I J C T A, 9(3), 2016, pp. 1705-1711

Spoof Detection of Fingerprint Biometrics using PHOG Descriptor

Arunalatha G.* and M. Ezhilarasan**

Abstract: Biometrics are used for authentication. It isused to recognize a person based on their unique characteristics. Among several biometrics, Fingerprint is the most widely used and acceptable biometrics. Biometric system has several advantages over traditional methods. But it can be affected by several attacks. In this paper type 1 attack is discussed which is performed at the sensor level. Differentiating a genuine biometric input from fake input is known as Spoof detection. The local features of fingerprint are extracted using Pyramid Histogram of Oriented Gradients image descriptor. It is used to detect whether fingerprint is real or fake.

Keywords: fingerprint, spoofing, spoof, detection, HOG, PHOG

1. INTRODUCTION

Biometrics refers to recognition of people by measuring physiological characteristics such as your hand geometry, iris and fingerprint behavioral characteristics such as signature, voice and gait. A biometric system consists of 5 modules. The sensor module is used to get input from the user. The feature extractor module extracts the features form the input image. The template database stores the enrolled templates. The matcher module cpmpares the input with database templates. The decision modules gives the final result gets input from individual, A biometric system can operate in one of the two modes:Verification mode or Identification mode: In the verification mode, the system checks a person's identity by comparing the biometric data with her own biometric template stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually by a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to find whether the claim is true or not. Verification is used for positive recognition, where the aim is to prevent multiple people from using the same identity. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. So the system conducts a one-to-many comparison to establish an individual'sidentity without the subject having to claim an identity. Identification is a critical component in negative recognition applications where the system establishes whether the person is who he denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience. While traditional methods of personal recognition such as passwords, keys, PINs and tokens may work for positive recognition, negative recognition can only be established through biometrics. There are seven basic criteria for biometric security system: uniqueness, universality, collectability, performance, permanence, acceptability and circumvention. Uniqueness indicate how uniquely and differently the biometric system will be able to recognize each user among groups of users. Universality indicates requirements for unique characteristics of each human being in the world which cannot be replicated. Permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will be affected by the age of the user. The collectability parameter requires the

* Research Scholar, Dept. of CSE Pondicherry Engineering College Puducherry, India, *Email: arunalathamaha@gmail.com*

** Professor, Dept. of Information Technology Pondicherry Engineering College Puducherry, India, *Email: mrezhil@pec.edu*

collection of each characteristic and trait by the system in order to verify their identification. Performance outlines how well the security system works. The robustness and accuracy are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable. Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process.

The rest of the paper is organized as follows: Section II gives a brief overview of Spoof detection systems. Section III presents the proposed system design for Spoof detection using PHOG. Section IV gives the classifier. Section V gives experimental results. Finally, Section VI concludes the paper.

2. SPOOF DETECTION

2.1. Biometric System Attacks

There are two types of attacks in biometric system [1]. I). Direct attacks. (type1) II). Indirect attacks. Direct attack can be carried out in the sensor level. To perform direct attack, knowledge is not necessary. To avoid direct attacks spoof detection techniques are used to differentiate between fake and real biometric input. Example presenting fake biometrics at the sensor: In this mode of attack, a possible biometric feature is reproduced and it is presented as input to the system. Examples include a fake finger, a copy of a signature, or a face mask. Type 2-Resubmitting previously stored digitized biometrics signals: In this mode of attack, a recorded signal is given to the system, bypassing the sensor. Examples include the presentation of an old copy of a biometric data or the presentation of a previously recorded audio signal. Type 3-Overriding the feature extraction process: The feature extractor is attacked using a Trojan horse. It produces feature sets preselected by the intruder. Type 4-Tampering with the biometric feature representation: The biometric features extracted from the input signal are replaced with a different set of fraudulent feature. Type 5-Corrupting the matcher: The matcher is attacked and corrupted to produce preselected match scores Type 6-Tampering with stored templates: The database of stored templates could be either remote or local. The data are distributed over several servers. The attacker can try to modify the templates in the database. It results in either a fraudulent individual is authorized or access is denied to the persons associated with the corrupted template.

Type 7-Attacking the channel between the stored templates and the matcher: The stored database templates are sent to the matcher through a communication channel. The data travelling through this channel can be modified and intercepted. Type 8-Overriding the final decision: If the final match decision can be overridden by the hacker, then the authentication system has been disabled. Although the actual pattern recognition framework has excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the match result. The various types of attacks for biometric system are shown in figure 1.

Differentiating a genuine biometric input from fake input is known as spoof detection. Spoof detection is a measure that determines whether or not the source of the image presented to a biometric sensor is from a living individual. The main reason for conducting spoof detection signs in fingerprint biometrics is to ensure that the sensor is capturing an image from real fingertip. It provides an extra level of security to the biometric system by working cooperatively with a matching algorithm that recognizes an enrolled user.

The methods for spoof assessment represent a challengingengineering problem as they have to satisfy certain requirements. (i) non-invasive, the technique should in no case penetrate the body or present and excessive contact with the user; (ii) fast, results should be produced in very few seconds as the user cannot be asked to interact with the sensor for a long period of time; (iii) user friendly, people should not be hesitant to use it;(iv) performance, it should not degrade the recognition performance of the biometric

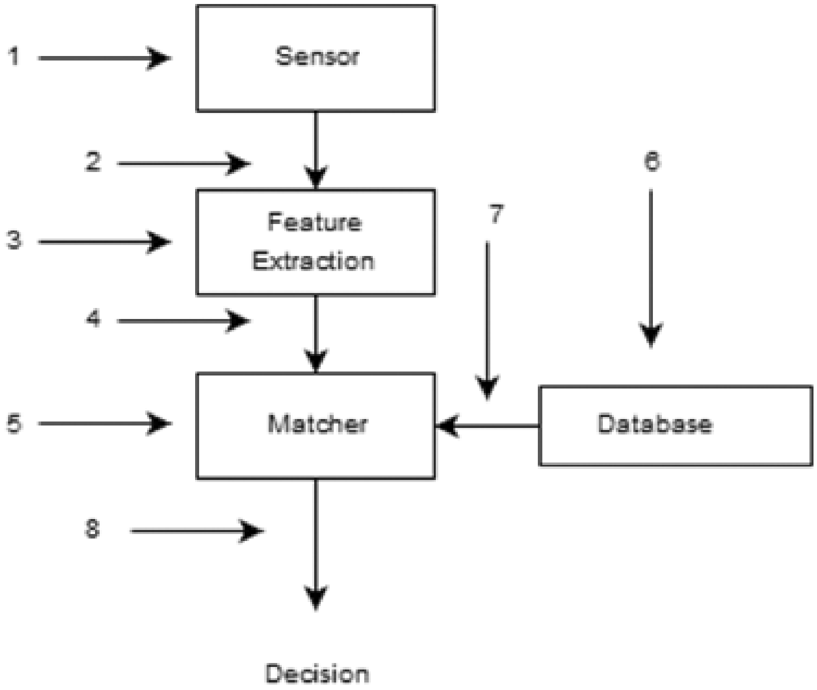

Figure 1: Attacks on Biometric System.

system. (v) low cost, a wide use cannot be expected if the cost is very high; There are two types of techniques for spoof detection. (i) Software-based techniques: In this type, no special hardware device is added to the sensor. The biometric features extracted from the feature extractor are used to distinguish between real and fake biometric input. (ii) Hardware-based techniques: In this type a special hardware device is added to detect whether the biometric input is real or fake.

2.2. Fingerprint Spoof Detection

Fingerprint is a pattern of ridges and valleys on fingertip. The fingerprint image is shown in figure 2. The fake fingerprint can be made from gelatin, clay, play-doh, silicone, latex, rubber etc. with user's cooperation or without cooperation.

In general, a fake fingerprint image does not have a good quality as a live one. The important idea to detect spoof by checking quality was implemented in [2]. A fast and convenient wavelet-based algorithm based on the computation of the standard deviation of the fingerprint image is proposed.

Spoof detection based on wavelet features is proposed [3]. The coefficients are altered using the zoom-in property of the wavelets. Wavelet packet analysis and multiresolution analysis are used to get information from high frequency and low frequency content of the images respectively. Daubechies wavelet is implemented for wavelet analysis. This algorithm is tested for training set and it differentiates live fingerprints from fake fingerprints.

A wavelet based approach to detect spoofis integrated with the fingerprint matcher [4]. Spoof is determined from perspiration changes in the fingerprint ridges. The proposed algorithm is applied to a data set of approximately 58 live, 28 cadaver and 50 spoof fingerprint images. This system of fingerprint matcher and spoof module reduces EER to 0:03%.

Direct attacks are evaluated for fake fingers that are generated from ISO templates [5]. Fingerprint image is reconstructed from minutiae templates to perform vulnerability evaluation against direct attacks by fake fingers. The evaluation of the ISO matcher is done with FVC2006 DB2 Database. Three quality measures based on ridge clarity and ridge strength are evaluated.

Figure 2: Fingerprint Image.

Spoof detection using texture features is proposed in [6]. The first order statistics such as entropy, energy, median, variance, kurtosis, skewness and coefficient of variations are measured to detect the fake fingerprint. This method produces False Reject Rate as 5.1 and False Acceptance rate as 7.69.

A new spoof detection method for fingerprint images is proposed [7]. The live fingers have a clear ridge-valley structure. But fake fingers have a distinct noise distribution because of the material's properties when placed on a biometric scanner. Using wavelet decomposition technique, statistical features are extracted in multiresolution scales. Based on these features, spoof detection is performed using neural networks and classification trees. This method produced approximately 90.9-100% classification of spoof and live fingerprints.

In [8] Fingerprint spoof detection based on quality measures for software based method is proposed. From feature extractor fingerprint quality measures based on ridge strength, ridge clarity and ridge continuity are extracted. The Feature vector is taken from best quality features. Fingerprint is classified as fake or real using classifier. The performance of the method is evaluated on databases LivDet 2009 and ATVS group. This method correctly classifies maximum 90% of the fingerprint images. The optimal ACE value is 6.56%.

A new method by combining ridge signal and valley noise analysis is proposed for spoof detection in fingerprint sensors [9]. This method estimates perspiration patterns along ridges in live images and noise patterns along valleys in spoof images. The signals representing grey level patterns along ridges and valleys are explored in frequency, spatial and wavelet domains. Based on these features, separation between live and spoof images is performed using standard pattern classification tools including neural networks and classification trees. This method produces an EER of 0.9% for an optical scanner.

A novel fake fingerprint identification method using multiple static features is presented [10]. These features extracted from one image are used determine the spoof of fingerprints. The power spectrum, ridge thickness, directional contrast, ridge signal and histogram of each fingerprint image are used as static features. The proposed method produces an EER of approximately 0% for capacitive sensor and 1.6% for optical sensors.

Distortions due to the rotation and pressure of the finger on a sensor produce different elastic characteristics of the materials. Spoofing can be detected by comparing these distortions through static features. The elastic deformation occurs by the contact of the fingertip with a plane surface was studied in [11], since a fake fingerprint presents different deformations than a real fingerprint. The elastic behavior was analyzed for a live and a fake finger by using a mathematical model relying on the extraction of a specific and ordered set of minutiae points.

3. PYRAMID HISTOGRAM OF ORIENTED GRADIENTS

Histogram of oriented gradients (HOG) [12] is a feature descriptor used in computer vision and image processing for the purpose of object detection. Histogram of oriented gradient (HoG) descriptors are used to capture information about the gradient orientations in localized areas of an image. To get this descriptor divide the image into small connected partitions called as cells. Then find magnitude of orientation of pixels. For each cell sobel mask is used to obtain local 1 D histogram of gradient directions. Finally the normalized histograms are combined together to form the features for an image. HOG is limited as it only accounts for the orientation of individual pixels, without regards to the spatial distribution of the image.

Pyramid of Histogram of Oriented Gradients [13]are used for better representation of the spatial relationship of the oriented gradients. The objective of the Pyramid Histogram of Oriented Gradient (PHOG) is to take the spatial property. The PHOG image descriptor is a concatenation of all the HOG vectors, each of which is computed for each grid cell at each pyramid. Consequently, level 0 is represented by K-bin histogram, level 1 is represented by a 4K bin histogram, etc., and the final PHOG descriptor of the entire image is a vector with dimensionality. For example, for levels up to L= 1 and K= 30 bins it will be a 150-vector. Each bin in the histogram represents the number of edges that have orientations within a certain angular range. The number of points in each grid cell is then recorded. This is a pyramid representation because the number of points in a cell at one level is simply the sum over those contained in the four cells it is divided into at the next level. The cell counts at each level of resolution are the bin counts for the histogram representing that level.

Algorithm:

1. Find Gradient values.
2. Compute a matrix for histogram value
3. Compute another matrix for gradient value
4. Region of Interest is extracted.
5. Number of pyramid levels and number of bins are specified.
6. Calculate sum of gradient values for all the bins.
7. Calculate sum of gradient values for all the Pyramid levels.

4. CLASSIFIER

The SVM is a powerful classifier with an excellent generalization capability that provides a linear separation in an augmented space by means of different kernels. The kernels map input data vectors onto a high-dimensional space where a linear separation is more likely, and this process amounts to finding a non-linear frontier in the original input space.

5. EXPERIMENTAL RESULTS

The database used in the experiments is the development set provided in the Fingerprint Liveness Detection Competition, LivDET 2009. It comprises three datasets of real and fake fingerprints (generated with different materials) captured each of them with a different optical sensor.

The Biometrika FX2000 (569 dpi) dataset comprises 520 real and 520 fake images. The fake images were generated with gummy fingers made of silicone. The CrossMatch Verifier 300CL (500 dpi) dataset comprises 1,000 real and 1,000 fake images. The fake were generated with gummy fingers made of silicone (310), gelatin (344), and playdoh (346). The Identix DFR2100 (686 dpi) dataset comprises 750 real nd 750 fake images. The fake images were generated with gummy fingers made of silicone (250), gelatin (250),

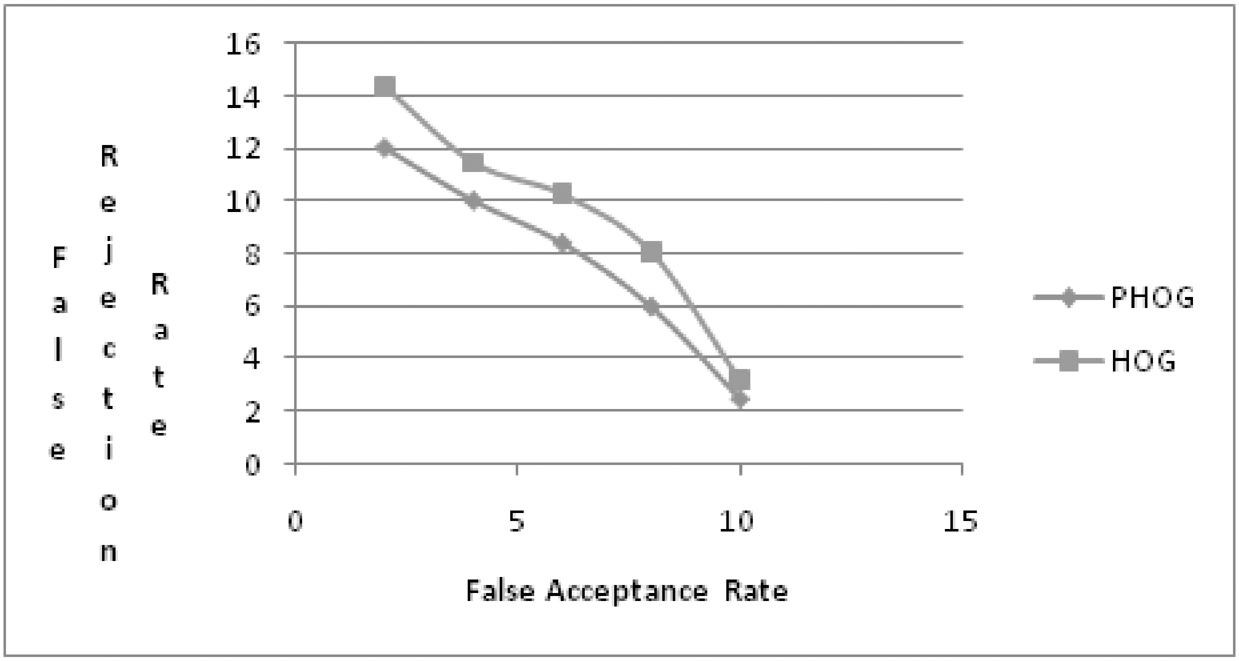

Figure 3: Comparison of Pyramid Histogram of Oriented gradients with Histogramof Oriented Gradients

and playdoh (250). The material with which the different fake images are made is known. These fakes were created using the consensual method: a volunteer put his finger on a mould of plasticine like material,

For each algorithm we calculated the False Rejection Rate (FRR) that is the value for which the percentage of misclassified live fingerprints. False Acceptance Rate (FAR) is equal to the percentage of misclassified fake fingerprints.

6. CONCLUSION

Biometrics identify people by measuring physiological characteristics. Biometric system has several advantages over traditional methods. But it can be affected by several attacks. In this paper the type1 attack is discussed which is performed at the sensor level. Differentiating a genuine biometric input from fake input is known as Liveness detection. The local features of fingerprint are extracted using Pyramid Histogram of Oriented Gradients image descriptor. It is used to detect whether fingerprint is real or fake.

References

[1] U. Uludag and Anil K. Jain, Attacks on biometric systems: A case study in fingerprints, Proc. SPIE, 5306: 622– 633(2004).

[2] K. C. Chan, K. So, Y. S. Moon, J. S. Chen and K. So Woo, Wavelet based fingerprint vitality detection. Electronic Letters, 41(20):1112–1113 (2005).

[3] AdityaAbhyankara and Stephanie Schuckersa, A wavelet based approach to detecting vitality in fingerprint scanners, SPIE Proceedings, 5404: 278–286 (2004).

[4] Aditya Abhyankar and Stephanie Schuckers, Integrating a wavelet based perspiration vitality check with fingerprint recognition, Pattern Recognition, 42: 452–464 (2009).

[5] Galbally Javier, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de-Rivera DavideMaltoni, Julian Fierrez, Javier Ortega-Garcia and Dario Maio, An evaluation of direct attacks using fake fingers generated from ISO templates, Pattern Recognition Letters, 31: 725–732(2010).

[6] Ankita Chaudhari and P. J. Deore, Spoof attack detection in fingerprint biometric system using histogram features, Proc. World Journal of Science and Technology, 2(4): 108–111 (2012).

[7] Tan and S. Schuckers, A New Approach for Vitality Detection in Fingerprint Scanners Based on Valley Noise Analysis, Journal of Electronic Imaging, 17(1): 011009-1 to 011009-9 (2008).

[8] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez and Javier Ortega-Garcia, A high performance fingerprint vitality detection method based on quality, Future Generation Computer Systems, 28: 311–321 (2012).

[9] B. Tan and S. Schuckers, Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise, Pattern Recognition, 4(8): 2845–2857 (2010).

[10] Heeseung Choi, Raechoong Kang, Kyoungtaek Choi, Andrew, TeohBeng Jin and Jaihie Kim, Fake-fingerprint detection using multiple static features, Proc. Optical Engineering (2009).

[11] A. Jain, Y. Chen and S. Dass, Fingerprint deformation for spoof detection. Biometric Symposium, (2005).

[12] Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In:Proceedings of the 2005 IEEE Computer Society Conference on Computer Visionand Pattern Recognition (CVPR 2005), Washington, DC, USA, vol. 1, pp. 886–893 (2005).

[13] Bosch, A., Zisserman, A., Munoz, X.: Representing shape with a spatial pyramidkernel. In: International Conference on Image and Video Retrieval, Amsterdam, July 9-11, pp. 401–408 (2007).