JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN ELECTRONICS AND COMMUNICATION ENGINEERING
ISSN: 0975 – 6779| NOV 16 TO OCT 17 | VOLUME – 04, ISSUE – 02

A STUDY OF FINGERPRINT LIVENESS DETECTION TECHNIQUES

[1]*S.R.LOKARE*, [2]*Dr. S.O.RAJANKAR*

[2]*Professer E&TC Department, SCOE, Pune*

[1, 2] **Department of Electronics and Telecommunication Engineering, Sinhgad College of Engineering, Savitribai Phule Pune University, Vadgaon (Bk.), Pune–411041, Maharashtra, India.**

sagar.lokare12@gmail.com sorajankar.scoe@sinhgad.edu

ABSTRACT :
We propose static software based programming approach in which only one single image feature sets are required. We propose to combine low level inclination highlights from Speeded-up Robust Features (SURF), pyramid extension of the Histograms of Oriented Gradient (PHOG) and surface elements from Gabor Wavelet using dynamic score level blend. The features extracted from these components of single image equally perform well on different fingerprint sensors. We remove these components from a solitary unique mark picture to beat the issues faced in dynamic software based programming approaches which require customer joint effort and longer computational time. Test examination done on LivDet 2011 data created a normal Equal Error Rate (EER) of 3.95% more than four databases. Also experiments performed on LivDet 2013 data achieved an average classification error rate (ACE) of 2.27%.

KEY WORDS: Fingerprint liveness, Low level Gradient Features, Textural features, Error rate, ACE.

1. INTRODUCTION

It is due to the possibility of making fake fingerprints for authentication purpose, there is a requirement of liveness detection of a fingerprint images. Among biometric systems, fingerprints systems are probably the best-known and widespread because of the fingerprint properties: universality, durability and individuality. Unfortunately it has been shown that fingerprint scanners are vulnerable to spoof attacks means it is possible to deceive a fingerprint system with an artificial replica of a fingertip. Therefore, it is important to develop countermeasures to those attacks. Liveness detection, with either hardware-based or software-based systems, is used to check if a presented fingerprint originates from a live person or an artificial finger.

Usually the result of this analysis is a score used to classify images as either live or fake.In a static programming based approach, a client is just required to place his/her finger on the sensor for a short duration of time in an undedicated way for a single image capture. A large portion of the works in fingerprint liveness identification utilizes a single feature set based approach. For example, the works in fingerprint liveness detection competition engineer's the feature extracted from a particular material for distinguishing fake fingerprint. Based on our investigation, we verify that a single feature set from a single classifier is deficient to perform comparably over various databases which are recorded utilizing distinctive fingerprint sensors. This is because distinctive sensors catch data in an unexpected way. In addition, various materials such as gelatin based fake fingerprint may not create similar features as compared to other materials, for example, latex or wood-stick. This is because fake fingerprints show distinctive intensity gradient and ridge shape because of the thickness of material utilized. The way toward making fake fingerprint also presents air bubbles.
Furthermore, it is not practical for the authentication system to have earlier information of the sorts of material used to make the fake fingerprint in genuine situations. In our method the fusion of features extracted from SURF, PHOG and GABOR WAVELET distinguishes well between live and fake fingerprints. Our proposed method performs well on all open source databases acquired from different fingerprint sensors.

The rest of the paper is organized as follows; in section II we discuss the need of liveness detection algorithm and system. In section III the related work is discussed. In section IV we analyze the existing methods and their drawbacks. In section V we present the proposed method. Finally in section VI we summaries our work and conclude the same.

II. MOTIVATION

The possibility to spoof a fingerprint based verification framework makes the need to build up a technique which can recognize live and fake fingerprint images. Both hardware and software based methodologies can be utilized to understood.

III. RELATED WORK

"Liveness Detection", a procedure used to decide the vitality of a submitted biometric, has been executed in fingerprint scanners in recent years. In the last recent years important research efforts have been concentrate the vulnerabilities of biometric frameworks to direct attacks to the sensor (did utilizing manufactured biometric characteristics, for example, sticky fingers or amazing iris printed pictures), and indirect attacks (completed against a portion of the internal modules of the framework).As Liveness Detection method is divided into two approaches i.e. hardware based approach and software based approach.

1) HARDWRAE BASED APPROACH

Hardware based approach requires finger's odor, temperature, oximetry, pulse etc., for that it requires the many additional devices. This approach also requires user's cooperation to measure the different variations of an image. It is costlier than software based approach.

The authors Denis Baldisserra and Annalisa Franco [7] proposed a new approach in fingerprint liveness detection to discriminate between real and fake images that is the acquisition of an odor analysis by means of electronic nose. An odor sensor (electronic nose) is used to sample the odor signal and an ad-hoc algorithm allows discriminating the finger skin odor from that of other materials such as latex, silicone or gelatin, usually employed to forge fake fingerprints. A chemical sensor is used to detect the odorants. For this work the promising sensor (FIGARO TGS 2600) is used which achieves EER of 7.48%.The drawback of this method is that it is more costlier and requires one user to deal with hardware.

P.V. Reddy and A. Kumar [9] proposed method for fingerprint liveness detection based on the principle of pulse oximetry and involves the source of light originating from a probe at two wavelengths. The light is partly absorbed by haemoglobin, by amounts which differ depending on whether it is saturated with oxygen or deoxygenated haemoglobin. We then perform the computations for the absorption at two wavelengths to estimate the proportion of haemoglobin which is oxygenated. The computed percentage of oxygen in the blood, along with the heart pulse rate, determines the liveness of the enrolled biometric. This technique relies on the physiological behavior of the arterial blood volume and oxygen saturation level changes (principle of pulse oximetry). The oxygen saturation level of arterial blood $S_pO_2\%$ is measured and used to ascertain the liveness decision from the presented biometric sample.

2) SOFTWARE BASED APPROACH

"L. Ghiani, D. Yambay and V. Mura"[1] proposed the fingerprint liveness detection based on software pogramming approach. This paper refers with the third international public competition for software-based fingerprint liveness detection and the second public assessment of system-based fingerprint liveness detection, proved to be an important competition. This competition was done for comparing both hardware and software based approaches. The number of participants, from both academic and industrial institutions, is growing with respect to previous editions. As a matter of fact entries were submitted from a total of ten participants demonstrating the state-of-the art in fingerprint liveness detection. Since an effective liveness detection algorithm is a key component to minimize the vulnerability of fingerprint systems to spoof attacks. In this paper recognition was done in two parts, Part 1: Algorithms and Part 2: System. The main advantage of this competition is that, it is open to all academic and industrial institutions. This LivDet 2013 database is used to perform experiments by confirming different sensors.

"D. Yambay and L. Ghiani" [3] proposed the different algorithms and systems based on LiveDet 2011. This paper refers to LivDet 2011 is the second international public competition for software-based fingerprint liveness detection and first public assessment of system-based fingerprint liveness detection. Entries were submitted from a total of five participants demonstrating the state-of-the art in fingerprint liveness. LivDet 2011 evaluates (1) Software applicable to four fingerprint sensors represented in the training data as well (2) Embedded hardware/software systems for liveness detection specialized to a specific fingerprint sensor. The best results shown were by Dermalog Algorithm in Part 1 and Dermalog again in Part 2. It is hoped that this competition will be continued in order to continually understand and promote the state of the art in liveness detection. Results of this competition are not reflective of performance for spoof attacks not included in this study. Creating effective liveness detection methodologies is an important step in minimizing the vulnerability of spoof attacks. This competition is used to minimize the vulnerability of spoof attacks. It is referred that features extracted from specific material for detecting fake fingerprint.

"Javier Galbally and Fernando Alonso-Fernandez" [4] proposed the novel fingerprint parameterization for liveness detection based on quality related measures has been proposed. The feature set has been used in a complete liveness detection system, and tested on two publicly available databases: (i) The database used in the 2009 LivDet competition, and (ii) The database captured at the ATVS group. These two challenging databases permit to test the proposed liveness detection scheme under totally different operational scenarios in terms of the technology used by the acquisition devices (flat optical, flat capacitive, and sweeping thermal), material with which the gummy fingers are produced (gelatin, silicone and playdoh), and procedure followed to generate the fake fingers. This method is proven to be robust to the multi-sensor. The analysis of the skin perspiration through the Image Quality was done in this paper. But drawback is, an input fingerprint image has to be assigned to one of two classes: real or fake.

"Emanuela Marasco and Carlo Sansone" [5] proposed the static software measures of single image are used to counteract with the drawbacks of dynamic software method. Before authors work, the morphological and perspiration based features are used separately to authenticate the liveness of fingerprint image. Both Morphological and Perspiration based features are combined to detect the liveness of a fingerprint image. It was shown that the feature selection process that choses the best feature set among the other features for each fingerprint sensor. It was noted from this paper that Average classification error is just 9.70% on Identix Database. It also examines the vitality by separately measuring the morphological and perspiration based features. So this method has proven to be an best method when there is detection of images takes place on the basis of perspiration.

"Jia Jia, Lianhong Cai and Kaifu Zhang"[14] proposed the method for fingerprint liveness detection based on the elasticity produced by the skin of an fingers. True fingerprints have greater elasticity than the falsely made fingerprints. In this paper, liveness detection was done by measuring the elasticity of fingerprint image skin. This method requires time series of images to be taken on sensor and great user cooperation. Discrimination was made on the basis of signal intensity of correlation coefficient of finger image and standard deviation of same. Fisher Linear Discriminant is used classify live and fake images. This method achieves an Equal Error Rate (EER) of 4.78%.

"Bozhao Tan and S. Schuckers" [8] proposed the new method which applies wavelet transform on the ridge signal extracted along the fingerprint images is proposed to detect liveness. Results show that it is possible for the capacitive DC and optical scanners to detect vitality using a single fingerprint based on the perspiration pattern specific to the live fingers. The method is purely software based and application of this liveness detection method can protect fingerprint scanners from spoof attacks. This method provides Fingerprint vitality authentication. It requires only live fingers for enrollment and authentication.

"Aditya Abhyankar and Stephanie Schuckers"[13] proposed the liveness detection method based on level 3 fingerprint features. Fingerprint features can be divided into level- 1, level-2 and level-3 categories, representing coarser to fine representation. Level-2 features, mainly minutiae points i.e ridge endings and bifurcations are the most studied fingerprint pointers and are used by most fingerprint matchers for recognition. Level-3 features are the least studied features and include pores, incipient ridges, line shapes, deformations, warts, scars and so forth. Although level-3 features require the capturing resolution to be very high for accurate detection, they effectively provide finer information about fingerprints. Level-3 features may provide more information in order to perform accurate authentication. In this study, fingerprint pores along the ridges are used for fingerprint matching. Wavelet based fingerprint enhancement techniques are implemented to ease detection of the level-3 features. This improved method achieves an equal error rate (EER) of 2.97%.

IV. EXISTING SYSTEM

Liveness detection has been an active research over the last several years. It has been proven that it is possible to spoof standard optical and capacitive sensors. 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, oximetry, etc.

DISADVANTAGES

They require an end user to interact with the additional hardware. On the other hand, software based methodologies don't utilize extra obtrusive biometric estimations. However, these methodologies are all the more difficult as they require the distinguishing proof of discriminative features to differentiate between fake and live fingerprint images.

V. PROPOSED SYSTEM

As illustrated in Fig. 1, we observe that it is extremely hard to outwardly separate amongst live and fake fingerprints. Although the difference in the pixel intensity of the gray-scale of the live and fake fingerprints image is hard to see, this distinction can be measured by figuring the mean and standard deviation estimations of the gray level image. Also, based on visual observation, there is more sweat pores in the live fingerprint as compared to the fake fingerprint images. Motivated by these minute differences,the configuration of low level components that can speak to separating attributes amongst live and fake fingerprints. The proposed method uses the Speeded up robust features (SURF) and Pyramid Histogram of Gradient (PHOG) to capture the gradient features of an fingerprint images which are obtained on different capacitive and dc sensors. Textural features are obtained by using Gabor Wavelets.

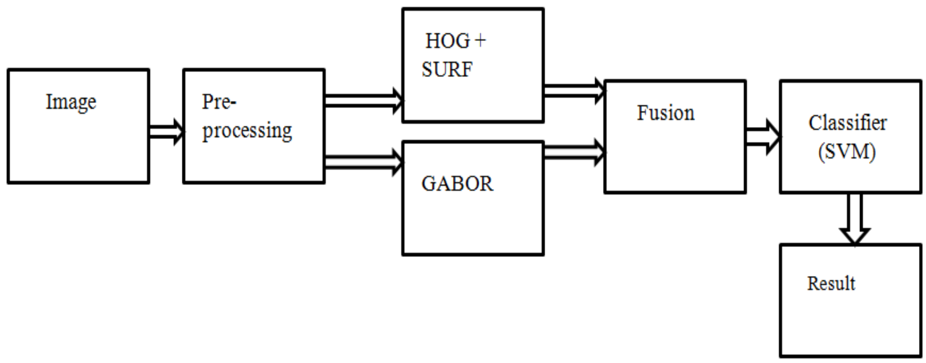

Fig 1:- Proposed System Architecture

First take the fingerprint image, then preprocessing takes place on that image, we improved the nature of the image by first trimming the fingerprint region in the image and afterward performing histogram equalization to increase the perception information. Figure 2. shows the block diagram of preprocessing.

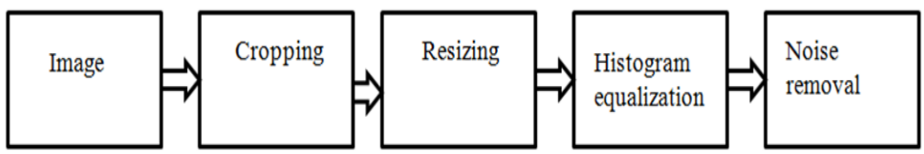

Fig 2:- Block Diagram of Preprocessing

The second stage is Feature Extraction Stage, in fingerprint validation frameworks; the image is generally captured from numerous subjects utilizing distinctive scanners. In this way, fingerprint images are typically found to be of different scales and turns. In certain situations, the fingerprint images are partially captured because of human mistakes. In order to obtain features that are invariant to these problems, we utilize different components that catch properties of live fingerprint images. We use the HOG and SURF .We chooses to use SURF as it is invariant to illumination, scale and rotation. HOG captures the force angles and edge directions to describe the shape and appearance in an image. We also use Gabor Wavelet to extract features from fingerprint images for texture analysis. Third stage is the Image Classification Stage. In this stage we use SVM classifier for the use of classification.

VI. CONCLUSION

In this paper, we make the review of different methods of Fingerprint Liveness Detection by surveying different Hardware and Software approaches. We proposed a novel technique for fingerprint liveness detection by joining low level elements, which include gradient features from SURF, PHOG, and texture features from Gabor wavelet. In addition, a powerful element score level integration module is proposed to join the outcome from the two individual classifiers. We did investigate two most prominently utilized databases from LivDet rivalry 2011 and 2013.
We investigate the use of local discriminative feature space on live and spoof fingerprint by using PHOG, SURF, GABOR and their combinations. Experiments performed on six sensors demonstrate that the combination of PHOG and SURF always works better than PHOG and SURF individually for LivDet 2011 and 2013 databases. This indicates that descriptors complement each other. Good recall rates

(accuracy). Features are robust to occlusion and clutter. This method is relatively efficient compared to older algorithms.

REFERENCES

[1]. L. Ghiani, D. Yambay, V. Mura, S. Tocco, G.L. Marcialis, F. Roli, and S. Schuckcrs, "Livdet 2013 fingerprint liveness detection competition 2013," in Biometrics (ICB), 2013 International Conference on, June 2013, pp. 1–6.

[2] A.K. Jain, "Next generation biometrics," in Department of Computer Science & Engineering, Michigan State University, Department of Brain & Cognitive Engineering, Korea University, 10 Dec 2009.

[3]. D. Yambay, L. Ghiani, P. Denti, G.L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011; fingerprint liveness detection competition 2011," in Biometrics (ICB), 2012 5th IAPR International Conference on, March 2012, pp. 208–215.

[4].Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generation Computer Systems, vol. 28, no. 1, pp. 311 – 321, 2012.

[5]. Emanuela Marasco and Carlo Sansone, "Combining perspiration- and morphology-based static features for fingerprint liveness detection," Pattern Recogn. Lett., vol. 33, no. 9, pp. 1148–1156, July 2012.

[6]. Reza Derakhshani, Stephanie A.C. Schuckers, Larry A. Hornak, and Lawrence O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," Pattern Recognition, vol. 36, no. 2, pp. 383 – 396, 2003, Biometrics.

[7]. Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni, "Fake fingerprint detection by odor analysis," in *Advances in Biometrics*, David Zhang and AnilK. Jain, Eds., vol. 3832 of *Lecture Notes in Computer Science*, pp. 265–272. Springer Berlin Heidelberg, 2005.

[8]. Bozhao Tan and S. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," in Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on, June 2006, pp. 26–26.

[9]. P.V. Reddy, A. Kumar, S. Rahman, and T.S. Mundra, "A new antispoofing approach for biometric devices," Biomedical Circuits and Systems, IEEE Transactions on, vol. 2, no. 4, pp. 328–337, Dec 2008

[10]. Shankar Bhausaheb Nikam and Suneeta Agarwal, "Ridgelet-based fake fingerprint detection," Neurocomput., vol. 72, no. 10-12, pp. 2491–2506, June 2009.

[11]. Yangyang Zhang, Jie Tian, Xinjian Chen, Xin Yang, and Peng Shi, "Fake finger detection based on thin-plate spline distortion model," in Advances in Biometrics, Seong-Whan Lee and StanZ. Li, Eds., vol. 4642 of Lecture Notes in Computer Science, pp. 742–749. Springer Berlin Heidelberg, 2007.

[12]. A. Antonelli, R. Cappelli, Dario Maio, and Davide Maltoni, "A new approach to fake finger detection based on skin distortion," in Proceedings of the 2006 International Conference on Advances in Biometrics, Berlin, Heidelberg, 2006, ICB'06, pp. 221–228, Springer-Verlag.

[13]. A. Abhyankar and S. Schuckers, "Towards in integrating level-3 Features with perspiration pattern for robust fingerprint recognition," Proceedings of 2010 IEEE 17th International Conference on Image Processing September 26-29, 2010, Hong Kong.

[14]. Jia Jia, Lianhong Cai, Kaifu Zhang, and Dawei Chen, "A new approach to fake finger detection based on skin elasticity analysis," in *Advances in Biometrics*, Seong Whan Lee and StanZ. Li, Eds., vol. 4642 of *Lecture Notes in Computer Science*, pp. 309–318. Springer Berlin Heidelberg, 2007.