human mistake fraud cases have turn into common and the fake fingerprint that has been prepared by the gelatin or latex will have more strength of edges in compare of live fingerprint which in some way acquires simple access to authentication systems. To decrease the limitations of the software based fingerprint authentication, we developed a static software approach in which the algorithm extracts features which are exclusive for each and every person. The extracted features from a fingerprint image can be specified as SURF, PHOG and gabor wavelet. These features are resolute to distinguish between fake and live fingerprints. The Gabor wavelets demonstrate optimal properties in both frequency and spatial domain which consecutively diminish the human based errors in the authentication systems [4].

II. STATEMENT OF THE PROBLEM

In this research, a method is proposed to overcome the restrictions faced in the static software based approaches where a single feature set unsuccessful to execute uniformly in excess of dissimilar fingerprint sensors and materials. This methodology extracts low level textural and gradient information for fingerprint liveness detection from a single image. It proposes the use of SURF features in amalgamation with PHOG to acquire gradient features that

distinguish well between fake and live fingerprint images. SURF features have a brief descriptor length which is dense and consumes less computational time in compare to LBP. Additionally, SURF is also invariant to scale and image rotation. PHOG feature descriptor extracts intensity gradient and edge directions to explain the shape and manifestation in an image. The PHOG extractor is also invariant to geometric and photometric transformation. Therefore, grouping of SURF and PHOG facilitate this method to execute likewise over a variety of sensors and materials.

Consecutively to acquire textural features, we suggest 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 discerning between live and fake fingerprint images.

- ✓ To the best of our knowledge, the suggested method is one of the only some work that executes well over a large open source dataset generated using six dissimilar sensors and six dissimilar materials. In this work, we examine the use of local distinguishable feature space on live and spoof fingerprints by using PHOG, SURF, GABOR and their amalgamation.
- ✓ Experiments executed on six sensors express that the amalgamation of PHOG and SURF always works better than PHOG and SURF individually for LivDet 2011 and 2013 databases. This specifies that these descriptors accompaniment each other. Also, the amalgamation of PHOG and SURF feature vector generates a strong distinguishable feature vector which executes extremely well in the area of fingerprint liveness detection.
- ✓ Unlike, LivDet 2013 competition winner and other top four teams which do not execute well on Crossmatch sensor, this method executes extremely well on Crossmatch sensor generating an average classification error of 2.5% in compare of 31.20% obtained in LivDet 2013 fingerprint competition.
- ✓ The proposed method is entirely software based and it is computationally not expensive, rapid and flexible for future adaptations. This method can be organized in real-time applications. At last, the outcome accomplished by this method does better the state of the art appreciably.

III. SCOPE OF THE RESEARCH

Biometric sensors are broadly employed to distinguish between particular ones that are allowed to involve in an activity and individuals that are not allowed to involve in that activity. For e.g., fingerprint sensors are generally utilized to find out whether a fingerprint provided by an individual matches information in a database, and if a match is find out, then the individual may be allowed to involve in an activity. For e.g. the individual may be permitted to go into a building or room or permissible to utilize an electronic device like as a mobile phone or an application running on a mobile device. Biometric sensors can be mislead and thus authorize an illegal individual to employ in an activity that is kept back for legal individuals. Spoofing a fingerprint sensor may be achieved in dissimilar ways. These consist of via a fake fingerprint, with body parts other than a finger, and by means of a dead finger from a person. While it is improbable that the exacting type of spoofing to be utilized on a fingerprint sensor will be recognized in proceed, it is significant to guard alongside all types of spoofs. As increasingly biometrics is utilized for user identification and/or verification, liveness detection becomes gradually more vital in turn to make sure admission security and correctness. Liveness detection is significant since a lot of methods of misleading an identification system and/or verification system make use of spoofs that are not alive. For e.g. a latex finger may be made to have ridges and valleys like a fingerprint of a legal user.

IV. METHODOLOGY

Image Acquisition: Image acquisition in image processing can be widely defined as the action of retrieving an image from a few sources, generally a hardware-based source, thus it can be accepted during whatever processes require to come about later. Performing image acquisition in image processing is all the time, the primary step in the workflow sequence because, exclusive of an image, no processing is achievable. The image that is attained is entirely unprocessed and is the result of whatever hardware was used to produce it, which can be very significant in some areas to have a reliable baseline from which to work.

Preprocessing: The objective of pre-processing is an enhancement of the image data that contains unnecessary distortions or improves some image features significant for additional processing. We improved the quality of the image by first cropping the fingerprint region in the image and median filtering is afterward applied on the cropped images devoid of diminishing the sharpness of the input image. To end with, histogram equalization is carried out to advance the compare of the image by expanding the intensity range over the entire cropped image. The output achieved after this stage is an image with a condensed noise and enhanced description of the ridge structure.

Feature Extraction: In fingerprint authentication systems, the image is generally captured from various subjects by using the dissimilar scanners. Hence, fingerprint images are usually obtained to be of dissimilar scales and rotations. In definite circumstances, the fingerprint images are partly captured caused by human errors. Sequentially to acquire features that are invariant to these troubles, various features use which capture properties of live fingerprint images. In this work, we decide to employ SURF as it is invariant to enlightenment, scale and rotation. SURF is also utilized because of its brief descriptor length. Although SURF is invariant to object orientation and scale transformation, it is not invariant to geometric transformations. Therefore, sequentially to recompense the restrictions of SURF, PHOG descriptors are used to extract local shape information to achieve more distinguishable features. Additionally, Gabor wavelet features are also integrated for texture analysis.

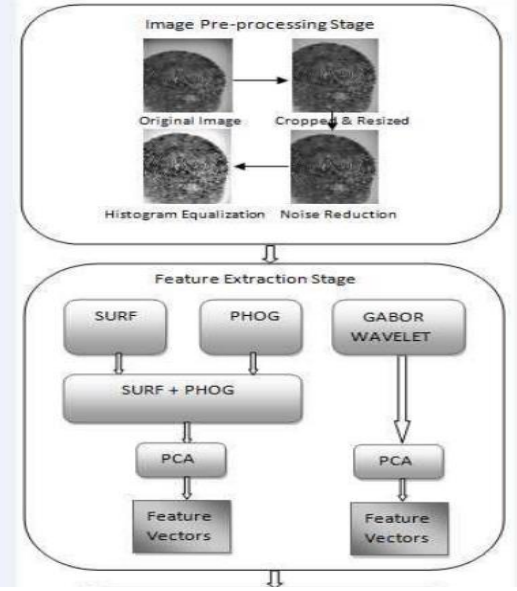

Figure – 1: : System architecture of the proposed Method

Feature Reduction using PCA: Extreme features increase computation times and storage memory. Moreover, from time to time they make classification more difficult that is called the curse of dimensionality. It is necessary to decrease the number of features. PCA is an efficient tool to diminish the measurement of a data set comprising of a large number of consistent variables although keeping most of the variations. It is accomplished by transforming the data set to a novel set of prearranged variables according to their variances or importance.

Classification: The classification procedure is done over the extracted features. Here, main innovation is the acceptance of SVM and Random Forest. RF and SVM classifier is applied over the features and the classification is done.

V. EXPERIMENTAL RESULTS

5.1 Importing and Exporting Images

Image Processing Toolbox chains images produced by a broad range of devices, containing digital cameras, satellite and airborne sensors, medical imaging devices, microscopes, telescopes, and other scientific instruments. It may visualize, analyze, and process these images in various data types, containing single- and double-precision floating-point and signed and unsigned 8-, 16-, and 32-bit integers. There are numerous modes to import and export images into and out of the MATLAB background for processing. Image Acquisition Toolbox can be used to obtain live images from Web cameras, frame grabbers, DCAM-compatible cameras, and other devices. Using Database Toolbox, images can be accessed which are stored in ODBC/JDBC-compliant databases.

5.2 Displaying and Exploring Images

Image Processing Toolbox expands MATLAB graphics to offer image display capabilities which are extremely customizable. It can construct displays with multiple images in a single window, interpret displays with text and graphics, and create specialized displays e.g. histograms, profiles, and contour plots. Additionally, to display functions, the toolbox provides a suite of interactive tools for exploring images and building GUIs.

5.3 Preprocessing and Post Processing Images

Image Processing Toolbox supports reference-standard algorithms for preprocessing and post-processing responsibilities that resolve frequent system problems, e.g. interfering noise, low dynamic range, out-of-focus optics, and the dissimilarity in color demonstration between input and output devices.

Image enhancement techniques in Image Processing Toolbox assist to improve the signal-to-noise ratio and accentuate image features by altering the colors or intensities of an image. It can:

- ✓ Perform histogram equalization
- ✓ Perform decorrelation stretching
- ✓ Remap the dynamic range
- ✓ Adjust the gamma value
- ✓ Perform linear, median, or adaptive filtering

5.4 Analyzing Images

Image Processing Toolbox gives a widespread collection of reference-standard algorithms and graphical tools for image analysis tasks e.g. statistical analysis, feature extraction, and property measurement.

Statistical functions analyze the common characteristics of an image by:

- ✓ Computing the mean or standard deviation
- ✓ Determining the intensity values along a line segment
- ✓ Displaying an image histogram
- ✓ Plotting a profile of intensity value

Edge-detection algorithms identify object boundaries in an image. These algorithms contain the Sobel, Prewitt, Roberts, Canny, and Laplacian of Gaussian methods. The dominant Canny method can detect true weak edges without being "fooled" by noise.

5.5 Working with Large Images

Few images are outsized that they are complicated to process and display with standard methods. Image Processing Toolbox offers exact workflows for working with larger images than or else possible. Devoid of loading a large image completely into memory, can create a reduced-resolution data set (R-Set) that partitioned an image into spatial tiles and resample the image at dissimilar resolution levels. This workflow develops performance in image display and navigation. A block processing workflow can be used to apply a function to each distinct block of a large image that considerably reduces use of memory.

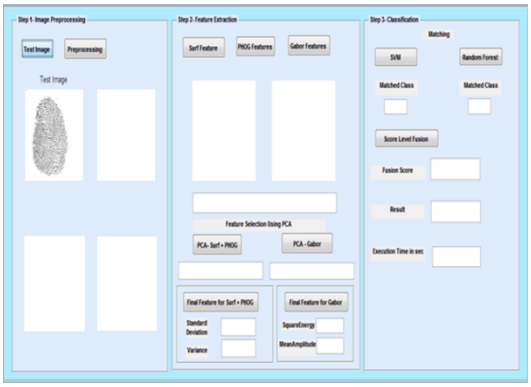

Figure 2. Input image

Figure 2 shows the collection of Test Image. This image will be used for preprocessing.

Figure 3. Image Preprocessing

Figure 3 depicts the preprocessing of the images. By Image Preprocessing we found the preprocessed Images e.g. Test Image, filtered image, cropped image, Enhanced image.

Figure 4.. Extraction of Gradient Features from SURF

The above figure 4.3 depicts the Extraction of gradient Features from SURF. After Preprocessing of the Input image, SURF features are extracted from preprocessed image.

Figure 5. Extraction of gradient features from PHOG

Figure 5 depicts the Extraction of gradient features from PHOG. After extracting the SURF features the features are extracted from PHOG.

Figure 6. Extraction of texture features from Gabor

Figure-6 depicts the Extraction of texture features from Gabor wavelet. After extracting the PHOG features the Gabor features are extracted.

Figure 7. Feature selection process using PCA method by combining SURF and PHOG features.

Figure 7 depicts the feature selection process. To perform this, we have used PCA method for selecting optimal features.

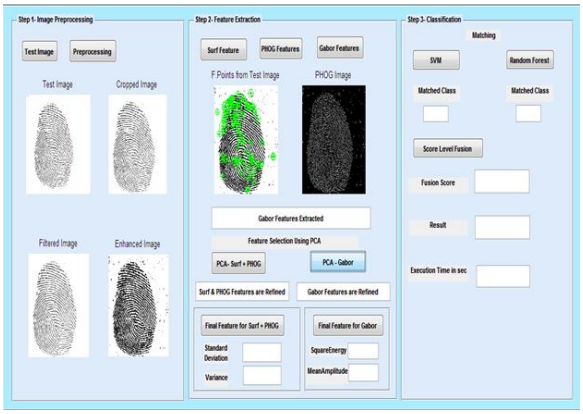

Figure 8. Feature selection process using PCA – Gabor

Figure 8 depicts the feature selection process using PCA- Gabor method. After selecting the optimal features using PCA with SURF and PHOG, to perform this, we have used PCA method with Gabor features.

Figure 9. Final Feature extraction for SURF and PHOG

Figure 9 depicts the Final feature for SURF and PHOG. After finding the optimal features we have found the Final feature for surf and PHOG.

Figure 10. Final feature extraction for Gabor

Figure 10 depicts the final feature for Gabor. After extracting the final feature for SURF and PHOG we found the final feature for Gabor method.

VI. CONCLUSION

A new technique for fingerprint liveness detection by combining low level features is developed which comprises gradient features from SURF, PHOG, and texture features from Gabor wavelet. Additionally, an efficient dynamic score level integration module is developed to unite the outcome from the two individual classifiers. Experiments are carried out on two most commonly used databases from LivDet competition 2011 and 2013. In detail 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 an important concert gain. The proposed method scored constantly low EER on the whole six sensors which were not experiential in the state of the art techniques.

VII. REFERENCES

[1]. Manju Kulkarni, Harishchanddra Patil "Liveness detection in fingerprint recognition technique using first order texture features" IJAET/Vol.II/ Issue IV/October-December, 2011.

[2]. Ana F. Sequeira and Jaime S. Cardoso "Fingerprint Liveness Detection in the

Presence of Capable Intruders" Sensors 2015, 15, 14615-14638; doi:10.3390/s150614615.

[3]. Sajida Parveen et. al. "Face anti-spoofing methods" current science, vol. 108, no. 8, 25 April 2015.

[4]. Emanuela Marasco and Arun Ross "A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems" ACM Comput. Surv. 47, 2, Article A, September 2014. DOI:http://dx.doi.org/10.1145/0000000.0000000

[5]. Y. Chung and M. Yung "Fingerprint Liveness Detection Based on Multiple Image Quality Features" LNCS 6513, pp. 281–291, Springer-Verlag Berlin Heidelberg 2011

[6]. Yujia Jiang and Xin Liu "Spoof Fingerprint Detection based on Co-occurrence Matrix" International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.8 (2015), pp.373-384 http://dx.doi.org/10.14257/ijsip.2015.8.8.38

[7]. Athos Antonelli et. al. "Fake Finger Detection by Skin Distortion Analysis" Ieee Transactions on Information Forensics and Security, Vol. 1, no. 3, September 2006.

[8]. Qinghai Gao "A Preliminary Study of Fake Fingerprints" I.J. Computer Network and Information Security, 2014, 12, 1-8 Published Online November 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.12.01

[9]. Arunalatha G. and M. Ezhilarasan "Spoof Detection of Fingerprint Biometrics using PHOG Descriptor" International Science Press, I J C T A, 9(3), 2016, pp. 1705-1711.

[10]. Dr. Chander Kant, Raksha "Spoof Attack Detection in Fingerprint Authentication using Hybrid fusion" IJCSCIJ Volume 4, 1 March 2013 pp. 59-64.

[11]. Devakumar et al., International Journal of Advanced Research in Computer Science and Software Engineering 7(3), March- 2017, pp. 70-76

[12]. Heeseung Choi, Raechoong Kang, Kyungtaek Choi, and Jaihie Kim "Aliveness Detection of Fingerprints using Multiple Static Features" International Science Index, Computer and Information Engineering Vol:1, No:4, 2007 waset.org/Publication/3945

[13]. Lekshmy. S. Mohan Joby James "Fingerprint spoofing detection using local binary pattern and Hog" ijastems-issn: 2454-356x) Volume.3, Special Issue.1, April.2017.

[14]. Shankar Bhausaheb Nikam and Suneeta Agarwal "Texture and Wavelet-Based Spoof Fingerprint Detection for Fingerprint Biometric Systems" First International Conference on Emerging Trends in Engineering and Technology, 2008.

[15]. Shankar Bhausaheb Nikam, Suneeta Agarwal "Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection" International Journal of Information and Computer Security Volume 3 Issue 1, June 2009.

[16]. Aditya Abhyankar and Stephanie Schuckers "Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques" IEEE International Conference on Image Processing, 2006, DOI: 10.1109/ICIP.2006.313158.

[17]. P. Venkata Reddy et. al. "A New Method for Fingerprint Antispoofing using Pulse Oxiometry" First IEEE International Conference on Theory, Applications, and Systems, 2007, 10.1109/BTAS.2007.4401916.

[18]. Mojtaba Sepasian, Cristinel Mares, Wamadeva Balachandran "Vitality Detection in Fingerprint Identification" Wseas Transactions on Information Science and Applications, Issue 4, Volume 7, April 2010.

[19]. Reiko Iwai, Hiroyuki Yoshimura "A New Method for Improving Robustness of Registered Fingerprint Data Using the Fractional Fourier Transform" Int. J. Communications, Network and System

Sciences, 2010, 3, 722-729 doi:10.4236/ijcns.2010.39096

[20]. R.Sowmiya, C.Dhivya,B.Nandhini, and T.Anand "Image quality assessment using Biometric Liveness Detection for fake Fingerprint" International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 08 Nov-2015.

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