A Survey on Fingerprint Liveness Detection Using Gradient and Texture Features

P.Shanthi [#1] and R.Madhumathi [*2]

[#]*Research Scholar,Department of Computer Science,Sakthi College of Arts and Science for Women,
Oddanchatram, India*

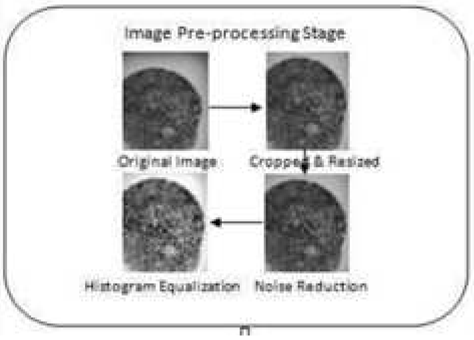
[*] *Assistant Professor, Department of Computer Science, Sakthi College of Arts and Science for
Women,Oddanchatram,India*

***Abstract*— Since, today, a wide and variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Biometric cannot be borrowed, stolen, or forgotten, and forging one is practically impossible. Fingerprints are the only basis for individual identification by biometric authentication process. Password based authentication systems are very very less secure than that of the fingerprint authentication where fingerprints and Iris are the only 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, I take a survey on a static software approach that combines all sorts of fingerprint features.**

***Index Terms*—Fingerprint liveness, low level features, Gabor filters, texture analysis, Biometric Security.**

I. Introduction

Biometrics is earlier 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.



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.

II. LITERATURE REVIEW

Manju Kulkarni ,Harishchanddra Patil [1] explained that fingerprint scanning was the one biometric identification technique presented these days that was frequently used. The security of fingerprint scanners had conversely been questioned and it had been shown that fingerprint scanners could be misleaded effortlessly, using easy, cheap techniques with artificial fingerprints. This work meant to explain liveness detection technique by means of first order texture features. The "Fin key Hamster" scanner artificial by "Nitgen Biometric solution, Korea", having 500 dpi resolution was utilized for this reason. To develop the database, live fingerprint of 20 persons were considered and their equivalent gummy finger by means of gelatin was made. The images were accumulated in the form of template which was created using image processing techniques. The steps comprise histogram equalization, binarisation, thinning, minutiae detection and false minutiae elimination. They developed Matching algorithm by using Euclidean distance technique. The developed algorithm for liveness was then incorporated. The consequences established perfect separation of live and not live for the normal conditions. False Rejection Ratio (FRR) was designed for genuine-live users and False Acceptance Ratio (FAR) was for genuine-not live, imposter-live and imposter-not live and obtained within acceptable range.

Ana F. Sequeira and Jaime S. Cardoso [2] suggested that, fingerprint liveness detection methods had been developed as an attempt to overcome the vulnerability of fingerprint biometric systems to spoofing attacks. Traditional approaches had quite optimistic about the behavior of the intruder assuming the use of a previously known material. This assumption was led to the use of supervised techniques to estimate the performance of the methods, using both live and spoof samples to train the predictive models and evaluate each type of fake samples individually. In addition to, the background was often included in the sample representation, completely distorting the decision process. Therefore, they proposed that an automatic segmentation step be supposed to perform to isolate the fingerprint from the background and truly decided on the liveness of the fingerprint and not on the characteristics of the background. Also, they argued that one couldn't aim to model the fake samples completely since the material used by the intruder was unknown beforehand. They approached the design by modeling the distribution of the live samples and predicting as fake the samples very unlikely according to that model. The experiments compare the performance of the supervised approaches with the semi-supervised ones that rely solely on the live samples. The results obtained differ from the ones obtained by the more standard approaches which reinforced their conviction that the results in the literature were misleadingly estimating the true vulnerability of the biometric system.

Sajida Parveen et. al. [3] described that in recent years, facial biometric systems received increased deployment in various applications such as surveillance, access control and forensic investigations. However, one of the limitations of face recognition system was the high possibility of the system being deceived or spoofed by non-real faces such as photograph, video clips or dummy faces. In order to identify the spoofing attacks on such biometric systems, face liveness detection approaches had been developed. Thus, the current approach was to integrate liveness detection within facial biometrics by using life sign indicators of individual features. This article presented a review of state-of-the-art techniques in face liveness detection, which were classified into two groups, namely intrusive and non-intrusive approaches. Here, each technique was discussed in terms of its implementation, strengths and limitations, as well as indications on possible future research directions that can be studied.

Emanuela Marasco and Arun Ross [4] discussed that several issues related to the vulnerability of fingerprint recognition systems to attacks had been highlighted in the biometrics literature. One such vulnerability involved the use of artificial fingers, where materials such as play-doh, silicone, and gelatin were inscribed with fingerprint ridges. Researchers have demonstrated that some commercial fingerprint recognition systems could be deceived when these artificial fingers were placed on the sensor, i.e., the system successfully processed the ensuing fingerprint images thereby allowing an adversary to spoof the fingerprints of another individual. However, at the same time, several countermeasures that discriminated between live fingerprints and spoof artifacts have been proposed. While some of these anti-spoofing schemes were hardware-based, several software-based approaches had been proposed as well. Here, they reviewed the literature and presented the state-of-the-art in fingerprint anti-spoofing.

Y. Chung and M. Yung [5] explained that recent studies had shown that the conventional fingerprint recognition systems were vulnerable to fake attacks, and there were many existing systems that needed to update their anti-spoofing capability inexpensively. They proposed an image quality-based fake detection method to address this problem. Three effective fake/live quality measures, spectral band energy, middle ridge line and middle valley line, are extracted firstly, and then, these features were fused and tested on a fake/live dataset using SVM and QDA classifiers. Experimental results demonstrated that the proposed method was promising in increasing the security of the existing fingerprint authentication system by only updating the software.

III. METHODOLOGY

A. 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.

B. 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.

C. 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. 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.

D. 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.

IV. CONCLUSION

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.

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] 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.

[7] 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

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

[9] 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

[10] 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.

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

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

[13] 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

[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.